

Alma Mater Studiorum – Università di Bologna  
In collaborazione con LAST-JD consortium:  
Università degli studi di Torino  
Universitat Autònoma de Barcelona  
Mykolas Romeris University  
Tilburg University

**DOTTORATO DI RICERCA IN**

**Erasmus Mundus Joint International Doctoral Degree in Law,  
Science and Technology**

Ciclo 29 – A.Y. 2013/2014

**Settore Concorsuale di afferenza: 12H3**

**Settore Scientifico disciplinare: IUS20**

**TITOLO TESI**

**Knowledge Production from Social Network Sites  
- Using Social Media Evidence in the Criminal Procedure**

---

**Presentata da: Chih-Ping Chang**

**Coordinatore**

**Prof. Giovanni Sartor**

**Relatore**

**Prof. Dr. Alberto Artosi  
CIRSFID, University of Bologna, Italy**

**Co- Relatore**

**Prof. Dr. Giovanni Ziccardi  
University of Milan, Italy**

**Esame finale anno 2018**

Alma Mater Studiorum – Università di Bologna  
in partnership with LAST-JD Consortium  
Università degli studi di Torino  
Universitat Autònoma de Barcelona  
Mykolas Romeris University  
Tilburg University

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in Law,  
Science and Technology  
Cycle 29 – a.y. 2013/14

**Settore Concorsuale di appartenenza: 12H3**

**Settore Scientifico disciplinare: IUS20**

(Title of the Thesis)

Knowledge Production from Social Network Sites  
- Using Social Media Evidence in the Criminal Procedure

---

Submitted by: Chih-Ping Chang

The PhD Programme Coordinator  
Prof. Giovanni Sartor

Supervisor (s)

Prof. Dr. Alberto Artosi  
CIRSFID, University of Bologna, Italy  
Prof. Dr. Giovanni Ziccardi  
University of Milan, Italy

**Year 2018**

## **Abstract**

This thesis focuses on the interaction between social network sites (SNS) and the legal system, trying to answer a specific question, that is, through introducing social media evidence, whether there is a change of finding facts and identifying the truth in criminal proceedings. To achieve the research objectives, three sub-topics should be discussed in turn; first, how can we transform information on social network sites to valuable evidence in court? In this part, the research will explore the proceedings of extracting information on SNS, such as posts, photos, check-in on Facebook etc., in order to use as evidence in the courtroom from the perspectives of law and internet forensic. Second, considering characteristics of these social media evidence, e.g. easy to be copied, deleted, tampered and transmitted, is it necessary to separate from evidence obtained through other technology or forensic science? Should the legal system need a new set of regulation on social media evidence? Third, how can we conquer challenges to core values in legal system, such as the privilege against self-incrimination or expectation of innocent in this digital era? As the positive contribution, this research tries to answer whether social network sites are a convenient tool for criminal prosecution, and whether internet forensics is useful to assist the investigational authority accusing the crime and finding the truth more accurately, to achieve the ultimate goal of the criminal procedure?

# Table of Contents

<b>INTRODUCTION.....</b>	<b>- 11 -</b>
<b>RESEARCH MOTIVATIONS .....</b>	<b>- 11 -</b>
<b>1. A START FROM A SIMPLE CASE, WHICH MIGHT HAPPEN DAILY .....</b>	<b>- 11 -</b>
<b>2. PRIVACY CRISIS? .....</b>	<b>- 14 -</b>
<b>3. INTERACTIONS BETWEEN THE LAW AND SCIENCE.....</b>	<b>- 19 -</b>
3.1 Negligence in Forensic Process .....	- 20 -
3.2 Paradigm Shift and New Objectivity.....	- 23 -
<b>RESEARCH QUESTIONS .....</b>	<b>- 27 -</b>
<b>METHODOLOGY.....</b>	<b>- 29 -</b>
<b>STRUCTURE OF THIS THESIS .....</b>	<b>- 31 -</b>
<b>CHAPTER 1 SOCIAL MEDIA EVIDENCE .....</b>	<b>- 38 -</b>
<b>1. DEFINITION .....</b>	<b>- 38 -</b>
1.1 Social Network Sites.....	- 39 -
1.1.1 Structure of Social Network Sites.....	- 41 -
1.1.2 Characteristics.....	- 42 -
1.2 Social Media .....	- 44 -
1.3 Social Media Evidence.....	- 45 -
<b>2. TYPES AND FORMATS OF SOCIAL MEDIA EVIDENCE.....</b>	<b>- 46 -</b>
<b>3. ACQUISITIONS (HOW TO GET IT?) .....</b>	<b>- 47 -</b>
3.1 Computer Forensics .....	- 48 -
3.2 Digital Forensics .....	- 48 -
3.3 Network/ Internet Forensics.....	- 49 -
<b>4. TYPES OF EVIDENCE IN LEGAL SYSTEMS .....</b>	<b>- 50 -</b>
4.1 Digital Evidence.....	- 51 -
4.2 Scientific Evidence .....	- 52 -
4.3 Social Media Evidence.....	- 54 -
<b>5. OTHER SIMILAR CHARACTERISTICS WITH DIGITAL EVIDENCE .....</b>	<b>- 54 -</b>
5.1 Vulnerable to Tampering.....	- 55 -
5.2 Possible to Recovery .....	- 55 -
5.3 Unlimited to Copy.....	- 56 -
5.4 Hard to Identify .....	- 57 -
5.5 Cannot directly to Sense or Understand by Human .....	- 58 -

5.6 Difficult to Collect ..... - 59 -

5.7 Dependence on the Environment ..... - 59 -

6. SUMMARY ..... - 60 -

**CHAPTER 2 SOCIAL MEDIA EVIDENCE IN CRIMINAL PROCEDURE ..... - 64 -**

**SECTION 1 DIFFERENCE BETWEEN TAIWAN AND AMERICAN LEGAL SYSTEM .....- 64 -**

**1. RULE OF EVIDENCE IN AMERICA..... - 65 -**

**2. RULE OF EVIDENCE IN TAIWAN ..... - 66 -**

**SECTION 2 AMERICAN LAW.....- 67 -**

**3. DISCOVERABILITY OF EVIDENCE ..... - 70 -**

3.1 Rules for Search and Seizure ..... - 72 -

3.1.1 The Standard: Reasonable Expectation of Privacy ..... - 72 -

3.1.2 Operation Rules of Search on Social Network Sites..... - 73 -

3.2 Obtain Evidence from Public Domain ..... - 76 -

3.3 Search with a Warrant ..... - 78 -

3.3.1 Probable Cause..... - 78 -

3.3.2 Requirement of Particularity ..... - 79 -

3.4 Exceptions for the Search without Warrant..... - 82 -

3.4.1 Search with Subject’s Consent ..... - 82 -

3.4.1.1 Consent..... - 83 -

3.4.1.2 Scope of Consent ..... - 84 -

3.4.1.3 The Third Party Consent ..... - 85 -

3.4.2 Exigent Circumstances..... - 87 -

3.4.3 Plain View Doctrine ..... - 90 -

3.4.4 Search Incident to Lawful Arrests..... - 91 -

**4. ADMISSIBILITY OF EVIDENCE ..... - 93 -**

4.1 Federal Rules of Evidence ..... - 94 -

4.2 Relevancy..... - 95 -

4.3 Hearsay..... - 96 -

4.3.1 A Statement Made by A Person Outside the Courtroom..... - 96 -

4.3.2 The Statement Is Offered for the Truth of the Matter Asserted..... - 97 -

4.3.3 An Exception of the Hearsay Rule..... - 97 -

4.4 Authentication..... - 98 -

4.5 The Best Evidence Rule ..... - 99 -

4.6 Character Evidence ..... - 102 -

**SECTION 3 TAIWANESE LAW..... - 105 -**

**1. THE BASIC PRINCIPLES OF EVIDENCE LAW ..... - 105 -**

1.1	Principle of Evidentiary Adjudication.....	- 105 -
1.2	Principle of Strict Proof/ Strengbeweis.....	- 106 -
1.3	Principle of Judicial Discretion/ freie Beweiswürdigung .....	- 107 -
1.4	Basic Concepts of Evidence Law.....	- 109 -
1.4.1	Admissibility/ Beweisfähigkeit.....	- 109 -
1.4.2	The Probative Value of Evidence .....	- 110 -
1.4.3	Hearsay.....	- 111 -
<b>2.</b>	<b>OBTAINING SOCIAL MEDIA EVIDENCE.....</b>	<b>- 113 -</b>
2.1	Rules for Search and Seizure .....	- 114 -
2.1.1	Purposes and Threshold .....	- 115 -
2.1.2	Proceedings and Manners of Implement.....	- 117 -
2.1.2.1	Application on Social media evidence/ digital evidence .....	- 119 -
2.1.3	Issues on Search with Warrant .....	- 122 -
2.1.4	Disposal after Seizure .....	- 126 -
2.2	Exceptions for the Search without Warrant.....	- 127 -
2.2.1	Search with Subject's Consent .....	- 127 -
2.2.1.1	The concept and scope of consent.....	- 128 -
2.2.1.2	The third party's consent .....	- 129 -
2.2.1.3	Consent from internet Service Provider or web server administrators .....	- 130 -
2.2.2	Exigent Circumstances.....	- 130 -
2.2.3	Search Incident to Lawful Arrest .....	- 132 -
2.3	Discussions.....	- 134 -
2.3.1	Is it enough to replace the warrant with subpoena to ask the party submitting digital evidence? .....	- 134 -
2.3.2	The object of traditional search and seizure is limited to physical objects.....	- 135 -
2.3.3	Dilemma of warrant for searching digital evidence .....	- 137 -
2.3.3.1	Establishing the necessity and the Probable Cause .....	- 137 -
2.3.3.2	The validity and specificity of the search warrant issued.....	- 138 -
2.3.4	Restrictions on warrantless search.....	- 140 -
<b>3.</b>	<b>ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE .....</b>	<b>- 141 -</b>
3.1	Social Media Evidence as Documentary Evidence.....	- 143 -
3.1.1	Documentary Evidence and its Investigation Procedure.....	- 143 -
3.1.2	Differences between Digital Evidence and Traditional Documentary Evidence.....	- 147 -
3.1.2.1	About data storage .....	- 147 -
3.1.2.2	Data preservation .....	- 148 -
3.1.2.3	Forms of presentation.....	- 148 -
3.1.3	Investigating Social Media Evidence.....	- 149 -
3.1.3.1	Social Media Evidence and Nature of Document .....	- 149 -

3.1.3.1.1 Possible1: Social media evidence is considered as the document.....	- 149 -
3.1.3.1.2 Possible 2: Social media evidence is different from documentary evidence.....	- 151 -
3.1.3.1.3 Possible 3: Social media evidence is similar to documentary evidence.....	- 152 -
3.1.3.2 Applicable Effect .....	- 154 -
3.1.3.3 Discussion .....	- 156 -
3.2 Social Media Evidence as Real Evidence .....	- 160 -
3.3 Summon an Expert Witness .....	- 162 -
3.3.1 Internet Forensics .....	- 163 -
3.3.2 Necessity of Summoning an Expert Witness .....	- 165 -
3.3.3 Steps of Forensics .....	- 166 -
3.3.4 Report.....	- 168 -
3.3.5 Challenges of Digital Forensics .....	- 169 -
3.3.5.1 Identity .....	- 169 -
3.3.5.2 Tampering .....	- 173 -
3.3.5.3 Reliability.....	- 173 -
3.3.5.4 Authorship.....	- 175 -
3.4 Make an Inspection .....	- 175 -
3.4.1 The Rule .....	- 176 -
3.4.2 Still Images/Photos .....	- 177 -
3.4.3 Voice Recording .....	- 179 -
3.4.4 Motion Pictures / Video .....	- 181 -
3.5 Discussion .....	- 184 -
3.5.1 Substitution among Evidence Methods.....	- 184 -
3.5.1.1 Forensics and inspection.....	- 184 -
3.5.1.2 Documentary evidence and investigation.....	- 187 -
3.5.1.3 Summary .....	- 188 -
3.5.2 Social Media Evidence Used as an Independent Evidence Type? .....	- 189 -
<b>4 PROBATIVE VALUE OF EVIDENCE .....</b>	<b>- 191 -</b>
4.1 The Rule.....	- 193 -
4.1.1 Rule of Experience.....	- 193 -
4.1.2 Rule of Logic .....	- 195 -
4.1.3 Rule of Evaluation .....	- 196 -
4.2 Judging the Probative Value of Social Media Evidence.....	- 197 -
4.2.1 The Application of Natural Science in the case of using Digital Evidence .....	- 199 -
4.2.2 Posts, Comments and Messages.....	- 201 -
4.2.3 Still Images/Photos .....	- 202 -
4.2.4 Voice Recording .....	- 203 -
4.2.5 Motion Pictures / Video .....	- 204 -

SUMMARY ..... - 205 -

**CHAPTER 3 EXTRACTING INFORMATION FROM SOCIAL NETWORK SITES ... - 214 -**

**SECTION 1 PRINCIPLES OF NETWORK FORENSICS ..... - 214 -**

**1. THE DEVELOPMENT OF PRINCIPLES OF DIGITAL FORENSICS ..... - 215 -**

**2. DISPUTE ON WHETHER TO ACCESS THE ORIGINAL DATA ..... - 219 -**

2.1 Do not access the original data..... - 220 -

2.2 Allow to assess the original data..... - 221 -

2.3 Practitioners are required to determine whether they have access to the original evidence..... - 225 -

2.4 Discussion ..... - 230 -

2.4.1 Traditional Forensic Science does not require practitioners to preserve but not to change the original exhibits. .... - 230 -

**3 ADJUSTMENT OF THE PRINCIPLES..... - 231 -**

**SECTION 2 FORENSIC TOOL FOR EXTRACTING INFORMATION..... - 234 -**

**1. DISK BACKUP SOFTWARE..... - 235 -**

**2. RECOVERY SOFTWARE ..... - 235 -**

**3. PASSWORD CRACKING TOOLS ..... - 235 -**

**4. FORENSIC TOOLKITS..... - 235 -**

4.1 EnCase ..... - 236 -

4.2 The Corner's Toolkit (TCT)..... - 236 -

4.3 Access Data's Forensic Toolkit (FTK)..... - 237 -

**5. OTHER TOOLS..... - 239 -**

**SECTION 3 PERFORMING THE FORENSIC PROCESS ..... - 240 -**

**1. PRESERVATION OF SME ..... - 240 -**

1.1 Identification of Evidence..... - 240 -

1.2 Backup of Evidence ..... - 240 -

**2. INVESTIGATION OF SME ..... - 241 -**

2.1 The Hidden Evidence..... - 241 -

2.2 Computer Search..... - 242 -

2.3 Trojan Defense ..... - 243 -

**3. CRIME SCENE RECONSTRUCTION ..... - 244 -**

3.1 Presentation of SME in Court ..... - 244 -

**4. DEFSOP (DIGITAL EVIDENCE FORENSIC STANDARD OPERATION PROCEDURE) - 245 -**

4.1 Phase 1: Building conceptions ..... - 245 -

4.2 Phase 2: The Preparation..... - 246 -

4.2.1	Authorization .....	- 246 -
4.2.2	Information Security Policy .....	- 247 -
4.2.3	Data Collection .....	- 247 -
4.2.4	Identification .....	- 247 -
4.2.5	Task Group .....	- 247 -
4.3	Phase 3: The Operation .....	- 248 -
4.3.1	Collection .....	- 248 -
4.3.2	Analysis .....	- 248 -
4.3.3	Forensics .....	- 248 -
4.4	Phase 4: The Report .....	- 249 -
4.4.1	Making a Report .....	- 249 -
4.4.2	Verifying Forensic Results .....	- 249 -
4.4.3	Preparation to Court .....	- 250 -
4.4.4	Filing and Learning .....	- 250 -
	<b>SECTION 4 POINTS TO TRANSFORM TO SOCIAL MEDIA EVIDENCE.....</b>	<b>- 252 -</b>
<b>1.</b>	<b>DIGITAL EVIDENCE VERIFIED BY HASH VALUE.....</b>	<b>- 252 -</b>
1.1	Meaning of Hash Value Verification .....	- 253 -
<b>2.</b>	<b>QUALITY ASSURANCE FOR DIGITAL EVIDENCE LABORATORIES .....</b>	<b>- 254 -</b>
2.1	Personnel .....	- 255 -
2.2	Environment and Facilities .....	- 255 -
2.3	Operating procedures .....	- 256 -
2.4	Method Verification .....	- 256 -
<b>3.</b>	<b>FORMAT OF FORENSIC REPORT.....</b>	<b>- 257 -</b>
<b>4.</b>	<b>CRIMINAL DEFENSE CHALLENGES IN COMPUTER FORENSICS.....</b>	<b>- 258 -</b>
	<b>SUMMARY .....</b>	<b>- 259 -</b>

**CHAPTER 4 SME, A PROCESS FROM INFORMATION TO EVIDENCE..... - 265 -**

<b>1.</b>	<b>COMPARISON BETWEEN LEGAL AND TECHNICAL SYSTEMS.....</b>	<b>- 265 -</b>
1.1	Technical Process to Form the Social Media Evidence .....	- 266 -
1.2	Legal Process to Form and Use the Social Media Evidence.....	- 266 -
1.3	The Comparison.....	- 267 -
<b>2.</b>	<b>ARGUMENTS IN THE COURT .....</b>	<b>- 268 -</b>
2.1	Disputes .....	- 268 -
2.1.1	When the social media evidence has been formed, whether the computer hardware and software was normal.....	- 268 -
2.1.2	Obtaining evidence is illegal. ....	- 269 -
2.1.3	There is a dispute about the legally preserved and identified.....	- 269 -

2.1.4 The actual production (criminal) person is questioned.....	- 269 -
2.1.5 Social media evidence has been tampered. ....	- 270 -
2.1.6 The printout or the representation of social media evidence may show a sense of error. .	- 270 -
2.2 Strategies .....	- 271 -
2.2.1 Source of evidence .....	- 271 -
2.2.2 Acquisition of evidence.....	- 271 -
2.2.3 Authorship of social media evidence .....	- 272 -
2.2.4 Digital evidence format.....	- 272 -
2.2.5 Digital evidence content.....	- 273 -
2.2.6 The time when social media evidence was established.....	- 273 -
2.2.7 The way that social media evidence presented at court .....	- 274 -
<b>3. THE ORIGINAL.....</b>	<b>- 275 -</b>
<b>4. IDENTITY .....</b>	<b>- 276 -</b>
<b>5. AUTHORSHIP .....</b>	<b>- 277 -</b>

**CHAPTER 5 COPY THE VIRTUAL WORLD: AUTHENTICITY OF SOCIAL MEDIA WEBSITE PRINTOUTS ..... - 280 -**

<b>SECTION 1 PRINTOUTS AND THE AUTHENTICATION ISSUE .....</b>	<b>- 282 -</b>
<b>1. THE VERY COMMON MEAN TO PRESENT IN THE COURTROOM.....</b>	<b>- 282 -</b>
<b>2. THE PROBLEM IS AUTHENTICATION.....</b>	<b>- 282 -</b>
<b>3. THE CONSTRUCTION OF THE AUTHENTICATION ISSUE .....</b>	<b>- 282 -</b>
<b>SECTION 2 SOLUTION IN LEGAL APPROACH .....</b>	<b>- 285 -</b>
<b>1. THE BASIC RULE.....</b>	<b>- 285 -</b>
<b>2. ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE IN LITIGATION .....</b>	<b>- 288 -</b>
2.1 Griffin v. Maryland .....	- 289 -
(1) The Case .....	- 289 -
(2) The Social Media Evidence at Issue.....	- 289 -
(3) The Court’s Reasoning .....	- 289 -
(4) The Comment .....	- 290 -
2.2 Commonwealth v. Williams .....	- 291 -
(1) The Case .....	- 291 -
(2) The Social Media Evidence at Issue.....	- 291 -
(3) The Court’s Reasoning .....	- 291 -
(4) The Comment .....	- 292 -
2.3 Tienda v. Texas.....	- 293 -
(1) The Case .....	- 293 -

(2) The Social Media Evidence at Issue.....	- 293 -
(3) The Court’s Reasoning .....	- 294 -
(4) The Comment.....	- 295 -
<b>3. THE STANDARD.....</b>	<b>- 295 -</b>
3.1 The Maryland Approach .....	- 296 -
3.2 The Texas Approach.....	- 297 -
3.3 Discussion .....	- 297 -
<b>SECTION 3 RECONSTRUCTION OF THE PRINTOUTS ISSUE.....</b>	<b>- 300 -</b>
<b>1. HOW TO PROVE A=A’ .....</b>	<b>- 301 -</b>
1.1 Original Electronic Evidence .....	- 301 -
1.2 Presenting Electronic Evidence at Trial .....	- 302 -
<b>2. LAW’S KNOWLEDGE OF SCIENCE .....</b>	<b>- 303 -</b>
<b>3. IN CONCLUSION, A RELATIVE REAL .....</b>	<b>- 305 -</b>

**CHAPTER 6 CONNECT THE VIRTUAL TO A REAL WORLD: THE ISSUE OF TROJAN DEFENSE .....** **- 311 -**

<b>SECTION 1 A BACKGROUND OF THE TROJAN DEFENSE .....</b>	<b>- 312 -</b>
<b>1. DEFINITION OF THE TROJAN.....</b>	<b>- 312 -</b>
1.1 Malware .....	- 312 -
1.2 Trojan .....	- 313 -
1.3 Rootkit.....	- 314 -
<b>2. DIGITAL EVIDENCE PRODUCED .....</b>	<b>- 315 -</b>
<b>3. TROJAN HAS THE NATURE OF OCCULT .....</b>	<b>- 316 -</b>
<b>4. WHAT THE TROJAN CAN DO .....</b>	<b>- 318 -</b>
<b>SECTION 2 TECHNICAL ISSUES .....</b>	<b>- 321 -</b>
<b>1. TROJAN SCENARIO.....</b>	<b>- 321 -</b>
1.1 Scenario 1.....	- 321 -
1.2 Scenario 2.....	- 321 -
1.3 Considering Volatile Evidence .....	- 322 -
<b>2. STANDARD OPERATING PROCEDURE .....</b>	<b>- 322 -</b>
2.1 Detecting the Trojan.....	- 323 -
2.2 Digital Forensics of Digital Activities.....	- 324 -
2.3 What to Do When Malware is Found.....	- 324 -
2.4 What to Do When Malware is not Found .....	- 325 -
<b>3 OTHER FORENSIC SOLUTIONS.....</b>	<b>- 326 -</b>
3.1 The Stepwise Discriminant Analysis .....	- 326 -
3.2 The Event Reconstruction Process.....	- 328 -



**2. ISSUE OF THE TROJAN DEFENSE..... - 380 -**  
**LEGAL MODEL TO REPRESENT THE PAST FACTS..... - 382 -**  
**BIBLIOGRAPHY ..... - 386 -**

**Table of Figures**

Figure 1 Ontology of Social Media Evidence..... - 38 -  
Figure 2 Evidential Materials filtering process..... - 68 -  
Figure 3 Search and Seizure under the 4th Amendment..... - 73 -  
Figure 4 Admissibility ..... - 107 -  
Figure 5 Negative condition- Beweisverbote ..... - 110 -  
Figure 6 Evidence review process ..... - 111 -  
Figure 7 Obtaining evidence process in forensic science ..... - 215 -  
Figure 8 The order of volatility in computer system..... - 222 -  
Figure 9 Digital Evidence Forensic Standard Operation Procedure (DEFSOP)-  
251 -  
Figure 10 The comparison of forensic and legal obtaining evidence process -  
268 -  
Figure 11 Analysis of SME legal issues ..... - 275 -  
Figure 12 Legal issues of social media evidence ..... - 283 -  
Figure 13 The way to judge the Trojan case..... - 334 -  
Figure 14 SME, a process from information to evidence..... - 375 -

# **Introduction**

## **RESEARCH MOTIVATIONS**

### **1. A Start from a Simple Case, Which Might Happen Daily**

In 2012, a Taiwanese notorious gang kidnapped a businessman for ransom with huge sum, but the victim's family could not pay the ransom. After several negotiations, kidnappers released the hostage to exchange money and a Mercedes-Benz. These gang members were quite cautious, and normally used pseudonyms and prepaid cards to contact each other, so the police neither got well information about these members and their connections, nor catch them immediately. However, around two weeks later, a policeman found one photo of this Benz from an ex-convict's Facebook, which the police was continuing to monitor him for a long term after he served his sentence. Then this policeman discovered the ex-convict's posts, photos, list of friends, comments and everything he put on his Facebook. In the meanwhile, the policeman continued tracking this suspect's activities. Finally the police uncovered this gang. This photo was used as a conclusive evidence to prove this ex-convict's participation of the kidnapping. While this may seem like an extreme example, the use of information from Facebook and other social network sites is becoming an important part of police investigations and criminal litigation.

This is a story about a smart police used Facebook as the investigative tool, found information as evidence, and finally punished the bad guys. For another case, a defendant in Kentucky, U.S., was jailed after he posted a photo of himself siphoning gas from a police car onto Facebook. The photo circulated through the town of 2,000, and before long, the defendant was charged with theft for unlawful tanking and spent the night in the slammer. After being released, the defendant posted this on his page:

“yea lol i went too [sic] jail over Facebook.”<sup>1</sup>We can find cases everywhere every day. There are countless cases involving defendants who are arrested because of information, photos, or admissions posted to social network sites. These stories let us realize that, what you put on your Facebook will become evidence to charge you one day, although social network sites were originally designed to connect your social network, exchanging thoughts, actions, feelings, interests and information among them. Someone may doubt these defendants careless and guilty, and we are responsible for what we posted or have done, and for protecting our privacy. But it is not fair that we give up using an imaginary, virtual social networking site, to exchange for the safety of personal privacy. In this internet era, using social network sites should not be a zero-sum game. Thus, some question arises.

Since social network sites were built as virtual communities and encourage users to create their virtual world and online social networks, why the government investigators can unbridled search and seizure information inside for criminal evidence, and charge the user with his own produced information? Will it be the invasion of privacy, if the government investigators arbitrarily access and obtain information from social network sites? If the user has made the privacy setting to limited information sharing, will it be the invasion of privacy, that the government investigators gather information on the users social network sites through another way, such as being a fake friend or cooperating someone happened to be his “Facebook friends”? Is there an issue of self-incrimination that the legal authorities use his own produced information to charge his crime? With high risks of being hacked, and easy to tamper or impersonate, is it possible the defendant didn’t post child pornography photos on the websites, but actually some other man did it, and how to argue and

---

<sup>1</sup> Eric Larson, 8 Dumb Criminals Caught Through Facebook, MASHABLE (Dec. 12, 2012), <http://mashable.com/2012/12/12/crime-social-media>

prove? Is it proper that the prosecutor directly printout Facebook pages with/without modify the content (ex. Cut the advertisement at the age of pages), or they select some information, copy and paste the content of some pages in a word file, and print them as evidence to present at the trial? Is this printout authentic? In a trial, the prosecutor obviously can directly interrogate the defendant or witness, but he has replaced by a Facebook printout and a police officer's testimony. Is the prosecutor's conduct against the right to confront cross-examination guaranteed by the constitution? In fact, a social network site doesn't have the content review mechanism; it relies on users report to regulate inappropriate or illegal contents. Postings on social network sites, in other words, may be fictional, but why we, especially being a prosecutor in a criminal case, rather believe these postings are facts, being true, instead of being virtual, fictions?

These questions reflect conflicts between the law and science, when a new technology is introduced into the legal system. They focus on the response of legal system and whether it is appropriate. Generally speaking, the privacy issue is always first raised, when a new technology is introduced into the legal system. This is because the innovation of science and technology will overturn the original world that people have acknowledged. On the issue of social network sites, such a communication platform breaks the wall, literal and conceptual, originally used to separate private and public space. Moreover, the legal system often borrows from the objectivity of science to build reliability of evidence. The main purposes of criminal proceedings are to reconstruct the past case, to identify the perpetrators, and to give their offenses appropriate punishments. This reconstruction of the past case is built by evidence. Science itself is such a system to explain the truth, and it is useful for the legal system using this nature of science to reconstruct the past fact. Especially the characteristic of social network site, it disclosures the defendant's motivation and

builds the connection between offenses and the criminal, which is the hardest part to prove in the criminal proceeding; moreover, it visualizes them. A visualized motivation is easy to convince the jury that the defendant is guilty, based on the most important rule of thumb developed by the natural science, "Seeing is Believing." However, does it really so stable, using scientific methods or technology as a means of proof? We will further discuss issue of privacy, and issues of interaction between the law and science below.

## **2. Privacy Crisis?**

With the rapid development of social network sites, investigating authorities increasingly accustomed to take advantages of information on the social network sites as a direction or means for the crime investigation. As the real case in Taiwan, the Police found the relationship between gang members and constructed a membership list from one suspect's Facebook interactive mode in the theft case, even though these suspects tried to get into contact without using phone, deliberately to avoid the Police finding clues by records of calls. Actually the Police more often use a pseudonym on Facebook to monitor a particular community, through adding the Facebook friends of them and collecting messages and reactions they have done. Another specific case occurred in the United States, in which a 19-year-old Florida woman, Rachel Stieringer, was investigated by the Florida Department of Children and Families, when she posted what she thought a humorous photo of her 11-month-old baby holding a bong on Facebook. Then the cops threw her in jail for processing drug paraphernalia. German media also reports, by means of opening the surveillance video of one Frankfurt murder scene on Facebook, the Police cracked this case very well because someone over the network provides clues to identify the murderer. In addition, since 2011, the Police in Lower Saxony have established a dedicated

Facebook account to publish the information of crime and suspects. People are encouraged to clue and inform the crimes, suspects, and even hints, by phone or e-mail. According to an online survey in 2012,<sup>2</sup> which are about 1221 federal, state and local law enforcement officers who use social media, the result shows that four out of five investigators used social media to gather intelligence during investigations. Half said they checked social media at least once a week, and the majority said social media helps them solve crime faster. Obviously, most investigators usually use Facebook as their first or favorite tool, as case studies show. Even in the courtroom, judges and juries now need to put more attention on social media evidence, since the police and prosecutors prefer information extracted from social network sites.

Due to the popularity and prevalence of social network sites, there is a multitude of information stored online and on third party servers. Users of social network sites have become accustomed to posting information depicting every minute detail of their lives, allowing friends and families to communicate easily and often. Status updates, personal information, and photographs loaded onto social media websites have become important sources of discovery in litigation, as these sources make it easier and cheaper to obtain information than ever before. However, courtroom use of information from Facebook and other popular websites often happens largely unbeknownst to users. Hence, some scholars worried, while E-discovery is an important tool for litigators, what privacy interests are we giving up for the use of this information?

In United States of America, the police's investigation should conform to requests of the 4th amendment, which guarantees people's privacy and even self-expression and self-identification.<sup>3</sup> When getting this object or document (including information

---

<sup>2</sup> This online survey was conducted by LexisNexis Risk Solutions and had a 2.8% margin of error. Heather Kelly, Police embrace social media as crime-fighting tool, CNN News, August 30, 2012.

<sup>3</sup> See Warshak, 631 F.3d at 286.

discovered on SNS) into evidence, the prosecutor needs to let it pass three stages asked by rules of evidence, which is relevancy<sup>4</sup>, authenticity<sup>5</sup> and non-exclusionary<sup>6</sup>. According to these rules, that photo showing suspect with the stolen car could be adopted by judge, if it was obtained under legal procedures, because it presents that the suspect drove the car after it was stolen, and this photo is ensured by technology of Photography. Obviously, these regulations and rules all concern one situation: that is when the state forced into the private sphere. Therefore, the main issue is changing from “should this photo be used as evidence” to “whether using this photo intervenes in the suspect’s privacy”.

U.S. Supreme Court<sup>7</sup> held that once the information is exposed to the public, the person possibly no longer has a reasonable expectation of privacy. In the case of *Romano v. Steelcase, Inc.*, the court indicated clearly, because the most important function of SNS is sharing personal lives on the internet, there was no reasonable expectation of privacy.<sup>8</sup> German Federal Constitutional Court<sup>9</sup> recognized there is no fundamental right to be interfered involved in this issue, when the police obtained the information from public internet and open communications. The court also recognized another exception, in which the police directly participate in public communication networks and obtain something as evidences from there. No fundamental right to be interfered either.

Opposition stances mostly focused on privacy issue and address redrawing the boundaries of public and private sector. Some scholar, like Lori Andrews (2011), she

---

<sup>4</sup> “The evidence must have a tendency to make the existence of any fact that is of consequence to determination of action more or less probable than it would be without the evidence.” See FED. R. EVID. 401-402.

<sup>5</sup> “The evidence must be what the proponent claims it to be.” See FED. R. EVID. 901(a).

<sup>6</sup> The evidence must not be subject to an exclusionary rule, such as Rule 404(a) or Rule 802.

<sup>7</sup> *Katz v. United States*, 389 U.S. 347 (1967).

<sup>8</sup> Lawrence Morales, Social media evidence: “what you post or tweet can and will be used against you in court of law”, 60 *The Advoc. (Texas)* 32, 33-34.

<sup>9</sup> BVerfG, Urteil vom 27.2.2008.

states the information privacy should guarantee the activities unfold through social networks, which called as “the second self”, and provides as sufficient as normal safeguard of personality in real. For endeavoring to assure and strengthen “the second self”, she claims information privacy theory should admit social networks are private spaces in advance, in order to consolidate the functions of information privacy.<sup>10</sup> In addition, the privacy is a kind of abilities that people can choose which parts in this domain can be accessed by others, and can control the extent, manner and timing of the use of those parts they choose to disclose. Helen Nissenbaum (2009) also tries to redefine privacy to give this issue a solution. She proposes “Privacy as Contextual Integrity” theory, which means personal information protection should follow different situations and conditions, and apply different norms according to the context. They are try to redefine boundary between public and private, in order to response that common point<sup>11</sup> shared by courts.

Meanwhile, legal scholars also notice fundamental rights will possibly be infringed in this situation, while the Police or prosecutors want to investigate or suit people according to the evidences from suspects’ SNS. For example, if a prosecutor suits the suspect by using his post-on messages or photos against him, this will cause a controversy about whether the self-incrimination principle is applied or not.<sup>12</sup> If a law enforcement agent use a pseudonym on Facebook in order to explore the potential criminal behaviors, his activities is restricted by entrapment, which is a possible defense against criminal liability. And like the Lower Saxony Police, who publish the offenders’ information on its own Facebook encouraging people to provide clues,

---

<sup>10</sup> In addition, the privacy is a kind of abilities that people can choose which parts in this domain can be accessed by others, and can control the extent, manner and timing of the use of those parts they choose to disclose.

<sup>11</sup> SNS is defined as public domain and posting information here would not be considered having a reasonable expectation of privacy.

<sup>12</sup> J.P. Murphy & A. Fonteilla, Social Media Evidence in Government investigations and criminal proceeding: a Frontier of New Legal Issues, 19 Rich. J.L. & Tech. 11.

some scholars are worried about this policy will due to invasion of privacy and point out that policy makes private citizens becoming as “virtual deputies” , which we do not expect for.

Furthermore, serious disagreements between admissibility and authenticity of evidence will arise, if these photos and messages are introduced in courtroom. When a prosecutor charges a defendant on the basis of materials from social network, his lawyer consequently will object by legitimacy and call reality in question, that is, “how could you prove these photos or messages really from my client?”

Through emphasizing that SNS is a public sphere and using evidence from SNS should comply with due process, proposition concludes information from SNS as social media evidence could be adopted by court in principle. Also connections between information from SNS and suspect/defendant could be proved by internet forensic and logic reasoning.

However, what showed or posted on the SNS presents what was happened in the real world? Proposition shares the common view, like this old saying, “a picture is worth than thousands words”, which inherits scientific objectivity, such as “seeing is believing”. We can easily find this presumption used in that standard of process for using evidence. Especially in the request of authenticity, it would not be doubt if the evidence is made from science and technology, such as the photo in the beginning case. Actually, the courts hold this objectivity assumption to all those classified as scientific evidence, but only focus on accuracy of collecting evidence and statements of expert witness in procedures. Therefore, this research is curious that how such an objective assessment is set up and how it affects the production process of legal arguments.

It is useless to refuse social media evidence into the court. Apparently this evidence has been widely used in crime investigations and litigations. And also, only

considering infringement of privacy is not effective. Because under the traditional public-private dichotomy to protect privacy, evidence from public or semi-public websites will be taken as admissible, if it is discoverable. We never doubt the content of this technical evidence, especially taking digital photos as evidence, but only judging the authenticity of the form. Maybe the real crisis is not about the privacy, but some fundamental values, gradually and unknowingly eroded. What we need to do is making conversations between law and science, in order to more fully utilize social media evidence, corresponding both legal justice and scientific fact.

Once a time, I asked a Taiwanese prosecutor whether the photo of a stolen car can be used as evidence. She answered without hesitation, “why not”. Of course, now we have already clarified it is not a meaningful question of being evidence. However, I found myself interested in her answer “why not”. This answer was not produced deliberately through her legal knowledge, but was made through her intuition. There were some presumptions: first, the suspect submitted this photo on his Facebook publicly. It is the same situation that the suspect stood on the street. No privacy should be considered. In accordance with the foregoing idea, there is no rule for search and seizure in public area, therefore this evidence is discoverable and can be introduced to the court. Second, this photo reflected the fact. It connected the suspect and the stolen car, and complemented the causation between them. The prosecutor thought the suspect stole that car; otherwise, there was no reason, in this photo, why this suspect was sitting in others’ car. Maybe we can say she believes in “seeing is believing”. Her thought reflects an illusion of objectivity from the scientific revolution. Science and technology are Spokesmen of facts.

### **3. Interactions between the Law and Science**

Actually the legal system always follows the traditional solutions when they are

challenged by new technology or scientific theories. Judges evaluate this new type of evidence by applying to or even analogy with the current rules. Sometimes they may ignore the difference between new type of evidence and traditional rules, causing difficulties or even unfair judgements. In court, the lawyer may argue for his client that the printout of the defendant's Facebook is not the same as what posted on the website, or his client didn't write this post or even he was hacked. But most of time, we should pay more attention that the court is too confident or fully accept the tendency of science. This may come from the scientific revolution, when scientific objectivity was established. We still have to ask whether science is as unshakable foundations, when a new technology or an existed scientific skill is introduced into the courtroom. Here I illustrate two possible problems which the scientific evidence may face: procedural operation errors and paradigm shift.

### 3.1 Negligence in Forensic Process

Amanda Knox,<sup>13</sup> an American Student studying in Italy, was charged with murder and the Italian prosecutor claimed she and her Italian boyfriend, Raffaele Sollecito, killed her British flat mate, Meredith Kercher, without mercy in 2007. The prosecutor also provided the DNA evidence, which was taken out from some drop of blood found on the victim's bra. Mainly according to this evidence but not only, they were found guilty by the first-level court (Corte d'Assise) in 2009, sentenced to 26 and 25 years respectively and held in detention. However, on 4th of October in 2011, Italian appellate court (Corte d'Assise d'Appello) overturned convictions by reasoning these judgments were lack of evidences, and released them in acquittals.<sup>14</sup> The most crucial reason is that the court adopted an independent expert's report, in which the

---

<sup>13</sup> Amanda Knox, [http://en.wikipedia.org/wiki/Amanda\\_Knox](http://en.wikipedia.org/wiki/Amanda_Knox) , the last date to visit: 25 Oct 2014.

<sup>14</sup> Murder of Meredith Kercher, [http://en.wikipedia.org/wiki/Murder\\_of\\_Meredith\\_Kercher#Italian\\_criminal\\_procedure](http://en.wikipedia.org/wiki/Murder_of_Meredith_Kercher#Italian_criminal_procedure) , the last date to visit: 25 Oct 2014.

expert pointed out this DNA evidence was polluted during gathering process and these forensic procedures are unreliable.

Some scholars support this judgment and declare the appellate court show its attitude, that forensics procedures shall be complied with requirements of due process.<sup>15</sup> They repeatedly stress that, although DNA evidence, as function of personal identification and environmental cognition, presented a convincing accuracy, its reliability actually depends on whether all kinds of conditions are satisfied during forensic and testing process. Besides, this evidence could not be alone to decide the whole facts of crime, or rather should be considered together with other relative evidence. Nevertheless, is it the only one factor influencing on scientific objectivity?

In March of 2010, Japanese Toshikazu Sugaya was pronounced innocent of the charge without argument, that before he was found guilty of kidnapping and killing a 4-year-old girl, and had been imprisoned for 17 years.<sup>16</sup> After this pronouncement, judges and the prosecutor, as representatives of the Japanese judiciary, bowed to Mr. Toshikazu and apologized for the erroneous judgment he got. This erroneous is because the DNA testing technology adopted by the district court was replaced with a new one. Japanese National Research Institute of Police Science (NRIPS) applied the D1S80 locus (MCT118) as DNA profiling process during 1990s, just when Ashikaga murder case was happened. By this way, when obtained samples are few, experts need to use varied chemicals and amplify samples in order to illustrate the DNA chromatogram. Although experts in NRIPS had already reported that samples in the crime scene matched defendant's DNA, they also mentioned this testing was only

---

<sup>15</sup> Chiou, Shian-Min & Lin, Yi-Long. 2007. The Offensive and Defensive Countermeasures of Digital Evidence in Court. *Journal of Information, Technology and Society*. Vol. 7, No. 1: Pp. 53-64 (in Chinese); Liou, Chiou-Ling. 2009. The Admissibility of Digital Evidence in Criminal Proceedings. Master thesis. College of Law, National Chengchi University. (in Chinese).

<sup>16</sup> Ashikaga murder case, [http://en.wikipedia.org/wiki/Ashikaga\\_murder\\_case](http://en.wikipedia.org/wiki/Ashikaga_murder_case), the last date to visit: 25 Oct 2014.

thousandth point two (1.2/1000) of accuracy; but nowadays the technology for retesting gets ninety-nine percent (99/100) of accuracy. It is a real progress in science and technology, except that, for Mr. Sugaya, this progress is late for 17 years. In the end, this research wants to know what the influence is, that such technological evidence impact on legal knowledge production.

Issues on the first Italian case are focused on forensic processing, requested following the correct and standard procedures. In that case, no one discussed relationship between scientific evidence and the truth, neither thought about whether science is as unshakable foundation. However, as Ashikaga murder case (the second one) shows, there is uncertainty in scientific community and paradigm shifting is acceptable in science. That is, even though the first judgment did not do anything wrong with using this DNA evidence and applying rules of evidence, it is still misjudgment because of change of DNA interpretation technology which restate what is the real fact. After Thomas Kuhn provided the concept of paradigm shifting, both legal and scientific systems have already known this phenomenon, nevertheless this shifting in science is irreversible, which means old paradigm is not only out of the mainstream discourse, but abandoned and replaced. Could legal system, which needs certainty and stable, just like in the situation of the second case, afford the effect brought by this irreversible?

On the other hand, these two cases showed us significantly different between fact-finding function in law and science. For science, the ultimate goal is to find the truth; fact-finding is the main activity of science. On the contrary, legal system works hard to find the truth behind a case, but also need to consider values guaranteed by Constitutional law. Just like the first case, her “not guilty” was not based on the fact, and maybe she was the murderer, but our legal system believe there was higher value needed to protect in this case. Different from science, fact-finding is not the end of

legal activities, and this fact is not built for the general principle, but for a very specific case, trying to represent the fact in the past.

### 3.2 Paradigm Shift and New Objectivity

Since the publication in 1543 of Nicolaus Copernicus's *On the Revolutions of the Heavenly Spheres* and Andreas Vesalius's *On the Fabric of the Human body* often cited as marking the beginning of the scientific revolution, the Science has the privilege to talk about the truth, which can connect to the objectivity. But, after Worthington's instantaneous photograph in his article on "the splash of drop and allied phenomena" was published in 1895, scientific traditions of idealizing representation, stripping away the accidental to find the essential, became a scientific vice. The scientific communities found no apparatus was perfect, and there should be room for error of judgment. A statement of truth is not absolutely unshakable, must rely on strong evidences, and will be represented dynamically. New form of unprejudiced, unthinking and blind sight, called scientific objectivity, is developing now.

Besides, other disciplines have been gradually questioning the objectivity under scientific boundary work. When we observe the development of US Supreme court, an obvious shift would be pointed out. From Frye standard<sup>17</sup> to Daubert standard<sup>18</sup>, the court used to accept that expert opinion based on a scientific technique is admissible only where the technique is generally accepted as reliable in the relevant scientific community, and then became to build some legal criteria to apply the scientific facts. The day is gone, taking standards from scientific communities as granted.

Under the boundary work, the Science has the privilege to talk about the truth,

---

<sup>17</sup> Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

<sup>18</sup> Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

which can connect to “the objectivity”. Therefore, through the third party’s words, legal system claims they use the modern trial procedures, unlike the inquisition or autocratic monarchy trial in the past. Because the Science proves the fact true, legal system can make the decision based on “truth”, which is correct and credible. Science can provide something can be observed, represented and in material. And legal system needs something must be definite, correct and reliable, just as what science can provided. This research supposes that reliability is based on the rule accepted by both scientific and legal communities, “Seeing is believing”, which came from the scientific revolution in 17<sup>th</sup> century.

But the science system allows the uncertainty in its system. In contrary, law must be clear, stable and norms relative. How to choose and adopt so-called “accuracy” scientific knowledge will lead to forming “the objectivity”. Besides, according to Kuhn, there is a paradigm shift in science System and this shift is irreversible, which means the former paradigm was discarded and never reversible. Could the legal system tolerate the effect from such irreversible paradigm shift?

On the other side, legal system is changing the way of government because of uncertainty and insecurity under a risk society. Violations are not the specific danger, but the possibility of danger in daily life. Legal system pays more attention on the prevention mechanism, such as sentencing prediction system, crime predict system, etc., which is different from personal punishment before. However, what is used to be the prevention mechanism from scientific knowledge, exits much uncertainty.

These phenomena point out one fact, that is, legal systems want to find the authority to justify its power of punishment in this modern democratic society.<sup>19</sup>

---

<sup>19</sup> In a democratic society, arbitrariness of judgments is questioned by spirit of democracy, such as counter-majoritarian difficulty advocated by prof. Bickel. See Alexander M. Bickel, *The Least Dangerous Branch: The Supreme Court at the Bar of Politics*, 2nd edition, Yale University Press (1986).

Different from the monarchy era, legal system use a series of procedure and convince people with “be to fact”, instead of religious divinity and ceremony. When evidences from SNS could be shown on court, guaranteed by science and technology and its objectivity, the defendant will bear the burden of proof about reality of these evidences, which originally should be protected by the presumption of innocence. Because one argument has been shared, “You are in the photo, which you must be there.” However, what science and technology can present somehow is more than its presence or absence on the surface. Moreover, taking social network sites as a virtual place, it is a clear and concrete expression of human social life. But when the state combines technology with reality/the truth, and given it monopoly on behalf of objectivity, the defendant’s right and the prosecutor’s power will change dramatically in criminal procedures.

Kuhn pointed out the possibility of scientific paradigm shift, but also opened a new development of scientific objectivity. In the judicial history, that Japanese case confirmed the cost of scientific paradigm shift. We need to think how much price of uncertainty should be tolerated by legal system. Especially, comparing with DNA evidence, there is more room for judges, juries, prosecutors, lawyers and defendants to make subjective interpretation of social media evidence. Everyone in the court room can make his/her own story via social media evidence. Therefore, is the imagination of its technical objectivity still unbreakable?

**In Sum**, the aim of science is to find out a universal theory to explain the objective natural world. The theory accepted by the scientific community must be described for the objective world and at the same time in any case to meet requests of the scientific explanation. This idea coincides with the finding-fact task in the criminal proceedings. Because the purpose of a criminal proceeding (no matter what

kind of) is to find the fact of the case, and then to apply regulations to this case. Science is able to provide assistance to find the truth in a general way. In other words, at the point on fact-finding, scientific theory and technology based on the scientific theory have the same goal with the law.

As the scholar pointed out, the law and science “*both are fact-finding institutions, but they blend normative and epistemic considerations in different ways, according to their particular institutional imperatives. Most importantly, the law finds facts in order to settle disputes, whereas science makes claims to extend previous lines of inquiry and enable new ones to take shape. Law, therefore, takes the case as its theater of operation and seeks to answer questions arising within narrow factual contexts; science attempts to produce facts that circulate beyond the circumstances of their production. These contrasts affect which issues are deemed worthy of investigation, how questions are framed, how and by whom inquiry is pursued, and what standards of validity are applied in testing knowledge.*”<sup>20</sup> However, “*a careful account would find congruence as well as clashes in the processes of law and science. The formal spaces of both institutions—courts no less than labs—are claimed to be dedicated to finding the truth, though with different ends in view: the law needs facts as necessary adjuncts to doing justice; science seeks facts more as an end in itself.*”<sup>21</sup>

Science aims to discover the truth of nature. The legal system, even though it also attempt to find the fact (reconstruct the past events), pursues more than fact as well as considers other value, such as constitutionally guaranteed rights, due process requirements, etc. To find the fact is a necessary but not only goal in the legal system, and there is more legal value than the fact to consider in a criminal case. This idea will be used in analysis in this thesis.

---

<sup>20</sup> Sheila Jasanoff, Law’s Knowledge: Science for Justice in Legal Settings, Public Health Matters, Supplement 1, 2005, Vol 95, No. S1, S49-58, at S52.

<sup>21</sup> Id, at S51.

## RESEARCH QUESTIONS

The motivation for this research is whether there is a violation of the principle of self-incrimination, or excessive infringement of freedom of speech or privacy, if the prosecutor uses the information on the defendant's Facebook to sue him. In order to answer this question, more questions are derived: what is so-called social media evidence? (Actually its definition is blurred and diversified, and still continuously developing.) How does the court use and evaluate this evidence? Except directly printing the websites out, how can we extract the information from social network sites reliably by technology, and how does the court or the jury evaluates these evidence? How does the court or the jury use the evidence to rebuild the past facts (crime facts)? How does these information produced in a virtual website connect the fact happened in the real world? (The influence of science and its scientific objectivity on the court) And whether the social media evidence has changed the way that the court constructed the truth/ crime fact; if there is a change, what is that?

Therefore, my research questions can be summed up as the legal truth produced by social media evidence. What the truth is can be traced upon the 16<sup>th</sup> century, when natural philosophers used experiments shows as means to persuade peers or support their hypothesis, and then they concluded with the concept of scientific objectivity. This conception not only enhances the rule of thumb, "Seeing is Believing", but also shapes meanings of true: it is unique, objective, and can be reproduced. From the legal perspective, finding the fact is not the end of the criminal proceeding; there are more values from the society and culture to be considered in a legal judgment. Thus, what is the legal true? Does it coincidence with the meaning of true in science?

To concrete research purposes, this thesis provides three questions to explain the legal truth produced by social media evidence. First, we need to answer what is the social media evidence (chapter 1). Not limited literal explanation, this thesis wants to

show the whole picture of a transforming proceeding, in which the information on social network sites was extracted by technology, filtered through rules of evidence, and then become admissible evidence that the jury can use to reconstruct the past fact. Thus, two more sub questions need to be discussed: how to introduce social media evidence into a trial (chapter 2), and how to extract information from social network sites by technique and science (chapter 3). Then I will discuss which values will be considered by the law, when using social media evidence to build the case, and what will legal system do to deal with this situation? And further I will propose a new picture to describe how information extracted from social networked sites becomes the evidence proofing the crime fact in the courtroom. I believe that social media evidence is not the real evidence fixed on the table, but a proceeding to show information transform (chapter 4).

Second, in this dynamic transforming proceeding, how does the court operate social media evidence to reconstruct the past fact? This thesis separates issues of social media evidence into two different situations to response this question. When using the printout as social media evidence (chapter 5), that is an attempt to present the visualized information on websites in court, via the form of a physical and readable document. What will legal system do to deal with this situation? When a Trojan Defense being arises (chapter 6), that is an attempt to challenge the supposed connection between the offense on social network sites and a criminal in the real world. What will legal system do to deal with this situation?

After completing the first and the second question, we will be able to get the legal and technical model processing social media evidence under the legal and technological context. Then the third question arises, that is, how the legal system reproduce the past fact through social media evidence (chapter 7)? We can specifically identify particularity of legal truth by comparing the technical approach.

## **METHODOLOGY**

There are two research methods in this paper: documentary analysis and comparison (compare the differences of different legal systems and compare the differences among different disciplines).

### **1. Documentary Analysis**

About the range of literature, this thesis first chose those articles directly discussing issues on social media evidence, and then extended those articles on digital evidence or electronically stored information (ESI) involved related issues. The third step is based on the specific topic for the keyword to collect the relevant literature, such as Trojan defense, the authenticity of the printouts of social media evidence. As a reinforcement of the background knowledge to provide the basis for meta-analysis, the thesis collected literature on the purpose and spirit of criminal proceedings, interaction between science and law, the role and significance of forensic science in criminal proceedings, Luhmann's system theory, and sociology or philosophy related to fact finding, such as Sheila Jasanoff's books and papers. In order to supplement knowledge of digital forensics/ network forensics, the thesis used Eoghan Casey's "Digital Evidence and Computer Crime" (2011), and Daniel & Daniel's "Digital Forensics for Legal Professionals- Understanding Digital Evidence from the Warrant to the Courtroom" (2012) as fundament, and on this basis, carried out an extended reading.

According to documentary analysis, this thesis attempts to point out, while a new technology is introduced into the legal system, the core operation of legal system would not be the acceptance of this new technology unconditionally, but would react with it, and transform this scientific knowledge to legal knowledge. Hence, except analyzing and discussing how the technology system and legal system produce the social media evidence, the thesis want to do this research from a Meta perspective,

which means the thesis will try to understand the question from a higher level, instead only from the question itself. While discussing the usage of social media evidence in criminal procedure, apart from issues on evidence law, the thesis would more like to discover more interaction between law and science as background knowledge, such as how to interpret science in the court room, what is the fact-finding function in legal system and how the legal system shares/bears the risk of uncertainty with using scientific standards. Therefore, this research will argue three topics to explain the interaction between social network sites and law through using social media evidence in criminal law. These three topics will be “usage of social media evidence in finding fact”, “different disciplines in legal system” and “doing justice by using science”.

The meta-analysis of this thesis will be based on Luhmann's system theory, on which we regard science and law separately as subsystems in a large social system, discuss its internal operations and symbols, and then analyze the interaction between systems when system coupling occurs.

## 2. Comparison Approach

In order to see the whole picture of this interaction, a comparative approach is introduced. I will compare social media evidence in legal system and forensic science. By comparing legal interpretations of different types of technology, it can help us find the need of building new rules for social media science, and also we can find the court's attitude to face the truth provided by science, and issues under this attitude, or find out another approach for the court to understand scientific knowledge.

The goal of this research is solve authentic of social media evidence in criminal procedure, so specific rule of evidence and judgments will be used. At the same time, this research wants to discover a principle or standard of finding the truth in the epistemological level, so in the research the research method of comparative law is adopted to find some standards. As the starter, American law and judgments will be

used as base, since they have the largest population in the world to use SNS and during legal issues on the SNS, they have already had sufficient cases and large number of discussions, which is sufficient and necessary as forming a theoretical basis. As a comparison object, I choose the Taiwanese law as the representative of civil law. Traditionally, Taiwan's criminal legal system has been transplanted from German law, especially the Code of Criminal Procedure (evidence law included). But in recent years, legislators introduced part of adversary system as amendment, such as hearsay rule. Therefore, Taiwanese legal system is a good platform for observation of the integration and differentiation between civil law and common law systems. It will be useful to build the common standard for social media evidence.

## **STRUCTURE OF THIS THESIS**

The main concern of this thesis is how information from social network sites is transformed the criminal evidence at the trial to represent the past fact, and discusses issues of social media evidence from legal and technical perspectives. Fact-finding, as the most important purpose in criminal proceedings, will be presented through social media evidence. Further, this thesis wants to use social media evidence to present how the legal system represents the past fact at the particular moment. The structure of the thesis is as follow.

Chapter 1, 2 and 3 discuss “what is social media evidence”, from three perspectives of literal meaning, evidence law and technology. On the literal interpretation, this thesis explains definitions and relation of social network sites and social media evidence, and types and nature of social media evidence. Then this thesis discusses what kind of social media evidence, filtered by Rules of evidence, will become evidence in legal sense accepted by courts. And finally, with the forensic technology, how to extract information from social network sites and transform

information to format of evidence in technical approach, in order to ensure the accuracy of digital data and fulfillment the reliability requirement of law. Then in Chapter 4, according to the research results of the first three chapters, the thesis explains three challenges when the court will introduces social media evidence into the proceeding of making judgement, and tires to find the solution through both legal and technical approaches. In this chapter, the first challenge, the original, will be discussed, and the second challenge, authenticity, and the third challenge, authorship, will be sequentially in Chapter 5 and 6.

Chapter 5 concerns, why the printout of a social network site post can be admissible at trial. When the police search and seizure digital information, a common way they use is to directly print out digital data obtained and ask the signature of the parties at the presence, without taking original digital data back. In addition to the issue on its original identity, this conduct to obtain evidence may have another two results. First, it will easily allege that is tampering evidence because the police wanted to frame the suspect and falsified evidence. Second, it is not easy to discovery hidden information. The core evidence associated with crime may not appear in the contents of files. Through discovery the original file, data related to the file, such as the original producer, creation time, modification date, and even GPS location display, can be revealed from hidden information. Therefore, authenticity of the printout always is the main issue of social media evidence.

This thesis attempts to discuss this issue from an information transforming point of view. That is, the printout of social network sites implies we want to copy activities happened in the virtual world. This is a procedure to prove  $A=A'$ . Forensic practitioners use methods of Hash value verification and image copy to ensure identity of original data and the result. In the legal system, the printout must be

authentic, which means this printout is correctly reflected the content of information on the social network site, and having been posted by the purported source. It is reasonably possible for a jury to find that the printout is authentic.<sup>22</sup> Thus, on issue of A=A', the legal system is more interested in the asserted content and authorship, instead technical issue of the printout itself. This thesis will analyze the legal approach, comparing the technical approach, and reconstruct the printouts issue in another way.

Chapter 6 discusses the Trojan defense, a common question on who really did it. In this thesis, to prove who did this post on SNS means we want to connect a specific internet character with a real person in the world. Actually, the present technology only can prove the issued post done by a specific IP address. Prosecutors need circumstance evidences to support their claims and connect to the defendant. Thus, this thesis first will explain the background of the Trojan defense , such as the definition, characteristics and functions of the Trojan. Then it discusses how to handle the Trojan defense in technical and legal approaches, and concludes how the legal system represents or actually constructs the past fact.

In Chapter 7, based on the scientific nature of social media evidence, this thesis reviews the meaning of facts in criminal proceedings and the principle of evidence-based judgement, and further challenges the purpose of fact finding in the contemporary criminal justice. This thesis argues that criminal litigation, as a field for the parties to settle disputes, does not pursue the scientific truth but chooses to be able to persuade the parties and to find a solution that can be accepted by both parties. With this social media evidence, which is mainly user-generated content, we can more clearly recognize the choice of legal system.

---

<sup>22</sup> United States v. Vidacak, 553 F.3d 344, 349 (4<sup>th</sup> Cir 2009).

As the conclusion, this thesis found when a new technology was introduced into the court, judges first analyzed the nature of this issue, then search similar object in the past cases, and applied the same approach to solve the problem. The point is analogy. For example, when searching computer is going to an issue, the US Supreme Court created the box theory to solve it. That is, the court stated, searching a computer is just like searching a box. The prosecutor needs a warrant with detail in the box or subscribing the object of this search. In the same situation, while the prosecutor wants to search a computer, they need to make a search plan with reason to apply a warrant. Therefore, most judges and scholars state there is no need to create a new regulation for new technology (social media evidence) and believe current rule of evidence is enough. I conclude with Judge Holmes's words: "*The life of the law has not been logic; it has been experience*".

## Reference

1. Adkins J (2011), Law Enforcement Guide to Social Media, Special Research Report, available at <https://nebula.wsimg.com/5bdda470f8982071d7ef98ed81038dfb?AccessKeyId=D535D04439DEB65C2F17&disposition=0&alloworigin=1>
2. Andrews, Lori (2013), I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy, Reprint edition, Free Press.
3. Bickel, Alexander M. (1986), The Least Dangerous Branch: The Supreme Court at the Bar of Politics, 2nd edition, Yale University Press.
4. Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition.
5. Chiou, Shian-Min & Lin, Yi-Long (2007), The Offensive and Defensive Countermeasures of Digital Evidence in Court. Journal of Information, Technology and Society. Vol. 7, No. 1: Pp. 53-64 (in Chinese)
6. Cole, Simon A. & Lynch, Michael (2006), The Social and Legal Construction of Suspects, 2 Annu. Rev. Law Soc. Sci. 39.
7. danah m. boyd & Nicole B. Ellison (2008), Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication. 13: P. 211.
8. Daniel, Larry E. & Daniel, Lars E. (2012), Digital Forensics for Legal Professionals- Understanding Digital Evidence from the Warrant to the Courtroom, Elsevier: Ma, USA.
9. Datt, Samir (2006), Learning Network Forensics, Packt Publishing.
10. English, Peter W. & Sales, Bruce D. (2005), More than the Law: Behavioral and Social Facts in Legal Decision Making, APA, USA.
11. Giannelli, Paul C. & Imwinkerltied, Edward J. (2012), Scientific Evidence, vol. I, 5<sup>th</sup> edition, LexisNexis.

12. Gilson, Cedric C. (2012), *The Law-Science Chasm. Bridging Law's Disaffection with Science as Evidence*, Quid Pro Books, New Orleans: USA.
13. Haak, Susan (2014), *Nothing Fancy: Some Simple Truths about Truth in the Law*, in: *Evidence Matters: Science, Proof, and Truth in the Law*, Cambridge University Press, 294-323.
14. Jasanoff, Sheila (1997), *Science at the Bar*, paperback edition, Harvard University Press, USA.
15. Jasanoff, Sheila (2005), *Law's Knowledge: Science for Justice in Legal Settings*, *American Journal of Public Health*, Supplement 1, Vol. 95, No. S1, S49-S58.
16. Kent, Karen, Chevalier, Suzanne, Grance, Tim & Dang, Hung (2006), *Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-86, available at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>
17. Leiter, Brian (2007), *Law and Objectivity*, in: *Naturalizing Jurisprudence: Essays on American Legal Realism and Naturalism in Legal Philosophy*
18. Lilly, Graham C. (1987), *An Introduction to the Law of Evidence*, 2nd ed., West Publishing, N.Y.
19. Liou, Chiou-Ling (2009), *The Admissibility of Digital Evidence in Criminal Proceedings*. Master thesis. College of Law, National Chengchi University. (in Chinese).
20. Lynch, Michael (2008), *Science, Common Sense, and DNA Evidence*, in: *Truth Machine*, 190-219.
21. McCartney, Carole (2012), *Forensic Identification and Criminal Justice. Forensic Science, Justice and Risk*, Routledge, NY: USA.
22. Morales, Lawrence (2014), *Social media evidence: "what you post or tweet can and will be used against you in court of law"*, 60 *The Advoc.* (Texas) 32.

23. Murphy, J.P. & Fonteilla, A. (2013), Social Media Evidence in Government investigations and criminal proceeding: a Frontier of New Legal Issues, 19 Rich. J.L. & Tech. 11.
24. Niesenbaum, H. (2009), Privacy in Context: Technology Policy and the Integrity of Social Life, Stanford Law Books, 2009.
25. Valverde, Mariana (2009), Law's Dream of a Common Knowledge, Princeton University Press.

# Chapter 1 Social Media Evidence

In order to limit the scope of research and further to focus on research questions, it is necessary to define several terms used in this thesis, such as social network sites (SNS), social media, and social media evidence (SME). Undeniably the definition of social media or social network sites is wide and broad. In this thesis, the term of social media evidence means that information obtained or extracted from social network sites then is used as evidence to proof crime facts in the criminal procedure. Therefore, this so-called social media evidence at least has two different meanings respectively from digital forensics and legal area, which will be discussed in each chapter. Here I will use this simple definition of social media evidence as the center, respectively, to explain each term and relationships between each other.

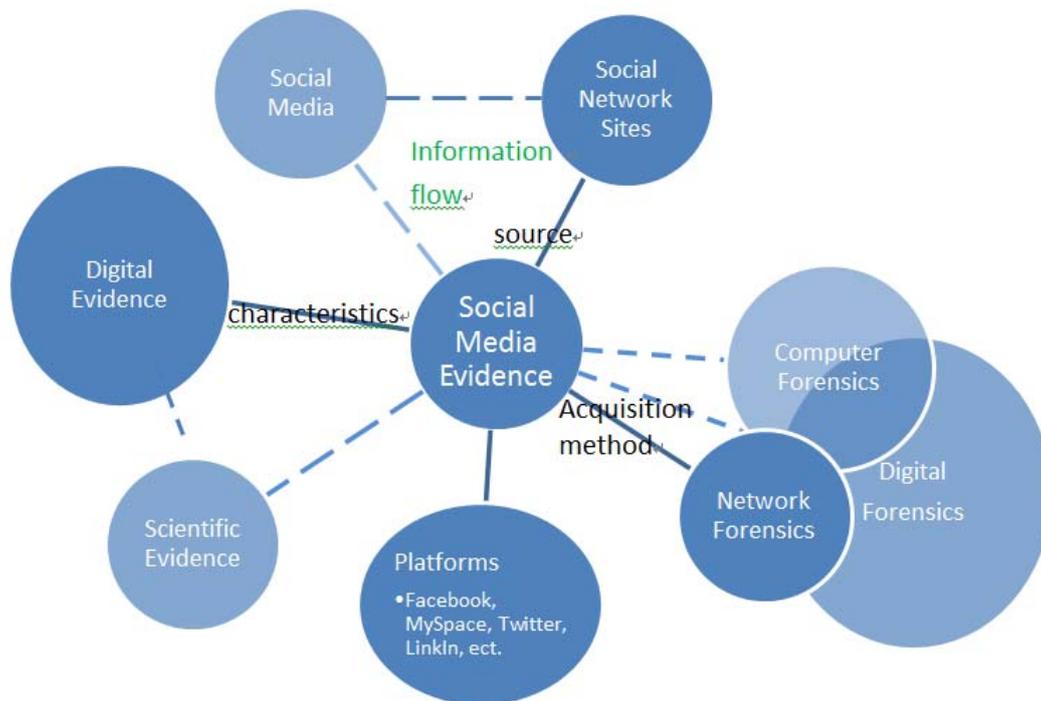


Figure 1 Ontology of Social Media Evidence

## 1. Definition

Social media evidence describes information extracted from social network sites

in order to be evidence presented at trial. This term literally stresses that media which this information depends on. A few American scholars call this kind of evidence as social network evidence, which enhances information is exactly from social network sites. But the mainstream academia calls it as social media evidence, and usually discusses information extracted from social network sides. In fact, most real cases in court are related to evidence obtained from Facebook, MySpace, and Twitter, and the courts didn't distinguish these terms of cases in the detail. Thus, we may think the term "social media evidence" as a phrase during the legal practice.

### 1.1 Social Network Sites

Social network sites refers to a group of people in the work, the environment or life relations have a common goal, purpose, demand or interest, resulting in the homogeneity of the organization, group. Organizations and organizations in society extend their concept to the Internet without face-to-face contact. They mainly use the computer network as an interactive interface and interact with each other on the Internet to share information, exchange goods, and so on. This is called the virtual community Virtual Community or network community Network community. A web application service designed to help people build social networks. After the appearance of Six Dgree.com, the first social networking site in the United States in 1997, a large number of social networking sites appeared each year. The earliest online community in China is BBS (Electronic Bulletin Board System), an academic website set up by students of the National Chiao Tung University Graduate School of Engineering to provide information exchange functions.

The most common<sup>23</sup> definition is one coined by danah and Ellison, which is, social network site(s) as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other

---

<sup>23</sup> Based on google scholar search engine, this article was cited 6778 times.

user with whom they share a connection, and (3) view and traverse their list of connections and those made by within the system. The nature and nomenclature of these connections may vary from site to site.<sup>24</sup>

Current social networking sites provide services and mechanisms for engaging with the online community, websites that allow users to connect and communicate, manage feelings, share experiences, communicate information, and deliver knowledge. Community sites also provide email, bulletin boards, discussion boards, message boards, graffiti walls, chat rooms, voting areas, photo galleries, calendar, games and other services.

Community websites can be divided into the following categories, including simple social online community sites, commercial categories, online matching, alumni community or a focused social networking site, such as Taiwan Bahamut is the focus of video games. Top 10 global social networking sites in 2010 are Facebook, LinkedIn, orkut, orkut (Brazil), Sina Weibo, Renren, odnoklassniki, Scribd, V Kontakte, Netlog; Taiwan's top ten community sites include Facebook, Chiamo blog, , Blogger, Blogger, Yam sky tribe, UDN blog, Sina blog, Windows Live Profile, Yahoo! Pluse and so on.

In addition to the community website as defined in the general definition, the concept of online community has also been gradually extended to different types of websites. Driving websites tends to be "socialized." In other words, there are more and more websites that integrate the concept of community into the operating elements of the website and extend customer service. For example, manufacturers set up a "web community" for their products on their websites so that consumers In which discussions, exchanges, and in the chat room set up 24 hours customer service staff to solve the problem for consumers, which virtually increase the value of the

---

<sup>24</sup> danah m. boyd & Nicole B. Ellison (2008), Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication. 13: P. 211.

product and visibility, especially for new products more helpful. In addition, this community website can also maintain good customer relationships and get the most direct customer feedback.

#### 1.1.1 Structure of Social Network Sites

The primitive social network is a kind of graph composed of node and edge, in which nodes represent people, and edges represent all kinds of mutual understanding between people Relationship. Often, the social network is constructed from a specific corpus, such as a Facebook community website, a network of experts within a company's organization, and intra-corporate relationships. The social network constructed by the data set is not completely static. As new members join in as time goes on, the number of nodes increases. At the same time, new members and old members will know each other and create new edges. We call this graphical structure evolving over time a Dynamic Social Network.

In addition, individuals in the social network may have different types of identities (such as students, teachers, performers and directors) or attributes (such as gender, interests and expertise), and there are many possible types of connections between individuals, such as friend relationship, family relationship, teacher-student relationship and cooperative relationship. This type of graphic structure that considers nodes and edges is called "Heterogeneous Social Network."

It can be seen from the above that the social network is regarded as a data structure that can effectively represent various kinds of interactions and connections among individuals. Unlike many data sets that are independent and come from the same and independent distributed identities (IIDs) Further linking individuals through multiple relativities allows for more time-evolving interactions with each other, making it easier to describe the intricacies of individual interactions in the real world.

Advantages of social network sites are to make it easy to know hundreds of

people, enhance personal social advantages, increase exposure, expand contacts and gain spiritual support, and establish contact with the workplace environment; the disadvantage is to expose personal privacy, the lack of verification of the true identity of users' mechanism.

### 1.1.2 Characteristics

According to the services provided by SNS, we can sort out the characteristics of several SNS, such as instant messaging, popularization, visual indicators, user-generated content, can be linked to other platform content. Instant Messaging (IM) is a system for real-time communication over the Internet, allowing two or more people to use the Internet to instantly deliver text messages, files, voice and video. Services are usually provided as websites, computer software or mobile applications<sup>25</sup>. For example, Facebook users can send messages to friends or other users via Message.

The vast majority of SNS are free to provide services, as long as people set an account, you can use the SNS service. It is very popular. At the same time, Facebook, such as glass house: semi-open space, public domain private; online public space has continuity, searchable, reproducibility, hidden audiences and other characteristics, resulting in privacy issues.

SNS provides visual annotation for users to express their opinions, such as on Facebook, users can use this symbol  to express their love for a hair piece. At the same time, users can also express different responses to postings through a variety of emotion patterns  such as "love", "wow", "haha", "sad" and "angry" emotions.

In addition to these features above, this essay would like to specifically describe

---

<sup>25</sup> [https://en.wikipedia.org/wiki/Instant\\_messaging](https://en.wikipedia.org/wiki/Instant_messaging)

the two SNS features: user-generated content and links. This paper argues that these two characteristics will make the evidence obtained from SNS as information (social media evidence) is special, different from the traditional evidence, but also different from the generalized digital evidence.

#### (1) User-generated content

Compared with Web1.0 Web Services, the social media features of Web 2.0 are that most of the platform operators themselves do not make content, and rely entirely on User-made Content (UGC) to attract user interaction, including the general users and institutional users (News media, TV stations, movie companies, etc.). Therefore, the focus of platform operators is how to create a platform based on the needs of different communities to attract users to interact on the platform and generate content.

#### (2) Connection

SNS's connection characteristics can be divided into two kinds, the first is the human link: 1) from the offline community to the online community: such as: Facebook; 2) extended links: such as: friends of friends; 3) platform recommended links: Users may be interested in people; 4) Tracking celebrity links. The second is the platform (technology) links: 1) links with other platforms: such as: Youtube, Flickr; 2) links with content sites: such as news sites; 3) link with other applications: Other networks and SNS platform link: Such as: use FB account login, directly to the FB. Links promote sharing and exchange. In the social media platform, people share words, photos, video contents, contacts, extension information (URL), product information, dialogue, emotion, meaning, assistance work, community feeling and cultural identity. Texts, photos (metadata), videos, networks, user profiles, geo info, URLs, access info, interactions, user logs, transitional data, meta data are exchanged between platforms on social media platforms.

SNS changed the user's life style. SNS will be the original weak link into a

strong link, my friends, friends, friends form a "my group" relationship. Changed the life style (punch selfie), business model (all kinds of SNS as a marketing channel), political communication (2008 Obama election) and so on.

## 1.2 Social Media

Social media is another term need to clarify with SNS. It refers to the use of Web-based and mobile technologies that enable people to communicate easily via the Internet to share information and resources.<sup>26</sup> Under this explanation, social media put more attention on devices of media, but it is the essentially similar with social network sites. Just like Brunty and Helenek's suggestion<sup>27</sup>, the definition of social media will be built on boyd and Ellison's definition of SNS, and added further two criteria. That is, a social medium (4) encourages its users to communicate with other users who are a part of the network and/or the site creators themselves, and (5) creates an environment for users to share content and/or connect through their similar interests. Even though Brunty and Helenek claimed social media is a border conception than boyd and Ellison's definition of SNS, and the biggest difference between SNS and social media is that SNS focus on the relations between members. In my opinion, both of them focus the relations between members, and SNS, like Facebook, also encourages its users to communicate members or others, and creates an environment for users to share content, qualified all criteria. Therefore, SNS and social media are not conflict conception. The significant difference between is that, using SNS to strengthen online communication and connection, and using social media to put more attention on the way to present that online connection.

Under this definition, types of social media include collaborative projects (e.g. Wikipedia), Blogs and Microblogs, location-based (e.g. Foursquare), content

---

<sup>26</sup> Adkins J (2011), Law Enforcement Guide to Social Media, Special Research Report, p. 1.

<sup>27</sup> Brunty and Helenek (2013), p.2.

communities (e.g. YouTube, 4chan), social network sites (e.g. Facebook, LinkedIn), virtual game worlds (e.g. World of Warcraft), virtual social worlds (e. g. Second Life), and dating sites (e.g. Match.com).

### 1.3 Social Media Evidence

Basically, there are two categories of evidence in evidence law: witness and real evidence (e.g. knife, body, computer in a theft case, etc.). The witness is a type of opinion evidence in American legal system, and this type includes several kinds, such as eye witness, expert witness, etc. The function of witness evidence is a connection of probandum (the asserted facts need to be proved) to this witness's opinion. Witnesses at the trial must be interactively cross-examined by both party sides to ensure that their statements can be trusted. By contrast, the real evidence means any tangible items presented in front of the jury at trial, and can be directly considered by the jury to reconstruct the past fact of this case. In fact, the real evidence will be admissible through a witness's testify, instead being presented alone.<sup>28</sup> Because of that, the entire evidentiary review proceeding focuses on the witness evidence in American legal system.

Additionally, the demonstrative evidence, a special type of real evidence, is evidence in the form of a representation of an object, as opposed to testimony, or other forms of evidence used at trial. It has no probative value, but can be used as items to explain or clarify issues of fact, such as maps, diagrams, models, photos, etc. "Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a

---

<sup>28</sup> Graham C. Lilly, *An Introduction to the Law of Evidence*, 2<sup>nd</sup> ed., West Publishing, N.Y., 1987, at 512-515.

demonstrative exhibit must “fairly and accurately” represent the real object at the relevant time.”<sup>29</sup> Part of social media evidence will fall into this category.

## **2. Types and Formats of Social Media Evidence**

Types of social media evidence are diverse and fully creative. Information on social network sites basically may be transformed to evidence, if it satisfies the relevance request and admissibility request under the federal rules of evidence. For example, Facebook provides a package download service that users can download the whole his information on Facebook, including files created by himself, his postings, comments, as well as data generated by system.<sup>30</sup> The common types of social media evidence are users’ profile, friend list, contents of postings or comments, photos, records of login (log files), etc.

Taking Taiwan law as an example, the common formats of social media evidence in court are:

(1) Digital instruments: The current common digital document editing sections are Microsoft Word, Excel, Power Point, WordPad, etc. Common digital file types are \*.txt, \*.doc, \*.xls, \*.ppt, \*.pdf, etc.

(2) Digital sound: The current common digital sound player soft wares are Windows Media Player, Real Player, Quick Time, etc. Common sound formats are \*.wma, \*.mp3, \*.rm, \*.midi etc.

(3) Digital video: The common video player soft wares are Windows Media Player, Real Player, Quick Time, Power DVD, etc. Common video editing soft wares are ACDSEE, PhotoShop, PhotoImpact, WindowsMovie Maker, etc. Common image formats are \*.jpg, \*.tiff, \*.bmp, \*.avi, \*.wmv, \*.asf, \*.mpg, etc.

(4) Conversed, decoded, restored digital data.

---

<sup>29</sup> [https://en.wikipedia.org/wiki/Demonstrative\\_evidence](https://en.wikipedia.org/wiki/Demonstrative_evidence)

<sup>30</sup> The detail can be found at <https://www.facebook.com/help/930396167085762>.

(5) Digital evidence using the program to display, such as Encase, Recognition system of vehicle license plates, etc.

(6) Digital data from website: E-mail, Internet instant messaging, Websites, etc.

(7) Digital data in computer and other storage devices are PDA, Digital recording pen, Digital camera, mobile phone, and so on.

### **3. Acquisitions (How to Get It?)**

The technical manner to extract information from social network sites and to exchange it as evidence presented at court is internet forensics. This is a new term that appears in the Internet 2.0 era, to precisely describe the forensic method just for network information. It is said that computer forensics was founded by FBI in 1984.<sup>31</sup> Computer forensics experts only had to be concerned with what information might be evidence exists or hides in a single computer or floppy disk. Then, as technology has progressed, experts have to consider varies types of data, created by a myriad devices. Digital forensics is the more broadly description for every information on computer or other type of electronic devices which might be evidence at court.<sup>32</sup> And network forensics is one of its sub-disciplines, which focus on how a network has been attacked, stopping the attack, and attempting to locate the attacker. Therefore, I think these three terms are not totally different, but presents a progress that the computer science and network technology have developed and constantly evolving. They have the chronological relationship and subsumption from broad to narrow sense. Computer forensics first appeared. Then digital forensics came with broad sense and network forensics focus on online activities. Their respective definitions are as follows.

---

<sup>31</sup> Larry E. Daniel & Lars E. Daniel, *Digital Forensics for Legal Professionals- Understanding Digital Evidence from the Warrant to the Courtroom*, 2012, Elsevier: Ma, USA, p. 14-15.

<sup>32</sup> Larry E. Daniel & Lars E. Daniel, *supra* note 31, at 15.

### 3.1 Computer Forensics

Computer forensics refers to “the collection, preservation, analysis, and presentation of electronic evidence for use in a legal matter using forensically sound and generally accepted processes, tools, and practices.”<sup>33</sup> It can be divided into two kinds of connotation. Narrowly, this refers to the science that collects information from the computer as evidence at court. At this point, forensic practitioners will face a variety of operating systems, packages (software), communication protocols and network environment. It is better to work as part of a team with expert consultation. In the broad sense, computer forensics not only collects the very meaningful digital data, but also contains password forensics, compression forensics, logical/computing forensics, and computer evidence processing. It is the science to obtain fragment data through the computer and depict the rough situation of the event to rebuild the data, accompanied by the fact to duly present the expert testimony, and then explore the computer evidence to preserve, identify, extract and file.

### 3.2 Digital Forensics

According to USA National Institute of Standards and Technology (NIST), “Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.”<sup>34</sup> Simply, it is the forensics for digital data. Generally information stored in computers is digital data, so the meaning of digital forensics refers to the digital data processing under the trend of

---

<sup>33</sup> Larry E. Daniel & Lars E. Daniel, *supra* note 31, at 3.

<sup>34</sup> Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-86, 2006, available at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

digital technology. That is, “*computer forensics becomes digital forensics*”.<sup>35</sup>

### 3.3 Network/ Internet Forensics

Network forensics is a kind of forensics aimed at using the Internet for crime. The procedure of network forensic is basically: first, to capture packets; second, to confirm the contents of the packet through specific filter conditions, such as filter information by date and time; third, to analyze and determine causes for the known and unknown type of packet. Generally, network forensics is part of digital forensics, but focuses on internet digital events and online activities investigation. Its purpose is to obtain evidence using manners accepted by the court, including monitor and capture relevant information of network traffic and network equipment generated.<sup>36</sup>

Difference between computer forensics and network forensics is the former mainly deal with static data, such as deleted, renamed and hidden files and other objects, register code, password protected files, emails, and carved data. The characteristic is the system state after collecting and making the image file. The procedure is based on the following steps: to identify the media at issue, to establish and verify a copy of the evidence, to investigate and analysis with the copy in depth, and to make a forensic report according to findings. On the contrary, the network forensics is dynamic. It must be pre-network traffic capture and preservation must be executed in advance, and then the forensics activities can be implemented.

Forensics is implemented for social network sites, such as Facebook, MySpace, Twitter, and LinkedIn, also known as social media forensics, which is one of sub-disciplines of digital forensics and network forensics. It focuses on “*the ability to locate and examine social media communication on the Internet and as artifacts left*

---

<sup>35</sup> Larry E. Daniel & Lars E. Daniel, *supra* note 31, at 15.

<sup>36</sup> Samir Datt, *Learning Network Forensics*, 2006, Packt Publishing, p.12.

on hard drives and cell phones.”<sup>37</sup> The investigative authority would like to examine people’s Facebook or Twitter accounts to find information about their online activities and communication of the person of interest.<sup>38</sup>

However, all hard/ floppy disk, network and memory forensics are closely related. In most cases, some or all forensics skills may be involved within a reasonable range. A supporting fact is the police want to obtain information from suspect’s Facebook account through his working computer.

#### **4. Types of Evidence in Legal Systems**

While talking about information extracted from social network sites as evidence from legal perspective, there are several terms related to this type of evidence, such as social media evidence, digital evidence, and scientific evidence. Basically, witness and real evidence are two main categories in the evidence law; for example knife and body are real evidence, but a person who saw the incident is called the eyewitness. In American legal system, Federal rules of evidence §702 regulates expert witness, who produces the scientific evidence and testifies scientific knowledge related to evidence and the case with his specialize. Thus, the scientific evidence is a type of evidence expressly stipulated in the evidence law, but needs to transform another format as expert witness presented in the courtroom. It must be produced by the expert, not being real evidence. Information extracted from social network sites may become the scientific evidence, if this evidence produced through the expert and scientific methods.

Digital evidence describes using information or digital data as evidence. It is a new type of evidence, differentiating from witness and real evidence. We use

---

<sup>37</sup> Larry E. Daniel & Lars E. Daniel, *supra* note 31, at 21.

<sup>38</sup> *Ibid.*

documents to record information traditionally (real evidence), and long time ago, we pass information by oral (witness), but now we have more pipelines to spread information, via telephone, fax, email, internet forum, instant message, etc. the most common part of these pipelines is we human cannot sense information without a specific device. Although digital evidence is not the common type of evidence specified in the evidence law (but the situation has gradually changed), it includes all type of information digitalized. Thus, it is a kind of nature of the evidence, and information extracted from social network sites is part of it.

#### 4.1 Digital Evidence

Considering the format of SME, this evidence cannot be touched physically, cannot be seen without the digital device, and cannot be understand, if there is no forensic practitioner to explain. Basically SME is just information, and it is necessary to identify it as evidence.

Digital evidence, also known as electronic evidence, “is any probative information stored or transmitted in digital form that a party to a court case may use at trial.”<sup>39</sup> It cannot be sensed physically, cannot be an object in the world, and will usually storage on electronic media in an electromagnetic or waves way. Therefore, it only can be accessed, analyzed or displayed through electronic devices. We can find SME and digital evidence, they share the same characteristics. Although SME is a subset to digital evidence, it can also apply the whole procedure for collection, preservation, and presentation of digital evidence.

Besides, this electronic record is not easy to obtain, easy to disappear, difficult to preserve, and simple to forge or alter. It is also difficult to prove the identity between raw data and obtained data, so it hardly becomes evidence in court. To overcome the

---

<sup>39</sup> Eoghan Casey, *Digital Evidence and Computer Crime*, Third Edition, 2011, Academic Press, p. 7-8.

above problems, forensic science and information science should be integrated with their own professional technology, in order to assist forensic investigators collecting the related evidence. Forensic science can provide scientific methodology to handling digital evidence, and information science can provide knowledge and technology about internet and information. It can be possible to ensure credibility and probative force of digital evidence in court, by using these two sciences.

#### 4.2 Scientific Evidence

Scientific evidence is the evidence forming or obtaining through the scientific method, such as DNA evidence. Theoretically, there are three conditions deciding whether this scientific evidence is reliable. (1) Effectiveness of the theory. For example, the voiceprint evidence is based on the theory that everyone has a different voice. Because everyone has a different shape of the oral cavity, and learned to speak effected in different environments, everyone has a different voice. (2) Effectiveness of technology. If we accepted the theory of “everyone has a different voice”, the next question will be whether there is an effective technology to distinguish each different individual voice. This theory still remains in the level of theoretical assumption, if there is no effective technology, that it is unable to identify the voice in the real world as evidence. (3) Correctly applying this technology in a particular case. The correct application of this technology depends on several factors: Status of Tools, equipment, and apparatus used; following proper procedures; adequate training and qualifications of the operator and experts.<sup>40</sup> forensic science complies with such a rule, and we can find in the section 2 of this chapter, that forensic science has been emphasizing the integrity of chain of custody and how to ensure the full reliability of evidence.

Social media evidence may be included in scientific evidence, when the evidence

---

<sup>40</sup> Paul C. Giannelli & Edward J. Imwinkelried, *Scientific Evidence* (2 Volume Set), 3<sup>rd</sup> Edition, 1999, Lexis Pub., p. 1-2.

is generated by the machinery system, such as time stamp of sending message, the IP address, etc., or when the evidence is produced by digital forensics, such as proving the reliability of this image print. When falling into the category of scientific evidence, an expert witness is necessary to show in the courtroom to explain evidence with his specialization, and apply the federal rules of evidence §702<sup>41</sup> in American legal system.

On the review standards of scientific evidence being admissible, in the early time, it was adopted General Acceptance Test which means the admissibility of this scientific evidence depends on the scientific theory or technology is accepted generally by its own scientific community.<sup>42</sup> By following this test, admissibility of the scientific evidence ties to the acceptance of a specific scientific community, which equals admissibility of the scientific evidence decided by scientists. The disadvantage is that, with rapid development of science and technology, new technology doesn't mean unreliable, and it is unfair to exclude the new technology just because it has not yet been accepted by most of scientists. Another disadvantage is that, generally accepted is a very vague standard. Since 1993, however, the legal system has shifted to the Reliability Test for whether the scientific evidence is admissible. "*Assessment of whether the reasoning or methodology underlying the testimony is scientifically valid, and of whether that reasoning or methodology properly can be applied to the facts in issue.*"<sup>43</sup> Other factors also need to be taken into account, such as the acceptance and the level of acceptance of theory and technology, error rate, cause of the error, etc. By following this test, the power to determine the admissibility of the

---

<sup>41</sup> Rule 702. Testimony by Expert Witnesses. A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case.

<sup>42</sup> *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). It is known as Frye Test.

<sup>43</sup> *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993). It is known as Daubert Test.

scientific evidence is transferred from scientists to judges. But the judge must reference the experts' opinion, instead of guesswork without reasoning.

#### 4.3 Social Media Evidence

This thesis defines social media as “information extracted from social network sites and used as evidence at court”. Therefore, it can be included in the conception of digital evidence. However, social media evidence emphasizes that information content is generated by the user and focuses on the link between the virtual and the real world in the program. Especially the latter, the nature of high connection with person of social media evidence allows investigating authorities to conveniently establish the relationship between the facts of the case and the perpetrator, such as motivation of crime. On the other side, because of the characteristics of digital evidence (such as easy to copy, hard to identify), it has led investigators to reinforce credibility of social media evidence through other supporting evidence.

When social media evidence is presented to the court as a witness through a forensic expert, the expert witness must follow the scientific evidence-related requirements to investigate it to ensure its admissibility. However, the investigation of scientific evidence is not applicable when the social media evidence is printed or presented in court on the screen in a way that judges or jurors feel directly. In civil law countries, judges will decide the status of social media evidence for different evidence investigation procedures. For example, if social media evidence is presented as the printout, then a documentary survey procedure is used; but if it is presented directly on the computer screen in the courtroom, an inspection proceeding will be used to investigate.

#### **5. Other Similar Characteristics with Digital Evidence**

The Reason this thesis calls that social media evidence has the similar nature with

digital evidence is because it, like digital evidence, has many characteristics different from traditional evidence, such as vulnerable to tampering, possible to recovery, unlimited to copy, hard to identify, cannot directly to sense and understand, difficult to collect evidence, and dependence on the environment.

### 5.1 Vulnerable to Tampering

Taking a traditional document tampering as the example, the tampering must be through a number of ways, such as forged signatures or seals, or altered content, and it may need a precise instrument review, in order to find it out. However, social media evidence, as digital evidence, can be altered or tampered through soft wares, which are easy to find online, and it is difficult to detect the forge or alteration existed. That is, this type of evidence is not only easy to tamper, but hard to detect the alteration, once this evidence has been tampered.

In a case with the issue of tampered time, forensic practitioners will use time stamp of metadata to compare with the asserted tampered time of data. Or we can use a program called “registry” to scan whether a tampering software is used in a specific device. The question is, even though we find this tampering software, a direct connection cannot be built between this software and the asserted tampered data. It is necessary to find more circumstantial evidence to reinforce this argument.

### 5.2 Possible to Recovery

The concept of deleting digital evidence is different from that we can completely delete documents through shredders and incinerators. In a digital space, the instruction of delete means asking the system to mark a release space signal on the location this data occupied, and this location is released to other data. However, before occupied by other file, data still exist but cannot find in the catalog, thus we can use forensic tools to recover it.

In the case of deleting a file through the recycle bin, the data can easily recover by

move out from the recycle bin, because the complete delete need a further instruction to do. But if the file is moved in the recycle bin and further deleted, we can use the “FinalData” program to recover the file. In another case of deleting an email through outlook express, we can also recover this email through the “FinalData” program. Besides, in the case of formatting the disk in window system, we still can recover data inside. Because quick format means to rid of the file tag, and general format means rid of the tag and mark this space can be covered. Both of them has the same meaning with the delete instruction, which is, before occupied by other data, the original data still exists just without a tag. Therefore, if we really want to delete data completely, the “Wipe Disk” program may be used to overwrite the original file in writing zeros or random numbers, to secure no one can use the recovery software to recover the deleted data.

### 5.3 Unlimited to Copy

Digital information carrier has the characteristics of reuse, and the copying of digital information is quick and easy, and unlimited. Moreover, it can disseminate any copy through the storage and transmission equipment. In addition, the form of digital evidence is a coded digit code or mathematical formula. The way of copying is to transfer the whole digital code to other media in sequence, and data can be transformed into what human can sense through the function of the processor. In theory, the signal transmitted only results in correct or garbled as long as no obstacles of transmission device encountered, and through the filter of the debugger, the duplicate of digital evidence is exactly the same as the original one<sup>44</sup>.

Therefore, the digital evidence is different from the copy of the general documentary evidence: copy of general documentary evidence is often copied,

---

<sup>44</sup> Chen-Jung Tsai & Yue-Ting Huang, Admissibility of Digital Evidence, Criminal Law Journal, Vol. 49, No. 2, P.4.

photocopied and other means, which will be different from the original document; however, digital evidence can easily be replicated through computer devices, and its copying speed is not only faster than traditional copy, but also the copy is the same as the original document. Moreover, digital data will not produce a copy different from the original copy, no matter what brand of computer, year and system; but traditional copy may produce shading changes because of the photocopier machine itself<sup>45</sup>.

#### 5.4 Hard to Identify

A document can be identified by the producer's handwriting and other evidence, even if it did not record the producer. But digital evidence raises another risk that the digital file may be produced as a fake identity, which highly possibly cannot be identified or found the real producer. For example, an e-mail can be sent to a third party on behalf of another person's name or account, resulting in increased difficulty in tracing the original sender<sup>46</sup>. The current electronic signature of the identity certification process is to prevent fraudulent use of the situation. Digital evidence is not like fingerprints or DNA (Deoxyribonucleic Acid) can be used as a basis for identifying each person; After investigation, the digital evidence can tell which computer was used to commit the crime, but still cannot directly know who the defendant is<sup>47</sup>. That is, in the case of digital evidence, though it is possible to identify by IP what kind of digital evidence is generated by this computer, it is difficult to judge whether the digital evidence was made by this computer user or transmitted by other computer users as long as someone obtains others' password to use others' computer. Especially in the case of social media evidence, social network sites require users accessing websites by accounts and passwords. Although the police and

---

<sup>45</sup> Chiou, Shian-Min & Lin, Yi-Long, The Offensive and Defensive Countermeasures of Digital Evidence in Court, *Journal of Information, Technology and Society*. Vol. 7, No. 1: p. 56.

<sup>46</sup> Shih-Chieh Chien, Shih-Feng Chien, Chia-Ming Liu, & Shao-Pin Chang, *Computer Forensics and Corporate Security*, Kingsinfo Press: Taiwan, 2004, p. 3-5.

<sup>47</sup> ICCL, True and False Digital Evidence, *Connectimes*, No. 170, 2005, p.91.

investigative authority can find the applicant by his account or IP dress, if the perpetrator is using an unlock wireless network or use someone else's wireless network password to connect the internet, the owner of the account, as found through IP, may not be the real perpetrator. Hence, digital evidence takes on hard-to-identify characteristic.

We can easily point out what this computer has done, but it is impossible to determine who is using this computer to perform this action. Digital data cannot be recognized by handwritings in the document. Even though the digital data have been marked the producer's name, its authenticity can sometimes be questioned. Therefore, it is not easy to confirm the producer by the digital content itself, but still need to be determined through other relevant facts or the assistance of computer-related technology.

#### 5.5 Cannot directly to Sense or Understand by Human

Digital evidence is electronically stored on electronic media<sup>48</sup>, such as CDs, flash drives, memory cards and more, which cannot be directly observed by the perception of human understanding if not through the specific display or printouts. Further even though the display can display the contents of digital data, the original file cannot be directly understood through display or its printouts. For example, the picture displayed on the web page we can directly see on the computer is the result of executing the browser program. However, if we view the original page of the webpage, it is mostly a long list of commands and numbers which lay people cannot directly identify the meaning represented by seeing, or one cannot directly interpret the image shown by the code<sup>49</sup>. Therefore, on the one hand, digital data is stored on

---

<sup>48</sup> Chen-Jung Tsai & Yue-Ting Huang, Admissibility of Digital Evidence, Criminal Law Journal, Vol. 49, No. 2, P.4.

<sup>49</sup> Chiou, Shian-Min & Lin, Yi-Long, The Offensive and Defensive Countermeasures of Digital Evidence in Court, Journal of Information, Technology and Society. Vol. 7, No. 1: p. 58.

electronic media, and contents of the digital data cannot be directly understood from its outfit; on the other hand, when using a display to show the digital evidence, it generally cannot be interpreted directly, if only the source code is displayed. Instead, it must be perceived and understood from the appearance through the result of program execution. In other words, the situation is similar to that of audio and video tapes. People have to display tapes on the equipment in order to listen or watch the contents of tapes. But they can directly recognized photos or documents by human perception without any conversion.

### 5.6 Difficult to Collect

Digital data is extremely annoying and may disappear in just a few seconds. Compared with the general criminal cases, the perpetrators may take dozens of times or even hundreds of time to deal with the knife, blood clothes and other things that can be evidence. Therefore, it is more difficult to obtain digital evidence than the general evidence<sup>50</sup>. Some digital evidence has the nature of temporarily exist, which usually disappear over time or after the computer is turned off, and it is hard to be collected at the first moment. Especially collecting information and other internet activities from websites, unless we keep monitoring the records, we can only leave a record of the connection and it is difficult to collect a complete set of evidence<sup>51</sup>. In addition, digital evidence can easily spread around the world via Internet connection, completely ignoring the existence of "national borders" in the real world, and making it difficult to be collected for the purpose as evidence at court<sup>52</sup>.

### 5.7 Dependence on the Environment

---

<sup>50</sup> Chen-Jung Tsai, & Wei-Ting Chang, Research on Computer Crime Evidence, Criminal Law Journal, Vol. 44, No. 2: p. 50.

<sup>51</sup> Shih-Chieh Chien, Shih-Feng Chien, Chia-Ming Liu, & Shao-Pin Chang, Computer Forensics and Corporate Security, Kingsinfo Press: Taiwan, 2004, p. 3-6.

<sup>52</sup> Shih-Jeng Wang, Hung-Jui Ke & ICCL, Information and Network Security: Eyes of Secret –State of the Art on Internet Security and Digital Forensics, DrMaster Press: Taiwan, 2006, p.589.

Information extracted from social network sites is based on the result of 0 and 1 binary operations. Inputs, storage, and outputs must rely on computer devices and soft wares. It would drive a result which the credibility of digital evidence is doubtful, if the hardware performance and operating conditions that produce and store digital data are not reliable, or the software program on which the computer depends is not reliable. Further, with the continuous improvement of technology, hardware and software equipment are continuously updated. If the compatibility between the old system and the new system is not good enough, the digital data cannot be accessed, so the digital evidence will be questioned. Or because computer access format changes, digital data only can be read through a certain format conversion. In the process of the format conversion, it is likely to cause the original data to be changed or destroyed, thus the digital data will lose the admissibility of evidence.

## **6. Summary**

In sum, we can see that social media evidence entails the characteristics of social network sites: (1) Participation. Social network sites encourage participation and promote feedback from site user. (2) Community. People can create their own community and share their common interests. This community can be a place to share information and gather information. (3) Public. Most social network sites enables user feedback and contribution in a way user can interact with others publically. Thus there are fewer barriers to access and use of these sites. (4) Communication. While traditional media provide one-way communication, social network sites provide two-way communication. (5) Connection. Most of social network sites getting popular by having more users and users connection to other members of the site. Sites also help users get in touch with those people whom the users no longer meet in their daily life. With these characteristics, social media evidence not only is a good source for government investigators to obtain criminal evidence, but also connect the criminal

and the offense and prove the defendant's motivation, which is the hardest part to prove in the criminal proceeding.

In format of evidence, social media evidence is a type of digital evidence, differentiating from objective items and witnesses to express their opinions. While presenting in the courtroom, the common way is to print the content of website pages out, as a document. It is also applied the rules for scientific evidence, when this social media evidence is produced by forensic practitioners via forensics, instead as the printout or screen shot by the police or lawyers.

According to descriptions above, we can extract features of these SNS. They are a profile page with basic personal information, public friending with public friends list, public commenting on friends' profiles, blogs, Photographs, instant (private) messaging, groups or discussion groups, gift giving, music playing, videos and games. Furthermore, if the police extract information from these websites and use them as evidence, now we define this kind of evidence as social media evidence. It shows this evidence is from web-based media and will be used based on its online connections. The most popular social media for investigators is SNS, such as Facebook and MySpace. The common types of social media evidence are photos, posts, friend list and location.

## Reference

1. Adkins J (2011), Law Enforcement Guide to Social Media, Special Research Report, p. 1.
2. Brunty, Joshua and Helenek, Katherine (2013), Social Media Investigation for Law Enforcement, Anderson: USA.
3. Chen-Jung Tsai & Yue-Ting Huang, Admissibility of Digital Evidence, Criminal Law Journal, Vol. 49, No. 2, pp. 1-32.
4. Chen-Jung Tsai, & Wei-Ting Chang, Research on Computer Crime Evidence, Criminal Law Journal, Vol. 44, No. 2: pp. 49-63.
5. Chiou, Shian-Min & Lin, Yi-Long, The Offensive and Defensive Countermeasures of Digital Evidence in Court, Journal of Information, Technology and Society. Vol. 7, No. 1: pp. 53-64.
6. danah m. boyd & Nicole B. Ellison (2008), Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication. 13: pp. 210–230.
7. Eoghan Casey, Digital Evidence and Computer Crime, Third Edition, 2011, Academic Press.
8. Graham C. Lilly, An Introduction to the Law of Evidence, 2nd ed., West Publishing, N.Y., 1987, at 512-515.
9. Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-86, 2006, available at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

10. Larry E. Daniel & Lars E. Daniel, Digital Forensics for Legal Professionals- Understanding Digital Evidence from the Warrant to the Courtroom, 2012, Elsevier: Ma, USA.
11. Paul C. Giannelli & Edward J. Imwinkelried, Scientific Evidence (2 Volume Set), 3rd Edition, 1999, Lexis Pub.
12. Samir Datt, Learning Network Forensics, 2006, Packt Publishing.
13. Shih-Chieh Chien, Shih-Feng Chien, Chia-Ming Liu, & Shao-Pin Chang, Computer Forensics and Corporate Security, Kingsinfo Press: Taiwan, 2004.
14. Shih-Jeng Wang, Hung-Jui Ke & ICCL, Information and Network Security: Eyes of Secret –State of the Art on Internet Security and Digital Forensics, DrMaster Press: Taiwan, 2006.

## **Chapter 2 Social Media Evidence in Criminal Procedure**

Since social media evidence is defined as information extracted from social network sites, used as evidence in court to proof crimes or refute allegations, there are two parts can be discussed: the subject is evidence in court and the other is information from social network sites. This chapter will discuss the possibility and problems that social media evidence is recognized in court, and by comparing the rules of evidence of the United States law (common law) and the Taiwan law (civil law), to find the general principle of social media evidence. The second part that how the information is actually obtained from social network sites will be discussed in Chapter 3.

### **Section 1 Difference between Taiwan and American Legal System**

The biggest difference between the Taiwan legal system and the American legal system is that the former is the civil law system; the latter is the common law system. In American legal system, the function of jury is used to determine the facts, and the judge decides the use of law in accordance with its determination. But judges in Taiwan legal system should make the whole judgement including fact determination and law application.

In the evidence law, regulations of these two legal systems are similar. In general, the evidential material must be legally obtained, admitted by court, be legally investigated in the courtroom, and then weighted its value by the jury or the judge. But rule of evidence in American law can apply to both civil and criminal cases, in which almost all of the terms unified apply every case regardless of the nature of litigation. The only exception is, due to the difference between the nature and purpose of civil and criminal law, that rules of criminal evidence have more stringent requirements than the rules of civil evidence in terms of burden of proof and proof of

standards.

## **1. Rule of Evidence in America**

The characteristics of the American legal system are confrontation and the jury system. Among them, the jury system is used to identify the facts of the case. In a jury trial, the judge does not engage in the determination of the facts, but acts on the control of the proceedings and applies the law in accordance with the facts as determined by the jury. The purpose of the jury system is to check and prevent the judge from arbitrary abuse of power, so the jurors are chosen from lay people without legal training. A problem arises, that is, how the jury should make the appropriate decision of facts in a particular case. The jurors have not been trained by law, and their opinions of facts may be subject to intentional or unintentional guidance and make prejudice under the influence of arguments between the parties (prosecutors and defenders). In order to prevent such inappropriate evidence will be presented in the trial and confuse the jury to determine the facts, the rule of evidence in American legal system ask the judge to determine the admissibility of evidence. The unqualified evidence should be excluded, and not be allowed as a basis for determining the facts.<sup>53</sup> Only the admissible evidence can be presented in the courtroom, and becomes the object judged by the jury.

In addition, Anglo-American law is based on party-oriented, that the parties will be their own litigation interests to make the greatest efforts of the confrontation. Based on this idea, the litigants have the power to investigate and submit evidence, which is different from the civil law system in respect of court litigation obligations. In the case of cyber evidence often used by SME, the application of the expert witness system in the court structure of such confrontation is the same as that of the civil law

---

<sup>53</sup> Graham C. Lilly, Daniel J. Capra, and Stephen A. Saltzburg, *Principles of Evidence*, 5<sup>th</sup> edition, Thomson Reuters: USA, 2009, pp. 23-27.

system. However, with the civil law system attempt by the neutral judge selected experts to make an objective appraisal report is different, the expert witness system for the way through the confrontation to find the truth, so by the fact that the most understanding of the dispute, the most interested in the parties Elect expert witness.

The rules of the Federal Rules of Evidence are divided into Chapter 1, "General Principles", Chapter 2 "Judicial Cognition", Chapter 3 "Presumption of Civil Action and Procedure", Chapter 4 "Evidence relevance and its limitations Chapter 5 "Refusal of Testimony", Chapter 6 "Witnesses", Chapter 7 "Opinions and Expert Testimonies", Chapter 8 "Rumors", Chapter 9 "True Certificates and Recognition", Chapter 10 " Documents, records and photographs "and Chapter 11" Other Provisions ". The law of evidence in the United States is divided into several stages: relevance (admissibility) credibility (credibility). In the case of a jury, the relevance and admissibility of the preceding stage shall be evidenced by the judge's judgment as to whether the evidence is admissible. Those who are deficient should be excluded from evidence. If the evidence is provided with such an admissibility, the credibility of the evidence at the post-stage stage shall be examined, that is, the extent to which the evidence may be accepted. And this judgment of the credibility of the fact that the scope of the matter, it should be decided by the jury. In the light of the admissibility of the law of evidence and the application of the exclusionary rule, the judge first filters the evidence and then the jury to measure the value of the evidence. Therefore, it is only the standard of the judge to judge the evidence, and it is not the measure of how much the evidence can prove the effect of the fact.

## **2. Rule of Evidence in Taiwan**

Taiwan legal system as in general adopted the civil law system, developing the written codes, and emphasizing on the court to lead the entire proceedings. The

Criminal Procedure Law was enacted in 1928, mainly in accordance with the provisions of the German Code of Criminal Procedure, and the law of evidence is also included in the Code of Criminal Procedure Law. Criminal cases by the prosecutor to prosecute, the court to hear; litigation party dissatisfied with the verdict, they can appeal up to the courts of the third instance. Court of the first instance or District Court and Court of the second instance or High Court is responsible the fact trail, and the function of court of the third court or Supreme Court is trail of law. However, in 2003, in order to meet the needs of the community, a substantial amendment to the Criminal Procedure Law, the most important evidence for the criminal law, also in the revision of a substantial revision. The direction of this amendment is mainly to study the United States criminal procedure law, to strengthen the prosecutor's burden of proof and the confrontation between the parties to the status. In the case of evidence, the hearsay rule now is introduced in Taiwan legal system.

Therefore, the existing law of evidence in Taiwan is mainly to require the prosecutor to bring the burden of evidence, and bear the burden of proof; the court only to supplement the right to investigate evidence. An evidence must be legally obtained (evidence to exclude the law), consistent with the statutory evidence method and after a legitimate investigation, the ability to obtain evidence, the judge was able to obtain evidence of evidence, according to their free evidence for the basis of the conviction. This is in contrast to the fact that the jury has decided that the judge is a legal decision.

## **Section 2 American Law**

This section will discuss how the information extracted from a social network site becomes the admissible evidence presented in the American courtroom; that is, we will discuss the admissibility of social media evidence through rule of evidence in

American. To establish the general principles, this section will focus on the federal rule of evidence, which can apply through the most cases in American.

General speaking, materials or information will be examined in a procedure before they comes out as evidence at trial. A foundation, used in determining or actually constructing the past fact, should be based on evidence which is filtered by the criminal proceeding and then get admissibility. This filter mechanism can filter undiscoverable, irrelevance, or inadmissible materials, based on rule of law.<sup>54</sup> On the other hand, through this filter mechanism excluded such evidential materials, evidence being discoverable, relevance, and admissible will be introduced at trial, and will be used to construct the past fact. This is the legal approach to secure purposes of the criminal and criminal proceeding by filtering one element and another.

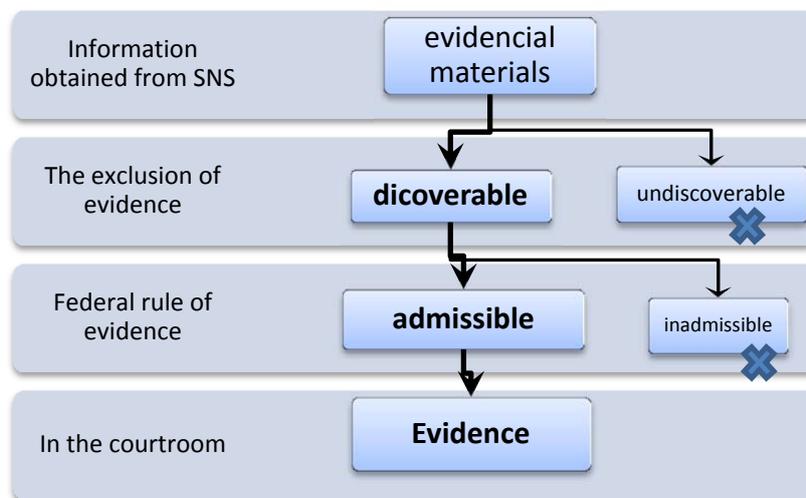


Figure 2 Evidential Materials filtering process

Two elements are in this filter mechanism, negative and positive. The negative element is that the evidential material should not be falling into the Exclusionary rule; in other words, the investigators are not allowed to obtain or gather information with

<sup>54</sup> The rule of law is the legal principle that law should govern a nation, as opposed to being governed by arbitrary decisions of individual government officials. It primarily refers to the influence and authority of law within society, particularly as a constraint upon behavior, including behavior of government officials. [https://en.wikipedia.org/wiki/Rule\\_of\\_law](https://en.wikipedia.org/wiki/Rule_of_law)

any means, and otherwise, those illegally obtained evidentiary materials will be thought undiscoverable, connected to the result of infringing the fourth amendment, to be excluded. For example, when the investigator tortured a defendant to obtain his confession,<sup>55</sup> this evidentiary material (the defendant's confession) is lead to be excluded. Once the evidentiary material is excluded, it has no chance to go into this filter mechanism, even with the positive element, and has no chance to become the evidentiary foundation. The premise of the evidentiary material going into the positive elements of filtering is not to be exclude, or in American system, to be discoverable.

The positive element is that, these legally obtained evidentiary materials will be proved at trial in accordance to type of evidence in law and its requesting proof procedure, and then they become evidential foundation of forming the truth. Types of evidence in law and its requesting proof procedure are regulated by different legal systems, although they share most of rules of evidence. For example, when the evidentiary material is a statement of the eye witness, the requesting proof procedure is to show this witness in the courtroom and to cross-examine his words by both parties. The positive element is varied and regulated in evidence law. In American legal system, the positive element is relevancy and admissibility which includes hearsay, authentication, the best evidence rule, and character evidence under the federal rule of evidence.

Therefore, through this filter mechanism getting discoverability and admissibility, only this evidentiary material becomes the evidence allowed at trial, and the object to be valued by jury.

Information obtained from social network sites shall be filtered in this system

---

<sup>55</sup> See Article 3 of the European Convention on Human Rights, "No one shall be subjected to torture or to inhuman or degrading treatment or punishment."

without any exception. After getting discoverability and admissibility, information is transformed as social media evidence adopted in the legal system. This social media evidence can be the object valued by the jury and can be used to build the fact.

Besides, although this filter mechanism is shared among legal systems, there is a difference among them, that is, to build a mechanism with a different structure of laws in different legal systems. Most of civil law countries regulate this filter mechanism in a chapter of evidence in the code of criminal procedure. On the contrary, as the case law country, American legal system restricts investigating tools under the bill of right in constitutional law, as well as the Exclusionary rule built by the Supreme Court, in order to form the first negative stage, also known as “discoverability”. Then, they set the second positive stage in the rules of evidence, including relevancy and admissibility. We will discuss the whole legal procedure from obtaining information on social network sites and transforming it to evidence at trial, in order to show that, how to form the evidence admitted by law through this filter mechanism.

### **3. Discoverability of Evidence**

Discoverability of Evidence is the mechanism to control the prosecution using legal-admitted way to obtain information as evidence. Connecting to the exclusionary rules, it will be excluded if the investigators obtain evidential materials with an illegal way. Also this kind of evidential materials is neither introduced into the trial, nor becomes the foundation of fact-finding. Thus, discoverability, equaling to not-excluded evidence, is the negative element while information becomes the evidence at trial. For regulating this situation, the most important regulation to control is the fourth amendment, which states,

*“The right of the people to be secure in their persons, houses, papers, and effects,[a] against unreasonable searches and seizures, shall not be violated, and no*

*Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”*

The fourth amendment is set for the protection of people’s privacy. The Supreme Court formed the conception of privacy derived from the extension of property in the early time; that is, whether there is an infringement of the fourth amendment depends on whether there is an invasion of people’s Trespass by the government. In *Olmstead*, the police did not invade the defendant’s Trespass, but tapped outdoors. Thus, it did not constitute an illegal search seizure in this case, because the police did not invade the defendant’s Trespass.<sup>56</sup> However, in the case of *Katz*, the Supreme Court turned over the precedent, to rebuild the connotation of the fourth amendment. The Supreme Court held from the privacy aspect, the fourth amendment should protect people’s expectation of privacy, instead of property here. Therefore, even though this disputed investigative mean of tapping the public phone line is the public area, it still invaded the defendant’s expectation of privacy.<sup>57</sup> This theory also constituted the privacy basis of other cases. For example, people has the reasonable expectation of privacy on their telephone or telecommunications, thus, the government need to follow the fourth amendment requirement, while conducting a search on one’s telephone or telecommunications. This *Katz* case has been implementing so far and also formed

---

<sup>56</sup> *Olmstead v. U.S.*, 277 U.S. 438 (1928). The court held “*Evidence of a conspiracy to violate the Prohibition Act was obtained by government officers by secretly tapping the lines of a telephone company connected with the chief office and some of the residences of the conspirators, and thus clandestinely overhearing and recording their telephonic conversations concerning the conspiracy and in aid of its execution. The tapping connections were made in the basement of a large office building and on public streets, and no trespass was committed upon any property of the defendants. Held, that the obtaining of the evidence and its use at the trial did not violate the Fourth Amendment.*” (Pp. 457-)

<sup>57</sup> *Katz v. U.S.*, 389 U.S. 347 (1967). The fact in this case is that “*petitioner was convicted under an indictment charging him with transmitting wagering information by telephone across state lines in violation of 18 U.S.C. § 1084. Evidence of petitioner's end of the conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the telephone booth from which the calls were made, was introduced at the trial. The Court of Appeals affirmed the conviction, finding that there was no Fourth Amendment violation, since there was "no physical entrance into the area occupied by" petitioner.*”

the limitation to the government launching a search or seizure in the privacy zone.

### 3.1 Rules for Search and Seizure

#### 3.1.1 The Standard: Reasonable Expectation of Privacy

Justice Harlan concurred in *Katz*, and provided an analysis to determine whether the governmental investigation has applied the fourth amendment. According to Harlan's theory, the range guaranteed by the fourth amendment is structured by the specific person's reasonable expectation of privacy. The reasonable expectation of privacy is a twofold requirement: first, "*a person has exhibited an actual (subjective) expectation of privacy*" and second, "*that the expectation be one that society is prepared to recognize as "reasonable."*" Later, it widely accepted as the standard for applying the fourth amendment. Thus, a legal search governed by the prosecution should be examined and comply with the following steps, in accordance to requests of the constitution.

First, the investigators must to make sure whether their conduct constitutes a search under the fourth amendment. That is, investigators must to make sure this searched subject's reasonable expectation of privacy. If this subject has a reasonable expectation of privacy, the search conducted by investigators must to fulfill requirements under the fourth amendment; but if he has no expectation of privacy, then requirements under the fourth amendment is not applied for investigators' searching conducts, which means this search can be implemented without warrant.

Second, if this search constitutes the conduct regulated by the fourth amendment, then investigators generally need a warrant issued by the judge to implement a legal search. To apply a warrant, investigators must clarify probable cause, and describe the searching range in detail to convince the judge to issue the warrant.

Third, if an under-the-fourth-amendment search is implemented without a warrant, exceptions should be considered. Exceptions are built by the case law, and must be limited in order to avoid too many exceptions replace the general rule. If the case is falling into one of exceptions, the search is legal, even though without warrants.

Fourth and finally, if a warrantless search is conform to the situation of the fourth amendment and doesn't fall into any exceptions, it is illegal and will cause the effect of excluding evidence obtained from this illegal warrantless search.

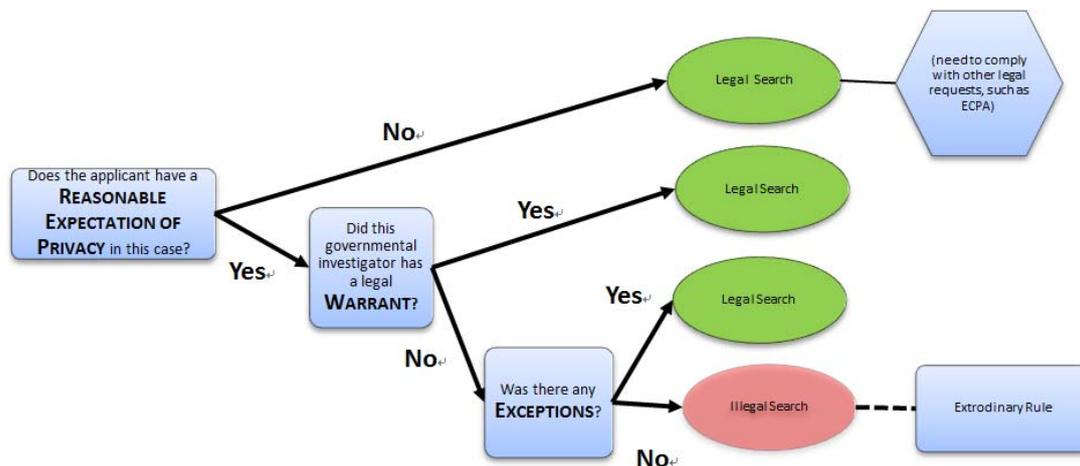


Figure 3 Search and Seizure under the 4th Amendment

### 3.1.2 Operation Rules of Search on Social Network Sites

In order to make sure the fourth amendment guaranteed, legislates regulate investigations and prosecutions, and provide them four legal tools in the Federal Stored Communication Act (SCA)<sup>58</sup> for utilizing social media sites.

#### (1) Preservation/Hold Letters<sup>59</sup>

<sup>58</sup> 18 USC §2701-2712.

<sup>59</sup> 18 USC §2703 (f)(1).

In SCA, the authorized governmental entity can require the specific social media provider preserve required records in any effort for a period of up to 90 days. The preserving time can be extended for another period of up to 90 days, if it is necessary. The required records include the system generated data, instead of users' information or contents. It should be note that, this request for preservation is only for preserving data existed in the system, but not for those in the future. Because preservation for the future data similarly equals conduct of wiretapping, this needs a warrant issued by the court and regulated by the Surveillance Act.

## (2) Subpoenas

A subpoena is an administrative order issued by the grand jury, and authorized the prosecution to require a social media provider providing relevance information. Since its administrative nature, the specific effect will be different by jurisdictions, and the police need to consult the prosecutor before they submit an application for the subpoena. With a subpoena, investigators can ask the social media provider to provide information such as name, length of service, credit card information, email address, and a recent login IP address. The range of provided information with a subpoena is wider than that with a preservation; to apply a subpoena is easier than to apply a warrant. Thus, a subpoena is the most common tool for the investigation. These subpoenas are limited by privacy right set forth in the Electronic Communication Privacy Act ( 18 USC 2510 ) .<sup>60</sup>

Although the subpoena is administrative, in the case of *People v. Harris*,<sup>61</sup> the courts star to note the constitutionality that the investigators use it to obtain information from social media evidence. Thus, the investigation cannot use the

---

<sup>60</sup> Brunty, Joshua & Helenek, Katherine (2013), *Social Media Investigation for Law Enforcement*, Elsevier Inc., MA: USA, p.79.

<sup>61</sup> *People v. Harris*, 945 N.Y.S.2d 505(Crim. Ct. 2012).

subpoena to replace a warrant in the case related to the privacy issues.

### (3) Court Orders (D order) <sup>62</sup>

With a court order, investigators can ask the social media provider to provide information, which includes not only records, but other information pertaining to the social media account and the basic subscriber records. It should be noted that, content of communication, including message headers and IP addresses, doesn't include in the range of information requirement with D order. However, investigators rarely apply for the D order, when they want to obtain the social media evidence, because of the high threshold for applying the D order. When an investigator wants to apply the D order, he needs to submit the application with specific and articulable fact, and prove that fact to the degree of reasonable belief. In the case of social media evidence, the threshold, a fact with reasonable belief, cannot be easy to satisfy, based on the nature of highly uncertainty of social media evidence. With the D order, investigators can gather more than just subscriber information.<sup>63</sup> The range of the D order depends on transactional information provided by the investigators, which can prove to be effective in tracing down and determining use on a specific social network site. Besides, some of social media providers have the policy, that they have an obligate of user notification, when the investigators require gathering the user's information on the social network sites. This notification some time will raise risks of evidence loss and difficult investigation. Thus, it is allowed the investigators stated on the D order, that this provider should not notify the user, in order to ensure obtaining evidence.<sup>64</sup>

---

<sup>62</sup> 18 USC §2703 (d).

<sup>63</sup> Subscriber information means any information held by a service provider, relating to subscribers of its services, other than traffic data or content data, and by which can be established: (i) the type of communication service used, the technical provisions thereof, and the period of service; (ii) the subscriber's identity, mail address, telephone and other access number, billing and payment information, and/or (iii) any information regarding the location of installed communications equipment. [http://itlaw.wikia.com/wiki/Subscriber\\_information](http://itlaw.wikia.com/wiki/Subscriber_information)

<sup>64</sup> Brunty, Joshua & Helenek, Katherine (2013), see supra note 60, Pp. 79-80.

#### (4) Search Warrants

The investigator can directly search the service provider or the suspect with a warrant. For apply a lawful warrant, the investigators need to follow a legal proceeding with sufficient diligence, and explain the probable cause in this case. The probable cause “*exists where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime can be found.*”<sup>65</sup> In the case of social media evidence, the difficulty is to define the search object, because the nature of social media evidence is information, instead of physical premises or objects, if an investigator wants to explain a probable course in this social media evidence case, he must visualize relevant information. The range for search social media evidence with a warrant includes messages, photos, videos, wall posts and location information to name etc. Different with other three tools, investigators can search not only records but content in the websites. Thus, the warrant is not only the most comprehensive range of search but also the most stringent threshold forensics tools.

The following scenarios will distinguish searches with a warrant or without a warrant, in order to discuss the legality that the investigating authorities launch a search in a specific situation.

#### 3.2 Obtain Evidence from Public Domain

Investigating authorities prefer for mining social network sites for evidence, especially those information from public domain. As mentioned above, this search subject has no reasonable expectation of privacy in the public domain, even though it

---

<sup>65</sup> *Ornellas v. United States*, 517 U.S. 690, 696 (1996). Also see Brunty, Joshua & Helenek, Katherine (2013), see supra note 60, p. 80.

is in internet. Even without a warrant and subpoenas, investigators can still find thousands of SME in open public areas. Especially people are careless on information they spread on social network sites.<sup>66</sup> Besides, a lot of people use social network sites,<sup>67</sup> but few pay attention to their privacy settings.<sup>68</sup>

Even though the user makes his privacy setting, however, the user may not be able to hold the protection of privacy. In order to bypass the warrant requirement, investigators may obtain information by creating a fake identity in the internet or seeking for a cooperating who happened to be a Facebook friend with the search subject, which will pierce the privacy protection of privacy setting on social network sites. In the case of *United States v. Meregildo*,<sup>69</sup> the defendant limited his information only for a group of friends, but the investigators still obtain these information by a cooperate witness who happened to be one of his friends. They gathered a huge amount of evidence from the defendant's Facebook. The defendant argued that this investigating conduct has already invaded his right guaranteed by the fourth amendment and moved to suppress the evidence gathered on his Facebook account. In this case, the court analogized the expectation of privacy recognized telephone conversation in the case of *Barone*<sup>70</sup>, to that in this case related to privacy setting on Facebook. In *Barone*, if the investigators record the phone conversation at least obtaining one party's consent, the other party cannot raise a reasonable

---

<sup>66</sup> 8 Dumb Criminals Caught Through Facebook, available at, <http://mashable.com/2012/12/12/crime-social-media/#28Chlc9FLag9>

<sup>67</sup> For example, as of the second quarter of 2016, Facebook had 1.71 billion monthly active users. available at, <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

<sup>68</sup> According to the statistic, twenty five percentages of Facebook users do not use any type of privacy control. See Shea Bennett, Facebook, Twitter, Pinterest, Instagram-Social Media Statistics and Facts 2012, All Twitter (Nov. 1, 2012, 6:00 AM), available at, <http://www.adweek.com/socialtimes/social-media-stats-2012/472135>

<sup>69</sup> *United States v. Meregildo*, No. 11 Cr. 576(WHP), 2012 WL 3264501 (S.D.N.Y. Aug 10, 2012).

<sup>70</sup> *United States v. Barone*, 913 F.2d 46, 49 (2d Cir.1990), (finding that a person does not have a legitimate privacy expectation in telephone calls recorded by the Government with the consent of at least one party on the call.)

expectation of privacy. Back to this case *Meregildo*, the defendant sharing information with his Facebook friend by the privacy setting; on the other side, his Facebook friends can freely obtain his information shared on his Facebook. The court stated, even though the defendant has a reasonable expectation of his own privacy, he has no expectation on that his friend must keep his shared information in private. When he spread information to his Facebook friends, his reasonable expectation on that information is end. Because those friends can freely access, print, or transfer that information, and share with the government. The court concluded that, there is no violation of the fourth amendment, that the investigators obtained limited-accessed information through the defendant's Facebook friend.

### 3.3 Search with a Warrant

#### 3.3.1 Probable Cause

According to the fourth amendment, when implementing a search and seizure, investigators need to explain a probable cause in the case, and point out the specific place for search and the person or the property they want to seizure. To prove the probable cause existed, investigators must reasonably confirm that a crime has occurred, evidence related to the crime exists, and that evidence of crime is currently located in the place to be searched.<sup>71</sup> The Supreme Court stated, in an application for search and seizure must has “*a fair probability that contraband or evidence of a crime will be found in a particular place.*”<sup>72</sup> It cannot set up the ground of a probable cause, if investigators only provide their suspicions of crime and evidence might be found in that place.<sup>73</sup> However, the Court never requests investigators' knowledge of a precise form of evidence or contraband they want to search or seizure. In the case of *United*

---

<sup>71</sup> Robert W. Taylor et al., *Digital Crime and Digital Terrorism* 244 (2006).

<sup>72</sup> *Illinois v. Gates*, 462 U.S. 213,238 (1983).

<sup>73</sup> *Brinegar v. United States*, 338 U.S. 160, 175 (1949).

States v. Reyes, the Court pointed out that, we cannot expect that a warrant can predict a precise form of evidence to be searched in this era of rapidly changing technology.<sup>74</sup> Investigators do not need to know that who owns the property to be searched.<sup>75</sup> A precise form and the property right have no influence on setting up a probable cause.

When investigators want to obtain the related evidence by searching a specific person's social network sites, usually their belief ground derives from a particular network or IP location of the account records. But it cannot prove the user's identify or location by just knowing an account or the IP location used. In this situation, the Court responded that, when the investigators want to set up a probable cause by a social network sites account or the IP address to apply a warrant for search, they need to provide additional information, proving the relationship between the records and the place to be search.<sup>76</sup>

### 3.3.2 Requirement of Particularity

The second requirement for apply a warrant for search is a specific description for the range to be search, as the fourth amendment states, "particularly describing ... the persons or things to be seized." This requirement is to prevent the investigators use a general warrant<sup>77</sup> to search any one's property in everywhere to find the evidence. In tradition, the court asks for two elements in line with the requirement of particularity. First, a description of property to be search should be precise enough to identify the search objects and other unrelated properties.<sup>78</sup> Second, the description should not be

---

<sup>74</sup> United States v. Reyes, 798 F.2d 380, 382 (10<sup>th</sup> Cir. 1986).

<sup>75</sup> United States v. McNally, 473 F.2d 934, 942 (3d Cir. 1973).

<sup>76</sup> United States v. Hay, 231 F.3d 630, 634 (9<sup>th</sup> Cir. 2000); United States v. Grant, 218 F.3d 72, 76 (1<sup>st</sup> Cir. 2000).

<sup>77</sup> Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

<sup>78</sup> Marron v. United States, 275 U.S. 192, 296 (1925); Davis v. Gracey, 111 F.3d 1472, 1478 (10<sup>th</sup> Cir. 1997).

too broad to include properties which cannot be searched.<sup>79</sup>

The cases on “particularity” are actually concerned with at least two rather different problems: one is whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized. It is difficult to apply these standards on obtaining social media evidence, because information on social network sites not only includes postings and photos, but includes profile (such as name, date of birth, address, current city, education, e-mail, gender, hometown, etc.) , records of internet activities, relationships of friends (such as the friends list, the groups, etc.), log files, face recognition data, locations, and records of external links account. This information is likely to be evidence in the case, but range of this information is quite unspecific. This is a dilemma: If we allow the investigators only provide the account to be search, then it is possibly a general warrant; but if we ask the investigators to describe the range to be search precisely, then some evidence might be missing because of an investigator’s poor knowledge. Thus, the investigators prefer to search the public area on the websites first, or use a subpoena asking the service providers to provide all information, instead of applying a warrant.<sup>80</sup>

Although there is no case on requirement of particularity about a search warrant for social media evidence, cases about searching computer for the digital evidence can be the references, because social media evidence has the same characteristics with digital evidence. If the investigators have a warrant, in which it describes the search objects are all computers and related stored devices, does this decryption break the requirement of particularity? In the case of *United States v. Hunter*, the Court held that

---

<sup>79</sup> *United States v. Upham*, 168 F.3d 535 (1999).

<sup>80</sup> Brunty, Joshua & Helenek, Katherine (2013), see *supra* note 60, Pp. 79-80.

it did not satisfied with the requirement of particularity under the fourth amendment, if a description on the warrant described the search objects as all computers, stored devices and soft wares.<sup>81</sup> The Court measured overall the case and held that, due to computers store vast numbers of records and computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent, “*Computer records searches are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy.*” On the contrary, in the case of *United States v. Upham*, the Court thought that, even though investigators described search objects as all computers and stored devices on a search warrant, it violated the requirement of particularity under the fourth amendment. The Court made the judgment depending on the specific situation in this case, that is, only when investigators conduct a comprehensive search, to ensure the discovery of evidence to be searched can be possible. Therefore, in this case, a search in all computers and stored devices is not extensive, but necessary.<sup>82</sup> Under this two cases followed by others, we can conclude that, the Court does not consider the requirement of particularity alone, but consider the presenting case as the whole to weigh different factors and values involved. Even though the conclusions are different, both of the Courts weigh different factors and values in the case, which is to weigh the interests of privacy protection under the Fourth Amendment and the interests of the state prosecution.

Besides, scholars also provide a theory, which takes the purpose of search as the baseline of requirement of particularity. When the computer itself is the evidence of a crime, the result of the crime, or the tool for committing a crime and the purpose of search is the computer and stored devices, investigator must describe the computer

---

<sup>81</sup> *United States v. Hunter*, 13 F. Supp. 2d 574 ( D. Vt. 1998).

<sup>82</sup> *United States v. Upham*, 168 F. 3d 532 ( 1st Cir.1999).

and stored evidence as search objects on the warrant. If the purpose of search is information stored in the computer, the description on this warrant should be to search for the related document files, but the stored devices.<sup>83</sup>

### 3.4 Exceptions<sup>84</sup> for the Search without Warrant

People have rights to be secure in their persons, houses, papers, and effects, and against unreasonable searches and seizures, which are guaranteed by the fourth amendment. Therefore, it requires a warrant when the government implements a search or seizure to the suspect or his belongs. However, there are some exceptions of a warrantless search recognized by the case law, which means, investigators can implement a search without warrant. Exceptions recognized by the case law are Search with Subject's Consent, Exigent Circumstances, Plain View Doctrine, and Search Incident to Lawful Arrests. Every exception has its own context and background, and the courts need to make their argument clearly, especially their weight for values. An exception admitted means reducing the guarantee by the fourth amendment. Thus, it is doubt to directly imply these exceptions in the case of social media evidence. The courts should build their arguments of these exceptions for social media evidence, if it is necessary. Here we will discuss the existed cases related to computer evidence to draw the line for social media evidence.

#### 3.4.1 Search with Subject's Consent

In general, the prosecution can implement a warrantless search, when people have the right to give a voluntary consent to search, even though there is no probable

---

<sup>83</sup> Thomas A. Johnson, Computer Crime and the Electronic Evidence, in Forensic Computer Crime Investigation (Thomas A. Johnson ed., 2006).

<sup>84</sup>Scholars call these exceptions as special needs doctrine. Ferdico, John N., Fradella, Henrt F., & Christopher D, Criminal procedure for the criminal justice professional. 2009. P. 252-272.

cause existed.<sup>85</sup> This exception follows the consistent logic of legal protection in privacy, which is, a person has ability and capacity to disclose or close his privacy, just as he can invite people to come his house.<sup>86</sup> Once he releases his private area, then the protection of privacy is reduced in this area. He has no more reasonable expectation of privacy in that opened area. This is in the rational thinking context based on the Enlightenment, that a rational person can decide whether or not to exercise his rights. In this context, the governmental investigators can search and seizure social media evidence just with one's consent, instead a warrant. But some other issues should be considered further.

#### 3.4.1.1 Consent

Consent may be express or implied,<sup>87</sup> but it must have come from voluntary. The consent is not valid, when it was given by any force, threat, or either expressly or implied coercion.<sup>88</sup> The court posed a totality of circumstances standard to determine whether this consent is voluntary. This totality of circumstances standard means the court must all environmental and personal conditions at the time, including Party age, IQ, education, physical and mental health. In addition, the court also consider that, whether the parties have been arrested or imprisoned, and whether the accused of their rights to refuse consent.<sup>89</sup>

It is the case that the police threat the suspect, if he does not give his consent, the police will apply a warrant to conduct the search. The Court stated that what the

---

<sup>85</sup> *Schnechloth v. Bustamonte*, 412 U.S. 218,219 (1973).

<sup>86</sup> It reminds me of the vampire legend, that taking privacy as a switch. In the legend, vampires cannot enter someone else's house at will, but need an invitation to come. This argument is similar to an English saying, "An Englishman's home is his castle". Both of them emphasize the scope of an individual privacy is the scope beyond his control. Thus, in the context, privacy protection is redarded as the implementation of the right to self-determination.

<sup>87</sup> *United States v. Milian-Rodriguez*, 795 F.2d 1558, 1563-1564 (11<sup>th</sup> Cir. 1985).

<sup>88</sup> *Schnechloth*, 412 U.S. at 228.

<sup>89</sup> *Schnechloth*, 412 U.S. at 226.

police did does not constitute a compulsion, thus the suspect's consent is effective even if he thought the police threat him.<sup>90</sup> However, if the police cheat the suspect to obtain his consent, then this conduct will affect the voluntary of this consent. For example, if the police claimed they had a warrant to search but in fact they didn't have it, then the suspect's consent based on this cheating will be taken as involuntary.<sup>91</sup>

#### 3.4.1.2 Scope of Consent

*“The scope of a search is generally defined by its expressed object, and is limited by the breadth of the consent given.”*<sup>92</sup> The scope of consent should depend on objective reasonableness, which means a rational person make a reasonable understanding of the consent based on communications between the police and people who give the consent.<sup>93</sup> According to this standard, the Court needs to explore the scope that whether investigators include the item to be searched in the scope of the consent is reasonable. In a case, the Court usually considers the special situation when the investigator seeks for the consent, that is, whether the investigators have expressly or impliedly limited the scope of search to specific types, range, or time. Due to adopting this measure of weigh, the scope of consent actually depends on every single fact in a specific case.

Reasons for the consent also can be the standard to determine the scope of consent. In the case of *United States v. Turner*, the police was seeking for related

---

<sup>90</sup> *State v. Smith*, 801 P.2d 975 (Wash. 1990).

<sup>91</sup> *Bumper v. North Carolina*, 391 U.S. 543, 548 (1968) , “The issue thus presented is whether a search can be justified as lawful on the basis of consent when that "consent" has been given only after the official conducting the search has asserted that he possesses a warrant. We hold that there can be no consent under such circumstances.”

<sup>92</sup> *United States v. Pena*, 143 F3d. 1363, 1368 (10<sup>th</sup> Cir. 1998).

<sup>93</sup> *Florida v. Jimeno*, 500 U.S. 248, 251 (1990), “The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of "objective" reasonableness -- what would the typical reasonable person have understood by the exchange between the officer and the suspect? The question before us, then, is whether it is reasonable for an officer to consider a suspect's general consent to a search of his car to include consent to examine a paper bag lying on the floor of the car. We think that it is.”

evidence of a sexual assault or attempted rape, and obtained the victim's neighbor's consent to enter his house and search the house and properties. During conducting the search, a policeman searched this neighbor's computer and found pornographies. The Court stated that, since the police have claimed this search for evidence relating to the sexual abuse when they were seeking the neighbor's consent, then the scope of the consent will deduce to evidence that perpetrators left behind in that case, instead of including files in the computer.<sup>94</sup> Therefore, it is not legal that a search in computer is over the scope of consent.

#### 3.4.1.3 The Third Party Consent

The Supreme Court formally established the legitimacy of the third party consent in the case of *United States v. Matlock*.<sup>95</sup> The Court built the right of the third party consent by common authority. Not limited to property law, the theory of common authority depends on whether the third party is authorized to use this property. If the third party has the joint control on this property in the most cases, then he has the common authority for the property.<sup>96</sup> When this person with the common authority gives his consent to the investigators for search the common properties, investigators conduct a legal search, even though other absence common user expressed oppositions. This theory aims to the common use of a property, that is, every user

---

<sup>94</sup> *United States v. Turner*, 169 F.3d 84, 88 (1<sup>st</sup> Cir. 1999), "We think that an objectively reasonable person assessing in context the exchange between Turner and these detectives would have understood that the police intended to search only in places where an intruder hastily might have disposed of any physical evidence of the Thomas assault immediately after it occurred; for example, in places where a fleeing suspect might have tossed a knife or bloody clothing. Whereas, in sharp contrast, it obviously would have been impossible to abandon physical evidence of this sort in a personal computer hard drive, and bizarre to suppose--nor has the government suggested--that the suspected intruder stopped to enter incriminating evidence into the Turner computer."

<sup>95</sup> *United States v. Matlock*, 415 U.S. 164 (1974).

<sup>96</sup> *Matlock*, at 169-172, "When the prosecution seeks to justify a warrantless search by proof of voluntary consent, it is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." Available at: <https://supreme.justia.com/cases/federal/us/415/164/case.html>

afford risks, which his privacy is disclosure and other user will allow the investigators to search the common part. Besides, this theory does not require the third party and the suspect have the same stake. Even though the presence party expressed his objections, the third party with the common authority still can give an effective consent.<sup>97</sup>

In the case of social media evidence, this theory raised an issue of the common account, which involved account and passwords. The Court has built its theory for an issue of passwords by case law. First, according to the common authority theory, the common users of a computer can give an effective consent for searching this computer.<sup>98</sup> Second, if some of common users coded their personal information, and keep the passwords secretly (not to tell other users), investigators cannot to search the password-protected files, even though they obtained the consent from other common user.<sup>99</sup> Third, if a common user told other users his passwords, then just like the rule number one, other users can give consents to search the password-protected files.<sup>100</sup>

---

<sup>97</sup> *United States v. Sumlin*, 567 F.2d, 684, 687-688 (6<sup>th</sup> Cir. 1977), “The holding of *Matlock* focused on whether or not the “permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected.” 415 U.S. at 171, 94 S.Ct. at 993. The rationale behind this rule is that a joint occupant assumes the risk of his co-occupant exposing their common private areas to such a search.”

<sup>98</sup> *United States v. Smith*, 27 F. Supp. 2d 1111, 1115-1116 (C.D. III 1998), “In this case, the Court is satisfied that the government has carried its burden of showing by a preponderance of the evidence that Ms. Ushman did maintain joint access to or joint control of the computer and surrounding area. The computer was located in an open, accessible area of her bedroom. In addition, children's toys were located there and children's software was actually stored on the computer. Also, the computer was also occasionally used in Defendant's absence. It is also clear, as the testimony reflects, that Ms. Ushman was not prohibited from accessing the alcove in her own bedroom. For example, Ms. Ushman testified that she entered the alcove area to place mail there and also indicated that Defendant had tried to teach her to use the computer.”

<sup>99</sup> *Trulock v. Freeh*, 275 F.3d 391, 403-404 (4<sup>th</sup> Cir. 2001), “Trulock's password-protected files are analogous to the locked footlocker inside the bedroom. By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. Moreover, because he concealed his password from Conrad, it cannot be said that Trulock assumed the risk that Conrad would permit others to search his files. Thus, Trulock had a reasonable expectation of privacy in the password-protected computer files and Conrad's authority to consent to the search did not extend to them. Trulock, therefore, has alleged a violation of his Fourth Amendment rights.”

<sup>100</sup> *United States v. Murphy*, 506 F.2d 529, 530 (9<sup>th</sup> Cir. 1974), “In considering all of the circumstances surrounding the search, we attribute special significance to the fact that Murphy delivered the key to Tucker. We conclude that Tucker's custody of the key gave him sufficient dominion over the premises to enable him to grant the necessary consent. Since Murphy himself put the premises under the

It is not surprising that the Court built this theory and argued these three scenarios. This is still inherited from the previous privacy context. In these cases, the passwords or code is similar to the door of a house, which ensures the line of privacy drawn by this person. By passing the passwords or keys, the person implies that he wants to share his privacy and afford risks of privacy violations.

Besides, if we found this third party actually without the common authority he claimed, the legitimacy of this search is on issue. In the cause of *Illinois v. Rodriguez*, the Court pointed out that evidence from this consent search will not be excluded, even though this third party without the common authority he claimed.<sup>101</sup> The Court explained, if a man of reasonable caution in the belief will get the same or similar results on facts in this case, that investigators can trust the third party and his common authority. Thus, even though the third party has no authority in fact, the search doesn't violate requirements under the fourth amendment.<sup>102</sup>

### 3.4.2 Exigent Circumstances

Investigators can implement a warrantless search when circumstance is exigent. An exigent circumstance is someone (investigators also included) suffered injuries,

---

immediate and complete control of Tucker, who voluntarily consented to the search, we hold that the search was not unreasonable.”

<sup>101</sup> *Illinois v. Rodriguez*, 497 U.S. 177, 188-189 (1990), “We see no reason to depart from this general rule with respect to facts bearing upon the authority to consent to a search. Whether the basis for such authority exists is the sort of recurring factual question to which law enforcement officials must be expected to apply their judgment, and all the Fourth Amendment requires is that they answer it reasonably. The Constitution is no more violated when officers enter without a warrant because they reasonably (though erroneously) believe that the person who has consented to their entry is a resident of the premises than it is violated when they enter without a warrant because they reasonably (though erroneously) believe they are in pursuit of a violent felon who is about to escape.”

<sup>102</sup> *Id.* “As *Stoner* demonstrates, what we hold today does not suggest that law enforcement officers may always accept a person's invitation to enter premises. Even when the invitation is accompanied by an explicit assertion that the person lives there, the surrounding circumstances could conceivably be such that a reasonable person would doubt its truth and not act upon it without further inquiry. As with other factual determinations bearing upon search and seizure, determination of consent to enter must “be judged against an objective standard: would the facts available to the officer at the moment . . . warrant a man of reasonable caution in the belief” that the consenting party had authority over the premises? [...] If not, then warrantless entry without further inquiry is unlawful unless authority actually exists. But if so, the search is valid.”

annihilation of relevant evidence, suspect's escape, or unduly impediment to investigation. If any reasonable person will believe, under that situation (an exigent circumstance), that conduct is actually to prevent someone (investigators also included) suffered injuries, annihilation of relevant evidence, suspect's escape, or unduly impediment to investigation, the investigators can implement expectedly a warrantless search.<sup>103</sup> In *United States v. Reed*, the court required the investigators consider the general factors relevant to a determination of the existence of exigent circumstances, which include: “ (1) the degree of urgency involved and the amount of time necessary to obtain a warrant; (2) the officers' reasonable belief that the contraband is about to be removed or destroyed; (3) the possibility of danger to police guarding the site; (4) information indicating the possessors of the contraband are aware that the police are on their trail; and (5) the ready destructibility of the contraband.”<sup>104</sup>

Because the nature of easy to loss of digital evidence, it is also common to find an exigent circumstance in a specific case for searching social media evidence. For example, Oregon U.S. District Court once held that investigators can implement a warrantless search for the contents of the suspect's pager. The reason this court mentioned is that, the content in a pager is easy to be cover for another message in a short of time, and more, these information is easily gone, while the pager is out of battery.<sup>105</sup> However, it should not allow that the purposes of search or seizure surpass preventing the necessary of destroying evidence, even though there is an exigent circumstance. And of course, investigators must stop their warrantless in any time, when this exigent circumstance is no longer existed. In the case of *United States v.*

---

<sup>103</sup> *United States v. McConney*, 728 F.2d 1195, 1199 (9<sup>th</sup> Cir. 1984).

<sup>104</sup> *United States v. Reed*, 935 F.2d 641,642 (4<sup>th</sup> Cir. 1991).

<sup>105</sup> *United States v. Romero-Garcia*, 991 F. Supp. 1223, 1225 (D. Or. 1997).

Doe, investigators implemented a warrantless seizure for a computer under an exigent circumstance, in case data in the computer will be destroyed. The court held that, this exigent circumstance was gone, while the computer is moved under the police's control; therefore, a further warrantless search for data inside is illegal, and the obtained information as evidence should be excluded. That is, it is only allow investigators to seize the computer under an exigent circumstance, but there is no justification for further searching the contents in this computer. A further search for the contents of the computer needs a warrant issued by the court.<sup>106</sup>

We can conclude in the context that, investigators can do a warrantless search or seizure, while the evidence has existed in a highly risk of being destroyed or gone. But, when this exigent circumstance is no longer existed or the evidence is moved under investigators' control, it requires another authority for the further search or view of the contents. However, in the cases of social media evidence, there is hardly an exigent circumstance. First, this exigent circumstance doctrine requires the possibilities of evidence destroyed or lost. Although social media evidence is easy to loss, the police or prosecutors usually require the party or service provider (e.g. Facebook) preserve evidence with a subpoena. By doing so, the party or the service provider is obliged to preserve the required social media evidence, which means they still have other legal responsible, even if they tries to destroy the evidence. Second, even though investigators seizure these social media evidence from the party's account or the service provider, the government still cannot control all information related to these social media evidence. It is possible that the suspect destroy evidence by accessing his account in any device connecting the internet. In other words, we cannot find the justification of doing a warrantless search for social media evidence

---

<sup>106</sup> Ralph d. Clifford ed., *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 2006, at 145-146.

based on an exigent circumstance.

Social media evidence actually is the type of information existing on the websites. It is hardly to apply this search and seizure doctrine developed from the concept of physical object. If we apply this doctrine narrowly, it might over limit the investigation; on the contrary, if we apply this doctrine widely, it will danger the privacy guaranteed by the fourth amendment. Thus, the better solution might be regulating social media evidence as information, instead as traditional physical objects.

### 3.4.3 Plain View Doctrine

The plain view doctrine means that, investigators can seizure any criminal evidence plated in the range of plain view. This doctrine is applied the contraband placed on public place, such as drugs, or bloodstained knife. Under this situation, it is really hard and unrealistic asking investigators to ignore this criminal evidence in their plain view. Actually, a request for ignore is unjust and immoral. For applying the plain view doctrine, investigators must be legal in the premises and obtain the evidence, showing its illegal appearance immediately and obviously.

This plain view doctrine only authorizes investigators to seizure contrabands they already have the right to view, which means, this doctrine doesn't create a new basis of authorization of search and seizure. In the cases related to computers, investigator should not apply this doctrine in order to open and view the computer files they don't have right to view before. The action, "open the file", cannot fall into the range of the plain view.<sup>107</sup> Thus, when involving the situation that information needs a further search, such as social media evidence, the plain view doctrine will be

---

<sup>107</sup> United States v. Villarreal, 963 F. 2d 770, 776 (5<sup>th</sup> Cir. 1992).

limited to apply. Especially if investigators want to search information on a private social network site, they need a warrant for search and seizure. It is difficult to apply this exception for a warrantless search, and it should be allowed to search one's social network sites without a warrant.

#### 3.4.4 Search Incident to Lawful Arrests

A search incident to lawful arrests means, when the investigators arrest the suspect legally, they immediately search the suspect and the range he can control without a warrant for this search. It is another exception of the warrant request. The purposes of this exception are to secure investigators' safety and to preserve evidence. Therefore, the legal practice has allowed some exceptions that, for the reasons of security and preservation, investigators should be allowed to implement a warrantless search after a lawful arrest, such as search the suspect's wallet and its contents,<sup>108</sup> copy the suspect's phone book(s) along with him,<sup>109</sup> and search the suspect's suitcase along with him.<sup>110</sup> In the case of *United States v. Robinson*,<sup>111</sup> the court allowed investigators to implement a legal warrantless search on the electronic pagers with the suspect, after arresting him lawfully. When investigators arrest the suspect lawfully, the courts consider the security of investigators and possibilities of evidence destroyed primarily, and allow investigators to search objects within the range the suspect can reach.

Information on social network sites should be displayed on a specific media or device, in order to be viewed by human beings. Therefore, if investigators want to

---

<sup>108</sup> *United States v. Castro*, 596 F.2d 674, 676 (5<sup>th</sup> Cir. 1997); *United States v. Molinaro*, 877 F.2d 1341, 1347 (7<sup>th</sup> Cir. 1989).

<sup>109</sup> *United States v. Rodriguez*, 995 F.2d 776, 778 (7<sup>th</sup> Cir. 1993.)

<sup>110</sup> *United States v. Johnson*, 846 F.2d 279, 283-284 (5<sup>th</sup> Cir. 1988); *United States v. Lam Muk Chiu*, 522 F.2d 330, 332 (2d Cir. 1975).

<sup>111</sup> *United States v. Robinson*, 414 U.S. 218 (1973).

search for social media evidence without warrant but search incident to lawful arrests, the only situation will be that, after a lawful arrest, investigators immediately search the suspect and an internet-connecting electronic device along with him. However, in the case of *Riley v. California*,<sup>112</sup> the Supreme Court denied that investigators can implement a legal search on the suspect's smart phone after arrest him lawfully, and further requested that investigators should obtain a search warrant for this smart phone, before they look up its contents.

David Riley was stopped his drive by the police because of the expired license plate, on 22 August 2009. A policeman accidently found out two guns in the car, and arrested Riley on the spot, when the police seized Riley's car and searched items inside the car. After this arrest, the police expropriated Riley's smart phone, and read some messages inside, finding Riley is dealing with gang members. Therefore, the police discovered more contents in Riley's smart phone and found more "interesting facts", including evidence to prove that Riley involved in the gang shootings one week ago. Although Riley argued that was an illegal search on his smart phone without a warrant issued by the judge, the trial court and the court of appellate held that, this warrantless search on the smart phone was legal, because this smart phone is related to the arrested suspect directly. The court of appellate further noted that, the legitimacy of a search will be doubt only when this smart phone was found later. But in this case, the police found it immediately while arresting Riley.

However, the Supreme Court stated that, the contents of this smart phone obviously cannot and will not danger the security of investigators, and since this smart phone has been transferred to the police, it is low probability of losing data inside during the police is seeking for a warrant. It is also possible to turn off the internet

---

<sup>112</sup> *Riley v. California*, 573 U.S. \_\_\_\_ (2014). Full text at <https://supreme.justia.com/cases/federal/us/573/13-132/opinion3.html>

connection, to prevent data loss by remotely remove or encrypt. Thus, the content of a smart phone should not be the object of incidental search. The Court further stated that, using the smart phone has become one part of our daily life in every moment every day. People record their life inside, including communications records, photos and videos labeled with the date and place, web search and browsing history, shopping list, GPS positioning, etc. A smart phone has a lot of personal information. If allowing the police can look up the suspect's smart phone without a warrant, the serious violations of personal privacy will possibly happen.

It should be noted that the court mentioned, ” *To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter.*” The Court seems to express its view on “the box theory” built by the past cases, and point out it should not apply in the case of searching a smart phone, because the nature and functions about a smart phone are not similar with a box. The Court further emphasis on that, “cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself.” That is, investigators incidentally seizure the suspect's smart phone and further search for information on the phone, even linking to related information on the web without warrant. It is definitely a violation of privacy guaranteed by the fourth amendment. These investigators' conducts obviously overstep the purpose of incidental search exception, protections of investigators' security, and break down the privacy range under the fourth amendment. This search should not be allowed.

#### **4. Admissibility of Evidence**

In the history of evidence law, British legal system is the first country adopting “petty jury” to divide fact-finding and decision-making. In this petty jury mechanism, jurors are obligated to decide what happened in this case based on evidence presented at trial, but judges decide applications of regulations based on the fact decided by the jury. A judge cannot participate in the decision of fact-finding. American legal system inherited the British tradition in fact-finding and decision-making dichotomy. The American evidence law system can be summarized into the following points. First, a plea bargain will carry out, after the prosecution. Only when the defendant advocates his not-guilty, then the process moves to the next stage, the trial. Therefore, if the defendant pleads guilty and the prosecutor accepted his plea, then the defendant is convicted without evidence base. That is, there is no room for applying the evidence law. Second, when the defendants assert his innocent, then the process moves to the trial. But it will first decide whether some kind of evidence should be excluded, and a juror who will be the member of fact-finding jury afterwards cannot allow participating in the process of this decision making. Third, pretrial motions are filed. Some of this motions related to evidence include “discovery” and motions to suppress evidence. The main concern in pretrial motions is considering relevancy and admissibility. In other words, the evidence, will be present in front of the jury, must have relevance with the fact asserted in this case, and this evidence will be not admissible, while probative value of this evidence will cause a unfair trial, confusion of issues, jury misleading, or consideration of the improper delay, waste of time, or unnecessary. The admissibility includes the hearsay rule. Fourth, at trial, the jury will find the fact based on relevant and admissible evidence, and then the judges will make the decision based on the fact that the jury found.

#### 4.1 Federal Rules of Evidence

The American legal system is multi-jurisdictional, which means, in general every state has its own legislature, making its set own legal norms. So it did in the evidence law area. The Federal Rules of Evidence was originally applied in cases under the federal jurisdiction. But recently it has gradually been accepted by states, and some states follow it to amend their evidence law, such as the Maryland Rules of Evidence. Therefore, the Federal Rules of Evidence is likely the guideline for evidence in the American legal system, which is the reason why this thesis chose it as the objective of discussing how to transform information to be the evidence helping the jury to build/construct the truth. The Federal Rules of Evidence used in this thesis is the newest edition, amended to December 1, 2015.

#### 4.2 Relevancy

The first requirement for transforming information, social media-related or otherwise into evidence is relevance.<sup>113</sup> Rule 401 states, “*Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.*”<sup>114</sup> The relevancy is to discuss whether a specific evidential material can help to prove the fact asserted or not. For example, if the present case is to prove A defamed B on his Facebook, the posting on A’s Facebook may have relevance with this case. But if the case is to prove A killed B, then this posting might be a proof of A’s motivation, but has no relevance with the fact that A killed B. Furthermore, the evidence has relevance with the case asserted, and according to Rule 402<sup>115</sup>, if the evidence is lack of relevancy in this case, it is not admissible and not allowed to be present at trial. A

---

<sup>113</sup> Thaddeus A. Hoffmeister, *Social Media in the Courtroom*, p.152.

<sup>114</sup> Federal Rules of Evidence 401.

<sup>115</sup> Federal Rules of Evidence 402 states, “*Relevant evidence is admissible unless any of the following provides otherwise: the United States Constitution; a federal statute; these rules; or other rules prescribed by the Supreme Court. Irrelevant evidence is not admissible.*”

relevant evidence is the first step to become the object to help the jury finding fact.

#### 4.3 Hearsay

Rule 801 (c) defined hearsay “*means a statement that: (1) the declarant does not make while testifying at the current trial or hearing; and (2) a party offers in evidence to prove the truth of the matter asserted in the statement.*”<sup>116</sup> Thus, the point to be thought as “hearsay” basically should be a statement, making outside the courtroom, in order to prove the truth of the matter asserted. We can define this point into a three-step test.

##### 4.3.1 A Statement Made by A Person Outside the Courtroom

The first step is whether information or the material from social network site (aka. Social media evidence) is a statement, which is defined by Rule 801 (1) as “a person’s oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion.” Also this hearsay rule prevents a person’s statement outside the courtroom because judges or jury have no chance in person to examine this person and his statement. It may raise issues of false and against the right to cross-examination. Considering the digital nature of social media evidence, by the way they are produced, we can divide information into two catalogs, computer-stored records and computer-generated records, to determine whether this social media evidence can be taken as a person’s oral assertion or others similar.

The computer-stored records is produced by human actions, including writing, painting, speaking etc., such as diary stored in the computer, the content of email, records in the instant message, posting on a social network site, or comments in the internet forum. This kind of information in general produced by a person to express his thought or feeling will be thought as a statement, for example, a posting on

---

<sup>116</sup> Federal Rules of Evidence 801 (c).

Facebook page.<sup>117</sup> However, it will not raise an issue of hearsay, if a computer-stored record is non-hearsay. For example, a statement made by the defendant in a third party talking in the internet chat room, or the content of an email that the defendant forwarded to the third party. This statement and the content of the email are the defendant's admission, which are non-hearsay, not applying the hearsay rule.<sup>118</sup>

On the other side, the computer-generated records are results of the operation of the computer program or software or information generated automatically by machines, therefore they are not the statements in Rule 801 (1), not applying the hearsay rule. For example, the time stamp used in social network sites whenever a user posts information on his account. This time stamp is automatically computer generated.

Therefore, in the context of social media evidence, hearsay can take the form of updates, messages, and photos captions.<sup>119</sup>

#### 4.3.2 The Statement Is Offered for the Truth of the Matter Asserted

The second step is whether the statement is to prove the truth of the matter asserted. In the case of *People v. Valdez*, the defendant's Myspace page was introduced at trial, not for proving the fact asserted by the prosecution, but for corroborating a victim's statement to investigator. Thus, the court thought this Myspace evidence not applying the hearsay rule and admissible.<sup>120</sup>

#### 4.3.3 An Exception of the Hearsay Rule

The third step is to check the exception list of the hearsay rule. Otherwise, the

---

<sup>117</sup> Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1 (2009).

<sup>118</sup> Federal Rules of Evidence 801 (d) (2).

<sup>119</sup> Thaddeus A. Hoffmeister, see *supra* note 113, p. 161.

<sup>120</sup> *People v. Valdez*, 135 Cal. Rptr. 3d 628 (Cal. Ct. App. 2011). The court held, "*Valdez's hearsay objection fails because the nature of the evidence here did not consist of declarative assertions to be assessed as truthful or untruthful, but rather circumstantial evidence of Valdez's active gang involvement. For example, a reasonable jury would understand its purpose was not to determine whether Valdez and his "Krew" were truly "Most Wanted" by the "Ladiez" in Orange County. Rather, as instructed, the jury was to consider the evidence in deciding what weight to give Castillo's opinion testimony.*"

evidence passed through two steps above is defined as hearsay, and should be excluded according to Rule 802, which states “*Hearsay is not admissible*”. Those exceptions<sup>121</sup> to the hearsay rule, more commonly related to the social media evidence including present sense impression,<sup>122</sup> excited utterance,<sup>123</sup> public records,<sup>124</sup> and business records,<sup>125</sup> might be considered case by case.<sup>126</sup>

#### 4.4 Authentication

Rule 901 (a) states, “*to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.*” This rule has two points: first, the federal rule of evidence has decided the proponent will have the burden of producing evidence; second, the burden of persuading is sufficient support. Thus, the proponent, who has the burden of producing evidence, should not produce the direct evidence, but can produce circumstantial evidence to prove his evidence authentic.<sup>127</sup> The proponent should not exclude all doubts<sup>128</sup> or prove to beyond any doubt.<sup>129</sup> Some of the courts held that “sufficient support” is preponderance of evidence, which means a reasonable judge will believe evidence provide by proponent is more credible true, or believe evidence is actually the evidence that the proponent claimed. Then this evidence is authentic. But, some of courts think that the burden of persuading as prima facie, instead of preponderance of evidence.<sup>130</sup>

---

<sup>121</sup> Federal Rules of Evidence 802, “*Hearsay is not admissible unless any of the following provides otherwise: a federal statute; these rules; or other rules prescribed by the Supreme Court.*”; Federal Rules of Evidence 803.

<sup>122</sup> Federal Rules of Evidence 803 (1).

<sup>123</sup> Federal Rules of Evidence 803 (2).

<sup>124</sup> Federal Rules of Evidence 803 (8).

<sup>125</sup> Federal Rules of Evidence 803 (6).

<sup>126</sup> Thaddeus A. Hoffmeister, see supra note 113, p. 162.

<sup>127</sup> United States v. Dhinsa, 254 F.3d 653, 658-659 (2d Cir. 2001).

<sup>128</sup> United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007).

<sup>129</sup> United States v. Piuta, 176 E.3d 43, 49 (2d Cir. 1999).

<sup>130</sup> SCS Communications, Inc. v. Herrick Co., Inc. 360 F.3d 329, 344 (2d Cir 2004).

#### 4.5 The Best Evidence Rule

The main feature of social media evidence is invisible information for human, but becoming visible through digital devices, such as computers, smart phones. The common and simple way to present the social media evidence in the courtroom is print out, that is, parties directly perceived through the senses to print or screenshot what the need on social network sites. When the printout itself is probandum or the proof foundation of proving the fact asserted, Rule 1002 is involved in this situation.

Rule 1002 is the original writing rule, as known as the best evidence rule, or known as the original writing rule, states, “*An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise.*” It emphasizes on the original manuscript of evidential material itself. In other words, When the purpose of submitting documents, records, or photos is to prove the content of this evidential material or prove that the alleged claim via this material, judges shall decide whether Rule 1002 apply in this situation. For example, considering that those documents were produced not on the purposes of a special case, official records or an authorized record or archive, indeed recording or archiving of documents, are reliable and the original writing rule may be excluded in this case.<sup>131</sup> In another case, since it can be proved through the witness, it is not necessary to follow the original manuscript request.

To properly apply the best evidence rule, the judge must determine *when “the contents” of a writing, recording, or photograph actually are being proved, as opposed to proving events that just happen to have been recorded or photographed, or those which can be proved by eyewitnesses, as opposed to a writing or recording*

---

<sup>131</sup> Federal Rules of Evidence 1005.

*explaining or depicting them.*<sup>132</sup>

*In re T.A.*,<sup>133</sup> a juvenile delinquent (T.A.) was adjudicated in two counts of felonious assault with firearm specification. The juvenile was charged that he was shoot a firearm at the house of A.P., whose cohabiting son had fought with T. A. earlier that day, and he might take revenge on A.P.' son by shooting. A. P. testified at trial, that her acknowledge to identify T.A. as the shooter was relied on information she receive from T.A's MySpace page. The printout of T.A's Myspace page was received from a neighbor shortly after the shooting and included T.A.'s photograph and an admission from T.A. about shooting. The defense counsel raised the objection, and the prosecution never admitted into evidence T.A.'s Myspace page. The case was appealed. The appellate court found that, to allow A.P. to testify about T.A.'s Myspace page was error but harmless<sup>134</sup>. According to the best evidence rules, the photographs were never admitted into evidence. In this case, A.P. verified T.A.'s identity through T.A.'s Myspace page; therefore the best evidence would have been T.A.'s Myspace page. This case illustrates how the best evidence rule works in a social media context.

Another question is, whether every printout of digital evidence is the original manuscript. The point of this question is that, if this kind of printouts is not allow being the original, then information need to be present on a computer screen every time in every proceeding. Generally this problem can be solved by the Federal Evidence Act 1001 (d).

---

<sup>132</sup> Lorraine v. Markel, 241 F.R.D. 534 (D. Md. 2007).

<sup>133</sup> 2011 WL 6145742 Ohio App. 8 Dist., 2011.

<sup>134</sup> A harmless error is a ruling by a trial judge that, although mistaken, does not meet the burden for a losing party to reverse the original decision of the trier of fact on appeal, or to warrant a new trial. Harmless error is easiest to understand in an evidentiary context. Evidentiary errors are subject to harmless error analysis, under Federal Rule of Evidence 103(a) ("Error may not be predicated upon a ruling which admits or excludes evidence unless a substantial right of the party is affected.") The general burden when arguing that evidence was improperly excluded or included is to show that the proper ruling by the trial judge may have, on the balance of probabilities, resulted in the opposite determination of fact. [https://en.wikipedia.org/wiki/Harmless\\_error](https://en.wikipedia.org/wiki/Harmless_error)

Rule 1001. (d) states, “ *For electronically stored information, “original” means any printout — or other output readable by sight — if it accurately reflects the information.*”<sup>135</sup> On the other hand, a correct computer printout will be able to meet the original manuscript request of the best evidence rule. For example, in the case of *Laughner v. State* (2002)<sup>136</sup>, the court held that, the policeman copy and paste the record of AOL<sup>137</sup> instant Message in a word file, meeting the best evidence rule. The defendant, Laughner, was charged in one count of attempted child solicitation, a class C felony. On appeal, he claimed that use of the word file as evidence should not be permitted. The defendant argued that the policeman posing as a child chat with him in a chat room of AOL, and copy and paste the content of this chat in a word file. And this content of chat is not using a AOL chat room function, which can save and download the original information, but just copying and pasting it in a word file, which allow user to editor or alter the content. Thus, what the policeman did is against the best evidence rule.

The Court of Appeal pointed out, Rule 1001 (d) should be considered in the issue of computer printout.<sup>138</sup> In this case, the testified policeman saved the conversations with Laughner after they were concluded, and the printout document accurately

---

<sup>135</sup> Federal Rules of Evidence 1001 was amended in 2011. Committee Notes on Rules states, “ *The language of Rule 1004 has been amended as part of the restyling of the Evidence Rules to make them more easily understood and to make style and terminology consistent throughout the rules. These changes are intended to be stylistic only. There is no intent to change any result in any ruling on evidence admissibility.*”

<sup>136</sup> *Laughner v. State*, 769 N.E.2d 1147 (Ind. Ct. App. 2002)

<sup>137</sup> AOL Inc. (simply known as AOL, originally known as America Online, stylized as Aol.) is an American multinational mass media corporation based in New York, a subsidiary of Verizon Communications. <https://en.wikipedia.org/wiki/AOL>

<sup>138</sup> This judgement was made in 2002, while Indiana Rules of Evidence 1001(3) then provides that when "data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is an `original.'" But now this rule was amended and moves to 1001(d), which is similar with the federal rules of evidence 1001(d). The Federal Rules of Evidence 1001(d): An "original" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout or other output readable by sight if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it.

reflected the content of those conversations. Therefore, the printouts could be found to be the "best evidence" of the conversations between them. Besides, the court pointed out, that Laughner just argued the originality of the document, instead challenged the foundation for admission of the documents established by the policeman's testimony about his knowledge of the conversations and that the printed documents accurately reflected the contents of the conversations. Then, the court concluded, admission of the printed documents would not be an abuse of discretion.

However, we cannot directly recognize the computer printout is real. Logically, "reflect the data accurately" should be explained that the content of the printout is consistent with the content of the original file in the computer. It is different from the discussion on counterfeit or alteration of the evidential material. We can conclude from the case above that, on the issue of printouts, the courts mainly concern "reflect the data accurately". The reason that Laughner lost his case might be his tacit consent to allow the policeman's testimony about his knowledge of the conversations, which reflected accuracy of the documents and built the foundation for admission of them. The further questions will be discussed in chapter 5.

#### 4.6 Character Evidence

The Federal Rules of Evidence 404 regulates the character evidence, and evidence of a crime, wrong or other act. In general, the character evidence cannot be admissible to prove that on a particular occasion the person acted in accordance with the character or trait.<sup>139</sup> The basic rule is information of a person's character cannot be used to prove that this person conduct a specific action just because he has such character. This propensity inference is generally forbidden, but there are some exceptions regulated in the Rule 404 (a) (2) & (3). Reasons for Rule 404 (a) are, on

---

<sup>139</sup> The Federal Rules of Evidence 404 (a) (1).

the one hand, the propensity inference may possibly cause an error; on the other hand, evidence to support the propensity inference usually raises issues of prejudice.

Besides, the Rule 404 (b) regulate another type of evidence of a crime, wrong or other act. It states, “*Evidence of a crime, wrong, or other act is not admissible to prove a person’s character in order to show that on a particular occasion the person acted in accordance with the character.*”<sup>140</sup> As the same structure of regulation with Rule 404 (a), it generally cannot to be used to prove the propensity inference, but still have some exceptions.<sup>141</sup>

There is a case, *United States v. Phaknikone*<sup>142</sup>, related to issues of improper character evidence arises with respect of social media. The defendant was charge with eight bank robberies. The prosecution built a theory, that the banks were robbed in a similar “gangster style,” including the method by which the robber held the gun. In order to connect the defendant to his theory and to prove the defendant committed these crimes, the prosecution introduced the defendant’ Myspace page with other evidence at trial. This Myspace evidence included the defendant’s profile page that listed the name “Trigga” with “\$100 bills...floating the screen”, his subscriber report, listing the full name “Trigga FullyLoaded” and email address “gangsta\_trigga@yahoo.com,” and two photos including one of the defendant bearing a tattoo, holding a handgun sideways (apparently gangster style), with a child and another man as passengers. The prosecution claims this Myspace evidence can prove the defendant’s identity and show the way he committed these crimes with gun. But

---

<sup>140</sup> The Federal Rules of Evidence 404 (b) (1).

<sup>141</sup> The Federal Rules of Evidence 404 (b) (2), “This evidence may be admissible for another purpose, such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident. On request by a defendant in a criminal case, the prosecutor must: (A) provide reasonable notice of the general nature of any such evidence that the prosecutor intends to offer at trial; and (B) do so before trial — or during trial if the court, for good cause, excuses lack of pretrial notice.”

<sup>142</sup> *United States v. Phaknikone*, 605 F. 3d 1099 (11th Cir. 2010)

the defendant objected and argued that it was improper character evidence and unduly prejudicial.

Although the defendant is ultimately guilty based on the overwhelming evidence, including his confession of committing at least four bank robberies, the court held that, *“The MySpace evidence is not evidence of identity: that is, evidence that Phaknikone robbed banks like a gangster. The subscriber report proved nothing more than Phaknikone’s nickname, the only name by which Lavivong had already testified he knew Phaknikone. The profile photographs accompanying the subscriber report and the photograph of Phaknikone and his ex-wife at a social event offer nothing to support a modus operandi about the bank robberies. The photograph of a tattooed Phaknikone, his face completely visible, in a car, holding a handgun sideways in his right hand, and with a child as a passenger, proves only that Phaknikone, on an earlier occasion, possessed a handgun in the presence of a child. Although the photograph may \*1109 portray a “gangster-type personality,” the photograph does not evidence the modus operandi of a bank robber who commits his crimes with a signature trait. The MySpace evidence is not evidence of a modus operandi and is inadmissible to prove identity.”*<sup>143</sup> Therefore, the court thought the Myspace information was such bad character evidence prevented by Rule 404 (b).

---

<sup>143</sup> United States v. Phaknikone, 605 F. 3d 1099, 1108.

## Section 3 Taiwanese Law

### 1. The Basic Principles of Evidence Law

As an important part of criminal proceedings, evidence law is regulated in Article 154 and subsequent articles of the Code of Criminal Procedure. It definitely chases the goal of the criminal procedure, finding the fact; at the same time, it will also apply for the general principles, such as “*nemo tenetur se ipsum accusare*”<sup>144</sup>, “*in dubio pro reo*”,<sup>145</sup> and the doctrine of the presumption of innocence.<sup>146</sup> Discussions here are principles applicable to evidence acquisition and use of evidence in evidence law, including principle of evidentiary adjudication, principle of strict proof (Strengbeweis), and principle of judicial discretion (freie Beweiswürdigung), and basic concepts of evidence law as well.

#### 1.1 Principle of Evidentiary Adjudication

Article 154 II of the Code of Criminal Procedure openly revealed, “*The facts of an offense shall be established by evidence. The facts of an offense shall not be established in the absence of evidence.*” That is so-called principle of evidentiary adjudication. According to this principle, the court’s judgements on the facts of the crime must be based on evidence. Interpretation of Constitutional Court No. 384 (1995)<sup>147</sup> recognized the principle of evidentiary adjudication was guaranteed by the constitutional law; Interpretation of Constitutional Court No. 582 (2004)<sup>148</sup> further

---

<sup>144</sup> No one is obliged to passively act as an aid to his own criminal charges. On the contrary, the state is not allowed to force any person to prove their crimes positively.

<sup>145</sup> This principle belongs to the basic principles of the criminal procedure recognized by countries under the rule of law. The significance is that if the evidence has been exhausted and cannot prove that the crime, the court should be in favor of the defendant's decision. In contrast, when the court found facts to be unfavorable to the defendant, it must be proved and accessed to convince. *See* Yu-Hsiung Lin, *in dubio pro reo* and Legal Evaluation, *The Taiwan Law Review*, No. 72, pp.18.

<sup>146</sup> This principle is expressly recognized in Article 154I of the Code of Criminal Procedure, “*Prior to a final conviction through trial, an accused is presumed to be innocent.*”

<sup>147</sup> Available at [http://www.judicial.gov.tw/constitutionalcourt/en/p03\\_01.asp?expno=384](http://www.judicial.gov.tw/constitutionalcourt/en/p03_01.asp?expno=384)

<sup>148</sup> Interpretation of Constitutional Court No. 582 (2004), available at

argued that the core connotation of this principle is the principle of strict proof.

## 1.2 Principle of Strict Proof/ Strengbeweis

Principle of strict proof means that proofs and investigations of criminal facts must use evidential methods regulated by the law and comply with statutory investigation procedures. The relevant provisions include:

- (1) Article 155 II states, “Evidence inadmissible, having not been lawfully investigated, shall not form the basis of a decision.” The so-called lawful investigation procedure refers to the strict proof process.
- (2) The procedure for investigating evidence is attached the trial. Thus, the basic principle governing the trial process is not only an element of the concept of a lawful investigative procedure, but also the relevant provisions related to principle of strict proof, which includes principle of direct trial,<sup>149</sup> principle of verbal arguments,<sup>150</sup> principle of public hearing.<sup>151</sup> In addition, the 2003 Amendment of criminal procedure introduced the hearsay rule, which is tied to the principle of direct trial to dictate statements outside the court. Therefore, the hearsay rule is also considered in the strict proof of the process, to become evidence of one of the positive elements of evidence.
- (3) The Code of Criminal Procedure enumerates the five evidential methods and its lawful investigative procedures, which are the defendant, the witness, documents, forensics, and inspection. Relevant regulations are the defendant's interrogation and confession ( §§94~100-3, 156, 288III), the witness (§§175~196, 166~171), the

---

[http://www.judicial.gov.tw/constitutionalcourt/en/p03\\_01.asp?expno=582](http://www.judicial.gov.tw/constitutionalcourt/en/p03_01.asp?expno=582)

<sup>149</sup> Article 159I states, “Unless otherwise provided by law, oral or written statements made out of trial by a person other than the accused, shall not be admitted as evidence.”

<sup>150</sup> Article 221 states, “A judgment shall be based on the oral arguments of the parties unless there is a special provision to the contrary.”

<sup>151</sup> See Article 379 of the Code of Criminal Procedure and Article 86 of Organic Act of Courts.

expert witness (§§197~210, 166~171), the document (§§165) and the inspection (§§ 164, 165-1, 212~219).

To sum up, the evidence of the crime in this case must be not prohibited to use (negative conditions), investigated lawfully through the strict proof (positive conditions), and then the evidence is considered admissible by court, which can be used as the basis of judgements in this case.

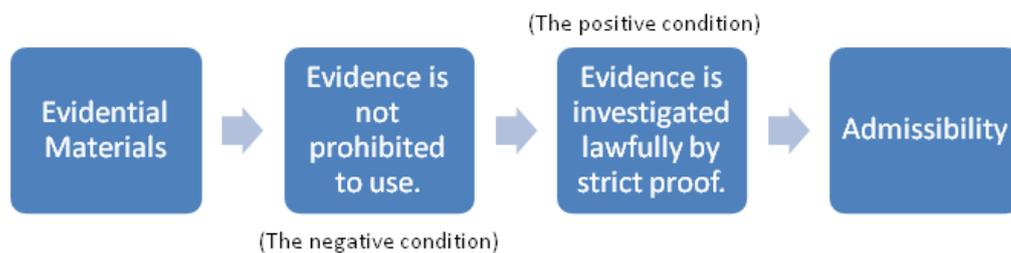


Figure 4 Admissibility

### 1.3 Principle of Judicial Discretion/ freie Beweiswürdigung

The principle of judicial discretion (freie Beweiswürdigung) is about how to evaluate the value of evidence (the probative value of evidence). Article 155I provides the rules for judges to evaluate evidence, that is, *“The probative value of evidence shall be determined at the discretion and based on the firm confidence of the court, provided that it cannot be contrary to the rules of experience and logic.”* Preceded the determination of the probative value of evidence, evidentiary materials must be admissible. Since inadmissible evidence should not be the foundation for judges making the judgment, there is no room for this kind of evidence to discuss the probative values of evidence at all.

Although the court has full freedom to decide the probative value of evidence,

there are still limitations to restrict the judge's discretion.<sup>152</sup> As mentioned above, admissibility is as a prerequisite for principle of probative value of evidence, so that Beweisvertungsverbote (the following figure 5) and principle of strict proof have formed the external limits of the judge's discretion. The former requests judges cannot adopt inadmissible evidence as basis of judgements; and the latter emphasizes that evidence are not strictly proofed should not be based on judgements through the judge's discretion. The inherent limitations of the principle of judicial discretion include the following provisions.

(1) The probative value of trial records is expressly stipulated in Article 47 of the Code of Criminal Procedure, that is, "*Trial records shall be the exclusive proof of the proceedings of the trial.*"

(2) Article 155I request that judge's discretion "*cannot be contrary to the rules of experience and logic.*" Many judges in the past misunderstood this provision and thought they can make judgements with their own experience or unconfirmed social consensus, for example, the court believed that the defendant's confession or witness's testimony in the first time is the most important evidence to solve the case, because such statements are less involved in other ideas or are interfered by others.<sup>153</sup> Actually rule of law means logic rules of reasoning and deduction; and rule of thumb bridge the court's observation and conclusion. Only the generally effective rule of thumb, especially the rule of thumb that has been proven in the natural sciences, has the effect of constraining the space for the court's decision in principle. For example, science confirmed that the father of A blood and the mother of A blood type will not

---

<sup>152</sup> See Yu-Hsiung Lin, freie Beweiswürdigung- Is the judge's discretion really free?, Taiwan Law Journal, No. 27, pp.13.

<sup>153</sup> See (93) Tai Shan Zhi No. 3778 Penal Judgment (2004) of the Supreme Court. Criticism: (94) Tai Shan Zhi No. 5549 Penal Judgment (2005) and (95) Tai Shan Zhi No. 2288 Penal Judgment (2006) of the Supreme Court.

give birth to children of B blood type. Therefore, the court cannot identify a child of B blood type as the natural child born by parents both of A blood type. Otherwise this judgement will be considered illegal and can be withdrawn by appeal.<sup>154</sup>

(3) Confessions must have reinforcement evidence. According to Article 156II, “*Confession of an accused, or a co-offender, shall not be used as the sole basis of conviction*”, the court cannot convince the defendant guilty with its firm confidence solely based on confession of an accused, or a co-offender. At this point the court should pay more attention that “*other necessary evidence shall still be investigated to see if the confession is consistent with facts.*” (Article 156 II).<sup>155</sup>

(4) Article 156IV states, “*Where an accused has made no confession nor has there been any evidence, his guilt shall not be presumed merely because of his refusal to make a statement or remaining silent.*” The court cannot convince the defendant guilty based on the situation that he remained silent, but the court can evaluate his silent in the case that the defendant **selectively** stated<sup>156</sup> on the individual questions.

## 1.4 Basic Concepts of Evidence Law

### 1.4.1 Admissibility/ Beweisfähigkeit

The evidence competence, so-called admissibility/ Beweisfähigkeit in the Code of Criminal Procedure, means that evidential materials should have the qualifications, by which these materials can be investigated at court for the purpose of finding the

---

<sup>154</sup> Yu-Hsiung Lin, Criminal Procedure Law, 7<sup>th</sup> edition, angel publish: Taiwan, 2013, p.492.

<sup>155</sup> About reinforcement evidence, there are many judgements available for reference, such as (92) Tai Shan Zhi No. 995 Penal Judgment (2003) of the Supreme Court, and (95) Tai Fei Zhi No. 265 Penal Judgment (2006) of the Supreme Court.

<sup>156</sup> The right to remain silent is the positive right that the legislature authorized the defendant can freely decide to open or close the use of his statement as evidence at one time in one trial. But if the defendant decided to testify at court, which means he open the use of his statement, the court can evaluate his statement with its own confidence, even though the defendant kept silent afterwards. See Yu-Hsiung Lin, supra note 154, p.163-164.

crime. According to the Code of Criminal Procedure<sup>157</sup>, the admissible evidence must meet negative and positive conditions. The negative condition is prohibition of using this evidence, which is similar to the exclusionary rules in the American law or Beweisverbotungsverbote in German law. For example, Article 156I states, “*Confession of an accused not extracted by violence, threat, inducement, fraud, exhausting interrogation, unlawful detention or other improper means and consistent with facts may be admitted as evidence.*”, or “*Evidence ... having not been lawfully investigated, shall not form the basis of a decision*” in Article 155II. In other words, the qualified evidence must be obtained through a lawful evidence collection process.

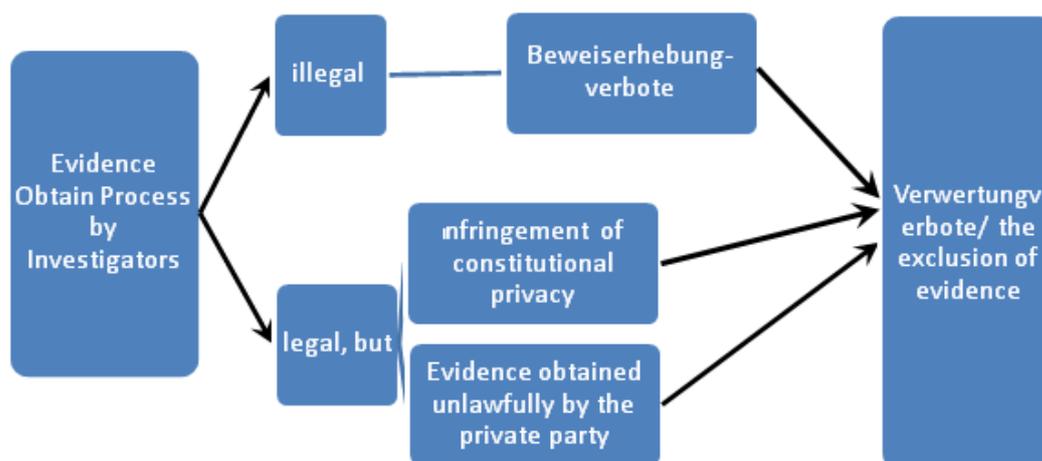


Figure 5 Negative condition- Beweisverbote

Evidence that is not prohibited must qualify both with positive conditions, so that it can finally get the admissibility. The positive condition, in a nutshell, is the principle of strict proof. In other words, evidential materials will finally get the admissibility only through the investigation procedure by strict proof, and therefore it can be the foundation to identify the facts of the crime.

#### 1.4.2 The Probative Value of Evidence

<sup>157</sup> Article 155 II of the Code of Criminal Procedure states, “*Evidence inadmissible, having not been lawfully investigated, shall not form the basis of a decision*”.

The probative value of evidence is the rule to be resolved what rules the judge based on to determine whether this evidence can be trusted, after this evidence obtained the admissibility. For example, whether the judge adopts the witness's testimony after this witness has been sworn and stated in the courtroom. This is the question of evidence evaluation. According to Article 155I, "*The probative value of evidence shall be determined at the discretion and based on the firm confidence of the court*", it is so-called the principle of judicial discretion.

The following figure is the entire process to show how the evidential material became the admissible evidence and was considered by judges as the basis of judging crime facts.

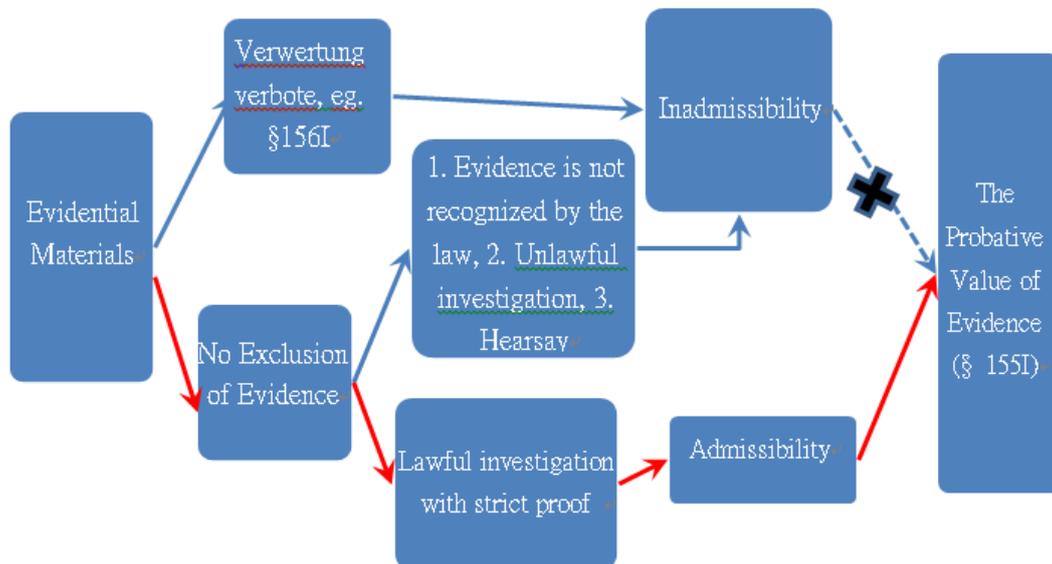


Figure 6 Evidence review process

### 1.4.3 Hearsay

The law of rumors is applicable to electronic evidence, and only when electronic evidence is used to prove the authenticity of the event reflected in its record information. Whether the digital evidence should be considered an exception to the hearsay evidence and should be excluded? What is the source of law? These two issues should belong to the subject of discussion in our criminal procedure law.

Taiwanese judicial practice has disputes on whether digital evidence/ social

media evidence is applicable to the hearsay rule; there is a claim that computer records are not hearsay evidence and is admissible. The reason supporting this claim is that computers automatically produce these records, which does not contain the elements of the confession and should not be considered as the confession of evidence. Therefore, it is not subject to the Criminal Procedure Law Article 159I.<sup>158</sup> A few scholars who support negative opinion think that, the computer records are hearsay evidence, and should be inadmissible at court. The following conclusions can be learned through the relative regulations and legal practices.

First, from the United States and Taiwan literature and the case can be found: In addition to electronic equipment generated records, rumors of electronic equipment storage records (second category) and mixed derivative records (third category) have the necessary and legal effects, That is, the "human-made" factors involved in the digital evidence, should be subject to rumors of the norms; as electronic equipment generated records, because it is actually physical evidence, does not contain "human-made" factors, it should not be hearsay to be standardized., only to be evidence of the standard test. This is consistent with the rumors of the law and the scope of the same, worthy of recognition.

Second, so far our country to accept the computer automatically generated records do not belong to hearsay evidence based on the source of evidence, mostly cited in Article 159-4 (2), "*In addition to the circumstances specified in the preceding three articles, the following documents may also be admitted as evidence: ... (2) Documents of recording nature, or documents of certifying nature made by a person in the course of performing professional duty or regular day to day business, unless*

---

<sup>158</sup> Article 159II of the Code of Criminal Procedure states, "*Unless otherwise provided by law, oral or written statements made out of trial by a person other than the accused, shall not be admitted as evidence.*"

*circumstances exist making it obviously unreliable;* "and, in addition to the circumstances mentioned in 159-4 (3), *“Documents made in other reliable circumstances in addition to the special circumstances specified in the preceding two Items.”*, as the general terms of the article. In these cases, Taiwan legal practice shares the same opinion with American legal system, on the matter of applying the hearsay rule to digital evidence.

Third, as to open before the negative for the computer automatically into a record whether it is hearsay evidence, whether the ability to evidence section, this article that is sure to take it as. Provided that the provisions of Article 830 of the Federal Rules of Evidence provide that the exceptions are "hearsay evidence", that is, the circumstances of the article are still hearsay evidence, except that the exception is adopted as the basis for the determination of the facts. As for the provisions of Article 159 of the Code of Criminal Procedure, the provisions of which are not exceptions to hearsay evidence, so the computer automatically generate records in Taiwan is not the hearsay evidence.

## **2. Obtaining Social Media Evidence**

For the acquisition of digital evidence, in principle, the law does not expressly stipulate, should still from the existing legal provisions to find the basis of legal authorization, and our current law on the acquisition or preservation of the evidence when the relevant provisions of the Criminal Procedure Law as the main , And the seizure of the law is the most effective direct evidence and the implementation of the preservation of evidence, it is in the digital evidence to obtain the criminal procedure in the search for seizure norms for the legal basis is a more appropriate way. But the problem is that the nature and characteristics of digital evidence is different from the general form of evidence, the existing criminal procedure law in the relevant

provisions of the search seizure, is sufficient to apply to all computer or cybercrime cases generated by the digital data , If the investigating authorities in the search for seizure, should be obtained in advance of the search ticket requirements, the investigating authorities how to obtain a warrant before the implementation of the site search, whether a warrantless search, whether the elements and the reasons are similar to the search seizure tradition Evidence of the requirements of the current investigation of computer or Internet crime in Taiwan, the investigation of this computer or Internet crime cases, digital evidence of the search and seizure and other procedures, only in accordance with the relevant provisions of Taiwan's current Criminal Procedure Law, but whether Really enough to fully apply to the acquisition of digital evidence, but also how to solve the case, cannot help but doubt.<sup>159</sup>

## 2.1 Rules for Search and Seizure

Because the existing criminal procedure law does not have the relevant definition or acquisition of the relevant evidence, but there are provisions of the electromagnetic record of the search for seizure, and because of the characteristics of electromagnetic records and traditional forms of evidence are not the same, but with the same evidence may be difficult to understand the characteristics of the people directly understand the understanding of the characteristics, in some cases may be the same or similar, for example, the case of corruption, the bribe will be all the bribe list and bribes to WORD text file or EXCEL form file storage computer hard disk, at the same time with digital data and computer processing by showing the symbols sufficient to show the characteristics of those who use it, it may be through the criminal procedure law on the electromagnetic record search for the provisions of the seizure The legal basis for obtaining the evidence.

---

<sup>159</sup> Chin-Li Wang, Research on Digital Evidence of Computer Network Crime Investigation, Taiwan Prosecutor Review, No. 13, 2013, p.18.

### 2.1.1 Purposes and Threshold

Search for the purpose of searching for a defendant or a third person's physical, object, electromagnetic record and forced disposal of a house or other premises for the purpose of discovering the defendant (including the suspect), the evidence of the offense or other objectionable confiscation. Search, according to different indicators and can be different classification. For example, according to the purpose of the search, the purpose of the purpose of the discovery of criminal evidence or may be confiscated, called investigation or investigation search, often followed immediately after the search behavior is a seizure procedure; the contrary, if The purpose of the search is to find the defendant or the suspect, then called the arrest of the search, so after the search behavior is usually followed by the arrest. Therefore, the search is not only a means of seizure, but also the enforcement of the arrest method (Article 8 of the Criminal Procedure Law, Article 3 and Article 131). If the object from the search as a benchmark, can be divided into the defendant (body), the defendant (objects, electromagnetic records, residential or other premises) or third, third person, called the defendant's search with a search for a third person. The defendant is the object of the right to sentence, on the one hand to enjoy a lot of procedural rights, on the other hand also forced to punish the corresponding tolerance obligations, so in the Criminal Procedure Law Article 122 I, if necessary, the search for the defendant The body and its objects; the other hand, the third person is not the object of the right to tort, it does not correspond to the defendant's procedural rights, but also as the defendant's endurance obligations, is, to launch a higher threshold for search, criminal procedure Article 22 II, provides that only a reasonable reason to believe the defendant or the existence of the object should be detained for the limit, had to search the third person and its objects, we can see that the defendant and the third person Search threshold is

different.<sup>160</sup> Basically, the so-called proclamation of the principle of proportionality as a criterion for reviewing the legitimacy of the search should be based on the fact that the national investigating authority must provide a factual basis for the principle of proportionality, and that the facts are only sufficiently clear Reasonable, and the so-called good reason is to have a more clear factual basis, enough to prove that there are search reasons exist, the difference between the two should be proof of the degree of difference.<sup>161</sup> Therefore, it is necessary for investigative authorities to consider the different threshold to search and seizure the defendant or a third party, no matter the object of their conduct is tangible entity (e.g. the body, objects and other dwellings) or invisible digital data (e.g. computer records, or social media evidence).

Seizure refers to the acquisition of material which may be evidence or confiscated, and for the possession of the mandatory punishment, the purpose is to preserve the evidence may be confiscated or confiscated. In the practice that the seizure is a kind of compulsory punishment, in order to seize the meaning of the implementation of the seizure and the implementation of the effect; thus, the meaning of the seizure is expressed in the case of the holder of the seizure and the entitlement of the person to be detained under the power of the investigating officer, the seizure of which is legally recognized by the investigative authorities.<sup>162</sup> The object of the seizure, that is, the object, is a matter of evidence, and the two are confiscated, which is expressly stated in the first provision of Article 133 of the Criminal Procedure Law. The former is in order to prevent the destruction or loss of evidence, the purpose is to preserve the evidence to facilitate future prosecution trial, which is based on the

---

<sup>160</sup> Yu-Hsiung Lin, *supra* note 154, p.352.

<sup>161</sup> Lai-Jier Her, *Legal Review on the Event of Searching Piracy MP3 in National Cheng Kung University*, *Taiwan Law Journal*, No. 23, 2001, p.87.

<sup>162</sup> Jiun-Yi Lin, *Criminal Procedure Law Textbook I*, 12<sup>th</sup> edition, Sharing publish: Taiwan, 2011, p. 331-332.

preservation of the future implementation of the purpose.<sup>163</sup>

The use of computers and the Internet has become the majority of people in this century's living and communication habits, a considerable part of the criminal behavior is gradually changing, and different from the type of crime in the past, so the electromagnetic record in the proof of the facts of the crime, the importance But the electromagnetic record has a special way to save, easy to modify and tamper with the form of special, not easy to distinguish between the original and other characteristics, and different from the traditional evidence, evidence and evidence, and in the investigation or litigation stage will challenges related to the ability to obtain and verify evidence of electromagnetic records.<sup>164</sup> In Article 122 of the Criminal Procedure Law, it is stated that the electromagnetic record is the object of the search and that it is divided into the threshold of the search for the defendant or the third person. Article 128 is also specified as the search for the electromagnetic record one of the things to be recorded. The purpose of the search for the seizure of electromagnetic records is to obtain an electromagnetic record that can be stored on a computer or network for evidence or confiscation in order to facilitate future prosecution proceedings or to enforce the execution. In the event of a search warrant, the relevant search in the Code of Criminal Procedure The specification of seizure, but the electromagnetic record is different from the traditional form of evidence. Therefore, it is different from the search procedure for the search and seizure of the electromagnetic record and the traditional evidence. However, it should be differentiated and different from the procedure.

### 2.1.2 Proceedings and Manners of Implement

---

<sup>163</sup> Shih-Yen Chu, *Criminal Procedure*, 3<sup>rd</sup> edition, Sanmin publish: Taiwan, 2007, p.133.

<sup>164</sup> Chia-Mei Kuo, *On the Definition and Method of Evidence of Electromagnetic Records - Comparing the Relevant Provisions of Canadian Electronic Evidence Uniform Law and Taiwan Criminal Procedure Law*, *Science & Technology Law Review*, Vol. 17 No. 4, 2005, p.12.

In order to obtain the electromagnetic record stored in the computer or the network, rather than the storage device itself, because the human sensory perception cannot directly understand the contents of the file information, must use the computer And other equipment in order to display the text, symbols, pictures or video, so the electromagnetic record search seizure execution procedures will be different from the implementation of the traditional search seizure is different from the implementation of traditional search seizure, belonging to a stage of search mode.<sup>165</sup>

In order to find the evidence of the crime or the confiscation of the object, and to enter the search should be the place, in the field search, in the process of discovery should be detained, based on the preservation of the necessary, for the detainment of the exclusion of the searched person Possession, and then by the law enforcement officers to obtain possession of the goods should be detained<sup>166</sup>. For example, the suspect in the Silver House took the opportunity to steal gold, the burglary process was recorded by the silver floor monitor, the police were reported, in accordance with the monitor screen, the line seized the suspect A and its residence, and by the prosecutor The court asked to issue a search ticket, enter the suspect's residence, looking for stolen gold that the case should be detained. In the case of search arrests conducted by such search methods, the police will complete the compulsory seizure and seizure at the search site and will not deduct all the items in the residence of the suspect A from the police station and check again to confirm whether there may be evidence or confiscated seizure. After all, the purpose of the search is to find the seizure and exclude the seizure of the seizure of the seizure of the seizure of the authorities, in order to facilitate the future prosecution and preservation of the

---

<sup>165</sup> Rong-Geng Li, Search and Seizure of Electromagnetic Records, National Taiwan University Law Journal, Vol. 41, No. 23, 2012, p. 1059.

<sup>166</sup> Chaur-Yi Huang, Criminal Procedure, enlarged edition, bestbooks publish: Taiwan, 2007, p.221.

implementation.

#### 2.1.2.1 Application on Social media evidence/ digital evidence

The social media evidence, as information, itself does not have a tangible form and cannot directly understand the content of the information it carries through the sensory perception of the general person. It must be restored by certain high-tech equipment to the information that can be understood by human sensory perception.<sup>167</sup> Therefore, in the implementation of the search record on the electromagnetic record, it must rely on some high-tech equipment to carry out, for example, the implementation of electromagnetic recording on the computer search. When the investigators want to get the matter is the electromagnetic record, the search seizure process will be different from the traditional search detention.

In the current search mode, the whole process will be classified into a carrier for searching for and detaining the electromagnetic record, such as a computer or a flash drive, and then the search is carried out in a two-stage search mode. In the search site other than to the investigation of the organs of the equipment, according to computer identification procedures, search for the carrier within the required electromagnetic recording of the two stages of implementation. For example, in the case of a criminal suspect B, the investigator will be allowed to enter the residence of B, and search for the electromagnetic record carrier such as computer equipment or hard disk, CD-ROM or flash drive, and detain it to the investigating authority. After the identification staff will be deducted from the carrier for computer identification, not in the search site search for the required files.<sup>168</sup>

Investigators searched the computer, found the electromagnetic records as

---

<sup>167</sup> Lai-Jier Her, Recording, Videotaping, Investigation of Electromagnetic Records (Article 165-1 II of the Code of Criminal Procedure), Taiwan Bar Journal, Vol. 8 No. 9, 2004, p.33.

<sup>168</sup> Rong-Geng Li, supra note 165, p. 1060.

evidence of the facts; whether in accordance with the Criminal Procedure Law Article 133 of the first one to seize, at the implementation level can detain the electromagnetic record alone. If not, whether the entire hard disk must be detained, or the hard disk information will be transcribed to the disk and detain the disk, in the specification, the detention can only be targeted for the body, for the electromagnetic record itself cannot be detained, can only use the electromagnetic record attached to or recorded in a body, such as hard disk or flash disk storage device, had to seize the storage device to obtain the inside of the electromagnetic record.<sup>169</sup>

Practically common electromagnetic record seizure, there will be the existence of the electromagnetic record of the storage device seized, with scientific and technological equipment to check the information recorded within the electromagnetic record to be seized, the storage device within the necessary electromagnetic records, copy the law enforcement unit held by the storage device, or the whole part of the computer together with its storage device with the seizure. But still distinguish between the circumstances to carry out, such as simply to prove the existence of text content, can be printed within the electromagnetic record of information to be seized. If the desired electromagnetic recording is stored in the storage system of the network system and only a very small amount of data is available, the storage device that seizes the entire network system will not conform to the principle of proportion, and the necessary electromagnetic records may be taken and reproduced in law enforcement units held by the storage device to be seized. If you want to obtain the electromagnetic record is a system file with the characteristics of the way cannot be presented by browsing, it should be the entire computer with its storage device with the seizure, and then computer identification to obtain evidence.

---

<sup>169</sup> Lai-Jier Her, *supra* note 161, p. 88.

Traditional search seizures and seizures of electromagnetic records, in the same way that no matter what kind of search to seize the seizure, the investigators must enter the searcher's premises and take possession of the particular article with coercion, but also There are differences, for example, in the traditional search seizure, for the evidence of things for the investigating authorities to obtain, is the seizure itself, such as criminal guns, on the contrary, in the electromagnetic record search seizure , In real terms, is not the carrier of the seizure, but the archives within the carrier. In other words, the carrier seized by the investigating authority is not evidence, but only a container for storing information that is used as evidence. Moreover, in the traditional search seizure, most of the search in the premises of the search, the scene to confirm whether the discovery of things should be detained, and obtain possession. However, when the investigating authorities want to obtain the object is the electromagnetic record, the investigators are mostly seized to find the carrier, and then in the investigation organs or other premises within the computer identification, search and confirm that there is no need for electromagnetic records. The former is a typical first search and then seized, the investigating authorities to obtain, there are quite a reason to be detained things, but the latter is to find the search site with or without carrier, and then seize the necessary information carrier, and then search the carrier the file.<sup>170</sup>

As a result of the Criminal Procedure Law on the electromagnetic record search seizure of the specification, only in the original provisions of the provisions of the electromagnetic record, but not in accordance with the electromagnetic recording and traditional physical evidence of the characteristics of the differences have different specifications, the current investigative authorities focus on the electromagnetic

---

<sup>170</sup> Rong-Geng Li, *supra* note 165, p. 1063-1064.

record. The search seizure is only cheap at the executive level and is not expressly provided for by law and not only affects the rights of the electromagnetic record holder or owner (the defendant or third party) to use the computer and other storage media for the storage of the electromagnetic record, after the detained computer and other storage media did not find any criminal information relating to the case, how to indicate that the seizure has been in due course. It can be seen from the above, the investigating authorities to obtain the electromagnetic records related to the case, should not be directly on the electromagnetic record itself for the search, should be found to save the case related to the electromagnetic recording of the storage device, and then to search the device to obtain electromagnetic records, This part and the digital evidence cannot be used as evidence of the body, alone and for the general people can directly understand the understanding of the senses, but also through certain equipment can only be learned from the same characteristics, but in the current law of the lack of norms and operating methods to act cheap Circumstances, so that the investigating authorities in the electromagnetic record for the search seizure or other means of acquisition, was not in line with due process of law, and cannot guarantee the basic rights of the people.

### 2.1.3 Issues on Search with Warrant

The search system is a kind of compulsory punishment against the basic rights of the people. It is a constitutional reserve in the United States law, that is, the people are not subject to unreasonable search seizure is the basic rights of the people protected by the constitution, while our country has not directly , The judicial officer, the prosecutor and the prosecutor shall, on behalf of the investigating officer, represent the organs of the public power of the State, and in the conduct of the search for the seizure of such public power in such a state, the elements, authorization, to the proper

legal procedures and the principle of legal retention, so in the criminal procedure law expressly provides the investigating authorities to perform a search to the court to issue a search ticket procedures and requirements.

In accordance with the provisions of Article 128 of the Criminal Procedure Law, Article 1 of the Criminal Procedure Law shall, in addition to the circumstances of Article 21, The provisions of the twenty-eight article, to the court of law to seize the search ticket, the search ticket should be recorded on the case, should search the defendant, the suspect or should be detained, should be added to search for the premises, objects or electromagnetic records and valid period, overdue implementation of the search and search should be returned after the search ticket will be the intention and other matters, and explain the reasons to facilitate the issuance of search tickets, in addition, the judicial police officers due to investigate the criminal suspects and evidence collection. If there is a search, if necessary, in accordance with the provisions of the second paragraph of one hundred twenty-eight, reported to the prosecutor after the permission to the court to issue a search ticket. The reason why there must be a search for the order of the warrant principle, the Department of the investigation organs in the implementation of the search process, the search for the object, the scope to be clear and detailed records, to avoid improper or excessive search and against the searcher Property rights or privacy, so when the search object is involved in electromagnetic records, it should be clearly recorded in the search ticket, to avoid illegal search situation. In order to determine whether the search system for which you want to search and seize is a computer host, a computer hard disk, an external storage device or an electromagnetic record stored on a computer's hard disk, the investigating authority shall, when searching for a search ticket, In order to determine the scope of the investigator in the implementation of the search for this

mandatory punishment as the scope, and the searcher of the corresponding bear the scope of their obligations clearly.

If the search ticket only records the search and seizure of the storage device entity such as a computer hard disk, it shall be less effective than the electromagnetic record stored in the storage device, and the storage device such as a computer hard disk must be recorded on the search ticket and the storage device of the electromagnetic record, was seized at the same time. Therefore, if the prosecutor or the judicial police officer to the judge to search for a ticket, in the letter of the request should be detained only records the computer hard disk, the implementation of the search, should only seize the computer hard drive, but the computer hard disk after detention , The prosecutor or the judicial police officer shall not boot the computer's hard disk and search for the electromagnetic record in the computer's hard disk, since the electromagnetic record is not within the scope of search and seizure, so as to exceed the contents of the search ticket, Electromagnetic record seizure, the seizure is no search ticket seizure.<sup>171</sup>

As the electromagnetic record is not like the general certificate or evidence, such as the murder case in the case of weapons, we can directly understand with the senses, electromagnetic records must use a specific machine or equipment can only show, so the electromagnetic record is usually digital data, stored in computer hard disk and other storage devices, such as a disk or a web server, if the investigating authorities in the investigation of computer or Internet crime cases, to the defendant, the suspect or third person held by the case related to the electromagnetic Record to search, in the court to seize the search ticket, in addition to the reasons should be made to make the court believe that the launch of the search is necessary or quite a reason, the search

---

<sup>171</sup> Ming-Yung Wang, Search and Seizure of Cybercrime, Law Journal, No. 191, 2003, p.50.

should be detailed records of the object to be searched, but the electromagnetic record storage The form of the form, the form of presentation is different from the evidence of the subject, and it is sometimes easy to be extensive and general, not clear enough, and the design of the search ticket is to allow the court to examine whether the investigating authority There is a fishing or unrestricted search, and improperly and overly infringed the seizure of the property or privacy purposes contrary . It is not easy to search for a particular search on the search ticket because the electromagnetic record may be stored in a different storage device at the same time, and may be placed in different places at the same time, and the data of the electromagnetic record may be too large or redundant. The relevant parts are difficult to determine and other factors, but also caused in the search ticket records on the electromagnetic record of the search seizure, cannot meet the requirements of specific clarity.

The search for how to record electromagnetic records on search tickets will not violate the specific principles of warranties, and should be classified as search for information on electromagnetic record carriers and related equipment and carriers. In order to seize the hardware of a computer or related equipment in particular premises, the investigating authority shall state that there are reasonable grounds in the case that it is believed to be evidence or confiscated. The court considers that there is a reasonable reason for the seizure of the hardware , And authorized to search for seizure, the search issued by the ticket specifically records the computer and the carrier and other objects, can meet the specific principles of clear requirements, as the investigating authorities want to obtain the storage device within the electromagnetic record, as evidence , The court should also specify the information to be searched by the investigating authorities, and not only the carrier such as magnetic disc, CD-ROM, computer hard disk or flash drive. Otherwise, the search ticket is no different from the

authorized investigators to conduct a general search, open all the files in the carrier or get any information, resulting in search behavior without restrictions, and with a clear specific principle contrary.<sup>172</sup>

In principle, the investigating authorities shall comply with the provisions of the Criminal Procedure Law concerning the search ticket and the search ticket should be specified, whether it is for the electromagnetic record or the digital evidence of such non-body or the general tradition of evidence of the seizure of evidence . But in the electromagnetic record or digital evidence of the search seizure, search tickets how to record that is a problem, such as the investigation of criminal information in the acquisition of the more accurate the more specific scope and object, in order to avoid the search ticket records are too general and general. As for the need to obtain electromagnetic records or digital evidence investigators must first find the existence of the electromagnetic record or digital evidence of the storage device, so the search should be clearly documented on the storage of the case may be related to electromagnetic records or digital evidence storage device, Take advantage of the search after the seizure.

#### 2.1.4 Disposal after Seizure

The purpose of the seizure lies in the fact that the disposition of evidence or confiscation is placed under the strength of the investigator, in other words, that the evidence is preserved and conducive to the future trial and execution. The manner of disposition after seizure is provided for in articles 113 to 141 of the Code of Criminal Procedure, including the seal, proper disposal, guarding and destruction of the auction.

---

<sup>172</sup> Rong-Geng Li, *supra* note 165, p. 1092-1093.

The provisions of the existing law on the seizure of seizure, the provisions of the existing law in Taiwan, only a little provision, is not complete, and the relevant provisions of the subjective evidence of the disposal of the application may not be much problem, but in view of electromagnetic Records are not the same as the traditional form of evidence, which may be in the form of digital, while stored in several computers, or in the network system, and storage of content may be like a library of books. As a result, there is doubt as to how the law enforcement officers should dispose of the seizure after seizure.

Moreover, if we want to seize the electromagnetic record of the seizure, there is no restriction or to the court to search for a ticket after the trial, the court should be how to consider, whether to add a certain burden. But also because of computer equipment and electromagnetic records in the use of modern life is very common, the parties may please return.

## 2.2 Exceptions for the Search without Warrant

The search, seizure, in the criminal procedure law with a warrant search, the principle of seizure, can also be called the search, but in exceptional circumstances, allowing the case without a search, can also be called Non-wanted search. This particular exception can be divided into consent to search, emergency search, incidental search, incidental seizure and seizure. In the case of computer-based or cybercrime cases, the seizure of detainees will also occur.

### 2.2.1 Search with Subject's Consent

According to the provisions of Article 131 of the Criminal Procedure Law, search, to accept the search for voluntary consent, do not use the search ticket. But the executive shall produce the document and record his intention in the transcript. It can

be seen that as long as the investigating authorities in the search by the search before the search, the consent of the search by the person, and its consent to set the transcripts, no search for votes, have to search, will not constitute an illegal search.

The search for seizures of electromagnetic records should also be the same applicable standard, that is, as long as the search by the searcher can perform the search, but the immediate problem is how to determine whether the searcher is voluntary consent, whether the scope of the search with the consent of the range Consistent. Moreover, the question was raised whether the searcher really has the right to consent, that is, whether the consent of the appropriate person.

#### 2.2.1.1 The concept and scope of consent

In practice, the judgment of consent must be the consent made by free will from the person who was searched, rather than by investigators' express or implication with coercion, concealment and other improper methods, or by the person's misunderstanding.<sup>173</sup> And the court for the evidence obtained from the consent of the search, since the consent of the consent of the person who has the consent of the consent, whether the consent of the record recorded by the searcher signed or issued a written statement of consent, and should integrate all the circumstances, including solicitation, the place of consent, the manner in which consent is made is natural rather than threatening, the strength of the subjective consciousness of consent, the degree of education, IQ, and the will of the autonomous have been succumbed to the person who performed the search, Agree that the search is not for voluntary consent, it should be more detailed reasons to review the results of the review, otherwise there is no reason to make a decision.<sup>174</sup> Basically, the consent of the search can block the

---

<sup>173</sup> (96) Tai Shan Zhi No. 5184 Penal Judgment (2007) of the Supreme Court.

<sup>174</sup> (94) Tai Shan Zhi No. 1361 Penal Judgment (2005) of the Supreme Court.

search of the illegal, so in the implementation of the electromagnetic record of the search, in principle, as long as the holder of the electromagnetic record that is searchers agreed to check the investigation organs of the illegal, but Provided that there is no need for the investigator to mislead the lure to cooperate with the investigation, or by the search person does not understand or no resistance to the case of consent.<sup>175</sup> In the consent of the search, only in the scope of the search by the consent of the search, in the electromagnetic record of the consent of the search, additional restrictions, such as the search by the people agreed to provide their computer hard disk or other storage devices within the electromagnetic Record, but did not agree with the investigators to obtain their access to the computer system password, such as investigators unauthorized access to the search by the computer password, the search, apparently surpassed by the consent of the search by the restrictions, and beyond the original consent of the scope of the search.<sup>176</sup>

#### 2.2.1.2 The third party's consent

From the provisions of Article 131 of the Criminal Procedure Law that in the consent of the search, the right to agree to the search organs to search for the search by the person, so as long as the search by the people, can be voluntary consent to the investigation Of the search behavior, from the meaning of the text to allow third parties agree to the possibility of search, that is, the investigator can be independent of the criminal case with a third party voluntarily agreed to a certain place to search. In my practice is also a clear recognition of the third person agreed to search, and attention is the common authority of the elements exist or not, regardless of the criminal case of the defendant in the subjective and objective whether the commitment of the common authority that the searcher may agree to investigate the

---

<sup>175</sup> Lai-Jier Her, *supra* note 161, p. 89.

<sup>176</sup> Ming-Yung Wang, *supra* note 171, p.54.

risk of personnel search.<sup>177</sup>

Whether the third person can agree to the search on the computer held by the electromagnetic record search, depending on whether the third person has access to the computer or access to information, if the third person there Agree with the search authority, and then further, to determine the scope of the consent of the third person, if the computer within a specific storage area is not a third person contact or have a friend password access, then the third person on the some do not have permission to do so. In addition, the use of the network has gone beyond the physical limitations of space, and thus in the search of the regional network or computer systems to the remote network services to provide managers of the occasion, the use of third parties and whether the password Protection, it becomes the most important factor to judge.

#### 2.2.1.3 Consent from internet Service Provider or web server administrators

In the search for electromagnetic records, consent authorized from internet service providers or web server administrators is a big problem. Because the administrator has to access the user's account and read its information, which may infringe the privacy of the parties, if the recognition of these providers or administrators have the right to agree to search the entire network system. But if the user can expect these service providers will enter the file of the user of the system, or the system is to provide services to the public and information are publicly shared, it should be recognized that internet service provider or web server administrators have been authorized the agree to search users' accounts.<sup>178</sup>

#### 2.2.2 Exigent Circumstances

---

<sup>177</sup> Rong-Geng Tsai, Yes,I do: Search with Consent and the Third Party's Consent, The Taiwan Law Review, No. 157, 2008, P. 113-114.

<sup>178</sup> Ming-Yung Wang, supra note 171, p.55.

Article 111 of the Criminal Procedure Law stipulates that the Prosecutor does have a good reason in the investigation that the situation is urgent and that the search for evidence of forgery, alteration, annihilation or concealment within 24 hours , Search or prosecute the prosecutor, the judicial police officer or the judicial police to carry out the search and report to the Attorney General. This provision is in order to enable the investigating authorities in the investigation of criminal cases, due to the urgency of the emergency call to search for votes, and the evidence is about to lose the situation cannot be immediately preserved, allowing the investigating authorities in the case of no search votes to search, As a basis for legal authorization for urgent search.

According to the provisions of the analysis, the subject of the search should be the prosecutor, or by the prosecutor command of the auxiliary investigation, that is, prosecutors, judicial police officers or judicial police. If investigators do not search quickly, there will be evidence of forgery, alteration, annihilation or concealment of the possibility, cannot be preserved. In the investigation practice, not to the prosecutor personally to the implementation of the command is necessary, such as the investigation of the main body to confirm the existence of evidence and emergency search is necessary, should be reported to the prosecutor, after its permission should be an emergency search, this Is also a prosecutor's punishment.<sup>179</sup>

The investigating organ shall consider the computer network related equipment and its electromagnetic recording in consideration of the emergency judgment of the search for electromagnetic records. If the investigators find that the computer's hard disk is damaged or stored, It is necessary to urgently and urgently search for the urgency of the search if the electromagnetic record used as evidence is annihilated,

---

<sup>179</sup> Yu-Hsiung Lin, *supra* note 154, p.361.

and if the computer's hard disk or other storage Device, placed in the control of the control and isolation of the defendant or the suspect's strength under the control of the electromagnetic record has been no annihilation of the possibility of urgency does not exist, then want to search the electromagnetic record should be re-search The ticket is suitable.<sup>180</sup>

### 2.2.3 Search Incident to Lawful Arrest

Article 130 of the Criminal Procedure Law provides that the prosecutor, the prosecutor, the judicial police officer or the judicial police to arrest the defendant, the suspect or the execution of the detention, detention, although no search ticket, have to search for their body, carry The carrying of the thing, the means of transport used and its immediate accessible premises. Which provides that the investigator, in the absence of a search warrant, in the case of a forced arrest, such as the execution of an arrest, carries the search for the body of the arrested person, the carrying of the thing, etc., with the aim of finding the probable person Attack the investigators' weapons, or may contain evidence of the loss.

The purpose of the search is to protect the safety of law enforcement officers and to prevent the defendant from annihilating the evidence. In the search and seizure part of the electromagnetic record, it is not intended to be used as an attacking weapon after arrest or detention of the defendant Electromagnetic recording or storage device, but to find an electromagnetic record or storage device that may have evidence of a crime related to the defendant, such as a flash drive carried on the defendant.<sup>181</sup>

In addition, in the process of incidental search will be found in the case with the

---

<sup>180</sup> Ming-Yung Wang, *supra* note 171, p.55.

<sup>181</sup> Yu-Hsiung Lin, *Kommentar- Durchsuchung und Beschlagnahme*, Angel publish: Taiwan, 2002, p.137.

electromagnetic record or should be detained in the matter, at this time should be in accordance with the provisions of Article 137 of the Criminal Procedure Law to implement the incidental seizure, There is no record of electromagnetic storage, there is no emergency situation exists, if you know the storage device within the electromagnetic record content, you must obtain a search ticket, can be searched.

In accordance with Article 152 of the Criminal Procedure Law, when the search or seizure is carried out, it shall be found that the articles of detention shall be seized and sent to the court or the prosecutor respectively. This situation is used in the search record of electromagnetic records, provided that there must be a legitimate search behavior first, and in the search process found another case to seize evidence or should be detained. For example, the investigating organs of the search for the voice of the request, in order to find corruption cases bribery register of electromagnetic records, but in the search process but accidentally found a list of drug trade, you can seize, but cannot turn to search and drug cases Of the electromagnetic record, you must re-search for the search ticket, and then perform the search side is appropriate.

When investigating a computer or cybercrime case, the most effective way to collect the electromagnetic record related to the case is to search for the seizure, and the criminal procedure law stipulates that, in addition to the urgency of the necessary search, The search should be sent to the court to issue a search ticket and indicate the object to be searched on the search ticket and state the reasons for consideration by the court. So the search is based on the principle of order, but sometimes the scene of the investigation of different circumstances, in order to avoid the loss of evidence or to protect the safety of investigators, the exception to allow no warrant search, but in the implementation of the investigators should pay attention to this Whether the seizure of the search will result in excessive infringement of the property or privacy of

the searcher, be sure to comply with the relevant norms in the Code of Criminal Procedure to ensure that the fundamental rights of the people are not overly infringed.

## 2.3 Discussions

2.3.1 Is it enough to replace the warrant with subpoena to ask the party submitting digital evidence?

In the face of a computer or cybercrime case, the investigating authority has acquired the number of records relating to the case in the event of an electromagnetic record, such as a computer hard disk held by a suspect or a network system in use, If it is stored in the case of a storage device, it shall be governed by the provisions of Paragraph 2 of Article 133 of the Criminal Procedure Law, by way of document, Digital evidence, so whether there is a search to avoid the search should be issued a search ticket, and should be included in the search ticket should be included in the search, by the official name of the way to replace the search seizure with doubt.

In accordance with the provisions of the Code of Criminal Procedure, for the owner, holder or custodian of the seizure, shall be ordered or delivered (article 33 II of the Criminal Procedure Law). The owner, holder or custodian of the seizure shall refuse to submit or deliver or resist the detainee without justification (subject to the provisions of the Criminal Procedure Law (138)). From the provisions of the open to know that such a proposed or delivery order when necessary to implement a strong seizure, with a strong nature of the mandatory punishment of the basic rights of the people against non-micro, but without the search should be in the search on the ticket Set out the writ of the matter to be recorded, and from the provisions of the open but cannot know, who have to launch such an order. In addition, although the proposed or delivered orders compared with the search seizure, the impact on the relative to the relatively minor, only when not in the delivery of coercive force, like only the nature

of the proposed or delivery orders 28. This article argues that since the same effect is required to be presented or delivered by the order and the search system to preserve the evidence or to obtain the object to be seized, it shall be the same as the request at the time of the search, the principle of the requirements.

### 2.3.2 The object of traditional search and seizure is limited to physical objects.

In the past, the type of traditional criminal cases, whether it is associated with the evidence of crime or the crime used by the things, are the average person to the eye or hand and other senses to understand and understand, in other words, the investigators want to search for seizure Object only need to be able to judge from the appearance of whether it is related to the crime case, so traditionally in the possession of evidence of the seizure of the seizure, the investigation of the seizure of the prosecution as a result of the relevant criminal prosecution law should be able to very clearly tested. In the definition of the scope of the search, the old Criminal Procedure Law only regulate the search and seizure rules for physical objects in Article 122 and the following provisions, but it did not consider individual provisions of conducting search and seizure for the intangible things.<sup>182</sup> However, after the subsequent amendments to the Criminal Procedure Law, there are updated electromagnetic records for the search seizure provisions, the purpose is to solve the problem of seizure of the absence of goods, but also in the application of controversy and problems.

The inclusion of the electromagnetic record as a search for the object of seizure and the search should be clearly documented seems to be in order to respond to the use of computer and network to generate a new type of criminal case of the evidence. If the electromagnetic record relating to the criminal material is already present in an entity, it should be covered by the concept of the preceding article and the search is

---

<sup>182</sup> Chaur-Yi Huang, *supra* note 166, p.201-202.

seized.<sup>183</sup> However, the search and seizure of electromagnetic records should be different from the search and seizure of digital evidence. The record of electromagnetic recording is limited to the record for computer processing. Even if the record is made in electronic, optical and other similar ways, it is essentially digital, But it must be through the relevant computer equipment to display its text, images and other means to express the meaning of the way, so the investigating authorities to obtain the electromagnetic record associated with the case, it is necessary to find the existence of the electromagnetic record of the computer where the premises, in essence, Search for tangible objects or places. However, digital evidence is not limited to records for computer processing, as long as it is stored in the form of digital data in computer hard drives, flash drives, other electronic storage devices or in the network system are digital evidence of the category. After all, the data for the use of evidence is not a body of information, cannot be directly investigated by the investigating authorities to conduct physical search and seizure.<sup>184</sup>

Accompanied by the seizure of the search behavior in order to preserve the evidence or seizure, in order to avoid the loss or destruction of the situation occurred in the traditional body after the seizure, has been placed in the investigating organs of the public power to grasp But if the defendant has previously copied the same version of the same version of the data, if the defendant in the prior to the first copy of the same version of the information, then the future of the defendant, the defendant, the defendant, the defendant, the defendant, The defendant in the court suggested that the version of the defendant would be subject to the determination of the ability of evidence and the judgment of the testimony if the version held by it was different from the previously seized version. This is another question of the problem, and it is

---

<sup>183</sup> Yu-Hsiung Lin, *supra* note 181, p. 62.

<sup>184</sup> Rong-Geng Li, *supra* note 165, p. 1111.

necessary to re-import the relevant regulations.

### 2.3.3 Dilemma of warrant for searching digital evidence

How to perform search seizure, whether to search for the seizure of the computer hard disk, flash drive, other electronic storage devices, or search the seizure of the digitized data itself, and how to search for the seizure of the computer hard disk, flash drive, other electronic storage devices, In particular, how to avoid the search process does not infringe the right to privacy reasonable expectations, because the search object in addition to the case to find the evidence of the crime, may also be related to the case has nothing to do with personal or other people's privacy information, this will be related to Search should be how to record and search the object of the selected, so this part of the determination can be followed by the follow-up search ticket with the search for the implementation of the seizure. How to make SME search under existing law in line with due process of law is an important issue and also involves the need for remediation to respond.

#### 2.3.3.1 Establishing the necessity and the Probable Cause

The search must have a search ticket, the prosecutor in the investigation if the necessary search and written reasons to explain to the court to issue a search ticket, the defendant or suspects are necessary to search, and the defendant or the suspect of the people must have a reasonable reason to search for the past, there is no big problem with the traditional body search, as long as it can be pointed out where or where there is something associated with the case, usually the court will think it is necessary or a reasonable reason, after all, tangible body is easy to understand the senses, but in the search for evidence of the registration of evidence will be controversial, whether it is stored in the computer hard drive, flash drive, other electronic storage device or It is difficult to clarify which part of the data in the

transmission of the network system belongs to the crime-related information or to the suspect, so the investigating authorities before the search for seizure, how to make the court believe that it is necessary or quite The existence of reason is a challenge.

Article 122 of the Criminal Procedure Law distinguishes between the search for the defendant or the suspect and the threshold of the search between the third person and is divided into two necessary conditions. There is a reasonable basis for the fact that the defendant, the body of the suspect, the place of residence, the place of residence or the electromagnetic record may be possessed as evidence of the offense or the relevant evidence; and whether there is a reasonable reason, Search subjective criteria to judge, there is still need to be based on the facts of the facts, with the necessary when the search right to start, the difference in the standard of reason is higher than necessary, the two elements should be the letter of the request, For the sake of the judge.

For the search and seizure of digital evidence, such as the existing criminal procedure law for the search for the direct application of the code, it seems that the program is not complete, because the digital evidence of this invisible digital data, with the traditional tangible body of many different characteristics, It should be necessary to separate the search for seizure of digital evidence separately to set the relevant search seizure norms to the proper legal procedures.

#### 2.3.3.2 The validity and specificity of the search warrant issued

Computer and Internet crime compared with the traditional criminal cases, with anonymity, privacy and cross-regional, and generated as evidence of criminal data used in the form of intangible data stored in the computer hard disk, the other Electronic storage devices and network systems. Therefore, in the collection of evidence related to the crime, often in the computer or network system, and the

traditional investigation process to collect and preserve the evidence of the object of the premises, books, etc., there are quite different characteristics, because stored in the computer Hard disk, other electronic storage devices and network systems in the digital data cannot see its ontology, and no inherent physical characteristics, and digital data with easy tampering, elimination, movement and replication and other characteristics, to specific search The object or object is quite difficult.<sup>185</sup>

Search ticket records search object clear and specifically to avoid the investigation organs have phishing search, such as the investigating authorities to find the evidence of the crime has nothing to do with the computer, since the search without detaining the computer and store its digital data, if we want to find the text file, nor want to open the file browsing view. In contrast, if only the computer hard disk, other electronic storage devices and the Internet system for the search for the object of the search, search seizure of the current capacity is already very large on the shelter device will become a serious threat of privacy, because the current computer or even if the Internet is used by individuals, it also contains a variety of documents, which contain a lot of private privacy or business secret information, if not to search for the seizure of the digital data to be specific, its privacy will not be lower than the invasion of residential search for.<sup>186</sup>

Search ticket records must be clear and specific requirements, the investigation of the investigation process, whether it is in the body of evidence or no body of the data obtained, as long as the investigation as a search for the nature of the seizure, it should It is not questionable to search for the seizure code in the existing part of the criminal procedure. However, in the absence of the body part, especially the

---

<sup>185</sup> Ming-Yung Wang, *supra* note 171, p.49.

<sup>186</sup> Marris Hsieh, *Applying Principle of Writ Doctrine to Computer Search and Seizure: Take American Law as a Mirror*, *Criminal Law Journal*, Vol. 48, No. 6, 2004, P.106.

intangible data, A variety of different forms of storage in the computer, computer hard drive, flash drive, other electronic storage devices, or in the absence of restrictions on the scope of the network system, so in the current criminal procedure law is not a single evidence of the search seizure alone. Under the circumstances, how to strictly observe the principle of clarity and specificity is the investigating authorities to face the challenges and challenges.

In the current Code of Criminal Procedure on the search of the seizure of the norms, the investigating authorities whether the defendant, the suspect or a third person to launch a search seizure, must obtain the court issued a search ticket, and must be included in the search on the search object , Object or scope in order to be clear and specific, and should elaborate on the reasons for the search for the court to consider and as a means of supervision and investigation as a means to avoid improper infringement of the basic rights of the search and to ensure the proper legal procedures to comply. Therefore, whether it is on the tangible objects or intangible digital data, although the defendant, the suspect or the third person to make a distinction between the launch, but this is only the launch of the different benchmarks, does not affect as long as the investigating authorities to launch Search for seizure of this compulsory punishment as a result of the writ should be consistent with the warrant and specific requirements.

#### 2.3.4 Restrictions on warrantless search

An emergency search for a warrantless search for digital evidence Search for seizure is a part of the preservation of the evidence, and the digitization of information is often easily eliminated by a few instructions or actions on a computer or network, as in a drug case , The seller uses the WORD editor to enter the number of drugs purchased by the buyer, the amount, or in the online chat room message

content involves blatant insult and other words, these can be deleted at any time without traces. Therefore, the investigation authorities in the implementation of search seizure, the emergency procedures, to obtain a search ticket may take time is too late to ask, to search for digital information is about to be eliminated or annihilated, are comprehensive considerations, and investigation It is debatable whether the organ can apply to the digital evidence in the past in the past.

As for the accompanying search part of the warrantless search, whether the computer, flash drive, other electronic storage device or the network system used by the search person is a silent search, based on the laws and regulations of the Criminal Procedure Law The provisions of Article 10 are to protect the safety of investigators and to prevent defendants or suspects from annihilating evidence and broaden the scope of the search. If it is to be accompanied by a search for a personal computer, a flash drive, other electronic storage devices, and may also meet the reasonable purpose of the search, but the part of the network system used by the search person, because the network is open for a specific majority. The use of the search, whether the incident will be improperly infringed to the search by people outside the information privacy, so whether it has been beyond the search for a reasonable purpose, there are doubts.

### **3. Admissibility of Social Media Evidence**

Article 155 II of Code of Criminal Procedure provides, “Evidence inadmissible, having not been lawfully investigated, shall not form the basis of a decision.” Admissibility is the qualification that the evidence can be submitted at court for the purpose of determining the facts of the crime. This qualification requires that evidence must have a natural relevance with facts of crime, be in line with legal procedures, and not be prohibited by law or excluded. Therefore, the main requires of

admissibility are evidence should be obtain legally and have a considerable correlation with facts to be confirmed. There are few positive regulations of admissibility, thus it mostly shapes its meaning by rule of evidence exclusion, such as hearsay rule<sup>187</sup>, rule of confession<sup>188</sup> and son on.

The way to proof admissibility must adopt the strict proof, that is, evidence must be provided in the scope of the law requires, and in the meantime, evidence must be investigated by lawful procedure. In line with the requirements of strict proof, the court has been cited as the basis for judging the facts of the crime, and vice versa.

At present, there are five kinds of evidence methods in the Taiwan Criminal Procedure Law: the defendant, the person card, the evidence, the appraisal and the investigation, and stipulates the corresponding proof procedure of the different evidence methods. Different from other non-digital evidence can immediately determine the evidence of their own methods and the corresponding proof of the program (such as the fierce knife should be presented directly on the court, so that the judge can directly view), SME in accordance with its appearance is presented and put forward, Many different forms of evidence can be applied. For example, the prosecutor printed the defamatory text published on his Facebook as evidence of the defendant's libel. This evidence will be recognized as an instrument and must be read aloud to the court. In another case, the defendant filed a defensive defense, the prosecutor asked the expert to issue a report that the IP should be involved in the crime should be owned by the defendant. At this point from the face of the information obtained by the evidence method is identified by the expert witness to

---

<sup>187</sup> Article 159I states, “*Unless otherwise provided by law, oral or written statements made out of trial by a person other than the accused, shall not be admitted as evidence.*”

<sup>188</sup> Article 156I states, “*Confession of an accused not extracted by violence, threat, inducement, fraud, exhausting interrogation, unlawful detention or other improper means and consistent with facts may be admitted as evidence.*”

appear in court or issued an identification report, read in court. Again, the prosecutor to the accused Facebook embedded pornographic film as accused of the defendant to distribute indecent articles. The captured video may be used as evidence, need to be played directly in court, and may require expert witnesses to further explain the relationship between the video and the defendant. The following will discuss the possible evidence of SME.

### 3.1 Social Media Evidence as Documentary Evidence

#### 3.1.1 Documentary Evidence and its Investigation Procedure

First, we must clarify the difference between the instrument and the evidence of the instrument. The former from the appearance of distinction, can be divided into the contents of the instrument as evidence, or the existence of the instrument, the state as evidence.<sup>189</sup> The evidence of the contents of the instrument should be investigated in the form of a documentary evidence; if the existence of the instrument, the state as evidence, we can not only read the way to investigate the state, should be identified or verified by evidence of the way .

The documentary evidence, that is, the documentary evidence, the method of investigating the contents of the instrument, is the legal evidence of the criminal procedure investigation procedure. Document evidence contains two parts: transcripts and general instruments, which is from the provisions of Article 165 we can see. Record refers to the provisions of Article 41 to Article 44, in the investigation process, the trial procedure, by the state investigating organs in accordance with the law of the production of public documents, including cross-examination, search transcripts, seizure transcripts, inspection transcripts, trial transcripts and so on; General

---

<sup>189</sup> Dung-Shiung Huang, Criminal Procedure Law, 6<sup>th</sup> edition, Sanmin publish: Taiwan, 1999, P.366.

instruments refer to other instruments other than transcripts. Such instruments are not limited to those produced by the State investigating authorities, the official documents of other offices, private documents of private or private groups, and the purpose of such Limited to the purpose of criminal proceedings, even for other purposes, also included. Therefore, the documentary evidence referred to refers to the legal evidence of the criminal evidence investigation procedure, if the evidence exists or the state as evidence should be identified or verified by the evidence method, not referred to in this article evidence.

The evidence of the documentary evidence for the reading, the transcripts within the file and other instruments can be evidence, the presiding judge should be the parties, agents, defenders or assistants read or to the gist. If the defendant does not understand its meaning, it shall be given a grievance (article 165). If the defendant does not understand the meaning of the person concerned, Therefore, the investigation of the documentary evidence, in addition to the weathering, or damage to the reputation of others, the principle should be submitted to the defendant to read, the rest to read or to the gist of the way, and with evidence to the investigation different. This document is based on the contents of the instrument as evidence, such as the provisions of article 39 below the provisions of the production of the document, has been guaranteed its true; such as non-statutory procedures for the preparation of the instrument, after reading or , The defendant can also determine its authenticity, no need to make it identified. However, if the book is not read, it is acceptable that the contents of the booklet are true and should be heard by both parties and investigates other necessary evidence.<sup>190</sup>

In principle, the contents of the instrument should be read to the parties, but if

---

<sup>190</sup> Hsun-Lung Wu, A Review on the Investigative Method of Real Evidence and Documentary in Taiwan Criminal Procedure, Taipei Bar Journal, No. 286, 2003, P.61.

the full text of the instrument is too much, if the whole reading may take too much time, it may be expedient for the litigation, as the case may be. However, since the instrument is used as evidence of the meaning of its contents, it is very important that the words and phrases are of the utmost importance, and that the difference between the words and the characters is not so rare, every word, every sentence may have room for scrutiny or dispute, therefore, the documentary evidence of the investigation should be read aloud, not simply as appropriate, and from the nature of the instrument, the parties if asked to read all, Ask for it. The defendant can neither be satisfied with the purpose of the statement, said the contents of the document are doubtful, if not in accordance with their requirements all read aloud, fear of the trial fair. If the defendant has any questions about the authenticity of the instrument or the ability to prove the evidence of the documentary evidence, the author of the documentary evidence of the evidence, Documentary evidence, should also be prompted to identify the defendant was properly.<sup>191</sup> In addition, if the instrument, such as weathering, or may damage the reputation of others and other unfit to read the situation, the parties have to read or report to the gist of the way.

However, the investigation of the documentary evidence is by way of aloud, but not all of the instruments, have to read only the way to read, that is consistent with the evidence investigation procedures. That is, the instrument is not necessarily a legal evidence investigation procedure, even if it is made by law or by way of a gist. The evidence of the book is still in line with the principle of direct trial of the principle, whereby the instrument can be divided into the original evidence of the instrument or derived evidence; such as evidence for the evidence is the original evidence, such as the slander of others written in the text, If the instrument is evidence of a derived

---

<sup>191</sup> Dung-Shiung Huang, *supra* note 189, P.367-368.

instrument, such as an instrument (a transcript of a transcript, a warning record, etc.) in which the witness is stated, the instrument shall not be read aloud only if the instrument is a documented evidence And that the legal evidence of the investigation. In fact, if all the statutory evidence methods and investigative procedures are to be recognized as a substitute for evidence, including witness statements, the defendant's confession, expert opinion and the results of the survey Etc., all the methods of evidence may be translated into the form of the instrument, such as the general permission to read the transcripts of the proceedings, not only the principle of overhead direct trial and the provisions of article 159 the hearsay rule, and even the whole strict rules and the meaning of the trial procedure.<sup>192</sup> However, for the purpose of preserving the evidence and the litigation economy, the exception is permitted to be examined in the form of a written examination of the transcripts of the investigation.

On the original proposed, Taiwan Criminal Procedure Law is not expressly provided, in this reference to the Civil Procedure Law Article 363 provides: "This provision provides that the object outside the instrument and the same utility with the instrument of the prospective use of the instrument or the former items, Technology equipment can always present its contents or make the original in fact difficult, only to present the content of its written and proof of its contents consistent with the original. "In addition, the use of traditional instruments, the practice can be common to the parties Instead of the original proposed, Taiwan Civil Procedure Law Article 352 of this although there are relevant provisions, but the lack of relevant rules and regulations of criminal law. Taiwan criminal procedure law is not as civil procedural law or the United States Federal Act 1002 article "best evidence law" provisions for the proposed text or the text as evidence of the conditions of no clear specification,

---

<sup>192</sup> Yu-Hsiung Lin, *supra* note 154, p.549.

when a party to make an instrument and when the copy is used as evidence and the other party objected, the court's handling may vary from person to person. Because the instruments used in the Code of Criminal Procedure cannot always be put forward, and sometimes the use of books or photocopies necessary, it should be imitated by the United States legislation, the use of the text or the use of the opportunity.<sup>193</sup>

### 3.1.2 Differences between Digital Evidence and Traditional Documentary Evidence

There are three major differences between digital evidence and traditional documentary evidence, including: mass storage, the way of preservation, and the form of presentation.<sup>194</sup> Since social media evidence has the same characteristics as the digital evidence, it also shares these differences.

#### 3.1.2.1 About data storage

It is the biggest difference with traditional documentary evidence that the storage of digital evidence is quite staggering. More than 500,000 pages of text can be stored on average in 1GB storage capacity, and a 500GB hard drive can contain the equivalent of about 250 million pages of text pages. The information is too large, thus it often leads the parties to spend too much time, efforts and money to find the necessary evidence. Using index function seems to be relatively easy, but it seems not precise enough only based on the index as a court to determine whether the digital evidence is "accessible". Because digital evidence has characteristics of "vulnerability" and "recoverability", the information must be collected rigorously and in accordance with certain procedures, to avoid the parties questioned the ability of evidence (admissibility).

---

<sup>193</sup> Hsun-Lung Wu, supra note 190, P.64-65.

<sup>194</sup> Bauccio, Salvatore J., E-Discovery: Why and how e-mail is changing the way trials are won and lost, 45 Duq. L. Rev. 269, 270-271(2007).

### 3.1.2.2 Data preservation

Digital data can be easily deleted or modified, although some of the software and procedures can be used to restore the digital data, but some "anti-forensics"<sup>195</sup> concept, the credibility of the digital evidence will be seriously damaged. Therefore, the focus of digital evidence is not only the "storage" concept, more important, is also must continue to maintain the original content does not change the content.<sup>196</sup> Those who are falsified or annihilated by evidence should have serious criminal penalties and fines. Article 165 in Criminal Code of the Republic of China<sup>197</sup> states, "*A person who forges, alters, destroys, or conceals evidence in the criminal case of another or makes use of such forged or altered evidence shall be sentenced to imprisonment for not more than two years, short-term imprisonment, or a fine of not more than five hundred yuan.*"

### 3.1.2.3 Forms of presentation

Because digital data may be incomplete or difficult to understand, the format of the presentation of digital data is important to the litigants. Digital data has the so-called "metadata or data about data", which does not exist in printed paper, covering a wide range of content, such as the last editor, the last editing time, and even the Privilege protection information.<sup>198</sup>

In addition, the digital data is the "original" type, but because the digital data is presented in the form of 0 and 1, must be through the computer equipment to present its content, so the practice of more paper or identification report of the way, let The

---

<sup>195</sup> The concept of anti-forensics, mainly refers to that forensic practitioners cannot restore the deleted information, for example, some suite of software can be completely deleted data; some anti-forensics behavior even tampered the digital data, resulting in an error in the final judgment.

<sup>196</sup> *supra* note 194, at 276.

<sup>197</sup> Republic of China is Taiwan's official name, rather than the People's Republic of China which indicates China.

<sup>198</sup> *supra* note 194, at 278.

court proceedings in the process of action against its contents of the offensive and defensive, so when the authenticity of the evidence is not controversial, only because of the effectiveness of the instrument or explain the dispute. It may be handled in the light of paragraph 2 of Article 352 in Taiwan Code of Civil Procedure, that is, “*A private document shall be produced in its original copy. Notwithstanding, where only the effect or explanation of such document is disputed, it may be produced in a written copy or photocopy form.*” That is to say, parties can present this digital evidence with the copy or printouts.

### 3.1.3 Investigating Social Media Evidence

Whether the digital evidence should be based on the evidence of the documentary evidence, should consider the presentation of the digital evidence, expressed in the form of digital evidence of the content or the existence of digital evidence, the type of evidence? If the evidence of evidence to evidence of the method of investigation, the first will still first clarify, digital evidence is readable?

#### 3.1.3.1 Social Media Evidence and Nature of Document

The first step is to discuss whether the evidence has the nature of the document and can be considered as documentary evidence. Different scholars have proposed three possibilities.

##### 3.1.3.1.1 Possible1: Social media evidence is considered as the document.

The traditional instrumental information is recorded in the paper on the paper, with the characteristics of reading; and data stored in digital data is a long string of 0 and 1 stored in magnetic media, in order to facilitate the design staff to read, usually The hex code of the hexadecimal representation, whether in 0 or 1 or hexadecimal representation of the internal code, cannot directly determine the contents of the

perception, it is not readable.<sup>199</sup> However, the content of such digital data is readable, only the use of digital data will be the same way the contents of the storage of non-paper storage media, and cannot read directly. The two methods of storage and the media is different, but it has the same function, that is, can record exactly the same content, Moreover, the digital evidence is usually the contents of its representative to illustrate a problem, and must be exported to print to Paper on the formation of written materials, began to be people to read, use, and thus have the characteristics of documentary evidence. That is, the Department of the book can be recorded in its content, and the way to digital data storage. Therefore, as long as the contents of the digital data using the computer's hardware and hardware output, appear on the text to restore the contents of the paper, so that it is readable. So the number of such information should be regarded as general documentary evidence.<sup>200</sup>

Such as non-traditional documents, such as computer programs or web programs, can be computer programs or web programs printed into a report, and then as a general document processing.<sup>201</sup> Such as e-mail content can be a kind of documentary evidence, digital evidence, displayed on the screen or printed out of the electronic file can be called the book card;<sup>202</sup> another example, although the web produced by electronic records, but it is Readability, reproducibility, and so on, so that the sound, image, or symbol appearing by recording, recording, recording, by machine or computer is regarded as an instrument, even if it does not use paper or other tangible material at all, and Not copied to it, without prejudice to its clerical nature, and pages

---

<sup>199</sup> Chen-Jung Tsai & Wei-Ping Chang, Research on Computer Crime Evidence, Criminal Law Journal, Vol. 44, No. 2, P.54.

<sup>200</sup> Hsien-Ming Chiu & I-Long Lin, The Offense and Defense Countermeasures of Digital Evidence in Court, Journal of Information , Technology and Society, Vol. 7, No. 1, 2007, P.55; Chen-Jung Tsai & Wei-Ping Chang, *supra* note 199, P.54.

<sup>201</sup> Chen-Jung Tsai & Wei-Ping Chang, *supra* note 199, P.54.

<sup>202</sup> Shiuh-Jeng Wang, Hung-Jui Ke & ICCL, Information and Network Security: Eyes of Secret –State of the Art on Internet Security and Digital Forensics, DrMaster Press: Taiwan, 2006, P.591.

are often used to transmit information related to the crime, such as sending a threatening letter, defamatory, pornographic images, etc., the establishment of the crime on the Internet, and The traditional crime established by this paper should be different. Taiwan legal practice has the Internet industry to provide e-mail applicant information and log files (log) information, IP address query records, that the Department of documents evidence.

Germany has the doctrine that, if through considerable technological equipment, evidence of evidence within the vehicle, and can get as read the document information, can also be regarded as documentary evidence.<sup>203</sup> Because as long as the information contained in the evidence contained in the human can understand, that is readable, after all, to modern technology and equipment to display information may be driven by the future situation. However, this only shows the readability of its digital data.<sup>204</sup>

3.1.3.1.2 Possible 2: Social media evidence is different from documentary evidence.

Supporters advocate digital evidence non-writers, starts from the point of view that the instrument must be readable. Scholars believe that the document evidence must have the characteristics of readability, take the video evidence as example, if the evidence is contents of the video, the evidence should be investigated in the same way with document evidence. However, in terms of the evidence of the content of the method, the text and readability for all litigation documents on the commonality of the instrument evidence, but the audio and video evidence lack such characteristics, thus it cannot be investigated through reading the written document in the courtroom.<sup>205</sup>

Then from the technical aspects of digital data, digital information is not all

---

<sup>203</sup> Claus Roxin, German Code of Criminal Procedure, trans. Li-Chi Wu, Sanmin publish: Taiwan, 1998, P. 308.

<sup>204</sup> Lai-Jier Her, *supra* note 167, p. 36.

<sup>205</sup> Yu-Hsiung Lin, *supra* note 154, p.550

printed by the paper after the beginning of its content, through the screen and other digital media playback, the same can understand the contents of digital data.<sup>206</sup> So some scholars believe that, it is still necessary to further clarify whether the content of digital data conforms to the concept of traditional documentary evidence in this way. It is not the general text file, but cannot be printed into the information can be printed, only in the implementation or implementation, to understand the meaning of the file And the function, at this time applicable to the identification of the evidence method, identify the identification of the program or file after the results and their results, in words or written report.<sup>207</sup>

#### 3.1.3.1.3 Possible 3: Social media evidence is similar to documentary evidence.

For the purposes of the instrument, Article 363 of Taiwan Code of Civil Procedure can be used as a reference, *“The provisions of this Item shall apply mutatis mutandis to non-documentary objects which operate as documents. Where the content of a document or an object provided in the preceding paragraph is accessible only through technological devices or it is practically difficult to produce its original version, a writing representing its content along with a proof of the content represented as being true to the original will be acceptable. The court may, if necessary, order an explanation of the document, object, or writing representing the content thereof provided in the two preceding paragraphs.”* It directly regulates the method of the investigation using the same way with document evidence.

In the case of criminal cases, whether the evidence of the existence of a document, the early practice of 1992 the 11th Criminal Divisions Conference of the Supreme Court discussed the case that the robbery to obtain other people's ATM card,

---

<sup>206</sup> Hsien-Ming Chiu & I-Long Lin, *supra* note 200, P. 55.

<sup>207</sup> Chen-Jung Tsai & Yue-Ting Huang, *Admissibility of Digital Evidence*, Criminal Law Journal, Vol. 49, No. 2, P.5.

entering the sender's password from the automatic and whether it is the establishment of a criminal law to counterfeit the crime of quasi-private. The resolution states that, electromagnetic record system in the state of continuity, recorded in the tape, disk and other objects on the meaning or concept. Although it is in the form of an invisible positive and negative magnetic gas on it, that is, by the language of such a computer-specific symbol to be expressed, but by the reproduction device to be printed, it can be processed by the machinery as an instrument and regeneration, it can be regarded as the protection of criminal law instruments. But a recent practical opinion thinks it should be a quasi-instrument.<sup>208</sup> In the case of CD-ROM, the resolution states that if the disc has been recorded to store the meaning or thoughts of the intended person, the sound, image or symbol displayed by the processing of the machine or the computer is sufficient to prove that it is intended, according to Article 220 II of the Criminal Law<sup>209</sup>, the digital content shall be treated as a quasi-instrument.

Some scholars<sup>210</sup> share the same view with the practice, for stored in the disk or CD-ROM within the digital data that should be regarded as quasi-instruments. The evidence of the cover certificate is visible and readable, and if it is an invisible object without visibility and readability, it cannot be used as evidence of the instrument. From the computer software with the physical concept, which is tangible; but the digital data itself is not readable, must be written by the computer and the printer after the operation of the written, beginning with readability, that is, there is a nature of documentary, so that the digital evidence is not alone in the disk or CD as evidence, and another printed with the written together as evidence, it has its meaning. Where

---

<sup>208</sup> 2005 the 12<sup>th</sup> Criminal Divisions Conference of the Supreme Court

<sup>209</sup> Article 220 II of Criminal Law, “*So shall be an audio recording, a visual recording, or an electromagnetic recording and the voices, images or symbols that are shown through computer process and are sufficient evidence of intention.*”

<sup>210</sup> Tun-ming Tsai, Criminal evidence law, Wunanbooks: Taiwan, 1997, p. 210-213.

the magnetic disk or optical disc of the digital data is used as evidence, the digital data and the written copies thereof shall be filed in court at the same time for the purpose of investigation, and in this case there shall be two, but usually not For the two independent evidence method, only as a separate evidence method, that is, to disk or CD-ROM as the original, and the printed copy of the book. Therefore, since the use of the evidence as a matter of view, the digital information of the book is higher than the object, so the law can be regarded as quasi-instrument.

The variety of digital evidence is quite diverse, whether it can be used as evidence of the instrument, whether the evidence is readable. Because the evidence of the instrument is read as a prerequisite, and the digital evidence is stored in the digital carrier, it cannot be directly from the appearance of its interpretation of the content, must be through the technology equipment has begun to appear, as the evidence required by the discrepancy does not match The However, the processing of existing instruments, most of the computer and other technical equipment through the typing and storage of file files, such as the complete negation of digital evidence of the clerical, cannot be used in the current society generally use computer processing materials and digital storage of the trend, and digital evidence Are investigated by investigation or identification, may delay or even paralyze the criminal proceedings of the evidence investigation. Therefore, this thesis argues that digital evidence is clerical, cannot be generalized, digital evidence can be divided into computer storage records and computer records, in the computer storage records of the situation, such as the text file storage, it should have a clerical, Such as pictures, still images, sounds, dynamic images, etc., should be based on the evidence or identification of the method of evidence for it.

### 3.1.3.2 Applicable Effect

The Code of Criminal Procedure Article 165-1 paragraph 1 states, “*The provision of the preceding article shall apply mutatis mutandis to other evidential items other than documents which have the same effect as the document.*” In paragraph 2, it says, “*Audio recording, video recording, electronic record or other similar evidential items that can be used as evidence, shall be played, by the presiding judge, with appropriate equipment to reveal the sound, picture, signals, or information to the party, agent, defense attorney, or assistant to identify, or their essential points explained.*” This part has been amended in 2003 and legislators reasoned that, in responding to new types of evidence with the progress and development of modern science and technology, we need to broaden the recognition of document in order to regulate these new types of evidence, such as audiovisual equipment, or computer information which does not be included in the original provisions.<sup>211</sup> They also cited Article 363 I of Taiwan Code of Civil Procedure (TCCP) and Article 306 II of the Japanese Criminal Procedure Law as reference. Thus, “other similar evidential items” may be explained as new type of evidence related to audiovisual equipment, computer information or other scientific technology products. That is, social media evidence which use information circulating with internet technology as evidence, should be also included because of its technical characteristics.

According to the paragraph 2, digital evidence shall be played with appropriate equipment in the courtroom, although legislators seemed to consider these new types of evidence as the quasi-document, which should follow the same investigating procedure with documentary evidence. The consideration of legislators is very practical that these evidential materials cannot be investigated without playing with the appropriate equipment and they should be presented in court in compliance with

---

<sup>211</sup> The minutes of the Legislative Council can be found on this website, <http://lis.ly.gov.tw/lglawc/lglawkm> But it only provides the Chinese version.

the principle of direct trail. However, legislators seem to have misunderstood if this provision really has been amended by reference to Code of Civil Procedure and Japanese Criminal Procedure Law. Since the provisions of Article 363<sup>212</sup> of the Code of Civil Procedure exempt the parties from the obligations of document originally submitted in court, the parties may submit writings only for the purpose of investigation. The purpose of the TCCP 363 is just the opposite of the intention of this paragraph 2 which requires evidence to be displayed in court. Besides, the provision of Japanese Criminal Procedure Law<sup>213</sup> is for the investigation of real evidence, rather than the investigation of document. It is not appropriate for the legislator to invoke the provision as a revised reference.

### 3.1.3.3 Discussion

(1) The legislator referred to the digital evidence as a quasi-instrument, and it was found that it was also misinterpreted by the evidence of the instrument

Digital evidence must rely on certain technology equipment can only show its content, and document evidence is readable, so as long as the trial judge can read directly. Digital evidence of the investigation method is to display the contents of the appropriate equipment rather than read, and some recording, video, electromagnetic recording of the contents of the show in court, may not be read by the presiding judge

---

<sup>212</sup> Article 363 of the Code of Civil Procedure states, "The provisions of this Item shall apply mutatis mutandis to non-documentary objects which operate as documents.

Where the content of a document or an object provided in the preceding paragraph is accessible only through technological devices or it is practically difficult to produce its original version, a writing representing its content along with a proof of the content represented as being true to the original will be acceptable.

The court may, if necessary, order an explanation of the document, object, or writing representing the content thereof provided in the two preceding paragraphs."

<sup>213</sup> Article 306(2) of Code of Criminal Procedure: "When examining material evidence ex officio, the presiding judge shall display the evidence to the persons concerned in the trial or order an associate judge or court clerk to do so." Available at <http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=02&dn=1&yo=criminal&x=14&y=2&ia=03&ky=&page=2>

its content, as long as the parties can identify, It is not appropriate to use a documentary evidence investigation method.

Moreover, some recordings, video recordings, electromagnetic records or other similar exhibits are not necessarily readable, and whether there is any doubt as to whether they can be identified or reported in a visible manner. Evidence of the information on the vehicle, whether in analogy, digital, induction or electromagnetic storage, must be a certain technology equipment to restore the human facial features can understand the information, that is, for recording, video, through the technology equipment to play or open, was informed of its information, such evidence investigation methods, and book evidence of reading aloud, of course, cannot be equal to the view. Therefore, such as recording, video and other evidence of the vehicle collateral instruments, the correct evidence of the investigation method should be the first to show the contents of the evidence of technology equipment, and then by the judge in court read its contents.

(2) Scholars believe that the Criminal Procedure Law Article 165 of the first two of the biggest errors should be recording, video and other evidence of the vehicle, do not distinguish between what the contents of the content, nor to distinguish between the facts of the case, The presiding judge can only do so in the way of the court.

To do so, it may cause litigation delay and waste of resources. More scholars have pointed out that the provisions of Article 165 of the provisions of Article 2 superfluous, legislators do not know the recording, videotapes lack of character and readability of the characteristics of the criminal evidence chapter and the criminal law called the difference between the instruments, and thus possible The misunderstanding of the concept of quasi-clerical material in criminal law, the

standard of the standard of criminal law, which is a completely different purpose of criminal law as a means of criminal proceedings, is obviously a misunderstanding of the strict proof of law, and the provisions of Article 165 of the provisions, The display of the contents of the display should be based on human facial features to explore, such as playing in court, the nature can be interpreted as belonging to the investigation of the evidence method, the new law is mistakenly included in the document evidence method, not enough to take.<sup>214</sup> The In addition, the provisions of this article, the practice may be caused by the delay in the delay of the proceedings, because the provisions of the presiding judge, such as with the use of tapes, videotapes, electromagnetic recording content as a basis for conviction, "should" in court with appropriate equipment The contents of the document, that is, as the book should be read out of the same court, otherwise the evidence investigation is illegal, but because of recording, video, or electromagnetic recording of the recording time is different, if the recording time is more often also asked to play in court, the cost of Time must be considerable, that will cause the delay in the proceedings.

(3) Basically, the display of sound, images, symbols or information by technology equipment shall be classified as evidence of evidence, rather than evidence of evidence.

Because of the recording, video, electromagnetic record is not readable, cannot read the way to read the book card, and the evidence of the survey method, in line with certain statutory conditions, still have to book evidence instead, that is, to read the record instead.

(4) The existing section 165-1 provides that the content of the discriminatory vehicle

---

<sup>214</sup> Yu-Hsiung Lin, Aerial View on 2003 Amendment of the Code of Criminal Procedure, in Yu-Hsiung Lin, Coercive Measure and Criminal Evidence, Angel publish: Taiwan, 2008, p. 461.

is informative and readable.

If the content of the information is readable, such as an electronic document, the presiding judge shall broadcast the contents of the instrument and display it with the technical equipment; if the information is not readable, The sound, the action, the state, etc., can only take the method of investigation evidence, the judge divided by the scientific and technological equipment in court inspection, but also read the record.<sup>215</sup>

In this paper, Article 165 (1) (2) provides that the type of "recording, video, electromagnetic record or other similar exhibits" shall be included in the summary of the evidence of the new form ), The provisions of Article 164 or Article 165 stipulate that the nature of the "video, video, electromagnetic record or other similar exhibits" shall be in the form of documentary evidence and physical evidence. Cover, "recording, recording, electromagnetic recording or other similar exhibits", with its contents as evidence, also with its existence or physical status as evidence, cannot be generalized. Moreover, the investigation of the evidence according to the strict proof of the law, should be based on five kinds of statutory evidence, documentary evidence and evidence of the classification of this way cannot be used as evidence of the basis of evidence, such as evidence of evidence method should be survey or identification, and To identify, identify, or prescribe the purpose of the evidence. Therefore, in the face of the evidence of this new type of evidence, the correct approach should be based on the use of five statutory evidence methods under the existing framework to distinguish between the types of "recordings, videos, electromagnetic records or other similar exhibits" If the digital evidence is readable, it should be investigated by evidence of evidence; if it is not readable, it should be based on the method of

---

<sup>215</sup> Lai-Jier Her, *supra* note 167, p. 38.

investigation; if the digital evidence involves highly specialized knowledge, it should be identified by the appraiser.

### 3.2 Social Media Evidence as Real Evidence

The evidence of the matter is evidence of the state of the object or the presence or the instrument. The nature of the evidence, the object of the body, the body of the body; objects can be divided into two kinds of things and instruments, evidence for the writers, the Department of its existence or state for its evidence, such as the Criminal Code Article 352 The words of the destruction of the instrument of destruction, the obscene words, pictures or other articles of the crime of the indulgence of the indecent articles, and the contents of the documents, as well as the contents of the documents, Of the book-like, slander the reputation of other letters, etc., is also evidence.<sup>216</sup>

Article 164 of this Law provides that "the presiding judge shall inform the parties, agents, defenders or assistants of the exhibits to identify them, and the evidence shall be made to the gist, if the defendant does not understand the meaning of the instrument." Therefore, the means of investigation of the evidence is a reminder, identification or purpose. In the case of evidence of the physical nature of the instrument, the State as evidence, not as evidence of its contents, or in addition to the meaning of its contents, and its physical nature, state as evidence, the instrument also Is evidence of the matter, it will be prompted to the instrument.<sup>217</sup> The evidence investigation procedure shall be unlawful if the defendant is not prompted to warn the list, or only to indicate the evidence but not to identify it, for the inability to secure the exhibits and to prevent the defendant from exercising his defense.<sup>218</sup>

---

<sup>216</sup> Pu-shing Chen, *Criminal Evidence Law*, Vanity press, 1992, P. 77-78 & P.375.

<sup>217</sup> Dung-Shiung Huang, *supra* note 189, P.366.

<sup>218</sup> Hsun-Lung Wu, *supra* note 190, P.60.

However, some scholars believe that evidence is only evidence or its source, instead an independent form of evidence. Taking the knife in a murder case as example, the knife will be investigated through the method of expert witness, if the court send this knife to forensic laboratory; If the court prompts the defendant to identify this knife during the trial, the method of evidence will be an inspection. In addition, playing audio and video in the courtroom, it essentially belongs to the perception of intelligence to identify the evidence method.<sup>219</sup>

Social media evidence as a physical investigation, refers to the need to pass the computer hardware and software equipment to hear, or see the contents of the material evidence,<sup>220</sup> for example, published articles in the face of the reputation of others, or the use of chat rooms to spread children obscene photo. The existence or status of the digital information is the purpose of the investigation of the evidence and shall give the defendant an opportunity to express his opinion and to have a direct connection with the defendant's criminal conduct, in order to clarify the constitution of the court. Whether the defendant is the same as the state of the evidence, and the court shall inform the defendant of the identity of the defendant, and the defendant shall be informed of the purpose of the defendant.

In addition, the data format of the Mp3 computer file, the program file and the files generated during the compilation process, such as the destination file, are not general text files, cannot be printed into a readable file, and printed into a report does not make any sense, Such documents are only in the implementation or implementation to understand the meaning and function of the file, so the nature of this type of file and physical evidence should be evidence of the way to investigate.<sup>221</sup>

---

<sup>219</sup> Yu-Hsiung Lin, *supra* note 154, p.457.

<sup>220</sup> Chen-Jung Tsai & Wei-Ping Chang, *supra* note 199, P.54.

<sup>221</sup> Chen-Jung Tsai & Wei-Ping Chang, *supra* note 199, P.56.

Digital evidence to the evidence of the way to investigate, only from the appearance of evidence to be classified, however, the evidence of the investigation, should still be strictly proved by the law, the legal evidence method. Where the digital evidence is not readable, its physical properties are physical evidence, but in the investigation procedure, the evidence shall be identified by means of evidence or inspection, and Article 164 shall be the physical nature of the evidence, It is not possible to use the evidence as a basis for the referee without prompting in the investigation or identification of the appraiser.

### 3.3 Summon an Expert Witness

Criminal proceedings based on evidence to determine the facts of the crime, then the court summons some of the expertise and experience is limited, it must be with the expertise of people, to supplement the court of professional knowledge and experience of the lack of experience for the purpose of identification. Identification refers to the experience of a person who has a special knowledge, a matter of a statement of its views, as a means of evidence. Judgment for the determination of social things, there is no need to rely on special expertise experience, and only in accordance with the general experience of daily life of society, we can cope with the free, it is not sent to send identification, the court can be judged by the general experience of the law; If it cannot be judged by the experience of the daily life of the general society, it shall be sent to the expert or specialized agency with experience and experience to determine it.

If the evidence of the crime is identified, it is determined by the expert or appraiser of the professional knowledge, but it is different from the task of the judge, and the identification is limited to the evidence of the court, and cannot directly substitute the judge for legal judgment. That is, when the evidence relates to the legal

evaluation, it is still the judge of the trial. At the same time, it is necessary to pay attention to the fact that the identification of the facts of the crime cannot directly restrain the judgment of the judge, and it is decided whether or not it is adopted by the judge. The court will independently examine whether the appraisal opinion is admissible and cannot accept the results of the appraisal without any conditions, and directly as the basis for the referee, the court even if the adoption of the appraisal opinion, still in the reasons for the decision, identification of independent evaluation of the evidence, the higher court before the commencement of the legal review; Similarly, the court does not adopt the judge's judgment, but also in the reasons for the decision that why not take the identification.<sup>222</sup>

### 3.3.1 Internet Forensics

Internet authentication, most of the use of the IP address of the Internet back to the inference, the line may find involved in the crime or the computer. In addition, the computer's digital evidence not only stay in the computer itself, the information will remain in the server, the server to record when the computer connected to which computers, and what requirements, to extract the information. Through the network packet analysis and monitoring software can collect a lot of information, such as time, source, network protocols, etc., through these messages, which computers can be on the Internet browsing history, combined with the case occurred, the location, Suspicious suspects.<sup>223</sup>

Internet authentication sometimes with the network monitoring software used together, such as sniffer<sup>224</sup> way, so that all the flow of packets<sup>225</sup> are complete

---

<sup>222</sup> Yu-Hsiung Lin, *supra* note 154, p.526.

<sup>223</sup> Kun-Lin Lin, Shih-Jeng Wang, Yueh-Hann Chang, Wen-Ya Chiang & Jia-Hong Huang, Unveiling Controversy of Trojan Defense on Internet Forensics, *Criminal Bimonthly*, No. 65, 2008, P.86-89.

<sup>224</sup> Sniffer (network sniffer) is a tool that can intercept, log and sometimes parse traffic passing over a network or part of a network. <http://www.forensicswiki.org/wiki/Sniffer>

<sup>225</sup> A network packet is a formatted unit of data carried by a packet-switched network. When data is

records and copy a copy of the system, the next data will be made to the image file storage Down, and these stored information Some systems will be directly encrypted and re-organized action, the purpose of this action is to ensure that the information will not be changed or deleted in the process, but will not be seen by a third person inside Content, and then the analysis and testing process, but generally there are two kinds of analysis methods, one is to analyze the text, the advantage is simple and can be stored and presented data; the other is the use of visualization Mode, the advantage is that we can use the visualization of the performance of the problem, or the use of visualization of the way, quickly show the information we want to see and analyze. When the analysis system will be placed in the expert system or knowledge base, and by the system for the first comparison to give advice, while adding some interactive ways, such as in the graphics found suspicious events, we can directly click on the graphics connection to know even Line content so that managers can easily trace suspicious events.<sup>226</sup>

Large-scale network authentication tools can even reach a decentralized architecture with front-end collectors collecting network packets, host log files or other information, full-time log files, and back-end for large databases and analysis centers that analyze and present the entire network , And has the functions of analysis log, traffic analysis, communication protocol analysis and packet interception. The method adopts packet interception, packet filtering, communication protocol analysis, data mining, IP search, IP conversion to graphics.<sup>227</sup> However, through the network software tools, although the packet can be recorded, but the daily record of the

---

formatted into packets, and packet switching is employed, the bandwidth of the communication medium can be better shared among users than with circuit switching. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. [https://en.wikipedia.org/wiki/Network\\_packet](https://en.wikipedia.org/wiki/Network_packet)

<sup>226</sup> Bill Lee, Emerging Computer Crime Investigation Technology - Network Forensics, Communication of the CCISA, Vol. 13, No. 1, 2007, P. 181.

<sup>227</sup> *Ibid.*

number of packets is very large, the focus should be on how such information can be found in the evidence to prove the crime. Therefore, the focus of network identification is not in the software tools, but how many packages and information to find suspicious events, this time the focus is to identify the professional and experience.

In the case of online evidence, the practice is often to the ISP or ICP<sup>228</sup> industry to retrieve information, ISP and ICP industry to more than paper to cover, this, the defendant will dispute the contents of the letter is wrong, that the data without evidence or There is not enough proof. If the defendant is only concerned with the correctness of the information provided by the practitioner, the court will not be held in practice. On the other hand, if the dispute raised by the defendant is indeed suspicious, the judge may ask the defendant for the reasons of the defendant's question, or summon the industry to witness the identity of the witness.

### 3.3.2 Necessity of Summoning an Expert Witness

Whether the digital evidence is to be passed through the legal evidence of the identification method, it is necessary to first determine whether the evidence is necessary for identification. The so-called identification of the need to identify the fact that the evidence is evidence of relevance, necessity and the possibility of investigation, then have to deal with the facts of the dispute, whether it is necessary to have a special experience in the special can only answer. If the court does not have the special expertise, the court will elect the identification, which is the necessity of identification, not the court. If the court does not have the special expertise, it can be discretionary.<sup>229</sup>

---

<sup>228</sup> ICP (Internet Content Provider) refers to industry provides a wide range of services on the Internet, such as Yahoo.

<sup>229</sup> Yu-Hsiung Lin, *supra* note 154, p.534.

As the rapid development of digital technology, requiring judges to judge their own knowledge is difficult, so by the authority of the computer identification expert assistance, by their evidence and identification process to confirm, it is more to protect the people's rights and justice Just before the confirmation of the facts of the crime. Therefore, the digital evidence should be carefully dealt with in accordance with the evidence processing procedures, by the experts to copy the evidence or copy the test, and then to each other to be personalized, as evidence of the facts of the crime.<sup>230</sup>

### 3.3.3 Steps of Forensics

The identification of digital evidence refers to the science of the evidence of the computer media and the analysis of its causes in the way of Zhou Yan's method and procedures for preserving, identifying, extracting, recording and interpreting computer media. (1) to obtain prima facie evidence without altering or destroying the exhibits; (2) proving that the evidence obtained is from the evidence of the seizure; and (3) analyzing the evidence without changing the exhibits. The purpose of digital identification is to collect, test and analyze, to preserve the evidence of computer crime, and to collect meaningful information from the computer, or to describe the event from the fragment data to carry out on-site reconstruction.<sup>231</sup>

In order to identify the information and related information of the case, it is necessary to understand the challenge of the case and the way it can take it. The first step is to identify the incident and the event identification. Including the point in time at which the case occurred, the information about the destruction or theft of the attack, the identification of which operating systems, which identification tools to use, and so

---

<sup>230</sup> Shiuh-Jeng Wang, Hung-Jui Ke, Chung-Huang Yang, Discussion on Evidence of Retention of Web Security, *Communations of the CCSI*, Vol.8, No.4, 2002, P.92.

<sup>231</sup> Shiuh-Jeng Wang, Hung-Jui Ke & ICCL, *supra* note 202, P.615.

on.

Second, the digital evidence is easy to add or delete, so it is necessary to preserve the digital evidence, especially the digital evidence is subject to additions and deletions. It will also avoid the deletion of important information due to the accidental process, or the timing of the change of the file at the time of collection. Do the custody of the custody of the management process. In addition, it is necessary to pay attention to the need for computer shutdown, will be careful consideration, because immediately turn off the computer power will cause the memory is running in the program or data loss; boot should also be careful not to use suspicious discs or driver.

Third, after obtaining the digital evidence will test and analyze the digital evidence, the general computer documents, pictures, sound, etc. can use a number of tools to view the software. The best way to use the backup file to identify the backup file backup method should use a special tool for character stream copy (Bit Stream Copy), and the general copy of the biggest difference is that the character stream copy of the copy of the information and the original. The same information is available to prevent the archives from being modified during the backup process when the copies are made identical to other investigators. However, the biggest problem is that the deleted files, in particular, these deleted files are sometimes the most important evidence, at this time to the remaining space in the disk to view, and the use of software for string search and file reconstruction.

Fourthly, after obtaining the evidence and analyzing, it is necessary to analyze and state the case; that is, how to analyze the relationship between the identification result and the suspect, to classify the evidence, to compare with the individual, to determine whether the results can be linked to the suspect People, and infer the behavior of the suspects. Finally, the results of the identification will be presented, it

must be clearly stated that in exploring the source of evidence, causes and the relationship between the suspects, to exclude all possible alternative explanations, to prove that one side interpreted as a single explanation, due to the relationship between evidence and causality Doubt, may be sufficient to affect the defendant's conviction or not.

#### 3.3.4 Report

The opinion of the appraiser is essentially evidence of the opinion, but the opinion is not the subjective opinion of the expert, but the evidence based on the experience of the special knowledge, the ability or the technical examination is still evidence.<sup>232</sup> Article 206 of the Criminal Procedure Law<sup>233</sup> of the identification of the provisions of the provisions of the identification of the identification of people, the identification of the process and its results, should be identified in words or written report. When there are several persons who have identified them, they may be reported together, but those who differ in opinion should make them report individually. The accreditation of the organs is also subject to the reporting obligations.<sup>234</sup>

Therefore, the contents of the identification report not only record the results of the identification, but should be included in the identification of the identification report. If there is no record of the identification, the lack of identification of the statutory requirements, the identification of the report does not have the ability to

---

<sup>232</sup> Dung-Shiung Huang, supra note 189, P.367-368.

<sup>233</sup> Article 206 of the Criminal Procedure Law states, “An expert witness shall be ordered to make a report of his findings and results verbally or in writing. If there are several expert witnesses, they may be ordered to make a joint report, but if their opinions differ, they shall be required to make separate reports. If a report of an expert witness is submitted in writing, he may be required to explain it verbally if necessary.”

<sup>234</sup> Article 208 I of the Criminal Procedure Law states, “A court or public prosecutor may request a hospital, school, or other suitable establishment or group to make an expert examination or to review the examination of another expert witness; also, subject mutatis mutandis to the provisions of Articles 203 through Article 206-1; if a report or explanation should be made verbally, the person who actually made an expert examination or the person who reviewed the examination of another expert witness may be ordered to do it.”

evidence.<sup>235</sup> The identification of the identification, refers to the identification of the choice of information, the use of identification methods and the reasons for the identification of the identification of the identification of the identification of the more detailed description of the identification results more credible, and whether the identification of admissibility, The identification of the elucidation depends not only on the identification of the results. In particular, when there are two opposite opinions on the same identification before and after the same identification, for example, if the identification made to the court is different from the identification made by the prosecution, the different opinions of the different appraisers are what can be adopted, what is not available, there is a need for further investigation. At this time, the court should consider other relevant evidence judgments, in the rules of experience and the law of the rules of their choice, and that the reasons for the judgment of the evidence, if there is still incomplete, according to Article 207, increase the number or increase others continue or otherwise identify.

### 3.3.5 Challenges of Digital Forensics

#### 3.3.5.1 Identity

To use digital evidence as evidence, it is important to ensure that the input and output of the digital data are in accordance with legal procedures. In order to avoid the defendant in order to avoid the truth of the evidence, therefore, the most important first step is to avoid destructive identification, because the digital evidence is easily modified by the addition and deletion of digital evidence. Traditional criminal identification experts can use the fingerprints, trajectories, blood, hair, etc. can be aware of the physical evidence to prove the relationship between the parties involved

---

<sup>235</sup> (94) Tai Shan Zhi No. 7135 Penal Judgment (2005) of the Supreme Court, (94) Tai Shan Zhi No. 6881 Penal Judgment (2005) of the Supreme Court, (93) Tai Shan Zhi No. 6562 Penal Judgment (2004) of the Supreme Court, (92) Tai Shan Zhi No. 2282 Penal Judgment (2003) of the Supreme Court.

in the crime, but the digital identification experts will develop new tools to collect, save, test, extract and evaluation The digital evidence that the naked eye cannot see to understand the intentions, motives, methods and methods of crime, and assess the property damage caused by computer-related crime. Digital evidence is similar to the traditional crime scene evidence, but its unique storage methods and easy to modify the characteristics of the search work and related evidence to save, transport, processing, analysis and other work, more complex than the traditional criminal identification work.<sup>236</sup>

Based on the characteristics of digital evidence and the difference with the traditional identification, before the identification of digital evidence, the first must avoid destructive identification. The so-called destructive identification, refers to the identification of digital evidence in the process, may be due to improper access to digital evidence damage. Because digital evidence is different from the traditional identification system for the identification of entities, which is not an entity and easy to modify, so at the beginning of the collection of digital evidence, it may cause damage to the digital evidence, for example, in the digital evidence storage time point as a proof of crime of the situation, the collection of the evidence due to improper access, resulting in digital data storage time changes, so that the evidence cannot be used as evidence of the evidence. Therefore, the identification of the evidence investigation method must comply with the legitimate procedures, can use the relevant computer tools to obtain digital evidence after identification. First of all, in the collection of digital evidence, in order not to change the case of digital evidence of the case of identification, it must consider whether the digital data can be backed up, and then to identify the backup data to ensure the integrity of the evidence, therefore,

---

<sup>236</sup> Jau-Hwang Wang, Forensics and Collection of Digital Evidence, Police Science Bimonthly, Vol. 34, No. 3, 2003, P. 135.

before the identification we should get the backup file first.

There are two ways to backup, the first for the pure data backup, this backup is mainly for the directory and file; the other for the mirror backup, that is, all the hard disk information, including hidden system data (the most common is Delete the file) all the backup in another new hard disk, if the cost allows, mirror backup of course, much better than the data backup. On this point in the practice of digital evidence identification can use the relevant hardware and software (such as Drive Image,<sup>237</sup> etc.) for the backup work, analysis is not directly against the original evidence, but the use of backup data to investigate.<sup>238</sup> When creating a backup file, it is necessary to copy the characters in a way that is different from the general copy. The general copy of the way, Ambient Data (Ambient Data) will not be copied to the new media. For example, the original data of the disk is A, B, C (deleted), D (deleted), E file, the general copy of the results of the information for the A, B, E file, character stream copy results were A, B, C (deleted), D (deleted), E file, that is, through the character stream copy mode, backup data and raw data the same, not just the same file, disk status should be the same, so not only To prove the same, can also use this method to search whether the disk has been deleted important evidence.<sup>239</sup>

Second, to prove that the captured data from the seizure of the evidence, the use of MD5<sup>240</sup> on the function of this operation proved that the two different content files using this function after the operation, resulting in the same probability of the hash

---

<sup>237</sup> Drive Image refers to creating an image on the original fixed or removable hard disk, magnetic field. An image here is storing the disk content and related information into a file, aka the image file. *see* Shiu-Jeng Wang, Hung-Jui Ke & ICCL, *supra* note 202, P.621.

<sup>238</sup> Ming-Feng Tsai, Explore the True Nature of Computer Forensics, *Criminal Bimonthly*, No. 4, 2005, P. 22.

<sup>239</sup> Shiu-Jeng Wang, Hung-Jui Ke & ICCL, *supra* note 202, P.622.

<sup>240</sup> MD5 is one of the Hash functions in cryptography. The hash value produced by MD5 operation is extremely reproducible. We will discuss further in Chapter 3; also *see* Shiu-Jeng Wang, Hung-Jui Ke & ICCL, *supra* note 202, P.624.

value<sup>241</sup> of 1/2128, So in the field of digital evidence identification, are mainly used to determine whether the original content has not been tampered with.<sup>242</sup>

As for the analysis of digital evidence, because the folder and file stored in the disk, due to system design considerations, even if it is deleted, the actual information still exists, but the file header with an identification code to delete the file, if the deleted information can be found, that may find important evidence, but if each storage media are data reduction, will spend a lot of time, and may not be able to find the necessary evidence, we will use the tool software for analysis and string search to confirm the need for restoring information.<sup>243</sup> Therefore, the analysis usually requires the use of related software tools, such as authentication and analysis software, file restoration software, disk view software, integrity verification software, keyword search software, password cracking software, anti-write tool software. It is noteworthy that commercial software should be used as far as possible; do not use private customization software to avoid being questioned by destructive identification.<sup>244</sup> In the identification, there are a variety of tools and software can be used, it can also be directly through the integration of tools for identification, such as Encase software, this software is equivalent to a combination of disk view, edit, string search tool, file view, verification and data recovery Tools, and can build disk information into a report.<sup>245</sup>

In order to avoid damage to digital evidence, the appraiser should avoid direct identification on the original data storage device, which is the data storage device

---

<sup>241</sup> A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. [https://en.wikipedia.org/wiki/Hash\\_function](https://en.wikipedia.org/wiki/Hash_function)

<sup>242</sup> Ming-Feng Tsai, supra note 238, P.22.

<sup>243</sup> Shiuh-Jeng Wang, Hung-Jui Ke & ICCL, supra note 202, P.631.

<sup>244</sup> Ming-Feng Tsai, supra note 238, P.23.

<sup>245</sup> Shiuh-Jeng Wang, Hung-Jui Ke & ICCL, supra note 202, P.632.

should be backed up before the backup, and then the backup data or hard disk Identification analysis. In fact, when the digital evidence analysis, because of time, cost and concept of immaturity and other factors, few of the backup, but the foreign judicial police in the identification of digital evidence, or even make four copies of a copy by the experts to identify, One for use in court, and two for the purpose of providing direct advice to the Prosecutor or the defense of the defendant.<sup>246</sup>

### 3.3.5.2 Tampering

Because the digital evidence is easily modified by the feature, and even after being tampered with, only from the appearance of difficult to identify, so in practice the defendant often argues that the evidence may have been tampered, and the evidence is not true and should not be admissible..

Taiwanese practice thinks that the digital evidence has been tampering with the idea, such as computer generated information, such as computer log file log information, because of its record with mechanical, regular, uninterrupted characteristics. The network IP address is not the average person can be learned, thus it is difficult to tamper with the computer record file, and it should be recognized as true.<sup>247</sup> And the defendant, if the defendant is to be tampered with the evidence, the court does not accept the defendant's defense, and that the digital evidence still Have evidence of ability.<sup>248</sup>

### 3.3.5.3 Reliability

American computer expert Michael Allison said, we can prove that a computer has been in the Trojan horse backdoor, but if the evidence as a court, but still not so

---

<sup>246</sup> Ralph D. Clifford, *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, California Academic Press, p. 105-107(2001).

<sup>247</sup> (95) Shan Yi Zhi No. 255 Penal Judgment (2006) of Taiwan High Court.

<sup>248</sup> (91) Su Zhi No. 1028 Penal Judgment (2002) of Taiwan Banqiao District Court.

sure, this is not a technical or method of the problem, but in an unreliable operating system, it is difficult for any user data or audit file to be used as a reliable and sufficient evidence for court judgment.<sup>249</sup> Computer software programs often appear BUG, need to constantly update the software, debugging, and computer programs written by people, the results can be controlled by the program designer cannot rule out the results of computer calculus for the user deliberately under the control of the results.<sup>250</sup>

However, when the defendant defended the reliability of the digital evidence program, the majority of US substantive judgments that the computer program is reliable or not, should the original user is really the program used in general routine transactions, such as general business activities, if the computer program engaged in business activities, is sufficient to confirm its reliability. The scholars agree with the opinion of the US courts, and in particular the number of IP records logged in to the defendant, regardless of whether the defendant uses a fixed IP or floating IP, the possibility of a program record error is extremely low.<sup>251</sup> However, if only one IP record points to the defendant, And the defendant is using floating IP, the prosecutor should reinforce the other evidence, or more in-depth investigation of the IP record is correct, cover the network server and the computer's time is not fully synchronized, in a few cases, a little bit of time difference May cause the floating IP system used by others, the practice has even occurred when dealing with information, in the conversion file format error, resulting in the court to check the IP completely wrong situation,<sup>252</sup> it should be careful to verify.

---

<sup>249</sup> Po-Jen Cheng & Chin-Chien Yu, Rethink on "Trojan horse case", *Communations of the CCSI*, Vol. 10, No. 1, 2004, P.143-144.

<sup>250</sup> Hsien-Ming Chiu & I-Long Lin, *supra* note 200, P. 59.

<sup>251</sup> (98) Shan Yi Zhi No. 1757 Penal Judgment (2009) of Taiwan High Court.

<sup>252</sup> (94) Yi Zhi No. 762 Penal Judgment (2005) of Taiwan Tainan District Court.

#### 3.3.5.4 Authorship

Digital evidence is not easy to personalize the characteristics, in particular, online evidence is often anonymous, may occur in the case of the evidence may be non-defendant of the situation, this is also a common defense of the defendant. Therefore, we must first determine the producer of the digital evidence. In general, when investigating the digital evidence, the data is stored in that evidence vehicle and the owner of the vehicle or the user is investigated. However, in some cases, even if the defendant is the owner of the vehicle or the sole user, it cannot prove that the information is produced by the defendant. For example, the prosecution will be suspected of distributing malicious programs on the Internet suspects computer hard drive to the professional identification of personnel analysis, and later proposed the computer hard disk with the identification of the criminal file results, this time still need to pay attention to the source of the evidence Questions, such as backdoor programs, wireless networks, cache files, and purchases of second-hand products. In particular, most people use the computer, often infected by the virus, such as a Trojan invasion or zombie program. Trojan defense related issues will be discussed in Chapter 6.

#### 3.4 Make an Inspection

In the case of digital evidence, the evidence is examined. That is, if the judge in court to the appropriate technical equipment to show the contents of the evidence, the judge, the Department of science and technology equipment to assist its hearing, visual and evidence of the contents of the vehicle can be interpreted as an investigation.<sup>253</sup>

---

<sup>253</sup> Lai-Jier Her, *supra* note 167, p. 36.

### 3.4.1 The Rule

An inspection means a method of investigation by means of sensory perception, such as viewing, touch, etc., of evidence or crime, such as place, person, object, etc. The inspection shall include the investigation of the place of the crime or other places of interest, the examination of the body, the examination of the body, the dissection of the body, the examination of the matter in relation to the case, or other necessary disposition.<sup>254</sup>

Article 212 of the Criminal Procedure Law provides, “A court or public prosecutor may make an inspection in order to investigate the evidence or circumstances of an offense.” On the basis of this, the judge is a judge, a judge or a prosecutor to investigate evidence of one of the powers, the trial by the judge, the investigation by the prosecutor, the clerk, judge assistant<sup>255</sup> have no such authority.

The main body of the investigation is a judge or a prosecutor. As for the judicial police officers have the right to implement the investigation, the views of scholars inconsistent. There is that the Act stipulates that the judge or the prosecutor is to carry out the investigation, the investigation is the legal authority of the judge and the prosecutor, from the non-judicial police officer to the judge or the prosecutor commissioned by the Registrar or the judicial police on behalf of The investigation, or only by the forensic physician for the autopsy of the autopsy, etc., since the non-legal investigation, but the investigation report, is still a reference for the referee, the doctor's report should be regarded as identification report; That the judicial police officers for the investigation of the necessity of crime, cannot be said that it is not for

---

<sup>254</sup> Article 213 states, “An inspection may include the following measures: (1) Examining the place of the offense or other place connected therewith; (2) Physically examining a person; (3) Examining a corpse; (4) Conducting an autopsy; (5) Examining property connected with the case; (6) Performing other necessary measures.”

<sup>255</sup> (95) Tai Shan Zhi No. 2342 Penal Judgment (2006) of the Supreme Court.

the investigation, but the judicial police officers do not have the right to punish, so the investigation, not forced to do so.<sup>256</sup>

The judge or the prosecutor after the investigation to make the transcripts, at the trial date, the court prompts, read the survey record of the way to investigate, but because the other judges of the collegial panel did not personally inquire, and the survey records for the original inspection Evidence method derived from the evidence of alternatives, involving the principle of direct trial. In Germany, the court in principle prohibits the reading of the transcripts, but in particular the permission to read the transcripts of the investigation, there are two reasons, one is to take evidence of the preservation of evidence, if not immediately investigation, will most likely lose the evidence; the other for the litigation economy In order to avoid the derogation of the rights of the parties, the legislator to make up for the right to the trial of the principle of direct trial, as in the trial proceedings, the litigation participants to travel far away from the crime scene is often too much trouble or expensive, cause a violation.<sup>257</sup>

#### 3.4.2 Still Images/Photos

Traditional photos are due to the original scene, through the camera composed of the camera lens, by the photographer press the shutter, the original scene that is reflected by the light to the reflective film, and then by the flushing process of the film or paper. And now the use of digital cameras more and more common, has gradually replaced the traditional camera, in criminal practice, for the use of digital cameras and the frequency is also getting higher and higher, especially digital cameras have been widely used in traffic accident handling crime scene jobs. Digital cameras

---

<sup>256</sup> Dung-Shiung Huang, *supra* note 189, P.260.

<sup>257</sup> Yu-Hsiung Lin, *supra* note 154, p.540.

and the traditional camera is the biggest difference between the digital camera or digital camera back is CCD or CMOS instead of silver halide film exposure technology, and CCD or CMOS is basically millions or even tens of millions of tiny electronic units Composition, when we press the camera shutter, the lens is to follow the general pattern of the traditional camera to reflect the light projection and focus on the CCD, CCD at this time under the exposure of different levels of light, the light will be converted into electronic signals, and pass To the rear of the processor to produce a digital image of the file. The digital camera records or stores the image in two ways, save it to a memory card and transfer it to a PC via a USB connection or card reader, or connect the camera directly to the computer directly via IEEE1394 or USB ( To large digital machine back or network type digital camera-based). These images can be displayed on the screen using the computer software or directly on the back of the digital camera TFTLCD LCD screen.<sup>258</sup>

In the preservation of digital images, the proposed storage media are: 35mm film, can only burn a disc, such as CD-R or DVD-R, etc., the reason is that the quality of these media, reliability, durability is better , For the current use of such as SM, CF and other magnetic cards or other magnetic media, there is the possibility of material damage, will be careful to prevent and avoid data damage, as such as inkjet printers, sublimation transfer Machine, laser printer, or photocopier is not recommended as a way to save the original image. In addition, in the image processing process, in order to ensure the integrity of the image and the process has not been changed the situation, so some of the processing steps for the record, as other does not affect the image integrity of the treatment, such as brightness adjustment, etc. The main purpose of the record is that the main purpose of the record is to reproduce the entire process by

---

<sup>258</sup> Hung-Chang Chang, Discussion on the Application of Digital Image Evidence, Criminal Bimonthly, No. 57, 2004, P.100.

others and to achieve the same result, so that the process can be evaluated and reviewed.<sup>259</sup>

Taiwanese practice for the investigation of the photo, is to understand the content of his facial senses, so the evidence of the expedition method.<sup>260</sup> In the case of digital photographs, digital images, the way in which they record or store images is different from that of traditional photographs, but as evidence, the images are used to prove the facts of the evidence, that is, by the judge, the prosecutor, Image content. As a result, digital photographs are printed or displayed on appropriate equipment as if they were to be washed with traditional photographs,<sup>261</sup> should be investigated by means of evidence. If the parties have doubts about the authenticity of digital photographs and figures that may be related to forgery or alteration, the non-judge can understand the facial senses, and whether the digital images are forged or altered create the situation, it should be identified by the identification, that is, to identify the evidence method of investigation.<sup>262</sup>

### 3.4.3 Voice Recording

Sound storage methods, the traditional way of storage to tape recorders stored in the tape, but with the digital technology equipment, such as recording pen, mobile phones, digital cameras, Walkman, etc., are provided with recording function, and the computer can also through the surrounding Expansion of equipment such as microphones, Internet telephony and other equipment can also be used for recording purposes, and if the digital recording of the sound, the file can be moved or copied

---

<sup>259</sup> Hung-Chang Chang, *supra* note 258, P. 101-102.

<sup>260</sup> (95) Tai Shan Zhi No.4195 Penal Judgment (2006) of the Supreme Court.

<sup>261</sup> (97) Shan Yi Zhi No. 1417 Penal Judgment (2008) of Taiwan High Court, (95) Yi Zhi No. 166 Penal Judgment (2006) of Taiwan Taipei District Court.

<sup>262</sup> (98) Tai Shan Zhi No. 4868 Penal Judgment (2009) of the Supreme Court, (97) Tai Shan Zhi No. 6251 Penal Judgment (2008) of the Supreme Court.

stored in a variety of digital vehicles. The contents of the recording as evidence, regardless of the tape or digital sound files, can not only by the appearance of its contents, tapes by the tape recorder or audio, and digital sound file 預 by computer and other technology equipment, Know its content. Therefore, the discussion of the method of investigating sound archival (recording) evidence can also be used as a reference for investigating digital sound files.

Scholars to tape evidence, for example, that the way to explore the meaning of the contents of the tape, it should be the investigation, that is, the court should be in the investigation of the program in court to play the tape, with facial features to explore the contents of its hidden, and this evidence investigation method is lawful.<sup>263</sup> The evidence of the practice of the tape in our country is also considered as evidence of the investigation, for example, (79) Tai Shan Zhi No. 4891 Penal Judgment (1990) of the Supreme Court, which has been practiced in the trial period. However, the appellant If the contents of the tapes are in conflict with the facts, and there is an important relationship between them, and they are not difficult to investigate or cannot be investigated, the procedure of "playing" is for the sake of clarity.

After the implementation of Article 165-1 of the Criminal Procedure Law, the practice has not changed this view, such as (93) Tai Shan Zhi No. 2263 Penal Judgment (2004) of the Supreme Court, for the investigation of the legitimate monitoring of the recording, that the defendant or litigation for the monitor recording. The court shall, in accordance with article 165-1 II of the Criminal Procedure Law, examine the procedure for investigating the evidence of the investigation of the surveillance and shall not follow the procedure of the hearing The basis of the defendant's guilt. The Supreme Court has made it clear that Article 165-1 is the

---

<sup>263</sup> Yu-Hsiung Lin, *supra* note 154, p.550.

inspection of the provisions of the survey, scholars also agree with the view, monitor the tape in terms of playback, because the contents of the tape is not meaning, readability, it is not a document evidence. If the court wants to proof this evidence by itself, it should make an inspection and play this evidence at court.<sup>264</sup>

The sound file is stored in digital form, and it is considered that it should be investigated by means of the evidence of the investigation and produced into an inspection record, such as live recordings recorded in a recording pen,<sup>265</sup> live recording disc<sup>266</sup>, alarm recording disc<sup>267</sup>, etc., by a judge or a prosecutor investigating the contents of the evidence of the investigation method. Therefore, the sound file (recording) is based on the investigation of the evidence method.

The investigation shall be carried out in accordance with the evidence investigation method of the survey, that is, the judge or the prosecutor shall carry out the investigation and shall be present by the parties and the defense to protect their presence. If a disco on is recorded by a judge's assistant, the contents of the CD-ROM are translated into the contents of the CD-ROM, nor are the persons surveyed, nor have they made the transcripts of the survey, not informing the parties and the defendants of the scene of the derived evidence, the evidence investigation procedure that is not appropriate.<sup>268</sup>

#### 3.4.4 Motion Pictures / Video

Dynamic video recording is the video, the traditional way of storage for the video, but now generally used in digital cameras, digital cameras, etc. are digital storage of dynamic image files, and the computer through the video camera, can also

---

<sup>264</sup> Lai-Jier Her, *supra* note 167, p. 37.

<sup>265</sup> (95) Shan Yi Zhi No. 1674 Penal Judgment (2006) of Taiwan High Court.

<sup>266</sup> (98) Tai Shan Zhi No. 5000 Penal Judgment (2009) of the Supreme Court.

<sup>267</sup> (97) Tai Shan Zhi No. 2047 Penal Judgment (2008) of the Supreme Court.

<sup>268</sup> (97) Tai Shan Zhi No. 6667 Penal Judgment (2008) of the Supreme Court.

be dynamic images To be stored. Although videotapes and digital video files are stored in a different way, their evidence and methods of investigation in criminal proceedings cannot be known through the appearance of videotapes or digital carriers. Therefore, the discussion of traditional video evidence can also be applied to digital dynamic image of the evidence method. Videotape is the use of cameras, the specific original scene or picture into an electronic signal, through the magnetic head to produce magnetic lines, and magnetize the particles on the video tape, its signal remains on the tape, when the picture to make the scene, only the tape through The head, which produces the same signal, can be generated from the same screen as the original recording. The videotaped evidence is based on the motion image of the projector on the screen as evidence, such as the picture of the stillness of the picture, but the continuity of the image flow, the observation of the facts, By the memory of the regeneration, and the fact that the situation again demonstrated, so with the witnesses of the confession has a very similar character, so in the litigation practice evidence that there is irresistible charm.<sup>269</sup>

In practice, such as the evidence to monitor the video as evidence, the early judgments such as (80) Tai Shan Zhi No. 4672 Penal Judgment (1991) of the Supreme Court, “Financial institutions to prevent crime, install the video recorder to monitor the use of automatic teller machines, the video The admission of the screen, depends on the mechanical force shot, without human operation, not subject to the subjective views, including their own evidence of the ability to court as evidence, that is, the presence or form of the video evidence , The method of investigating the evidence shall, in accordance with the provisions of section 164 of the Code of Criminal Procedure, prompt the videotape to be identified by the defendant; if the picture taken

---

<sup>269</sup> Li-Ching Chang, On Admissibility of Photo and Video Evidence, *The Military Law Journal*, Vol. 33, No. 12, P.22 & P. 24.

by the videotape is evidence, the proceedings shall be made by the prosecutor or the court. The court shall investigate the evidence and, if it has been in accordance with the provisions of Article 165 I, the contents of the transcript shall be read or addressed to the defendant, that is, if the record is made.” This case will be divided into video tape to the presence of video, type of evidence or to take the picture as evidence, such as the admission of the screen as evidence, should be investigated in the way of investigation. The point should pay attention to those who, although made after the transcripts, the way to document the investigation of the investigation record, but still should be the legal implementation of the investigation procedure as a prerequisite. After the court to monitor the video screen as evidence, also that the inspection should be the way to investigate evidence.<sup>270</sup>

When practically using digital motion as evidence, most of the dynamic video files are stored in the disc after the court, such video discs, including live video discs<sup>271</sup>, police alarm records recorded<sup>272</sup>, the court also to the investigation of the Evidence method to investigate the contents of the disc. In addition, for example, the report screen of the media, such as the way of CD-ROM, video recording methods, the Department of the Department of inspection discs to whom the way.<sup>273</sup>

And the implementation of the investigation, it is necessary to investigate the evidence according to the investigation method. The implementation of the investigation, only the narrow court or the prosecutor had the right to implement this investigation, the law did not give the judicial police (officer) have to implement the investigation to obtain evidence of authority. Judicial police (officer) made

---

<sup>270</sup> (97) Shan Yi Zhi No. 341 Penal Judgment (2008) of Kaohsiung Branch, Taiwan High Court, (98) Shan Zhong Su Zhi No. 27 Penal Judgment (2009) of Kaohsiung Branch, Taiwan High Court, (90) Shan Su Zhi No. 3559 Penal Judgment (2001) of Kaohsiung Branch, Taiwan High Court.

<sup>271</sup> (98) Tai Shan Zhi No. 4961 Penal Judgment (2009) of the Supreme Court.

<sup>272</sup> (98) Tai Shan Zhi No. 4209 Penal Judgment (2009) of the Supreme Court.

<sup>273</sup> (98) Yi Zhi No. 547 Penal Judgment (2009) of Taiwan Taipei District Court.

"inspection process video disc", because the judicial police (officer) does not have the means to implement such evidence of the basic authority, and "survey record" is evidence of lack of evidence. Article 165-1 II of the Criminal Procedure Law states that *"Audio recording, video recording, electronic record or other similar evidential items that can be used as evidence, shall be played, by the presiding judge, with appropriate equipment to reveal the sound, picture, signals, or information to the party, agent, defense attorney, or assistant to identify, or their essential points explained."* If the search video disc is to be used as evidence, it shall be practiced on the day of trial to display the sound, image and make the parties, agents, defenders or the auxiliary person to identify or to the gist of the investigation of evidence procedures, the beginning of the law.<sup>274</sup>

### 3.5 Discussion

#### 3.5.1 Substitution among Evidence Methods

When investigating social media evidence, applications of these five evidence methods will depend on what is the matter of the judge's desire to prove such information in principle. But the evidence is not entirely irreplaceable, in exceptional circumstances, such as the inability to obtain prima facie evidence; the judge also has other evidence to replace the original evidence method.<sup>275</sup>

##### 3.5.1.1 Forensics and inspection

When to use forensics? When to make an inspection? The practice that the inspection and forensics are in the evidence after the results of the inspection or forensics results, respectively, with a transcript or appraisal report submitted to the court. The distinction between the two is the extent to which the implementer is

---

<sup>274</sup> (97) Tai Shan Zhi No. 1357 Penal Judgment (2008) of the Supreme Court.

<sup>275</sup> Lai-Jier Her, *supra* note 167, p. 35.

required to make judgments and the need for special expertise. In the actual operation of the words, the inspection of the formation of the results of the survey, its display, the evidence obtained, or cannot help but subject to the subjective judgment of the request. Inspection and forensics of the same method for the investigation of evidence, whether the implementation of the inspection, or whether the forensics, and whether the voice of the person should be the intention, and for this punishment, the court inherently discretionary circumstances free to decide the right. However, if the evidence proves that there is an important relationship between the facts to be confirmed, the parties have argued for the result of the investigation, and the inquisitor cannot distinguish between the authenticities. The forensics of the expertise and the identification of the person shall be determined by the person who is capable of investigating the evidence. Otherwise, it is difficult to investigate the contrary to the evidence of the investigation. In the case of evidence to be confirmed by the investigation of the evidence method is still unclear, and by the expertise of the forensics of further professional forensics of the necessary, the Supreme Court that should be further identified, this approach is worthy of recognition. However, the subject of the inspection is the court or the prosecutor, other agencies such as the investigation of the Ministry of Justice investigation, whether it can be identified as an inspection, there are still questions.<sup>276</sup>

Practice for the photo, image of the investigation, the first evidence of the investigation method, but if the parties to the digital image of the real question, then involved in professional knowledge, and photos, images with or without forging, alteration of the situation, it is difficult by the judge to facial features Perception of understanding, this time can be identified by the professional identification of people.

---

<sup>276</sup> (96) Tai Shan Zhi No. 2724 Penal Judgment (2007) of the Supreme Court.

For example, in the case of evidence as evidence, as the Taipei City Government Works Bureau Construction Management Office illegal removal of the defendant, suspected of computer synthesis, the transformation of the photo as a violation of the removal of the contents of the report, The Ministry of Justice Bureau of Investigation Bureau to high magnification view, and then FUJIFinePix S2-Pro monocular digital camera remake, than to look at the details of the image of the photo, comprehensive study, the "photo in the placard demolition of personnel images, in addition to placards contained in the figures There is the difference between the words, the same clothes, and the height of the placards are exactly the same, the neck exposed part of the shape and size are exactly the same, the abdomen by the sunlight to produce bright spot shape, the size of almost uniform, significant unreasonable light and shadow phenomenon; and its characters The use of computer graphics editing software frame selected pattern of residual unreasonable edge lines, judged from the same image screen, the box selected, copied to different digital photos in the results of synthetic transformation "and other reasons, after forensic identified case report Attached to the demolition of the demolition of the scene after the photos were edited by computer graphics editing software, for altered by.<sup>277</sup> For video discs, it is usually the first to investigate the evidence, but if the video discs are likely to be altered, they should be sent by the appraiser.<sup>278</sup>

In addition, the court for the shooting of digital images such as unrecognizable, such as poor resolution, the first through the identification, and the use of computer software to enlarge the digital image analysis and processing, after amplification, analysis of the digital image, according to the inspection method of evidence.<sup>279</sup>

---

<sup>277</sup> (98) Shan Su Zhi No. 1423 Penal Judgment (2009) of the Supreme Court.

<sup>278</sup> (97) Shan Yi Zhi No. 341 Penal Judgment (2008) of Kaohsiung Branch, Taiwan High Court.

<sup>279</sup> (95) Jiao Shan Su Zhi No. 2711 Penal Judgment (2008) of Taichung Branch, Taiwan High Court

### 3.5.1.2 Documentary evidence and investigation

The difference between a book certificate and an investigation can be made from a human understanding point of view. The documentary evidence emphasizes readability, and the so-called readability means that the data can be presented in a textual way, and that the text has an understandable meaning, to understand the ideological content contained in the instrument; the principle of investigation is based on scientific knowledge, logical reasoning, rule of thumb, etc., to push things of reason. If the content shown in the digital information is not a letter and a sign, it is also regarded as a quasi-instrument and is helpless and readable. At this time, the judge continues to use the other reasoning to judge his intention. In this case, it should be closer to the evidence of inspection.<sup>280</sup> In addition, the instrument is more in line with the direct trial, and the investigation is often a direct case of the exception.<sup>281</sup> As a result of the fact that the state of the crime scene cannot be presented to the court, the legislator had to allow the investigating authority to first consult the first time for the investigation. In this way, because the non-judge's own investigation, in principle, is contrary to the principle of direct trial, but if not so, fear will paralyze the judge's trial process, so the legislator had to specifically allow, as a direct trial exception. In the case of a judge, if the judge confirms that the evidence is evidence of the evidence of the documentary evidence, it shall be read or made with the appropriate equipment. If it is recognized as the method of finding the evidence, it shall simply read in advance the inspection record Yes, it is clear that the investigation is more in line with the lawsuit promptly but is detrimental to the direct trial.<sup>282</sup>

Sometimes, when investigating the digital evidence may use two kinds of

---

<sup>280</sup> Lai-Jier Her, *supra* note 167, p. 36.

<sup>281</sup> Yu-Hsiung Lin, *supra* note 154, p.549.

<sup>282</sup> Lai-Jier Her, *supra* note 167, p. 36-37.

evidence at the same time, the evidence is the same as the instrument, and the defendant does not understand its meaning, should be the main purpose, and to the purpose of reading a kind, is the documentary evidence of the investigation method, When the evidence is an instrument, the court may simultaneously use the two methods of evidence (inspection) and the purpose of the investigation (read aloud) at the same time when the court investigates the procedure for the investigation of evidence.<sup>283</sup> In addition, as digital data can be compressed by the vast amount of information, making it the most commonly used way to store information, and if necessary, it can be printed as a written, in this case, if the digital data In the case of evidence, not only should the computer software be presented, nor should it be printed in writing for the investigation or investigation of the court.<sup>284</sup>

### 3.5.1.3 Summary

The investigation of the digital evidence must be in accordance with the strict proof of the law, that is, the method of investigating the evidence of the evidence should be based on five statutory evidence and evidence investigation procedures. However, the legal evidence method is not completely fixed, digital evidence to computer and other technology equipment appears or output, such as sensory perception, it should be the evidence of the investigation method, however, such as digital evidence involving a high degree of technical and professional , For example, if the defendant's defense evidence may be falsified or altered, it cannot be judged by the appearance of the digital evidence, and whether or not there is a counterfeit change investigation, that is, the judge can directly understand the senses, Evidence is sent by an expert who has specialized knowledge and technology. In addition, although the digital evidence is printed or otherwise exported, it is possible to read the

---

<sup>283</sup> Yu-Hsiung Lin, *supra* note 154, p.545.

<sup>284</sup> Tun-ming Tsai, *supra* note 210, P. 210.

way, but sometimes the evidence is an instrument file, but some archival information cannot be printed in a way that is printed, for example, the date of establishment of the document, the date of modification And other information can be displayed on the screen through technical equipment such as computers, by the judge or the prosecutor to investigate the evidence of the investigation method.

### 3.5.2 Social Media Evidence Used as an Independent Evidence Type?

As evidence of the new type of evidence, there are digital evidence should belong to the evidence or documentary evidence of the dispute; evidence method, there are also said that the book or book card that different views. Therefore, for the investigation of digital evidence, some scholars advocate should belong to another type of new evidence method can only be in response to the particularity of digital evidence. This argues that the digital evidence should be a new type of evidence, because the digital evidence has two characteristics, one for the digital evidence to the stored information to prove the fact that the evidence, the other for the digital evidence in binary form Stored in the storage medium, the former to make digital evidence with some of the characteristics of documentary evidence, but the latter makes the digital evidence is different from all the types of evidence. Once the data is digitized, we can use the computer to edit, modify, and not have other evidence of relatively stable and reliable features. Therefore, it is necessary to add evidence of new types in the Code of Criminal Procedure in order to avoid concurrence of the attribution of the nature of the digital evidence and whether there is a unified view of the evidence of the evidence.<sup>285</sup>

In specific cases, the role of digital data to prove the role has been different, which directly affect the evidence of the nature of the evidence and evidence of the

---

<sup>285</sup> Hsien-Ming Chiu & I-Long Lin, *supra* note 200, P. 55.

way, because the digital data by the computer after the presentation of the type of numerous, in the litigation The status of the law is all-encompassing, so the court to investigate, often occurs fuzzy evidence investigation method of the situation, which reflects the digital data to re-locate the evidence of the necessary attributes of the method. Therefore, it is necessary to amend the digital data as a separate method of evidence of the new species, and in the Criminal Procedure Evidence chapter set a separate evidence section.<sup>286</sup>

In the case of recording evidence, the recording itself may be considered evidence, but the translation of the recorded content may also be considered as a documentary evidence, the witness or the confession of the defendant may also be considered a witness, it is difficult to judge, because there are several traditional evidence of recording or tape The method is characterized by an independent evidence method that is used as a method other than five evidences, which is more appropriate. And because of the contents of the recording due to non-evidence, documentary evidence or evidence, so the evidence investigation method cannot be in accordance with Article 164 of the prompts of evidence survey, it should be in court to confirm its contents, and the documentary evidence should be read Have the same meaning, which also shows the particularity of the recording evidence.<sup>287</sup>

In the case of video evidence, video is also a method of evidence other than traditional evidence, that is, recording and video are new evidence methods. If the video is used as evidence, the video itself is not a matter of matter, may not be used as evidence, and video content will be broadcast for the case occurred after a record role, it has the role of book certificate. In the case of video recording of the scene, the video content as a transcript of inspection, although this should still be as an

---

<sup>286</sup> Hsien-Ming Chiu & I-Long Lin, *supra* note 200, P. 61.

<sup>287</sup> Tun-ming Tsai, *supra* note 210, P. 195.

independent evidence method is appropriate.<sup>288</sup>

However, some scholars do not recognize SME as an independent type of evidence. Under the strict proof of the request, the evidence investigation should be consistent with five kinds of statutory evidence, that is, the defendant, witness, identification, investigation, the instrument of these five kinds of statutory evidence, originally did not allow the creation of five kinds of evidence outside the " The sixth method of evidence, the essence of which is that, first of all, even if the court uses the sixth method of evidence, the court has no relevant investigation procedure to follow, the court should be how to identify its investigation process becomes a problem; Secondly, The court may create a sixth kind of evidence, not only should not be allowed, but also unnecessary, the existing law provides that the court may create a sixth instance of the evidence, not only should not be allowed, but also unnecessary, the existing law provides for the purpose of the criminal investigation of the defendant. Five kinds of statutory evidence methods, has been able to meet the needs of various evidence survey information, such as the meaning of the contents of the tape, should play the court, this is the evidence of the survey method, if we want to compare the voiceprint, because of non-ordinary people involved in facial sensory Can distinguish the professional ability, it should be used to identify the evidence method, for example, to the defendant to suggest evidence, also Facial features in order to ascertain the perception of evidence method inquest type of evidence, evidence sixth methods are wrong.<sup>289</sup>

#### **4 Probative Value of Evidence**

---

<sup>288</sup> Tun-ming Tsai, *supra* note 210, P. 196.

<sup>289</sup> Yu-Hsiung Lin, Cover Pandora's Box: J.Y. Interpretation No. 582 of the Constitutional Court Ends the Sixth Form of Evidence, in Yu-Hsiung Lin, *Coercive Measure and Criminal Evidence*, Angel publish: Taiwan, 2008, p. 342-343.

The probative value of evidence means function of the evidence, which can proof the facts of crime, and its degree of proof function. The evaluation of evidence is based on the principle of evidence. The principle of free evidence does not have any hard law to prescribe what evidence of evidence is higher than other evidence, and in addition to requiring the judge to reach a subjective confirmation that there is no reasonable suspicion to be convicted, there is no hard law that " Under what conditions can be considered that the facts of the crime have been proved or not proved, "the fundamental starting point is to recognize the case differences, so how to assess the evidence and the value of the evidence can only be commissioned by the judge according to the specific circumstances of the case, but to avoid the judge There are no restrictions on the principle of arbitrary and free evidence. The restrictions include: evidence must be based on the ability to bear evidence, and in addition to the principle of the law clearly defined, still have to comply with the rules of experience and the rules of the constraints.<sup>290</sup>

Article 155 of the Criminal Procedure Law states that, "the probative value of evidence shall be determined at the discretion and based on the firm confidence of the court, provided that it cannot be contrary to the rules of experience and logic." This article is the principle of the principle of free evidence, that is, the proof of evidence by the judge according to free evidence, but in the evaluation is not without restrictions, must comply with the rule of law and rule of law.

In addition, there are other legal express limits on the principle of free evidence, including article 47, "Trial records shall be the exclusive proof of the proceedings of the trial.", Article 156 (2), "Confession of an accused, or a co-offender, shall not be used as the sole basis of conviction and other necessary evidence shall still be

---

<sup>290</sup> Yu-Hsiung Lin, *supra* note 152, p.15-18.

investigated to see if the confession is consistent with facts.”, and Article 100-1(1) & (2), “The whole proceeding of examining the accused shall be recorded without interruption in audio, and also, if necessary, in video, provided that in case of an emergency, after clearly stated in the record, the said rule may not be followed. Except for the circumstances prescribed in the Proviso of the preceding section of this article, if there is an inconsistency between the content of the record and that of the audio or video record regarding the statements made by the accused, the said portion of the statement shall not be used as evidence.” In the investigation of digital evidence, the degree of proof of the level of judgment must be subject to the rule of thumb and rule of the rule of the restrictions.

#### 4.1 The Rule

##### 4.1.1 Rule of Experience

The evidence of the evidence, if the fact that the court of law to determine their own discretion, and its judgments, should still be subject to the rule of thumb and rule of rule.<sup>291</sup> In other words, if the evidence proves that the force is free to judge by the court, it shall not violate the rules of experience and the law of the law. If the court investigates all the evidence according to law, the judgment of the proceeds shall be judged by the fact that the parties shall not act as an appeal Reason for the Third Trial.<sup>292</sup>

In the litigation system, regardless of whether the litigation structure of the parties, or authoritarianism, because of the adoption of self-evaluation of evidence, is the evaluation of the evidence, the fact that the judge, given the discretion of the

---

<sup>291</sup> (53) Tai Shan Zhi No. 2067 Judicial Precedent (1964) of the Supreme Court, (45) Tai Shan Zhi No. 1172 Judicial Precedent (1956) of the Supreme Court.

<sup>292</sup> (27) Shan Zhi No. 2079 Judicial Precedent (1938) of the Supreme Court.

magistrate discretion, the law is not evidence of the evaluation , But in order to make a reasonable judgment, it should also be based on the rule of thumb, and based on this rule of thumb to judge, there should be a reasonable scientific basis, not simply the subjective experience, The freedom of judgment of the magistrate is not directly limited by the law, but in order to prevent it from being arbitrarily determined, there is no specific means such as evidence, evidence acquisition or evidence value, that is, the use of the rule of thumb Objectively various standards.<sup>293</sup>

The so-called rule of thumb refers to the rule of the people based on the experience of ordinary daily life, rather than contrary to the objective should be considered a certainty, non-reason, nor personal subjective speculation.<sup>294</sup> In other words, the rule of thumb is the objective existence of the rules, not only by the judge's own handling experience, knowledge to infer, neither the subjective experience of the judge, nor the subjective speculation. In the application of the rule of thumb, it is necessary to distinguish between the "generally effective" rule of thumb and the rule of "non-generally effective rule of experience". If the rule of law is generally valid, especially the rule of thumb that has been verified by natural science, The validity of the law, that is, in accordance with a scientific expertise recognized by the fact that the judge, even if the judge may not believe the individual, should be taken as the basis for the referee; if not a generally effective rule of thumb, Has the effect of restraining free evidence, the judge will carefully examine the specific circumstances of the case, the atmosphere, in order to refer to the rules of experience revealed by the high probability to determine the authenticity of the facts.<sup>295</sup>

The rule of thumb is an important principle in the evaluation of evidence, and the

---

<sup>293</sup> Pu-shing Chen, *supra* note 216, P.431.

<sup>294</sup> (28) Shan Zhi No. 2595 Judicial Precedent (1939) of the Supreme Court.

<sup>295</sup> Yu-Hsiung Lin, *supra* note 152, p.22.

scope of the evidence is very wide, and its value is different. Whether the evidence contains the facts of the evidence, the value of the evidence and what is closer to the truth and its proximity, the choice of evaluation, and the possibility of identifying the facts. In the modern criminal procedure, the judgment of the value of the evidence, the discretion of the magistrate, is not directly restricted by the law, but the magistrate has the discretion to judge the value of the evidence, but the discretion is not Standards, should maintain its rationality, and the rule of thumb is one of the criteria to maintain the rationality of the fact that the Department to determine its closest to the real knowledge, and the fact that the determination of the method should be the nature of things, shape And the causal relationship, etc., based on the reasonable criteria of the rule of thumb, how to choose the rule of thumb to determine the value of the evidence, which is sufficient to determine the truth close to the truth, and to resolve the possibility of objection.<sup>296</sup> Therefore, the evidence of evidence, the court inherent freedom to judge the right, still follow the rules of thumb, that is, not contrary to the experience of daily life, beyond the facts to make subjective speculation.

#### 4.1.2 Rule of Logic

The rule of law is the law of objective existence, which has objective and universal appropriateness, and has the subjectivity of the rule of experience. The relativity is different, its function lies in the appropriateness and appropriateness, and the suitability refers to whether the evidence and the fact are Whether it is suitable for the determination of the facts of the offense; the appropriateness means that it is reasonable to judge whether the evidence and the facts are reasonable.<sup>297</sup>

---

<sup>296</sup> Pu-shing Chen, *supra* note 216, P.434.

<sup>297</sup> Pu-shing Chen, *supra* note 216, P.439-440.

It is also argued that the law of reasoning refers to the logical rules of reasoning and deduction, and the value of the evidence of the judge's comprehensive evaluation of the evidence. To judge the truth of the facts, it is necessary to follow the basic logic rules of general reasoning and deductive conclusions, such as reasoning Committing the error of the circular argument; otherwise it is a violation of the law of reason. Secondly, the possible option as a necessary conclusion is also a violation of the law of the case, for example, assuming that the specific circumstances of the case, the fact that the truth may only be A, B, C three, if the judge according to the specific evidence to exclude A, and Refers to the exclusion of A, but suddenly argued that C is a violation of the law of reason, because in accordance with the logic of reasoning rules, excluding A, B, C are possible options, not necessarily derived C conclusion.<sup>298</sup>

#### 4.1.3 Rule of Evaluation

However, based on the rules of experience and the requirements of the law, the subjective process of the judge's determination must be blameless, that is, it must be based on objective, rational, logical and general rule of thumb On the basis of the argument, the rule of judgment of the evidence is given as follows:<sup>299</sup> 1. Other options If validly excluded by rational argument, the judge should be in accordance with the option of the referee; on the contrary, the excluded, there is a reasonable Suspect, the judge cannot reach the guilty conviction, not to be guilty. 2. The defendant's proof of absence, proved to be hypocritical, does not mean that the defendant has proved the crime. 3. The subjective confirmation of the judge should not base on the objective cannot be established on the basis of the rule of thumb, nor directly to the rule of non-general effective rule as the only basis for judging. 4. The value of evidence depends on the circumstances of the case, context. 5. The value of

---

<sup>298</sup> Yu-Hsiung Lin, *supra* note 152, p.22.

<sup>299</sup> Yu-Hsiung Lin, *supra* note 152, p.25-25.

indirect evidence is sometimes higher than direct evidence. 6. Simply theory, it is not enough to imagine a reasonable suspicion that it is not enough to constitute the basis of a judgment of innocence.

#### 4.2 Judging the Probative Value of Social Media Evidence

Where the evidence of the lawful investigation, its proof of power, by the judge free to judge, and the evidence of the testimony, although the freedom to judge, and for the choice of evidence, not to be restricted by law, but not free Evidence of fact that this from the provisions of Article 154, "the facts of the crime, according to evidence that no evidence cannot presume their criminal facts" and Article 155, paragraph 1, "evidence of evidence, by the court free to judge" , The court is free to judge as evidence of evidence, is not true.<sup>300</sup>

The judge's free evidence should have its boundaries, in particular, this judgment must be consistent with the rules of experience and rules of law, and constitute the judge free evidence of the restrictions. The court shall, in accordance with the principle of free trial and evidence, have the right to choose the right to choose, and whether it shall be re-authenticated, and the court shall also have the power to decide.<sup>301</sup> However, if the evidence is established in accordance with the standard operating procedures and the technical measures established in the computer digital technology are in compliance with the requirements of the regulations, the standard operating procedures can also be described as expertise Especially the rule of thumb, and therefore, the judge should, in principle, respect the standard operating procedures established by the expert if there are no other special reasons.<sup>302</sup>

---

<sup>300</sup> Pu-shing Chen, *supra* note 216, P.416.

<sup>301</sup> (80) Tai Shan Zhi No. 1063 Penal Judgment (1991) of the Supreme Court.

<sup>302</sup> Chen-Jung Tsai & Yue-Ting Huang, *supra* note 207, P. 25.

Moreover, because the digital evidence is not easy to individualize the characteristics of the analysis of the case, must be combined with other evidence to determine. Failure to properly evaluate the digital evidence and without experimentation, integration, and evidence relevance may lead to erroneous conclusions.<sup>303</sup> Such as the US *Liser v. Smith* case, the police in the investigation of the 54-year-old hotel female student Vidalina Semino Door murder case found that shortly after the death of the victim, someone has used the victim's financial card withdrawal, the police according to the financial card Check the screen, found Jason Liser for the murder of the case of the suspects. Although the bank manager reminded the police that the time of the monitor screen and the real time may not match, the police still released Jason Liser's photo as a murder suspect and Jason Liser was subsequently arrested. The bank said Jason Liser used a financial card earlier than the time of the incident, and the user was the financial card of his girlfriend, not the victim's financial card. The police then found that the cash withdrawal was found and the time was not correct. Jason Liser used the cash dispenser as early as before the incident. Finally, the police arrested two other suspects suspected of homicide in accordance with the clues to the victim's debit card. Jason Liser pleaded guilty to investigating Jeffrey Smith, who was responsible for the arrest of the law, and advised against illegal arrests, defamation and misrepresentation. The court held that Jeffrey Smith did not try to understand the way the monitor screen was operated and did not inquire about the way it was operated, and arrested Jason Liser only on the basis of the monitor screen information, even though the police subsequently found the arrest and was released immediately Jason Liser, also cannot be exempt, so that the police have fault.<sup>304</sup>

---

<sup>303</sup> Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 112 (Academic Press) (2004).

<sup>304</sup> *Liser v. Smith* 254 F.Supp.2d 89 (D.D.C., 2003).

To prove the facts of the crime, it is necessary to accumulate sufficient evidence to achieve a certain proof of validity, so that the information stored in the computer can never become part of the evidence, but only the computer stored information itself, its proof Force is quite weak, the computer data itself as a sufficient evidence of the crime, will rely on other evidence to strengthen.<sup>305</sup> More evidence of the absolute need relies on other relevant evidence to reinforce, in order to make computer evidence to achieve a certain proof of force.<sup>306</sup> In the evaluation of digital evidence, different digital evidence of different levels of different evaluation, this time, we can refer to the American scholar Eoghan Casey proposed digital evidence guilty conviction level, such as the defendant allegedly spread obscene picture of the case, the defendant computer After the identification, from the defendant computer network browser history found that the web browser will open some files, or automatically pop up the window, etc., this evidence may make a judgment on the defendant to commit innocence; and, for example, the defendant Suspected of the Internet blog allegedly slander the case of others, after the investigation from the defendant's Internet IP address, Internet user account registration information, network traffic and other information, are pointing to the defendant of the defenders, and the defendant only one person to live , According to open evidence, may reach the defendant to determine the extent of guilt.

#### 4.2.1 The Application of Natural Science in the case of using Digital Evidence

Because digital evidence often involves scientific knowledge and technology, it is necessary to rely on various natural science conclusions to evaluate the evidence of evidence in the judgment of evidence. The so-called natural science conclusion, refers to the natural science has been confirmed matters, are generally effective rule of

---

<sup>305</sup> Jung-Chien Huang, *The Limit of Criminal Penalty*, Angle publish: Taiwan, 1999, P.205-206.

<sup>306</sup> Chen-Jung Tsai & Wei-Ping Chang, *supra* note 199, P.57.

thumb, is also the most certain rule of thumb. However, due to the fact that natural science has confirmed the problem, it is found in the courtroom mainly through the operation of the appraisal system. Therefore, it not only involves the professional knowledge of the natural sciences, but also the relationship between the judge and the appraiser.<sup>307</sup>

However, the natural science to confirm the matter, sometimes only probable rate, but also the statistics on the conclusion of it, not necessarily an absolute one hundred percent. Only when the statistics is on the very high or very low probability, for the evaluation of evidence have a direct benefit.<sup>308</sup> For example, digital evidence is susceptible to additions and deletions, and is not easily perceived from the appearance. At this time, if the defendant's defenses are tampered with, or the evidence presented in the court is not from the evidence, the evidence has been In the course of the investigation was destroyed, then how to prove that digital evidence has not been modified, that is, through the computer theory survey, this time, through the hash algorithm for the hash algorithm for a mathematical program, the possibility of establishing similar data Digital fingerprint method, the file by the hash algorithm calculation, we can determine whether the file has been modified. On the contrary, some figures are only statistically conclusive, and the judge is bound by such statistics, and other evidence judgments should be combined. For example, in a digital evidence investigation, the defendant sometimes does not deny that the telephone The defendant all, but advocated its computer has been poisoned or by the Trojans and other malicious programs invasion, so the e-mail is not sent by the defendant. The defendant's computer poisoning or Trojans invasion of the defense, although the number of computer poisoning is quite 559, but this is the conclusion of the statistics,

---

<sup>307</sup> Yu-Hsiung Lin, *supra* note 152, p.23.

<sup>308</sup> Yu-Hsiung Lin, *supra* note 152, p.23-24.

does not mean that the defendant's computer is also poisoned, even if the defendant computer poisoning or by the Trojan invasion, However, the virus or the Trojans have a lot of patterns and appear in different ways. In other words, even if the defendant's computer is poisoned or attacked by a Trojan horse, it is not equivalent to the fact that the e-mail is not sent by the defendant. Therefore, the judge should investigate other evidence.

Even if it is a natural scientific conclusion, the judge will define the scope of the rule of thumb that is "generally valid", that is, natural science does not equate to legal relations, natural science often can only confirm a fact, a criminal establishment of the premise, but may not be able to directly export the results of the establishment of the crime.<sup>309</sup> For example, the defendant allegedly obstruct the reputation of others posted on the Internet blog, for the majority of people cannot see a total of common news, after investigation, posted the text of the computer IP address from the defendant to apply for the network account, but this only To prove that someone has used the defendant's computer and posted the text, the perpetrator should be with the defendant and have the opportunity to use the defendant computer, but cannot be equivalent to the text is indeed the defendant.

#### 4.2.2 Posts, Comments and Messages

In the case of Posts, Comments and Messages as a proof of the facts of the crime, it is not possible to use only e-mail as the only evidence of the facts of the crime, since it is not possible to judge the producer from the outside, that is, the characteristic of the SME. In general, the applicant for the investigation of an e-mail account, but the applicant for an e-mail account, does not exclude the possibility that an e-mail account has been compromised by another person; we must further

---

<sup>309</sup> Yu-Hsiung Lin, *supra* note 152, p.25.

investigate the IP address of the e-mail, the web server login record, and so on.

#### 4.2.3 Still Images/Photos

In the photo evidence of the ability to obtain a guarantee, we should judge the value of the evidence of the photo, that is, the proof of the photo. The level of proof of a digital photograph must be determined by the expression of the content of the photograph, whether it is capable of presenting a certain degree of fact, or a logical offense, and obtained the judge's decision. Digital photos can be edited or data compression to restore the distortion (such as the scene is a straight line to digital camera processing, compressed archive, and then re-printed out to become a curve or broken), for digital photos facing the problem, this time, digital photos How to prove the power, by the judge according to the principle of free evidence, the discretion of the right to choose, whether the camera, the court has the right to decide.

In the evaluation of the photo of the proof force, should be divided into: attached to the transcripts or identification of the book, the proof of the record or identification of the same book; as for the supplement or clarity, attached to the complaint or the letter of the photo, The force should also be considered in the same way as the complaint or complaint. However, in the use of evidence for the photo, the most valuable photos of the scene, which is due to the implementation of the crime after the history, cannot be traced back, only by the time of the photographs were visible, so, if the court Put forward the photographs taken at the time to prove the facts of the crime in the past, the value of the evidence cannot be ignored.<sup>310</sup> In addition, if the photo is taken by the police, the legitimacy of the photograph taken on the scene is neither a problem, and as evidence to prove the facts of the crime, it is generally considered to have a higher evident force. In addition, the practice is to monitor the video screen as

---

<sup>310</sup> Tun-ming Tsai, *supra* note 210, P. 208.

a picture of the case of evidence, from A watch video remake of the photo, with the same time, another angle B monitor video camera compared to the dynamic picture, monitor the video screen for the dynamic image, And the remake of the photo as a static image, so the monitor video screen remake of the photo force is certainly lower than the surveillance video dynamic picture.<sup>311</sup>

#### 4.2.4 Voice Recording

Where there is no problem in the evidence of the recorded content, it is necessary to reproduce the facts, and to confirm the identity of the recording, to the identity of the confession or the identity of the confession.<sup>312</sup> And recording often in the way of recording translation of the court, such as the contents of the audio translation of the question, we should investigate the recording files, recording files proved to be higher than the proof of speech translation force.

In the case of the court, the trial proceedings may be documented in detail if the proceedings of the trial proceedings shall be on the contrary, Misunderstanding of the statement of the meaning of the situation, such as the trial record has been questioned, we can prove through the court recording. Because of the recording of the court for the recording equipment set by the court, so its impartiality and authenticity cannot be doubted, therefore, is given a high degree of proof, especially with the clerk in court produced by the trial transcripts, court recording proof Article 5 of the court's recording method stipulates that the litigation case shall, if recorded, be recorded by the clerk or other interested person, and shall be produced in accordance with the law and shall be assisted by the recording. If there is any objection to the transcript, the clerk shall broadcast the contents of the recording, and if the result is verified, if there

---

<sup>311</sup> (97) Jiao Shan Su Zhi No. 109 Penal Judgment (2008) of Taiwan High Court.

<sup>312</sup> Tun-ming Tsai, *supra* note 210, P. 194.

is any misunderstanding or omission, it shall be corrected or supplemented by the recording. If the transcript is correct, it shall be accompanied by the objection. It can be seen that the court recording has a higher testimony than the trial record.<sup>313</sup>

#### 4.2.5 Motion Pictures / Video

As the video for the dynamic image, is generally considered to have a higher proof force. And video can be divided into intra-court video and outside the court video, the purpose of the video within the court, nothing more than in the court to prove that the proceedings carried out in full accordance with the law, since a highly proven value. In addition, the legitimacy of the various acts of action carried out by the presiding judge, the appointed judge, the adjunct judge and the various litigation participants may also be proved. In particular, the video appears in the portrait and its actions, can provide the basis for identification, is the court video also has the same testimony with the trial record.

As for off-court recordings, such as video recorded by surveillance video equipment, it is recorded as a result of the perpetrators' behavior at the time of the offense, but as a criminal evidence, the image of the video content must be fairly clear and comparable , Can be used to identify the identification of the defendant. If we cannot defend the face of the face, the body and move for a further comparison of the observation, since the naked eye only seen with the defendant similar video portraits, that the video content of the defendant is no doubt.<sup>314</sup> Therefore, the proof of the video evidence depends on the clarity of the video decision.<sup>315</sup>

---

<sup>313</sup> Tun-ming Tsai, *supra* note 210, P. 195.

<sup>314</sup> (82) Tai Shan Zhi No. 1687 Penal Judgment (1993) of the Supreme Court.

<sup>315</sup> Tun-ming Tsai, *supra* note 210, P. 199.

## **Summary**

### 1. The significance of social media evidence in Taiwan law

This thesis considers that social media evidence is for the court as evidence of electromagnetic records or electromagnetic traces. Because the adoption of this definition can be with Taiwan existing legal and practical insights; also it can be with the rules of classification of evidence of convergence; to highlight the particularity of SME; and take the legislative principles of science and technology, to accommodate any emerging technology possibilities.

### 2. The application of social media evidence in Criminal proceedings

This thesis argues that social media evidence should have evidence of evidence and evidence to prove force, rumors of the law, the law of exclusion of evidence, documentary evidence and the best evidence of the law, the rules of evidence and other evidence applicable.

### 3. Admissibility and probative force of social media evidence

For admissibility of social media evidence, this thesis argues that in the case of legal reasons, it should be excluded from the exclusionary rules of evidence ability in accordance with the Criminal Procedure Law. As for the circumstances of the court's discretion, except the reference matter listed in the legislative reasons for the 2003 revised Criminal Procedure Law, this thesis thinks, it is considered that the following points may be used for reference: 1, in the case of legality, social media evidence obtained in contravention of the law enforcement or prohibition, such as a violation of the Telecommunications Surveillance Act, Seizure or other improper means of electronic evidence, in violation of rumors of the electronic evidence, etc., should be excluded .2, in terms of authenticity, there is no authenticity of social media evidence,

such as computer equipment is not under the normal operation; The social media evidence submitted by one of the evidence is incomplete, fragmented and discontinuous; the evidence shall be deemed to be inadmissible without legal preservation and cannot prove that the electronic evidence is true. When determining the admissibility of SME, I think the following directions should be considered: first, based on the form of proof that the authenticity of evidence considerations, the court should consider the accuracy and integrity of social media evidence, such as the evidence in the formation, storage, reproduction or transmission, collection and other aspects of the impact and the extent of its impact and other factors; and second, based on the actual proof of force considerations, the court should base on facts and laws to evaluate the value of social media evidence through inner conviction.

#### 4. Social media evidence and the hearsay rule

From the United States and Taiwan legal doctrine and practice, it can be found that it is necessary to apply the hearsay rule to social media evidence, especially to electronic equipment storage records and mixed derivative records, except the electronic equipment generated records. That is, the social media evidence generated by the "man-made" factor is subject to the rules of hearsay. As for the records generated by the electronic equipment, it is in fact the physical evidence and does not contain "human factors". Therefore, it should not be regulated only by hearsay rule. So far, Taiwan legal system accepts social media evidence to apply the hearsay rule mostly based on of Article 159-4 (2) of the Code of Criminal Procedure, *"In addition to the circumstances specified in the preceding three articles, the following documents may also be admitted as evidence...(2) Documents of recording nature, or documents of certifying nature made by a person in the course of performing professional duty or regular day to day business, unless circumstances exist making it obviously*

*unreliable...*”, as well as the general provisions of (3), “(3) *Documents made in other reliable circumstances in addition to the special circumstances specified in the preceding two Items.*” We can find that Taiwan and the United States share the same opinion on whether the hearsay rule can be applied to social media evidence issues.

#### 5. Social media evidence and exclusionary rules

The prosecutor or the judicial police officer inquired of the defendant or the suspect, who was arrested and arrested for the arrest of the defendant or the suspect who was in breach of the statutory obstacle or during the night interrogation. Evidence of a witness; or evidence of opinion of the witness; violation of the Legislative Yuan on June 15, 1969, the fifth session of the sixth session of the first The electronic evidence derived from the provisions of Paragraphs 1 and 2 of Article 7 of the Communications Protection and Inspection Act adopted by the 18th meeting shall be excluded and shall not be taken as evidence. In addition, for the illegal search, seizure of the electronic evidence obtained; in violation of the Legislative Yuan on June 15, 1969, the sixth session of the fifth session of the eighteenth meeting of the Security and Protection Law and Article 5, the judge shall, in addition to the circumstances expressly excluded by law, allow the judge to consider the balanced maintenance of human rights and the public interest, and the discretionary power of the evidence of the electronic evidence. As for the electronic evidence obtained by private law, according to the provisions of Article 158 of the Criminal Procedure Law, the evidence obtained by private law cannot be applied.

#### 6. Social media evidence and authenticity

The Taiwan Criminal Procedure Law adds to Article 165 of the Code of Criminal Procedure in 1992. It generally regulates the existing forms of evidence such as

recordings, videos and electromagnetic records, as well as all kinds of evidence that may be new in the future and expressly Equipment, display of sound, images, symbols or information "for recording, electromagnetic recording or other similar evidence of the investigation method." The provision examines the future possibilities of technology, reserves the space for development, and is inherently flexible. However, the Code of Criminal Procedure for certificate of the truth is not expressly provided, so it lacks standards can be followed in practice. It is very common for the modern society to put forward tapes, videotapes and electromagnetic records as evidence. The appearance of these items is not readable and should not only be used as a "hint" for investigation. According to Article 165, the presiding judge shall, in such a manner as to prescribe such evidence, display the sound, the image, the symbol or the information in the appropriate equipment.

#### 7. Social media evidence and the best rule of evidence

The Taiwan Code of Criminal Procedure does not have a similar provision in the rules of the best evidence under the Federal Rule of Evidence in the United States, and there is no specification for the conditions under which the instrument is made as evidence. But the instruments used in criminal proceedings cannot be made to the original, and sometimes there is a need to use the text or the shadow of the necessary, should be imitation of the United States legislation. The provisions of the use of the text should be made, or expressly allowed to use Taiwan Code of Civil Procedure Article 353, *"The court may order the production of the original copy of a document. Where the order for production of the original copy is disobeyed or the original copy cannot be produced, the court may determine the evidentiary weight of the written copy or photocopy of the document as produced by free evaluation."* Besides, because of lack of the best evidence rule, the court has the obligation to investigate evidence.

Meanwhile taking into account the Code of Criminal Procedure Article 161 I, "*The public prosecutor shall bear the burden of proof as to the facts of the crime charged against an accused, and shall indicate the method of proof.*", I think, about the investigation of social media evidence, the court and the prosecutor should cooperate with each other to investigate and prove the crime, in order to achieve the goal of the criminal procedure, finding the facts.

## References

1. Andrews, Lori (2012), *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*, Free Press (January 10, 2012).
2. Bauccio, Salvatore J., *E-Discovery: Why and how e-mail is changing the way trials are won and*
3. Bill Lee, *Emerging Computer Crime Investigation Technology - Network Forensics*, Communication of the CCISA, Vol. 13, No. 1, 2007, P. 181.
4. Brunty, Joshua & Helenek, Katherine (2013), *Social Media Investigation for Law Enforcement*, Elsevier Inc., MA: USA, p.79.
5. Chaur-Yi Huang, *Criminal Procedure*, enlarged edition, bestbooks publish: Taiwan, 2007, p.221.
6. Chen-Jung Tsai & Wei-Ping Chang, *Research on Computer Crime Evidence*, *Criminal Law Journal*, Vol. 44, No. 2, P.54.
7. Chen-Jung Tsai & Yue-Ting Huang, *Admissibility of Digital Evidence*, *Criminal Law Journal*, Vol. 49, No. 2, P.5.
8. Chen-Shan Lee, *Move the Weight on the Balance of Communication Security and Surveillance: Commentary on J.Y. Interpretation No. 631 of the Constitutional Court*, *Taiwan Law Journal*, No.98, 2007, p.284-285.
9. Chen-Shan Lee, *To Those Who Can Catch Up, Face up to Personal Data Protection: Commentary on J.Y. Interpretation No. 603 of the Constitutional Court*, *Taiwan Law Journal*, No.76, 2005, p.228.
10. Chia-Mei Kuo, *On the Definition and Method of Evidence of Electromagnetic Records - Comparing the Relevant Provisions of Canadian Electronic Evidence Uniform Law and Taiwan Criminal Procedure Law*, *Science & Technology Law Review*, Vol. 17 No. 4, 2005, p.12.
11. Chin-Li Wang, *Research on Digital Evidence of Computer Network Crime Investigation*, *Taiwan Prosecutor Review*, No. 13, 2013, p.18.
12. Claus Roxin, *German Code of Criminal Procedure*, trans. Li-Chi Wu, Sanmin publish: Taiwan, 1998, P. 308.
13. Dung-Shiung Huang, *Criminal Procedure Law*, 6th edition, Sanmin publish: Taiwan, 1999, P.366.
14. Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 112 (Academic Press) (2004).

15. Ferdico, John N., Fradella, Henrt F., & Christopher D, Criminal procedure for the criminal justice professional. 2009. P. 252-272.
16. Graham C. Lilly, Daniel J. Capra, and Stephen A. Saltzburg, Principles of Evidence, 5th edition, Thomson Reuters: USA, 2009, pp. 23-27.
17. Hoffmeister, Thaddeus A. (2014), Social Media in the Courtroom, Praeger, USA.
18. Holtzman, David H. (2006), Privacy Lost: How Technology Is Endangering Your Privacy, Jossey-Bass; 1 edition (October 13, 2006).
19. Hsien-Ming Chiu & I-Long Lin, The Offense and Defense Countermeasures of Digital Evidence in Court, Journal of Information , Technology and Society, Vol. 7, No. 1, 2007, P.55.
20. Hsun-Lung Wu, A Review on the Investigative Method of Real Evidence and Documentary in Taiwan Criminal Procedure, Taipei Bar Journal, No. 286, 2003, P.61.
21. Hung-Chang Chang, Discussion on the Application of Digital Image Evidence, Criminal Bimonthly, No. 57, 2004, P.100.
22. Jau-Hwang Wang, Forensics and Collection of Digital Evidence, Police Science Bimonthly, Vol. 34, No. 3, 2003, P. 135.
23. Jiun-Yi Lin, Criminal Procedure Law Textbook I, 12th edition, Sharing publish: Taiwan, 2011, p. 331-332.
24. Johnson, Thomas A. (2006), Computer Crime and the Electronic Evidence, in Forensic Computer Crime Investigation (Thomas A. Johnson ed., 2006).
25. Jung-Chien Huang, The Limit of Criminal Penalty, Angle publish: Taiwan, 1999, P.205-206
26. Kun-Lin Lin, Shih-Jeng Wang, Yueh-Hann Chang, Wen-Ya Chiang & Jia-Hong Huang, Unveiling Controversy of Trojan Defense on Internet Forensics, Criminal Bimonthly, No. 65, 2008, P.86-89.
27. Lai-Jier Her, Legal Review on the Event of Searching Piracy MP3 in National Cheng Kung University, Taiwan Law Journal, No. 23, 2001, p.87.
28. Lai-Jier Her, Recording, Videotaping, Investigation of Electromagnetic Records (Article 165-1 II of the Code of Criminal Procedure), Taiwan Bar Journal, Vol. 8 No. 9, 2004, p.33.
29. Li-Ching Chang, On Admissibility of Photo and Video Evidence, The Military Law Journal, Vol. 33, No. 12, P.22 & P. 24.

30. Marris Hsieh, Applying Principle of Writ Doctrine to Computer Search and Seizure: Take American Law as a Mirror, *Criminal Law Journal*, Vol. 48, No. 6, 2004, P.106.
31. Mei-Chih Tsai, Relevant Disputes about Network Monitoring in the Communication Security and Surveillance Act, *Science & Technology Law Review*, Vol. 11, No. 12, 1999, P.37.
32. Ming-Feng Tsai, Explore the True Nature of Computer Forensics, *Criminal Bimonthly*, No. 4, 2005, P. 22.
33. Ming-Yung Wang, Search and Seizure of Cybercrime, *Law Journal*, No. 191, 2003, p.50.
34. Nissenbaum, Helen (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books).
35. Pu-shing Chen, *Criminal Evidence Law*, Vanity press, 1992, P. 77-78 & P.375.
36. Ralph d. Clifford ed., *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 2006, at 145-146. pp. 2011).
37. Ralph d. Clifford ed., *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 2006, at 145-146.
38. Ralph D. Clifford, *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, California Academic Press, p. 105-107(2001).
39. Robert W. Taylor et al., *Digital Crime and Digital Terrorism* 244 (2006).
40. Rong-Geng Li, Search and Seizure of Electromagnetic Records, *National Taiwan University Law Journal*, Vol. 41, No. 23, 2012, p. 1059.
41. Rong-Geng Tsai, I Am Listening to You ( Part I): J.Y. Interpretation No. 631 of the Constitutional Court, Principle of Writ Doctrine, and Amendment of the Communication Security and Surveillance Act, *Taiwan Law Journal*, No. 104, 2008, P.48-49.
42. Rong-Geng Tsai, I Am Listening to You ( Part II): J.Y. Interpretation No. 631 of the Constitutional Court, Principle of Writ Doctrine, and Amendment of the Communication Security and Surveillance Act, *Taiwan Law Journal*, No. 105, 2008, P.53.
43. Rong-Geng Tsai, Yes,I do: Search with Consent and the Third Party's Consent, *The Taiwan Law Review*, No. 157, 2008, P. 113-114.
44. Shea Bennett, Facebook, Twitter, Pinterest, Instagram-Social Media Statistics and Facts 2012, All Twitter (Nov. 1, 2012, 6:00 AM), available at,

<http://www.adweek.com/socialtimes/social-media-stats-2012/472135>

45. Shih-Yen Chu, Criminal Procedure, 3rd edition, Sanmin publish: Taiwan, 2007, p.133.
46. Shiuh-Jeng Wang, Hung-Jui Ke & ICCL, Information and Network Security: Eyes of Secret –State of the Art on Internet Security and Digital Forensics, DrMaster Press: Taiwan, 2006, P.591.
47. Shiuh-Jeng Wang, Hung-Jui Ke, Chung-Huang Yang, Discussion on Evidence of Retention of Web Security, Communations of the CCSI, Vol.8, No.4, 2002, P.92.
48. Steven Goode, The Admissibility of Electronic Evidence, 29 REV. LITIG. 1 (2009).
49. Taylor, Robert W. & et al., Digital Crime and Digital Terrorism 244 (2006).
50. Thaddeus A. Hoffmeister, Social Media in the Courtroom, p.152.
51. Thomas A. Johnson, Computer Crime and the Electronic Evidence, in Forensic Computer Crime Investigation (Thomas A. Johnson ed., 2006).
52. Tun-ming Tsai, Criminal evidence law, Wunanbooks: Taiwan, 1997, p. 210-213.
53. Yu-Hsiung Lin, Aerial View on 2003 Amendment of the Code of Criminal Procedure, in Yu-Hsiung Lin, Coercive Measure and Criminal Evidence, Angel publish: Taiwan, 2008, p. 461.
54. Yu-Hsiung Lin, Cover Pandora's Box: J.Y. Interpretation No. 582 of the Constitutional Court Ends the Sixth Form of Evidence, in Yu-Hsiung Lin, Coercive Measure and Criminal Evidence, Angel publish: Taiwan, 2008, p. 342-343.
55. Yu-Hsiung Lin, Criminal Procedure Law, 7th edition, angel publish: Taiwan, 2013, p.492.
56. Yu-Hsiung Lin, freie Beweiswürdigung- Is the judge's discretion really free?, Taiwan Law Journal, No. 27, pp.13.
57. Yu-Hsiung Lin, in dubio pro reo and Legal Evaluation, The Taiwan Law Review, No. 72, pp.18.
58. Yu-Hsiung Lin, Kommentar- Durchsuchung und Beschlagnahme, Angel publish: Taiwan, 2002, p.137.
59. Yu-Shun Lin, Commentary on J.Y. Interpretation No. 631 of the Constitutional Court and the Communication Security and Surveillance Act, The Law Monthly, Vol. 51, No. 11, 2007, P. 1740.

## **Chapter 3 Extracting information from Social Network Sites**

This chapter will discuss how to use technology, mainly internet forensics, to obtain social media evidence. As the basic knowledge, the way that the network works and the evidence that may be obtained is shown below. In this chapter, we will discuss the forensic tools as a means of extracting information from social network sites and how to implement internet forensic to obtain social media evidence. Besides, we will discuss technical issues on transforming information to the evidence at court in the third section.

### **Section 1 Principles of Network Forensics**

Digital forensics is worked for the identification of digital data, and forensic practitioners specialize in acquisition, inspection and analysis of digital data. Its purpose is to collect, test, and analysis data from internet or computer stored. By preserving computerized evidence of crime and collecting meaningful information from the computer or drawing a rough picture of the incident from the piece of information to carry out live reconstruction. In this way, the digital forensics can be defined as a method of preserving, identifying, extracting, documenting and interpreting computer media evidence and analyzing its causes in a way and procedure.

For obtaining and analyzing data as reliable evidence at court, its basic principles are (a) obtaining the original evidence without change or damage to the case of evidence; (b) proving that the evidence obtained from the seizure of the exhibits; and (c) analyzing the copy without changing the exhibits or original data.<sup>316</sup>

---

<sup>316</sup> Shiuh-Jeng Wang, J. S. Lee & Fu-Hau Hsu, *The Security of Information, Intelligence and Mobile Networks in Applications*, DrMaster press: Taiwan, 2015, p. 10-9.

In order for the evidence to be obtained to have evidence, the forensic scholars believe that it is necessary to comply with SOP to ensure that the resulting evidence is evidence.<sup>317</sup>

A detailed description of the qualification process can be found in Section 2, Section 4 DEFSOP. Here is a simple chart showing the steps of the evidence collection and identification procedures. A detailed discussion of the qualification process can be found in Section 3.

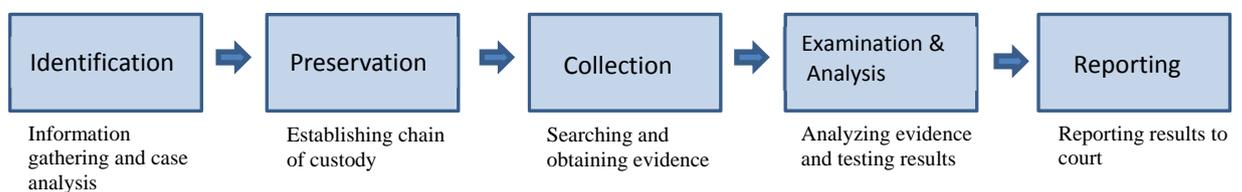


Figure 7 Obtaining evidence process in forensic science

As a means of obtaining social media evidence, network forensics is a kind of forensic science for detecting the crime by using internet, such as the online game to steal the game currency identification work that is. The scope of its forensics is more limited to the network operating environment, and may be interpreted as included in the computer identification (or digital identification), for the use of the network derived from the face of cybercrime investigation operations. Naturally should also apply the principle of digital forensics.

## 1. The Development of Principles of Digital Forensics

The ultimate purpose of the digital forensics is to present the facts of the case of

---

<sup>317</sup> Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3<sup>rd</sup> edition, Academic press: USA, 2011, pp.187-190; Shiu-Jeng Wang, J. S. Lee & Fu-Hau Hsu, *The Security of Information, Intelligence and Mobile Networks in Applications*, DrMaster press: Taiwan, 2015, pp. 10-10-10-12.

evidence in the court, and for the court to use, to restore and clarify the facts.<sup>318</sup> So whether the evidence is admissible and the evidence is as the same as the original are the key whether the court will adopt it or not. In order to meet the court's ability to evidence and the authenticity of the evidence requirements, over the past decade has been related to the number of identification process and principle. The following examples illustrate the principle of digital identification in recent years.

(1) In 2001, Digital Forensic Research Workshop (DFRWS 2001)<sup>319</sup> established the principle “*work from an exact copy of the original data*”, in case changing digital evidence.<sup>320</sup>

(2) In 2008, US National Institute of Justice (NIJ) published a document titled “Electronic Crime Scene Investigation: A Guide for First Responders, 2nd Edition.”<sup>321</sup> In this guidance manual, “*when dealing with digital evidence, general forensic and procedural principles should be applied:*

■ *The process of collecting, securing, and transporting digital evidence **should not change the evidence.***

■ *Digital evidence should be examined only by those trained specifically for that purpose.*

■ *Everything done during the seizure, transportation, and storage of digital*

---

<sup>318</sup> Inikpi O. Ademu, “A New Approach of Digital Forensic Model for Digital Forensic Investigation”, International Journal of Advanced Computer Science and Application, Vol 2, No.12, 2011.

<sup>319</sup> The first workshop on digital forensic research was held in Utica, USA during the 7<sup>th</sup> and the 8<sup>th</sup> of August, 2001. More than 50 academic researchers, professors, and digital forensic analysts and practitioners participated and discussed the following four issues: a framework for digital forensic science, trustworthiness of digital evidence, detection and recovery of hidden data, and network forensics.

<sup>320</sup> Palmer, G. (2001), "DFRWS Technical Report: A Road Map for Digital Forensic Research," First Digital Forensic Research Workshop (DFRWS), New York: Air Force Research Laboratory, pp. 14-31. available at <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

<sup>321</sup> NIJ Special Report, Electronic Crime Scene Investigation: A Guide for First Responders, 2nd Edition, <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>

*evidence should be fully documented, preserved, and available for review.”<sup>322</sup>*

(3) European Network of Forensic Science Institutes (ENFSI) proposed the following five general principles in the “*Guidelines for Best Practice in Forensic Examination of Digital Technology*”<sup>323</sup> in 2009.

*A. The general rules of evidence should be applied to all digital evidence.*

*B. Upon seizing digital evidence, actions taken **should not change that evidence.***

*C. When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.*

*D. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.*

*E. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.*

(4) UK Association of Chief Police Officers (ACPO) published the “*Good Practice Guide for Digital Evidence* (the 5<sup>th</sup> edition)<sup>324</sup> in 2012. This guide provides guidance on the testing of various types of computer equipment, enabling the practitioners to dispose of high-tech products in a timely and appropriate manner. The four principles of dealing with digital evidence were listed in this guide.

Principle 1: **No action** taken by law enforcement agencies, persons employed within those agencies or their agents **should change data** which may subsequently be relied upon in court.

---

<sup>322</sup> NIJ Special Report, *supra* note 321, p. vii.

<sup>323</sup> <https://cryptome.org/2014/03/forensic-digital-best-practice.pdf>

<sup>324</sup> ACPO Good Practice Guide for Digital Evidence V.5, [http://www.digital-detective.net/digital-forensicsdocuments/ACPO Good Practice Guide for Digital Evidence v5.pdf](http://www.digital-detective.net/digital-forensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)

Principle 2: *In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*

Principle 3: *An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*

Principle 4: *The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.*

(5) Richard Adams, Val Hobbs, and Graham Mann coined “The Advanced Data Acquisition Model (ADAM)” in 2013<sup>325</sup>, and mentioned that forensic practitioners must comply with ADAM Principles.

*1. The activities of the digital forensic practitioner **should not alter the original data**. If the requirements of the work mean that this is not possible then the effect of the practitioner’s actions on the original data should be clearly identified and the process that caused any changes justified.*

*2. A complete record of all activities associated with the acquisition and handling of the original data and any copies of the original data must be maintained. This includes compliance with the appropriate rules of evidence, such as maintaining a chain of custody record, and verification processes.*

*3. The digital forensic practitioner must not undertake any activities which are beyond their ability or knowledge.*

---

<sup>325</sup> Richard Adams, Val Hobbs, & Graham Mann, The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice, Journal of Digital Forensics, Security and Law, Vol. 8(4), 2013, p. 25-48, available at <http://ojs.jdfsl.org/index.php/jdfsl/article/view/110/198>

*4. The digital forensic practitioner must take into consideration all aspects of personal and equipment safety whilst undertaking their work.*

*5. At all times the legal rights of anyone affected by your actions should be considered.*

*6. The practitioner must be aware of all organizational policies and procedures relating to their activities.*

*7. Communication must be maintained as appropriate with the client, legal practitioners, supervisors and other team members.*

In order to ensure that the identity of the evidence, in fact, to prohibit the external changes in the amount of evidence, unless there are reasonable grounds and confirm the results of the operation will not cause evidence to change the next, in order to have experience and training qualified personnel. For evidence, therefore, in order to avoid controversy, in the preparation of digital identification procedures, that is to follow this principle to prohibit the change of the original and use a copy of the operation as a test analysis ; However, this principle applies to easy-to-disappear information such as mobile device identification or cloud identification, so that the analysis of the operation of the identification staff to limit, so that the court, the prosecution and lawyers confused the situation, and even lawyers questioned the mobile device identification process why not use a copy Analysis, why changes the original and so on. So there is much debate about the "work from an exact copy of the original data" principle, which was first laid out by DFRWS 2001.

## **2. Dispute on whether to Access the Original Data**

The state of the exhibits is a constant changing digital operating environment.

From the digital storage device to be tested, to obtain the relevant clue data, the original state of the confirmation is a difficult problem. Especially when the original state is constantly changing, access to digital evidence of the technology, is art or science (art or science), or investigation or identification (investigation or science), there is room for controversial discussion.

## 2.1 Do not access the original data

"Should not access the original evidence" claims, should give priority to the application of laboratory accreditation, does not apply to field investigation. But the cloud or smart phones and other identification, due to the identification of functional limitations, in the laboratory identification, there are still "access to the original Evidence "of the potential needs.

(1) DFRWS 2001 emphasized the reliability of digital evidence.

In order to obtain the Trustworthiness of Digital Evidence, the experts discussed how to get the structure of the data unchanged since it was first obtained when the data was first acquired. In order to ensure data integrity and to accurately and truly present the facts of the event (Palmer, 2001), DFRWS 2001 states that "the original exhibits cannot be accessed, and only the original copy of the original data"

However, the problem itself is flawed, without considering the volatility of the evidence, dynamic and urgency, should consider the law enforcement agencies in the field of immediate analysis needs, by suspects (or people) in conjunction with exploration, video certificates and appropriate explanation And so on, rather than blindly to the point of view of the laboratory, consider the integrity of data or reliability, the establishment of the traditional identification of science does not have the principle of digital identification: "not access to the original evidence." Seemingly

solve the trust of the rational controversy, but triggered a law enforcement agency practice is not feasible controversial issues.

(2) NIJ emphasized the integrity of digital evidence.

NIJ since 2004 to advocate the implementation of digital evidence inspectors should receive appropriate training. When collecting or dealing with digital evidence, the integrity of the evidence should not be affected. The process of collecting, inspecting, storing or converting digital evidence should be documented for future review by experts. The guidelines published in 2008 also extend the claim.

## 2.2 Allow to assess the original data

"Access to original evidence" should be given priority to field surveys. Law enforcement agencies must also refer to the relevant standards, the legal basis for access to the original exhibits of the standard operating procedures to reduce the impact of changes in the impact of digital evidence.

(1) The FBI emphasized the scientific method of forensic science (2000)

In 2000, FBI proposed the FBI's standards principle in order to guide the action of the agents and officers. One of them is, "Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner" (Standards and Criteria 1.7).<sup>326</sup> Law enforcement agencies to carry out the dynamic test of the exhibits, is bound to have access to the original exhibits, may also lead to local changes, damage or damage to the behavior of digital evidence, it is necessary to perform qualified professionals to reduce the degree of damage.

---

<sup>326</sup>

FBI's

standards

principle

<https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#IOCEInternationalPrinciples>

(2) In 2002, the Internet Society (ISOC) provided a Request for Comments (RFC), No. 3227 Guidelines for Evidence Collection and Archiving.<sup>327</sup>

In order to provide guidelines for the collection and backup of evidence for security incidents, incident handling, law enforcement officers and system managers, it emphasizes the collection of information in volatile order. Investigators to collect information will be traces of contact with the destruction of the crime scene, to minimize the traces of their own, and can distinguish between collectors or attackers left the human traces. Each time the investigator collects the evidence, it should process the evidence to be tested and order the volatility of the order of volatility. While the computer system volatile from high to low order (ISOC, 2002), as follows:

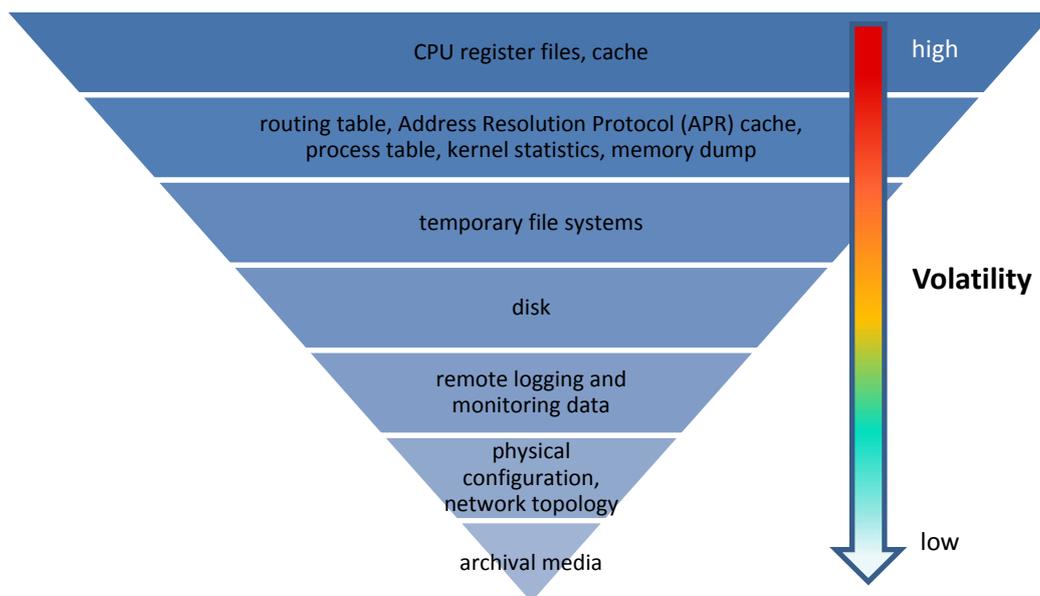


Figure 8 The order of volatility in computer system

In addition, the submissions reminded that the investigation or identification of personnel to access the original exhibits should avoid or reduce the change of information. In considering the volatility of the evidence of the order of evidence, in order to effectively collect data, the recommendations (ISOC, 2002):

<sup>327</sup> RFC No. 3227 Guidelines for Evidence Collection and Archiving, <https://www.ietf.org/rfc/rfc3227.txt>

(1) Do not complete the evidence before the collection, do not shut down. When you collect data, you can reduce the change in your data content, catalog, or file access time, and avoid using methods that change your data.

(2) As much as possible to capture the correct system information screen, keep the date and time containing the detailed notes.

(3) As far as possible the use of batch processing of the tool set, to avoid writing to be evidence of storage media.

(4) The signature and date shall be accompanied by a note or a printed document.

In the face of the collection or analysis of the choice, the submissions that the first to collect information, and then analysis. When the computer system is small and enough time, you can gradually check slowly, but when the computer is too much, you have to set through the suite tool set, quickly check a large number of computer files, in a limited time, to achieve the purpose of investigation. But if the analysis changes the file access time, it should be executed on the full copy of the image file.

(3) ISO / IEC 27037: 2012, emphasizing the relevance, reliability and adequacy of digital evidence<sup>328</sup>

ISO / IEC 27037: 2012 Information technology - Confidentiality technology - Digital evidence identification, collection, access and conservation guidelines for individuals involved in potential digital evidence of computers, mobile phones, digital cameras and video recorders, navigation and positioning systems or other storage equipment Identify, collect, acquire and preserve, provide digital Evidence First

---

<sup>328</sup> Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic (PDF Download Available). Available from: [https://www.researchgate.net/publication/283226153\\_Standard\\_ISO\\_270372012\\_and\\_Collection\\_of\\_Digital\\_Evidence\\_Experience\\_in\\_the\\_Czech\\_Republic](https://www.researchgate.net/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic) [accessed Oct 5, 2017]

Responders, Digital Evidence Specialists, Incident experts (Incident) Response Specialists, Forensic Laboratory Managers Collect information guidelines. Law enforcement agencies can rely on the standard analysis, to submit digital evidence to ensure the integrity of digital evidence. Although the standard for the digital evidence of the investigation and practice guidelines cannot replace any region's laws and regulations, ISO / IEC 27037: 2012 International Standard Descriptions accomplished to proceed as soon as possible by participating in the early stages of the investigation, including the initial response, obtaining sufficient potential digital evidence.

A. Principles of dealing with digital evidence: relevance, reliability and adequacy

Most of the jurisdiction or organization, taking into account the three principles of relevance, reliability, and sufficiency, do not just consider whether the court accepts the problem (ISO / IEC, 2012) , Rather than hastily identified the original exhibits are not allowed to access the trust.

(a) Relevance refers to a key to proving or negating a case. Digital evidence is relevant, depending on the case, whether the evidence proves or negates the critical matter of the case;

(b) Reliability, which ensures the true meaning of the digital evidence. The on-site forensics may not need to collect all the information or make a complete copy of the original exhibits, although the reliability is defined differently in different jurisdictions, the general reliability is defined as the true meaning of the evidence that ensures the specific presentation of the digital evidence;

(c) Suitability refers to the collection of sufficient potential evidence that the matter to be clarified is indeed inspected or investigated. When the time or cost (amount of money) is the key or difficult focus, the field handler will know which matters are the

focus and it is appropriate to know how the site investigation or laboratory identification should be handled.

#### B. Procedures for the processing of digital evidence

In the case of digital evidence handling processes, follow the documented procedures to ensure the reliability of the potential digital exhibits and to follow the following principles:

- (a) Minimizing manipulation with digital devices or digital data.
- (b) Documenting all actions and changes made to the digital evidence, so that an independent expert is able to form their own opinion regarding the reliability of submitted evidence.
- (c) Proceeding in accordance with the laws of the country
- (d) DEFR should not act beyond his or her competence.

#### 2.3 Practitioners are required to determine whether they have access to the original evidence

This is in line with the requirements of on-site investigation and laboratory accreditation, and the application of on-site investigation and laboratory accreditation should be included in the current mainstream argument, and by the actual training of the actual implementation of the staff, on their own To determine whether to "access the original exhibits" and to take full responsibility.

- (1) 1999-2014, SWGDE emphasized on forensically competent.

In February 1998, the establishment of the Digital Evidence Scientific Working Group (SWGDE, Scientific Working Group on Digital Evidence), with the United States to develop standard procedures for the International Organization of Computer

Evidence (IOCE, International Organization on Computer Evidence), the common development of cross- Evidence of recovery, preservation and inspection.

It emphasizes that the appraiser should talk to the investigators and carry the necessary tools and equipment to the scene to avoid wasting time and energy in the process of collecting the facts. It is necessary to collect relevant evidence, information and information.

A. In principle, the original exhibits cannot be accessed, the access to the original exhibits, the maintenance of digital evidence of the trust

The International Hi-Tech Crime and Forensics Conference, held in London, UK, from 4 to 7 October 1999, first proposed a draft standard for the exchange of digital evidence, followed by a US law enforcement agency use. The draft points out: Upon seizing digital evidence, actions taken should not change that evidence. When it is necessary for a person to access original digital evidence, that person must be forensically competent. ( SWGDE and ICOE, 2000 )

B. Evidence Triage / Preview, the relevance, reliability, and adequacy of maintaining digital evidence

In September 5, 2014, SWGDE's Best Practices for Computer Forensics,<sup>329</sup> acknowledging the need for classification and preview of evidence, are continuing. In 2010, American experts Stephen Pearson and Richard Watson advocated the Digital Triage Forensics concept, access to the original exhibits, and quick access to demand information (Pearson and Watson , 2010), and add the following points (SWGDE, 2014):

---

<sup>329</sup> SWGDE, Best Practices for Computer Forensics , 2014, <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics>

(a) Digital forensics pre-action

Evidence classification is the forefront of digital identification action, as the patient detection and classification mechanism, seeking to quickly collect information, in the shortest possible time to get the best results. The traditional digital evidence program focuses on digital evidence to begin checking the image copy and hash function validation, and the classification of evidence is also considered as a preview program for traditional digital evidence (Cantrell, 2012). The server may not be able to pull the plug (or shut down) to avoid damaging the system, affecting legitimate business operations, or adversely affecting the server's organization. In principle, the scene computer shutdown, do not boot. Only trainees can reboot, perform evidence classification or preview procedures (SWGDE, 2014).

(b) Depending on the case need to determine whether to access the original exhibits

Executing an evidence classification or preview program in an execution system can affect the timestamp record of the file. Evidence classification may be unwell to all conditions, and previewing evidence may miss some evidence of value. Because each method of evidence has different advantages and disadvantages, different role appraisers or performers should be able to judge according to different situations on their own, due to time and time to determine the procedures and methods of evidence, and bear full responsibility (SWGDE, 2014).

(c) Complement each other and cannot be replaced

Many organizations have no expertise to perform the collection of digital evidence. Evidence classification and preview can only be carried out by suitably trained professionals. When the classification of evidence cannot achieve the purpose of identification, no professionals or time, can still be copied through the image

processing. Evidence classification or preview program, cannot replace the image copy of the complete inspection of the reliability of the technology. Likewise, a complete examination of the image copy technique cannot replace the relevance, reliability, and adequacy of evidence classification or preview methods.

(2) In 2007-2012, the British Association of Senior Police Officers (ACPO), emphasizing appropriate explanations for handling actions

The ACPO, Association of Chief Police Officers is an important think tank for police and government departments in the UK. In 2007, the Good Practice Guide for Computer Based Electronic Evidence was proposed. (ACPO, 2012), the analysis is as follows:

A. Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

All digital evidence should apply the same legal norms and apply to derivative documentary evidence. The documentary evidence shall be construed as: to prosecute, inform or report the duties of that party, the first contact with the law enforcement agency, or the current condition of the possession of the evidence, shall not be deleted, and shall be presented to the court as it is.

B. Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Operating systems and other programs often change, add and delete electronic storage content, the user may not be informed, automatically change the data status. If the investigator is to extract the partial / selective data for the complete electronic

device's physical / logical extraction, or sorted batch processing, the image should be produced and professional judgment should be used to capture relevant and critical evidence. If the data is processed, there is no local side, there may be far-end, will face the dilemma cannot get the image, direct access to the original data as necessary procedures. Those who have such prerequisites and pragmatic considerations have the ability to retrieve information and provide explanations to the court with direct access to the original information. If the information to be taken is placed in another jurisdiction, careful consideration is given to the application of enforcement rights.

C. Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

It is critical to demonstrate the objectivity of the court proceedings and the consistency and completeness of the evidence. How to recover evidence and the presentation of evidence acquisition procedures is necessary. The preservation of the evidence should be of a certain degree, which must be: when the evidence is presented to the court, an independent third party can repeat the same procedure to re-examine and achieve the same result. However, if the same procedure cannot be repeated on the site, the reliability of the data can be examined by documentary records such as live video. In the digital evidence survey, the main challenge is evidence of the static outcome of the dynamic event; especially when the dynamics of the evidence occur, the identified digital evidence may not be available or incomplete. Any evidence change should be recorded, the evidence of the loss of the collection process can be recorded, and the evidence collection method should be judged on the basis of the case.

D. Principle 4: The person in charge of the investigation has overall responsibility for

ensuring that the law and these principles are adhered to.

It is noteworthy that these principles do not exclude the proportion of digital evidence method (search, seizure should be in line with the principle of proportion, also for large business organizations). (Such as clues, information, information, evidence) and survey resources (such as team manpower, time limits, pending cases), it is necessary to determine the focus and scope of the survey. This includes a technical or non-technical risk assessment, such as a specific type of device-specific potential evidence (such as Unix-like system with inode<sup>330</sup> attribute, can delete the file time), or the suspect's historical criminal record.

## 2.4 Discussion

Access to the original evidence helps to clarify the status of the network and traffic, such as the possibility of data on the Internet may be uncertain when dealing with cloud evidence. Internet traffic and traffic are both short-lived and must be retrieved when they are transmitted. The capture of the current network packet is a copy of the backup information, no comparison with the original data similarities and differences. Collecting digital evidence can not only focus on static data, network dynamic data should also be noted, to avoid missing important evidence.

2.4.1 Traditional Forensic Science does not require practitioners to preserve but not to change the original exhibits.

From 2004 to 2011, American scholar Eoghan Casey argued that it was

---

<sup>330</sup> The inode is a data structure in a Unix-style file system that describes a filesystem object such as a file or a directory. Each inode stores the attributes and disk block location(s) of the object's data. <https://en.wikipedia.org/wiki/Inode>

unrealistic to access the original exhibits. And in his book *Digital Evidence and Computer Crime*: "It is wrong for some of the people who are engaged in the identification that digital evidence cannot be changed to meet the requirements of identification" (Casey, 2011). Traditional knowledge of scientific DNA testing, no requirement to change the original evidence, identification of DNA evidence samples, the test itself is a devastating test, will change the DNA samples, still meet the identification requirements and has been accepted by the court (Casey, 2011). Fingerprint identification is the same, test the original evidence. As long as the changes in the evidence to make a reasonable explanation, then the change does not affect the evidence in the identification of the essence. But with a standard to state: "save but not change any evidence", with the original traditional scientific requirements of different identification. In other words, the preservation of anything did not change the original evidence of the criteria, with the traditional forensics of scientific requirements inconsistent phenomenon. Such a statement is quite dangerous and unreasonable in court proceedings. From the understanding of the case, the image file backup, data recovery, keyword search and site reconstruction and other systems analysis of evidence down, failed to quickly and efficiently handle exhibits, often lead to the rapid accumulation of proof items, unfavorable litigation get on.

### **3 Adjustment of the Principles**

In recent years, the principle of digital forensics has been gradually revised and adjusted in response to the characteristics of volatile exhibits and the flexibility of investigation activities, especially in the case of evidence of mobile devices.

(1) 2014 US NIST, "*Guidelines of Mobile Device Forensics*"

The American National Institute of Standards and Technology published the

Mobile Device Forensics (NIST-SP-800-101 Revision 1) <sup>331</sup> in 2014, which describes the characteristics of the mobile device, the processing flow and the way, In the analysis section, it is mentioned that the mobile device is captured far less than the computer, and one of the factors is limited by the way the authentication tool can provide it. Therefore, in this guideline, it is recommended to use the cable for evidence, But if it is not feasible, you can choose wireless or other destructive way to carry out, but when the method is proposed, it should assess its risk and impact; so in different cases have different evidence focus, for example, sexual abuse cases may focus on Whether the relevant photos or films involved in the case, the focus of online fraud may be the history of web browsing; without prejudice to the evidence before the evidence can be moderately modified evidence, but the evidence should be a detailed record of the evidence and bear the burden of proof , To explain why the way to evidence is the best way to deal with.

In addition, the National Institute of Standards and Technology (NST) also conducts tests on various types of digital identification equipment or software for the test methods, reference materials and verification standards for mobile device forensics equipment. According to the functions, performance and correctness of digital identification tools and equipment After the certification, the list will be published on the Internet, including the Cellebrite UFED series products, XRY, EnCase Smartphone Examiner and other well-known mobile device forensic equipment; these through the list, the most popular law enforcement agencies should be Cellebrite And CRY's forensic equipment, Cellebrite also helped the FBI crack the iPhone for the year (2016), but its approach was to use a system vulnerability (similar to hacking), which could also alter the original Evidence of consistency concerns,

---

<sup>331</sup> NIST SP-800-101 · <http://csrc.nist.gov/publications/PubsSPs.html#800-101>

whether for the domestic hospital, seized, argued by the parties to be observed.

(2) The British Police Association presented the Digital Evidence Best Practice Guide, 5th Edition

In principle 1, law enforcement officers are required to take no action to change the exhibits and to avoid contamination of the exhibits for the exhibits to be presented to the court. The usual method is to place the smartphones in the isolation bag, but after the bag, Because the phone will continue to search for signals, so the power will continue to wear out, resulting in power shortage shutdown, in order to avoid power shortage shutdown, and sometimes external power supply to avoid power shortage, but found that external power supply, may become a smart phone Antenna or isolation bag cannot completely isolate the signal from the situation. In addition, if you choose to turn off the phone, and sometimes encounter exhibits power key damage, and sometimes may be due to shut down or battery removal led to loss of volatile data; if the phone to maintain the boot state, the phone data may be by the wireless network Way to delete the remote.

In addition, mobile phone authentication tools cannot fully support all models of smart phones, so often by the identification of personnel to manually extract, and then the application of Principle 2 also questioned, questioned the identification of manual methods to assess whether the impact of evidence Integrity. For example, when an employee retrieves a photo, the access time of the photo file is changed, or the unread message is read, and the read status is changed. Or sometimes for the acquisition of critical evidence files must be installed within the smart phone third-party software, this approach is strictly to destroy the integrity of the evidence, but it is the current use of foreign methods, such as New Secure (formerly known as via Forensic) Authentication software via Extract.

Therefore, the principle of focus on the identification of personnel are eligible to analyze the evidence, whether the operational steps can have sufficient reason to explain the relevance of evidence and evidence, evidence action will have an impact on the evidence, just as the identification of personnel to the scene investigation and evidence, In the evidence at the same time also undermine the scene, but no one to question the scene of the investigators.

Unfortunately, the current domestic digital evidence is still in the past is still in the past, the concept of computer forensics, prohibit the identification of mobile devices to change and change, there is no electronic evidence in accordance with the relevant provisions of the law, the current identification staff can only take the safest evidence Way, that is, as far as possible not to cause controversial evidence method - "do not change the original", by the identification of equipment for standard evidence, but these foreign production of evidence collection equipment or follow the domestic law "not change the original" old identification staff cannot grasp.

In sum, although the necessity of changing the original data should be considered and still many hurdles are not easy to be over, the following principles are often agreed upon on an international basis:

- The act of collecting digital evidence should not result in any alteration of the data in question, wherever this is possible;
- All handling of digital evidence (from collection through to preservation and analysis) must be fully documented;
- Access to original digital evidence should be restricted to those deemed "forensically competent".

## **Section 2 Forensic Tool for Extracting Information**

## **1. Disk Backup Software**

This software should have the “Bit-stream copy” function. The normal copy function just makes a copy of data from the file explorer. But using bit-stream copy, the complete state of this hard-disk usage can be duplicated, even a copy of deleted data as well.

## **2. Recovery Software**

This software can recover the deleted data existing in a hard-disk. In order to destroy the evidence against themselves, whether the plaintiff or the defense, they usually delete important data or crime tools from computers. Therefore, investigators will use the recovery software appropriately and restore all these files to find the evidence.

## **3. Password Cracking Tools**

These tools can crack basic input output system (BIOS), passwords of the system administrator and passwords of encrypted files, and contribute to data collection. Excessive protection measures would obstruct information gathering by a forensic officer, especially when crime data is encrypted, it is hard to access. Therefore the password cracking tool can make a forensic work easier.

## **4. Forensic Toolkits**

In order to make the forensic work more efficient, some software combine multiple necessary functions, such as functioning as disk backup and recovery. Also these forensic toolkits provide the HASH function<sup>332</sup>, and automatically generate

---

<sup>332</sup> Hash Function is a method to establish the “digital fingerprint” of any data. It compresses information or data into summary, in order to reduce quantity of data to very small pieces and fixed data format. This function will disrupt and mix data, and then re-establish a digital fingerprint called “hash values”. Hash value is usually used to represent a short random alphanumeric string. Good hash

reports from collected data. Common forensic toolkits are introduced as follow.

#### 4.1 EnCase<sup>333</sup>

It is the most popular forensic toolkit at present, and can support a variety of operating systems, such as FAT16, FAT32, NTFS, Macintosh HFS, HSF+, Sun Solaris UFS, Linux EXT2/3, Reiser, BSD FFS, Palm, TiVo Series One and Two, AIX JFS, CDFS, Joliet, DVD, UDF and ISO 9960. EnCase has fully functions and a friendly interface, so it can lead forensic investigators to produce image duplicate step by step. Besides, it functions in bit-stream copy, HASH-MD5 verification and Cyclic Redundancy Code (CRC), in order to verify the integrity of the evidence. Moreover, it can check all data of operating system, such as file space, unallocated space and data of the exchange file. Except basic function to view file creation time, file modification time, access time, username and file attribute, it can show the content of file and uses drawing display, supporting ATR, BMP, GIF, JPG, PNG and TIFF. In analyzing files, EnCase can recognize known signatures, in case changes of the file extension to hide the evidence. It not only supports multiple formats of e-mail, such as Outlook, Outlook Express, Yahoo, Hotmail, Netscape Mail, MBOX, AOL 6.0, 7.0, 8.0, 9.0, PFCs, but also supports many types of browser, such as IE, Mozilla Firefox, Opera, Apple Safari. Finally, it can make forensic report automatically, presenting in Rich Text Format (RTF) or Hyper Text Markup Language (HTML).

#### 4.2 The Corner's Toolkit (TCT)<sup>334</sup>

TCT is written in C and perl language, and can search or analysis data in Unix (Unix-like) operating system. TCT is composed of three parts. They are Grave-robber,

---

function rarely makes hash conflict in the input field. It is unique. Therefore, it can be used to prove the identity of data.

<sup>333</sup> <http://www.guidancesoftware.com>

<sup>334</sup> <http://www.porcupine.org/forensics/tct.html>

MACtime and Unrm & L Lazarus. Grave-robb er is the main tool of TCT, functioning in data extraction or data storage. It will scan the whole system and extract information needed under normal circumstances. However, if a user is not authorized, Grave-robb er will stop the user accessing Root files. After the implementation, it will build MD5 signature of all output data and storage it in data/hostname -e/MD5\_-all. If the user cannot take all output data, the user can just take MD5\_-all. It also help the user to do forensic. MACtime functions in collecting Mtime, Atime and Ctime. Mtime is modified time, which means the last time that the file is modified. Atime is access time, which means the last time this file is accessed. Ctime is change time, which means the last time to change this file. These time data are easy to tamper, so investigators must handle these data very carefully, to ensure the correctness of evidence. Unrm & L Lazarus are recovery tools, which can restore a damage file or a missing file. Unm is written in C language. It can find unallocated files and proceed with potential data mining. L Lazarus can search required information from Unm or other sources. It can be applied on a file system, such as UFS, EXT2, NTFS, FAT32.

#### 4.3 Access Data's Forensic Toolkit (FTK)

FTK is a forensic toolkit recognized by the US government and American courts. Its specialties are simple use and quick analysis. FTK includes five different forensic tools. They are Forensic Toolkit (main interface), which functions in forensic and analyzing data; Password Recovery Toolkit (PRTK), which functions in analyzing, cracking and restoring passwords; Registry Viewer, which functions in analysis and decryption of the log file; Wipe Drive, which functions in removing drive data and information completely; and FTK Imager, which functions in previewing digital evidence and obtaining images. FTK is the main analyzing tool in this toolkit, functioning in analyzing, extracting, organizing, and saving digital evidence. FTK

makes an index of the whole text, so it can search and filter information effectively. It supports FAT 12/16/32, NTFS, EXT2/3 and supports image formats, such as EnCase, Ghost (Forensic Image Only), Linux DD, SMART, and CD and DVD format (CDFS, Alcohol(\*.mds), ISO, NERO(\*.nrg), CloneCD(\*.ccd)).

TABLE functions of forensic software

	<b>EnCase</b>	<b>FTK</b>	<b>TCT</b>
<b>Wipe Disk</b>	O	O	N/A
<b>Duplicate</b>	O	O	O
<b>Validate Image</b>	O	O	O
<b>File Recovery</b>	O	O	O
<b>EXT2/3 Support</b>	O	N/A	O
<b>FAT 16/32 Support</b>	O	O	O
<b>NTFS Support</b>	O	O	N/A
<b>E-mail Search</b>	O	O	N/A
<b>Keyword Search</b>	O	O	O
<b>Password Recovery</b>	O	O	O

<b>CDFS Support</b>	O	N/A	O
<b>View Registry</b>	O	O	N/A
<b>Image Gallery</b>	O	O	N/A
<b>Generate Report</b>	O	O	O

## 5. Other Tools

Except those forensic tools mentioned before, there are other tools necessarily in uses and will be able to assist in evidence collection in the crime scene. For example, since digital data cannot be directly recognized by people, forensic investigators will use the notebook to view most of the digital data immediately. It is helpful to collecting evidence. Then they will storage necessary data or information may be used as evidence in a flash drive or a portable hard drive, which functions in storage and backup. Although the main task is extracting information from the social network site or collecting digital information, the related environment, such as display of the computer, or connections of cables and lines, should be also clearly recorded. Forensic investigators can use a camera and a video camera making a record, in order to rebuild this crime scene or event site. In the meanwhile, investigators also need to record the whole procedure of evidence collection and indicate the time line, in writing. Besides, a label can help to mark a line and its corresponding jack.

## Section 3 Performing the Forensic Process

### 1. Preservation of SME

#### 1.1 Identification of Evidence

The first step of internet forensic to collect data is identifying where to find possible evidentiary data related the present case. In general for digital evidence, forensic investigators may search the computer belong to the defendant or the victim/ the plaintiff, and its media for storage such as hard-disks, random access memory (RAM), and Cache<sup>335</sup>. One thing should be noticed when collecting data from computers, that is, data storage in RAM or Cache disappears easily as the computer is turned off, and its backup requires the special software. Besides, the smart phone or the tablet should be the possible place to find related evidence, especially most people like to use APP to connect their social websites. Other possibilities still can be discovered, for examples, customer connection record provided by internet service provider (ISP), or credit card records.

#### 1.2 Backup of Evidence

Considering digital data can be modified easily, scientific tests or techniques should operate in other computer, in order to ensure the integrity of the original data. Hence, it is necessary to make a backup in advance. For the backup, forensic investigators should use a formatted hard drive with sufficient capacity, to make sure that there is no other remaining information would be interfere with the acquired data. For the complete usage record of the hard disk, a bit-stream copy is required and at least two (or more) duplicates are necessary. One of duplicates is for inspection and analysis of evidence, and another is for verification purpose. Through calculating

---

<sup>335</sup> [https://en.wikipedia.org/wiki/Cache\\_\(computing\)](https://en.wikipedia.org/wiki/Cache_(computing))

HASH from the original data and duplicates, investigators will ensure tested data is the same with the original data. Besides, another duplicate can be taken as additional backup, in case of damage or overwritten of the raw data. When collecting specific part of data and its storage position has been known, two duplicates can be made in general way to copy files, instead of bit-stream copy.

Collected evidence should be appropriately stored and strictly regulated, to ensure its security. Seized computer equipment or devices should place in centralized custody, prohibited authorized personnel to enter this place. On the software side, obtained digital evidence should be encrypted, to avoid authorized personnel to access or modify them.

## **2. Investigation of SME**

### 2.1 The Hidden Evidence

Using bit-stream copy can obtain the whole files, especially including deleted data, encrypted data and data in slack space. The problem is the content of these data cannot be recognized directly, so forensic investigators will use tools to view this data.

- (a) Deleted Data: in computing, the delete file command means to release the space occupied by the deleted data and allow other files to use this space. This deleted file in theory should be still there until covered by other files. Forensic investigators can recover the deleted file through recovery software before the old file was covered.
- (b) Encrypted Data: data is protected by password or encryption. It is also difficult to access the content of data without passwords. Forensic investigators will use password cracking tools to crack passwords and access information. There is

commonly used software or programs with passwords protect function, such as zip file (compressed file), Microsoft Office, and Portable Document Format (PDF).

Data in slack space: Cluster is the unit to calculating the amount of space for file storage in the computer. The size of the cluster will vary with the size of the file system. For example, in this computer one cluster is 4KB. The user save a 7KB file and this file will occupy two clusters in this computer. Two clusters are 8KB, that is, there will be 1KB space leftover. Because one cluster only provide one file to use, that 1KB leftover cannot provide to other file to storage data. After covering and overlapping other files several times, there will be many pieces of information leftover in slack space. These pieces of information may become material evidence. Although information is not complete, if investigators can find the connection or relevance with the case, they may get the key of this case.

## 2.2 Computer Search

The search object here is automatically generated computer record. This record may not directly prove or support the case, but it can be taken as the clue for investigation. For example, investigators can view “temporary internet files” (C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files) to realize the user’s internet history. This record also keeps pictures and text on the viewed websites. “Connection Record” (C:\Documents and Settings\Administrator\Local Settings\History) keeps URLs that the user has connected. “Favorites” (C:\Documents and Settings\Administrator\Favorites) records websites that the user likes or visit often. “Recent” (C:\Documents and Settings\Administrator\Recent) records documents or files that the user used recently. Although that document or file was deleted, investigators still can find shortcut links of that document, and associate alleged facts or the case with these filenames.” Instant

messaging software” is preset to store the contents of the conversation and received files in (C:\Documents and Settings\Administrator\ My Documents). Investigators can use these records to catch the user’s social network, connection and conversation to others.

When investigators perform the computer search, they can use the search function in Windows system to find the target more efficiently. This function provides filename search, keywords search, content search, etc., and the filter by date, type and file size. Investigators also need to notice the recycle bin in the computer. Simply moving the documents or files into the recycle bin will not delete them, so there might be some clue or evidence for the case.

### 2.3 Trojan Defense

Although Forensic investigators can determine obtained information from a specific IP location or a computer, it is difficult to determine who created this data. In practice, when investigators find evidence from defendant’s Facebook to prove his guilty of affront, the defendant normally objects and claims: “I didn't do it. I don’t know who did this. Maybe my account was hacked.” That is so-called Trojan Defense. It is due to that digital evidence is not easy to identify, and there is indeed a highly possibility to be hacked. Here are some cases.

(a) Back Door: If the use often downloads unknown programs or open unknown emails, his computer may be implanted backdoor(s). Then the hacker can use this backdoor to add, modify or delete files in this computer, or use this computer as the springboard to attack others computers. The hacker can delete or modify the records with this backdoor, in order to destroy evidence.

(b) Wireless Network: The hacker will scan Wi-Fi access points with some programs,

and use high power wireless AP to cover the target AP, in order to let the user's computer connecting to his own AP. Then the hacker can access the user's computer and obtain any information he needs. The hacker also can use users account engaging in cybercrime. Perhaps users will bear the consequences of the crime.

(c) Cache File: There are often Popup Ad Windows jumping out, when the user surfs the websites. Some of these programs preset to save images automatically. Even the user close this window immediately, advertising pornographic images have been stored in the computer. The user has no idea about why these images are in his computer.

(d) Used Product/ Second-hand Product: some used products still keep documents or programs inside, and some programs may be malwares. It is difficult for the buyer to prove these files do not belong to him, because at present he is the owner.

### **3. Crime Scene Reconstruction**

After forensic investigators collected related digital data, they will make a connection between the case and digital data, observing the relevance among different evidences. Then combining digital evidence with the time line, investigators can simulate the case and the order of each event in this case. A case is composed of Actor(s), motivation and purpose, the first time event, the occasion, and means.

#### **3.1 Presentation of SME in Court**

To present SME in a courtroom is a big challenge. Because people cannot directly understand digital data, which is an electronic record, written in 1 and 0. Only through computer equipment or digital devices, digital evidence has been given meanings to people and the court. Besides, to persuade judges or jurors, documentation of the

forensic procedure and other details, including collection, preservation and analysis, is the best way presenting in court. The purpose of documentation is to persuade legal system believe that evidence has not been destroyed and modified artificially.

Another challenge related to presentation of SME in court is the presentation itself. Because judges or jurors, they might not be familiar with computing and might not have computer expertise. A forensic practitioner should explain his own expertise in a clear and sophisticated way. The expert must explain how they produce this SME, how this SME can prove the case or fact in/directly, and what the relevance between case or events and evidence is. Moreover, the expert should point out identify of SME, which undoubtedly can make a connection with the defendant. A good presentation in court can make great influence on judges or jurors to accept the evidence that forensic practitioner provided.

#### **4. DEFSOP (Digital Evidence Forensic Standard Operation Procedure)**

Most of forensic scientists believe that,<sup>336</sup> building a standard operation procedure (SOP) for obtaining digital evidence is important and pressing at present. They think, through building SOP, standardized norms and tools, and certification, forensic investigators' capacity can be promoted, and also the credibility of their report in the courtroom can be strengthen. Furthermore, a complete SOP should response to the rule of evidence in court and will enhance the capacity and competency of digital evidence. It is necessary to realize rules of evidence and combine them in SOP. Therefore, a digital evidence forensic standard operation procedure will include four phase: building conceptions, preparation, operation, and report.

##### **4.1 Phase 1: Building conceptions**

---

<sup>336</sup> Eoghan Casey, 2004, Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet, Second Edition.

During this phase, forensic investigators will learn principles of digital evidence forensic, related regulations and norms, and a central idea. As principle, the guideline should be in general, instead of in detail. It should concern characteristics of digital evidence, to ensure no change of digital data, Integrity of the original data, and transport and preservation safely. It also needs to make sure there will be professional staff, certified tools and complete record of forensic procedure. Besides, it should think about “best evidence rule” and “the minimally invasive principle” requested from legal communities.

Forensic investigators should realize legal norms and rules of evidence are important. Only evidence, following the law, and responding requirements of authenticity and reliability in rules of evidence, will be accepted in court. This SOP also needs to regulate qualifications of personnel, and certifications of tools and environment.

Forensic investigators should keep this central idea in mind, that is, digital evidence is easy to disappear, modify and delete, so their work is not only to find the trace of evidence, but to force it to remain the trace of evidence. In other words, digital forensic is not only applied after the crime, but before the crime. They can make security mechanism and response plans in advance. After crime, they can obtain and preserve evidence safely, and identify and restore data carefully. The key point of a perfect digital forensic is prevention.

## 4.2 Phase 2: The Preparation

### 4.2.1 Authorization

Before operating digital forensic, investigators need to have the “power of attorney” (from private part) or the “search warrant” (from the court), or the situation

is applied for emergency exception made by law. In order to ensure capacity of digital evidence in the courtroom, investigators should follow the law and norms by SOP, and then performance their work.

#### 4.2.2 Information Security Policy

Both the company and the government should develop information security policies, because allowing digital investigation might cause risks on the business. Therefore, making the information security policy to draw a line for digital investigation and reduce negative influence on business activities.

#### 4.2.3 Data Collection

Forensic investigators can hold 4W1H principle to prepare the data collection. 4W1H means Who, What, When, Where and How. They are basic questions but help investigators to build the whole picture very quickly.

#### 4.2.4 Identification

When the investigator found someone suspected, then he can use that 4W1H principle to identify information obtained. He also can provide identified information to the police or other investigator, in order to conduct the next step.

#### 4.2.5 Task Group

Before going to the crime scene, forensic investigators should be separated into different task groups by their expertise. The command system should be built firstly, and communication channels should be established in advance. The command system should indicate the case in advance, explain the purpose, scope, and focus of this search, and assign individual tasks, in order to maximize the effectiveness of the work.

## 4.3 Phase 3: The Operation

### 4.3.1 Collection

Collecting digital evidence can be divided into the following six works: (1) Scene investigation and photography, (2) Identification and Records, (3) Preservation, (4) Collect and backup, (5) Search and Seizure, and (6) Packing and shipping. Preservation is the most important part of data collection, because the preserved data will become evidence in court to present the case or support the claims. Besides, comparing with traditional evidence, digital evidence is easier to delete and to modify. Therefore, investigators must put more attention on preservation of evidence. There are some useful tools to preserve the evidence, such as making record on site, taking a video, or using MD5<sup>337</sup>.

### 4.3.2 Analysis

After collecting and packing evidence, the next step should send the whole package to the police for storage. On the other hand, if digital data need to further identify, investigators should send the whole package to the digital evidence laboratories, in order to analyze information. However, if there is a special circumstance requiring an analytical work on site, investigator should follow these three steps to ensure the integrity and accuracy of the data analysis. They are (1) Backup and Records, (2) Inspection and Search, and (3) Analysis and Custody.

### 4.3.3 Forensics

When the digital evidence is still very large, it is necessary to do a further forensic research. The research project can be divided into (1) Data Extraction, (2) Comparison, (3) Individualized, and (4) Crime scene reconstruction, in order to

---

<sup>337</sup> <https://en.wikipedia.org/wiki/MD5>

ensure correctness and completeness of the information analyzed.

Because digital data is easy to hide or alter, one individualized evidence is the lack of convincing. Therefore, it is better identifying multiple source of individualized evidence, in order to convince the court to accept this evidence. For example, if an investigator wants to provide a dial-up Internet message from Mr. A, it is better he also provide A's phone number, internet account, bill address, IP and Mac address to show these individualized evidence all belong to Mr. A. The investigator can uses identification server and Call-ID system to find evidence.

#### 4.4 Phase 4: The Report

##### 4.4.1 Making a Report

A report to the forensic result should present real contents without any lies. The content should include the reporting unit; the case identification number; the investigator's name; the date and time of receive digital evidence; the date and time of this report; a description of a series of test projects, including the serial number, practices, and procedures; inspectors and their signatures; a description of forensic evidence, in the meanwhile explaining the chain of custody of issues processes; and forensic results. In remarks, it should indicate qualifications for forensics personnel, forensic tools and environment of the laboratory.

##### 4.4.2 Verifying Forensic Results

A correct forensic result is built on following the above SOP to performance. It also needs to explain used technology and tools. Forensic investigators should write down the whole forensic procedure and used tools, in order to review or examine its correctness by the third party and set up its credibility.

#### 4.4.3 Preparation to Court

When a forensic investigator is called as expert witness, he/she will prepare the forensic result, and the proof to show the whole procedure under SOP. In the trial, he/she should use the normal words and general conversation to explain the finding, upholding honesty and impartiality, with his/her expertise.

#### 4.4.4 Filing and Learning

Due to this digital forensic is an ongoing and progressive technology, building an archive will be useful to share experiences and skills, construct type of cases, and cumulate expertise. It is also effective to educate students systematically.

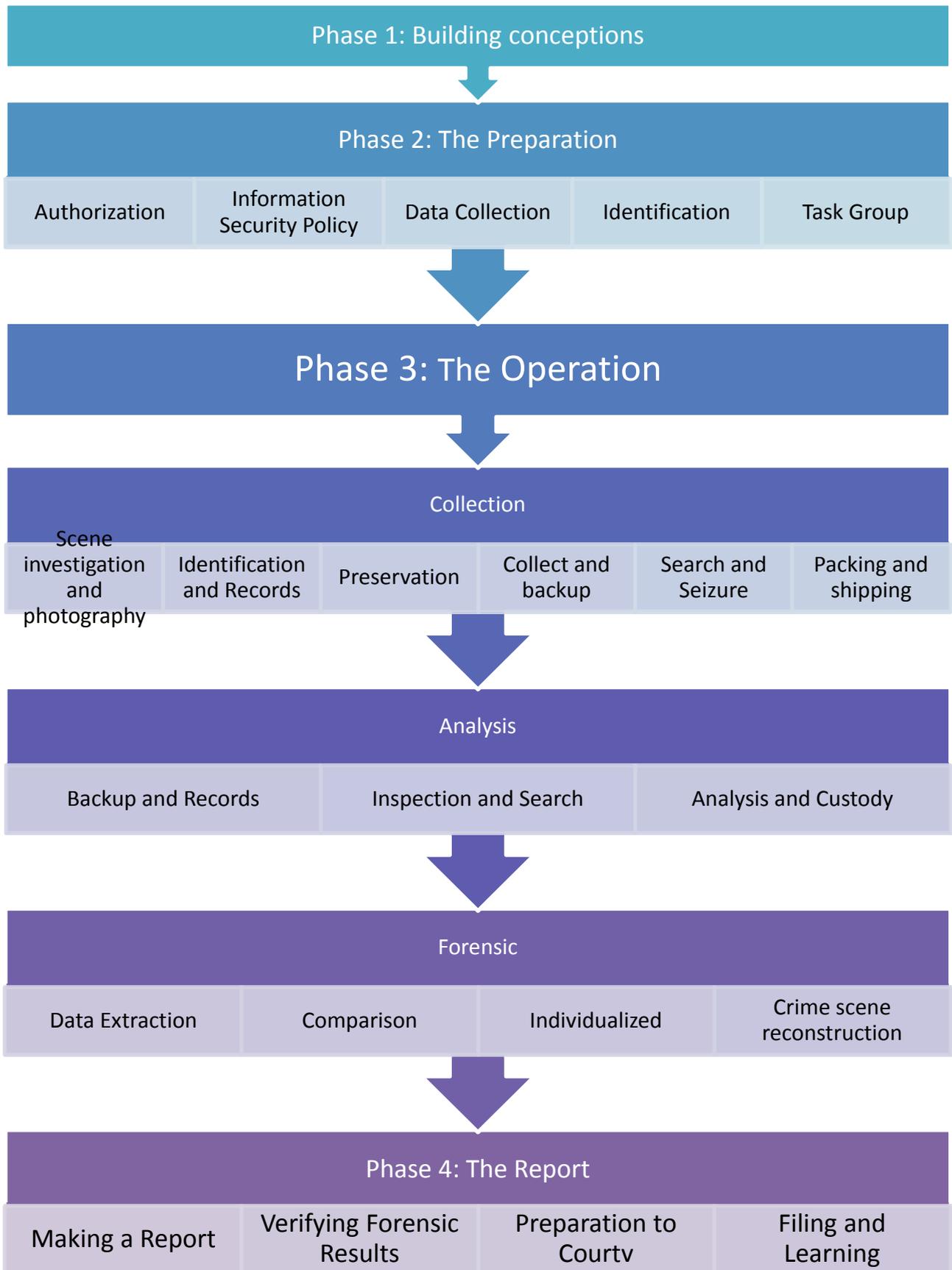


Figure 9 Digital Evidence Forensic Standard Operation Procedure (DEFSOP)

## **Section 4 Points to Transform to Social Media Evidence**

Once a scholar pointed out<sup>338</sup>, the investigative result will not be adopted by the court, if there is no any standard operation procedure to ensure consistency and quality of digital evidence. Even more, these untrusted digital data will lead to wrongful convictions, where the guilty will be released and the innocent will be convicted. The British Science and Technology Committee also claimed that,<sup>339</sup> any scientific technology or theories to produce evidence, should provide the proof of validity. Otherwise, evidence produced by these methods will not be adopted in court. Therefore, forensic science also should build the corresponding operation standards, in order to ensure that digital forensic and its results can be approved by legal communities and other societies.

### **1. Digital Evidence Verified by Hash Value**

The same string calculates the same Hash value, and the probability that different strings calculate the same Hash value is very low, which is too low to recognize its existence. Thus, if the results of the calculation are two different Hash values, then these two strings are not different. Hash values can be applied at various aspects, for example, the file sharing. In case that someone modified the file and adds the malware inside, the provider will publish the Hash value of this file. After downloading the file, the recipients can calculate the Hash value of this download file, comparing with the one the provider published. Then he will know whether the download file is the same with the original file. Likewise, it can also be applied in the field of computer forensics and digital evidence. In order to avoid to damage the original file or hard

---

<sup>338</sup> J. Jordaan, "A Sample of digital forensic quality assurance in the South African Criminal Justice System", *Information Security for South Africa (ISSA)*, pp. 1-7, 2012.

<sup>339</sup> Science and Technology Committee, *Forensic Science on Trial*, 2004.

disk, it is necessary to duplicate a copy for doing forensics. After making the copy, it is also necessary to calculate Hash value of both files to make sure they are the same.

Here is an example to show the different between the strings and Hash values. It is very clear, just with some space, the Hash value is totally different. Therefore, we can use this mechanism to verify the identity of the two files.

String	MD5 Hash	SHA-1 Hash
Social Media Evidence	3c4e5e1db630ebe4daa3e2847c9821db	8cf20113c2284e46ce696cc3c56fdf5f816abf62
SocialMediaEvidence	ad5bc5e290b8b0117cd1bd365384a1d6	262b4abb7b4ecdaa091ef56b159e32bac1f981f4

Reference: <http://www.miraclesalad.com/webtools/md5.php> ; <http://www.miraclesalad.com/webtools/sha1.php>

In order to make sure the identity between the original file and the digital forensics image file, the forensic practitioners usually calculate MD5 hash value of them. MD5, a common encryption algorithm, can convert any string into a Hash value with the fixed length of 128-bit. There will be  $2^{80}$  possibilities, so it is almost impossible that different digital data has the same MD5 Hash value. That is, if these two digital files have the same Hash value, then these two files can be deduced the same. In addition, MD5 is one of verification method, and there are several methods to achieve the same effect of verification, such as SHA-1 Hash.

### 1.1 Meaning of Hash Value Verification

Evidence verified by the Hash value is not necessarily true. The forensic practitioner will hold that this evidence verified by the Hash value, therefore this evidence is not tampered. In other words, the purpose of Hash Value Verification is to make sure the forensic practitioners not tampering this evidence during the forensic

proceeding. However, the problem is raised before the beginning of forensics.

In a criminal case, the police investigate at the beginning, then move the case and evidence to the prosecutor, and finally the prosecutor will decide whether to prosecute based on related evidence. These investigative authorizations are obligated to make sure that evidence will not be tampered from being obtained to being presented in the courtroom. It is the issue of chain of custody,<sup>340</sup> and can be proved by Hash value verification. But we cannot know whether someone tampered the evidence before the time of obtaining. Therefore, facing the issue of genuine evidence, two factors should be considered. First, before obtaining, we need to consider whether the evidence related is false at the very beginning. Second, during obtaining and presenting in the court, we need to consider whether the evidence related has been improperly damaged in collecting or forensic process. In fact, after collecting evidence, the forensic practitioners usually reserve the original evidence, and duplicate one or two forensic image files for doing forensic, in case damaging the original evidence. The forensic practitioners only test and analyze the forensic image files, instead the original file. Then, they report the final result as the reference for the courts.

Therefore, Hash Value Verification is not to prove the obtained evidence is true, but to make sure the copy is totally the same as the original one. On the other hand, the effectiveness of digital forensics bases on two factors: reliability of forensic tools, research methods, and qualified experts, and the identity of the original and duplicative files.

## **2. Quality Assurance for Digital Evidence Laboratories**

---

<sup>340</sup> Chain of custody (CoC), in legal contexts, refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. [https://en.wikipedia.org/wiki/Chain\\_of\\_custody](https://en.wikipedia.org/wiki/Chain_of_custody)

Except DEFSOP, ISO/IEC 17025 provides the quality assurance for digital evidence laboratories and is widely accepted in the international community. Even in the United Kingdom and in the United States, their current approaches are also based on ISO 17025 as the main standard of quality assurance for forensic institutions. In addition, they develop supplementary instructions for specific areas, depending on the actual status.

## 2.1 Personnel

ISO 17025 requires that, the digital evidence laboratory (DEL) should make a requirement about qualification for forensic personnel working in the laboratory. This requirement must clearly explain every part of capacity requested, including education, training, experience, and practice. DEL also has to ensure workers in the laboratory are qualified. British Forensic Science Regulator follows ISO 17025 to make the requirement for forensic personnel.<sup>341</sup> In the United State, they basically follow ISO 17025, but increase three more requires. They are (1) technical staff should have the educational background comply with his position, at least having a BSc; (2) technical staff working in special area must have a certification; (3) A person in charge of presentation and report, he/she must have sufficient training, experiences, and expertise.<sup>342</sup>

## 2.2 Environment and Facilities

ISO 10725 requires that, environment and facilities should contribute to the correct execution of the test, and will not cause the test results invalid. The special condition, which will change environment or features of facilities and make an

---

<sup>341</sup> Forensic Science Regulator (2014).Codes of Practice and Conduct: for forensic science providers and practitioners in the Criminal Justice System, version 2.

<sup>342</sup> Scientific Working Group on Digital Evidence, “SWGDE Model Quality Assurance Manual for Digital Evidence Laboratories”, Version 3, Sep. 2012.

influence on the research result, should be documented. DEL should separate work area into the control zone and limit zone. The guest must be authorized and register before entering work area. The limit zone should not open to unauthorized people. The storage area should have access control and security measures, to prevent theft or interference. Regulation for storage should be sufficient to prevent loss, deteriorate, and pollute, and to ensure integrity of evidence. These conditions apply to the examination before and after the program.

### 2.3 Operating procedures

ISO 10725 requires that, every methods or approaches used must be recorded in written. Before testing, the technology and skills must be validated. If the DEL introduces a new method, they must examine this method in the laboratory and prove its efficacy and characteristics written in its description. This examination should be record. When the customer did not assign any method or technology, DEL should pick up international, regional, or national standard, or select an appropriate approach issued by famous technical organizations, or related scientific books or journals. Otherwise, DEL must choose the appropriate method assigned by equipment manufacturers. Both American and British standards follow ISO 17025 in this section.

### 2.4 Method Verification

ISO 10725 requires that, before applying in a real case or testing, methods and tools used in the laboratory should be verified. This verification may be implemented by the scientific community, such as in the case related to the standard method or methods have been published. Or DEL itself also can implement this verification under the case of methods developed by DEL itself, or the previously acknowledged method with significant changes. DEL must certify methods other than the above

suitable for the intended use. DEL can extend the requirement of verification, in order to meet the needs of the intended application or applications. DEL should record the research result, procedure used for verification, and a statement, whether this procedure and methods are compliance with intended use.

British standard basically follows ISO 10725. However, it requires that, implementing this verification must consider levels of personnel capacities, characteristic of testing, difficulties, and acceptance of this tool in majority of forensic science and criminal community. In American, they also add a requirement for general acceptance.<sup>343</sup>

### **3. Format of Forensic Report**

Forensic reports are not required to use a uniform format, but still must meet certain requirements in order to be accepted by courts. For instance, the contents of a forensic report should include: (1) professional knowledge and skills. It involves profession and qualification of forensic practitioners. (See 3.3.1) (2) Professional and reliable instrument of forensic. It considers whether these forensic tools have been accepted by courts, such as Encase, a forensic toolkit generally accepted, is reliable. (See 3.3.2) (3) Reliability of forensic method. (See 3.3.3 and 3.3.4) For example, to avoid the variation of the original digital evidence, it is necessary to make copies and use them to do forensics, comparison and reserve.

It is important to consider words as simple, clear, and understanding and easy to read for legal professionals, when writing a forensic report. Because forensic science has a strong profession and hard terminologies to understand, it is better to present these procedural or technical descriptions with illustrations, figures, tables or charts in

---

<sup>343</sup> Super note 16,17.

the courtroom.

Digital forensics has a high uncertainty. Possibly because of easy to tamper, the forensic practitioners make a definitive conclusion with difficulty. For example, the forensic practitioners need to clarify whether the defendant's computer was implanted the Trojan. They are obligated to explain the method used in forensics. It is worth to note that the method used by these forensic practitioners may not be able to find all the Trojans in the defendant's computer. Thus, they cannot say "there is a Trojan" or "there is no Trojan" in the forensic report. They need to use the words, "By using A method, we cannot find the Trojan in the defendant's computer", or "By using B method, we found a malicious program".

After finding out the Trojan, the next step is to analysis its role in this implanted computer. Even if disclosing the purpose of this implanting Trojan, it is still hard to prove that the Trojans is related to criminal activities that the defendant committed, without other digital evidence in support of the absence. In sum, the biggest drawback of digital forensic report is unable to answer in the affirmative. Forensic results are highly uncertain. Maybe it can learn from the weather report to present probability as results. However, it still remains the issue of presentation of probability as results, because there is no objective indicator to determine the level of probability.

#### **4. Criminal Defense Challenges in Computer Forensics**

Scholars<sup>344</sup> propose several criminal defense challenges in computer forensics, such as (1) how to prove the defendant intentionally possess the digital contraband (such as child pornography); (2) how to prove the defendant is lack of knowledge.

---

<sup>344</sup> Rebecca Mercuri, Criminal Defense Challenges in Computer Forensics, in S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 132-138, 2010; Agnes Kasper and Eneli Laurits, Challenges in Collecting Digital Evidence: A Legal Perspective, in T. Kerikmäe, A. Rull (eds.), The Future of Law and eTechnologies, DOI 10.1007/978-3---319-26896-5\_10.

Usually lack of knowledge is no excuse in legal system, because most of time it can be proved by circumstantial evidence; (3) Confusing time Stamps. For example, the forensic practitioners forget explain the time zone and daylight savings time; (4) Prosecution may impede or observe the defendant discovery process; (5) Defense is unable to authenticate materials and copies. For digital materials, many law enforcement labs have standardized on the use of MD5 and SHA1 hashes for proving duplicates of evidence the same; <sup>345</sup>(6) Proprietary software tools. As mentioned in part 3.3.2, the reliability of forensic tools is very important, which can be thought the key of the whole forensic procedure; (7) Exculpatory evidence may be uncollected, withheld or destroyed. Based on easy to loss of social media evidence, the police may destroy the evidence for the defendant to reduce the difficulties to charge the defendant. It is just a hypothesis. ; (8) Access to legitimate service can carry a high degree of risk. It means the digital service we use every day, like email, social networking sites, file sharing etc. is not only an object of criminal investigating, but the source pool for business investigation, both of which threaten our privacy. These challenges provide us a chance rethinking the current systems regulating social media evidence.

## **Summary**

We can find that, for this digital forensic science, the most important part is to ensure that the identity between obtained evidence and original evidence is the same. To make sure the forensic results, they try to build SOP, make records, and produce documents. This is totally the scientific methodology. Through SOP and records, we can represent the same forensic procedure happened before, and also we can rebuild the crime scene. Besides, we also can find the whole scientific communities still

---

<sup>345</sup> R. Mercuri, id at. 135.

follow the general acceptance principle. The scientific knowledge is based on peer review, which is also accepted by other academia communities and becomes the general rule for knowledge production.

Unlike the science, legal system doesn't put too much concern on reality of this social media evidence. They have already accepted the premises; scientific evidence in principle must be true. Judges allow the evidence into courtroom by law, but adopt it to make the argument by their knowledge. In Chapter 2, we have discussed social media evidence in court. First, we saw what kind of regulations apply for social media evidence, and discuss the problem inside. Second, we discussed the concept of expert witness, which is the real way to show digital evidence, social media evidence or scientific evidence in court. That would be interesting to dig from history and from comparative law. Then we reviewed the whole procedure, from information to evidence, and analysis reasoning of judgments about social media evidence.

## References

1. Adkins J (2011), Law Enforcement Guide to Social Media, Special Research Report, p. 1.
2. Agnes Kasper and Eneli Laurits, Challenges in Collecting Digital Evidence: A Legal Perspective, in T, Kerikmäe, A. Rull (eds.), The Future of Law and eTechnologies, DOI 10.1007/978-3---319-26896-5\_10.
3. Association of Chief Police Officers, "Good Practice Guide for Digital Evidence", 2012.  
<http://www.dcs.kcl.ac.uk/staff/richard/7CCSMCFC/ACPO-gpg-digital-evidence-v5.pdf>
4. Carolyn Elefant, The "Power" of Social Media: Legal issues & Best Practices for Utilities Engaging Social Media, 32 ENERGY L. J. 1 (2011)
5. danah m. boyd & Nicole B. Ellison (2008), Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication. 13: P. 211.
6. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd edition, Academic press: USA, 2011, pp.187-190.
7. Forensic Science Regulator (2014).Codes of Practice and Conduct: for forensic science providers and practitioners in the Criminal Justice System, version 2.  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/351197/The\\_FSR\\_Codes\\_of\\_Practice\\_and\\_Conduct\\_-\\_v2\\_August\\_2014.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351197/The_FSR_Codes_of_Practice_and_Conduct_-_v2_August_2014.pdf)
8. Graham C. Lilly, An Introduction to the Law of Evidence, 2nd ed., West

Publishing, N.Y., 1987.

9. I-Long Lin and Yun-Sheng Yen, 2011, "VOIP Digital Evidence Forensics Standard Operating Procedure", International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No.1.
10. Inikpi O. Ademu, "A New Approach of Digital Forensic Model for Digital Forensic Investigation", International Journal of Advanced Computer Science and Application, Vol 2, No.12, 2011
11. J. Jordaan, "A Sample of digital forensic quality assurance in the South African Criminal Justice System", Information Security for South Africa (ISSA), pp. 1-7, 2012.
12. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, 2006, Guide to Integrating Forensic Techniques into Incident Response.  
<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
13. Markus Huber, Martin Mulazzani, Manuel Leithner, Sebastian Schrittwieser, Gilbert Wondracek, Edgar Weippl, 2011, Social Snapshots: Digital Forensics for Online Social Networks, ACSAC '11 Proceedings of the 27th Annual Computer Security Applications Conference.
14. National Institute of Justice (2008).Electronic Crime Scene Investigation: A Guide for First Responders. <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>
15. Palmer, G. (2001), "DFRWS Technical Report: A Road Map for Digital Forensic Research," First Digital Forensic Research Workshop (DFRWS), New York: Air Force Research Laboratory, pp. 14-31. available at <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

16. Paul C. Giannelli & Edward J. Imwinkertied, Scientific Evidence, Michie Co., 1993.
17. Rebecca Mercuri, Criminal Defense Challenges in Computer Forensics, in S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 132-138, 2010.
18. Richard Adams, Val Hobbs, & Graham Mann, The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice, Journal of Digital Forensics, Security and Law, Vol. 8(4), 2013, p. 25-48, available at <http://ojs.jdfsl.org/index.php/jdfsl/article/view/110/198>
19. Science and Technology Committee (2004).Forensic Science on Trial: Seventh Report of Session 2004–05. <http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf>
20. Scientific Working Group on Digital Evidence, “SWGDE Model Quality Assurance Manual for Digital Evidence Laboratories”, Version 3, Sep. 2012. <https://www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20QAM%20for%20Digital%20Evidence%20Laboratories-v3.0>
21. Thaddeus A. Hoffmeister, 2014, Social Media in the Courtroom: A New Era for Criminal Justice?.
22. U.S. Department of Justice, 1999, Forensic Examination of Digital Evidence: A Guide for Law Enforcement. <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
23. Wang, Shih-Jeng, Lin, Chu-Hsing & Tso, Ray-Ln (2013), Digital Forensics and Security in Applications of Computer and Mobile Systems, DrMaster Press,

Taipei: Taiwan.

24. Wilson C, Boe B, Sala A, Puttaswamy Krishna P. N., & Zhao Ben. Y. (2009),  
User Interactions in Social Networks and their Implications, ACM EuroSys 2009,  
p. 1.

## **Chapter 4 SME, A Process from Information to Evidence**

As a temporary conclusion, this chapter explains that social media evidence is not a fixed concept, but a process from information to evidence at court. Its importance is to be evidence accepted by the court. Second, this chapter will discuss evidentiary issues of social media evidence and suggest that the key issue is the “connection”. In a criminal case, the court's argument is to connect the facts of the crime and the defendant sued by the prosecutor. This is quite difficult. However, the emergence of social network sites seems to provide a breaking point for the court: for example, the link between Facebook account and its registered e-mail. Meanwhile, the characteristics of SME (vulnerable to tampering and possible to recovery) also make it difficult for the court to link the real world and the virtual world. In addition, although the legal system and the scientific communities are in the pursuit of fact finding, unlike scientific communities taking fact finding as the ultimate goal, the legal system in the punishment of criminals, not only considers the facts of the crime, but also premeditates the impact of criminal policy on society.

### **1. Comparison between Legal and Technical Systems**

After the discussion of Chapter 1, 2 and 3, we can find that SME is a floating concept: different from the traditional evidence of the fierce knife, corpse, SME because the investigators or the defendant how to use and have different evidence Way, for example, when the defendant was accused of libel, the face of his face with attack or insulting text of the post itself is evidence, the current legal system are recognized as printed documents for the evidence. However, when the defendant argued that the Facebook account was created by someone else or his account was hacked, the defendant may have made a connection to the IP location or other location evidence to exclude the possibility of issuing their own. This is the reason for the

nature of SME information. How information is translated into legal evidence can be divided into technical and legal channels in two ways, that is, the SME in this paper, in fact, refers to the information into evidence of a process.

### 1.1 Technical Process to Form the Social Media Evidence

Computer evidence processing is mainly through the inspection of the computer's technical methods, backup, inspection and analysis of computer crime evidence, and by the law enforcement agencies standard processing procedures to protect the computer evidence to serve as evidence of court proceedings. In the computer forensics, practitioners first should be important before the backup data to complete the preservation of evidence. All data must be backup in necessary situation. Computer forensics should be carried out in the backup data non-destructive identification; if necessary, the original data should be analyzed, but the identification process to be detailed records or video certificates. Computer evidence processing procedures should pay attention to save evidence, test evidence, analysis of evidence and results presented.

### 1.2 Legal Process to Form and Use the Social Media Evidence

General speaking, materials or information will be examined in a procedure before they comes out as evidence at trial. A foundation, used in determining or actually constructing the past fact, should be based on evidence which is filtered by the criminal proceeding and then get admissibility. This filter mechanism can filter undiscoverable, irrelevance, or inadmissible materials, based on rule of law. On the other hand, through this filter mechanism excluded such evidential materials, evidence being discoverable, relevance, and admissible will be introduced at trial, and will be used to construct the past fact. This is the legal approach to secure purposes of the criminal and criminal proceeding by filtering one element and another.

More specifically take the Taiwan Law as example, the evidence of the crime

must be not prohibited to use (negative conditions), investigated lawfully through the strict proof (positive conditions), and then the evidence is considered admissible by court, which can be used as the basis of judgements in this case. Evidence that is not prohibited must qualify both with positive conditions, so that it can finally get the admissibility. The positive condition, in a nutshell, is the principle of strict proof. In other words, evidential materials will finally get the admissibility only through the investigation procedure by strict proof, and therefore it can be the foundation to identify the facts of the crime.

### 1.3 The Comparison

We can find that, for this digital forensic science, the most important part is to ensure that the identity between obtained evidence and original evidence is the same. To make sure the forensic results, they try to build SOP, make records, and produce documents. This is totally the scientific methodology. Through SOP and records, we can represent the same forensic procedure happened before, and also we can rebuild the crime scene. Besides, we also can find the whole scientific communities still follow the general acceptance principle. The scientific knowledge is based on peer review, which is also accepted by other academia communities and becomes the general rule for knowledge production.

Unlike the science, legal system doesn't put too much concern on reality of this SME. They have already accepted the premises; scientific evidence in principle must be true. Judges allow the evidence into courtroom by law, but adopt it to make the argument by their knowledge.

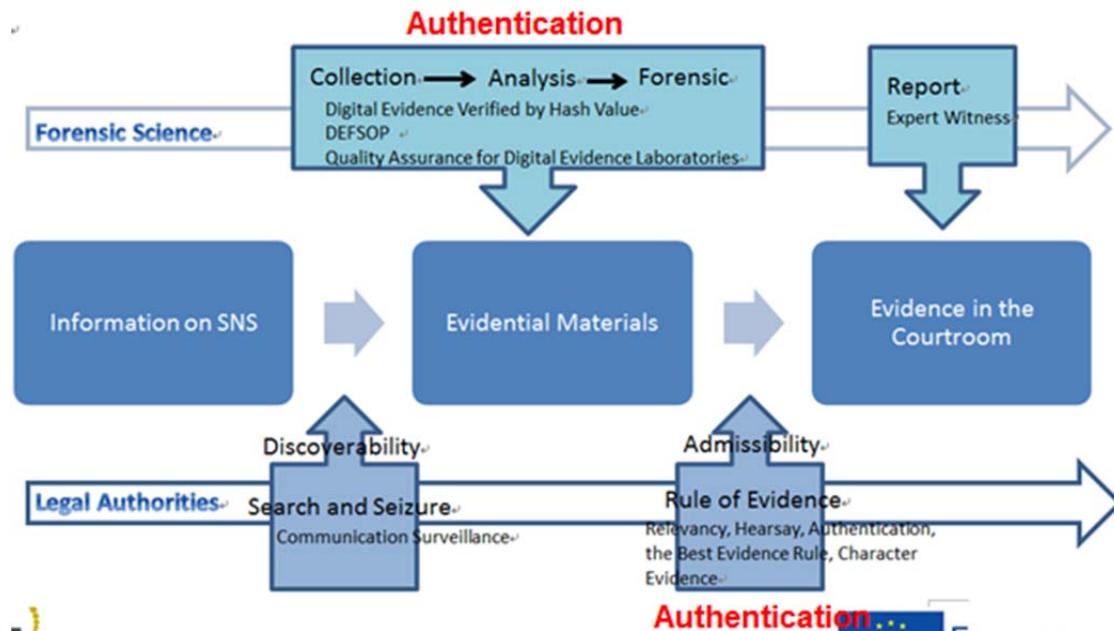


Figure 10 the comparison of forensic and legal obtaining evidence process

## 2. Arguments in the Court

When an SME is submitted to court, considering characteristics of these social media evidence, e.g. easy to be copied, deleted, tampered and transmitted, both parties will naturally object to the evidence against them. The defendant or the prosecutor will argue for the following points, in order to exclude this social media evidence, also because of these characteristics of these social media evidence.<sup>346</sup>

### 2.1 Disputes

At present practice in the litigation, disputes of evidence ability often occur, mainly in the following situations:

2.1.1 When the social media evidence has been formed, whether the computer hardware and software was normal.

How does the electronic hardware and software, such as computer machinery,

<sup>346</sup> Here is cited in the proceedings may occur for the evidence of the claims of the classification is mainly from Taiwan's legal practice from the order. Due to the characteristics of SME, I believe can also be used as a reference for other legal claims. For information on Taiwan's digital evidence of attack and defense, please refer to Hsien-Ming Chiu & I-Long Lin, The Offense and Defense Countermeasures of Digital Evidence in Court, Journal of Information , Technology and Society, Vol. 7, No. 1, 2007, P.55.

operating system or application, work in the normal state when the electronic evidence is formed, if the operation is abnormal, will it affect the correctness of the electronic evidence? For example, the defendant may defend the operating system of the computer involved in the use of the system is unstable, there are loopholes<sup>347</sup>, resulting in a record error; or external interference<sup>348</sup>, so that the generated electronic records recorded in the wrong record of its IP position, to the defendant was misunderstood Permeate the server without permission.

#### 2.1.2 Obtaining evidence is illegal.

Whether the law enforcement officers are in compliance with the laws and regulations of the electromagnetic record,<sup>349</sup> whether they have obtained the electromagnetic record by means of illegal intrusion into the computer of others, the appropriateness of intercepting others' e-mails or chat records on the Internet, and even the type of cases undertaken or transferred in line with the authorities in charge,<sup>350</sup> are the focus of discussion.

#### 2.1.3 There is a dispute about the legally preserved and identified.

The point of contention is whether the social media evidence is legally preserved at the time of the incident or after the incident and presented to the court in the appropriate form. The other point is whether the evidence has been altered or forged, if the social media evidence is made for the victim or the teller.

#### 2.1.4 The actual production (criminal) person is questioned.

Electronic records, such as computer records, are represented by "0" and "1" digitized electromagnetic records, unless the user uses a specific identification method, such as public and private key encryption, electronic signature, etc., only from the

---

<sup>347</sup> (95) Shan Zhi No. 2214 Penal Judgment (2006) of Taiwan High Court.

<sup>348</sup> (94) Jiao Sheng Zhi No. 288 Traffic ruling (2005) of Taiwan Taipei District Court.

<sup>349</sup> (91) Su Zhi No. 1028 Penal Judgment (2002) of Taiwan Banqiao District Court.

<sup>350</sup> *Id.*

electronic evidence itself can not Directly prove the identity of its creator. On the contrary, the news of the development of the media, hackers implanted Trojans to others computer as a springboard for the news of the news of repeated news, so the parties to the proceedings are often against the computer hacked into the Trojan horse, was used as a tool for the springboard;<sup>351</sup> Hacking after the use of its computer to spread the bad reputation of others e-mail; or wireless network is not encrypted and was stolen.

#### 2.1.5 Social media evidence has been tampered.

Such social media evidence must be excluded if the court or litigation proves that the electronic evidence has been tampered with.<sup>352</sup> However, if only the possibility of tampering with the computer system is confirmed, it is not sufficient to consider that the electronic evidence is not admissible and should be excluded.<sup>353</sup>

#### 2.1.6 The printout or the representation of social media evidence may show a sense of error.

Electromagnetic recording of "0" and "1" of the combination of magnetic gas, stored in the carrier, cannot understand the meaning of human through the perception, this time will be displayed on the computer screen or printed for the paper for reading, the general salty Recognize the more appropriate way. But the electromagnetic record in the conversion process, with the display card, screen computer, memory, storage carrier, CPU, printer and other hardware and operating systems, applications and other software interaction between the interaction. So there may be an error when the electromagnetic recording is converted to a screen display or paper document. For

---

<sup>351</sup> (94) Shan Su Zhi No. 564 Penal Judgment (2005) of Taiwan High Court.

<sup>352</sup> (94) Shan Su Zhi No. 564 Penal Judgment (2005) of Taiwan High Court, (92) Su Zhi No. 1411 Penal Judgment (2003) of Taiwan Taipei District Court, (91) Yi Zhi No. 2968 Penal Judgment (2002) of Taiwan Banqiao District Court.

<sup>353</sup> Although the possibility, that this computer system has been changed, does not affect the admissibility of evidence, the court is able to weigh the value of the evidence by judge's confidence to prove its value.

example, want to print the page, but there are garbled or grid; or if the normal view of the PDF file on the screen, printed in some places when there are garbled, etc. are common computer users common situation.

## 2.2 Strategies

After finishing the above points, we will be able to draw the following classification, and as a court activities to find out their attack countermeasures and defense countermeasures.

### 2.2.1 Source of evidence

Social media evidence can be made by anyone with any computer at any time. So it is necessary to examine the source of the evidence, in order to clarify where this evidence is extracted from and its relationship with persons involved in this case. When one of the parties in the litigation proposes evidence about the source, this party wants to prove the relevance of the case and the person, such as the social medial evidence from someone's computer, storage equipment, etc. Therefore, the opposition party will argue that social media evidence presented in the court room has no relevance with the person in this case. They might argue that this evidence is not from the case related to the parties. Meanwhile, the party has two strategies to strengthen his defense: first, to prove the source according to the testimony form who obtained this social media evidence; and second, to prove the source by other reinforcement evidence which can prove the source of social media evidence is related to the person of this case.

### 2.2.2 Acquisition of evidence

Legally collecting evidence is the premise having evidence admitted by court, so it is necessary to check the way in which the evidence is obtained. In the case of social media evidence, evidence presented at court is from the websites, e-mail, storage equipment, etc. The opposition party will argue that evidence at court was

from illegal acquisition. For example, the content of the conversation on Facebook Messenger filed by the prosecutor is made by fraud. The prosecutor pretended as a friend and set a trap, in order to obtain evidence of the crime. Meanwhile, the prosecutor has two strategies to strengthen his argument: first, to submit a written order issued by the court for approval of the communication, if there was the network communication surveillance; and second, to disclosed methods and procedures for collecting digital evidence.

### 2.2.3 Authorship of social media evidence

No matter it was produced by anonymous or named, social media evidence cannot be identified in the same way as the documentary evidence which can be identified by the author's handwriting. So it is necessary to examine the relationship between the author of the social media evidence and the person in question. In this case, what to be confirmed is social media evidence is associated with someone in the content, such as the intimidation content was sent by someone's Facebook Messenger, or The contents of the Facebook posts have mentioned the relevant person, or the author is the case related person. The opposition party definitely will argue that social media evidence presented at court was not made by the claimed person. For example, the prosecutor sued the defendant intimidating the victim and presenting conversation between the defendant and the victim on Facebook Messenger as evidence. The defendant objected this evidence and claimed that is not his account or someone hacked his account wrote that threatening letter. The defense measures in this case should be collecting other social media evidence and evidence other than social media evidence, such as real evidence or physical evidence to strengthen the tie between the threatening letter and the defendant in this case.

### 2.2.4 Digital evidence format

Because the digital evidence format is diverse, the method of displaying its

contents is different. It is necessary to check the format of the original digital evidence, and determine whether the original format of the digital evidence is faithfully to present the content of evidence. In this case, what should be confirmed is submitted social media evidence is in a state where the content is available to access. The opposition party will argue that the format of submitted social media evidence is non-original (storage) format, which will affect its identity with the original information. As defense measures, the party will call expert witnesses, introduce the internet forensics, or please the court to make the inspection, in order to prove that the change in the format of social media evidence didn't change the contents of this evidence.

#### 2.2.5 Digital evidence content

Since social media evidence as the digital evidence has the characteristic of alteration or deletion with no trace, it is necessary to check whether the contents of the original digital evidence are consistent with the contents presented at court. In this case, it is to be confirmed that contents of the social media evidence can be directly proved to be confirmed facts, such as the conversation on Facebook Messenger, posts involved in defamation or hate speech on Facebook, etc. The opposition party will argue that the presented content of social media evidence was altered or partly deleted, so that it does not match the content presented on the social network sites. As defense measures, the proposed party can introduce internet forensics to prove that the contents of the social media evidence has not been added or deleted; or the party can call the expert witness or testify by self to explain the whole process from extracting information from social network sites to present evidence at court.

#### 2.2.6 The time when social media evidence was established

The establishment time, the modification time and the access time of social media evidence can be used to check whether the evidence of the court has been changed.

Usually the matter related to time to be confirmed is the intersection between the time at which the evidence is established and the time of important facts in this case, such as where the party is located when photos were posted on Facebook. For this proposition, the other party defends with other evidence to prove that social media evidence is made with the relevant parties in the case or with other evidence to prove that when establishing the social media evidence, the parties have the intersection with the time and space.

#### 2.2.7 The way that social media evidence presented at court

Social media evidence is presented in a variety of ways, and the most convenient way to view this digital evidence is playing the recording files in court or print the content of social network sites out. At present legal practice, the court prefers to introduce printouts of the social media evidence as the method of investigating evidence. The printout is the result that the social media evidence was output by the printer, which may be questioned the original of evidence. Therefore, it is necessary to examine the way that make social media evidence has been faithfully presented the original evidence of digital content at court. The party who submitted printouts of the social media evidence will face these objections that contents of the printout are different from the original content of the social media evidence, or the original social media evidence of the printout no longer exists. At this time, the party may request the court make the inspection that the court can use the computer to access the content of social network sites comparing with contents of the printout to determine their consistency; or the party may submit other evidence to prove contents of the printout are real when the original evidence was gone.

In summary, we can sort out the digital evidence will face the challenge is nothing more than (as Figure), one for the parties to question the digital information has been tampered with, destroyed, and the original different. As the digital evidence

with no trace of the characteristics of the addition or deletion, court presented to the court of the evidence cannot be ruled out the destruction of the possibility of modification. The second is to question the reliability of computer programs that generate digital data. Computer users know that computer software programs often appear bug, need to constantly update the software, debugging, and computer programs written by people, the results can be designed by the program designer cannot rule out the results of computer calculus for the user deliberately control The next result. The third is to question the identity of the author, the evidence of this factor has the identity of the creator is not easy to determine the characteristics, even if the evidence can be proved to be evidence of the facts, but in the case of individualization of the evidence, the face of this negative The parties to the evidence will argue that any person is likely to produce exactly the same amount of evidence.

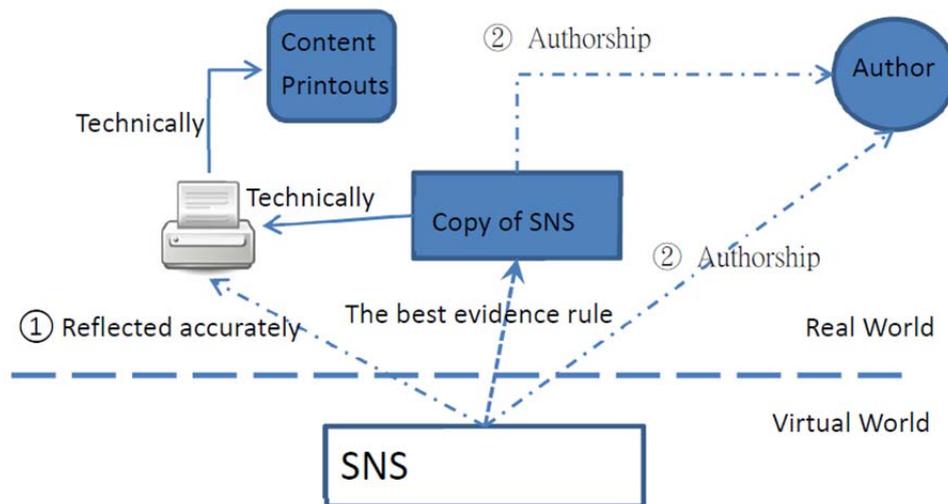


Figure 11 analysis of SME legal issues

### 3. The Original

In the case of digital evidence, there will be a printed copy or copy of the use of the problem, our law is not expressly provided, which can refer to the United States federal evidence law the best evidence of the principle, according to the Federal Act

1001 (3) The information is stored on a computer or similar equipment, its printed material or other visually readable output and showing the correct response to its information, as well as the original; section 1001 (4) provides for the original electronic reproduction. Into the same thing, that is, a copy. In accordance with articles 1003 to 1005, he shall not be able to obtain the original intentionally, or shall not be deemed to be held by, The official record, etc., the parties did not have to put forward the original, if only to make a copy or other evidence still have evidence of 497. In the case of photographs, photographs may be evidence of a copy of the evidence or a separate copy of the evidence, such as a copy of the evidence, in the case of evidence, the relationship with the transcript of the document, transcripts. The use of the Anglo-American law must comply with the principle of the best evidence, non-proof of the original cannot be made, not to photo as evidence, and to find the real, and should be proven when the photo was correct.

At present, the consensus of the legal profession, with digital evidence as a documentary evidence, although there is no best evidence of the provisions of the law, this issue can refer to the provisions of the United States law, stored in the digital carrier data, by computer and other equipment. Printed or exported, if the contents of the digital data can be accurately reflected, that the print or other output is the original, as evidence to prove the facts of the crime.

#### **4. Identity**

The identity of the evidence refers to the procedure that is presented in the court to prove that the evidence of the evidence and the original evidence must be consistent, that is, whether there is evidence of the use of the evidence, before the presentation of the evidence, the applicant must prove the number. Evidence conforms to the authenticity requirements. Article 901 of the Federal Act provides proof of the authenticity of the evidence, and can be applied to digital evidence. To prove the

identity of the evidence, that is, the control of the evidence chain, in the digital identification to be divided into two levels to talk, one for the entity evidence, the other for the digital evidence contained in the digital data; because the digital evidence is abstract, easy Destruction, and so on. Therefore, the identity of digital evidence is often the focus of litigation attack and defense, digital identification personnel in order to avoid unnecessary disputes, coupled with digital evidence can be without loss of reproduction and other characteristics, it is usually a copy of the original way to produce copies of evidence , And a copy of the evidence to carry out identification work, to avoid changes in the original and the original seal for third-party re-inspection; so "the original cannot be changed" to become the highest standards of personnel and judicial personnel and the identification of the highest iron law.

From the discussion of Chapter 2 can be drawn, issues are raised: how to representing information on SNS accurate (the main problem is authentication), and whether it can use to prove in technology. These questions will be discussed further in Chapter 5.

## **5. Authorship**

Computer information is only 0 and a combination of handwriting with the traditional instruments can be identified by handwriting identification of the identity of the producer is different, Moreover, the characteristics of network anonymity, many network technology allows users to anonymous way Internet access, such as anonymous e-mail, or by code into the chat room without having to provide a real name. Therefore, when the law enforcement agency to the electronic evidence to the suspect to tell, the suspect is often questioned its authenticity, advocated by the electronic evidence produced by others, is also about the characteristics of digital evidence mentioned in the "human nature is not easy to determine ". In addition to the

"human nature is not easy to determine" mentioned in the hidden information to reinforce the problem of difficult to confirm the owner of digital evidence, but also referred to the application of ADSL network lines, may not be real Internet users, etc., in this also raised some questions The situation of the identity of the digital data producer. Among them, the most common digital information is undoubtedly an e-mail, clever criminals can easily change the letter of the header information, in the name of others or anonymous way to show the sender, was received with "god@heaven.com" for the send The e-mail of the person, which is called "God's letter" (Godmail). The reason for this is that the current e-mail architecture is too old and there is no universally effective mechanism to verify its authenticity, so when you receive a letter from Bill Gates to teach you to get rich quickly, It is not necessarily Bill Gates to send, and perhaps even Bill Gates have received this letter, of course, not to mention the name of God sent the letter of God. For those who can easily tamper with the sender, through the letter content (non-web e-mail box) IP address to trace the source of the letter. But the IP address may not be true, and it can still be used to disguise its true IP address through special techniques such as IP spoof or switch service. In addition, there are many free services on the Internet, such as Yahoo's free e-mail box, this free service in the user identity authentication mechanism is very weak, often cannot represent the actual identity of the actual user, even if the need for identity card number, still Through the identity card number generator, easy to produce in line with the coding logic of the identity card number, and to cover up their true identity. These questions will be discussed further in Chapter 6.

## **Reference**

Hsien-Ming Chiu & I-Long Lin, The Offense and Defense Countermeasures of Digital Evidence in Court, *Journal of Information , Technology and Society*, Vol. 7, No. 1, 2007, p. 53-64.

## **Chapter 5 Copy the Virtual World: Authenticity of Social Media Website Printouts**

Different from traditional objective evidence, social media evidence has its own characteristics with easily tampering, recoverability, and cannot be read without using other devices (such as computer). Simply taking print-out from social network sites must be questioned its original identity. When the police search and seizure digital information, a common way they use is to directly print out digital data obtained and ask the signature of the parties at the presence, without taking original digital data back. In addition to the issue on its original identity, this conduct to obtain evidence may have another two results. First, it will easily allege that is tampering evidence because the police wanted to frame the suspect and falsified evidence. Second, it is not easy to discovery hidden information. The core evidence associated with crime may not appear in the contents of files. Through discovery the original file, data related to the file, such as the original producer, creation time, modification date, and even GPS location display, can be revealed from hidden information. Therefore, how to show this kind of evidence in the courtroom will be arguably the most important task for ruling social media evidence.

In this chapter, we will discuss printouts and the authentication issue. First the printout is identified as the very common mean to present the social media evidence in the courtroom and its authentication is the core issue at trail. The construction of the authentication issue involves two questions: whether this printout was accurately reflected the content of the social network website, and who the real author is. The legal approach will be discussed in section 2 and a case study is used to show the whole consideration by courts. Although the main stream believes courts take different approaches, the Maryland approach and the Texas approach, to solve this

printouts issue, we consider there is no difference between these two approaches, but rather take into account issues of accurate reflection and the authorship. Furthermore, we consider this printout issue as the question, how to prove  $A=A'$ . The most common way to make sure the accurate reflection of the social media information is the image copy. However, even though threshold to access this technical image copy is low, it is rarely to find the prosecution using this technology to printout the social media information. Instead, the prosecution prints the social media evidence directly. They have the solid belief in technical accuracy, reliability and trustworthiness. Besides, Law's knowledge of science is actually depending on the judge's education and experiences. To combination these two factors, we can conclude that the fact/truth that legal system pursues is a relative, persuasive facts.

## **Section 1 Printouts and the Authentication Issue**

### **1. The Very Common Mean to Present in the Courtroom**

Printouts or screenshots is the very common mean to show social media evidence in the court room. Usually the prosecution just needs to find the needed social network sites, select the wanted contents, and print them out. As the documentary, printouts are presented in the courtroom as the evidence to prove the constructed case.

### **2. The Problem Is Authentication**

The problem is that, the defendant will challenge the qualification of this evidence: first is the discoverability of printouts. It is related to the investigative means of obtaining the evidence. In the case of social media evidence, issue of violation of privacy guaranteed by the fourth amendment often arises, such as whether the social network sites is as the public domain, whether the investigative authorizations can use a subpoena to obtain information on the social network sites instead of a warrant, or whether the subject's consent can justify this search without warrant (chapter 2); second, the admissibility of this evidence. Usually the arguments will be focused on the authentication issues. Although there are other factors will affect the admissibility of evidence, issues of authentication is the main point in American legal system.

### **3. The Construction of the Authentication Issue**

We can illustrate the construction of issue of printouts based on judgments and literatures in American legal system. According to Rule 901, *“To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”*, the courts divided authentication requirement into two factors in the case of social media evidence, that is, (1) *“Printouts of web pages must first be*

*authenticated as accurately reflecting the content and image of a specific webpage on the computer,”* and then (2) in order to be relevant, the printout “*must be authenticated as having been posted by that source.*”<sup>354</sup> The judge acts as a gatekeeper in determining whether the party offering the evidence has fulfilled this requirement of relevance.<sup>355</sup>

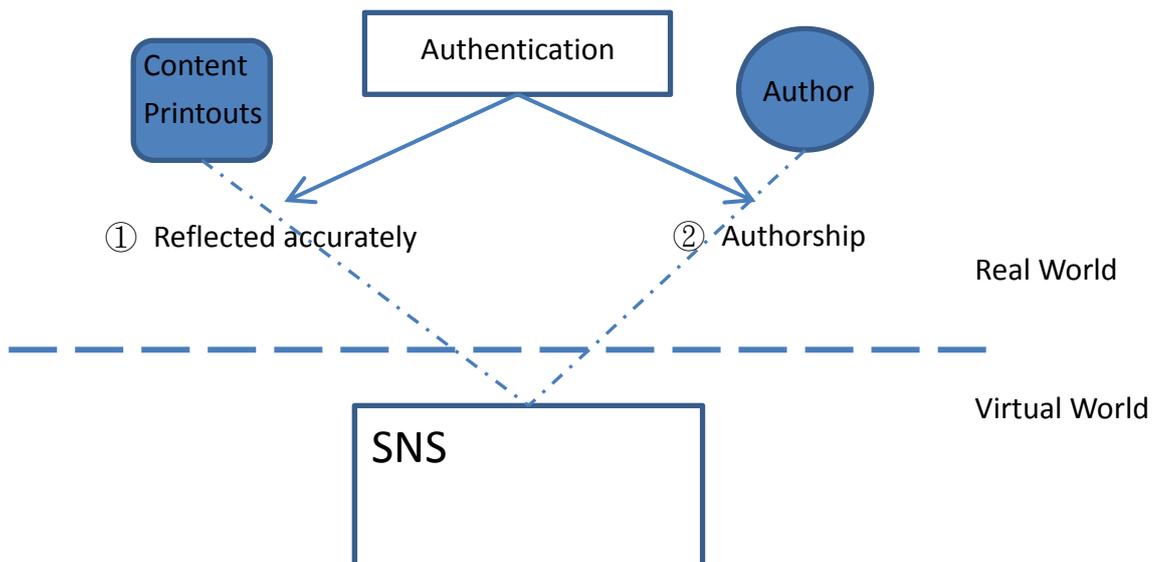


Figure 12 legal issues of social media evidence

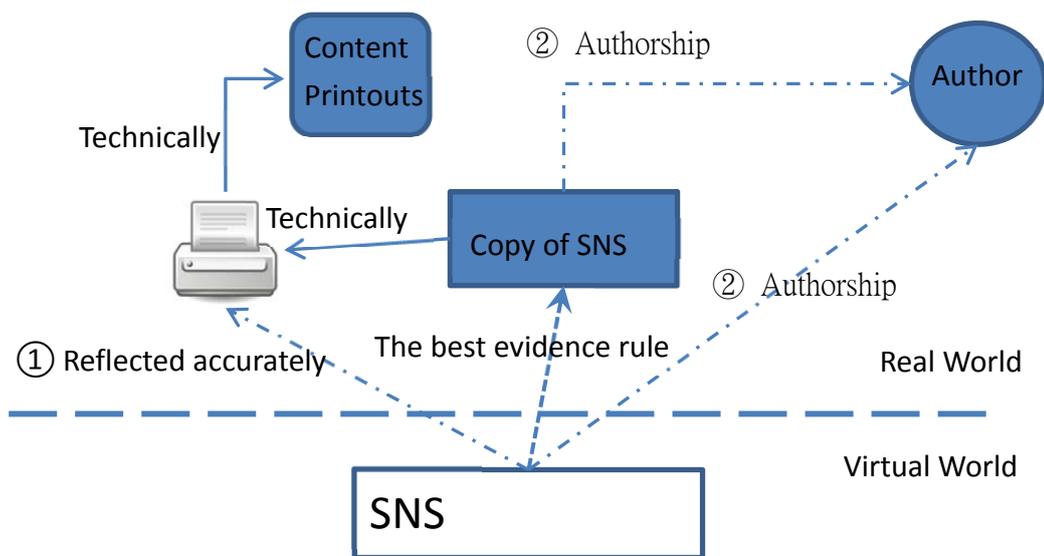
However, when we add the technical factor inside, this construction can be drawn in more detail as follow. Actually the printouts cannot produced themselves, thus the prosecutions usually print social media evidence out by using a printer, or they may ask forensic practitioners to assist them to extract information from social network sites (SNS) and transform it as evidence to present in the courtroom. We have discussed the basic way and forensic procedure in Chapter 3, and then how to reflect the printouts accurately will be discussed in the next section. It is related to the best evidence rule. Besides, even printing by a printer, there is still an issue, which is the court’s attitude to believe the technology. Accepting the computer files as the effective

<sup>354</sup> MCCORMICK ON EVIDENCE § 221 (Kenneth S. Broun et al. eds., 7th ed. 2014).

<sup>355</sup> FED. R. EVID. 104(b).

evidence is not absolute. The courts had discussions around 1990's. Therefore, we will analysis approaches discussed then to solve the issue of computer printouts as evidence, trying to find the useful arguments to rethink the issue of social media evidence as printouts.

As for the issue of authorship, it usually goes along with the Trojan defense, which we will discuss more in Chapter 6. In American legal system, the courts are developing two different approaches to solve this printout issue (including accurate reflection and authorship), the Maryland test and the Texas test. We will discuss in the next section.



## Section 2 Solution in Legal Approach

### 1. The Basic Rule

According to the rules of evidence discussed in Chapter 2, information from the social network site must be discoverable and admissible, and then it becomes evidence (social media evidence), which can be presented in front of the jury as the base to build the truth. Thus, a lawful obtained printout of the social network site, which can be accepted by the court, still need to be reached the admissibility request. This request includes three elements, which are to be relevant, to be authentic, and not to be the hearsay. It is not hard to make the relevancy of evidence at issue, but printouts from a webpage commonly draw hearsay objections.<sup>356</sup> Courts, however, typically apply the rationale that such printouts are not “statements”, but are rather merely images and text found on the websites.<sup>357</sup> Furthermore, among these three elements, the main admissible issue of this printout evidence is authentication.

The courts in American legal system basically think that, the request of authentication, regulated in the Federal Rules of evidence 901, simply asks that the evidence provider presenting the evidence make a prima facie<sup>358</sup> showing of genuineness, and remains space to the fact finder to decide authenticity.<sup>359</sup> Authentication of digital information can be accomplished by direct proof, circumstantial evidence, or a combination of both.<sup>360</sup> In Federal Rule of Evidence 901 (b) (1), the party can authenticate the evidence by “*testimony that a matter is*

---

<sup>356</sup> Browning, John G., Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites, 14 SMU Sci. & Tech. L. Rev. 465, 480.

<sup>357</sup> Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002).

<sup>358</sup> In the American legal system, “prima facie” in the pretrial means all evidence provided by the prosecution are presumed to be admissible, and are not questioned their reliability. That is, “The test is that was there ‘some evidence’ which, if unexplained would warrant a conviction by a trial jury”. Rideout v. Superior Court, 432 P.2d 197 (Cal. 1967), dissenting.

<sup>359</sup> Fed. R. Evid. 901, and Telewizja Polska USA, Inc. v. Echostar Satellite, No. 02 C3293, 2004 WL 2367740, at \*6 (N.D. Ill. Oct. 15, 2004).

<sup>360</sup> Browning, *supra* note 356, 479.

*what it is claimed to be*".<sup>361</sup> For example, if the person in question acknowledged his screen name, admitted authorship, and admitted to printing the instant messages from his computer, then this instant message from the social network sites were authenticated by direct proof according to Federal Rule of Evidence 901 (b) (1). Besides, in Federal Rule of Evidence 901 (b) (4), the evidence can be authenticated by "*appearance, contents, substance, internal patterns or other distinctive characteristics taken in conjunction with circumstances.*"<sup>362</sup> For example, the instant message was authenticated not only by the defendant and other witnesses confirming his screen name, but also by the fact that when a meeting was arranged with the screen-name user, the defendant showed up to the arranged meeting.<sup>363</sup> That fact is called circumstantial evidence regulated in Federal Rule of Evidence 901 (b) (4).

In this authentic issue of website printouts, courts vary on the extent of testimony required by Federal Rule of Evidence 901 (b) (1).<sup>364</sup> Some courts<sup>365</sup> require that testimony must point out who actually posted that information on the social network site. Such testimony can be proffered through an affidavit or a statement from someone with personal knowledge, such as the website's webmaster. Some courts require a sufficient testimony from the person who created the printout being offered that the image "*actually reflects the content of the website and the image of the page on the computer at which the [screenshot] was made.*"<sup>366</sup> Some courts in between the two ideas require different evidence depending on the circumstances. Sufficient circumstantial indicia of authenticity are recognized by courts, such as time and date stamps, and web address, to support a reasonable juror in the belief that the

---

<sup>361</sup> Fed. R. Evid. 901 (b) (1).

<sup>362</sup> Fed. R. Evid. 901 (b) (4).

<sup>363</sup> United States v. Tank, 200 F.3d 627, 630-31 (9<sup>th</sup> Cir. 2000).

<sup>364</sup> Browning, supra note 356, 479.

<sup>365</sup> In re Homestore, Inc. Sec. Litig., 347 F. Supp. 2d 796, 782-83 (C.D. Cal. 2004).

<sup>366</sup> Toytrackerz LLC v. Koehler, No. 08-2297-GLR, 2009 WL 2501329, at \*6 (D. Kan. Aug. 21, 2009).

documents were as they purported to be.<sup>367</sup>

To authenticate contents of the social network site, the party offering the printouts as evidence must introduce sufficient evidence for a reasonable jury to conclude that the exhibit is what the sponsoring party claims it to be. At a minimum, the testimony from the person who performed the online research on the social network sites and printed the social media pages should be proffered. Scholars give this testimony a specific content, which should describe when and how the page was found, describe the circumstances of the search, and verify the copy accurately reflects what was viewed online. The webpage itself and any page on the site reflecting its ownership should be printed out with URL listed.<sup>368</sup> Further, one should be prepared to offer evidence that the author of the posting or other social media content actually wrote it. This evidence can consist of an admission by the author, a stipulation entered into by the parties, the testimony of a witness who assisted in or observed the creation of the content or other indications or content from the profile itself that connects it to the author.<sup>369</sup>

Now we can conclude, the evidence required to meet the authentication threshold is quite low.<sup>370</sup> The first reason is that, individualization on social network sites, such as photos of the author, background information, information about author's hobbies and interests, and commentary by the user, provides courts with a reasonable assurance under the Federal Rules of Evidence 901(b)(4). The more personal information is provided to authenticate the social media evidence, the more possible courts take it as a reasonable assurance to accept the evidence admissible.<sup>371</sup> Another

---

<sup>367</sup> Perfect 10, Inc. v. Cybernet Ventures, Inc., *supra* note 357, at 1154.

<sup>368</sup> Browning, *supra* note 356, 480.

<sup>369</sup> Browning, *supra* note 356, 481.

<sup>370</sup> State v. Bell, 2008-Ohio-592, 882 N.E.2d 502, 512 (C.P. Clermont County Ct. 2008).

<sup>371</sup> Tienda v. State, No. 05-09-00553-CR, 2010 WL 5129722, at \*5 (Tex. App.—Dallas Dec. 17, 2010, pet. granted).

reason is that printouts of the social network website can be sufficiently authenticated by examining the purpose for which the social media evidence is being offered. When the limited purpose of establishing intent and planning, and its probative value exceeded any danger of unfair prejudice, courts hold the admission of the social media evidence.<sup>372</sup> In short, the key to authenticating evidence from someone's social network site(s) is to demonstrate the connections between that individual and the evidence being offered. After all, social network sites are all about establishing connections and so is authentication.<sup>373</sup>

## **2. Admissibility of Social Media Evidence in Litigation**

The basic rule is generally taken by courts in American legal system. This rule requires a low authentication threshold, that is, the party providing the printout evidence only reaches a prima facie standard, and authenticates the printout by the required testimony. But when the Maryland high court made the judgment in the case of Griffin v. Maryland in 2011, the main stream in the American legal system thought this judgment raised the admissibility threshold of social media evidence, and preferred the more flexible Texas approach in the case of Tienda v. Texas made in 2012. In practice, this admissibility issue of social media evidence continues to evolve. We thus study several leading cases in order to show the whole picture of legal approach to solve the authenticity issue of the printout. These cases were selected by a cross-comparison of references, to make sure these are leading cases. Although these cases are in the state level, instead of the federal level, judgments of these cases are widely discussed and followed by other courts in the American legal system.

---

<sup>372</sup> People v. Liceaga, No. 280726, 2009 WL 186229, at \*4 (Mich. Ct. App, Jan. 27, 2009); Hall v. State, 283 S.W.3d 137, 149 (Tex. Crim. App. 2009, pet. Ref'd.).

<sup>373</sup> Browning, *supra* note 3, 484.

## 2.1 Griffin v. Maryland

### (1) The Case

In the case of Griffin v. Maryland, the defendant was charged with killing Darvell Guest in the women's restroom of Ferrari's bar in Perryville, Maryland. At the first trial, which ended in a mistrial, the defendant's cousin Dennis Gibbs testified that he didn't see the defendant "*pursue the victim into the bathroom with a gun.*"<sup>374</sup> But in retrial, Gibbs testified that he saw Griffin and Guest "*go into the bathroom, and that no one else went in. He then heard multiple gunshots.*"<sup>375</sup> Gibbs claimed that the reason he changed his testimony because he was threatened by Griffin's girlfriend Jessica Barber via her MySpace page at the first trial. The alleged Barber's MySpace page contained the following statements: "I HAVE 2 BEAUTIFUL KIDS...FREE BOOZY!!!!JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"<sup>376</sup>

### (2) The Social Media Evidence at Issue

The prosecution offered printouts of these statements in order to explain Gibbs's evolving testimony. In order to authenticate printouts, the prosecution provides the lead investigator who made these printouts as the witness, instead of calling Barber to testify. The investigator testified he knew that MySpace page belonged to Barber because the MySpace profile had a picture of Ms. Barber and the defendant, referenced her children, had her birthdate (10/02/1983) and location of Port Deposit, and referenced the defendant's nickname (Boozy).<sup>377</sup>

### (3) The Court's Reasoning

Although the intermediate appellate court upheld the trial court's ruling of guilty,

---

<sup>374</sup> Griffin v. State, 995 A. 2d 791 (Md. Ct. Spec. App. 2010).

<sup>375</sup> *Id.*

<sup>376</sup> *Id.*

<sup>377</sup> Griffin v. State, 19 A.3d 415 (Md. App. 2011), at 418.

the Maryland's high court overruled the intermediate court and remanded the case for a new trial. The high court thought the trial judge abused his discretion in admitting the MySpace evidence, because the picture of Ms. Barber coupled with her birthdate and location were not sufficient distinctive characteristics on a MySpace profile to authenticate its printout. The high court raised the possibility of fraudulent use of the account. It stated "*someone other than Ms. Barber could have not only created the site, but also posted the 'snitches get stiches' comment.*"<sup>378</sup> The high court also provided possible alternative methods for authenticating social media evidence, that is, (1) to question the purported creator of the social media information, (2) to search the computer of the person who purportedly created the social media information, or (3) to have the social media provider link the social media information to the person who purportedly created it.<sup>379</sup>

#### (4) The Comment

In this case, we can find the Maryland's high court still followed the basic rule, which is, "*one should be prepared to offer evidence that the author of the posting or other social media content actually wrote it. This evidence can consist of an admission by the author, a stipulation entered into by the parties, the testimony of a witness who assisted in or observed the creation of the content or other indications or content from the profile itself that connects it to the author.*" Especially in those possible alternative methods provided by this high court, the court strengthened the connection between the social media information and the purported creator is the most important element to authenticate these printouts evidence. The court pointed out the possibility of fabricating or tampering the social media information, in order to emphasize again the connection between the social media information and the

---

<sup>378</sup> *Id.* at 423 (quoting *Griffin v. State*, 995 A.2d 791, 805 (Md. Ct. Spec. App. 2010)).

<sup>379</sup> Hoffmeister, Thaddeus A. (2014), *Social Media in the Courtroom. A New Era for Criminal Justice?*, Prager, USA, at 158.

authorship has not been established in this case. The prosecution should call Ms. Barber as witness to authenticate these printouts evidence, instead of the lead investigator who even didn't assist in or observe the creation of the content or other indications or content from the profile itself that connects it to the author. Thus, we thought this social media evidence was refused because the prosecution didn't authenticate it in a proper way.

## 2.2 Commonwealth v. Williams

### (1) The Case

In the case of Commonwealth v. Williams, the defendant Dwight Williams was convicted of the first-degree murder for the shooting death of Izaah Tucker.<sup>380</sup> At trial, a witness for the government testified that the defendant had a gun on the night of the murder, and further testified she received four MySpace messages from the defendant's brother Jesse Williams, urging her not to testify or to claim a lack of memory prior to the trial.

### (2) The Social Media Evidence at Issue

The prosecution offered the MySpace messages into evidence to explain why the witness appeared reluctant to testify and call this witness to authenticate these messages. The witness testified that she knew the messages were from Jesse because his picture was on his MySpace account and he used the screen name "doit4It", and she reposted back to three of the four messages sent by Jesse.<sup>381</sup> The testimony was admitted without objection.

### (3) The Court's Reasoning

On appeal, the Massachusetts Supreme Judicial Court found the admission of these MySpace messages to be in error. Comparing the MySpace messages to a phone

---

<sup>380</sup> Commonwealth v. Williams, 926 N.E. 2d 1162 (Mass. 2010).

<sup>381</sup> *Id.* at 1172.

call, the court stated, “A witness’ testimony that he or she has received an incoming call from a person claiming to be ‘A’, without more, is insufficient evidence to admit the call as a conversation with ‘A’.”<sup>382</sup> Although the foundational testimony had established that “the messages were sent by someone with access to the defendant’s MySpace Web page,” there was no evidence regarding “the person who actually sent the message.”<sup>383</sup> However, due to strong evidence of the defendant’s guilt, the error was not sufficient to overturn the defendant’s conviction.

#### (4) The Comment

This social media evidence at issue is MySpace message alleged sent by Jesse Williams, and can be authenticated by Jesse’s testimony based on the basic rule. But in this case, the prosecution called the witness who was the receiver of these messages to testify, and the witness’ assurance is based on only the picture of profile and the screen name. Thus, the court thought the risk of fabricating or tampering the social media information is high and there is no more evidence to prove Jesses is that person who created these messages. The problem remains that there is no solid foundation to connect the social media information and the real creator or the person alleged to create these information.

In this case, the court made a comparison of social media to the telephone, and we think it misses the mark.<sup>384</sup> Unlike the telephone, social network sites provides many and diverse indicators to prove a user’s identity, such as photos of the author, background information, information about author’s hobbies and interests, and commentary by the user etc. Thus there must be some methods to provide circumstantial evidence to prove the connection between the social media information and the authorship. Scholars also commented this case that based on the application of

---

<sup>382</sup> *Id.* at 1172 (citing *Commonwealth v. Hartford*, 194 N.E.2d 401 (Mass. 1963)).

<sup>383</sup> *Id.* at 1172-73.

<sup>384</sup> Hoffmeister, *supra* note 379, 159.

the reply doctrine<sup>385</sup> and the fact that the witness testified that she responded to three of the four MySpace messages from Jesse Williams, it might have been more inclined to find the MySpace messages admissible.<sup>386</sup>

## 2.3 Tienda v. Texas

### (1) The Case

In the case of *Tienda v. Texas*, the defendant Ronnie Tienda Jr. was charged with the drive by murder of David Valadez. After being convicted of murder, Tienda appealed the decision, claiming that the trial court should not have admitted evidence from MySpace pages alleged to be managed by the defendant. The Fifth Circuit Court of Appeals affirmed the conviction, as did the Court of Criminal Appeals.<sup>387</sup>

### (2) The Social Media Evidence at Issue

The prosecution offered several MySpace accounts into evidence allegedly belonging to the defendant. For example, the accounts contained postings such as, “If you ain’t BLASTIN, You ain’t LASTIN. I live to stay fresh!! I kill to stay rich!! RIP, David Valadez.”<sup>388</sup> Each account was linked to email address including Tienda’s name or nickname (“ronnietiendajr@” or “smileys\_shit@”), had a profile name matching either Tienda’s name or nickname (Smiley Face), listed Tienda’s hometown (D TOWN or dallas) as the location, and containrd photographs of a man who

---

<sup>385</sup> The case of *Sunbelt Health Center v. Galva*, 7 So.3d 556 (Fla. 1st DCA 2009) is a good example of this scenario and what is known as the “reply letter doctrine.” In finding that the handwritten signature should have been admissible, the appellate court discussed the “reply letter” doctrine: “*the requirements of the evidence code are satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. The use of circumstantial evidence to authenticate is permissible. Authentication occurs in a situation where the offered item, considered in light of the circumstances, logically indicates the personal connection sought to be proved. Pursuant to the “reply letter” doctrine, a letter can be authenticated upon a showing that it was “apparently in reply” to an earlier letter sent to the purported author of the reply letter. Once a prima facie case of authenticity has been established, the document is authenticated, and the trier of fact must resolve any disputes regarding the genuineness of the exhibit.*”

<sup>386</sup> Hoffmeister, *supra* note 379, 158.

<sup>387</sup> *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012), at 634.

<sup>388</sup> *Id.* at 635.

resembled Tienda.<sup>389</sup> To authenticate this MySpace evidence, the prosecution did not rely on the defendant, but instead used the victim's sister Priscilla Palomo, who initially found the defendant's MySpace profiles and offered them to the police. During cross examination at the trial, Ms. Palomo admitted that it was possible to create a bogus MySpace page and the information reportedly written on Tienda's MySpace page was known to others.

### (3) The Court's Reasoning

The appellate court determined that the trial court didn't abuse its discretion in admitting the MySpace evidence. There were three reasons. First, these MySpace were registered to a person with the defendant's name or nickname. Second, the multiple photographs tagged to these MySpace accounts were clearly of the defendant. Third, the defendant's profile referenced the victim and his murder along with the defendant's home monitoring. In comparing this case to the case of Griffin, the appellate court noted that "*there are far more circumstantial indicia of authenticity in this case than in Griffin.*"<sup>390</sup> Therefore the appellate court concluded that "*it is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted boastful messages about David Valadez's murder and the circumstances of that shooting, was aware of the music played at Valadez's funeral, knew when the appellant was released on pretrial bond with electronic monitoring and referred to that year-long event along with stealing the photograph of the grinning appellant lounging in his chair while wearing his ankle monitor. But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie*

---

<sup>389</sup> *Id.* at 634-36.

<sup>390</sup> *Id.* at 633. Also see Hoffmeister, *supra* note 26, 160.

*showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages.”*<sup>391</sup>

#### (4) The Comment

The most important reasoning in this case is that *“that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages.”* The court in Tienda reiterated, under the Federal Rules of evidence 901, the request of authentication simply asks that the evidence provider presenting the evidence make a prima facie showing of genuineness, and remains space to the fact finder to decide authenticity. It didn’t deny the risk of fabricating or tampering the social media information, but admitted *“there are far more circumstantial indicia of authenticity in this case than in Griffin”*, even though the prosecution neither called the defendant as the witness to authenticate the MySpace evidence. Comparing this case with the Griffin case, we may conclude the core issue of authenticating printouts of social network sites or the social media evidence is the connection between the social media information and the authorship. The best way mentioned in the Griffin case is to call the alleged creator to testify. The alternative is to authenticate the connection by sufficient circumstantial evidence, established in the case of Tienda. From the current cases, we can conclusion it is not sufficient if there are only a photo of the alleged creator coupled with few personal information as the circumstantial evidence, such as the profile photo and the screen name in the case of Commonwealth v. Williams.

### **3. The Standard**

As mentioned above, since 2011, courts have dealt with the authenticity issue of

---

<sup>391</sup> *Id.* at 633.

social media evidence differently, and main stream believes that most of courts make decision these two different approaches, the Maryland approach and the Texas approach.<sup>392</sup> The most likely source for the separation is Honorable Paul W. Grimm’s 2013 article, *Authentication of Social Media Evidence*.<sup>393</sup> Two separate approaches to authenticating social media evidence were clearly drawn; the first approach involves courts setting “an unnecessarily high bar for the admissibility of social media evidence”, and the second approach determines “the admissibility of social media evidence based on whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic.”<sup>394</sup> A 2014 case, *Paker v. State*, references this article to discuss the Maryland approach and the Texas approach, and decides to follow the later one.<sup>395</sup> Other current cases are, referencing this article for distinguishing these two approaches to authenticate social media evidence, *Harris v. State*,<sup>396</sup> and *Sublet v. State*.<sup>397</sup>

### 3.1 The Maryland Approach

In 2011, the Maryland Court of Appeals laid out a “high standard” for authenticating social media evidence in *Griffin v. Maryland*. The content of this Maryland approach classified by Grimm is to emphasize the ease with which an individual can both make a MySpace profile in another person’s name as well as access another party’s MySpace profile.<sup>398</sup> The court noted as an initial matter that

---

<sup>392</sup> Flanagan, Elizabeth A. (2016), #Guilty? *Sublet v. State* and the Authentication of Social Media Evidence in Criminal Proceedings, 61 Vill. L. Rev. 287; Cummings, Douglas J. Jr. (2015), *Authenticating Social Media Evidence at Trial: Instruction from Parker v. State*, 15 Del. L. Rev. 107; Angus-Anderson, Wendy (2016), *Authenticity and Admissibility of Social Media Website Printouts*, 14 Duke L. & Tech. Rev. 33.

<sup>393</sup> Angus-Anderson, *supra* note 392, 43.

<sup>394</sup> Grimm, Paul W., Lisa Yurwit Bergstrom & Melissa M. O’Toole-Loureiro (2013), *Authentication of Social Media Evidence*, 36 AM. J. Trial Advoc. 433, 441.

<sup>395</sup> *Paker v. State*, 85 A.3d 682 (Del. 2014).

<sup>396</sup> No. 42, slip op. (Md. Apr. 23, 2015).

<sup>397</sup> No. 59, (Md. Apr. 23, 2015).

<sup>398</sup> *Griffin v. State*, *supra* note 377, at 423-24.

authentication requires that the proponent produce evidence sufficient to demonstrate that item is what the proponent claims it to be.<sup>399</sup> Although the court proffered a non-exhaustive list of other methods the prosecution could authenticate the social media evidence, its analysis suggests a belief that social media evidence should be held to a higher standard of authentication than other evidence.<sup>400</sup>

### 3.2 The Texas Approach

In 2012, the Texas Court of Criminal Appeals took a less restrictive approach to authenticate social media evidence in the case of *Tienda v. Texas*, which is known as the Texas approach. In this approach, courts need not be persuaded that the proffered evidence is authentic. Instead, the court only needs to decide whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic.<sup>401</sup>

Thus, it is thought, different from the strict approach in the case of *Griffin*, as long as there is sufficient evidence of authenticity such that a reasonable jury could conclude that evidence was authentic, the proffered evidence then meets the authentication burden.<sup>402</sup>

### 3.3 Discussion

Actually as we discuss above, there is no need to separate authenticity of social media evidence into these two approaches. There is no huge difference between the Maryland approach (*Griffin v. Maryland*) and the Texas approach (*Tienda v. Texas*). The main issue of these cases is how to connect the social media information and the authorship, and the basic rule is applied in these cases. Further, determining

---

<sup>399</sup> *Griffin v. State*, *supra* note 377, at 423.

<sup>400</sup> *Griffin v. State*, *supra* note 377, at 427-28.

<sup>401</sup> *Tienda v. State*, *supra* note 387, at 638.

<sup>402</sup> *Angus-Anderson*, *supra* note 392, 37-38.

admissibility of these printouts involves two steps: (1) printouts of web pages must first be authenticated as accurately reflecting the content and image of a specific webpage on the computer, and then (2) in order to be relevant, the printout must be authenticated as having been posted by that source.<sup>403</sup> We can use these two steps to analysis the leading cases.

In the case of *Griffin v. Maryland*, the oft-quoted holding stated, “*the potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that [the witness] was its creator and the author of the ‘snitches get stitches’ language.*”<sup>404</sup> In Grimm’s article, he put more attention on the first half of this statement, attributing the court’s holding to an overly suspicious view of social media evidence. However, it is actually the second half that explains this decision. The court held printouts from the MySpace website not admissible, because the prosecution failed to connect the statements to the purported creator. The methods introduced by the court are ways to prove the connection between the social media information and the authorship. In *Griffin*, the court only focused on whether the second prong, having been posted by that source, has been satisfied and concluded the printouts had been improperly admitted during the trial.

In the case of *Tienda v. Texas*, a greater amount of circumstantial evidence supported a finding that “*the MySpace pages belonged to the appellant and that he created and maintained them.*”<sup>405</sup> Thus, both of these two prongs are satisfied, which means using this greater amount of circumstantial evidence authenticates the webpage

---

<sup>403</sup> Angus-Anderson, *supra* note 392, 45.

<sup>404</sup> *Griffin v. State*, *supra* note 377, at 424.

<sup>405</sup> *Tienda v. State*, *supra* note 387, at 645.

and connects that page to the purported author.

In the case of *Commonwealth v. Williams*, scholars believe the court acknowledged the two-prong requirement for admitting communications by comparing the web messages to a phone call.<sup>406</sup> The court found even though the prosecution established the fact that there is someone to send threatening messages to the witness, the prosecution had provided no evidence to prove who this person actually was. Thus, the social media evidence was not admissible because the connection between the social media information and the authorship was not built. Now we can conclude that there is no higher or strict standard for admitting the social media evidence. Rather, we need to consider the two-prong requirement while authenticating the social media evidence.

---

<sup>406</sup> Angus-Anderson, *supra* note 392, 46.

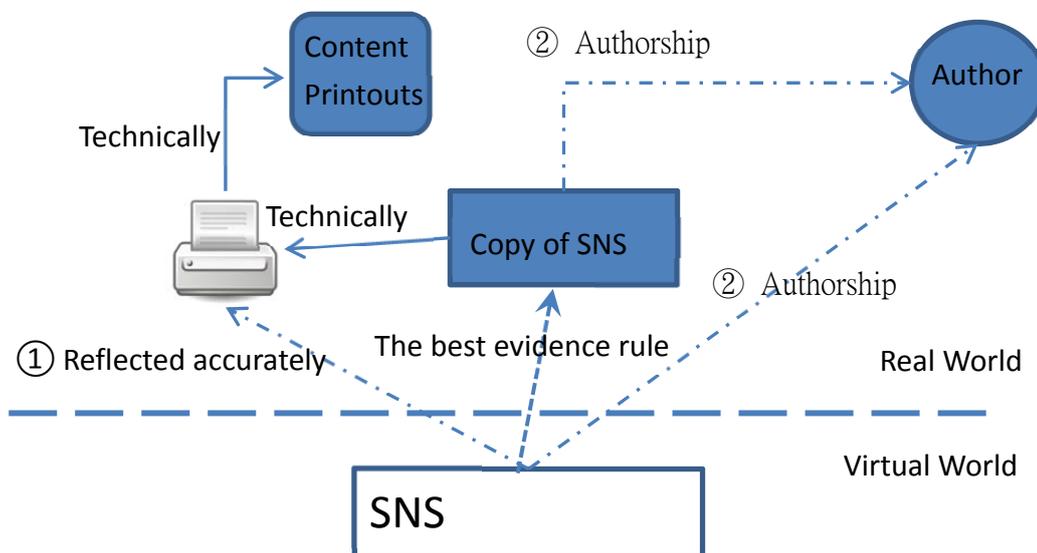
### **Section 3 Reconstruction of the Printouts Issue**

Let us return to this figure mentioned at the beginning. The website printout is a format of presenting social media evidence in the courtroom, and courts focus on how to authenticate this printout. As the conclusion of previous section, determining admissibility of printouts involves two steps: (1) printouts of web pages must first be authenticated as accurately reflecting the content and image of a specific webpage on the computer, and (2) in order to be relevant, the printouts must be authenticated as having been posted by that source (the authorship issue). We can find there is less discussions in step (1) in the case study, but courts put more efforts to establish connection of the authorship. One of sure and credible reasons to explain this attitude by courts is that, judges make a presumption to believe these printouts reflected contents on social network sites accurately, if information on social network sites was printed through a printer or any technology. In other words, judges or parties may argue the way to collect information from social network sites or make the social media evidence. For example, the defendant objected a printout evidence presenting conversations between the victim and him in a chat room, because this record was made by an investigator copying the conversations in a chat room and pasting the contents in a Word file; the investigator is likely to easily change or falsify the content of the dialogue. But they rarely questioned how the document was printed. It might be silly to question the function of a printer, which was designed for the purpose of correctly print the content of digital files. We instead want to point out the reliability of technical productions is not taken for granted by the legal system. In 1990's, computer printouts as evidence was a controversial issue.<sup>407</sup> Therefore, we think the real question in this printouts issue should be how to copy the virtual world to the real

---

<sup>407</sup> Johnson, Mark A., Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?, 75 Msq. L. Rev. 439; Freeman, Edward H. (1998), The Use of Computer Records as Courtroom Evidence, available at <http://www.ittoday.info/AIMS/DSM/8203351.pdf>.

world (presenting in the courtroom). Then we can divide this procedure into several steps: first extracting information from the social network site, second making a record file to present extracted information in the screen, and third print this record out or screenshot extracted information on devices in order to show evidence in the courtroom. Based on these steps, the core issue will be how to prove extracted information is exactly information on that social network site, or how to prove the record file exactly equals extracted information, which we can understand as the question, how to prove  $A=A'$ .



## 1. How to Prove $A=A'$

While we are thinking the question, how to prove  $A=A'$ , we focus on accurately reflection of the visual output. Thus, there is an original file, there will be a copy of that file, and there must be the accurately reflection of the original file. The most common way to make sure printouts accurately reflected the original files is the image copy. We will discuss as follow.

### 1.1 Original Electronic Evidence

The meaning of proving  $A=A'$  is to make sure the copy or printouts equal to the

original information. In a technical perspective, a mere bit-stream copy of a graphical image file does not provide a completely accurate printout or other output readable by sight unless Window-supported forensics tools or other viewers are used to non-invasively create an accurate visual output of the recovered data, without changing any of the data. If the computer file is compressed, encrypted, transmitted as email attachment, it will be recognized as the original file when this file is decompressed, decrypted and opened after receiving. It is mandatory that the original data remain unchanged, but whether that data is compressed, encrypted or converted to a different file format in its stored state is immaterial as long as the data itself is not compromised. This is one of the reasons the MD5 hash and verification processes are so important. Even though the file format of the data in question may change, the integrity of that data must remain intact.

## 1.2 Presenting Electronic Evidence at Trial

In the case of *Amstrong v. Executive Office of the President*, the court ruled that a hard copy paper printout of an electronic document would not “*necessarily include all the information held in the computer memory as part of the electronic document.*”<sup>408</sup> The court further noted that without the retention of a complete digital copy of an electronic document such as an email message, “*essential transmittal relevant to a fuller understanding of the context and import of an electronic communication will simply vanish.*”<sup>409</sup>

When providing testimony, many forensic practitioners present evidence through screenshots in a PowerPoint presentation format, or take EnCase software with them into Court for a live demonstration.

In order to show the context and metadata associated with the link files, including

---

<sup>408</sup> *Amstrong v. Executive Office of the President*, 1 F.3d at 1280.

<sup>409</sup> *Id.*

file-created dates, full path location and other information, EnCase screenshots is useful to present as evidentiary exhibits in the courtroom. These screen-capture exhibits provided the most accurate visual display of the data as it existed on the defendant's computer at the time of seizure. The court allowed the screenshots into evidence.<sup>410</sup>

In summary, there are actually some methods which can prove  $A=A'$  with a real meaning. However, the authentication of printouts of social network sites in legal system is not relevancy of this real meaning. We can precisely define this legal authenticity as the identification. Its function in the evidence law is to identify the purported evidence being exactly what is proponent claimed to be. Since the fact that the legal system chased is different from the scientific system, we will further discuss what the Law's knowledge of science is to be used to construct the past fact or establish the foundation of evidence.

## **2. Law's Knowledge of Science**

Back to the debate on computer printouts as evidence in 1990's, we can draw the picture of law's knowledge of science. The debate focused on whether stricter foundations for computer printouts are required. As the same consideration of printouts of social network sites, the party against the computer printouts will raise issues of fabricating or tampering information. A computer printout may contain false information. The argument for requiring a stricter foundation than is required rests on two related premises. First, the legal community does not adequately appreciate the limits of computer technology and therefore does not apply the existing rules in a manner that assures fairness and justice. Second, a computer printout carries with it

---

<sup>410</sup> United States v. Dean, 135 F.Supp.2d 207, fn. 1. (D. Me.).

false indicia of trustworthiness, accuracy, and reliability.<sup>411</sup> Based on the prejudicial nature of computer printouts, a stricter foundation for computer printouts is needed. This approach concerns the different between technology and law, and tries to avoid misuse and misunderstanding of the computer technology. However, the argument against new rules of evidence and stricter foundation requirement for computer printouts won the debate and dominate the existing rules of evidence.

This argument is based on the premise that technological advances and experience have improved the trustworthiness and accuracy of computer printouts. It made a presumption of reliability.<sup>412</sup> Reasons support this presumption are (1) machine and human mistakes can be minimized by new techniques of prevention, detection and correction; (2) computers do not introduced any new evidentiary issues and the possible of errors did not begin with the arrival of computers, rather, it has always existed; (3) the legal community and jurors have an increased awareness of the limits of computer reliability; and (4) requiring proponents of computer printouts to supply extensive foundation testimony unfairly burdens the proponent of such evidence, and increased the complexity and decreases the efficiency of trials.<sup>413</sup> We can find that the first reason is based on the belief of scientific objectivity, and the rest of reasons are based on practical considerations. Any doubts regarding the accuracy of the evidence should affect the weight, not the admissibility, of evidence.<sup>414</sup> Further, any doubts the trier of fact has, including reliability, accuracy, and trustworthiness, should affect the weight given the evidence, not its admissibility.

Therefore, we can divide the truth of the computer printout evidence into two

---

<sup>411</sup> Johnson, Mark A. (1992), Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?, 75 Msrq. L. Rev. 439, 445.

<sup>412</sup> Peter M. Storm, Comment, Admitting Computer-Generated Records: A Presumption of Reliability, 18 J. Marshall L. Rev. 115 (1984), at 153-54.

<sup>413</sup> Johnson, Mark A., *supra* note 411, at 446.

<sup>414</sup> Peter M. Storm, *supra* note 412, at 134-135.

part; one is referred to the reality connect to the nature world, known as scientific truth, and the other is the authenticity under the rules of evidence, created by the legal system. The law believes technology based on scientific knowledge is objective and accurate, because technology is implemented mechanically without individual selfishness and personal desires. Then it can make sure the accuracy of this implementation, and then gets reliability and trustworthiness. These natures are facts, belonged to the trier of fact, which is determined by the jury through their experience and knowledge.

As to the law's knowledge of science, it is apparently referred to the judge's scientific knowledge, which was established by his education, experiences, and even common senses. On the surface, the legal system respects the scientific system and remains independent of the production of scientific knowledge. However, if there is demand, especially when there is an objectivity requirement, the legal system often internalizes scientific knowledge into legal standards via the judge's knowledge and experiences. We cannot define this legalized scientific knowledge as non-scientific knowledge, but it is for sure that the objectivity of such scientific knowledge has been affected. Despite assumption of reliability is built, the facts assessed through such knowledge or jurors' experience appear to be no longer a natural fact, but rather a relative, persuasive fact.

### **3. In Conclusion, A Relative Real**

As we discuss above, the authenticity issue of printouts of social network sites are actually the question of how to copy the virtual information to the real world. The core issue of this question is how to prove  $A=A'$ . There are some methods can ensure the copy or the printout equaling to the original file through the technology. However, these methods are not common to be used in the legal system. The judge prefers to

remain the fact issue to the reasonable jury, which make the decision via knowledge educated, personal experiences and common senses. As for the admissibility issue, the legal system created the whole evidence evaluation system to ensure evidence presented in front of the jury is relevant and admissible. Under this rules of evidence, the legal system created the conception of authenticity, which is not to prove A=A', but to identify A being A that the proponent claimed. Take the defamation case as example, a person X claimed that Y spread false texts on his own Facebook and then damage the X's reputation. If we want to prove whether there the defamation is, the forensic practitioners will try to extract information from Y's Facebook, make copies of information, verify the copy and the original information, and then prove these printouts of the defamation accurately reflected and exactly coming from Y's Facebook. On the contrary, the proponent only authenticates printouts of the defamation, no matter through testimony or circumstantial evidence, and these printouts will be accepted. The requirement is "*the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.*"<sup>415</sup> The issue of fact, which means whether X has been libeled by Y, is remained to the reasonable jury to decide.

Back to the authenticity issue of social media printouts, courts believe that the printout itself was not a problem. The printout generally can be accurately reflected through printed by a printer or screenshot by other technology. This belief is based on the presumption of reliability, which is discussed previously. Therefore the rest of issue is to prove when and how this printout was produced and the connection with people. Basically the value of evidence depends on the jury, as the fact finder, determining the trustworthiness of the evidence. What the judge can do in the criminal proceeding is to identify evidence at issues being exactly what the proponent claimed

---

<sup>415</sup> The Federal Rules of Evidence 901 (a).

it to be. The authentication proceeding does not involve identify or construct the fact. Furthermore, the legal system provides parties a chance to participate in this evidence evaluate proceeding, and establish their claims through cross-examination in the courtroom. Thus, we can conclude that even though the prosecution's main task is to find the past fact and the criminal, the fact created or found in most cases is not the reality of a case, but a relative fact which can be accepted by parties, the prosecution, the jury, and even the whole society.

## Reference

1. Angus-Anderson, Wendy (2016), Authenticity and Admissibility of Social Media Website Printouts, 14 Duke L. & Tech. Rev. 33.
2. Browning, John G. (2011), Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites, 14 SMU Sci. & Tech. L. Rev. 465.
3. Coughlan, Steve & Currie, Robert J. (2013), Social Media: The Law Simply Stated, 11 Can. J. L. & Tech. 229.
4. Cummings, Douglas J. Jr. (2015), Authenticating Social Media Evidence at Trial: Instruction from Parker v. State, 15 Del. L. Rev. 107.
5. Flanagan, Elizabeth A. (2016), #Guilty? Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings, 61 Vill. L. Rev. 287.
6. Freeman, Edward H. (1998), The Use of Computer Records as Courtroom Evidence, available at <http://www.ittoday.info/AIMS/DSM/8203351.pdf>.
7. Grimm, Paul W., Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro (2013), Authentication of Social Media Evidence, 36 AM. J. Trial Advoc. 433.
8. Johnson, Mark A. (1992), Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?, 75 Msrq. L. Rev. 439. Available at: <http://scholarship.law.marquette.edu/mulr/vol75/iss2/6>
9. Lawrence Morales II (2012), Social Media Evidence: “What You Post or Tweet Can and Will Be Used against You in a Court of Law”, 60 The Advoc. (Texas) 32.
10. Marcum, Catherine D. & Higgins, George E. (2014), Corrections and Social Networking Websites, in: Social Networking as a Criminal Enterprise, CRC press, 221-229.
11. McCarthy, Terrence W. & Nichols-Gault, Allison (2014), A Guide to the Admissibility of Social Media/ Electronic Evidence in Alabama, 75 Ala. Law.

- 42.
12. McPartland, Molly D. (2013), An Analysis of Facebook “Like” and Other Nonverbal Internet Communication Under the Federal Rules of Evidence, 99 Iowa L. Rev. 445.
  13. McPeak, Agnieszka (2014), Social Media Snooping and its Ethical Bounds, 46 Ariz. St. L.J. 845.
  14. Mercuri, Rebecca (2010), Criminal Defense Challenges in Computer Forensics, In: Goel S. (ed.) ICDF2C 2009, LNICST 31, pp. 132-138.
  15. Murphy, Justin P. & Fontecilla, Adrian (2013), Social Media Evidence in Government Investigations and Criminal Proceedings: a Frontier of New Legal Issues, 19 Rich. J.L. & Tech. 11.
  16. North, Evan E. (2013), Facebook Isn’t Your Space Anymore: Discovery of Social Networking Websites, 58 Kansas L. Rev. 1279.
  17. Pannozzo, Allison L. (2012), Uploading Guilt: Adding a Virtual Records Exception to the Federal Rules of Evidence, 44 Conn. L. Rev. 1695.
  18. Parker, Christopher E. & Swearingen, Travis B. (2012), “Tweet” Me Your Status: Social Media in Discovery and at Trial, 59-FEB Fed. Law. 34.
  19. Robbins, Ira P. (2012), Writing on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence, Minnesota Journal of Law, Science & Technology, Vol. 13, No. 1, 1-36. American University, WCL Research Paper No. 2011-31. Available at: <http://ssrn.com/abstract=1949332>
  20. Sholl, Emma W. (2013), Exhibit Facebook: The Discoverability and Admissibility of Social Media Evidence, 16 Tul. J. Tech. & Intell. Prop. 207.
  21. Taylor, Kathryn R. (2014), “Anything You Post Online Can and Will Be Used against You in a Court of Law”: Criminal Liability and First Amendment

Implication of Social Media Expression, 71 Nat'l Law. Guild Rev. 78.

22. Uncel, Megan (2011), Comment, "Facebook Is Now Friends with the Court":  
Current Federal Rules and Social Media Evidence, 51 JURIMETRICS 43.
23. Wilson, John S. (2007), MySpace, Your Space, or Our Space? New Frontiers in  
Electronic Evidence, 86 Oregon L. Rev. 1201.

## **Chapter 6 Connect the Virtual to a Real World: The Issue of Trojan Defense**

According to Chapter 5, the printout issue will raise four scenarios: (1) when the social network sites account is actually true (authorship is true), and the content of the posting is true, then this social media evidence is authentic and can be present in front of the jury deciding its value to rebuild the past fact; (2) when the account is true, but the content is false, then this social media evidence is still authentic and let to the jury to decide its value (the jury can decide whether believe it or not); (3) When the account is false, but the content may be true, the authentication issue is raised, the judge must to decide whether this social media evidence is admissible, because this account might be hacked or shared with others; (4) when both the account and the content are false, the judge must exclude this social media evidence because it is not authentic. This evidence should not present in front of the jury in theory. Thus, we can conclude that, as long as the account is true or no one claimed its false, then this social media evidence will be left to the jury to decide its factual value; but if the account is false or claimed false, then the judge must decide authentication of this social media evidence. Furthermore, form the defendant's aspect, as long as there is any false, no matter in part of account or content, he has the chance to raise the Trojan defense, and claims, "It was not me. There is someone who did it. "

Then the prosecutor is obligate to connect the crime to this defendant by using this social media evidence. Precisely the prosecutor needs to connect the defendant to this virtual identity, trying to realize a virtual figure to the real person, who is exactly standing in the courtroom just across from him.

		Account in SNS	
		True	False
Content of SNS	True	SME is authentic. Jury will decide its value.	Authentication? (Trojan Defense)
	False	SME is authentic. Jury will decide its value. (Trojan Defense?)	Authentication? (Trojan Defense) Value?

## Section 1 A Background of the Trojan Defense

### 1. Definition of the Trojan

A Trojan Defense, also known as SODDI (Some Other Dude Did it), means the defendant cannot prove his innocent, but argued someone or a Trojan invaded his computer and committed the crime. This defense raises evidential issues of reliability and reality, which may cause the jury to bring a guilty in an acquittal, or worse, an innocent guilty. It is real that everyone will be the victim, if his computer was infected with Trojans, was deliberately framed by some others, or was treated as a “zombie”<sup>416</sup> to attack other computers. Here are three terms related to the sense of the Trojan defense.

#### 1.1 Malware

Malware is defined a set of instructions that run on your computer and make

---

<sup>416</sup> A zombie computer means this computer is controlled by others (maybe the criminal or hackers), instead its owners or authority users. This computer will be used to attack other computers, just like a puppet controlled by the puppeteer, in order to avoid be tracing the real location. The attacker use the jump to attack the victim’s computer for secret information or valuable digital data, or for control more computers, building up the botnet to make a more large-scale attack, such as DDoS (Distributed Denial of Service attack). More detail found, [https://en.wikipedia.org/wiki/Zombie\\_\(computer\\_science\)](https://en.wikipedia.org/wiki/Zombie_(computer_science)), [https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)

your system do something that an attacker wants it to do.<sup>417</sup> In terms of currently developing information technology, definitions of the malware have been rather vague. It may include all soft wares or programs through malicious behavior to achieve the purpose, such as Trojan, Virus,<sup>418</sup> Computer worm,<sup>419</sup> Backdoor,<sup>420</sup> Keystroke logging,<sup>421</sup> Spyware<sup>422</sup> etc. A computer may infect a malware through sending and receiving an unknown e-mail, Phishing,<sup>423</sup> Drive-by Downloads,<sup>424</sup> Browser exploit,<sup>425</sup> instant messaging with malicious friends, downloading free software, decryption software, Web 2.0 Security Vulnerabilities,<sup>426</sup> or “Autorun.inf” in plug and play devices (Autorun Virus). Once the computer is infected, the malware may hide itself in system, modify the regedit of system, or implant backdoors. An infected computer may have these symptoms, such as unexplained system crashes, system becoming unstable and slow, antivirus and firewall exception errors, unknown error warnings or the hard disk could not be opened. We may use these signs to determine whether the computer at issued is infected by the malware.

## 1.2 Trojan

A Trojan is a type of malicious software (globally known as malware) that is either packaged along with a useful piece of software or pretends to be a piece of useful software itself.<sup>427</sup> Hackers often use it with Backdoor, connecting computers between the hacker and the victim, to steal someone’s account and password or

---

<sup>417</sup> ED Skoudis & Lenny Zeltser, *Malware: Fighting Malicious Code*, Prentice Hall press, 2003, p.3.

<sup>418</sup> [https://en.wikipedia.org/wiki/Computer\\_virus](https://en.wikipedia.org/wiki/Computer_virus)

<sup>419</sup> [https://en.wikipedia.org/wiki/Computer\\_worm](https://en.wikipedia.org/wiki/Computer_worm)

<sup>420</sup> [https://en.wikipedia.org/wiki/Backdoor\\_\(computing\)](https://en.wikipedia.org/wiki/Backdoor_(computing))

<sup>421</sup> [https://en.wikipedia.org/wiki/Keystroke\\_logging](https://en.wikipedia.org/wiki/Keystroke_logging)

<sup>422</sup> <https://en.wikipedia.org/wiki/Spyware>

<sup>423</sup> <https://en.wikipedia.org/wiki/Phishing>

<sup>424</sup> [https://en.wikipedia.org/wiki/Drive-by\\_download](https://en.wikipedia.org/wiki/Drive-by_download)

<sup>425</sup> [https://en.wikipedia.org/wiki/Browser\\_exploit](https://en.wikipedia.org/wiki/Browser_exploit)

<sup>426</sup> [https://en.wikipedia.org/wiki/Vulnerability\\_\(computing\)](https://en.wikipedia.org/wiki/Vulnerability_(computing))

<sup>427</sup> Bowles, Stephen & Hernandez-Castro, Julio (2015), *The First 10 Years of the Trojan Horse Defence*, *Computer Fraud & Security*, January 2015, p.5.

Confidential information or both. A Trojan also can be used in controlling the victim's computer to attack other computer. Then the legal authority can find this zombie computer but is hard to trace the hacker's location.

In general, a Trojan is a malware of delivery mechanism. Its main function is using system vulnerabilities and allowing hackers to freely access information inside the infected computer. Most Trojans are implanted directly from hackers, or via P2P software, email, file sharing, or removable devices. The clever part of Trojan is not usually a separate file, but combined with other executable files (known as ".exe"). Therefore, it becomes a part of the executable file, and when starting the executable file, the Trojan is also activated. Surprisingly, we can make a Trojan with "Trojan-making Kits", which is easy to find in the internet and can package the Trojan into a useful program. A pirated useful program (ex. Microsoft Office) or popular game software is the ideal place to hide the Trojan. For breaking the security measures of the original program, "program unlooper"<sup>428</sup> is used to cheat the security measures, and meantime, it also change the computer settings. While a person installs and runs a pirated program, he might activate the Trojan, sending his information to an unknown person. It is sad but true, the situations often happen because many people prefer to download the pirated program (especially the free one) with or without intention. Making easy and spreading rapidly and widely, that is also the reason why the courts think this Trojan defense carefully. It happened every second in the world.

### 1.3 Rootkit

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be

---

<sup>428</sup> <https://en.wikipedia.org/wiki/Unlooper>

allowed (for example, to an unauthorized user), while at the same time masking its existence or the existence of other software.<sup>429</sup> Depending on different rules and hidden skills, it also can make a backdoor in the system, in order to allow an unauthorized user identified as the administrator accessing the system, or use its integrated malicious code to collect information inside the computer or accounts and passwords.

Recently, most Trojans has been used the hidden technology of Rootkit, leading to more new variants of Trojans, which are more and more difficult to predict. The Trojan Defense can justify itself through features of Rootkit, thus we need to analysis Rootkit with the digital forensic tools and procedures, in order to solve the Trojan defense issue. The internet will only continue to flourish in the future, from wired to Wi-Fi, and from telephone to smart phone. Malwares are constantly passing between the internets, resulting in ever-increasing cybercrime. At the same time, issues of Trojan defense continuigly challenge professional and credibility of forensic technology.

## **2. Digital evidence produced**

Here are some types of digital evidence in the victim's computer produced by the Rootkit.

(1) Information of IP and network interface card: Using internet is necessary to run the Trojan or Rootkit, which is provided by an ISP (internet service provider)<sup>430</sup>. Therefore, we can ask the ISP to provide the audit records, which reserved event identifiers to provide information about the type of server events or activities. Then we may analysis and compare information of IP and network interface card to search an attacker or unauthorized person's trace.

---

<sup>429</sup> <https://en.wikipedia.org/wiki/Rootkit>

<sup>430</sup> [https://en.wikipedia.org/wiki/Internet\\_service\\_provider](https://en.wikipedia.org/wiki/Internet_service_provider)

(2) Connection information: We can gather information of connecting the internet from the victim's computer system. This information includes records of sign-in or sign-out the network, records of attacking or connecting the firewall, or the port information, which is used to prove an authorized connection or abnormal network activity occurred.

(3) Malware: We can use forensic tools to find the source code of a malware or Rootkit, or its existence at the scene, to prove that the computer was indeed invaded by a malware.

(4) Digital activities: Digital activities are determined primarily on the basis of the system audit records, to prove that someone actually invaded this computer or this computer was used to commit a crime. Types and quantities of audit records are quite complicated, and invalid, incorrect or falsified time information will cause a lot of garbage information. Forensic officers will spend a lot of time in dealing with such information.

### **3. Trojan has the Nature of Occult**

(1) Obfuscation<sup>431</sup> added in the Trojan

Functions of a Trojan may include hiding the IP address of the control terminal, remote control, intercepting the network packet<sup>432</sup>, recording keyboard input data (keystroke logging), passing messages, and providing packets to the zombie computers. The attacker implanted the victim's computer a program with the

---

<sup>431</sup> In software development, manual obfuscation is the deliberate act of creating obfuscated code, i.e. source or machine code that is difficult for humans to understand. Like obfuscation in natural language, it may use needlessly roundabout expressions to compose statements. Programmers may deliberately obfuscate code to conceal its purpose (security through obscurity) or its logic, in order to prevent tampering, deter reverse engineering, or as a puzzle or recreational challenge for someone reading the source code. [https://en.wikipedia.org/wiki/Obfuscation\\_\(software\)](https://en.wikipedia.org/wiki/Obfuscation_(software))

<sup>432</sup> A network packet is a formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, packet switching is possible and the bandwidth of the communication medium can be better shared among users than with circuit switching. [https://en.wikipedia.org/wiki/Network\\_packet](https://en.wikipedia.org/wiki/Network_packet)

foregoing function, and then compiled this Trojan, adding the junk code to change the originating point code<sup>433</sup> of the original program. Such an operation is called obfuscation, which is a special computer program development tool, typically used as the reverse engineering<sup>434</sup> protection, anti-crack protection, and anti-piracy protection of the commercial software.

This obfuscate mechanism converts binary system code into the new binary system code, which is very difficult to analyze, or completely different with the source code, but the function did not change. That is, the original program function and logic are same, but transformed into other forms of presentation. It aims to completely hide specific implementation details or architecture of the program in its source code. If we want to disassemble or reverse engineering an obfuscated program, this binary system of machine code will be garbled or render meaningless messages, to protect the source code and the machine code.

(2) Packer<sup>435</sup> is used in the Trojan

The attacker also often uses the packers/shelling technology to hide Trojans. Through this packers/shelling operation to modify computer language or code in the Trojan, it with different features cannot be detected, deleted or quarantined by antivirus soft wares.

---

<sup>433</sup> It is a unique address for a node (Signaling Point, or SP), used in MTP layer 3 to identify the destination of a message signal unit (MSU). In such a message you will find an OPC (Originating Point Code) and a DPC (Destination Point Code); sometimes documents also refer to it as a signaling point code. Depending on the network, a point code can be 24 bits (North America, China), 16 bits (Japan), or 14 bits (ITU standard, International SS7 network and most countries) in length. [https://en.wikipedia.org/wiki/Point\\_code](https://en.wikipedia.org/wiki/Point_code)

<sup>434</sup> Reverse engineering, also called back engineering, is the processes of extracting knowledge or design information from anything man-made and re-producing it or re-producing anything based on the extracted information. [https://en.wikipedia.org/wiki/Reverse\\_engineering](https://en.wikipedia.org/wiki/Reverse_engineering)

<sup>435</sup> Packers provide runtime compression of executable. The original exe is compressed, and a small executable decompressor id prepended to the exe. Upon execution, the decompressor unpacks the compressed executable machine code and runs it. Packers are neutral technology that is used to shrink the size of executables. Many types of malware use packers, which can be used to evade signature-based malware detection. See Eric Conrad, Seth Misener, and Joshua Feldman, CISSP Study Guide, Syngress, 2015, p. 139.

A packer, similar to encryption and compression, is a variation of the algorithm. For example, a section of code is Social Media Evidence: aaa. After encrypted, it may become `sh*eh^$sfgdji%as1`. Then the compiler software cannot resolve the internal program, but the computer can recognize under the premise that the encryption is written on computer logic. Conversely, shelling employs a restore method in a packed program, to restore the encrypted content. In former example, after packer, what we can see is `“sh*eh^$sfgdji%as1”`. Employing shelling in `“sh*eh^$sfgdji%as1”`, the contents can disassemble back to Social Media Evidence: aaa. Anti-virus software sometimes determines a file as the malware based on its packer. After all, safety programs typically do not encrypt or packers. Most malicious programs will packer, unless the programmer does not want his source code to be analysis.

#### **4. What the Trojan can do**

For lay persons, the Trojans defense seems to be very credible, and hackers seem to do anything. Thus, the defendant may be there will be a psychological speculation, and then raises the Trojan Defense to absolve his charges. Here are some examples to explain the possibility of Trojan defense, and test whether the Trojan defense really so do anything.

- (1) The defendant claim that someone remote his computer and login his email account, sending defamatory letters to the victim.

Generally, the attacker collected the victim's account and password, and then he usually remote a zombie computer to access the victim's account and send the email, for security reason (he cannot be trace by the police). It is necessary to check the IP address of email deliver, in order to realize where actual sending source is. In some cases, the attacker uses the victim's computer directly to send the email. As reference

for determine whether this email sent from this computer, the sent item should be first checked. But if sending the email through the command-line interface<sup>436</sup>, the backup file is not even found inside in Outlook, and the abnormal status doesn't appear on the screen. Because sending the email through the command-line interface doesn't need to control the mouse, it is hard to find abnormal. If the police are confidence that the defendant send the mail, then the first step is to search whether there is the Trojan existed in the defendant's computer. Second, the sending time and before/after may help to find the trace of invasion in this computer.

In this case, the defendant's computer may indeed have been implanted the Trojan, and the hacker may also use his account to send emails. However, it is just one of possibilities. The forensic practitioners need more solid evidence to build this case.

- (2) The defendant argued it was not him but someone hacker his account to leave a message about the compensated dating in the internet forum.

In a perspective of forensic science, first, it is different between implanting the Trojan and VPN (virtual private network)<sup>437</sup>. While the hacker remotes the defendant's computer to leave the compensated dating on line, his digital activities will be showed on the screen. Theoretically, the system is unable without showing any abnormal situations to allow the defendant playing computer/online games, while the hacker remotes this computer to leave the message in the internet forum through a Trojan. Thus the forensic practitioners can check digital activities on this computer with its timeline, and then they may find evidence to prove what the defendant claimed.

---

<sup>436</sup> A command-line interface is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). [https://en.wikipedia.org/wiki/Command-line\\_interface](https://en.wikipedia.org/wiki/Command-line_interface)

<sup>437</sup> A VPN is a private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. [https://en.wikipedia.org/wiki/Virtual\\_private\\_network](https://en.wikipedia.org/wiki/Virtual_private_network)

From the experience, once an attacker successfully hacked and implanted a Trojan with remote function, he has no need to pretend this victim with his personal information just to do more secret protection. Most hackers invade other computers in order to prove his abilities or steal information. Using the victim's name to post the compensated dating in the internet forum is not smart for the attacker's security, unless he just want to spoof this victim. Therefore, this Trojan defense has a high probability to be false.

- (3) The defendant A and B were charged in using the victim C's eBay account to make the fraudulent trading. Both A and B argued they are hacked by someone. They didn't commit the crime.

The point of this case is the possibility that the defendants' computers were controlled by others. Even though the forensic practitioners prove the hacking activities can connect to the defendants' computers, it cannot be excluded that the malicious activities were made by the Trojans implanted in the defendants' computers. Therefore, we need to consider circumstantial evidence.

For example, the defendant applies an internet account and shares the network with others. When other people use this account with a sharing device, these internet activities will be attributable to the defendant's conducts. Furthermore, if the forensic practitioners indeed found the Trojan in this defendant's computer and some evidence to prove it related to malicious activities, this case have a high possibility that the defendant's computer is manipulated by someone to do malicious activities and its IP address is intentionally left. It is not enough that taking the IP address alone as the evidence to consider who is the criminal hacking C's account and committing the fraud. The Trojan defense should be taken into account while the defendant raises this issue.

## Section 2 Technical Issues

### 1. Trojan scenario

According to 2005 research pointed out, there are two scenarios of Trojan to find what can the overall Trojan package do, and what evidence would be left behind.<sup>438</sup>

#### 1.1 Scenario 1

In this scenario, the victim installed the up-to-date antivirus software in his computer, and downloaded a free game packed a Trojan from a Peer-to-Peer network. This Trojan is designed to deliver a number of payloads including a backdoor. This backdoor has been compressed, so the antivirus software cannot detect it. However, the backdoor would be detected as soon as it is released and decompress. Thus, the Trojan first deliver its antivirus killer program to disable the antivirus software. Then the backdoor is deployed and installs itself, allowing the attacker to remote the victim's computer. Meanwhile, the backdoor sends an email to notify the attacker and establish an outbound connection over a port. Thus, the research suggested putting a network sniffer between the victim's computer and the internet, in order to capture the notification output.<sup>439</sup>

#### 1.2 Scenario 2

A worse scenario is the Trojan is designed not only with backdoor and antivirus killer, but also with a firewall killer and false registry entries. A firewall killer program can disable personal firewall software, and false registry entries will make a routine to implant false registry keys into the victim's computer, in order to ensure

---

<sup>438</sup> Haagman, Dan & Ghavalas, Byrne (2005), Trojan Defence: A Forensic View, Digital Investigation 2, 23-30.

<sup>439</sup> Haagman, Dan & Ghavalas, Byrne (2005), see supra note 438, 27.

stealthy start-up if rogue processes.<sup>440</sup> This is more complex to be detected.

### 1.3 Considering Volatile Evidence

Generally the digital forensics will follow this primary rule for processing a computer crime scene, which is “to acquire the evidence without altering the original.”<sup>441</sup> Thus, in most situations, the forensic practitioners will choose to “pull the plug” to ensure the evidence on the hard disk remain intact, while volatile information such as running processes, network connections and data stored in memory are lost. This research enhanced volatile information should be gathered especially considering a potential Trojan defense. *“A list of open network ports can help support or refute the presence of an active backdoor, memory often contains useful information such as decrypted application or passwords, sometimes malicious code that has not been saved to the disk and only runs from memory can be obtained.”*<sup>442</sup>

## 2. Standard Operating Procedure

A Trojans defense forensic procedure is a necessary forensic procedure when the computer is claimed to be threatened by viruses, Trojans, backdoors, or other malware. There are some factors should be considered in this procedure, such as identity of the defendant (possible offenders/innocent), un/infections of the malware, and comparison of records of digital activities. The processes is first to determine the possibility of the offender and the innocent based on currently obtained digital evidence, then to detect and analysis the malware in the disputed computer, and finally to discriminate digital activities according to various records collected.

---

<sup>440</sup> Haagman, Dan & Ghavalas, Byrne (2005), see supra note 438, 27.

<sup>441</sup> Kruse, Warren G. & Heiser, Jay G. (2002), Computer Forensics: incident response essentials. Indianapolis: Addison-Wesley.

<sup>442</sup> Haagman, Dan & Ghavalas, Byrne (2005), see supra note 438, 28.

## 2.1 Detecting the Trojan

If the Trojan was found in the disputed computer, then further questions should be considered, such as whether this Trojan is reliable (Maybe someone implant it after the crime.), or whether other malware or Rootkit exist. The forensic practitioners need to identify the type of the Trojans, to learn the way this malware invaded, and to find the time this malware invaded and data generated by this malware. The time stamp is useful to compare digital activities recorded in the computer and the assertions made by parties. There will be two possibilities depending on the identity of the defendant: First, the perpetrator attempts to clear him himself and carefully crafted this crime scene. He may intentionally implant a Trojan to confuse the forensic practitioner. Second, the defendant is actually innocent. The forensic practitioners should not make any assumptions about the parties or have any stereotypes. They should be judged these digital activities in a fair principle, and then fairly present results of these two possibilities.

On the other hand, the Trojan was not found in the disputed computer. The forensic practitioners need to consider whether the Trojan really do not exist, and whether there is human error or evidential pollution problems. These situations will cause the evidence lose its reliability and will not be admissible at trial. Combining with the identity of the defendant, we might get two possible results. First, the forensic practitioner found the solid evidence to refute this offender's unfounded defense. In this situation, the offender may be unable to provide evidence to prove his innocence; therefore he argued an unfounded defense in order to disrupt the investigation. Second, although the defendant is actually innocent, there is no trace to show his account or computer was invaded. In this case, the defendant's defense will be rejected by the court, as the same result as the first situation. The Forensic

practitioner needs to conduct further procedure to determine these digital activities.

## 2.2 Digital Forensics of Digital Activities

After detecting the Trojan, the forensic practitioner should further consider digital activities in the disputed computer. Even though there existed a Trojan in the disputed computer, it does not naturally represent related to the improper digital activities. In this procedure, the forensic practitioner is obliged to find the evidence, proving improper digital activities actually existed in this computer. For example, the forensic practitioner can use time stamp to determine the defendant's alibi. Digital activities can be divided into two categories by objects, which are Host-based evidence and Network-based evidence. The audit records in the disputed computer are Host-based evidence, including the system files, digital media, time, and audit records. The audit records in the internet are Network-based evidence, including external connections records, connection time or connection port information, or ISP audit records. According to the content of Host-based evidence and Network-based evidence, forensic practitioners analyze digital activities and the defendant's statements, and meanwhile range degree of evidence probative force in accordance with obtained digital evidence. Therefore they can present stronger digital evidence at trial.

In summary, we can further discuss technic issues of the Trojan defense invoked in the following two scenarios.

## 2.3 What to Do When Malware is Found

When the forensic practitioners have found the malware in the defendant's computer, they need to (1) identify the capabilities of this application through information provided by antivirus vendors or use the process of reverse engineering to make sure the natures and functions of this founded malware; and (2) point out how

the malware was installed on the system, when it is installed, and if it was ever run.<sup>443</sup> Besides, finding the malware doesn't mean it should be responsible for the illegal activity. The better countermeasure is to find evidence to show that a specific user did this illegal conduct. For example, the forensic practitioners may consider the login records provided by ISP to show the network traffic while the crime is conducted, or discover the records of account assessing to build the connection between the defendant and the internet crime or the alibi for him.

#### 2.4 What to Do When Malware is not Found

When the forensic practitioners didn't find the trace that a malware was implanted in the defendant's computer, he may claim another reason to explain this no-malware-found situation. For example, the defendant may further claim that a **wiping tool**<sup>444</sup> is used in his computer. A wiping tool is used to eventually overwritten the deleted data space by computer, for prevent this data being recover. Receiving a delete instruction, most currently operating systems will mark the deleted data space a free space, rather than wipe data by default, and a special application is needed to be installed. As other software used in the computer, a wiping tool cannot uninstalled itself, and some trace must be found in this computer asserted using a wiping tool. Thus, there are three countermeasures to rebut the defendant's claim.

The first countermeasure is trying to find operating-system-generated copies of the un/installed records of a wiping tool in temporary files and in memory. These copies are also created by the operating system in memory, but lost when a computer is powered off. Additionally, when the memory is full of data, some of the data will be

---

<sup>443</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), The Trojan Horse Defense in Cybercrime Cases, 21 Santa Clara High Tech. L. J. 1., at 49.

<sup>444</sup> This thesis introduced "wipe disk" with the same function in Chapter 3.

saved to the swap space<sup>445</sup>, and exist after the computer is powered off. If the operating system does not wipe data by default, the temporary files and swap space may contain evidence of malware or the wiping tool.<sup>446</sup>

The second countermeasure is considering that wiping tools may leave signatures behind. The low-level system structure may show signs that a wiping tool was used because one of the entries is all zeros or has invalid data.<sup>447</sup> However, these signatures will be overwritten by normal system activity, so the time factor is important for forensics. The third countermeasure is used when no malware has been found and signatures of wiping tools have been found. The forensic practitioners cannot conclude directly that maybe a malware is existed and related to the illegal activities. They need to consider further the possibility of wiping the asserted malware or actually wiping other files or soft wares, such as wiping sensitivity data.

### **3 Other Forensic Solutions**

#### **3.1 The Stepwise Discriminant Analysis**

In order to provide forensic practitioners an objective standard to determine whether contraband images were intentionally downloaded or downloaded without the defendant's consent or knowledge, a 2004 research<sup>448</sup> created a method with the stepwise discriminant analysis to solve this question. According to this research, they run four scenarios with seven variables in three trials using a 10 GB master image of Windows XP install, and analyzed the resulting data by the stepwise discriminant analysis. These four scenarios are (1) the innocent defendant visits a website with pop

---

<sup>445</sup> Simply, the swap space is the operating system splits hard disk space as use of the memory, in order to make sure that system will not be crashed, when the memory is full of data. The further introduction can find at <https://en.wikipedia.org/wiki/Paging#SWAP-SPACE>.

<sup>446</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 50.

<sup>447</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 50.

<sup>448</sup> Carney, Megan & Rogers, Marc (2004), The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Volume 2 Issue 4.

outs that contain illicit images, but immediately closes the window; (2) the innocent defendant downloads and unzips an archive file that seems clean, but contains illicit images; (3) An attacker is remotely controlling the innocent defendant's computer and downloads the illicit images and save them to his home directory; (4) the guilty defendant visit the website containing illicit images, saves them to his home directory, then views and saves these images to a floppy disk, and opens them once from the disk. Thus the researchers concluded seven variables may help to determine the defendant's intention downloading these illicit images. These seven variables are (1) average of the difference between file creation times; mode of the difference between file creation times; (3) median of the difference between file creation times; (4) number of references to contraband items stored on local disk in the Recent Folder; (5) number of references to contraband items saved to/ opened from external devices in the Recent Folder; (6) number of thumbnails that exist for contraband images; (7) number of images created within five minutes of visit to contraband websites. Variables (1) to (3) is picked up based on the premises, that human response time is much slower than automated processes. Variables (4) and (5) use the function of the Recent Folder as the measure. The Recent Folder will record any files recently saved or opened from local or external disk, and basically number of references to these digital activities must be zero, if the defendant is innocent (except the case of being hacked). If the defendant unintentionally downloads these illicit images, it is less likely he will have viewed the directory and the thumbnail theoretically will not be created. (Variables (6)) And the last measure, Variables (7), is intended to distinguish between situations whether the defendant has visited the contraband website or not.

As the results, 100% of the cases were classified correctly and the cross-validated accuracy rate was 83.3% using these variables. Thus this research indicates that it is possible, with a given statistical significance and accuracy rate, to determine whether

the defendant owns illicit images in his local or external disk with intention, and the use of discriminant analysis can provide an empirical foundation<sup>449</sup> for determining the veracity of the defendant's explanations. The limitations of this research are the small sampling data, and the sensitivity of chosen variables, but are not uncommon in other forensic sciences.

The way to apply this research to the Trojan defense is that, first, to build a number of alternate scenarios for how the Trojan could have been installed and operated without the defendant's knowledge. The second step is to list variables of the hard disk or network traffic record<sup>450</sup> they would expect to be different between scenarios, such as registry keys,<sup>451</sup> file creation time, alibis, etc. Then the forensic practitioners have a large number of trials done for each scenario in an appropriate environment. The third step is using the discriminant analysis to determine which variables are useful, what the level of significance is, and how often the model is correct. This research concluded, "*Once the discriminant model has been created, evidence gathered from the suspect's computer and ISP could be measured for the same characteristics and by using the discriminant functions as demonstrated earlier, classified with a known level of significance and accuracy.*"<sup>452</sup>

### 3.2 The Event Reconstruction Process

This process is trying to reconstruct digital crime sense, and to determine if evidence was created by a user of the computer or an attacker using a back door.

Further discussion can be found in Chapter 3.

---

<sup>449</sup> Especially large enough trials would reduce the uncertainty to acceptable levels.

<sup>450</sup> Evidence used could include more than simply the hard drive image in the case of Trojan defense, and records from ISP would also be useful in establishing a timeline.

<sup>451</sup> If the key records show a spam program has been run a hundred times, it may provide a clue for intent.

<sup>452</sup> Carney, Megan & Rogers, Marc (2004), The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Volume 2 Issue 4, p. 7.

## **Section 3 Legal Issues**

### **1. Definition of Trojan Defense**

This SODDI defense in fact has been existed in legal system for a long time. The defendant always argues his charge and contends some other person did it instead of him, no matter this defendant is guilty or not in the reality. It is very common in practice, and the situations include intrusion of the unknown third party, such as the Trojan defense, and defending the credibility of evidence obtained by law enforcement or parties. Now how the court faces these various defenses is in focus.

So-called Trojan defense means the defendant argues that internet attacks are not relative to him, but are conducted by hackers through implanting the Trojan in this disputed computer. In this era of rampant Trojans, these situations do occur.

### **2. How the Trojan Defense is used**

There are two scenarios that the defendant will raise the Trojan defense. First, the defendant argues he did not commit the crime, which means the crime was committed but attributes its commission to someone other than the defendant. Second, the defendant technically committed the crime but lacked the *mens rea* required for conviction, which means the defendant engaged in conducting the crime but lacked intention. In the first scenario, the defendant attempts to raise a reasonable doubt in his case, and he tries to deny his intention in the second scenario.

#### **2.1 Raise Reasonable Doubt**

While a Trojan defense is raised, the defendant gives the jury an alternative theory of the crime, which he tries to raise a reasonable doubt in his case, and let the jury believe the true offender is someone other than him. The defendant is not obligated to identify who is that true offender, but need to raise the jury's doubt to a

reasonable level, which means the defendant's proposal can convict a reasonable third party to believe it may possibly happen. Then the prosecutor must show that malware was not responsible for the commission of the crime charged in this particular case.<sup>453</sup> Therefore, in the evidence law, a Trojan defense is used to reduce reliability of theory of crime made by the prosecutor and also the prosecutor is obligated to provide evidence to prove that the defendant's theory is not reliable.

## **2.2 Negate mens rea**

*mens rea* (Criminal mentality) and *actus reus* (crime) are the two basic elements of subjective and objective aspects of the crime in the common law system. *mens rea* is the mental state should be condemned by a society, when the perpetrator implements of a social harm behavior. It includes intention, knowledge, recklessness, and negligence in legal category. A criminal case cannot be built in lack of any one of the two elements. Some defendants use the Trojan defense merely to deny their *mens rea* in the situations where these defendants cannot deny they engaged in conduct that constitutes the *actus reus* of the crime.

## **2.3 Establishing the Defense**

To establish a Trojan defense, the defendant has to introduce as least some evidence establishing (a) a Trojan horse program or other malware was installed on his computer (b) by someone else (c) without his knowledge.<sup>454</sup> In the situation a malware found in the defendant's computer, he may point out the malware found in his computer was responsible for the conduct being attributed to him, in order to support his defense. Once again, the prosecutor has the burden of proof, which he needs to prove this malware didn't exist during the time of crime, or it is irrelevant to this illegal conduct. In other situations, there might not be the malware in the

---

<sup>453</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 17.

<sup>454</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 18-20.

defendant's computer, and the defendant is hard to raise a reasonable doubt merely by presenting the malware. The defendant may assert he is lack of knowledge of the computer technology and remind the jury the high risks of being hacked, or he may "deliberately" leaving his computer unsecured to support the possibility to be hacked.<sup>455</sup>

### **3. How can the prosecution respond**

#### **3.1 Establish Defendant's Computer Expertise**

When the defendant claim as above that lack of knowledge led to his computer was invaded by the Trojan or other malwares, the prosecutor may be able to show the defendant actually has the knowledge of computer technology to rebut the defendant, such as prove the defendant is a black hat hacker,<sup>456</sup> or he work in the computer security field. Or contrarily, the defendant asserts he has computer expertise and then challenges the reliability of the forensic report, in which they don't find any malware in the defendant's computer. The prosecutors can response even though the defendant might have some expertise, but he is not expert in computer forensics. If the forensic practitioner could not locate the Trojan, there is no reason to expect the defendant can identify the Trojan or realize it has been implanted in his computer.<sup>457</sup>

Prosecuting a knowledgeable defendant is difficult, but the prosecutor can use the defendant's computer expertise to argue this defendant is less likely to fall victim to such an attack, when this defendant invoke a Trojan defense. The prosecutor can build his argument successfully based on evidence of the defendant's computer expertise, including testimony about the defendant's general computer expertise, as well as testimony from expert witness who can show that the computer was protected by a

---

<sup>455</sup> Micah Joel, Safe and Insecure, Salon.com, at [http://www.salon.com/2004/05/18/safe\\_and\\_insecure/](http://www.salon.com/2004/05/18/safe_and_insecure/)

<sup>456</sup> A black-hat hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain. [https://en.wikipedia.org/wiki/Black\\_hat](https://en.wikipedia.org/wiki/Black_hat)

<sup>457</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 22.

firewall and by up-to-date antivirus software, especially when the malware is not found.<sup>458</sup> Moreover, the prosecutor can use the defendant's computer expertise to point out in front of the jury the trend that the defendant preplanned his Trojan defense or suggested his counsel to do it.

### 3.2 Character Evidence

In order to exclude the prosecutor's strategy of using the defendant's computer expertise against himself, he will raise the issue of character evidence in two scenarios.

#### 3.2.1 Federal Rule of Evidence 404 (a)

First, the defendant may challenge that the prosecutor is improperly introducing character evidence against federal rule of evidence 404 (a) (1), which states "*Evidence of a person's character or character trait is not admissible to prove that on a particular occasion the person acted in accordance with the character or trait.*" Character evidence denotes an individual's personality traits, such as a violent disposition or honesty.<sup>459</sup> This principle blocks resort to the general propensity argument, for example, the prosecutor claims the defendant has violent disposition, therefore he must be the murderer in this violent case. However, the prosecutor can respond, that evidence of the defendant's computer expertise and the expert witness's testimony are not part of the defendant's character, thus Rule 404 (a) is not applicable.

#### 3.2.2 Federal Rule of Evidence 404 (b)

Second, the defendant claim that the prosecutor attempts to use evidence of the defendant's act to prove as aspect of his character by showing act in conformity with

---

<sup>458</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 23.

<sup>459</sup> Fed. R. Evid. 404 Advisory Committee's Notes.

that character trait. For example, the defendant claim, that the prosecutor argues that since the defendant secured his computer leading to no malware founded, he is responsible for the illegal conduct, instead of the Trojan. Therefore, it is the situation under federal rule of evidence 404 (b) (1)<sup>460</sup>, and this evidence should not be allowed.

On the contrary, the prosecutor can response the defendant's claim with federal rule of evidence 404 (b) (2)<sup>461</sup>, that is, the prosecutor just want to use the evidence to prove the defendant's "*motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident*" in this case. Then this evidence should be allowed. However, the court may want to give a limiting instruction to reduce the potential prejudice resulting from introducing such evidence.<sup>462</sup>

### 3.3 Negate the Factual Foundation of Defense

There are two basic tactics law enforcement can use to negate the factual foundation of a Trojan defense.<sup>463</sup> First is using the technical analysis to rebut the defendant's claim. In this tactics, the prosecutor has different argument in two scenarios: when the malware has been found or has not been found. In the first scenario, the prosecutor will focus on whether this malware could have functioned as the defendant claims, and in the second scenario, the prosecutor will focus on whether there is the wiping tools installed in this computer.<sup>464</sup> Another tactic is a traditional legal approach used in every criminal case, which is an approach to establishing motive, intent, and culpable conduct. In the case of Trojan defense, on the one hand, the prosecutor can show the extent to which this computer was utilized for unlawful

---

<sup>460</sup> Federal Rule of Evidence 404 (b) (1) states, evidence of a crime, wrong, or other act is not admissible to prove a person's character in order to show that on a particular occasion the person acted in accordance with the character.

<sup>461</sup> Federal Rule of Evidence 404 (b) (2) states, his evidence may be admissible for another purpose, such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident.

<sup>462</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 26.

<sup>463</sup> Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), see supra note 443, at 26.

<sup>464</sup> Issues have been discussed in section 2 of this chapter.

purposes; on the other hand, the prosecutor can point out how the evidence relating to the crime is stored on the defendant's computer.

#### 4. A General Way to Judge

The important issue raised by the Trojan defense in the legal system is how to prove the defendant is that criminal committing that crime. While the case is related to digital activities, the issue turns to be how to connect the virtual criminal activities to the real person. Basically, we need to determine what kind of crime it is and what features it has, and then we can deduce behavioral characteristics of this crime. Comparing with digital evidence obtained, we may find the possibility of the accused crime. Now we apply this judging model in the case of child pornography photos where the Trojan defense is most commonly raised.

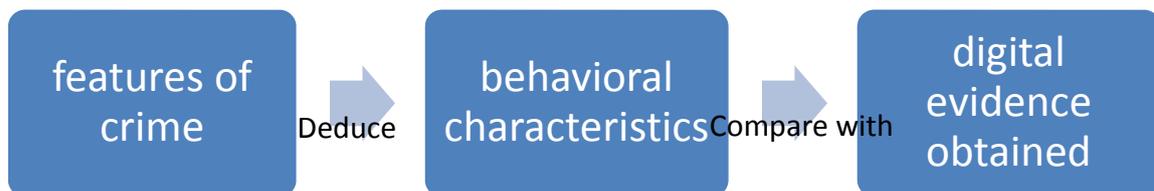


Figure 13 the way to judge the Trojan case

##### (1) Child pornography photos

In this situation, the defendant always argues those child pornography photos found in his computer were not downloaded by him. There must be someone hacked or implanted the Trojan to do that. Some features of this crime are numbers of child pornography, the perpetrator's preferences, and the perpetrator's sexual habit. These offenders interested in child pornography mostly search these photos online and "appreciate" these photos one by one, looking pictures carefully and slowly, maybe with their fantasy. It is a typical pedophilia's behavioral characteristic in this type of

crime. If the forensic practitioners collect some digital activities such as these thirty child pornography photos were downloaded at the time as the package, or these thirty different website were accessed at the same time or at one second, it raises a probable cause that these photos may be downloaded by a machine. Because according to the behavioral characteristic above, if the defendant is a pedophilia, for the preference or the pursuit of inner desire, the defendant may prefer to view these photos one by one than download them as package. That is how we compare a person's behavioral characteristics with digital evidence to determine the possibility of the accused crime. Of course, there are far more factors we need to think about. Here it is just a simple example.

## (2) Account theft

Another case that the defendant will raise the Trojan defense to argue his charges is that his account was stole by someone and this someone did malicious activities, while the prosecutors charge the defendant committing a crime based on his account as evidence. For example, in a case of internet trading fraud, a thief used A' account to trade with the victim (buyer), and took the money but did not have the goods sent to the buyer. Thus, prosecutors accused the account holder, A, of fraud. The defendant A argues that his account was stolen, but the police cannot find the IP address which is used by the thief to connect the buyer in trade.

Due to very common situation of account theft, the defendant's claim is likely to be true. But the point is how to prove. In this case, the behavioral characteristic is using other's account, which means, the thief in theory will connect this account through a different IP address. Thus, the first step is to request the trading platform to provide use records, and to confirm which IP address is connected to this account during the time of trading. There are two possible situations as follow. First, the IP

address doesn't belong to the defendant, such as it comes from another country. Then it is highly possible that the defendant is innocent, unless he presented in that country during that time or he used the VPN to hide his IP address. The latter situation requires further digital forensics to prove. Second, the IP address belongs to the defendant. In this situation, the only way to prove the defendant's innocent is that his computer was implanted the Trojan and someone use it to control his computer to commit the crime. Thus, this situation also requires further digital forensics to prove (a) the Trojan was actually implanted in the defendant's computer, or some trace of Trojan can prove it, (b) this Trojan did these malicious activities in this case, and (c) other circumstantial evidence can prove the defendant has no relevancy with these malicious activities, such as the defendant has the alibi while these malicious activities occurred.

### (3) Computer is hacked

There is another common situation that the defendant will raise the Trojan defense when he claims that his computer was hacked. For example, the mainframe computer of the A company was hacked and most data inside were deleted, causing a huge amount of loss. The police trace the invading IP address and find it belongs to the former employee B, and then bring B to justice. B argues he didn't invade A's computer to delete the data. There was someone implanted the Trojan into his computer and controlled it to commit the crime.

In this case, if B's argument is true, then the forensic practitioners must find (a) the Trojan was actually implanted in the defendant's computer, or some trace of Trojan can prove it, and (b) this Trojan did these malicious activities in this case. Furthermore, factors (a) and (b) only prove a Trojan related to the crime actually existed in the defendant's computer. To prove the defendant's innocent, technically

factor (c) other circumstantial evidence is required, but in legal system, inverting the burden of proof occurs. That is, the prosecutor and the police need to prove B is the person who invade A's computer. In this case, a solid structure of evidence to prove that the defendant is the person who invaded the victim's computer at least contains the crime result of the deleted data base, the invading IP address related to the defendant, and other circumstantial evidence to connect the defendant and this invasion.

## 5. Judging by circumstantial evidence

For the purpose of connection the malicious actor on the web to a specific person in the real world, it is not enough just to prove the Trojan existed in the disputed computer. More evidence is required to prove the relationship between the defendant and the crime, which is called circumstantial evidence, "*evidence that relies on an inference to connect it to a conclusion of fact.*"<sup>465</sup> Modern legal system does not provide the quantity or quality of circumstantial evidence. Whether the circumstantial evidence is trustworthy depends on a jury in the case law system or judges in the civil law system to decide whether they are convinced by the circumstantial evidence and its advocated arguments. It applies the same rule in the Trojan defense case.

For example, someone stole the victim's account and password in an online game. Then he accessed the victim's account and stole all the virtual treasures. The police traced the invading IP address, found the defendant have that IP address, and brought the defendant into justice. The defendant claimed his computer was hacked. He argued his computer is continually connecting the internet 24 hours a day without setting a firewall, and everyone is easy to invade his computer. The defendant also claimed that he has the alibi during the time of incident. In this case, the invading IP

---

<sup>465</sup> [https://en.wikipedia.org/wiki/Circumstantial\\_evidence](https://en.wikipedia.org/wiki/Circumstantial_evidence)

address is the only direct evidence provided. The prosecutor needs more circumstantial evidence to build the case.

The point in this case is to link the defendant to the malicious actor online. Except the trace of the Trojan in this disputed computer, several other factors should be considered as follow: (1) the hacker's habits; for example, a hacker impossibly access the victim's account through the defendant's IP address every two days in six consecutive days. According to the hacker's habits, he may have many accounts and passwords, and it is necessary to access one account so frequently increasing his risks. (2) poor connection quality through the Trojan; for example, since the hacker already got the victim's account and password, it is more reasonable that he access this account through an internet café. Because there the hacker can get better speed and quality of network connection and also can hide him himself easily. The connection is poor, if the hacker connects to the defendant's computer through the Trojan, and then remotes this computer to access the victim's account. (3) Unreasonable alibi; for example, the defendant claimed when the case occurred he was not at home. He was helping his brother move the house in the neighborhood and then stayed there for nights. But according to the investigation, his brother lives just next door to the defendant and states he didn't remember whether the defendant stayed in his house overnights and the exactly date. (4) Timing of reboot the computer. For example, while the judge asks the defendant to send his computer to do digital forensics, the defendant states that he just reboot his computer one day before. This is quite doubtful that the defendant formats his system at this timing. Although it is not impossible to recover the data in a formatted computer, the fact that the defendant picked up this time to reboot imply he want to hide something. This can be the circumstantial evidence to support his guilty.

## **6. Reinforcing evidence**

As mentioned above, circumstantial evidence is used to supplement the insufficient of direct evidence and links evidence and facts of the case through inference. However, how much evidence can be called “sufficient” to build the case? Here we will discuss the reinforcement of evidence.

The first question is, like many cases, the prosecutor only have the invading IP address as evidence. This is also the situation for many network intrusion cases, in which cases the main evidence are results of the crime (ex. The deleted data base or the stolen virtual treasures), and suspected attacker's IP records and actual registrant through further detecting the records. But it is doubtful that this actual registrant is exactly the attacker. The most common situation is the police traced the records and found the network administrators. Network administrators will receive subpoenas, which state the IP address they own is involved in attacking other computers, and they are obligate to cooperate with investigation and defense at trial. Moreover, if the hacker attacked other computers through their computer all around the country, the network administrators will be busy complying subpoenas from local courts, even though they are one hundred percent innocent. Therefore, in the case that the suspect doesn't plead guilty, the prosecutor should not build the case just by results of the crime, and the suspected attacker's IP records. The prosecutor needs other evidence to reinforce his case. In this situation, the prosecutor may ask network administrators to provide evidence can prove their computers were attacked, such as the implanted Trojan, unknown login records, or abnormal digital activities in their computers.

The further question is how to reinforce evidence in a case. The answer will be found case by case. For example, in that “computer is hacked” case, the prosecutor has two kinds of evidence: the suspected attacker's IP records and results of the crime

(deleted data base). About the suspected attacker's IP records, the prosecutor may reinforce evidence on the possibility of the Trojan invasion. He can send this disputed computer to do digital forensics, to find whether there is the Trojan involved. About results of the crime, the prosecutor may reinforce evidence on the defendant's alibi during the time of invasion. It is obvious, if the defendant cannot or didn't use his computer to connect the network during the attack time, or the connections neither came from the place where the defendant was nor were used VPN to pretend from there, the defendant has the alibi, which may prove his innocent. Besides, the prosecutor also can use the connection between results of the crime and the suspect's past position to reinforce evidence in this case. If the suspect was the network administrator in the victim's company, he has more knowledge and chances to commit this crime than in another situation, if the suspect was the accounting in the company with little knowledge on computer science.

For another example, in the stolen virtual treasures case, the prosecutor also has two kinds of evidence: the suspected attacker's IP records and results of the crime (the stolen virtual treasures). About IP records, the prosecutor can reinforce evidence on the possibility of the Trojan invasion, and about results of the crime, on the defendant's alibi during the time of invasion. The prosecutor can further reinforce evidence on results of the crime through proving the possibility that a hacker playing the online game through the defendant's computer with bad connection quality.

In sum, we can conclude three points for reinforcing evidence in the Trojan defense cases. First, the possibility of the Trojan invasion can be used to reinforce evidence on the suspected attacker's IP records, and it can be proved through digital forensics. Besides, we need to think further, that is, if we cannot find the Trojan in the defendant's computer, it doesn't mean there was no the Trojan in this computer; even though we found the Trojan in the defendant's computer, it doesn't mean this Trojan

was related to the attack activity. Second, the connection of the case and the possibility of being hacked can explain the relationship between the defendant and the case, emphasize the defendant's motivation and reinforce the evidence on results of the crime. For example, the former employee is disgruntled to be fired, and invaded the company's system and deleted data as revenge. The prosecutor can make a complete story by profiling this former employee, such as he was the network administrator, who is familiar with the company's system, in order to link the defendant to this case. Third, the defendant's alibi is always the best way to reverse the burden of proof. For example, the defendant can raise his alibi and convince the court. If it is accepted by the court, then the prosecutor is obligated to turn over this alibi or rebuild another story to convince the judge or jury that the defendant actually committed this crime.

## Summary

1. When the Trojan defense is raised, the legal system cannot determine whether a Trojan exists, but it moves the burden of proof between parties. For example, it is the prosecutor's obligation to prove the defendant implemented a fraud online. But when the defendant objected with a Trojan defense, that is, the defendant claimed there is someone else did it, but not he, then the defendant need to provide evidence at least to prima facie level to convince the court there might be a hack invaded his computer. If he succeeded, then it is the prosecutor's turn to prove his original theory (the defendant did it), or to prove this case is not related to the Trojan.
2. The forensic practitioners usually can provide evidence to prove possibility of being implanted a Trojan, and relationship between the Trojan (if found) and this disputed malicious digital activities. The standard operating procedure is firstly to detect the Trojan, and secondly to make digital forensics of digital activities. When a malware is found, forensic practitioners need to identify this malware and its invading traces to prove this malware is related to the case; on the contrary, when the malware is not found, forensic practitioners need to prove no wiping tool is used. Then they can conclude the malware is not related to this case.
3. The defendant can use the Trojan defense to raise reasonable doubt, negate mens rea, and establish the defense. And the prosecutor can respond to the defendant's Trojan defense by establishing defendant's computer expertise, and negating the factual foundation of defense. For a judge, circumstantial evidence and reinforcing evidence are necessary, because even using forensics, there is still a gap between this virtual crime and the real person who did it.
4. The forensic science can prove the computer was invaded by a hack or implanted

a malware, but it is hard for forensic practitioners to build a solid or real connection between the computer and the real criminal. Unfortunately, there is only one thing that the legal system wants to prove, which is who did this crim. Thus defendants and prosecutors provide more circumstantial evidence to reinforce their theory, in order to convince the judge or the jury to believe their story and make the favorable judgment for them.

5. We can find the different between the forensic science and law in this Trojan case. The forensic science proves the past fact, whether there was the malware; but the legal system construct the past fact, that is the defendant who did it or who did not do it.

## Reference

1. Bowles, Stephen & Hernandez-Castro, Julio (2015), The First 10 Years of the Trojan Horse Defence, Computer Fraud & Security, January 2015, 5-13.
2. Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), The Trojan Horse Defense in Cybercrime Cases, 21 Santa Clara High Tech. L. J. 1. Available at: <http://digitalcommon.law.scu.edu/chtj/vol21/iss1/1>
3. Carney, Megan & Rogers, Marc (2004), The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Volume 2 Issue 4, Available at: <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B2CCCB-E6FC-6840-AF4A01356B9B687A.pdf>
4. ED Skoudis & Lenny Zeltser, Malware:Fighting Malicious Code, Prentice Hall press, 2003.
5. Haagman, Dan & Ghavalas, Byrne (2005), Trojan Defence: A Forensic View, Digital Investigation 2, 23-30.
6. Wang, Shiuh-Jeng, Lin, Chu-Hsing & Tso, Ray-Ln (2013), Digital Forensics and Security in Applications of Computer and Mobile Systems, DrMaster Press, Taipei: Taiwan.

## **Chapter 7 Finding Fact through Social Media Evidence**

This chapter is based on the above discussion of social media evidence (SME) to further analyze how the court has made a statement of truth through the evidence law, what is different from the scientific statement of truth, and how the court uses science or scientific features of SME to form its own authenticity of culture. This thesis will focus on the scientific nature that SME has, such as using internet technology, information or IP address obtained through digital forensics, detecting malwares by soft wares, etc. This scientific nature plays an important role to influence the fact finder (the judge or the jury) to decide what the fact is in a criminal case.

From the discussion in Chapters 4 and 5, it can be seen that the use of SME can be interpreted as a court attempt to link the information on the social network with the crime or criminals in reality to prove that the past criminal facts exist. The most common way of obtaining evidence is to allow the litigants to directly print out the information they need. In the United States law, it is mainly through the verification procedures to make these printouts admissible; And in the Taiwan law, the court usually requires the consent of the parties to make evidence admissible, and the investigative procedures of these printouts are to read them in the courtroom as documentary evidence or to display them through computer or such instrument as an inspection by judges. Although the information on social network sites has a variety of properties, judges, prosecutors and litigation parties both believe that at least they can read the information content directly through the computer or related equipment assistance to understand. Of course, if the information obtained from social network sites is meta data, the court will conduct an audit and investigation of the evidence's ability through a system of accredited or expert witnesses. In addition, if the action of this link is questioned, for example, the printout of websites is correct or the account

is hacked, the most effective way to troubleshoot, the court believes, is to establish credibility through internet forensics. Behind this operation, it implies the judge's own understanding and trust in science and technology, and through this cognition and trust, judges form the legal influence on acceptability of the evidence (the effect is small) and the usage (the effect is impact). The impact may flood into other systems, such as the criteria for obtaining evidence in forensic science.

In fact, the way that building the past facts of the crime bases on forensic expert's report or evidence trusted by science cannot reconstruction the entire truth., which involves the entire social science and technology level and cultural value, as well as the judge's personal knowledge and integrity of the faith. The fact of judgements based on evidence made by these rules is rather the relatively convincing fact. Unlike the mainstream opinion that the purpose of the Code of Criminal Procedure is to find the truth, this thesis advocates, the purpose of the Code of Criminal Procedure is making the national penalty power justified. The legal system built a set of proceedings (including evidence screening and use procedures): prosecutor or plaintiff sues and submits evidence, the defendant and his defender deny and refute, the prosecutor reaffirms the arguments against the defendant, the defendant refutes again and makes the final statement, and finally the judge makes a judgment (or jury verdict) in accordance with the evidence presented by the two parties, reasoning in the judgment in order to let both parties accept the final restored fact by the court (The truth). If one party or both parties are dissatisfied, they may continue to appeal. However, most of the modern countries set restrictions of numbers of appeals and the importance of the case, in the reason of judicial resources and litigation economy. In somehow, the function of the modern state's criminal procedure law is a means of legitimizing state power, rather than finding the fact. The state gives the parties the opportunity to present their opinion through the design of criminal

procedure, in order to find an acceptable solution to quell the dispute between the parties. The purpose of the Code of Criminal Procedure is its own procedure, which will be more clearly to see through the SME operation.

In order to illustrate this argument, this thesis will discuss how the criminal proceeding thinks about the fact and the principle “evidence-based” judgement in present legal system. Behind these conceptions and principle in evidence law, we can found the ultimate goal ruling the whole proceeding in the present legal system, which is finding fact. Therefore, this thesis will analyze this main purpose of modern legal system and try to build the argument that the criminal proceeding is not the way to find the past fact, but the way to find the acceptable solution for parties and justify the state power to punish its own people.

### **1. The Status of Fact in Criminal Proceedings**

The division between Criminal law and the criminal procedure, in fact, has been presumed to the latter function is to prosecute the crime and punish the prisoners. Since the initiation of criminal proceedings is intended to result in a correct referee in accordance with the substantive criminal law, it is necessary to find the entity as a necessary prerequisite, that is, to find out what is happening in fact. Because it is only when the actual occurrence of what is the case, in accordance with the substantive criminal law to determine the incident does not meet the legal provisions of the crime, but also to get a correct decision.

Found that the entity is true, contains positive and negative meaning: for innocent defendants, only when the referee to confirm and reveal the innocent, it is found in the real entity; the other hand, for the real prisoners, only when the referee to confirm the facts of the crime When a penalty is imposed in accordance with the criminal law, the entity is true and correct. Therefore, the real meaning of the entity is found to be

absolutely free, without permission, to punish the crime.<sup>466</sup> Such ideas, which seek to discover the truth of the crime, do not tolerate innocence and innocence, nor allow the idea of impunity, are derived from the notion of justice and are therefore called the principle of justice.<sup>467</sup>

## **2. Basic Thinking of Evidence-Based Judgements**

The modern criminal procedure law advocates that the facts of the crime must be based on evidence. Article 154 II of the Taiwan Criminal Procedure Law provides that, “*The facts of an offense shall be established by evidence. The facts of an offense shall not be established in the absence of evidence.*” This is generally referred to as “evidence-based judgements principle”.<sup>468</sup> Therefore, according to evidence that the facts of the crime, that is, according to evidence to prove that the elements of the crime of criminal elements, that is, evidence of the object, is the elements of the composition of criminal law elements. Therefore, the elements of the composition of the criminal law, that is, to determine the facts of the crime to be admitted.

Identified in the criminal procedure law, has always been considered to belong to the court to investigate evidence of the auxiliary method. All kind of trace left behind after the crime is an important way to restore the truth of the crime. Therefore, after the crime of such a variety of evidence, is to become a criminal prosecutor to collect the object, but the prosecution of the criminal evidence collected whether it belongs to the perpetrators of criminals left, and enough to prove the use of crime? How should the court confirm that the evidence of the crime is related to the facts of the prosecution when the prosecutor sends the evidence of the crime collected at the scene of the crime to the court for its mercy? As a result of the prosecution sent to

---

<sup>466</sup> Yu-Hsiung Lin, supra note 154, p.7-8.

<sup>467</sup> Yu-Hsiung Lin, supra note 154, p.8.

<sup>468</sup> Pu-shing Chen, supra note 216, P. 13; Tun-ming Tsai, supra note 210, P. 195, Yu-Hsiung Lin, supra note 154,P. 450.

these criminal evidence, and some to the naked eye observation, you can know that it is related to the crime between the facts, but some criminal evidence, you can not only human senses to detect Its relationship with the facts of the crime. For example: in the crime scene to find hair, blood, fingerprints, cigarette butts, warheads, shoes and other crimes left after the traces of the traces of these traces only by the human facial features cannot determine the crime between the case of what Relevance. At this time, the court shall borrow the auxiliary method of scientific identification to investigate and determine whether there is any connection between the evidence of such crimes and the fact of the prosecution. This is the origin of “evidence forensics”.

Secondly, it is generally said that the evidence is a kind of relativity, and the evidence is so evidence that it must have the relevance of the facts, that is, the evidence is evidence of the existence of the fact that it is evidence of fact. In the case of the whole crime fact dealt with in the criminal procedure, the fact that the facts of the crime, which are usually caused by the facts of the crime (the core facts) and other corroborating facts, are evidence of the evidence and evidence of the fact that the natural offense can be divided into the core crime The core factual person refers to the fact that the crime was established, so the evidence of the core facts can be referred to as the core evidence, then the core evidence, the evidence of the innocence or the evidence; The establishment of the facts of the crime, and the facts of the evidence to prove the facts of the crime. The main scope of criminal evidence is usually based on the evidence of the establishment of the facts of the crime as the core, all the evidence concept is from the core concept, that is, the establishment of the crime or not the information, as the core foundation, The information of other facts, such as the motive of the criminal act, the objective condition of the criminal act, and the discretionary punishment, are all within the scope of criminal evidence, and the fundamental condition is the basis of the factual relevance of the evidence. The evidence is so

evidence, the fact that the relationship between the relationship 2, and the objective existence of the facts, whether it can be defined as a criminal fact? According to the requirements of the statutory principles of criminal law, a certain objective existence of the facts of the existence of the existence of the surface is a simple fact, whether it is a criminal fact, the subject of the legal composition of the binding or not, that is, the existence of a certain fact In the criminal law constitute the elements of the norms, the party was a criminal fact, this crime is the criminal procedure to prove the facts, At the beginning of the criminal procedure, it is necessary to identify the case with certain constituent elements as a guide, and to form evidence of its entity gradually, and finally to achieve a certain understanding of the fact that it meets the requirements of the elements, that is, in criminal proceedings the entity formation process. If, from the point of view of the law of evidence, the main proving matter in criminal proceedings is the fact that the constituent elements are.

Human rights protection is the world's universal value. Based on human rights protection, the crime shall be determined by evidence; and evidence shall be found in criminal facts. Therefore, the Universal Declaration of Human Rights, the World Convention on Human Rights, the European Convention on Human Rights and the United States Constitution Amendment are all unequivocal: the defendant has no self-certification obligations, and that the facts of the crime must be evidenced; with no evidence the court shall not be found in criminal facts. It has become the principle of presumption of innocence, to ensure the important principles of the defendant's human rights. Whether the evidence must be related to the facts of the crime has become the basis for the determination of the facts of the crime, that the prosecutor to submit evidence and the facts of the crime is related. And whether the association of the evidence of the crime is sometimes unknown, the court for the investigation of the evidence of the crime, it has the responsibility. However, some of the evidence of the

crime is complex, and often the judge cannot be unable to identify the evidence of relevance, when the court must be evidence of the relevance of the prosecution to be identified. Unfortunately it is the norm in legal practice. On the identification of evidence relevance, in the end the identification of the results are correct and credible, and on whether the evidence to determine the relevance of the right, and on the evidence whether the data have the ability to qualify, the court with the gatekeeper responsibility should have their own review. But the law should be based on the law to review the correctness of the report. So far, the domestic literature is still in-depth discussion. In view of the fact that scientific evidence is increasingly used as a criminal court to determine the facts of the crime, and scientific evidence is sufficient to become evidence, often become a case can avoid miscarriage of justice, an important indicator.

### **3. The Application of Forensic Science in Court**

In legal cases, forensic practitioners use the methods accepted by scientific communities, such as to identify, collect, save, analyze, report evidence, and other objective investigation procedures. They focus on scientific methods which can be repeatable and verifiable, to obtain evidence. Actually the forensic science helps the court clarify the classification and individualization of evidence at issue, and assists judges to form conclusions, or opinions in the case. So called the classification is an attempt to determine the original state or type of evidence; the individualization uses a series of traits to identify the evidence; and the conclusion is the result that derived from the fact, which should be an objective description. For example, finding the deleted Trojan horse program in the victim computer, the forensic practitioner can make the conclusion that this computer possibly has been installed the Trojans. As for the opinion, here it refers to conclusions made in accordance with scientific

knowledge, test results, or their own experience. Compared to conclusions, opinions are more subjective. For example, in the above case of Trojan, the forensic practitioner can infer the time that the victim's computer was installed the Trojans in accordance with the collected evidence and report it to the court.

However, the forensic report is not bound to restrain the court's decisions or the jury's judgements in the current legal systems. The function of this report in litigation is that an expert or witness reports or states his opinion based on the special knowledge or experience in the criminal proceedings, in order to supplement the court's knowledge of the dispute and to assist the judges or jury in judging the authenticity of the facts. Because the forensic report only has the function of supplementing the court's special knowledge of this case, the court can freely determine whether the appraisal opinion can be taken. So the court or the jury will not be forced to accept this forensic report definitely. In the case involved special knowledge or professional matters, the court shall investigate the suitability and credibility of this forensic report through the oral arguments, make the conclusion based on all information, and explain the basis of the evidence in the judgment.<sup>469</sup> Although the forensic practitioner has made *factum probandum* the ultimate conclusion, the court still needs to synthesize other evidence, and makes its own judgement, rather than being bound by this forensic ultimate conclusion.<sup>470</sup>

#### **4. Rethinking of Fact-Finding Function in the Criminal Proceedings**

##### **4.1 The Assumption of Fact Finding in the Criminal Proceedings**

Both the U.S. criminal suit and the Taiwan criminal suit point the ultimate goal of litigation to the issue of "true discovery." In the case of the United States law, the goal of criminal proceedings lies in the fact that the facts are reconstructed effectively

---

<sup>469</sup> Reference to Taiwan cases, No. 2074 Penal Judgment (2005) of the Supreme Court.

<sup>470</sup> Reference to Taiwan cases, No. 1657 Penal Judgment (2009) of the Supreme Court.

through the deduction and inference of evidence in the past, and the law is applied accordingly.<sup>471</sup>

However, the discovery of past, objective truth is in fact a difficult one, since this fact must have occurred for criminal proceedings, and no one can reproduce any moment of the moment. Therefore, the only solution to the criminal procedure is to take the broken down from past time and space, that is evidence. The reason why the criminal procedure law should discuss evidence is exactly the attempt to reconstruct this past truth.

Beginning with the introduction of the concept of "substantial reality" by the criminal system in the Roman Empire, any criminal prosecutor is constantly looking for where this truth lies. Initially, the litigant obtained the confession from the defendant, as no one knew more about the past than the defendant did. However, since the criminal procedure gained so-called "enlightenment", every scholar who specializes in criminal procedure law keeps telling us that other evidence should be used to confirm past truths rather than defendants. What is regrettable, however, there still seems to be a gap that seems to have to exist between "reconstructed past truths" and "past truths", even if criminal proceedings can reconstruct past truths through evidence. Facing this inevitable gap, the legal system must naturally have some ways of dealing with it. The basic idea of this approach is that the legal system believes that past and objective truths can be fully reproduced in criminal proceedings as long as they can find a way to "find out the truth effectively".

In fact, the most direct and effective choice of this approach is the use of so-called scientific evidence, because the court's task in the trial process is to rebuild past facts through the use of evidence. These fact-finders must have some tools to be able to assist them to identify the facts. Science, a system of knowledge about the study of

---

<sup>471</sup> Lilly, *An Introduction to the Law of Evidence*, 2nd ed., West Publishing, N.Y., 1987, at 1 & 5.

the objective world, happens to make a perfect combination with the Criminal Procedure Law at this level of “fact finding”.

Therefore, the structure of the Criminal Procedure Law is actually operating the following mode of discussion: First, setting the goal of litigation is to find out the truth, so criminal proceedings presupposed a few basic concepts:

1. The past and objective fact is there.
2. From this moment's perspective, fact-finders (judges or juries) can effectively (but not necessarily) perceive this truth through the reorganization of evidence.

These two basic assumptions can be said that the idea of the process of criminal proceedings. Until now, anyone with a slight concept of criminal procedure law could clearly recognize the existence of this view. In other words, regardless of whether the fact finder is separated from the legal judge in the entire litigation structure, the criminal procedure system considers that the fact finder has ability to find the truth, who can find the truth through collected evidence related to the crime fact at a certain degree. We can clearly find out in this argument, that the subject (fact finder) can recognize the object (the fact) at least in the level of fact finding. The purpose of the Criminal Procedure Law is to find the truth. These assumptions are in fact so-called “Mind–body dualism” in philosophy. Under the dualism, the criminal procedure law distinguishes the “fact finder” who observes the objective reality from the past and the “past and objective fact” that the fact finder has to know.

Therefore, a very basic phenomenon inevitably occurs: the Criminal Procedure Law has the same concept and the same philosophical position as the scientific discourse in the level of fact finding. This philosophical position is the so-called mind-matter dualism. It is of course possible to assist criminal proceedings in the entire fact-finding process by developing the scientific discourse of mind-matter dualism to the extreme, because science is the observation of the real world. When a

criminal fact finder is to carry out the real task of observing the external world, his ideal choice is to use science as a tool. In fact, scientific evidence emerges from such an idea and is used in criminal proceedings.

Therefore, we can find the following presupposition related law and science in the criminal proceedings:

3. As the science exploring the external objective world, if it can be used as evidence, then it certainly can be a good tool to find the facts.

Based on the above arguments, this paper argues that the operation of any scientific evidence in criminal proceedings is actually carried out under these three different presuppositions. The three presuppositions work together at the level of assertion of facts and further elucidate the facts of the past. Under this argument, scientific evidence, of course, is the discovery of the most powerful real weapon.

#### 4.2 Criticism of the Presumptions

It is worth pondering that these three presuppositions are actually not a natural thing. For example, prior to the development of criminal justice in Rome, the focus of criminal proceedings was not on “discovering the truth”, but on the community's internal or external reconciliation, so scientific evidence would not be highly effective at this level. From this perspective, the third presupposition is actually based on the first and second presuppositions. The reason why science can intervene in the field of criminal justice is actually by virtue of the first and second presuppositions.

However, if we analyze the scientific discourse on which scientific evidence relies, although scientific discourse appears apparently capable of solving the objective reality outside the human mind, in fact any scientific discourse is based on a specific position.<sup>472</sup> Similarly, in order to find the truth, criminal proceedings are

---

<sup>472</sup> Martin Goldstein and Inge F. Goldstein, *How We Know An Exploration of Scientific Process*, Da Capo Press: U.S.A, 1981.

naturally permeated with scientific objectivism when using scientific evidence, because the connotation of scientific evidence is a kind of evidential material exploring past truths based on scientific objectivism.

We can understand that the presuppositions of criminal proceedings may be problematic on two levels: First, the criminal procedural law default litigation subjectivity (fact finder) can find the objective reality. More appropriate argument about this point of view should be that the fact finder has constructed facts in his subjective consciousness and treated this fact as an objective reality; Second, scientific evidence aims at discovering objective facts. However, in reality, science does not reveal a true knowledge system. Science is only accidental in certain situations. Science's conclusion cannot be equated with objective reality. Science and reality are conceptually unequal and all traceability must be based on the subjective consciousness of the fact finder.

Through the examination of these two different levels, it is virtually impossible to prove some objectively existing fact in scientific evidence, because all facts are derived from subjectivity - that is, the construction of consciousness by fact finder.

From such an analysis, we can clearly see that the inequality between science and objective reality and the integration of this unequal gap through the sense of subject matter. The later happens to be the issue on “freie Beweiswürdigung/ Judicial discretion” in criminal proceedings. That is to say, although the scientific evidence presented in the trial court does not necessarily prove the criminal facts effectively, at least until all the facts are ascertained by the fact finder (ie the judge or the jury) and given the discretion of his freie Beweiswürdigung, a considerable conclusion can come out. Although the result is made through the awareness and thinking of the fact finder, it can at least be used in criminal proceedings as an objective and realistic alternative, and then the litigation ends. From the approach of Husserl, it is clear that

when we emphasize that all facts can be assessed by the fact finder's freie Beweiswürdigung, the result of the lawsuit is just getting one without knowing whether it equates with objective truth.

However, Luhmann uses another way of thinking. He believes that any truth is constructed under the operation of the social system. There is no so-called absolute real existence, because when the system distinguishes the system and the environment from the moment, the system constructs a "present truth". But this truth exists only in the "present moment" and does not have long-term stability. This "present truth" is rather than just the result of the "present" systematic observation. Therefore, the truth that is found under scientific discourse (ie, the scientific system) must be two things to discuss with the legal system. The legal system is based on the "legal / illegal" set of symbols in a real framework, while the scientific one is based on the set of "true / not true" symbols. The realities of these two groups of different symbols are entirely different levels of problems. No one set of symbols out of the real structure can be over the other group. In other words, neither the realities of the scientific system nor the realities of the legal system have absolute objectivity.<sup>473</sup>

In Luhmann's view, the issue of subjective consciousness is rather the product of a structural coupling. The concept of the subject is a product of the coupling of many social systems, biological systems and psychosocial systems. The presumed human subjectivity in European classical philosophy is actually a concept that never existed. Similarly, in criminal proceedings, all the facts and evidence presented in litigation are the choices of meaning that result from the operation of the social system. These

---

<sup>473</sup> Chueh-An Yen, Construction and Cognition: A Brief Comment on the Realism and Anti - realism of Jurisprudence by Luhmann 's Constructivist Epistemology, in Wen-Hsiung Lin ed., Contemporary Basic Law Theory, Sharing publish: Taiwan, 2001, P.338; Luhmann, Social Systems, trans. by Bednarz, Jr. & Baecker, Stanford Univ. Press, 1995, p. 25-26; Luhmann, Niklas, "The Unity of the Legal System", in: Autopoietic Law: A New Approach to Law and Society, Walter de Gruyter, Berlin 1987, pp.24-25.

choices of meaning are diverse and complex. It is impossible for us to make any absolute final judgment about these pluralistic and complex choices of meanings, so that certain facts or evidences are absolute in the pluralism of meaning and exclude the meaning of the original pluralism.

Then, in the course of Luhmann's approach, the *freie Beweiswürdigung* may become a measure of absolute certainty, since the *freie Beweiswürdigung* of evidence is a definitive conclusion on the many evidences of criminal proceedings. Because the specific meaning of a piece of evidence has been locked once it has been validated by the fact finder. Multiple openness of the original meaning naturally disappears. In addition, under Luhmann's analysis, the scientific evidence is only the product of the operation of the scientific system. It should not have any unique superiority *per se*.

#### 4.3 Discussion

According to the above analysis, it is clear that scientific evidence does not help the determination of fact, because whether we negate the first or second presupposition, the third presupposition will not be justified. Then a worthwhile question emerges, that is, if we can go straight to the third presupposition from the second presupposition without reviewing the first presupposition (The past and objective fact is there.), it is clear that the fact finder is unable to realize the fact. Therefore, the scientific evidence on the finding fact level cannot help the fact finder to determine the truth. In this case, the so-called "break" (*Entfaltung*) takes place between the cognitive ability of the subject (fact finder) and the object (known fact). Obviously, this view derived from mind-body dualism has no way to deal with the break here. In the same way, the scientific exposition, also derived from mind-body dualism, cannot deal with the cognition of subjects and objects in this situation.

In fact, such cases often occur in criminal proceedings. Take forensic psychiatric assessment as the example, it is a scientific method of identification that aims to assist

a judge or jury in ascertaining the facts. Therefore, identification technology is the tool that a fact finder uses to discover the truth. However, what is the problem that “whether the person is in the state of insanity” (fact which the fact finder has to find out) cannot be observed through the method of forensic psychiatric assessment. The reason for Husserl lies in the fact that “the fact finder always observes only in his consciousness. Even though he is shown through a psychoanalytic report, the fact finder still handles the fact that *whether the person is in the state of insanity* from his own point of view”.<sup>474</sup>

Hence, the question here will translate into: “How to deal with the fact that the fact finder has no way of identifying the facts”. In other words, it seems that the entire criminal legal system can collapse when scientific evidence cannot effectively assist the fact finder, because in any event, the fact finder's identification of the facts is forever rooted in the consciousness-centered hierarchy. Well, we are bound to find a reasonable way of arguing theoretically. As mentioned earlier, the solution to the Husserl theory lies in the profound understanding of the importance of subjective consciousness. In the sense of subjectivity, any conscious “object of intention” is merely a process of choice of meaning. In this process of choice of meaning, the perspective of the subject's consciousness on the subject of intention is determined by the influence of many different factors.

This point of view in the litigation system is that any fact finder cannot effectively ascertain the fact because all the problems are formed in his consciousness. The role of evidence here is not to prove the objective truth, but it only provides assistance for the fact finder to form the “intention of the object” in subjective consciousness. In other words, the function of rules of evidence still cannot be ruled

---

<sup>474</sup> Husserl, *The Idea of Phenomenology* (abbreviated as *idea*), trans. by Alston and Nakhnikian, Martinus Nijhoff Publishers, Hague, 1964, p. 15-16.

out. At this level, scientific evidence is also a way to assist the subject in understanding the intention of the object. Further, it must be noted that evidence may assist the subject to solve the problem, but the final result will still come from the fact finder's subjective consciousness. As long as the fact finder can take a complete view of the evidence, he should be able to obtain a result that is "reasonable" but not necessarily the same as the objectivity in reality. This result still can justify a reasonable conviction in criminal proceedings.

There is a situation that has come to be known quite literally in legal practice, that is, no matter scientific or non-scientific evidence, the important issue is what degree of proof that evidence can provide the fact finder (judge or jury) to find the fact. As long as the fact finder can make factual inference under "common sense," it is in principle a reasonable and acceptable factual determination.

This argument is actually very common. As far as the German Code of Criminal Procedure is concerned, since both fact finder and the finder of law are principally judges with judicial competence, the judge relies on the premise that the evidence is not contrary to common sense to prove the proof of scientific evidence and decide what the past and objective facts are. Thus, as long as the judge's assertion is consistent with common sense, evidence is, in principle, treated as a tool to assist the judge in discovering the truth (forming his consciousness), which is also considered to be reasonable.<sup>475</sup> Compared with the German Code of Criminal Procedure, the U.S. criminal trial procedures put the issue over to the jury because the jury can make decisions without any reasoning. As long as the jury does not have any other violations of the law, in principle, evidence also considered to be reasonable.<sup>476</sup>

In fact, under the modern criminal procedure system, all important evidence

---

<sup>475</sup> Beulke, *Strafprozeßrecht*, 5. Aufl., C.F. Müller, Heidelberg, 2001, S.12-13.

<sup>476</sup> Chen-Shen Yen, *The Case of O. J. Simpson and Disputes over the American jury system*, *America & Europe Monthly*, Vol. 11, No. 1, P.116.

must be presented in court to make sense. This is what is called direct adjudication or the hearsay rule. Once the evidence is not presented before the trial, it is not only unable to make the fact finder concretely form his consciousness, nor can it make the consciousness formed by the fact finder maintain a certain degree of reliability.

However, while the contemporary criminal justice system shapes the facts and the final lawsuit through this mechanism of subjective consciousness, in theory, subjective consciousness should be a way of reviewing all the evidence to make a comprehensive judgment, and scientific evidence as tools for prove the facts is only part of it. Scientific evidence should not fully prove the facts to be proved under the overall context of subjective consciousness. Moreover, according to the analysis of the previous chapters, it is clear that the actual situation is obviously evidence of scientific nature has more power than the traditional evidence. This force can be so powerful as to change the legislation so that it can be accepted by the judiciary. In other words, while the system of criminal procedure considers this mechanism would not prove the crime fact only based on the single evidence, but what is actually happens in the reverse of evidence cases involving computers. Therefore, in the whole design system, there is actually some scientific point of view to convince scientific evidence that it has not actually been eliminated in any way. Scientific evidence actually replaces the verification function of *freie Beweiswürdigung* with some strength. Or, we can say, when the function of *freie Beweiswürdigung* meets scientific evidence in finding fact level, the fact finder is virtually powerless and incompetent to change the result approved by scientific evidence.

In other words, the crux of the problem lies that when the legal system uses the fact finding as the goal of the proceedings, the formulation of such a goal will still inadvertently invade the confirming person's subjective consciousness-forming process. That is, the requirement of forming a subjective consciousness is to form the

fact finder's confirmation of the facts. When we acknowledge such an approach, subjective consciousness of "fact" remains under the control of Scientism, because this view is indifferent to the existence of an objective reality, but it gives the discovery of the true commandment at the same time as the lawsuit. The real example is like this: Although in the above perspectives and considerations, both scientific and non-scientific evidence should be viewed from the rational concept of the subject (the fact finder). However, the actual litigation structure tells us that the more innovative the technology is, the more power it can bring to a judge or jury! Any evidence produced in a scientific manner is, of course, highly evidentiary or evidence of litigation. Obviously, under the litigation structure now adopted, because the subjectivity of the fact finder is used to unify the problem that the subject and the object cannot really know each other, the contradiction is that the scientific evidence with the positive significance obviously cannot be taken by the subjective power is eliminated.

Returning to the three previous presuppositions, when we discuss issues on scientific evidence, as long as we are objective about the first hypothesis, then the fact finder must always try to affirm the truth, resulting that he still cannot get rid of the idea that "the fact is there" in his mind. In other words, if we cannot deny the first presupposition, the fact finder will always be cognizant of the facts. Even though what he identifies actually comes from his subjective imagination of fact, the factual imagination remains a conscious function that is considered to be factual. Therefore, the influence of scientific discourse will be deepened to the fact finder's consciousness. What the fact finder to do is to affirm the facts, so naturally science has been a greater help to him than any other non-science disciplines; under this context, scientific evidence earns more power than such other evidence. Then, we can say that, if we still believe the fact finder will and should find the objective truth, he

definitely holds the scientism, because the great power of scientific evidence still affects how the subjective consciousness of the fact finder is shaped.

However, Luhmann pointed out that Husserl desired to integrate the object through the subject is impossible, because either the subject or the object is only the product of system structure coupling. Instead, what is real is the notion of a system that takes functional operation as its core proposition, whereas a meaningful system at this level refers to the so-called social system. Luhmann further argue that the composition of any social system comes from communication. We cannot imagine that there is a social system that is not composed of communication and communication is a meaningful choice. The scientific system as a social system, of course, is only a kind of communication, so the scientific system simply cannot understand what actually the real world is. The scientific system only shapes the realities of a scientific system through communications; compared with science, law as a system, of course, tries to reconstruct the past fact through the legal code. In other words, science only observes the scientific truths shaped by the “true / not true” of the scientific code, but this truth does not necessarily equal the truth to be understood in criminal proceedings. As we have created a criminal justice system centered on the "determination of facts" through the mechanism of the fact finder, we have put the scientific evidence, which has the significance of fact recognition, at the heart of criminal justice. Because criminal justice emphasizes “fact finding” the scientific code, the scientific evidence is bound to have great significance in the practice of criminal justice.

In fact, the real emphasis lays on the first presupposition which is on the relationship between criminal justice and fact finding. If we overemphasize the function of fact finding, it inevitably brings about the expansion and deification of scientific evidence. Because the true function of the scientific code can never be

removed, it is further deepened, no matter whether it is found in the objective reality or in the subjective view of the fact finder. What we should further understand is that the so-called fact finding is merely a choice of meaning given through science. In the context of different systems, this truth is nothing more than a choice of meaning given through science. With a time-to-space replacement, the meaning of this fact finding shifts completely. Therefore, Luhmann clearly pointed out that this view of the dualism is fundamentally unacceptable.

Based on Luhmann's theory, this thesis argues more positively that the first presupposition should be that the past fact is gone, and nothing exists there. Only when we have broken this presupposition "the truth is out there" in the criminal justice system, scientific evidence can be returned to what Luhmann calls functional differentiation under the functional subsystems, that is, scientific evidence is only a single aspect and it impossibly brings complete and irresistible effect to the proceeding of the lawsuit. Therefore, the relationship between scientific evidence and criminal procedure should be understood in terms of two systems at different levels: one is using codes of "true / not true" in scientific evidence, which deals with the scientific facts built by scientific discourses; the other is using codes of "legal / illegal" in the criminal justice system. Criminal justice does not presuppose the truth. The real premise of criminal justice lies in whether we can screen those who are criminals through the proceeding of litigation. This screening is conducted at another level of "legal communication". Only when this important concept is recognized can our criminal justice be set free from the great curse of scientific evidence.

However, the argument in this thesis will be very seriously questioned, because what is left in criminal proceedings when criminal proceedings are no longer based on true findings?

## 5. Suggestion

It can be said that the discovery of the real entity (fact finding) is a litigation target is developed in accordance with the inquisitorial system; fact finding is not the purpose of suits in Roman law. When the inquisitorial system is replaced by “Akkusationsprinzip” which means a separate complaint system of prosecutors and trial judges, it is found that the purpose of fact finding has not been abandoned at the same time. Instead, it has become the core proposition of the criminal procedure system. This paper argues that the criminal procedure based on the fact finding will present extremely serious danger at the level of scientific evidence. That is to say, when the criminal fact is found through its subjective consciousness by the fact finder, the subjective consciousness of the fact finder cannot resist the power of scientific evidence under highly scientific myths. Therefore, this thesis argues that unless the fact-finding commandment of criminal proceedings is denied, otherwise, there is simply no way to lift the threat posed by scientific evidence.

The question is, how do we reconstruct our legal system of criminal procedure when we negate the purpose of fact finding? As the discourse at the beginning of this chapter, it is better to discard the fictional purpose of discovering reality and revisit the proceedings as a mechanism for settling disputes. Such a claim is not unique to this thesis. In the historical course of the development of Criminal Procedure Law, the settlement of disputes has also been the pursuit of the entire lawsuit. In addition, Luhmann also believed that disputes need to be resolved through the system/institutions<sup>477</sup>. From the perspective of the development of human history, the handling of disputes in human society takes the form of self-help relief (Selbsthilfe, in Luhmann’s word) in the earliest primitive society. As the society becomes more and more complicated, it is not enough to deal with the disputes through self-help relief

---

<sup>477</sup> Luhmann, Niklas, *Legitimation durch Verfahren*, Suhrkamp: Frankfurt a. M., 1983, p. 100-101.

alone. Therefore, certain specific organs for resolving disputes will be inevitably developed. These organs are the so-called courts. This is an inevitable phenomenon in a complex and structured society.

In other words, the “institutionalization” of settling disputes over correction is an inevitable trend of development in modern society. Institutionalized court proceedings to resolve social disputes must naturally resolve the disputes in various institutional ways and get the result after the dispute has been resolved. The institutionalization is usually practiced in modern society by creating organizational or procedural norms in the criminal procedure, by creating “role assumption” (For example, a judge who is a neutral third person can make a fair verdict; In Taiwan Code of Criminal Procedure, Article 2 states that “*A public official who conducts proceedings in a criminal case shall give equal attention to circumstances both favorable and unfavorable to an accused.*”) that are different in the process, and by whom the parties seek the result of the dispute based on the rules of procedure. Of course, the result of the dispute is unpredictable in principle; by so doing, it is possible to require the parties to settle the proceeding in accordance with the norms of the procedure in the process of dispute resolution.<sup>478</sup>

However, the function of Luchaman's institutionalized dispute resolution mechanism underlined here is to manifest the dissatisfaction of the parties expressly and to resolve and absorb their dissent, all of which must follow “the existing form of the proceedings”. Facing this question, he reasoned, the motivation for the parties to proceed according to the existing form of litigation lies in the uncertainty of the outcome of litigation. Precisely because the intentions cannot be expected before the litigation starts, there is a risk of non-compliance with the procedures, so the parties

---

<sup>478</sup> Luhmann, *supra* note 477, p. 120.

will naturally try their best to keep the program under control.<sup>479</sup>

Through Luhmann's theory of litigation procedure, we can clearly understand that the precondition for the state to launch the power to enforce its criminal punishments lies in participating in the established procedure through the parties concerned. Any dispute should be solved in the procedure. The goal of the procedure is not the pursuit of some form of justice or lawful purpose; the goal of the procedure lies in the resolution of the procedure itself.

We can find the further argument while applying Luhmann's theory to the criminal justice system. Criminal justice, in the sense of law, is a matter of choosing to deal with criminals, and legislators presuppose the existence of two opposing antagonisms in criminal proceedings. Therefore, the real purpose of criminal justice is not to “discover the truth in conformity with justice”; the purpose of criminal justice is rather to provide a forum for the parties to settle disputes, to allow parties to express their grievances and opinions in places and to provide both parties with opportunities for trial reconciliation. In other words, the function of criminal litigation lies in providing two parties fields for communication and in this field shaping the choice of meaning for both parties. In any case, this choice of meaning must have nothing to do with discovering reality.

Thus, it is clear that the function of scientific evidence in criminal proceedings only affects the formation of communication mentioned above to a certain extent. Scientific truth shaped by scientific evidence has nothing to do with criminal proceedings. The code used in criminal proceedings differs from that used in scientific evidence and science system. Scientific evidence is only an environment in which criminal proceedings can be conducted. Based on the openness of system operations Luhmann talked about, scientific evidence can influence the selection and editing of

---

<sup>479</sup> Luhmann, *supra* note 477, p. 116.

code programs to other system, but the selection and deciding of code programs remains a matter of internal system operation.

The character of the criminal justice system is both open and closed: in an open sense, it can accept the assistance provided by scientific evidence in order to make the judgement in the procedure; but in a closed sense, the issue of the criminal justice system can only be solved with internal legal code in the criminal justice system. Scientific evidence never determines the choice of code for criminal proceedings. Therefore, the true meaning of scientific evidence in criminal justice should lie only in the openness of the system, and whether it can affect the decision of criminals in the criminal justice system. In addition to this, the judgement and punishment of the offender's decision is absolutely irrelevant to scientific evidence<sup>480</sup>.

## **6. Summary**

There are three presuppositions on scientific evidence in the criminal procedure law. This thesis argues that the discussion of scientific evidence does not seem to proceed from the scientific evidence itself because it is actually under the three presuppositions. On the other hand, the questions of Husserl and Luhmann take the second and the first presuppositions differently. As to Husserl's questioning, he attempts to reconstruct the mechanism of fact determination through the fact finder's subjectivity. However, there are apparently some blind spots in the analysis of the structure of scientific evidence with his theory. The blind spot is that he cannot avoid being influenced by the truth about science when the finding truth is still an important indicator in the fact finder's consciousness. Unfortunately, Husserl's theory apparently cannot emphasize that under the subjective sense it will be so severely affected by science. Therefore, this thesis argues that this issue should be cut from the observation

---

<sup>480</sup> Mau-Sheng Lee, Confession and the Structure of the Facts, in Mau-Sheng Lee, Power, Subject and Criminal Law, Vanity press, 1998, P. 120-121.

and analysis of Luhmann by understanding that the truth of the structure of science is totally different from the truth of other social systems. Only when this viewpoint is understood, the observation of scientific evidence cannot be over-valued, and return to fairness, that is, scientific evidence is just a choice of meaning. We cannot expect this choice of meaning to find truth. On the contrary, if the objectivity of this choice of meaning is overemphasized, the criminal process will become a science-centric as all things will become treated through scientific evidence, which apparently overvalues science.

As stated above, the core of the entire scientific evidence should be based on the discovery of the true commandment of the entity by criminal justice. However, this truth, which is evaluated in the scientific system and freely passed by judges, is in fact completely accepted under the scientific objectivism which Husserl referred to. If we hope that criminal justice will not be excessively influenced by scientific objectivism, there is in fact no way other than to give up the true concept of the entity. Further, when we give up the truth of the entity, the litigation system will not be unable to proceed smoothly. The alternative solution to the problem lies in the self-worth of the procedure: providing the field of reconciliation, allowing the parties to try reconciliation in the field and achieve the final result.

In this context, the meaning of scientific evidence in criminal proceedings will change from “tools to find the fact” to “assurance of providing continuing legal access”. The scientific theory of scientific evidence is just the environment for legal communication. Legal communication takes place on the "legal / illegal" symbols in the legal system. As long as the defendant is found guilty in the litigation through common sense choices, the litigation can be terminated.

In short, the true focus of the scientific evidence should lie in the fact that scientific evidence can only provide an environmental and system-related

programmatic influence on the conduct of criminal justice communication. But scientific evidence has never been, and should not be, understood as a way of finding so-called truth in criminal proceedings, because no matter what kind of approach to prove the fact, criminal justice has never been confirmed that the objective truth is the only basis for conviction. Criminal justice affirms that the perpetrator was communicating through the legal system symbols.

## Reference

1. Beulke, Strafprozeßrecht, 5. Aufl., C.F. Müller, Heidelberg, 2001.
2. Chen-Shen Yen, The Case of O. J. Simpson and Disputes over the American jury system, *America & Europe Monthly*, Vol. 11, No. 1, P.116.
3. Chueh-An Yen, Construction and Cognition: A Brief Comment on the Realism and Anti - realism of Jurisprudence by Luhmann 's Constructivist Epistemology, in Wen-Hsiung Lin ed., *Contemporary Basic Law Theory*, Sharing publish: Taiwan, 2001.
4. Husserl, *The Idea of Phenomenology* (abbreviated as *idea*), trans. by Alston and Nakhnikian,
5. Lilly, *An Introduction to the Law of Evidence*, 2nd ed., West Publishing, N.Y., 1987, at 1 & 5.
6. Luhmann, Niklas, "The Unity of the Legal System", in: *Autopoietic Law: A New Approach to Law and Society*, Walter de Gruyter, Berlin 1987, pp.24-25.
7. Luhmann, Niklas, *Social Systems*, trans. by Bednarz, Jr.. & Baecker, Stanford Univ. Press, 1995.
8. Luhmann, Niklas, *Legitimitation durch Verfahren*, Suhrkamp: Frankfurt a. M., 1983.
9. Martin Goldstein and Inge F. Goldstein, *How We Know An Exploration of Scientific Process*, Da Capo Press: U.S.A, 1981.
10. Martinus Nijhoff Publishers, Hague, 1964.
11. Mau-Sheng Lee, Confession and the Structure of the Facts, in Mau-Sheng Lee, *Power, Subject and Criminal Law*, Vanity press, 1998, P. 91-128.
12. Volk, *Strafprozeßrecht*, C.H.Beck, München, 1999.

## **Conclusion:**

### **Answers to the Research Questions**

This thesis is devoted to discussing how the information extracted from social network sites is “correctly” used as evidence in criminal proceedings, and further, from the perspective of meta-analysis, the thesis argued the fact-finding function in criminal proceedings. What is the definition of social media evidence is still quite vague. This thesis attempts to define it as “information extracted from social network sites and used as evidence in criminal proceedings” in Chapter 1. In addition to the nature of the user-generated content and the connection of the real and the virtual world, social media evidence has characteristics similar with digital evidence, such as easily tampered with, copied in large quantities, and difficult to identify. In Chapter 2, the thesis compares two legal systems: one is the U.S. law (the common law system) which uses the most social media evidence and the Taiwan law as the representative as the civil law system. The purpose of this comparison is to find the legal system benchmark. Then this thesis discusses how to extract information through technology which refers to digital forensics in this thesis in Chapter 3. The purpose of comparing the evidence collection methods of legal system and network identification is to explore the challenge and help of science and technology on legal norms, especially real discovery. This thesis argues that at this level, there are two main problems with social media evidence: one is how to properly reflect the content on the website, such as the possibility of using printed materials directly or copying and pasting the content in a new document; the other is how to link the evidence to the real author, which is also a common defense called Trojan defense in criminal proceedings. (Chapter 4) In

Chapter 5 and 6, this thesis analyzes and discusses two issues. Finally, based on the scientific nature of social media evidence, this thesis reviews the meaning of facts in criminal proceedings and the principle of evidence-based judgement, and further challenges the purpose of fact finding in the contemporary criminal justice (Chapter 7). This thesis argues that criminal litigation, as a field for the parties to settle disputes, does not pursue the scientific truth but chooses to be able to persuade the parties and to find a solution that can be accepted by both parties. With this social media evidence, which is mainly user-generated content, we can more clearly recognize the choice of legal system.

As it mentioned in the introduction, the point to answer the research questions is law's knowledge of science, which means the whole procedure that when a new technology is introduced into the legal system, the court learn this technology and apply it into the case, and then create a new standard for using this technology, or even transfer it into a new understanding to build the fact. Social media evidence is a good example to examine this procedure that how the legal system using the evidence to construct the past fact. Based on its nature of personalization, using social media evidence can solve the most difficult legal issues in criminal proceeding, that is who did the crime and why he did it (motivation of the crime).

Now we find the legal system prefer to use analogy to apply the new technology. As discussion in chapter 2, when the court needs to decide whether the investigators can search files in a seized computer, it doesn't have precedents before, but has the experience of incidental search on the box. Then the court analogizes the file as the box. Especially in the case of social media evidence, which cannot be touched, felt, or seen as real evidence, the court tend to use its experience to determine the discoverability and admissibility of this evidence. It is not based on the scientific nature, but on experience, or we can say the court's knowledge and believe. We need

to point out that, no matter what kind of scientific standards the legal system built for evidential usage to construct the past fact, what the legal system built is a persuasive fact based on experience and analogy.

## **WHAT IS SOCIAL MEDIA EVIDENCE?**

Social media evidence (SME) was defined literally, as well as characteristics and functions, in order to differentiate from other existing evidence in the criminal procedure. This thesis defines social media evidence as “information extracted from social network sites and used as evidence in the criminal proceedings”. By this definition, there are two points to be noticed: first, it is information from social network sites; second, it should be evidence in the criminal proceeding. In the technology system, asking “what is social media evidence” is transferred to “how to extract information as evidence from social network sites?” which is a dynamic process. Similarly in the legal system, the question should be asked as how to introduce evidentiary material from social network sites into the courtroom. Since the evidence is the primarily manner to constitute the fact in the legal system, it actually discussed different approaches to find the fact between legal and technical systems, while asking what the social media evidence is.

We consider social media evidence as the information flow on social network sites. Data, originally constituted by the 1s and 0s, was extracted from social network sites, transformed to evidence materials in court, and became the evidence eventually used as the ground of a judgment. This complete process is as shown below.

## from information to evidence

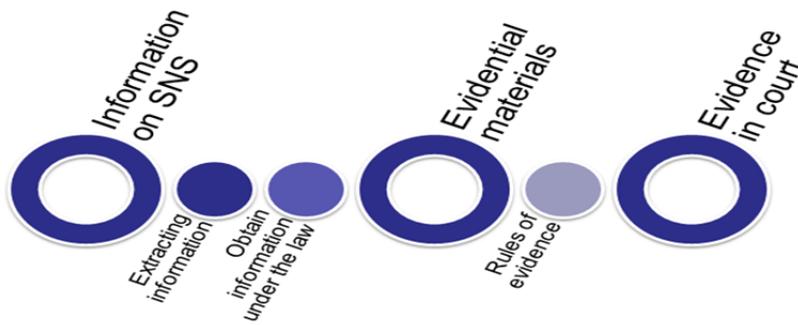


Figure 14 SME, a process from information to evidence

### 1. Definition, Nature and Characteristics of Social Media Evidence

Social media evidence describes information extracted from social network sites in order to be evidence presented at trial. This term literally stresses that media which this information depends on. A few American scholars call this kind of evidence as social network evidence, which enhances information is exactly from social network sites. But the mainstream academia calls it as social media evidence, and usually discusses information extracted from social network sides. In fact, most real cases in court are related to evidence obtained from Facebook, MySpace, and Twitter, and the courts didn't distinguish these terms of cases in the detail. Thus, we may think the term "social media evidence" as a phrase during the legal practice.

Social media evidence entails the characteristics of social network sites: participation, community, public, communication, and connection. With these characteristics, social media evidence not only is a good source for government investigators to obtain criminal evidence, but also connect the criminal and the offense and prove the defendant's motivation, which is the hardest part to prove in the criminal proceeding.

In format of evidence, social media evidence is a type of digital evidence, differentiating from objective items and witnesses to express their opinions. Because it has the nature of digital evidence, it is vulnerable to tampering, and possible to

recovery. While presenting in the courtroom, the common way is to print the content of website pages out, as a document. It is also applied the rules for scientific evidence, when this social media evidence is produced by forensic practitioners via forensics, instead as the printout or screen shot by the police or lawyers.

Types of social media evidence are diverse and fully creative. Information on social network sites basically may be transformed to evidence, if it satisfies the relevance request and admissibility request under the federal rules of evidence. The common types of social media evidence are users' profile, friend list, contents of postings or comments, photos, records of login (log files), etc.

## **2. Social Media Evidence in Forensics**

We can find that, for this digital forensic science, the most important part is to ensure that the identity between obtained evidence and original evidence is the same. The common way to prove  $A=A'$  is adding MD5 Hash value to verify digital documents. To make sure the forensic results, they try to build SOP, make records, and produce documents. This is totally the scientific methodology. Through SOP and records, we can represent the same forensic procedure happened before, and also we can rebuild the crime scene. Besides, we also can find the whole scientific communities still follow the general acceptance principle. The scientific knowledge is based on peer review, which is also accepted by other academia communities and becomes the general rule for knowledge production.

Unlike the science, legal system doesn't put too much concern on reality of this social media evidence. They have already accepted the premises; scientific evidence in principle must be true. Judges allow the evidence into courtroom by law, but adopt it to make the argument by their knowledge. In Chapter 2, we talked about social media evidence in court. First, we will see what kind of regulations apply for social

media evidence, and discuss the problem inside. Second, we will discuss the concept of expert witness, which is the real way to show digital evidence, social media evidence or scientific evidence in court. That would be interesting to dig from history and from comparative law. Then we will rethink about the whole procedure, from information to evidence, and analysis reasoning of judgments about social media evidence.

### **3. Social Media Evidence at Trial**

We can find in the criminal proceeding, the legal system set a rule of evidence, considering variety of values to filter materials that the investigators obtain, in order to ensure evidence presented in front of the jury is relevance and compliance with legal value requirements. Then the jury decides with their experience, how to reconstruct the past fact based on evidence. After getting conclusions, the jury tells the fact, and the judge applies legal provisions to that determined fact with his professional legal knowledge.

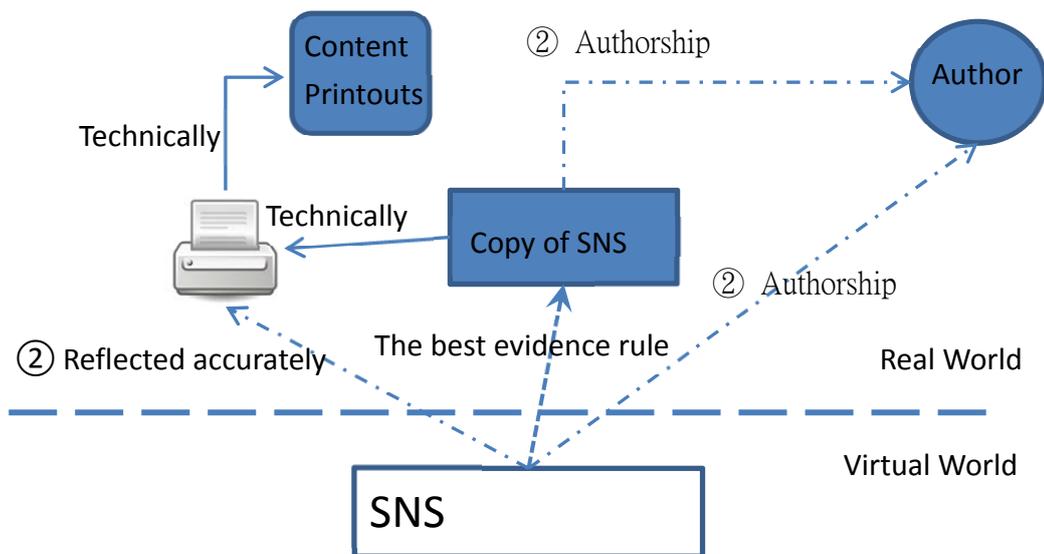
Most legal scholars concern evidentiary issues in admitting social media evidence in court. They specifically focus on authentication issues. However, this approach may have been already limited by inherent controversies in the legal system. It can hardly jump out of those deadlocks, such as infringement of privacy and public-private dichotomy. Some scholars try to re-define or re-demarcated the boundary between public area and private space, and even someone tried to create a new theory to give up this dichotomy. Unfortunately legal scholars have yet to find a convincing answer on privacy issue. Moreover, it is previously accepted as the premise, that science and technology present objectivity of nature. Under this approach, the point of authentication is just to prove that evidence obtained in crime scene is the same as evidence shown in court (identity issue). Few people question

what this evidence turns out to be, how to transform a meaningful form from the information, or what scientific significance and value of network forensics tools are. No one ask that, what kind of fact will be found through those tools and shown in court. Will it change courts' knowledge of the truth?

## **APPLICATIONS OF SOCIAL MEDIA EVIDENCE**

### **1. Issue of Printouts**

Printouts or screenshots is the very common mean to show social media evidence in the court room. The problem is that, the defendant will challenge the qualification of this evidence: fist is the discoverability of printouts. It is related to the investigative means of obtaining the evidence. In the case of social media evidence, issue of violation of privacy guaranteed by the fourth amendment often arises, such as whether the social network sites is as the public domain, whether the investigative authorizations can use a subpoena to obtain information on the social network sites instead of a warrant, or whether the subject's consent can justify this search without warrant (chapter 2); second, the admissibility of this evidence. Usually the arguments will be focused on the authentication issues. Although there are other factors will affect the admissibility of evidence, issues of authentication is the main point in American legal system. The courts, according to Rule 901, divided authentication requirement into two factors in the case of social media evidence, such as correct reflection and authorship, and we can illustrate the construction of issue of printouts on them. The judge acts as a gatekeeper in determining whether the party offering the evidence has fulfilled this requirement of relevance.



The legal system thought there is no problem in technical part (printout itself), because the technology always makes sure the reflections correct and that is the technology designed for. Thus, issues of SNS printouts are accuracy and authorship. The second question is also connected to the Trojan defense. To deal with these authentic issues of social media evidence, the American legal system developed two approaches: the Maryland approach and the Texas approach. The first method is often seen as overly skeptical of social media evidence, setting the bar too high for admissibility. The second approach is viewed as more lenient, declaring that any reasonable evidence should be admitted in order for a jury to weigh its sufficiency. More and more courts follow the second approach that the social media evidence will be authentic in prima facie and leave it to a reasonable juror to decide. However, the supposed difference between the two sets of cases and suggests that courts are not actually employing two distinct approaches. The Maryland Approach courts are not holding social media content to a higher standard than the Texas Approach courts, but are merely responding to a lack of evidence connecting the proffered content to the purported author.

Besides, we should not take it granted that what the printer print is correct and reliable. For example, the prosecutors cut and paste some contents on SNS, make them as a word document, and then print it as the evidence. This printout should be doubt because the document is made or created by the prosecutors. It equals the prosecutors created the evidence to trap defendant to the crime. Actually in 1990's when the first time a computer document was introduced as the evidence at trial, it aroused heated discussion. The court at that time did not take the computer document authentic just because the file was made by the machine. What's more, the digital forensics provides many methods (such as image print, website full-page print, etc.) to make sure the printout reflected correctly.

On the other hand, the reason that the court can accept the printout authentic without requiring a forensic method, might be what the legal system seek for is not a real fact, but the balance among the victim, the defendant, the prosecutions, and the whole society. Thus, the legal system use social media evidence to construct a fact that can be accepted by every party related to this case.

## 2. Issue of the Trojan Defense

A Trojan defense means the defendant cannot prove his innocent, but argued someone or a Trojan invaded his computer and committed the crime. In the case related to social media evidence, there are four possibilities shown as the following form.

		Account in SNS	
		True	False
Content of SNS	True	SME is authentic. Jury will decide its value.	Authentication? (Trojan Defense)
	False	SME is authentic. Jury will decide its value. (Trojan Defense?)	Authentication? (Trojan Defense) Value?

Thus, we can conclude that, as long as the account is true or no one claimed its false, then this social media evidence will be left to the jury to decide its factual value; but if the account is false or claimed false, then the judge must decide authentication of this social media evidence. Furthermore, from the defendant's aspect, as long as there is any false, no matter in part of account or content, he has the chance to raise the Trojan defense, and claims, "It was not me. There is someone who did it."

The forensic practitioners usually can provide evidence to prove possibility of being implanted a Trojan, and relationship between the Trojan (if found) and this disputed malicious digital activities. The standard operating procedure is firstly to detect the Trojan, and secondly to make digital forensics of digital activities. When a malware is found, forensic practitioners need to identify this malware and its invading traces to prove this malware is related to the case; on the contrary, when the malware is not found, forensic practitioners need to prove no wiping tool is used. Then they can conclude the malware is not related to this case.

The defendant can use the Trojan defense to raise reasonable doubt, negate mens rea, and establish the defense. And the prosecutor can respond to the defendant's Trojan defense by establishing defendant's computer expertise, and negating the factual foundation of defense. For a judge, circumstantial evidence and reinforcing evidence are necessary, because even using forensics, there is still a gap between this virtual crime and the real person who did it.

The forensic science can prove the computer was invaded by a hack or implanted a malware, but it is hard for forensic practitioners to build a solid or real connection between the computer and the real criminal. Unfortunately, there is only one thing that the legal system wants to prove, which is who did this crim. Thus defendants and prosecutors provide more circumstantial evidence to reinforce their theory, in order to convince the judge or the jury to believe their story and make the favorable judgment

for them.

We can find the different between the forensic science and law in this Trojan case. The forensic science proves the past fact, whether there was the malware; but the legal system construct the past fact, that is the defendant who did it or who did not do it.

## **LEGAL MODEL TO REPRESENT THE PAST FACTS**

We can divide the production of social media evidence into two steps. The first step is to extract information from social network sites. The legal system takes a totally different approach from the forensic science. In the digital forensics, experts focus on two questions: how to extract information from SNS and how to identify the copy and the original file ( $A=A'$ ). But in the legal system, the thinking order of these questions is quite different.

The task of the criminal law is to punish the criminal, thus, the prosecutions first find the victim or crime, then search for evidence, build a theory about this crime (what, when, where, who, how, and why), and find the person to charge this crime. The legal system will focus on how to connect this crime to the person, and how to punish him under the law. In the case of social media evidence, the question will be how to obtain information from a person, instead of from SNS. In traditional, when the investigators want to obtain information from a person, they need to follow rules to protect people's privacy, property or liberty, such as a warrant for search under the 4th amendment. In this case, we can further find out that, the court does not really care the opposition  $A=A'$ , which means the consistency of obtained information from website to the real copy. But the court cares whether this investigative method to obtain information follows the due process under the frame work of legal order.

The second step is to present this evidence in the courtroom. In the digital

forensics, experts build a procedure to ensure the reliability of evidence. They use pictures, records, copies and the SOP to prove it. But the legal issue of evidence in the courtroom is admissibility, which means the evidential material can be accepted as evidence by the court and become the base for the jury to decide the past fact. Rules of evidence is used in this stage, and its function is to filter unnecessary, irrelative, injustice, unfair, prejudging, misleading and biased material and exclude them out of the courtroom. In such filter system, every layer contains a particular value guaranteed by law, such as the hearsay rule, which require the witness should present in the courtroom in order to be cross-examined by the defendant and the prosecutor. This rule is not only for finding the fact, but also for chasing the fair trial guaranteed under the constitutional law. Therefore, we can prove even though the law and science both chasing the fact, finding the truth is the goal of scientific research, but for a legal system, it need a persuasive fact to be accepted by parties and the society. In conclusion, finding fact is not the end of the task of the criminal procedure, but a fair trial is.

Now we can conclude that, (1) the analogy is the most important approach that legal systems use to solve a new issue while a new technology is introduced. And this approach is based on the so-called “common, and general,” human experiences, which will be differentiated by history, culture and social habits; (2) through this approach, the legal system transform this new technology under its knowledge, and do not necessarily comply with the original rule of his new technology, but develop a new standard for its own case; (3) in the case of social media evidence, the court did not consider the nature of SNS and analogized this information as what it experienced before. It neither reaches the fairness and justice in a specific case, nor implement values guaranteed by the legal system; (4) Since we have already understand the

nature of social media evidence and the operation of the legal system, the analogy approach should be given up and try to introduce the forensic approach to use information as evidence.

## REFERENCE

1. Hogan, Brendan W. (2012), Griffin v. State: Setting the Bar too High for Authentication Social Media Evidence, 71 Md. L. Rev. Endnotes 61.
2. Koops, B. J. (2009), Technology and the Crime Society: Rethinking Legal Protection, TILT Law & Technology Working Paper No. 010/2009 23 March 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 006/2009, p. 1-22. Available at: <http://ssrn.com/abstract=1367189>
3. Kopec, Mark C. (2012), What Happens on Myspace Stays on Myspace: Authentication and Griffin v. State, 42 U. Balt L. F. 164.
4. Laurin, Jennifer E. (2015), Criminal Law's Science Lag: How Criminal Justice Meets Changed Scientific Understanding, 93 Texas L. Rev. 1751.

## Bibliography

1. Adams, Richard, Hobbs, Val & Mann, Graham (2013), The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice, Journal of Digital Forensics, Security and Law, Vol. 8(4), p. 25-48, available at <http://ojs.jdfsl.org/index.php/jdfsl/article/view/110/198>
2. Ademu, Inikpi O., Inmafidon, Cris O. & Preston, David S. (2011), "A New Approach of Digital Forensic Model for Digital Forensic Investigation", International Journal of Advanced Computer Science and Application, Vol 2, No.12, 175-178.
3. Adkins, J (2011), Law Enforcement Guide to Social Media, Special Research Report, available at <https://nebula.wsimg.com/5bdda470f8982071d7ef98ed81038dfb?AccessKeyId=D535D04439DEB65C2F17&disposition=0&alloworigin=1>
4. Andrews, Lori (2012), I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy, Free Press.
5. Angus-Anderson, Wendy (2016), Authenticity and Admissibility of Social Media Website Printouts, 14 Duke L. & Tech. Rev. 33.
6. Bauccio, Salvatore J. (2007), E-Discovery: Why and How E-mail Is Changing the Way Trials Are Won and Lost, 45 Duq. L. Rev. 269-291.
7. Beulke, Werner (2001), Strafprozeßrecht, 5. Aufl., C.F. Müller, Heidelberg.
8. Bickel, Alexander M. (1986), The Least Dangerous Branch: The Supreme Court at the Bar of Politics, 2nd edition, Yale University Press.

9. Bowers, C. Michael (2014), *Forensic Testimony-Science, Law and Expert Evidence*, Elsevier: USA.
10. Bowles, Stephen & Hernandez-Castro, Julio (2015), *The First 10 Years of the Trojan Horse Defence*, *Computer Fraud & Security*, January 2015, 5-13.
11. boyd, d. m., & Ellison, N. B. (2007),. *Social network sites: Definition, history, and scholarship*, *Journal of Computer-Mediated Communication*, 13(1), article 11. <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>
12. Bradley R. Johnson (2011), *Untagging Ourselves: Facebook and the Law in the Virtual panoptic on*, 13 *T.M. Cooley J. Prac. & Clinical L.* 185.
13. Brenner, Susan W., Carrier, Brian, & Henninger, Jef (2004), *The Trojan Horse Defense in Cybercrime Cases*, 21 *Santa Clara High Tech. L. J.* 1. Available at: <http://digitalcommon.law.scu.edu/chtlj/vol21/iss1/1>
14. Browning, John G. (2011), *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 *SMU Sci. & Tech. L. Rev.* 465.
15. Brunty, Joshua & Helenek, Katherine (2013), *Social Media Investigation for Law Enforcement*, Elsevier Inc., MA: USA.
16. Carney, Megan & Rogers, Marc (2004), *The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction*, *International Journal of Digital Evidence*, Volume 2 Issue 4, Available at: <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B2CCCB-E6FC-6840-AF4A01356B9B687A.pdf>
17. Casey, Eoghan (2004). *Digital Evidence and Computer Crime*, Second Edition, Academic Press: USA.

18. Casey, Eoghan (2011). *Digital Evidence and Computer Crime*, Third Edition, Academic Press: USA.
19. Chalmers, Alan E. (1992), *What is This Thing Called Science?*, 2nd ed., J.W.Arrowsmith Ltd, Bristol.
20. Chang, Hung-Chang (2004), *Discussion on the Application of Digital Image Evidence*, *Criminal Bimonthly*, No. 57, P.99-109.
21. Chang, Li-Ching (1987), *On Admissibility of Photo and Video Evidence*, *The Military Law Journal*, Vol. 33, No. 12, P. 16-26.
22. Chen, Pu-Shing (1992), *Criminal Evidence Law*, Vanity press, Taipei: Taiwan.
23. Chiou, Shian-Min & Lin, Yi-Long (2007), *The Offensive and Defensive Countermeasures of Digital Evidence in Court*. *Journal of Information, Technology and Society*. Vol. 7, No. 1: Pp. 53-64.
24. Chiu, Hsien-Ming & Lin, I-Long (2007), *The Offense and Defense Countermeasures of Digital Evidence in Court*, *Journal of Information , Technology and Society*, Vol. 7, No. 1, P.53-64.
25. Chueh-An Yen (2001), *Construction and Cognition: A Brief Comment on the Realism and Anti - realism of Jurisprudence by Luhmann 's Constructivist Epistemology*, in Wen-Hsiung Lin ed., *Contemporary Basic Law Theory*, Sharing publish: Taiwan.
26. Clifford, Ralph D. ed. (2001), *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, California Academic Press.
27. Clifford, Ralph D. et al. (2006), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 2nd Edition, Carolina Academic Press.
28. Cole, Simon A. & Lynch, Michael (2006), *The Social and Legal Construction of Suspects*, 2 *Annu. Rev. Law Soc. Sci.* 39.

29. Coughlan, Steve & Currie, Robert J. (2013), Social Media: The Law Simply Stated, 11 Can. J. L. & Tech. 229.
30. Cummings, Douglas J. Jr. (2015), Authenticating Social Media Evidence at Trial: Instruction from Parker v. State, 15 Del. L. Rev. 107.
31. Daniel, Larry E. & Daniel, Lars E. (2012), Digital Forensics for Legal Professionals- Understanding Digital Evidence from the Warrant to the Courtroom, Elsevier: Ma, USA.
32. Datt, Samir (2006), Learning Network Forensics, Packt Publishing.
33. Eisenberg, Ulrich (1999), Beweisrecht der StPO(Spezialkommentar), 3. Aufl., C.H.Beck, München.
34. Elefant, Caroly (2011), The “Power” of Social Media: Legal issues & Best Practices for Utilities Engaging Social Media, 32 ENERGY L. J. 1.
35. English, Peter W. & Sales, Bruce D. (2005), More than the Law: Behavioral and Social Facts in Legal Decision Making, APA, USA.
36. Faigman, David (2007), Anecdotal Forensics, Phrenology and Other Abject Lessons from the History of Science, Hastings L.J. 59, 979-1000, as cited in C. Michael Bowers, Forensic Testimony-Science, Law and Expert Evidence, Elsevier: USA, 2014, p. 24.
37. Ferdico, John N., Fradella, Henrt F., & Christopher, Totten D (2009), Criminal Procedure for the Criminal Justice Professional, Wadsworth Publishing: USA.
38. Flanagan, Elizabeth A. (2016), #Guilty? Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings, 61 Vill. L. Rev. 287.
39. Foster, Kenenth R & Huber, Peter W. (1999), Judging Science: Scientific

Knowledge and the Federal Courts, The MIT Press: USA, 1999.

40. Freeman, Edward H. (1998), The Use of Computer Records as Courtroom Evidence, available at <http://www.ittoday.info/AIMS/DSM/8203351.pdf>.
41. Giannelli, Paul C & Imwinkelried, Edward J. (1993), Scientific Evidence, 3 edition, Lexis Pub.
42. Giannelli, Paul C. & Imwinkelried, Edward J. (2012), Scientific Evidence, vol. I, 5<sup>th</sup> edition, LexisNexis.
43. Gilson, Cedric C. (2012), The Law-Science Chasm. Bridging Law's Disaffection with Science as Evidence, Quid Pro Books, New Orleans: USA.
44. Gladysz, L. M. (2012), "Status Update: When Social Media Enters the Courtroom", 7 I/S: J.L. & Pol'y for Info. Soc'y 691.
45. Goldstein, Martin & Goldstein, Inge F. (1981), How We Know An Exploration of Scientific Process, Da Capo Press: U.S.A.
46. Goode, Steven (2009), The Admissibility of Electronic Evidence, 29 REV. LITIG. 1.
47. Grimm, Paul W., Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro (2013), Authentication of Social Media Evidence, 36 AM. J. Trial Advoc. 433.
48. Haagman, Dan & Ghavalas, Byrne (2005), Trojan Defence: A Forensic View, Digital Investigation 2, 23-30.
49. Haak, Susan (2014), Nothing Fancy: Some Simple Truths about Truth in the Law, in: Evidence Matters: Science, Proof, and Truth in the Law, Cambridge University Press, 294-323.

50. Haber, L. & Haber, R.N. (2003), Error Rates for Human Latent Fingerprint Examination, In: Ratha, N.K. (Ed.), *Advances in Automatic Fingerprint Recognition*, 2003, Springer-Verlag: New York, p. 339-360.
51. Haber, L. & Haber, R.N. (2008), Scientific Validation of Fingerprint Evidence under Daubert, *Law Probability and Risk* 7(2), p. 127-141.
52. Her, Lai-Jier (2001), Legal Review on the Event of Searching Piracy MP3 in National Cheng Kung University, *Taiwan Law Journal*, No. 23, p.82-89.
53. Her, Lai-Jier (2004), Recording, Videotaping, Investigation of Electromagnetic Records (Article 165-1 II of the Code of Criminal Procedure), *Taiwan Bar Journal*, Vol. 8 No. 9, p.33-38.
54. Hoffmeister, Thaddeus A. (2014), *Social Media in the Courtroom*, Praeger, USA.
55. Hoffmeister, Thaddeus A. (2014), *Social Media in the Courtroom: A New Era for Criminal Justice?*, Praeger.
56. Hogan, Brendan W. (2012), *Griffin v. State: Setting the Bar too High for Authentication Social Media Evidence*, 71 Md. L. Rev. Endnotes 61.
57. Holtzman, David H. (2006), *Privacy Lost: How Technology Is Endangering Your Privacy*, Jossey-Bass; 1 edition (October 13, 2006).
58. Hsieh, Marris (2004), Applying Principle of Writ Doctrine to Computer Search and Seizure: Take American Law as a Mirror, *Criminal Law Journal*, Vol. 48, No. 6, P.78-115.
59. Huang Chaur-Yi (2007), *Criminal Procedure*, enlarged edition, bestbooks publish: Taiwan.
60. Huang, Dung-Shiung (1999), *Criminal Procedure Law*, 6th edition, Sanmin publish: Taiwan.
61. Huang, Jung-Chien (1999), *The Limit of Criminal Penalty*, Angle publish: Taiwan.

62. Huber, Markus, Mulazzani, Martin, Leithner, Manuel, Schrittwieser, Sebastian, Wondracek, Gilbert & Weippl, Edgar (2011), Social Snapshots: Digital Forensics for Online Social Networks, ACSAC '11 Proceedings of the 27th Annual Computer Security Applications Conference.
63. Husserl, Edmund (1973), *The Idea of Phenomenology*, trans. by William P. Alston and George Nakhnikian, 5<sup>th</sup> impression, Martinus Nijhoff, The Hague: Netherlands.
64. Jasanoff, Sheila (1997), *Science at the Bar*, paperback edition, Harvard University Press, USA.
65. Jasanoff, Sheila (2005), Law's Knowledge: Science for Justice in Legal Settings, *American Journal of Public Health*, Supplement 1, Vol. 95, No. S1, S49-S58.
66. Johnson, Mark A. (1992), Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?, 75 *Msqr. L. Rev.* 439. Available at: <http://scholarship.law.marquette.edu/mulr/vol75/iss2/6>
67. Johnson, Thomas A. (2005), *Computer Crime and the Electronic Evidence*, in *Forensic Computer Crime Investigation* (Thomas A. Johnson ed., 2005), CRC Press.
68. Johnson, Thomas A. (2006), *Computer Crime and the Electronic Evidence*, in *Forensic Computer Crime Investigation* (Thomas A. Johnson ed., 2006).
69. Jordaan, J. (2012), "A Sample of digital forensic quality assurance in the South African Criminal Justice System", *Information Security for South Africa (ISSA)*, 1-7.
70. Kasper A., Laurits E. (2016), Challenges in Collecting Digital Evidence: A Legal Perspective. In: Kerikmäe T., Rull A. (eds) *The Future of Law and eTechnologies*.

Springer, Cham.

71. Koops, B. J. (2009), Technology and the Crime Society: Rethinking Legal Protection, TILT Law & Technology Working Paper No. 010/2009 23 March 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 006/2009, p. 1-22. Available at: <http://ssrn.com/abstract=1367189>
72. Kopec, Mark C. (2012), What Happens on Myspace Stays on Myspace: Authentication and Griffin v. State, 42 U. Balt L. F. 164.
73. Kuo, Chia-Mei (2005), On the Definition and Method of Evidence of Electromagnetic Records - Comparing the Relevant Provisions of Canadian Electronic Evidence Uniform Law and Taiwan Criminal Procedure Law, Science & Technology Law Review, Vol. 17 No. 4, p.12-17.
74. Laurin, Jennifer E. (2015), Criminal Law's Science Lag: How Criminal Justice Meets Changed Scientific Understanding, 93 Texas L. Rev. 1751.
75. Lawrence Morales II (2012), Social Media Evidence: "What You Post or Tweet Can and Will Be Used against You in a Court of Law", 60 The Advoc. (Texas) 32.
76. Lee, Chen-Shan (2005), To Those Who Can Catch Up, Face up to Personal Data Protection: Commentary on J.Y. Interpretation No. 603 of the Constitutional Court, Taiwan Law Journal, No.76, p.222-234.
77. Lee, Chen-Shan (2007), Move the Weight on the Balance of Communication Security and Surveillance: Commentary on J.Y. Interpretation No. 631 of the Constitutional Court, Taiwan Law Journal, No.98, p.283-291.
78. Lee, Mau-Sheng (1998), Confession and the Structure of the Facts, in Mau-Sheng Lee, Power, Subject and Criminal Law, Vanity press, pp. 91-128.
79. Lee, Rong-Geng (2008), I Am Listening to You ( Part I): J.Y. Interpretation No.

- 631 of the Constitutional Court, Principle of Writ Doctrine, and Amendment of the Communication Security and Surveillance Act, Taiwan Law Journal, No. 104, P.47-60.
80. Lee, Rong-Geng (2008), I Am Listening to You ( Part II): J.Y. Interpretation No. 631 of the Constitutional Court, Principle of Writ Doctrine, and Amendment of the Communication Security and Surveillance Act, Taiwan Law Journal, No. 105, P.43-56.
81. Lee, Rong-Geng (2008), Yes,I do: Search with Consent and the Third Party's Consent, The Taiwan Law Review, No. 157, 2008, P. 102-125.
82. Lee, Rong-Geng (2012), Search and Seizure of Electromagnetic Records, National Taiwan University Law Journal, Vol. 41, No. 23, P. 1055-1116.
83. Leiter, Brian (2007), Law and Objectivity, in: Naturalizing Jurisprudence: Essays on American Legal Realism and Naturalism in Legal Philosophy
84. Lilly, Graham C. (1987), An Introduction to the Law of Evidence, 2nd ed., West Publishing, N.Y.
85. Lilly, Graham C., Capra, Daniel J and. Saltzburg, Stephen A. (2009), Principles of Evidence, 5th edition, Thomson Reuters: USA.
86. Lin, I-Long and Yen, Yun-Sheng (2011), “VOIP Digital Evidence Forensics Standard Operating Procedure”, International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No.1.
87. Lin, Jiun-Yi (2011), Criminal Procedure Law Textbook I, 12th edition, Sharing publish: Taiwan.
88. Lin, Kun-Lin, Wang, Shih-Jeng, Chang, Yueh-Hann, Chiang, Wen-Ya & Huang, Jia-Hong (2008), Unveiling Controversy of Trojan Defense on Internet Forensics, Criminal Bimonthly, No. 65, 2008, P.85-96.
89. Lin, Yu-Hsiung (2001), freie Beweiswürdigung- Is the judge's discretion really free?, Taiwan Law Journal, No. 27, pp.13.

90. Lin, Yu-Hsiung (2001), in dubio pro reo and Legal Evaluation, *The Taiwan Law Review*, No. 72, pp.18.
91. Lin, Yu-Hsiung (2002), *Kommentar- Durchsuchung und Beschlagnahme*, Angel publish: Taiwan.
92. Lin, Yu-Hsiung (2008), Aerial View on 2003 Amendment of the Code of Criminal Procedure, in Yu-Hsiung Lin, *Coercive Measure and Criminal Evidence*, Angel publish: Taiwan..
93. Lin, Yu-Hsiung (2008), Cover Pandora's Box: J.Y. Interpretation No. 582 of the Constitutional Court Ends the Sixth Form of Evidence, in Yu-Hsiung Lin, *Coercive Measure and Criminal Evidence*, Angel publish: Taiwan.
94. Lin, Yu-Hsiung (2013), *Criminal Procedure Law*, 7th edition, angel publish: Taiwan, 2013.
95. Lin, Yu-Shun (2007), Commentary on J.Y. Interpretation No. 631 of the Constitutional Court and the Communication Security and Surveillance Act, *The Law Monthly*, Vol. 51, No. 11, pp. 1740.
96. Liou, Chiou-Ling (2009), *The Admissibility of Digital Evidence in Criminal Proceedings*. Master thesis. College of Law, National Chengchi University..
97. Luhmann, Niklas (1983), *Legitimitation durch Verfahren*, Suhrkamp: Frankfurt a. M.
98. Luhmann, Niklas (1987), "The Unity of the Legal System", in: G. Teubner (Ed.), *Autopoietic Law: A New Approach to Law and Society* (pp. 12-35), Walter de Gruyter, Berlin.
99. Luhmann, Niklas (1995), *Social Systems*, trans. by Bednarz, Jr. & Baecker, Stanford Univ. Press.
100. Lynch, Michael (2008), *Science, Common Sense, and DNA Evidence*, in:

Michael Lynch, Simon A. Cole, Ruth McNally & Kathleen Jordan (2011), Truth Machine: The Contentious History of DNA Fingerprinting, pp.190-219, University Of Chicago Press.

101. Marcum, Catherine D. & Higgins, George E. (2014), Corrections and Social Networking Websites, in: Social Networking as a Criminal Enterprise, CRC press, 221-229.

102. McCarthy, Terrence W. & Nichols-Gault, Allison (2014), A Guide to the Admissibility of Social Media/ Electronic Evidence in Alabama, 75 Ala. Law. 42.

103. McCartney, Carole (2012), Forensic Identification and Criminal Justice. Forensic Science, Justice and Risk, Routledge, NY: USA.

104. McPartland, Molly D. (2013), An Analysis of Facebook “Like” and Other Nonverbal Internet Communication Under the Federal Rules of Evidence, 99 Iowa L. Rev. 445.

105. McPeak, Agnieszka (2014), Social Media Snooping and its Ethical Bounds, 46 Ariz. St. L.J. 845.

106. Mercuri, Rebecca (2010), Criminal Defense Challenges in Computer Forensics, In: Goel S. (ed.) ICDF2C 2009, LNICST 31, pp. 132-138.

107. Mercuri, Rebecca (2010), Criminal Defense Challenges in Computer Forensics, in S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 132-138.

108. Morales, Lawrence (2014), Social media evidence: “what you post or tweet can and will be used against you in court of law”, 60 The Advoc. (Texas) 32.

109. Murphy, J.P. & Fonteilla, A. (2013), Social Media Evidence in Government

- investigations and criminal proceeding: a Frontier of New Legal Issues, 19 Rich. J.L. & Tech. 11.
110. n Chu, Shih-Ye (2007), Criminal Procedure, 3rd edition, Sanmin publish: Taiwan.
111. National Institute of Justice (2008).Electronic Crime Scene Investigation: A Guide for First Responders. <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>
112. Nissenbaum, Helen (2009), Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford Law Books).
113. North, Evan E. (2013), Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites, 58 Kansas L. Rev. 1279.
114. Palmer, G. (2001), "DFRWS Technical Report: A Road Map for Digital Forensic Research," First Digital Forensic Research Workshop (DFRWS), New York: Air Force Research Laboratory, pp. 14-31. available at <http://www.dfrws.org/2001/dfrws-rm-final.pdf>
115. Pan, Shi-Mo & Chen, Chen-Ming (1995), Science in Modern Society, Shu Xin Publishing House.
116. Pannozzo, Allison L. (2012), Uploading Guilt: Adding a Virtual Records Exception to the Federal Rules of Evidence, 44 Conn. L. Rev. 1695.
117. Park, Robert (2003), The Seven Warning Signs of Bogus Science, The Chronicle of Higher Education 49 (21), 20.
118. Parker, Christopher E. & Swearingen, Travis B. (2012), "Tweet" Me Your Status: Social Media in Discovery and at Trial, 59-FEB Fed. Law. 34.
119. Robbins, Ira P. (2012), Writing on the Wall: The Need for an Authorship-Centric

Approach to the Authentication of Social-Networking Evidence, Minnesota Journal of Law, Science & Technology, Vol. 13, No. 1, 1-36. American University, WCL Research Paper No. 2011-31. Available at: <http://ssrn.com/abstract=1949332>

120. Roxin, Claus (1998), German Code of Criminal Procedure, trans. Li-Chi Wu, Sanmin publish: Taiwan.
121. Science and Technology Committee (2004).Forensic Science on Trial: Seventh Report of Session 2004–05. <http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf>
122. Scientific Working Group on Digital Evidence, “SWGDE Model Quality Assurance Manual for Digital Evidence Laboratories”, Version 3, Sep. 2012. <https://www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20QAM%20of%20Digital%20Evidence%20Laboratories-v3.0>
123. Sholl, E. W. (2013), “Exhibit Facebook: the Discoverability and Admissibility of Social Media Evidence,” 16 Tul. J. Tech. & Intell. Prop. 207.
124. Sholl, Emma W. (2013), Exhibit Facebook: The Discoverability and Admissibility of Social Media Evidence, 16 Tul. J. Tech. & Intell. Prop. 207.
125. Skoudis E. D. & Zeltser, Lenny (2003), Malware: Fighting Malicious Code, Prentice Hall press.
126. Taylor Robert W. et al. (2005), Digital Crime and Digital Terrorism, 1 edition, Prentice Hall.
127. Taylor, Kathryn R. (2014), “Anything You Post Online Can and Will Be Used

- against You in a Court of Law”: Criminal Liability and First Amendment Implication of Social Media Expression, 71 Nat’l Law. Guild Rev. 78.
128. Tsai, Chen-Jung & Chang, Wei-Ping (2000), Research on Computer Crime Evidence, Criminal Law Journal, Vol. 44, No. 2, P.54.
129. Tsai, Chen-Jung & Huang, Yue-Ting (2005), Admissibility of Digital Evidence, Criminal Law Journal, Vol. 49, No. 2, P.5.
130. Tsai, Mei-Chih (1999), Relevant Disputes about Network Monitoring in the Communication Security and Surveillance Act, Science & Technology Law Review, Vol. 11, No. 12, 1999, P.32-45.
131. Tsai, Ming-Feng (2005), Explore the True Nature of Computer Forensics, Criminal Bimonthly, No. 4, P. 18-23.
132. Tsai, Tun-Ming (1997), Criminal Evidence Law, Wunanbooks: Taiwan.
133. U.S. Department of Justice (1999), Forensic Examination of Digital Evidence: A Guide for Law Enforcement, available at: <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
134. Uncel, Megan (2011), Comment, “Facebook Is Now Friends with the Court”: Current Federal Rules and Social Media Evidence, 51 JURIMETRICS 43.
135. Valverde, Mariana (2009), Law’s Dream of a Common Knowledge, Princeton University Press.
136. Wang, Chin-Li (2013), Research on Digital Evidence of Computer Network Crime Investigation, Taiwan Prosecutor Review, No. 13, p.13-28.
137. Wang, Jau-Hwang (2003), Forensics and Collection of Digital Evidence, Police Science Bimonthly, Vol. 34, No. 3, P. 133-156.
138. Wang, Ming-Yung (2003), Search and Seizure of Cybercrime, Law Journal, No. 191, 2003, P. 45-62.
139. Wang, Shiuh-Jeng, Ke, Hung-Jui & ICCL, Information and Network Security:

Eyes of Secret –State of the Art on Internet Security and Digital Forensics, DrMaster Press: Taiwan.

140. Wang, Shiuh-Jeng, Ke, Hung-Jui & Yang, Chung-Huang (2002), Discussion on Evidence of Retention of Web Security, Communations of the CCSI, Vol.8, No.4, 2002, P.89-100.
141. Wang, Shiuh-Jeng, Lee, J. S. & Hsu, Fu-Hau (2015), The Security of Information, Intelligence and Mobile Networks in Applications, DrMaster press: Taiwan..
142. Wang, Shiuh-Jeng, Lin, Chu-Hsing & Tso, Ray-Ln (2013), Digital Forensics and Security in Applications of Computer and Mobile Systems, DrMaster Press, Taipei: Taiwan.
143. Wilson, C, Boe, B, Sala, A, Puttaswamy, Krishna P. N., & Zhao Ben. Y. (2009), User Interactions in Social Networks and their Implications, ACM EuroSys 2009, p. 1.
144. Wilson, John S. (2007), MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence, 86 Oregon L. Rev. 1201.
145. Wu, Hsun-Lung (2003), A Review on the Investigative Method of Real Evidence and Documentary in Taiwan Criminal Procedure, Taipei Bar Journal, No. 286, P.53-68.
146. Yen, Chen-Shen (1996), The Case of O. J. Simpson and Disputes over the American Jury System, America & Europe Monthly, Vol. 11, No. 1, P.116.