Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DOTTORATO IN DIRITTO E NUOVE TECNOLOGIE: INDIRIZZO DI INFORMATICA GIURIDICA

Ciclo XXV

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

CARATTERISTICHE INNOVATIVE NELL'ACQUISIZIONE DI DATI DI INFORMATICA FORENSE IN AMBIENTI VIRTUALI

Presentata da: **BARDARI ULRICO**

Coordinatore Dottorato
CHIAR. MO
PROF. GIOVANNI SARTOR

Relatore
CHIAR. MO
PROF. CESARE MAIOLI

Esame finale anno 2013

Indice generale

INTRODUZIONE

La disciplina dell'informatica forense ha origine in ambienti giuridici di *common law* ad alta evoluzione tecnologica come gli Stati Uniti[1] e la Gran Bretagna e ha visto sorgere numerose agenzie specializzate fornitrici di servizi di informatica forense, di formazione e in taluni casi vendono il *computer forensics tool kit*, valigetta virtuale analoga a quella che l'anatomo-patologo usa per acquisire materiali da utilizzare nelle perizie di medicina legale.

In Italia la disciplina viene lasciata molto alla libera interpretazione dei singoli consulenti tecnici che in sede civile o penale che agiscono in qualità di "longa manus" della parte che ne richiede l'intervento.

Questo problema è persistito anche successivamente al recepimento della Convenzione di Budapest da parte dell'Italia con la L.18 marzo 2008, n. 48.

Mancano soggetti preposti al delicato ruolo della progettazione e mantenimento di una *catena di custodia* per garantire che non si sono prodotte alterazioni ai dati dal momento del loro sequestro al momento del dibattimento e per tutte le fasi dell'iter processuale.

Troppo spesso il consulenti tecnici che si propongono all'Autorità Giudiziaria sono impreparati oppure non riescono a descrivere adeguatamente la propria competenza nella relazione conclusiva o in udienza.

[1] La data di nascita della Computer forensics è il 1984, quando il laboratorio scientifico dell'FBI e altre agenzie investigative americane iniziarono a sviluppare programmi da utilizzare nell'esame dei dati presenti nei computer. Nello stesso anno, per rispondere alla crescente richiesta di investigazioni in ambito informatico, fu creato, all'interno dell'FBI, il Computer Analysis and Response Team (CART) con il compito fondamentale di procedere nei casi in cui si rende necessaria l'analisi di un computer.

Il codice di procedura penale non fa distinzioni qualitative sulla custodia di un documento cartaceo e di un documento informatico.

Nell'ambito di un procedimento penale o civile una analisi informatica forense è volta a conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer (o qualunque supporto digitale si venga chiamati ad analizzare).

A livello generale si tratta di individuare le modalità migliori per:

- acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano,

- garantire che le prove acquisite su altro supporto siano identiche a quelle originarie,

- analizzare i dati senza alterarli.

In particolare, in ambito penale per un'acquisizione ed analisi di supporti informatici oggetto d'indagine, vista la natura dell'oggetto e il rischio di compromissione in ogni momento, è indispensabile il ricorso (da parte dei PM che, a norma dell'art. 358 cpp., si accingono ad indagare) all'art. 359 per l'assunzione di una prova deve necessariamente essere espletata da personale esperto.

In Italia dottrina e giurisprudenza relative a temi di informatica forense sono presenti per quasi ogni ambito giuridico a causa del veloce processo d'informatizzazione con sistemi di comunicazione digitale sempre più veloci e sempre più diffusi.

Vi è poi la convergenza tra personal computer, gli elettrodomestici e la telefonia mobile in apparecchiature individuabili in *personal digital device.*

In questo contesto si può concretamente formulare l'ipotesi che ogni procedimento civile o penale necessiti di un'analisi informatico forense.

Il V.F.A. (Virtual Forensic Ambient), nome sintetico dato alla struttura progettata e sperimentata, è stato pensato per dare la possibilità ad ogni attore giudiziario di poter disporre dei contenuti dei supporti informatici senza dover conoscere necessariamente le tecniche di informatica forense e senza dover utilizzare strumentazioni particolari.

Il risultato delle virtualizzazioni dei dischi e delle macchine possono essere fruibili da qualunque elaboratore connesso alla rete internet se preventivamente autorizzato.

Il progetto risulta efficace qualora vengano adottate le linee guida informatico forensi già adottate nel Common Law**:**

- verificare accuratamente lo stato di ogni supporto magnetico,

-ispezionare quaderni, fondi di tastiera e monitor per individuare eventuali *password*,

- ricostruire (*tracing*) l'attività di un accesso abusivo dalla rete[2]

- individuare virus e altro software malevolo[3],

- ricostruire la successione dei compiti e delle azioni,

- confrontare tra loro gli indizi,

- individuare il ruolo che assume il sistema oggetto della indagine,

- considerare il ruolo delle persone che utilizzano il sistema per individuare eventuali individui indiziati, informati dei fatti o in grado di rivelare la *password*[4],

[2] A tal fine è necessaria un'approfondita conoscenza dei protocolli di rete e dei server di posta elettronica in modo da poter individuare il punto di partenza dei dati e dei messaggi stessi. In questa attività si dimostrano particolarmente utili i sistemi di IDS (Introduction Detection System).

[3] Per codice malevolo [5] si intende il software che è utilizzato per ottenere e mantenere un potere o un vantaggio non autorizzato su un'altra persona; modalità tipiche del suo utilizzo riportate in letteratura comprendono: accesso remoto, raccolta dati, sabotaggio, blocco di un servizio (*denial of service*), intrusione in un sistema, furto di risorse informative, circonvenzione dei meccanismi di controllo degli accessi, necessità di riconoscimento di stato sociale, autosoddisfazione (l'*hacker* buono).

- effettuare un accurato inventario delle attrezzature ispezionate,
- ripetere almeno due volte le analisi per avere certezza della meticolosità delle operazioni eseguite.

Per conservare la prova informatica vengono osservate opportune cautele affinché le prove non siano maneggiate da personale non autorizzato e siano conservate in luoghi sicuri e adeguatamente presidiati come sedi giudiziarie o Data Center adeguati alle norme sul trattamento di dati sensibli.

L'obiettivo è quello di proteggere l'integrità della prova e di evitare che la mancanza di una custodia appropriata sia eccepita nel processo.

Nel sistema progettato ogni attività viene documentata attraverso la conservazione di *file di log*[5] e la creazione di *snapshot*[6] in momenti differenti dell'analisi.

Dal punto di vista del metodo, una doppia copia iniziale è il sistema di snapshot servono affinchè l'indagine di informatica forense non avvenga sul sistema informatico originale ma su copie dei dati e dei sistemi fedeli su cui lavorare in un secondo tempo.

La sperimentazione considera la catalogazione degli strumenti utilizzati, compresi software e versioni utlizzate.

La metodologia usata per analizzare i dati viene spiegata nel dettaglio e tiene conto del chi e del tempo impiegato.

---

[4] L'analisi comportamentale e la ingegneria sociale di solito consentono di affinare la ricerca delle persone colpevoli di reati. La seconda fa riferimento principalmente alle modalità con cui password e simili informazioni riservate vengono carpite da persone ignare e non coinvolte nel reato; la prima consente di effettuare una correlazione tra i dati acquisiti e le modalità di azione di una persona sospetta. I suoi passi tipici vanno dalla definizione di un insieme di sospetti alla comprensione dei possibili motivi di comportamento doloso, per poi effettuare le interviste alle persone interessate e gli interrogatori ai sospetti, comprendere eventuali errori compiuti da chi gestisce la sicurezza.

[5] File che eseguono la registrazione cronologica delle operazioni man mano che vengono eseguite.

[6] Uno snapshot è la registrazione dello stato del sistema congelata in preciso istante e di sola lettura.

Deve essere applicato un sistema di verifica e di registrazione dei procedimenti usati, che renda possibile la ripetizione da parte di terze parti.

Il software utilizzato viene conservato nel tempo perché solitamente i programmi vengono aggiornati di frequente, mentre i processi durano anni.

I. IL PROGETTO DI RICERCA

PREMESSA

Lo sviluppo, la sperimentazione e la realizzazione di questo progetto di ricerca non sarebbe stato possibile senza l'indispensabile contributo dei seguenti collaboratori:

Stefano Bianco, informatico forense di lunghissima esperienza, ha contribuito a fornire idee utili alla concretezza degli obiettivi da perseguire.

Luca Guerrieri, noto per la sua lunga esperienza d'informatico forense, riconosciuta a livello internazionale, nonché sviluppatore di "Forlex" ha curato tutta la parte di scrittura del codice sorgente rendendo concreto e tangibile il lavoro sviluppato nella lunga fase di progettazione.

Il dott. Marco Rubboli del CESIA ha supervisionato tutte le operazioni di installazione e creazione dell'infrastruttura di rete e ha collaborato alla configurazione delle stesse.

1. ARTICOLAZIONE DEL PROGETTO

Il progetto consiste nella sperimentazione di un'analisi informatica forense di supporti digitali inerenti un ipotetico procedimento per cui si richiederebbe una CTU, con la partecipazione diretta della P.G. e della A.G. rendendo disponibile, sotto forma di macchine e dischi virtuali, il contenuto dei supporti sequestrati che potrà essere visionato alla pari del supporto originale.

La prima fase ha previsto l'acquisizione dei supporti informatici sequestrati in duplice copia fisica attraverso strumenti d'acquisizione noti tramite fibra ottica.

La copia fisica è stata realizzata in formato intellegibile e compatibile per permettere la migliore fruibilità alle parti.

Si è convenuto che tra i possibili supporti d'idonea capacità, esistenti in commercio, ove riversare la copia di sicurezza, si scegliesse l'*hard disk esterno* poichè ad un costo più contenuto ed in grado di rendere meglio fruibili-trasportabili i dati nelle future fasi del procedimento. D'obbligo precisare che per garantire l'inalterabilità del contenuto bisognerà sempre avvalersi di un dispositivo di protezione in scrittura per evitare accidentali modifiche.

Si può giungere in questo modo alla preservazione dell'integrità, della riservatezza e della disponibilità del dato.

Depositata la copia fisica con le dovute garanzie di ripetibilità si procede alla creazione di dischi e macchine virtuali delle copie riversate nei server del Data Center e l'eventuale *Crack* (rottura) delle Password di accesso ai profili utente dei vari sistemi operativi.

Ovviamente in questa fase vi potrebbe essere un'alterazione di una delle copie fisiche utilizzate per la virtualizzazione ma di fatto grazie ad un sistema di cache e di snapshots si preserva il dato originale da tale rischio.

Per rendere visibile tutto il contenuto del PC come se fosse stato accesso in un momento successivo al sequestro si ha ovviamente un'alterazione di alcuni file di sistema, tuttavia possono essere preservati tutti i dati contenuti nel supporti ripristinando la *Virtual Machine* al primo avvio.

La scelta di operare il *Password Cracking* è stata studiata ad-hoc per lasciare all'utente finale la possibilità di scegliere se fruirne o meno e, eventualmente, della modalità

d'accesso (es. se azzerare la password di amministratore potendo così accedere a tutti i contenuti, oppure la password di utente per consentire una visualizzazione più fedele al contesto in cui agiva l'indagato).

Dopo aver riversato i dati, creato le macchine e i dischi virtuali e quant'altro richiesto dall'operatore si stabilisce una VPN (Virtual Private Network) tra il Data Center e l'A.G. o la P.G. operante (anche entrambe) per consentire a chi sia preventivamente autorizzato al trattamento dati di poter visualizzare i contenuti di ogni singolo supporto.

Oltre alla modalità di accesso alle informazioni in VPN per ridurre ulteriormente le possibilità di accesso indesiderate o non autorizzate in un test specifico è stato utilizzato un sistema di rilevazione e valutazione di credenziali biometriche con l'ausilio di un apparato dedito al riconoscimento dell'iride[7].

Rispondendo alla necessità giuridica della genuinità della prova è sempre possibile effettuare l'estrapolazione dalla copia fisica integra di quei dati che la A.G. e/o la P.G. operante ritenessero utili ai fini dell'indagine.

Solo attraverso tale procedura il dato estrapolato può ritenersi copia fedele all'originale.

---

[7] Telecamera per il riconoscimento dell'iride "**Authenticam**", realizzata da Panasonic e funzionante con il software Private ID di Iridian Technologies, porta alla totale eliminazione di password e garantisce nuovi standard di sicurezza sia in caso di PC locali che in caso di reti Client/Server. "**Authenticam**" fornisce un'autenticazione di elevatissima affidabilità in pochi secondi. È sufficiente fissare lo sguardo verso la telecamera da una distanza di circa 48 - 53 cm per l'acquisizione dell'immagine digitalizzata dell'iride, il cui codice viene quindi confrontato con i dati contenuti in data base.
Viene così garantita un'autenticazione ad altissima fedeltà in tempo reale. L'architettura del server KnoWho della Iridian può consentire l'integrazione con sistemi di sicurezza preesistenti.

2. L'ATTIVITA' SPERIMENTALE

Le sperimentazioni tecniche svolte hanno trovato applicazione nei laboratori della Biblioteca Giuridica Antonio Cicu siti a Bologna in via Zamboni 27-29, con un'importante apporto tecnologico da parte del CESIA (Centro Servizi Informatici dell' Università di Bologna).

Sono state installati 3 Server:

- ESXi: HP ProLiant DL585 (G2) Generation 2 - 4 x Dual-Core AMD 8212 2.0 GHz - 32gb RAM - 7 x 72GB SAS Drive
- NAS: HP ProLiant DL380 (G3) Generation 3 - 2 x Intel Xeon 2.8 GHz - 5gb RAM - 6 x 300GB Ultra320 SCSI Drive
- WEB (5000€): HP ProLiant DL380 (G3) Generation 3 - 2 x Intel Xeon 2.8 GHz - 4gb RAM - 6 x 36GB Ultra320 SCSI Drive

Prima di procedere all'acquisizione dei supporti da analizzare, al fine di accertare le caratteristiche hardware dei supporti stessi, si è proceduto alla verifica della reale configurazione installata utilizzando apposito software.

I supporti sono acquisiti fisicamente e integralmente, utilizzando un modulo di protezione in scrittura hardware "TABLEU mod. T35es" ed il software "EnCase versione 6.17", al fine di poter rendere fruibile il contenuto, senza alterare i dati presenti.

Si è scelto il software EnCase, già utilizzato nell'attività forense in U.S.A. e in Europa occidentale, perché in possesso di una licenza con chiave hardware oltre ad essere ormai un software largamente noto per la sua affidabilità ed aderenza ai crismi della Digital Forensics.

Altre copie dei supporti attivi (PC, Notebook, Smartphone, ecc.) sono state eseguite con la distribuzione Linux e gli strumenti in essa disponibili per acquisizione ed

analisi forense open source Forlex 2.0.5 per consentire la successiva virtualizzazione delle macchine.

Entrambi i sistemi accedono ai dischi in modalità RO (Read Only), dando la possibilità di vedere in anteprima o di copiare fisicamente il contenuto degli stessi in un'altra unità.

Le copia fisiche eseguite con EnCase e Forlex è stata riversate prima su alcuni hard disk di dimensione idonea a contenere la capacità dei supporti da analizzare e in seguito nel server "NAS" attraverso connessione diretta al server o su rete locale Gigabit.

Durante la copia, i dati sono stati compressi e riversati in una serie di file in formato noto e "aperto" per permettere eventuali ulteriori verifiche, nonché, a maggior garanzia, è stata effettuata un'operazione di *hash*[8] gli stessi.

Il risultato dell'operazione di *hash* effettuata al momento dell'acquisizione, confrontato con quello risultante dalla lettura del supporto nei quali sono stati riversati i dati copiati, devono risultare uguali a garanzia che i dati siano inequivocabilmente gli stessi.

Nella progettazione è stata considerata la possibilità che il disco con le copie fisiche possa giungere già pronto da inserire nel sistema di virtualizzazione, ma prevede anche l'opportunità di eseguire copia fisica con gli strumenti idonei descritti direttamente da parte di chi amministra il Virtual Forensic Ambient.

[8] Nel caso studiato MD5 hash è una funzione matematica a 128 Bit secondo la quale, qualsiasi argomento dato in input, restituisce un risultato sempre delle stessa lunghezza . Le possibilità di argomenti diversi e risultati di output uguali è di 1/2 128. La corrispondenza tra i due valori dunque è garanzia dell'autenticità dei dati analizzati.

In via preliminare è necessaria una "ricognizione" degli *hard disk* al fine di determinare il Sistema Operativo delle macchine valutando quale fosse la loro destinazione.

Le copie fisiche riversate nel server "NAS" sono salvate in formato noto (esempio immagine creata con DD[9]) e da queste sono state create delle macchine e dei dischi virtuali anche con l'ausilio del protocollo iSCSI (descritto nei paragrafi successivi).

Per incoraggiare i giuristi a proseguire nella lettura dei prossimi paragrafi, partiamo dalla fine anticipando l'esito della sperimentazione mostrando i principali output messi a disposizione dell'utente finale:

- la possibilità di navigare su un disco virtuali di pari contenuti all'originale da una qualunque postazione remota dotata di internet e di comune Browser web (Fig.1)
- la possibilità di accendere una macchina virtuale da una qualunque postazione remota dotata di internet (Fig.2)

Fig.1 Disco virtuale montato con WebDAV

[9] dd è un comando dei sistemi operativi Unix e Unix-like, è tipicamente usato per la copia di dispositivi a blocchi e può essere usato per creare file sparsi

Fig.2 Desktop remoto della macchina virtuale realizzata con il VFA

Sostanzialmente dopo aver generato i file di configurazione di VirtualBox (vbox) ed i relativi dischi virtuali (VDI), con una tecnica che permette la protezione in scrittura delle immagini disco originali, si permette l'azzeramento della password di Amministratore del Sistema Operativo con un software di Password Craking (nella sperimentazione creato ad hoc con una versione customizzata per i vari sistemi Microsoft di BurtPE[10])

[10] **BartPE** è un programma per creare un CD avviabile basato su Microsoft Windows XP o Server 2003. In sostanza è un CD avviabile basato sul sistema operativo Windows XP, offre alcune caratteristiche interessanti nel risolvere i problemi di Windows. BartPE può essere avviato e utilizzato senza scrivere o modificare dati sul disco rigido, cioè funzionando solo ed esclusivamente all'interno della memoria RAM.

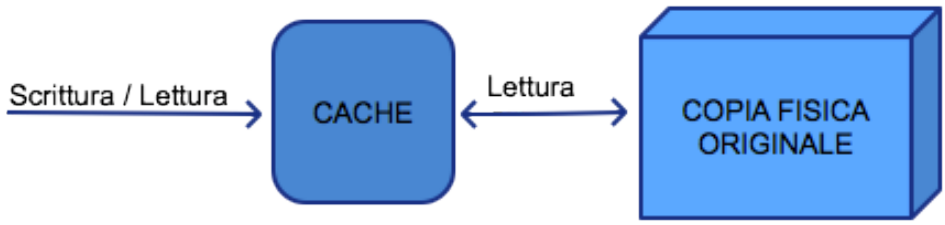


Fig. 3 Sistema di protezione dalla scrittura con memoria cache

Terminata l'operazione di azzeramento della password di amministratore e/o di utente (a discrezione di chi deve effettuare le analisi) ogni file di copia fisica viene nuovamente posta in protezione di scrittura ed avrà ad esso associati dei file di configurazione di Virtual Box che permette di visualizzare una macchina virtuale corrispondente a quella reale accessibile con i diritti di amministratore di sistema senza però poterne alterare il contenuto.(FIG. 1 e 2)

L'inalterabilità del contenuto della macchina virtuale non è stata concepita con l'intento di preservare l'integrità della macchina che la P.G. operante andrà a visionare (l'integrità è garantita dagli *Hash* delle copie fisiche effettuate con EnCase o Forlex e depositate unitamente all'elaborato), ma anche per mantenere inalterati i contenuti delle cartelle, dei file e le rispettive posizioni.

3. TECNOLOGIE ADOTTATE

3.1 SAS (SECURE AUTHENTICATION SYSTEM)

Il SAS è un sistema di autenticazione che permette la gestione dell'accesso a servizi offerti attraverso la piattaforma web.

Le tecnologie impiegate sono il linguaggio PHP ed MXML (Macromedia Flex Markup Language) mentre per l'esecuzione sono stati utilizzati i sistemi Apache e MySQL.

Il sistema di autenticazione tratta un controllo basato su "ticket" concesso al momento dell'autenticazione.

	userid	username	password	level	group	ticket	active
	1	luca	3dfea430c9ea20a3b6ad60fa5cdac2ad	1	1	0	1
	2	utente005	3dfea430c9ea20a3b6ad60fa5cdac2ad	4	1	0	1
	3	ulrico	3dfea430c9ea20a3b6ad60fa5cdac2ad	3	1	ecdafa14acf0278bcc06bf9483e27748	1
	6	utente001	3dfea430c9ea20a3b6ad60fa5cdac2ad	5	1	0	1
	7	amministratore	3dfea430c9ea20a3b6ad60fa5cdac2ad	2	1	0	1
	12	utente002	3dfea430c9ea20a3b6ad60fa5cdac2ad	5	1	0	1
	13	utente003	3dfea430c9ea20a3b6ad60fa5cdac2ad	5	1	0	1
	14	utente004	3dfea430c9ea20a3b6ad60fa5cdac2ad	5	1	0	0

Fig.4 Associazione del "ticket" all'utente autorizzato all'accesso

In pratica, la visualizzazione dei contenuti è permessa solo se sono presenti, contemporaneamente più condizioni.

Resta importante specificare che il sistema di login ha la peculiarità di effettuare la fusione e criptazione delle credenziali di accesso, inserite dall'utente, direttamente lato client.

Il client, infatti, realizza l'*hashing* md5 di username, password e di una stringa di caratteri in formato immagine, generata casualmente dal sistema e visualizzata direttamente a video con il sistema durante l'avvio di una sessione http CAPTCHA[11]. (FIG.5)

[11] L'acronimo deriva dall'inglese "completely automated public Turing test to tell computers and humans apart" ed è un test fatto di una o più domande e risposte per determinare se l'utente sia un umano (e non un computer o, più precisamente, un bot)

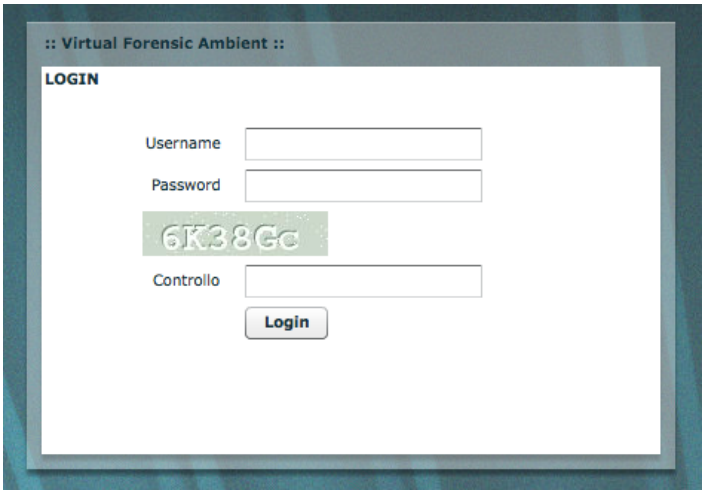


Fig. 5 Interfaccia di autenticazione

L'*hash* di queste informazioni viene trasmesso al server di autenticazione. Quest'ultimo, ricevuta tale informazione, controlla innanzitutto che l'utente esista (in caso negativo non prosegue e rilancia la pagina di login).

Nel caso in cui esista prova a generare la stessa stringa hash con le informazioni in suo possesso.

Username	Level	Group	Azioni
luca	1	1	edit
utente005	4	1	edit
ulrico	3	1	edit
utente001	5	1	edit
amministratore	2	1	edit
utente002	5	1	edit
utente003	5	1	edit
utente004	5	1	edit

Fig.6 Elenco utenti sistema

Se l'esito è positivo vuol dire che nessuno ha alterato i dati, altrimenti non consente le successive operazioni e rimanda immediatamente alla pagina di login.

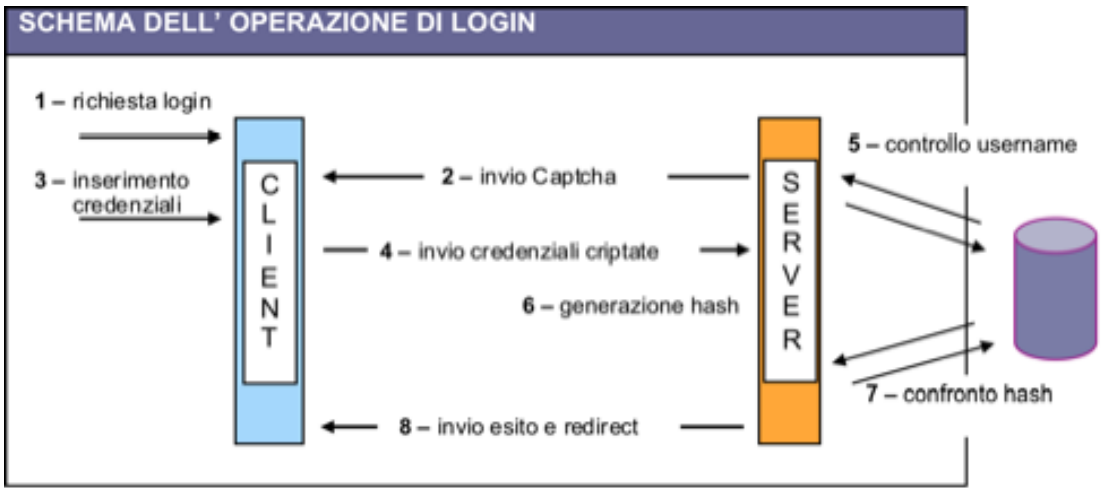


Fig. 7 Schema di login

La sequenza delle operazioni eseguite dal sistema di autenticazione è la seguente:

1. richiesta di login
2. visualizzazione pagina di login con avvio del client grafico per il successivo invio della stringa CAPTCHA per criptare le credenziali di accesso;
3. inserimento da parte dell'utente delle credenziali di accesso criptate;
4. invio delle credenziali di accesso al server
5. il server controlla l'esistenza della username in caso affermativo procede altrimenti ripete la visualizzazione della pagina di login
6. il server genera una stringa di hash composta dagli stessi dati inviati al client (Captcha + username + password)
7. il server confronta le due stringhe hash (ricevuta e generata) nel caso coincidano procede, altrimenti ripete la visualizzazione della pagina di login
8. invio esito delle operazioni di login e successivo redirect all'area privata.

3.2 SISTEMI OPERATIVI E FILE SYSTEM ADOTTATI

Al fine di garantire la massima versatilità del sistema progettato ci si è avvalsi di svariate tecnologie note ai sistemisti.

Ognuna di queste tecnologie, spesso è già completamente implementata in software, applicative e distribuzioni Linux e/o BSD[12].

Per la realizzazione l'intera piattaforma di lavoro, necessaria al coordinamento ed alla realizzazione delle diverse risorse, è stato impiegato il sistema operativo DEBIAN Linux.

Questa distribuzione gode di una serie di caratteristiche concordi alla politica realizzativa del progetto di ricerca ed in particolare:

- è in grado di garantire maggiore stabilità (specie nel *branch* STABLE);
- garantisce un'ottima aderenza allo standard POSIX[13];
- la predisposizione ad integrare diverse tecnologie innovative attraverso un'enorme comunità di sviluppatori.

DEBIAN Linux permette inoltre di utilizzare tutte le più note applicazioni realizzate per la *Digital Forensics* rendendo di fatto VFA scalabile.

L'area storage (SAN – Storage Area Network) è stata realizzata utilizzando il sistema operativo FreeBSD.

---

[12] L'acronimo BSD (Berkeley Software Distribution) indica la variante originaria di Unix sviluppata presso l'Università di Berkeley in California e alla base di una delle due famiglie principali di sistemi operativi liberi attualmente più diffusi, tra cui gli esponenti più noti sono FreeBSD, OpenBSD, NetBSD, PC-BSD, DesktopBSD, FreeSBIE, DarwinOS (il cuore unix di Mac OS X) e DragonFly BSD (con le sue distribuzioni FireflyBSD e GoBSD) (Wikipedia)

[13] POSIX (o Posix: Portable Operating System Interface for Unix) è il nome che indica la famiglia degli standard definiti dall'IEEE denominati formalmente IEEE 1003. Il nome standard internazionale è ISO/IEC 9945

La distribuzione FreeBSD viene utilizzata soprattutto per la gestione di tipo server è nota per la sua stabilità e scalabilità della parte di networking ma anche di *storaging*.

Il sistema operativo FreeBSD è in grado di affrontare efficacemente anche le problematiche di sicurezza. Attualmente sono disponibili tre sistemi di *firewall* integrati : IPFW, IPFilter e PF.

I *file system*[14] utlizzati per la realizzazione del progetto sono ZFS e EXT3.

ZFS è un *file system* con capacità di indirizzare uno spazio di memoria elevato[15] per i sistemi di sicurezza integrati (metodo transazionale ad oggetti copy-on-write; *snapshot*; compressione; blocchi a dimensione variabile; Priorità I/O con *scheduling* di tipo *deadline*; ecc.).

ZFS permette la realizzazione:

- di oggetti denominati *Dataset* (un *dataset* è simile ad una directory su di un volume ma si comporta come un *file system* e quindi supporta *snapshot*, quote e compressione);
- di *Snapshots* (copia *read-only* del *file system* al momento);
- dei Device virtuali (*virtual devices*).

Ext3 è un *file system* utilizzato su sistemi GNU/Linux.

La velocità di scrittura e di lettura lo rendono adatto all'esecuzione di operazioni di una macchina Linux.

---

[14] il filesystem è una struttura utilizzata per l'organizzazione dei dati in un dispositivo ad accesso diretto, ad esempio un disco rigido; tali dispositivi si contrappongono a quelli ad accesso sequenziale, tipicamente i nastri magnetici.

[15] ZFS è un file system a 128 bit: può quindi fornire uno spazio di 16 miliardi di miliardi di volte la capacità dei file system attuali a 64 bit. I limiti del ZFS sono stati progettati per essere così ampi da non essere mai raggiunti in una qualsiasi operazione pratica. Bonwick affermò che "per riempire un file system a 128 bit non sarebbero bastati tutti i dischi della terra". (Wikipedia)

Ext3 è un *file system journaled*, pertanto, si riduce notevolmente la possibilità di incorrere in errori, malfunzionamenti hardware, interruzioni di alimentazione o di connessione con altre risorse.

3.3 SISTEMI DI CONDIVISIONE

Il protocollo adottato per per la condivisione di directory fra computer e lo scambio di file e messaggi è il CIFS (Common Internet File System) noto anche come SMB (Simple Message Block).

Trattasi di un protocollo di livello applicativo che si basa su una struttura client-server[16] ed ha una logica di tipo request-response[17]. Una condivisione SMB una volta montata è considerata come un device locale e per tanto potrà essere utilizzata in maniera trasparente alla sua reale locazione fisica.

SMB nato originariamente da un progetto di IBM e poi ampiamente sviluppato da Microsoft, è quello utilizzato di default da Windows per la condivisione dei file.

La sua presenza nel panorama informatico è ormai affermata rendendo assicurata l'integrazione di un client SMB in ogni tipo di S.O. e di dispositivo che abbia accesso a tecnologie di network.

Questo protocollo utilizza il TCP/IP e permette di applicare politiche di sicurezza come autenticazione utente e controllo della concessione di accesso ad una porzione di filesystem.

---

[16] I sistemi client/server sono un'evoluzione dei sistemi basati sulla condivisione semplice delle risorse. La presenza di un server permette ad un certo numero di client di condividerne le risorse, lasciando che sia il server a gestire gli accessi alle risorse per evitare conflitti di utilizzazione tipici dei primi sistemi informatici

[17] Il sistema request/response fornisce informazioni relative alle richieste inviate dall'utente all'applicazione web mentre il secondo ci consente di inviare messaggi di risposta al client.

Il server controlla la presenza dell'utenza nel suo elenco utenti ad ogni richiesta di accesso, in caso positivo procede a controllare i diritti sul filesystem.

Il processo avrà esito positivo se l'utente ha i diritti per accedervi altrimenti verrà negato l'accesso lasciando l'utente autenticato al server ma senza condisione.

Oltre a quanto descritto una caratteristica fondamentale di SMB è la sua scalabilità sia per la gestione utenti (perchè facilmente interfacciabile con server DB oppure LDAP) che per la gestione di condivisioni (con limite puramente fisico).

Per consolidare l'archiviazione di dati su dispositivi virtuali, dando l'illusione al server di lavorare su dischi locali è stato utilizzato il protocollo ISCSI (Internet Small Computer Systems Interface).

L'ultima implementazione del protocollo lo rende davvero competitivo rispetto al Fibre Channel, tanto che molti produttori di NAS lo integrano nativamente.

iSCSI è una tecnologia che permette di collegare un dispositivo a blocchi residente su di un'altra macchina (*target*) attraverso lo *stack* IP (utilizzando le porte fisiche n. 860 e 3260), permettendo alla macchina che lo monta (*initiator*) di usarlo come un dispositivo connesso ad essa fisicamente.

Infine vi è la possibilità di applicare politiche di sicurezza con autenticazione CHAP (username e password) e Mutual CHAP nonchè di indirizzare a livello IP delle risorse permettendo il routing e l'uso del sistema DNS.

Al fine di rendere il WWW un mezzo di lettura e scrittura come se fosse una directory remota - *web share* – è stato utilizzato un set di istruzioni del protocollo HTTP noto come WebDAV (Web-based Distributed Authoring and Versioning).

La sua realizzazione avviene impiegando server web (es.: Apache).

All'interno di tale condivisione possiamo dunque creare, modificare, spostare i file contenuti.

Il protocollo offre anche un sistema di protezione da sovrascrittura dei file, di gestione della proprietà (creazione, rimozione, modifica, ecc.), oltre ad elevato numero di funzionalità.

WebDAV permette, inoltre, il controllo degli accessi (anche su server DB) e s'integra facilmente con tutti i moderni sistemi operative.

3.4 LINGUAGGI DI PROGRAMMAZIONE UTILIZZATI

PHP (acronimo ricorsivo per PHP: Hypertext Preprocessor) è un linguaggio di *scripting general-purpose open source* orientato al web.

Come altri linguaggi di *scripting* può essere integrato direttamente nel codice HTML che compone una pagina.

Esso, infatti, trova la sua massima applicazione nella realizzazione di siti web ed interfacce grafiche offerte attraverso i relativi server.

Deve la sua notorietà anche alla facile integrazione con sistemi database quali MySQL e alla totale integrazione con il server http Apache grazie al relativo modulo *libapache2-mod-php5*.

JAVASCRIPT è un linguaggio di *scripting* orientato agli oggetti comunemente usato nella creazione di siti web.

JavaScript è stato standardizzato dalla ECMA con il nome di ECMAScript ed è anche uno standard ISO é un linguaggio interpretato ed è debolmente tipizzato nonchè debolmente orientato agli oggetti.

HTML (HyperText Markup Language) è un linguaggio di markup utilizzato per la formattazione di documenti ipertestuali comuni nel WWW e note anche come pagine web. Non si stratta di un linguaggio di programmazione ma solamente di un linguaggio di formattazione che descrive dunque le modalità di presentazione e visualizzazione grafica

AJAX (*Asynchronous JavaScript* and XML) è una tecnica di sviluppo software per la realizzazione di applicazioni web interattive (*Rich Internet Application*). Lo sviluppo di applicazioni HTML con AJAX si basa su uno scambio di dati in background fra *web browser* e server, che consente l'aggiornamento dinamico di una pagina web senza esplicito ricaricamento da parte dell'utente.

BASH SCRIPT, che non è proprio un linguaggio di programmazione, viene utilizzato per organizzare il flusso operativo di una sequenza di comandi su console BASH.

3.5 PIATTAFORME SERVER, VIRTUALIZZAZIONE E FORENSICS

Le piattaforme server adottate sono Apache HTTP Server e MySQL.

Apache HTTP Server, è un software che realizza le funzioni di trasporto delle informazioni, di *inter network* e di collegamento, più diffuso.

Apache ha il vantaggio di offrire anche funzioni di controllo per la sicurezza.

MySQL è un motore di database relazionale molto diffuso. La sua notorietà è dovuta alle sue ottime performance ed alla sua semplicità di gestione, nonché per la sua velocità, flessibilità ed affidabilità.

La virtualizzazione permette di emulare alcuni dispositivi hardware (hard disk, scheda grafica, scheda di rete, ecc.) in tal modo, in concorso con opportune tecniche, è possibile ricreare un intero sistema informatico.

Per implementare un sistema di virtualizzazione che sia in grado di offrire ottime performance ma anche elevate opportunità di configurazione è stato scelto Oracle VirtualBox.

Questo sistema può essere configurato anche attraverso una interfaccia CLI, semplificando l'esecuzione di script di automatizzazione.

Il progetto è inoltre dotato di una VirtualBox Main API che comprende tutte le interfacce COM pubbliche ed i componenti messi a disposizione da VirtualBox server e VirtualBox client library.

Per investigare su dispositivi di memorizzazione ovvero su immagini di dischi una libreria ed un insieme di comandi *The Sleuth Kit* (TSK).

La funzionalità più importante di TSK è la capacità di analizzare volumi e dati a livello di *file system*.

4. V.F.A. - VIRTUAL FORENSIC AMBIENT

V.F.A. (Virtual Forensic Ambient) è la denominazione sintetica data al progetto di ricerca ed in particolare all'ambiente di lavoro operativo.

Questo sistema, permette la virtualizzazione di tutte le procedure che gestiscono la fonte di prova digitale.

Il VFA coordina la gestione e gli accessi alle risorse unendo tra loro tecnologie note e stabili.

Ciò consente di inserire il sistema anche in realtà esistenti senza sconvolgerne l'operatività.

La possibilità di accedere alle risorse offerta dal VFA attraverso sistemi operativi e dispositivi già disponibili agli utenti finali (ma anche agli amministratori) lo rendono scalabile e compatibile rispetto alle future tecnologie.

4.1 MYSQL

Il server DB, per il VFA è il luogo ove vengono strutturate le informazioni ed associati gli oggetti.

Es.: un'immagine disco associata ad un supporto che fa parte di un caso al quale hanno accesso un certo numero di utenti.

Il DB consta in 2 databases:

1) Auth - Destinato a memorizzare le informazioni inerenti le credenziali di accesso infatti in esso si memorizzano le tabelle (Fig. 8) :

- users : gli utenti con i relativi livelli operativi
- profili : i profili utente - nome cognome ecc.

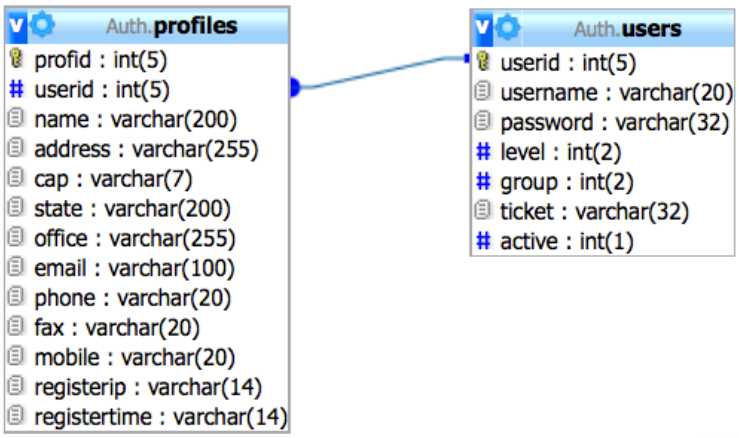


Fig.8 Datbase Auth

2)Casi - Destinato a memorizzare tutte le informazioni inerenti le entità che sono chiamate in causa da un Procedimento Penale ed i supporti di memorizzazione che esso include (Fig. 9) :

- procedimenti: tabella dei procedimenti ove si registrano le caratteristiche di un procedimento
- supporti: tabella in cui si gestiscono i supporti e le loro caratteristiche
- immagini: tabella in cui si gestiscono le immagini disco e le loro caratteristiche
- usersprocs: tabella in cui si associano gli utenti ed i procedimenti
- vdis: tabella dei dischi virtualizzati
- vms: tabella delle machine virtuali

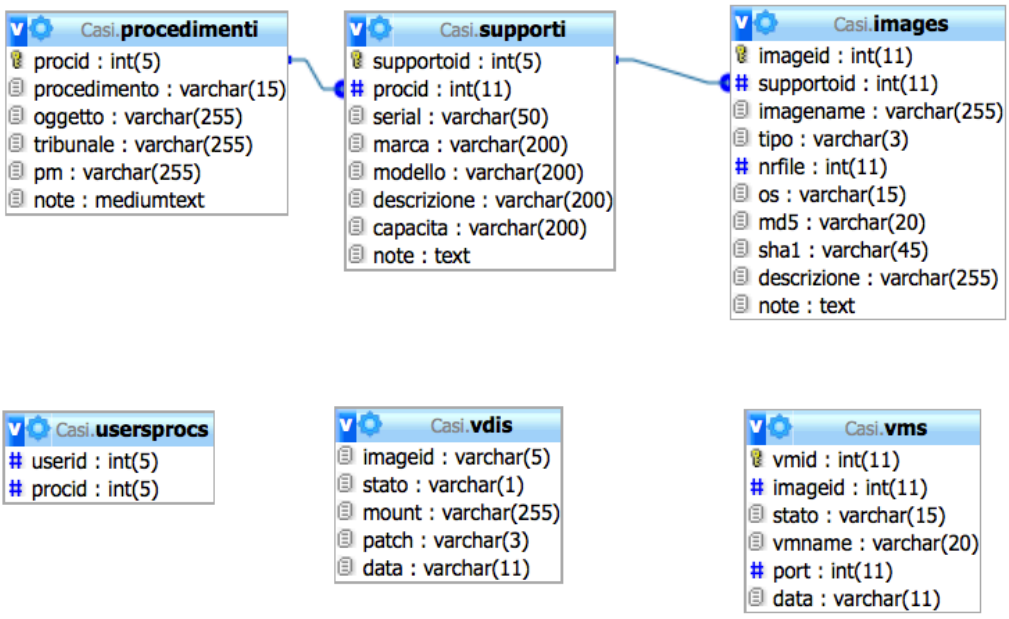


Fig. 9 Database Casi

4.2 WEBGUI

Il server di WEBGUI[18] è il sistema che permette l'interfaccia a tutte le funzionalità ed alle precedenti risorse elencate.

Tutte le operazioni di mounting, creazione, applicazione patch, ecc. si possono realizzare sia da riga di comando sia da interfaccia WEBGUI.

In realtà la WEBGUI, lavorando con il server DB, permette di gestire il sistema evitando di porlo in una condizione d'instabilità ovvero di incongruità.

[18] WebGUI può essere considerato un Content Management System ma anche un application framework in quanto svolge entrambe le funzioni. È scritto in Perl ed è open source in quanto rilasciato con licenza GNU General Public License nel 2003

Fig.10 Home Page VFA

L'accesso alla WEBGUI avviene solo se assegnatari di un certificato e di credenziali di accesso.

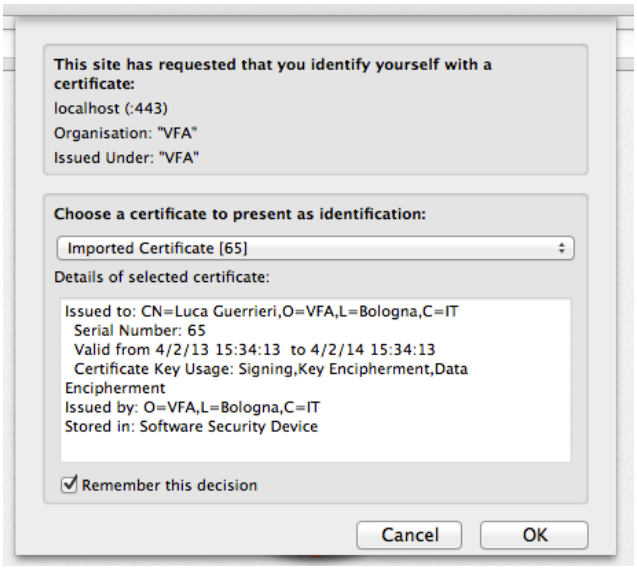


Fig.11 Importazione del certificato

In questo modo la risorsa sarà disponibile solo agli utenti preventivamente registrati (identificati direttamente e personalmente) ed a cui è stato concesso un certificato con scadenza pari alla durata dell'incarico.

Si pensi ad esempio al conferimento d'incarico di un C.T.U. ai sensi del art.359 c.p.p. , il certificato potrebbe valere 90 gg. al termine dei quali, in caso di proroga verrebbe rinnovato, altresì non sarebbe più permesso l'accesso alla WEBGUI per scadenza del mandato.

A seguito della fase di login, dunque l'utente avrà a disposizione i seguenti strumenti di gestione

Fig.12 Barra dei menù

Fig.13 Desktop dell'applicativo

Iniziando dalla voce menu inerente il profilo utente si avranno i seguenti links:

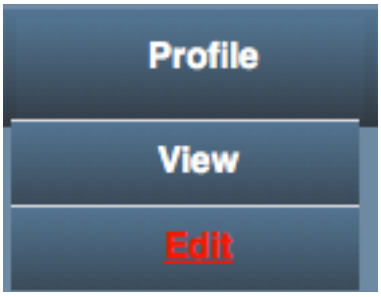


Fig.14 Menù gestione utenti del sistema

Da questi sarà possibile non solo visualizzare (View) le informazioni inerenti il profilo dell'utente con cui si è effettuato accesso al sistema

Fig. 15 - Visualizzazione del profilo utente

ma anche la modifica (Edit)

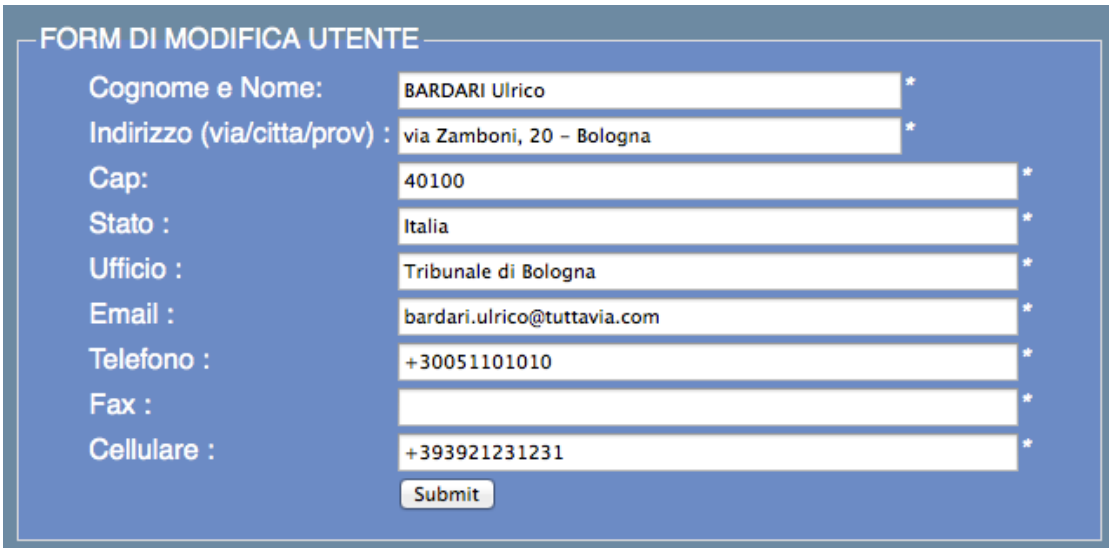


Fig. 16 Form per modifiche all'utente

4.3 PIXA FRAMEWORK

Il PiXA Framework, è il framework alla base di tutto il sistema, un insieme di classi e funzioni che permettono l'implementazione di tutte le funzionalità dell'interfaccia di gestione e il relativo ulteriore sviluppo. Per la realizzazione sono state impiegate le tecniche del OOP[19] (Object Oriented Programming) oltre ad utilizzare funzionalità specifiche per la connessione a risorse realizzate con altri linguaggi come XML[20].

[19] La programmazione orientata agli oggetti (OOP, Object Oriented Programming) è un paradigma di programmazione che permette di definire oggetti software in grado di interagire gli uni con gli altri attraverso lo scambio di messaggi. È particolarmente adatta nei contesti in cui si possono definire delle

La scelta è ricaduta su PHP (Hypertext Preprocessor) anche per la semplicità e la velocità del ciclo di sviluppo, nonché per l'ampia documentazione.

Con PiXA sono state realizzate tutte le funzionalità.

4.4 PATCH

VFA è in grado di applicare una PATCH per rendere, in caso di necessità, una immagine di un disco di una macchina fisica compatibile con un ambiente virtuale.

L'attività tecnica si realizza attraverso i seguenti passaggi:

1. monta l'immagine disco rendendola un dispositivo (*device*) di memorizzazione accessibile

Fig.17 Interfaccia di "virtualizzazione" di una immagine disco di un dispositivo con S.O.

2. crea un disco VDI con il *device* appena creato
3. crea un'apposita macchina virtuale per l'applicazione della patch

relazioni di interdipendenza tra i concetti da modellare (contenimento, uso, specializzazione). Un ambito che più di altri riesce a sfruttare i vantaggi della programmazione ad oggetti è quello delle interfacce grafiche.

[20] XML (sigla di eXtensible Markup Language) è un linguaggio di markup, basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.

Fig. 18 - Interfaccia di realizzazione ed applicazione della patch

4. applica la patch da live CD

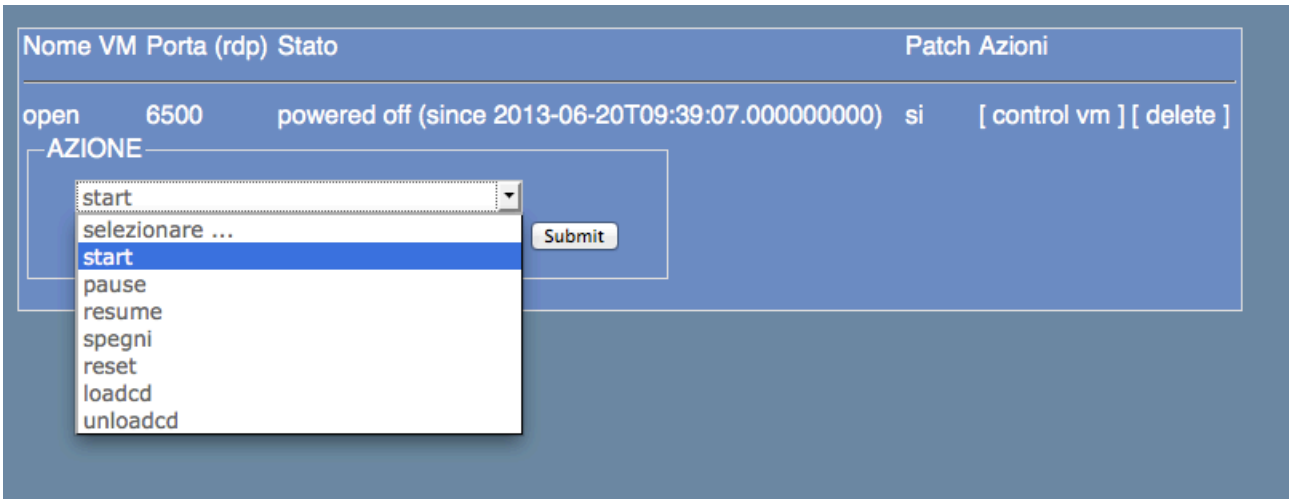


Fig. 19 Avvio della macchina virtuale per l'applicazione della patch

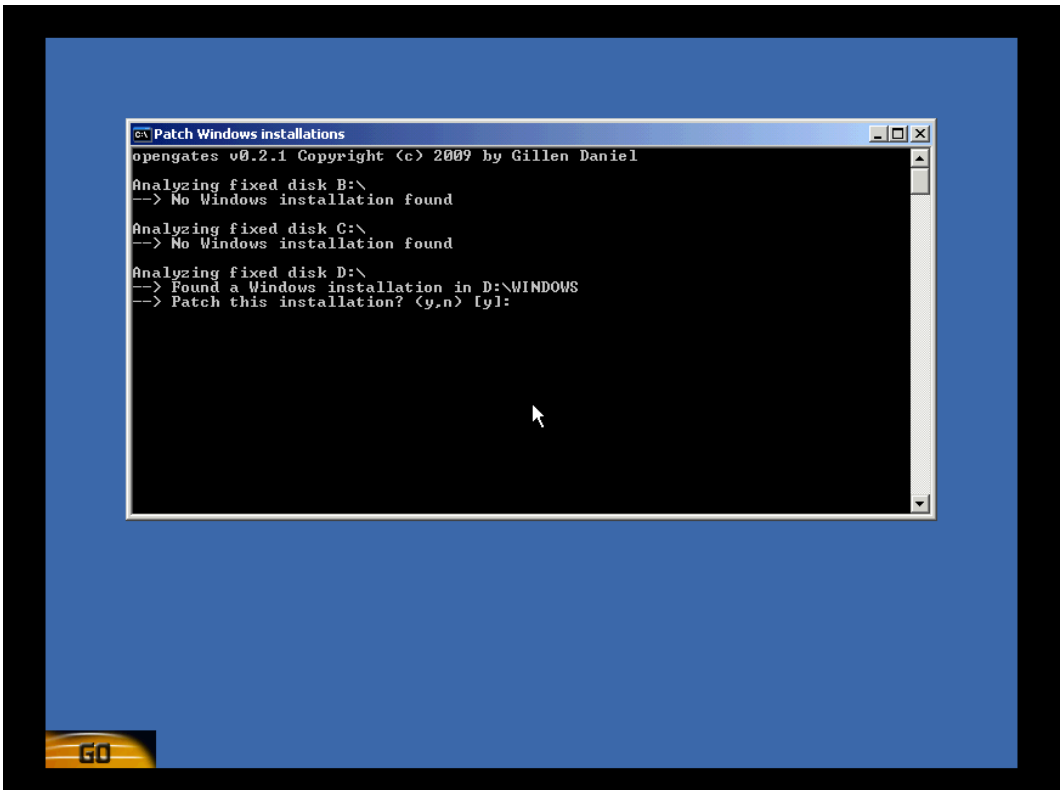


Fig. 20 Applicazione della patch

5. rimuove la macchina

A questo punto il disco VDI è pronto per essere connesso ad una macchina virtuale convenzionale per essere avviato.

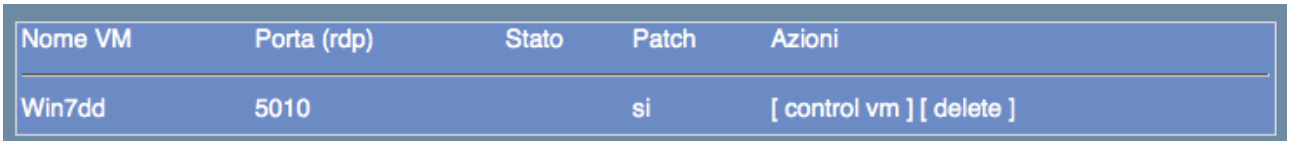


Fig. 21 Interfaccia di gestione macchine virtuali

Si noti come non sia presente in riferimento all'applicazione della patch in quanto nella colonna Patch vi è espressione della sua precedente avvenuta applicazione.

4.5 FUNZIONAMENTO DEL VFA

All'interno del VFA sono state identificate le seguenti entità:

- Caso

  Un caso è il c.d. procedimento penale o comunque l'insieme di riferimenti che rendono unico un iter documentale riferito ad uno o più reati per i quali si procede.

Fig. 22 Menù gestione casi

- Dispositivo/Supporto

Il dispositivo elettronico di memorizzazione (es.: hard disk, usbstick, memoria sd, ecc.)

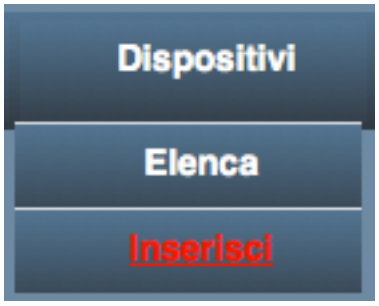


Fig.23 Menù gestione dispositivi

- Immagine

  Sono i file generati durante l'operazione di "acquisizione" del contenuto del supporto. L'immagine può essere in formato dd (disk dump) oppure EWF oppure E01.

Fig.24 Menù gestione immagini disco

- Disco VDI (per macchine virtuali)

  Disco virtuale utile ad eseguire macchine virtuali

- Immagine montata

  La presentazione del contenuto di una immagine disco come disco reale

Fig.25 Menù gestione dischi virtuali

- Macchina virtuale

  Macchina virtuale che emula una macchina reale utilizzando dischi virtuali (vdi) prodotti con apposite tecnologie da immagini disco.

Fig.26 Menù gestione macchine virtuali

La gestione dischi virtuali consente la creazione o la distruzione dei *drives* virtuali con i quali realizzare le macchine virtuali oppure per creare un disco virtuale che montato sarà visualizzato nel suo contenuto.

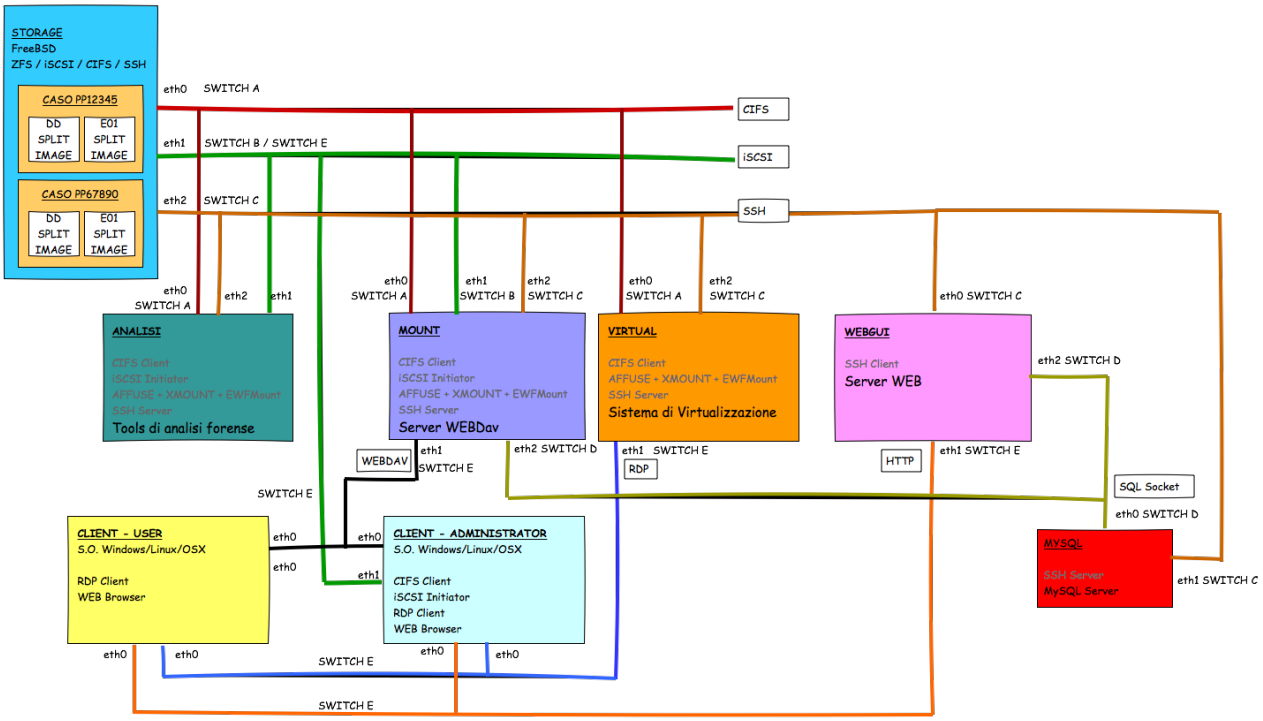


FIG.27 Schema generale del "Virtual Forensic Ambient

Come si può notare dallo schema (FIG.27) sono state definite diverse aree operative.

Il dispositivo STORAGE è stato realizzato con sistema operativo FreeBSD e file system ZFS.

Le condivisioni sono offerte attraverso CIFS e iSCSI.

1. Alla definizione di un Caso, il sistema crea un Dataset e lo rende disponibile ad un gruppo di utenti oltre che ad un gruppo di amministratori, ma con diversi privilegi;

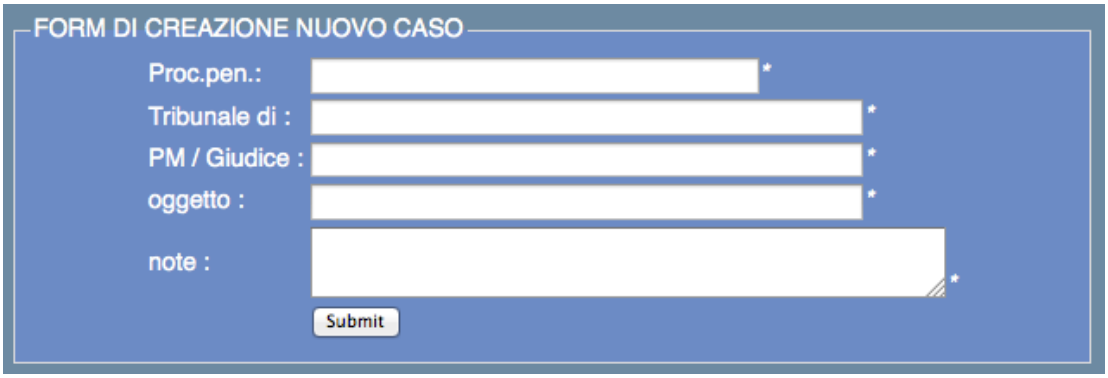


Fig. 28 Form creazione nuovo Caso

2. L'amministratore censisce tutti i dispositivi di memorizzazione presenti nel Caso e li inserisce nel VFA oltre ad associarli al relativo Caso;

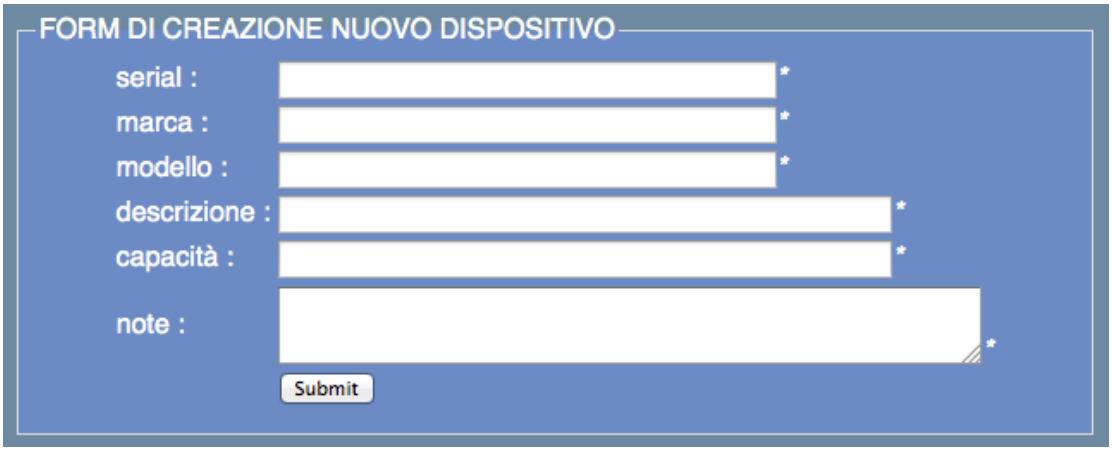


Fig.29 Form di creazione di un nuovo dispositivo

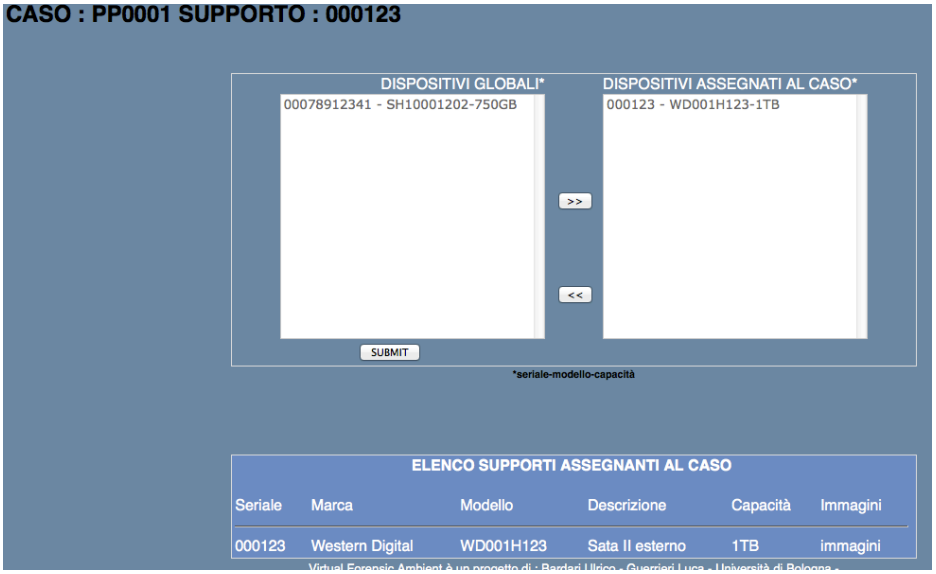


Fig.30 Interfaccia di gestione dei supporti e dei relativi casi

3. L'amministratore realizza l'upload delle immagini disco
4. L'amministratore associa le immagini disco ai relativi supporti. Si noti come in questa fase si possono associare, se realizzate, tutte le immagini realizzate da quel supporto (magari con diverse tipologie di file contenitori : DD; EWF; E01, ecc)

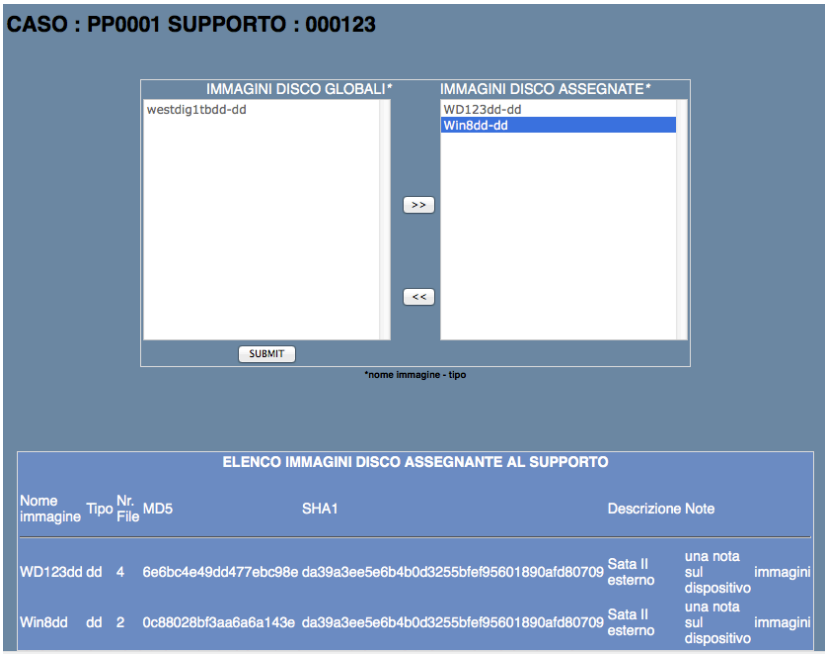


Fig. 31 Interfaccia di gestione per l'associazione delle immagini ad ogni dispositivo

5. L'amministratore esegue lo *snapshot* del *Dataset* ;
6. Si clona lo snapshot per la successiva condivisione;
7. Si condivide con CIFS;
8. Si crea un volume (ZVOL) per lo storaging delle attività di analisi
9. Si condivide via iSCSI.

Il dispositivo di Analisi esegue l'estrazione di dati (es. immagini, documenti word, documenti pdf, ecc.) nella seguente sequenza:

1. monta la giusta share CIFS
2. monta il volume iSCSI
3. esegue l'analisi di ogni disco riversando l'esito delle ricerche all'interno del volume

L'attività di analisi è svolta da TSK.

Per raggiungere lo scopo non è necessario montare l'immagine in quanto TSK riesce ad analizzare il contenuto di immagini "splittate" (divise in più parti) di dischi senza doverle necessariamente ricostruire.

Il dispositivo di MOUNT permette di montare un'immagine disco come se fosse un disco reale al fine di poter fruire del contenuto attraverso una normale "navigazione". La tecnologia usata è WEBDAV (in sola lettura):

1. monta la giusta share CIFS;
2. monta l'immagine disco rendendola un dispositivo (device) di memorizzazione accessibile;
3. monta in loop il device;
4. condivide attraverso Webdav il mountpoint.

Fig.32 Interfaccia di creazione disco virtuale VDI

Il sistema che virtualizza le immagini disco e ne permette l'avvio con macchine virtuali sviluppa la seguente sequenza di operazioni:

1 monta la giusta share CIFS;

2 monta l'immagine disco rendendola un dispositivo (device) di memorizzazione accessibile;

3 crea un disco VDI con il device appena creato;

Fig.33 Esito operazione e percorso per la creazione della macchina virtuale

4 crea una macchina virtuale con il disco VDI;

Fig. 34 Disco virtualizzato; possibilità di connetterlo ad una nuova macchina virtuale

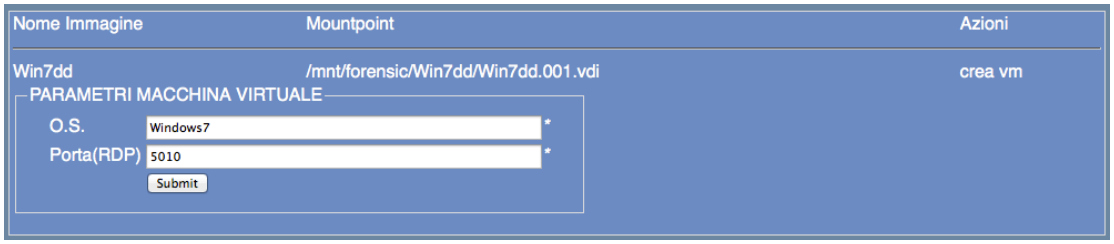


Fig.35 Creazione macchina virtuale per uso utente

In seguito sarà possibile gestire la macchina virtuale attraverso un apposito menù che offrirà le diverse opzioni operative (avvio / reset / spegnimento / pausa / resume / ecc.)

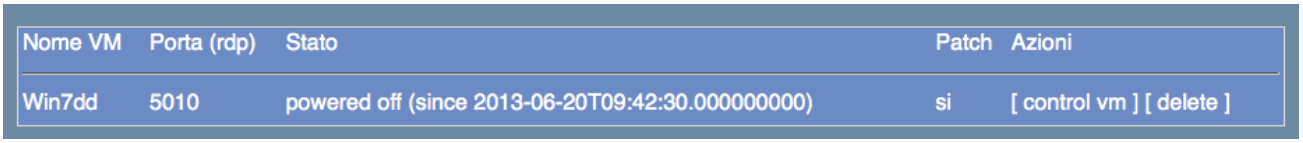


Fig.36 Esito creazione macchina virtuale

5. COSTI D'IMPIANTO

L'architettura di rete adottata per la sperimentazione risulta particolarmente abbondante sia per le finalità poste dalla ricerca sia per l'effettiva applicazione all'interno di un Tribunale o Procura della Repubblica.

Per soddisfare la richiesta di attività di analisi informatica forense di tutte le Procure di una regione medio-grande (quali ad esempio Veneto o Emilia Romagna) si possono utilizzare sostanzialmente 2 sistemi: un sistema ESXi *VMware* uno *storage* SAN.

ESXi è un sistema operativo dedicato alla virtualizzazione – nel gergo *bare metal hypervisor* – sviluppato da *VMware*, basato su un *kernel*[21] proprietario.

Tenuto conto che un server EXSi di marca affidabile può far girare circa 20 macchine virtuali in ambiente *VM Ware*.

VMware ESXi è la versione gratuita del famoso software di virtualizzazione *VMware* ESX.

In particolare, *VMware* ESXi 4 è installabile direttamente su un dispositivo di memorizzazione senza dover disporre di Windows o di *GNU/Linux* ed è disponibile solo per piattaforme x86 a 64 bit, a differenza della versione precedente che funzionava su hardware a 32 bit. Si tratta di un sistema operativo che contiene tutte le funzioni per creare, avviare e gestire le macchine virtuali senza programmi superflui come un'interfaccia grafica curata.

Data la volontà di contenere i costi d'impianto, la virtualizzazione è senz'altro una tematica di rilievo ed è interessante la possibilità di creare, con una spesa minima, un

[21] costituisce il **nucleo** di un sistema operativo. Si tratta di un software avente il compito di fornire ai processi in esecuzione sull'elaboratore un accesso sicuro e controllato all'hardware. Dato che possono esserne eseguiti simultaneamente più di uno, il kernel ha anche la responsabilità di assegnare una porzione di tempo-macchina (scheduling) e di accesso all'hardware a ciascun programma

server ESXi per creare in maniera scalabile cluster virtuali capaci di eseguire operazioni con la stessa efficacia di macchine reali.

Un'architettura SAN lavora in modo che tutti i dispositivi di memorizzazione siano disponibili a qualsiasi server della rete di cui la SAN in questione fa parte.

Una SAN può essere anche condivisa fra più reti interconnesse, anche di natura diversa: in tal caso uno dei server locali fa da ponte fra i dati memorizzati e gli utenti finali.

Il vantaggio di un'architettura di questo tipo è che tutta la potenza di calcolo dei server è utilizzata per le applicazioni, in quanto i dati non risiedono direttamente in alcuno di questi, ma sulla rete SAN appunto.

Normalmente una SAN utilizza dischi collegati con una o più catene (o array) di tipo RAID per migliorare le prestazioni e aumentare l'affidabilità del sistema.

Come previsto nella fase di sperimentazione, gli utenti e gli amministratori devono poter accedere ai dati in modo rapido e sicuro e quindi la filosofia dell'architettura SAN è quella più adatta perché in grado di integrare le caratteristiche principali dei tradizionali sistemi di memorizzazione:

1. Alte prestazioni
2. Alta disponibilità
3. Scalabilità
4. Facilità di gestione

Inoltre offrono una connettività *any-to-any* tra server e dispositivi di *storage*, aprendo in tal modo la strada al trasferimento diretto di dati tra periferiche di memorizzazione, con conseguenti indubbi miglioramenti dell'efficienza dello spostamento dei dati e di processi, e nel caso studiato per la replica dei dati.

Tutto questo attraverso un'architettura di rete dedicata alla gestione e archiviazione dei dati, in grado di non sovraccaricare i server nelle operazioni di scrittura e lettura dei dati.

L'impiego di ogni tecnologia di networking proposta per le reti SAN consente di:

1. raggiungere distanza di connettività superiori e prestazioni migliori rispetto a quanto non sia possibile dall'attuale tecnologia SCSI;
2. facilitare il compito di centralizzare la gestione dello storage che traineranno l'adozione di strategie di gestione remota e di protezione dei dati;
3. consolidamento dello storage e del *clustering* dei sistemi;
4. condividere i dati tra piattaforme diverse;
5. la protezione dei dati e il *disaster recovery*.

Potranno beneficiare di queste prestazioni tutte quelle applicazioni che richiedono un'elevata ampiezza di banda, quali ad esempio:

1. Storage e data consolidation;
2. Salvataggio di data base;
3. Applicazioni distribuite;
4. Applicazioni cluster;

5. Alta affidabilità;
6. Archivi di immagini, foto, grafica e dati multimediali;
7. Controllo e gestione dati;

Questi sistemi per i vantaggi elencati consentono di avere un prodotto adattabile alla previsione di richiesta di analisi nell'ambito di un singolo Procedimento fino alla gestione delle analisi richieste da più Procure o Tribunali fino all'ipotesi più ambiziosa di un sistema centralizzato nazionale.

Il costo da affrontare principalmente è quello dell'acquisto iniziale della struttura di rete, dopo di che ci si baserà su un 15-20% annuo rispetto alla spesa effettuata per il calcolo dell'assistenza, manutenzione e aggiornamento delle licenze.

Ad esempio un V.F.A. inserito in una struttura di rete composta da 2 server ESXI con 20 macchine virtuali ciascuno e un server SAN "*netapp* 2020" con una baia dischi *sata* da 2Tb per totali 100 Tb sarebbe in grado di servire l'attività di supporto consulenziale per le Procure di una Regione come il Veneto.

Il costo d'investimento iniziale, solo per il primo anno di messa in opera, potrebbe aggirarsi attorno ai 130.000 euro, importo che sarebbe di per se già al di sotto del costo delle CTU affidate in un anno solare dalle stesse Procure, ma vi sarebbe un abbattimento notevole per gli anni successivi in quanto sarebbe sufficiente sostenere un costo di circa 50.000 euro annui di assistenza/manutenzione / licenza.

Ciò consentirebbe di ammortizzare la spesa già dal primo anno, riscontrando grossi risparmi a partire dal terzo anno di fruizione del sistema.

Si è tenuto conto dei costi in euro, ma non si è calcolato il risparmio in termini di tempo e di fruibilità delle risorse da parte di accusa, difesa e giudice che potrebbe

portare ad esiti migliori ai fini della ricerca della verità ed abbattere i tempi di una fase procedimentale notoriamente lunga.

II. IL CYBER CRIME E LE INVESTIGAZIONI DIGITALI

1. LA CRESCITA DEL FENOMENO DEL *CYBER CRIME*

La legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti «*computer's crimes*», non ha enunciato, quale oggetto di tutela, la definizione di «sistema informatico», ma ne ha presupposto il significato ed i profili tecnici.

Invece l'art. 1 della Convenzione europea di Budapest del 23 novembre 2001 fornisce la definizione di «sistema informatico» individuandolo in «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati».

Attraverso tali definizioni per i reati informatici l'intendimento è che coinvolgano necessariamente l'utilizzo di un sistema di elaborazione, nel senso che la condotta dell'agente deve essere rivolta verso un computer o presupporre l'utilizzo di uno strumento tecnologico automatizzato.

Un'attività criminale che coinvolge sia il sistema informatico che il sistema telematico può generalmente definirsi come crimine informatico, compreso l'accesso non autorizzato, danneggiamento o cancellazione di dati, sistemi di interferenza con il funzionamento di un sistema informatico mediante l'immissione, trasmissione, danneggiamento, cancellazione, deterioramento, alterazione di dati informatici, uso improprio di dispositivi, furto d'identità e frodi elettroniche.

Nella categoria dei crimini informatici, eterogenei per modalità operative e scopi

della condotta, possono essere distinte alcune tipologie[22]:

– crimini con finalità di profitto per l'autore e di danno per la vittima (appropriazione o manipolazione di programmi e di informazioni, frodi elettroniche, ecc.);

– crimini diretti contro il computer allo scopo di provocarne la distruzione o l'inservibilità (sabotaggio, vandalismo, danneggiamento informatico);

– crimini correlati all'uso del computer per procurare danni ad individui o a intere collettività (estorsione, esercizio arbitrario delle proprie ragioni, attentato ad impianti di pubblica utilità, ecc.).

I reati in esame non solo minacciano la sfera privata ed il patrimonio, ma possono agevolare la rapida circolazione delle informazioni, venendo a costituire un efficace mezzo di comunicazione utilizzato anche per scopi illegali.[23]

Alcune fattispecie di reato tradizionali, come furti di informazioni, spionaggio, frodi, gioco d'azzardo, prostituzione, traffici vari, molestie, minacce, pedofilia, pornografia, criminalità organizzata e terrorismo, hanno subìto una evoluzione e sono in grado di articolarsi in prevalenza all'interno dei nuovi sistemi di comunicazione digitale (*cyberpedofilia, cyberterrorismo, cyberstalting, hacking*, diffusione di virus informatici, frodi telematiche, *spamming, netstrike*, diffusione di informazioni illegali on-line).

[22] F. MUCCIARELLI, Commento a: L. 23 dicembre 1993 n. 547 – Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, in Legisl. pen., 1996, 4, 57.
[23] M.M. ALMA-C. PERRONI, Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici, in Dir. pen. e proc., 1997, 3-4, 504.

L'approccio iniziale degli *hacker* era rivolto alla conoscenza dei sistemi informatici e della loro sicurezza, pertanto violando i sistemi con azioni non dannose.

I sostenitori dell'*hacking* sono motivati da fini artistici e politici, ma spesso sono indifferenti circa l'uso di mezzi illegali per raggiungerli.

Infatti il termine «*hacker*» nella sua accezione originaria (dall'inglese «to hack» che letteralmente significa «fare a pezzi» o «tagliare»), indica una persona per la quale la programmazione informatica costituisce una vera e propria passione, con l'obiettivo di dominare le macchine, di smontare i sistemi, di osservare come sono costruiti e come funzionano per scoprirne peculiarità nascoste e debolezze, o per innovare ed implementare le applicazioni.

Tuttavia, con la crescita dell'industria informatica, sono emersi i casi di violazione dei sistemi informatici per il proprio profitto personale.

Questa sottocategoria di hacker è stata definita "*cracker*".

Negli ultimi mesi del 2003 è stato possibile arrestare numerosi sospetti aderenti alle nuove Brigate Rosse, proprio grazie allo studio del traffico telefonico, *e-mail* e telematico riguardante alcune utenze considerate rilevanti dagli inquirenti.

In tale circostanza sono stati utilizzati sistemi di analisi particolarmente sofisticati ma adeguati all'oggetto d'indagine sviluppando modelli matematici e statistici grazie al contributo umano e tecnologico fornito dall'Università degli Studi di Bologna.

L'arresto della brigatista rossa Nadia Desdemona Lioce, il 3 marzo 2003, dove perse la vita il Sovrintendente della Polizia di Stato Emanuele Petri e il brigatista rosso

Antonio Galesi, ha fatto rinvenire alla Polizia Giudiziaria alcuni supporti informatici portatili poco diffusi in commercio in uso ai terroristi.

Galesi e Lioce sospettati di essere legati alle nuove BR e agli omicidi Biagi (19 marzo 2002) e D'Antona (20 maggio 1999) avevano un modo di comunicare per via telefonica e telematica assolutamente sicuro ed anonimo e solo il sequestro dei supporti utilizzati ha potuto fornire qualche indicazione in merito alla magistratura.

Inoltre, per indagare su quelle utenze telefoniche o indirizzi di posta elettronica, gli inquirenti hanno avuto bisogno dei tabulati sul traffico relativi a ben 4 anni prima.

Per internet a quei tempi non esisteva ancora una disciplina specifica e la durata e la modalità di conservazione erano legate alla collaborazione spontanea delle imprese fornitrici di servizi di telecomunicazioni.

L'evento che ha dettato l'evoluzione della normativa di settore è stato senza dubbio l'attacco terroristico alle Torri Gemelle di New York dell'11 settembre 2001.

L'organizzazione dell'attentato è avvenuta con sistemi di comunicazione oggi diffusissimi ma all'epoca innovativi, si tratta del VOIP (Voice Over IP).

Questa scoperta corredata di tutte le informazioni più utili alle indagini sono state ricavate dalle successive analisi sui supporti informatici sequestrati agli attentatori.

La stessa rivendicazione dell'attentato a Biagi venne diffusa via e-mail a circa 550 indirizzi e l'analisi della provenienza della mail ha portato ad una utenza telefonica cellulare intestata ad un nome fittizio e ad un internet point di Roma dove non venivano registrati i nomi delle persone che avrebbero fruito del servizio internet.

Una nuova stagione di terrorismo internazionale ha avuto inizio con quell'attentato, e le istituzioni hanno dovuto rispondere rafforzando gli strumenti di indagine di cui sono dotati la magistratura, le forze dell'ordine e servizi segreti.

Un esempio lampante è stata la pronta emanazione da parte del congresso statunitense dello Usa Patriot Act[24], il quale concedeva importanti deleghe, quasi in bianco, alle forze di polizia per intercettare le comunicazioni via internet, anche senza autorizzazione specifica da parte del giudice.

In Italia nello stesso periodo veniva varava la legge n. 431 del 14 dicembre 2001[25] e la legge n. 438 del 15 dicembre 2001[26].

Nel nostro ordinamento entra il reato di terrorismo internazionale e vi si applicano le disposizioni speciali sulla criminalità organizzata.

Negli ultimi anni Internet oltre ad essere stato un luogo di informazione, comunicazione, commercio e cultura ha facilitato anche l'attivismo politico (*"hactivism"* e *"cyber protest"*).

Con *"hactivism"* riguarda l'attività, politicamente motivata ed eseguita per via informatica, di attacco e da parte di hacker a siti Internet e network.

La *"cyber protest"*, invece, coinvolge non necessariamente interessi politici, ma problemi più ampi come quelli sociali, economici, culturali, religiosi o altro.

[24] acronimo di Uniting and Strengthening Usa by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

[25] Conversione in legge, con modificazioni, del decreto-legge 12 ottobre 2001, n. 369, recante misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale

[26]Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2001, n.374, recante disposizioni urgenti per contrastare il terrorismo internazionale

I noti eventi legati al terrorismo nazionale ed internazionale precedentemente citati, nonché quelli che stanno seguendo, danno nuovo impulso all'attivismo politico e alla protesta cibernetica.

Il problema è se tali azioni compiute nel *mondo virtuale*, sono capaci di produrre effetti nella vita sociale, ed eventualmente quali sono gli strumenti legislativi esistenti o da promulgare per tutelare la pace sociale.

Il termine *cyber war* nasce dalle occasioni in cui è accaduto che, a seguito di un incidente diplomatico – politico o ad un attacco di guerra convenzionale, seguisse un attacco informatico.

Un precedente famoso è quello del maggio del 1999, quando gli USA hanno bombardato accidentalmente l'ambasciata Cinese a Belgrado durante la campagna aerea della NATO.

A questo atto di guerra convenzionale, seguì il danneggiamento, in nome della Cina, di molti siti Web Americani nonché la diffusione di un gran numero di e-mail di solidarietà alla causa cinese.

Il sito della Casa Bianca fu messo fuori uso per tre giorni a causa dell'enorme quantità di e-mail ricevute[27].

Questa *cyber war*, fu però condotta in modo disorganizzato, in tempi troppo brevi e colpendo un limitato numero di siti. Non ha così provocato ingenti danni.

Questa azione di guerra informatica fra Paesi - sembra infatti che gli attacchi siano partiti tutti dalla Cina - ci fa comprendere come i fatti politici e sociali che accadono

[27]Come affermato dal rapporto NICP ottobre 2001

nel mondo tangibile si riflettono e producono attivismo ed effetti immediatamente nel mondo virtuale.

Fino ad oggi i fatti del mondo tangibile hanno prodotto danni ben più ingenti di quelli del mondo virtuale, ma d'ora in avanti potrebbe non essere più così.

Fra Israele e Palestina si combatte già da tempo una guerra informatica. Il 6 ottobre del 2000, con una sorprendente coincidenza con la violenza nelle regioni, subirono danneggiamenti 40 siti web israeliani e 15 siti palestinesi.

Successivamente gli hackers palestinesi colpirono ogni tipo di sito israeliano che fossero capaci di compromettere, spesso distruggendoli con messaggi come "*free palestine*" o "*free kashmir"28*.

Dalla guerriglia urbana condotta con strumenti poverissimi come pietre, bastoni si passa ad una guerra informatica avente, per gli eserciti di hackers contrapposti, un identico obiettivo: oscurare, infettare, *crackare* i siti degli avversari.

Paesi poveri e poco evoluti socialmente sono capaci di condurre una guerra informatica con virus[29] e strumenti altamente tecnologici che li rendono identici per potenzialità offensiva, ma non per quella difensiva, ai paesi occidentali.

Possiamo già trarre una conclusione scontata: fra occidente e oriente vi è certamente una disuguaglianza del "mondo tangibile".

L'occidente è evoluto socialmente, economicamente, militarmente.

Una guerra compiuta con i mezzi tradizionali "difficilmente" proclamerebbe vincitori i paesi orientali.

---

[28] Fonte rapporto NICP, ottobre 2001

[29] Si pensi a QuickFire, virus utilizzato contro il Ministero degli Esteri Israeliano che ha fatto saltare un server inviandogli getti di 32mila e-mail proveniente dallo stesso indirizzo di posta elettronica

2. LE INVESTIGAZIONI DIGITALI

Attualmente la scienza delle investigazioni digitali, ovvero l'analisi del dato digitale in un'ottica di eventuale e futura produzione in giudizio, rappresenta un argomento molto importante.

Ogni questione giuridica, dal diritto di famiglia al diritto tributario, dai rapporti commerciali ai crimini, sta assumendo sempre più una forma digitale.

In sempre più casi l'aspetto digitale diventa preminente anche quando la questione non ha direttamente a che fare con la tecnologia.

Come vedremo nel dettaglio nei prossimi capitoli i Consulenti Tecnici e gli operatori di questo settore si occupano di gestire correttamente l'acquisizione, la catalogazione, l'analisi e l'illustrazione in un eventuale giudizio di fonti di prova digitali, agendo spesso direttamente sulla scena del crimine.

Per garantire una corretta acquisizione, occorre conoscere ed adottare tecniche avanzate strettamente correlate alla tecnologia cui ci trova davanti.

Spesso in fase di analisi e di gestione di una fonte di prova di tipo digitale si è spesso costretti ad attuare vere e proprie azioni di attacco e di *hacking* per cercare di recuperare informazioni più complete e precise.

Ad esempio l'esperto deve prestare molta attenzione nei confronti dei vari *file system* o sistemi operativi rinvenuti sui dischi contenuti negli elaboratori, deve comprendere la reale natura del supporto facendo molta attenzione anche alla possibilità di rovinarlo durante le operazioni, deve saper interpretare il sistema di cifratura eventualmente utilizzato, deve saper estrapolare dati dalle aree nascoste del disco e deve conoscere la collocazione dei file temporanei e di quelli cancellati.

Tutti questi elementi rendono spesso anche l'esperto di *computer forensics* un informatico attento oltre che competente, ma anche un investigatore dotato d'intuito, tenacia, curiosità ed amore per la verità.

2.1 INTEGRITA' DEL DATO

Un primo punto importante, nella fase iniziale del trattamento dei dati a fini investigativi. richiede di soffermarsi sul concetto di integrità di quei dati che verranno a costituire una eventuale fonte di prova.

Per integrità s'intende, in questa sede, un aspetto molto semplice da comprendere: i dati, durante le operazioni, non devono essere in alcun modo modificati rispetto al loro stato originale.

Questo statement forse banale diventa però estremamente difficile da rispettare nella pratica e in un contesto digitale, nel quale l'intrinseca fragilità del dato è fenomeno comune e dove alcuni contesti particolari, ad esempio operare *live*[30] su un sistema o su una rete non permettono di evitare modifiche allo stato del sistema e del dato.

In un contesto simile, la prassi corrette per l'investigatore è quella di riuscire a fare "attraversare" al dato digitale tutto l'eventuale iter giudiziario, dalla scoperta dello stesso fino alla fine del procedimento, facendolo rimanere integro.

L'integrità del dato originale permette, come diretta conseguenza, la possibilità di successive e multiple copie ed analisi dello stesso, eventuali confronti anche a distanza di mollo tempo e, soprattutto, nell'immediatezza del fatto. la conservazione corretta della fonte di prova.

Si noti un aspetto interessante: l'idea di modifica al sistema che può avere in mente il giurista (probabilmente correlata al concetto di documento cartaceo) è differente, e

[30] Attività svolta su un sistema in funzione

molto meno sottile rispetto alle reali modifiche che avvengono in un sistema anche con operazioni apparentemente innocue che non modificano lo stato di fatto.

Ad esempio spostare un file da una cartella all'altra, o aprire un file per visionarlo causano modifiche successivamente contestabili.

Nella sentenza di primo grado per li delitto di Garlasco furono tenute in considerazione le modifiche apportate al sistema a causa di apertura e spostamento di file e inserimento di supporti magnetici da parte degli investigatori che per primi ebbero nella propria disponibilità il notebook dello Stasi.

In questo contesto la non ripudiabilità può essere intesa come la validità dell'esito delle investigazioni digitali e non contestabilità in un ambito legale.

Questo è un concetto classico di ripudiabilità mutuato anche dal mondo della firma elettronica della certificazione e del documento digitale.

Si procede raccogliendo fonti di prova che con un buon grado di certezza attribuiscono un fatto avvenuto in un ambiente elettronico a un soggetto, a un computer o ad una rete.

Sarà compito dell'esperto costituire una fonte di prova digitale che possa non essere ripudiata alle eventuali contestazioni di una controparte o di altri esperti circa il metodo con cui è stata acquisita.

Vi è poi la non ripudiabilità intesa come impossibilità da parte di un soggetto che ha commesso determinate azioni di contestare, rinnegare o escludere alcuni suoi comportamenti sui dati e sui sistemi.

2.2 LA FONTE DI PROVA E LA CATENA DI CUSTODIA

Il concetto più generico di catena di custodia (COC: *chain of custody*) si riferisce alla documentazione cronologica o alla traccia che mostra il sequestro, la custodia, il controllo, il trasferimento, l'analisi, e la disposizione di elementi di prova, fisica o elettronica.

Questi aspetti sono strettamente correlati al concetto di genuinità della fonte di prova.

Infatti il procedimento di gestione della fonte di prova digitale non deve presentare lacune dal momento della scoperta del dato (il sequestro o l'accesso alla scena del crimine) sino alla conclusione di qualsiasi tipo di operazione (la presentazione dei risultati dell'analisi in dibattimento).

Nella gestione del dato digitale a fini investigativi deve intendersi come una catena dove ogni anello è un'azione legata a un istante temporale o ad un arco temporale.

Al termine delle operazioni deve essere documentato ogni singolo passaggio durante la gestione della fonte di prova non ci devono essere fasi non descritte e documentate.

2.3 IL SUPPORTO ORIGINALE E LA COPIA

L'attività di cristallizzazione prevede di fissare in un certo istante lo stato dei dati che dovranno poi essere analizzati.

Tra le migliori pratiche diffuse tra gli operatori di *digital forensics* si segnala quella di effettuare una *bit-stream image* [31] del supporto o dei supporti che si ritengano utili ai fini d'indagine.

[31] Copia clone o immagine bit-per-bit

In pratica si lascia l'originale integro e si effettuano una o più copie identiche all'originale, sulle quali poi condurre le operazioni di informatica forense necessarie.

Nell'ambito del procedimento penale si tratta di un'attività che possa garantire così la ripetibilità degli atti ai sensi dell'art.359 c.p.p. che consente ai vari attori del procedimento di poter intervenire autonomamente sul dato, applicando metodologie proprie all'analisi, mantenendone inalterata l'integrità.

L'identicità di una copia fisica all'originale viene garantita dalla verifica di *hash,* già descritta nei capitoli precedenti, che può essere in qualche modo paragonato al DNA umano.

Qualora fosse impossibile garantire l'inalterabilità del supporto d'origine sarà sempre considerata migliore la pratica della *bit-stream image*, ma dal punto di vista procedimentale durante la fase di copia si agirà ai sensi dell'art. 360 c.p.p. (accertamenti non ripetibili) alla presenza delle parti, mantenendo comunque l'autonomia degli esperti nella fase di analisi.

E' importante riconoscere l'importante differenza tra una copia semplice di dati, ovvero lo spostamento di file da un disco all'altro e una copia clone, ossia la duplicazione di un disco su un disco immagine comprendendo anche tutte le parti vuote e/o nascoste e solo questo tipo di copia permette all'investigatore di avere una fotografia precisa e affidabile del supporto originale.

La copia immagine può essere effettuata utilizzando strumenti di protezione in scrittura hardware detti *write-blocking*[32], o strumenti software (spesso insiti nelle distribuzioni live basate su sistemi Unix per l'analisi informatica forense).

[32] si segnalano Tableu (www.tableu.com), Logicube (www.logicube.com) , Wiebwtech (www.wiebwtech.com), Intelligent Computer Solution (www.ics-iq.com), Voom Tecnologies (www.voomtech.com) MyKeyTechnology (www.mykeytech.com) e Digital Inelligence (www.digitalintelligence.com)

Data la natura del dato digitale una buona copia immagine ai fini dell'analisi, ha lo stesso valore di un nuovo originale.

Ciò consente all'investigatore di avere di fronte un quadro investigativo da analizzare che è identico a quello della scena del crimine ma, al contempo il tecnico è libero di operare modifiche anche invasive, nel tentativo di recuperare i dati.

Un prassi migliore da seguire è quella di fare più copie permettendo così all'investigatore anche esperimenti di hacking distruttivi, dal momento che, in caso di incidenti, potrà continuare l'analisi su altre copie.

2.4 STRUMENTI DI ANALISI PER L'INFORMATICA FORENSE

L'hardware più importante nella valigetta del bravo investigatore informatico è quello che serve a fare le copie-clone di cui si parlava in precedenza e a bloccare in scrittura i supporti per impedire modifiche all'originale.

I primi acquisti di solito effettuati da un esperto sono, quindi, un *write-blocker* e un sistema per effettuare copie, ma spesso alcuni apparecchi hanno queste due funzioni unite.

Le maggiori difficoltà pratiche e i maggiori costi sono rappresentati dall'interfaccia, ossia nella necessità di reperire cavi e strumenti idonei ad acquisire qualsiasi tipo di hardware e disco sul mercato.

Il dispositivo di base utilizzato per mantenere l'integrità dei reperti originali durante l'analisi è rappresentato, si diceva, dal write-blocker: il modello T35u di Tableau (dal 2010 un marchio della Guidance Software), ad esempio, supporta l'acquisizione per le interfacce IDE e SATA e sfrutta la tecnologia USB 3.0 o FIREWIRE 800, che permette una maggiore velocità delle copie forensi.

L'alternativa più economica è rappresentata dall'UltraDock v.5 proposto da un'altra azienda americana, la WiebeTech. Tale modello consente le medesime operazioni a quasi la metà del prezzo. Un breve cenno merita inoltre la serie "Duplicator", sempre della Tableau (il TD3, top della gamma. dispone anche di un monitor touchscreen rivoluzionario), poiché consente la copia del sorgente originale in contemporanea con due unità distinte. Inoltre il Duplicator esegue automaticamente la verifica degli errori presenti sul supporto d'origine, calcola l'hash e produce tutti i log delle operazioni compiute (che successivamente possono essere esportati salvandoli su una chiavetta USB).

Funzionalità analoghe sono garantite da "Forensic Dossier", prodotto dalla Logicube.

Per quanto riguarda i software, fondamentale è, per i sistemi operativi GNU/Linux, il comando dd che, digitato da riga di comando, consente di produrre file di immagine in formato RAW, è uno strumento molto semplice e che richiede risorse minime per la sua esecuzione.

Sempre in ambito open source si segnalano la già citata distribuzione Forlex, Helix e DEFT, che integrano al loro interno diversi tool utili per l'analisi forense.

DEFT, acronimo di Digital Evidence & Forensics Toolkit, è una distribuzione Linux live cd atta ad usi di Computer Forensics; nata nel 2005 per esigenze didattiche legate al corso di Informatica Forense della facoltà di Giurisprudenza dell'Università degli studi di Bologna.

Nel 2006 ha avuto una mutazione nel breve termine che ha portato un cambiamento negli obiettivi finali del progetto trasformandola in un sistema che risponde a pieno alle esigenze dei professionisti del settore.

DEFT è un sistema operativo che usa la memoria RAM del computer per il suo funzionamento pertanto non va ad alterare in alcun modo il contenuto di eventuali dispositivi collegati all'apparato dove lo si sta utilizzando.

Al suo interno sono presenti numerosi strumenti applicativi open source per la computer forensics.

Dal punto di vista degli applicativi commerciali EnCase (sempre prodotte dell'americana Guidance Software) reppresenta sicuramente il software di riferimento.

EnCase include sia tool utili all'acquisizione forense che all'analisi dei file e soprattutto alla generazione di una reportistica dettagliata.

L'alternativa a EnCase è FTK ·Forenrics Toolkit di AccessData, il quale dispone di un intuitivo programma di imaging del disco proprietario denominato "FTK imager".

La questione si complica ulteriormente nell'esecuzione e nei costi qualora i supporti da trattare siano dispositivi mobili quali Smartphone, Tablet o dispositivi digitali portatili.

In questo ambito aumentano a dismisura i tipi di interfaccia per connettere i supporti all'unità di acquisizione, ma anche i software di analisi devono avere la capacità di riconoscere le più svariate architetture di *file system* e tipologie di sistema operativo mobile.

Come termine di paragone si pensi che per un dispositivo di acquisizione hardware per supporti tradizionali (hard disk IDE o SATA, chiavi USB) occorre qualche centinaio di euro, mentre per un dispositivo hardware per l'acquisizione di un dispositivo mobile occorrono diverse migliaia di euro.

3. IL FENOMENO DELLA “DEMATERIALIZZAZIONE”

Per dematerializzazione si intende quel processo di eliminazione del “cartaceo” e di limitazione della produzione di nuovi documenti cartacei, attraverso la creazione di iniziative volte a promuovere la nascita di documenti informatici.

La dematerializzazione costituisce una delle linee di azione più significative per la riduzione della spesa pubblica, in termini sia di risparmi diretti (carta, spazi, ecc.), sia di risparmi indiretti (tempo, efficienza, ecc.) ed è uno dei temi centrali del Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005 n. 82).

Sebbene la percezione diffusa sia che de materializzare significhi sostituire banalmente un documento cartaceo con un documento elettronico, tanto dal punto di vista informatico quanto organizzativo, non rispecchia la complessità degli strumenti che vengono utilizzati e soprattutto non considera il tema della conservazione dei documenti, che ne deve garantire identità e integrità a fini giuridici e storici.

La conservazione del documento digitale è un'operazione complessa e rischiosa. Complessa perché continua nel tempo a fronte di una innumerevole serie di variabili, rischiosa perché ogni intervento finalizzato alla conservazione (copiatura, migrazione, addirittura anche il semplice accesso, etc.) mette intrinsecamente a repentaglio il documento stesso nella sua forma originaria.

Sotto il profilo scientifico, il documento informatico è, al pari del documento cartaceo, una cosa contenente dei segni, cioè una "res signata". Pertanto, essa ha una sua materialità evidente, che anzi gli permette strutturalmente e ontologicamente di essere un documento, proprio in quanto entità materiale.

I documenti sono diventati file, la foto cartacea sta per essere sostituita da quella digitale, le audiocassette sono diventati file MP3, per i messaggi SMS (attualmente superati da sistemi di messaggistica istantanea quali "iMessage", "Whatsapp" e "Viber") e per molti altri beni si sta perdendo il senso del peso e delle dimensioni.

Si pensi alla rapidissima diffusione degli e-book e della stampa on-line che stanno progressivamente cambiando le abitudini di milioni di lettori.

Nessuno mai, ad esempio, avrebbe potuto pensare ad un attacco terroristico condotto attraverso la posta tradizionale, tuttavia la diffusione del batterio dell'antrace attraverso la normale corrispondenza ha destato, non solo la preoccupazione per la vita umana, ma anche portato al collasso del più classico e semplice mezzo di comunicazione.

L'esistenza di precedenti "*proteste cibernetiche*" e la promulgazione di diversi atti legislativi in diverse Nazioni fanno pensare che il terrorismo informatico non è cosa troppo fantasiosa. Forse è ancora presto per un attacco informatico capace di insidiare l'equilibrio, la stabilità e la sicurezza della società civile. Forse i terroristi usano Internet e le reti di comunicazione ancora come "mezzo" di comunicazione e non come "fine" di distruzione

III. IL COMPUTER E IL SISTEMA GIUDIZIARIO

La *computer forensics* attende a due diverse modalità ricostruttive del fatto, la prima della quali (cd. *computer generated-evidence*)[33] postula l'impiego dello strumento informatico ai fini dimostrativi attraverso l'implementazione di simulazioni riproduttive della fattispecie sostanziale, mentre la seconda (cd. *computer derived-evidence*) fa riferimento alla digitalizzazione del dato probatorio[34].

Lo strumento del computer è utilizzato per ricostruire un avvenimento mediante produzioni di immagini oppure è finalizzato all'analisi di dati digitali ricavati attraverso la soluzione di sistemi di equazioni matematiche contenute nel software.

In particolare la *computer generated-evidence* viene utilizzato all'interno della cornice tipica di una prova costituenda quale l'esperimento giudiziale, mentre, nella forma della *computer derived-evidence* esso costituisce il supporto di una prova documentale.

1. IL SISTEMA INFORMATICO NEL SISTEMA GIUDIZIARIO

Tra i molti settori della società nei quali l'uso del *computer* ha rivoluzionato abitudini e potenzialità di sviluppo vi è sicuramente quello riguardante l'amministrazione della giustizia [35].

---

[33] F. SBISÀ, *Cenni sul* computer *come strumento di prova nel processo penale*, in Il Foro ambr., 2000, p. 95.

[34] La partizione della *computer forensics* nelle due categorie della *computer derived-evidence* e *computer generated-evidence* è elaborata da L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 145. La materia verrà approfondita *infra*, Cap. 3, par. 4.

[35] Cfr. K. O' CONNOR, *Computer animations in the courtroom: get with the program,* in *Florida Bar Journal,* 1983, voI. 20, p. 2

Nonostante un'iniziale esitazione all'utilizzo della tecnologia informatica, il *computer* ha incominciato a essere introdotto negli uffici legali e ad essere utilizzato dagli organi deputati all'amministrazione della giustizia principalmente come strumento per la redazione e conservazione degli atti.

In un secondo momento l'uso di tale mezzo ha consentito la creazione di banche dati dalla potenzialità infinita e di semplice e veloce consultazione (agevolando così le ricerche giuridiche sia per gli avvocati che per i magistrati) ; infine, si è affermato quale strumento di illustrazione (nel primo periodo) e di formazione (in seguito allo sviluppo dei criteri di ammissibilità) della prova nelle aule di giustizia [36].

Oggi, infatti, nel sistema processuale statunitense, sia civile che penale, l'utilizzo dei sistemi multimediali viene comunemente adottato ed è principalmente indirizzato alla ricostruzione probatoria di fatti mediante l'utilizzo di specifiche e tassative procedure che derivano da una prassi ormai ampiamente sperimentata e affermata.

Il tipo di ausilio che la tecnologia informatica può fornire cambia a seconda della materia o del caso specifico in cui è necessario il suo uso.

Nel campo civile, dove il *computer* intervenne per la prima volta in una causa per risarcimento dei danni intentata dai familiari delle vittime di un disastro aereo, il suo impiego è legato maggiormente a questioni di brevetti industriali per i casi di concorrenza sleale e violazione del segreto industriale o per i casi di risoluzione del contratto per prodotti realizzati in modo differente da quanto previsto negli accordi o con risultati non sufficienti[37].

---

[36] Cfr. A. Reese, *Forensic animation helps bring cases to life in court,* in La*w Personal Computer, 1991,*vol. l5, p. 1.

[37] Cfr ., ad esempio, il caso *Holland v. Diek Youngberg Chevrok/-Bui4k, lnc.,* 348 N.W. 2D 770, Minnesota Court of Appeal, 1984, dove il convenuto ha dimostrato, attraverso una simulazione, che l'autocarro acquistato dall'attore non era difettoso e poteva raggiungere la velocità di cinquantacinque miglia all'ora a pieno del carico .

In materia penale, il ricorso a tale tecnologia registra una maggiore frequenza in casi di incidenti aerei e automobilistici dove è necessario ricostruire con la maggiore precisione possibile gli eventi ai fini di valutare le singole responsabilità dei soggetti che ad essi hanno dato origine - ma compare anche in casi di omicidio, rapina e aggressione, sempre al fine di ricostruire la dinamica dei fatti.

Tra le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici c'è il cosiddetto "esperimento giudiziale" virtuale in cui si impiega il computer per riprodurre un fatto tramite attraverso la realtà virtuale tanto che si parla di "computer generated evidence"[38] nel processo penale.

Il continuo evolversi delle capacità tecniche dei sistemi informatici e la loro applicazione in sede processuale ha consentito di ottenere evidenti vantaggi sia in termini di chiarezza espositiva e illustrativa (riguardo all'audizione di un consulente tecnico o alle conclusioni finali delle parti), sia in termini di compressione dei tempi processuali, oltreché di formazione della prova.

A tali fini nelle aule penali il *computer* è utilizzato per casi che richiedono la soluzione di questioni riguardanti i movimenti dei corpi nello spazio e la loro visualizzazione prospettica[39], ma ovviamente anche per spiegare cosa è successo durante l'utilizzo di uno strumento tecnologico, cioè temi fondamentali sia in fase di elaborazione delle conclusioni dei consulenti tecnici, che in fase di descrizione e comprensione delle stesse[40].

---

[38] Cf. P.Tonini, Manuale di procedura penale, Giuffré, 2010, p.320

[39] Cfr. E.M. Chaney *Computer simulations: how they can be used at trial and tbe argument for admissibility,* in *Indiana Law Review*, 1986, voI. 19, p. 735.

[40] SuI punto cfr., E.A. HANNAN, *Computer* general *evidence: testing. tbe envelope,* in *Defense Counsel }ournal,}u1y,* 1996, vol. 63, p. 356, in cui sono state individuate le specifiche ipotesi in cui l'uso delle *computer general evidence* assume un'estrema utilità: .. quando la visualizzazione di un evento , oggetto o condizione è resa complessa per la presenza di fattori dinamici che possono difficilmente essere spiegati verbalmente; quando assume rilevanza il tempo di realizzazione dell 'evento; quando la ricreazione dell'evento nella realtà fisica è impossibile o di difficile attuazione; quando l'evento o il principio che deve re spiegato dipende da fattori che rendono la materia troppo

L'utilizzo degli elaboratori elettronici è quindi nato dall'esigenza di efficienza e celerità del sistema giudiziario ed è divenuto strumento per garantire affidabilità e comprensibilità della prova.

Nel processo penale la funzione probatoria di questa tecnologia consiste nel ricostruire l'accadimento di un fatto sulla base dei dati reali ricavati dalle indagini o comunque noti.

Il *computer* può essere utilizzato per ricostruire un fatto mediante l'analisi di dati e l'elaborazione di conclusioni attraverso la soluzione di sistemi di equazioni matematiche contenute nel *software.*

Per scoprire le utenze telefoniche dei brigatisti rossi che uccisero il Prof. Marco Biagi furono analizzati i traffici delle celle BTS[41] agganciate dai telefoni cellulari nei mesi precedenti all'omicidio con l'ausilio di potenti computer e software specifici correlando funzioni matematiche e formule statistiche con spunti investigativi.

L'uso di tali strumenti, oltre a fornire un'immediata percezione da parte del giudice e della giuria delle spiegazioni fornite - con ciò semplificando i problemi di esposizione, di apprendimento, di comprensione e di ricostruzione complessiva e organica dei dati forniti, che altrimenti si devono ottenere con laboriose testimonianze, consulenze tecniche, perizie, ispezioni, etc. - , offre altri vantaggi ancora più rilevanti.

In primo luogo, il *computer* è in grado di supplire alla mancanza di taluni dati, ottenendoli con rigore oggettivo e al riparo da errori soggettivi mediante calcoli basati su leggi scientifiche; in secondo luogo, abbrevia i tempi dell'accertamento, in

---

complessa per una esposizione orale ; quando è necessario illustrare l'evento secondo diverse prospettive al fine di ottenere una chiara ed esaustiva spiegazione delle conclusioni dell'esperto.

[41] stazione radio base, in sigla BTS (del corrispondente termine inglese "base transceiver station"), indica il sottosistema di ricetrasmissione di un segnale radio dotato di antenna ricetrasmittente che serve i terminali mobili di utente coprendo una determinata area geografica detta appunto *cella radio*.

quanto, grazie all'enorme potenza di calcolo delle macchine moderne, ottiene in un tempo molto ridotto gli stessi risultati che gli esperti sarebbero in grado di ottenere solo dopo mesi di calcoli; in terzo luogo, nel caso specifico delle ricostruzioni, diviene indispensabile quando sarebbe troppo costoso o pericoloso ottenere il medesimo risultato nella realtà fisica anziché nella realtà virtuale.

1.1. ANIMAZIONE, RICOSTRUZIONE E SIMULAZIONE.

Nel campo processuale l'utilizzo dei sistemi di *software* persegue il fine di illustrare, ricostruire o simulare un evento di cui si devono individuare le cause o le fasi di svolgimento; il risultato di tale attività si concretizza nelle *computer generated evidence.*

Tale locuzione si riferisce ad ogni tipo di prova che sia ottenuta mediante l'uso del *computer,* ma racchiude in sé, a seconda dell'utilizzo che deve esserne fatto, tre diverse categorie: *l'animazione,* la *ricostruzione* e la *simulazione.*

Questa ripartizione serve a regolarne l'utilizzabilità nel processo, in quanto per ognuna di esse viene fissato un ambito di impiego e, di conseguenza, sono stabiliti dei criteri per fissarne i limiti di ammissibilità in sede processuale e per valutare l'affidabilità della relativa procedura di realizzazione.

L'animazione consiste in un filmato bi-dimensionale formato da una serie di immagini create dal *computer* e registrate in rapida successione su un videoregistratore così da creare l'illusione del movimento; può quindi includere sintesi di immagini, testi e suoni così da offrire un sussidio visivo che permetta di illustrare e dimostrare concetti indescrivibili con immagini ferme.

In altre parole, rappresenta la fase conclusiva della ricostruzione di un fatto ottenuta con altri mezzi di prova, utile per una più facile e immediata rappresentazione e

comprensione della elaborazione stessa; il suo è, dunque, un ruolo di mero ausilio illustrativo di una conclusione ottenuta con altri mezzi probatori.

Quanto alla *ricostruzione* e alla *simulazione,* va premesso che comunemente questi termini sono usati intercambiabilmente in quanto, pur costituendo due sviluppi differenti della animazione scientifica, possono essere utilizzati congiuntamente nell'ambito di un medesimo caso.

L'esperienza statunitense mostra infatti come la *ricostruzione-simulazione* di un fatto mediante *computer* non sia altro che una medesima attività praticata in due opposte direzioni: ricostruire un evento per evidenziare come sia realmente accaduto; ipotizzare una modificazione dell'evento in conseguenza dell'intervento di alcune variabili o dimostrare che anche con tale inserimento di variabili l'evento rimane il medesimo.

In primo luogo, con la *ricostruzione* di un fatto si può puntare a dimostrare ciò che è realmente accaduto, utilizzando dati che sono tratti dalle indagini sul fatto analizzato.

Tali dati, che riportano le misurazioni reali riguardanti forma, misura, massa, proprietà fisiche e meccaniche di un oggetto (ad esempio del veicolo coinvolto in un caso automobilistico), sono elaborati attraverso formule scientifiche e mediante il programma vengono simultaneamente tradotti in immagini tridimensionali fatte muovere secondo le leggi della meccanica e della fisica.

La *simulazione*[42] è, invece, l'estrapolazione di un evento creata artificialmente. Avvalendosi dei dati fattuali conosciuti - espressi in termini matematici - si può ulteriormente sviluppare la rappresentazione di un accadimento oltre la sua base

[42] Cfr. M.J. ENKE, *Admissibility of computer-generated animated reconstruaion,* cit., p. 436.

fattuale o matematica, al fine di dimostrare ciò che sarebbe successo in condizioni diverse.

Per la creazione delle *computer generated evidence* vengono impiegate formule di leggi scientifiche (chimiche, fisiche, matematiche ecc.) e, attraverso le leggi proprie del ragionamento induttivo e del metodo scientifico, viene ricavato il risultato ricostruttivo e rappresentato in un'immagine completa e animata.

II *computer* è, quindi, utilizzato per analizzare i dati immessi dall'operatore e per produrre delle conclusioni basate sul *software* adottato.

Il risultato di tale attività assume forma (animazione, ricostruzione o simulazione) e valore *(demonstrative* o *substantive evidence)* differente a seconda dello scopo che viene perseguito, caso per caso, dalle parti processuali.

È quindi compito della parte che intende usufruire di tali tecnologie individuare quale sia la categoria entro cui le stesse devono essere racchiuse; tale scelta dovrà quindi riflettere l'obiettivo che il richiedente intende realizzare.

1.2. LA REALIZZAZIONE

II processo preparatorio rappresenta il nucleo fondamentale dell'utilizzo delle *computer generated evidence,* in quanto il relativo giudizio di affidabilità, ai fini del loro utilizzo in sede giudiziaria, dipende dalla sua verifica.

A seconda dei casi è possibile identificare due differenti scopi cui è diretto l'utilizzo di tali mezzi in sede processuale. Da un lato, *l'animazione* e la *ricostruzione* possono servire ad illustrare la testimonianza dell'esperto; nella prima ipotesi *l'animazione* permette di rendere visibile ciò che dall'esperto viene riferito oralmente, nel secondo caso la *ricostruzione* traduce in immagini il risultato della elaborazione dei dati oggettivi emersi dalle indagini relative a un determinato evento.

In entrambe le ipotesi l'obbiettivo è di rendere più facile ed immediata la percezione e la comprensione di ciò che viene riferito dall'esperto; in entrambi i casi ciò che costituisce prova ai fini della valutazione del giudice o della giuria è esclusivamente la testimonianza dell'esperto.

Diverso è il discorso relativo alla *ricostruzione-simulazione*; in questo caso viene ricreato un evento - che nella pane simulativa viene riprodotto secondo diverse ipotesi ricostruttive - attraverso l'elaborazione dei dati fattuali immessi nello specifico programma; il *computer* - mediante il ricorso all'applicazione di leggi scientifiche e principi matematici - può supplire alla mancanza di alcuni dati attraverso la propria elaborazione di quelli emergenti dalle indagini. In tal caso i predetti strumenti probatori non costituiscono più solo il mezzo per illustrare l'opinione dell'esperto ma divengono, essi stessi, l'elemento di base su cui l'esperto costruisce la propria opinione.

Ai fini di regolare l'ammissione di tali mezzi di prova le Corti statunitensi hanno consolidato il principio secondo cui il dato di riferimento è la tipologia di apporto che la parte richiedente assegna al singolo strumento: quando è prettamente illustrativo lo stesso può rientrare esclusivamente nella categoria delle c.d. *demonstrative evidence;* altrimenti, se viene offerto con una valenza probatoria indipendente dalla deposizione dell'esperto, il quale viene chiamato a illustrare le caratteristiche del sistema adottato e a riferire sulle procedure osservate nella realizzazione del risultato finale che viene mostrato in dibattimento, esso assurge alla categoria delle *substantive evidence.*

È evidente che chiedendone l'ammissione come *demonstrative evidence* se, da un lato, ne viene ridotta la valenza probatoria, dall'altro viene semplificata la verifica che deve essere superata ai fini dell'ammissione come mezzo di prova nel dibattimento.

Quanto alla sola *simulazione,* che indubbiamente rappresenta la tipologia più evoluta tra quelle osservate, va rilevato come il suo utilizzo e la sua classificazione abbiano subito una triplice progressione.

Inizialmente essa ha costituito esclusivamente la base per i pareri che gli esperti erano chiamati a rendere nei processi, ma il relativo uso quale strumento processuale non era contemplato.

Successivamente è stata utilizzata per corredare la deposizione resa dall'esperto giungendo ad essere classificata nella categoria delle c.d. *Demonstrative evidence;* quindi, ancora senza un valore probatorio autonomo.

A seguito della continua evoluzione scientifica e, grazie a questa, della accertata e diffusa affidabilità dei sistemi informatici utilizzati, la *simulazione* è oggi utilizzata anche come autonomo mezzo di prova: in tal caso è classificata come *substantive evidence*[43].

2. LE COMPUTER GENERATED EVIDENCE NEL PROCESSO PENALE STATUNITENSE.

In questo paragrafo verranno illustrate sinteticamente le regole poste dal sistema giudiziario statunitense all'utilizzo della *computer generated evidence* nel processo e

[43] L'uso della simulazione ribalta il procedimento logico attraverso cui l'esperto giunge alla conclusione dato che quest'ultimo ~ può inserire nel computer una serie di variabili oltre ai dati conosciuti al fine di testare differenti ipotesi ricostruttive. Pertanto è sulla base del risultato ottenuto dalla elaborazione del programma, che l'esperto è in grado di costruirsi un opinione sul caso specifico, cfr. E.A. HANNAN, Computer generated evidence; cit., p. 355.

come queste tendano a conciliare l'esigenza di diffondere l'utilizzo di tale strumento probatorio con il rispetto delle garanzie e dei ruoli delle parti processuali.

2.1. L'AMMISSIBILITÀ NEL DIBATTIMENTO

La diffusione dell'utilizzo delle *computer generated evidence* nel processo penale ha comportato l'esigenza di regolarne l'ammissibilità attraverso la creazione di specifici e tassativi criteri che devono essere osservati a seconda della valenza probatoria con cui tale prova scientifico-tecnica viene proposta.

Nel caso in cui sia proposta come *demonstrative evidence* i requisiti per l'ammissibilità sono maggiormente incentrati sulla sua rilevanza; nel caso in cui è richiesta quale *substantive evidence* gli stessi diventano più severi e sono diretti maggiormente alla autenticazione della procedura attraverso cui è stato ottenuto il risultato probatorio di cui si chiede l'ammissione.

In sintesi, se il richiedente intende utilizzare la *computer generated evidence* solo per illustrare l'ipotesi sorretta dall'esperto ma non dimostrarne (attraverso il mezzo scientifico di cui chiede l'utilizzo) la veridicità , deve essere solo accertato che l'utilizzo di tale strumento probatorio permetterà alla giuria di comprendere con più facilità e immediatezza la teoria esposta dall'esperto.

Se, invece, il richiedente vuole utilizzare il mezzo scientifico quale strumento di formazione della prova , deve ottenerne l'autenticazione, vale a dire l'esperto deve testimoniare sulla sua affidabilità e sulla natura e precisione di procedimento utilizzato per l'ottenimento del risultato finale di cui si chiede l'ammissione come prova .

Il tema dei criteri di ammissibilità e di affidabilità ha assunto particolare interesse con riguardo alla *ricostruzione-simulazione* nel momento in cui la stessa è stata

riconosciuta come prova scientifico-tecnica autonoma, in quanto le Corti per controbilanciarne la rilevante valenza probatoria sono divenute più severe nella previsione dei relativi standard di ammissibilità.

Tale tema, che si è giovato dell'elaborazione giurisprudenziale e dottrinaria avutasi nell'arco di decenni sul più generale campo della prova scientifica, ponendo problemi particolari per il suo apprezzamento nell'ambito del processo causa l'elevata componente tecnico-scientifica, ha fondato la propria regolamentazione sul disposto normativo contenuto nelle *Federal Rules of evidence.*

2.2 LE FEDERAL RULES OF EVIDENCE.

Sul piano normativo, secondo le regole federali devono essere verificate tre fondamentali condizioni: rilevanza logica, autenticità e rilevanza giuridica della *computer generated evidence.*

Quanto alla rilevanza logica (che corrisponde alla nostra nozione di pertinenza) le regole nn. 401 e 402 delle *Federal Rules of Evidence* stabiliscono che è sufficiente dimostrare che la prova richiesta sia attinente a ciò che deve essere dimostrato. Secondo tali regole deve essere valutato se l'elemento di cui si chiede l'utilizzazione come mezzo di prova (quindi nella forma della *ricostruzione-simulazione)* possiede secondo la logica giuridica il sufficiente valore probatorio per giustificarne l'ammissione al dibattimento[44], vale a dire se il dubbio circa la sussistenza o meno di un fatto possa trovare una più probabile soluzione mediante quella prova piuttosto che senza la sua ammissione.

[44] Cfr . Il commento alla regola n. 401 in cui sono riportati i lavori preparatori che contengono tale definizione di relevancy, in Federal Criminal Code and Rules, 1998, Rule of Evidence, Relevancy, Artide IV, Rule 401, 242.

Tale requisito deve essere soddisfatto anche attraverso la verifica dell'autenticazione della prova di cui si chiede l'ammissione.

La regola n. 901 indica vari metodi per stabilire l'autenticità (che corrisponde alla nostra nozione di veridicità - attendibilità) della prova tecnico-scientifica, ma relativamente alla *computer generated evidence* deve essere richiamata la regola 901 (b), secondo cui la prova può essere autenticata se si « descrive il processo o il sistema usato per produrre il risultato e dimostrando che quel processo o sistema produce un determinato risultato » .

A tale scopo la parte richiedente ha quindi l'obbligo di:

1) qualificare colui che ha realizzato la *computer generated evidence* come esperto nella materia producendo il suo curriculum e le precedenti esperienze nella specifica materia;

2) dimostrare che il programma utilizzato al fine di realizzare la *computer generated evidence* sia riconosciuto e accettato dalla comunità scientifica;

3) dimostrare, e questa è la fase più complessa, l'attendibilità e la precisione della procedura di immissione dei dati nonché la individuazione e selezione dei dati che sono stati inseriti nel programma per la realizzazione della *computer generated evidence;*

4) dimostrare l'attendibilità e la correttezza del risultato finale attraverso la verifica dei calcoli compiuti dal programma utilizzato;

5) infine dimostrare che il risultato finale mostrato alla giuria non possa essere soggetto a distorsioni nel momento in cui viene esposto in aula.

Vi è poi, in osservanza del principio della parità delle parti nel dibattimento, un ultimo onere assegnato al richiedente; deve essere infatti dimostrato che tutti gli

elementi esposti al giudice ai fini dell'autenticazione della prova di cui si chiede l'ammissione siano stati resi noti, con un congruo termine, alla controparte in modo che la stessa abbia avuto la possibilità di controdedurre in merito.

Non solo, deve anche essere osservato il principio secondo cui a tutte le parti processuali deve essere concessa pari opportunità per svolgere la propria difesa e, quindi, il giudice ha l'onere di verificare se anche chi non ne abbia le possibilità economiche possa usufruire di tale strumento probatorio o comunque non subisca un palese indebolimento della propria posizione processuale nel caso in cui non lo faccia.

Inoltre, quanto alla rilevanza giuridica (che corrisponde alla nostra nozione di utilità - non superfluità) la regola n. 403, più che individuare i requisiti di utilità della prova, stabilisce che deve essere evitato che la stessa possa costituire motivo di confusione o incomprensione dei fatti da parte della giuria; in sintesi deve essere verificato che non ostacoli il corretto giudizio che l'organo popolare è chiamato a esprimere.

A tal fine sono stati individuati una serie di effetti pregiudizievoli collegati all'ammissione di una *computer generated evidence* sulla sussistenza dei quali il giudice può basare il rifiuto dell'ammissione della prova. Risolta la verifica di tali problematiche può essere confermata la rilevanza della prova e quindi ne può essere disposta l'ammissione.

II lavoro compiuto dalla Commissione può essere così sintetizzato. In primo luogo, nell'ambito delle nuove regole viene nuovamente specificata la differenza tra ricostruzione-simulazione e animazione: con la prima si giunge ad una conclusione che permette di mostrare come l'evento di cui si discute si è realizzato, mentre con la

seconda non viene offerta alcuna opinione ma ci si limita a illustrare una conclusione che da altri, e con differenti strumenti, è stata raggiunta. Ma i due punti più rilevanti sono quelli relativi alla tutela del diritto di parità delle parti e del contraddittorio. Quanto a quest'ultimo, viene infatti stabilito che la parte che intende utilizzare questo tipo di strumento probatorio nel dibattimento ha l'obbligo di darne comunicazione scritta alle controparti e di mettere a disposizione delle stesse tutti i dati riguardanti la prova di cui si chiede l'ammissione. Le controparti hanno, quindi , sessanta giorni di tempo per decidere se opporsi , o meno, all'ammissione della prova richiesta. Quanto invece al principio di parità delle parti, se vi è un soggetto processuale che non ha le possibilità di assumere un esperto, è previsto che lo stesso possa essere nominato dalla Corte.

Grande attenzione è stata posta alla fase di presentazione della prova, con l'indicazione di specifici obblighi in capo al proponente che permettano alle altre parti di interloquire concretamente in merito all'utilizzabilità della prova richiesta. Peculiare è poi la disciplina della udienza prevista in caso di opposizione all'utilizzo della prova, dato che prevede ampi poteri del giudice sia in termini modificativi che limitativi dell'uso che della prova potrà poi essere fatto in dibattimento. Infine, non si può non sottolineare come la previsione della trasmissibilità dello strumento di prova nella sua materialità alla Corte d'Appello conferisca alla sua valutazione di ammissibilità un valore assolutamente preminente, dato che si ammette, implicitamente, che eventuali violazioni processuali relative a tale profilo potranno essere oggetto di giudizio delle Corti superiori.

2.3 GLI STANDARDS OF ADMISSIBILITY.

La giurisprudenza ha regolato l'ammissibilità delle *computer generated evidence* rifacendosi, principalmente, ai fondamentali *leading cases* trattati in tema di testimonianza scientifica (c.d. *Scientific testimony)*, con cui sono stati creati gli *standards* per l'ammissibilità delle prove scientifico-tecniche, che hanno trovato applicazione analogica anche in relazione alle *computer generated evidence.* Le Corti però, già prima della pronuncia *Daubert,* si sono trovate ad affrontare casi specifici che non potevano essere risolti solo sulla base dello *standard* individuato nel caso *Frye;* quindi, ne hanno elaborato il contenuto adattandolo alle specifiche situazioni di volta in volta affrontate.

Riguardo ai temi generali quali l'autenticità della prova e la possibile influenzabilità della giuria è evidente che abbiano assunto analoga rilevanza sia i giudizi civili che quelli penali , dato che vi è stato un notevole sforzo comune della giurisprudenza per individuare in maniera sempre più appropriata e specifica i requisiti da osservare nella valutazione delle prove scientifico tecniche e, in seguito alla loro evoluzione, anche delle *computer generated evidence.*

Con riferimento, più specifico, al processo penale, il caso *People v. Mc Hugh* - sempre precedente alla pronuncia *Daubert,* cosicché i giudici si sono indirizzati allo *standard* stabilito nel caso *Frye* – nel quale per la prima volta la *computer generated evidence* nella forma della *simulazione* ha assunto valore di prova tanto da costituire il principale degli elementi probatori su cui si è fondato il giudizio di assoluzione.

La vasta elaborazione della giurisprudenza statunitense e il successivo sforzo legislativo in precedenza richiamato sono il frutto dello svilupparsi, del diffondersi e dell'ormai generalizzata sperimentazione e accettazione delle *computer generated*

evidence come strumento avente la capacità di ricostruire fatti storici e quindi idoneo ad essere utilizzato come mezzo di prova nel processo.

Di queste la *simulazione* ha ormai attinto un tale livello di generale affidabilità da essere per l'appunto adottata costantemente nella prassi delle Corti americane come prova scientifico-tecnica. L'evoluzione della tecnologia ha consentito di riconoscere a questo strumento probatorio il valore di *substantive evidence,* cioè di mezzo di prova autonomamente idoneo, mediante l'elaborazione di dati fattuali ricavati dalle indagini, ad accertare le modalità di accadimento di un fatto.

Ciò non toglie che l'attenzione dei giudici è sempre indirizzata non solo alla verifica dell'attendibilità dello strumento tecnologico e all'affidabilità del metodo utilizzato per l'ottenimento del risultato proposto alla loro attenzione, ma anche al rispetto del diritto al contraddittorio già in fase di ammissione della prova nonché della parità delle parti con riguardo all'effettiva possibilità di addivenire alla scelta di utilizzare tale strumento di prova.

Infatti, se da un lato le suddette prove possono dare luogo a complesse questioni con riguardo alla loro corretta natura o classificazione, dall'altro lato possono essere fonte di confusione per la giuria in merito al valore di ciò che rappresentano (creare una falsa convinzione rispetto al fatto che ciò che mostrano è reale o ipotetico); possono, inoltre, determinare una posizione di sfavore nei confronti della parte che non è in condizioni di usufruirne; possono, infine, essere oggetto di manipolazione e, quindi, di travisamento dei fatti.

Più nello specifico è noto come la classificazione della prova come scientifico-tecnica imponga una valutazione che non sempre può essere alla portata del giudice, dato

che richiede una valutazione altamente specializzata di cui il giudice non può essere portatore.

Ma anche nel caso in cui il giudice riesca a pervenire a un giudizio sulla scientificità dello strumento probatorio offerto, si può spesso creare l'equivoco di ritenere i concetti di validità scientifica e ammissibilità come equipollenti.

Non sempre, infatti, la validità scientifica di un metodo o di una tecnologia ne giustificano l'ammissione in ambito giudiziario perché ciò che assume rilievo è anche la valutazione della metodologia che è posta a fondamento dell'utilizzo dello strumento probatorio nonché lo scopo per cui tale strumento viene utilizzato.

Ad esempio, anche in presenza di una tecnologia o di uno strumento comunemente riconosciuto come affidabile può essere raggiunto un risultato scorretto nel caso in cui venga applicato un metodo errato o fondato su dati sbagliati. Inoltre, può accadere che l'evoluzione di una tecnologia già ampiamente utilizzata in ambito forense, pur presentando caratteristiche differenti e innovative dalla precedente - che, pertanto, dovrebbero essere sottoposte a un nuovo e più severo vaglio -, ottenga un'immediata diffusione in ambito forense anche al di là della propria reale affidabilità.

Infine, deve essere verificata la comprensibilità e la credibilità dello strumento e della metodologia scientifica proposta, dato che una decisione fondata su una prova di cui alle parti sfugge la comprensione risulta, inevitabilmente, inficiata alla propria base.

La valutazione che il giudice deve compiere è, quindi, duplice: prima deve *verificare la validità e l'accuratezza dei metodi utilizzati per la creazione della* prova e poi deve verificare la rilevanza e l'affidabilità del risultato presentato come prova, non senza tralasciarne la comprensibilità e credibilità.

Decisioni che, comportano conoscenze tecniche specifiche e, quindi, richiedono l'intervento degli esperti, ma che, proprio per l'altrettanto elevato connotato giuridico che le caratterizza , non possono che provenire dal giudice.

L'esigenza è, quindi, di dare al giudice gli strumenti per compiere tale valutazione, ma anche alle parti quelli per poter effettuare un controllo sul suo operato.

La soluzione è quella, già intrapresa dalla giurisprudenza e poi tentata dal legislatore, di creare criteri e procedure di valutazione sempre più specifici in modo da "guidare" l'attività del giudice e, nel contempo, delimitarne l'ambito di discrezionalità per ottenere una più diffusa uniformità.

Riguardo alla giuria (o al giudice laddove la decisione sulla colpevolezza o meno dell'imputato sia assunta da quest'ultimo) il problema dell'utilizzo delle *computer generated evidence* assume rilevanza in un momento successivo alla fase della loro ammissione, vale a dire assume rilievo nella fase della loro valutazione ai fini della emissione del verdetto.

Generalmente, rispetto alla prova scientifico-tecnica, si crea quello che nella letteratura nordamericana viene definito come il "*paradox of nonscientist judges and jurors deciding disputes about science*".

Così come il "nostrano" paradosso di Carnelutti definisce che nel valutare le conclusioni raggiunte dall'esperto, il giudice deve esprimersi su qualche cosa che, chiamando in giudizio lo stesso esperto, ha appena confessato di non conoscere.

Tali paradossi, a cui si aggiunge il fatto che notoriamente i giurati sono facilmente influenzabili e decidono anche in modo irrazionale senza offrire alcuna garanzia rispetto all'emissione di un verdetto ragionevolmente fondato, in genere si rafforza di fronte a una prova scientifica dato che i predetti difetti riguardano la valutazione

di dati, formule scientifiche e strumenti in relazione ai quali può sussistere nell'inconscio della giuria la possibile presunzione di infallibilità di ciò che viene presentato.

E evidente che la visione da parte del giurato di *un'animazione,* di una *ricostruzione* o di una *simulazione* che abbiano valore *demonstrative* possa essere, invece, ben più convincente e rimanere più facilmente impressa rispetto a un'altra prova, ad esempio la testimonianza, che abbia, però, valore *substantive.*

In tal caso si può, cioè, arrivare a uno stravolgimento del valore delle prove, che assumono una diversa valenza non nel rispetto delle regole processuali, ma solo in dipendenza della forma mediante la quale le stesse sono formate nel dibattimento.

Davanti all'utilizzo di una *computer generated evidence* il giurato, cioè, non solo deve affrontare l'indubbio impatto che una presentazione visiva opera, ma deve confrontarsi anche con la presunzione di credibilità ed aderenza alla realtà che accompagna ciò che viene rappresentato mediante lo strumento informatico.

IV. LA CONSERVAZIONE DEI DATI E IL CODICE PER LA PROTEZIONE DEI DATI PERSONALI

1. LA CONSERVAZIONE DEL DATO

E' necessario adottare strumenti d'indagine, utili alla difesa della sicurezza collettiva, bilanciando la necessità della conservazione del dato con la tutela dei dati personali dei cittadini.

Questi valori costituzionalmente rilevanti trovano, in relazione al periodo storico e all'orientamento della società, dei punti di equilibrio diversi a seconda dei casi.

Il dibattito su tale equilibrio si sviluppa all'interno della classe politica, della magistratura, nel settore delle telecomunicazioni, tra i tecnici e i tutti soggetti della società civile.

Chiunque di questi interagisca nella società o in sedi istituzionali[45], determina la disciplina della archiviazione dei dati sul traffico attraverso il confronto ed le eventuali pressioni, anche presso le istituzioni sovranazionali.

Le tecniche e le modalità di conservazione e di indagine sui dati riguardanti il traffico e la consapevolezza sulla loro reale invasività aiuteranno nell'orientarsi rispetto a questo annoso dibattito, il quale rimane destinato rideterminare nel tempo il suo punto di equilibrio.

La conservazione dei dati riguardanti le comunicazioni private (telefoniche o telematiche) costituisce un importante sostegno per lo svolgimento di indagini riguardanti diversi crimini.

[45] Come è avvenuto ad esempio nelle audizioni informali presso le commissione giustizia della camera o nel del gruppo interministeriale per la sicurezza delle reti e le intercettazioni telefoniche

Per alcuni esperti, inoltre, in assenza di dettagliate specifiche tecniche, rimane aperto anche il problema della scindibilità dei meri dati sul traffico (file di log) dai contenuti delle e-mail.

Pietro Saviotti, pubblico ministero impegnato nelle indagini sulle nuove Br, ex-consulente del ministero della giustizia[46] e specialista in reati telematici presso la procura di Roma, ricorda che solo a tre anni dal delitto D'Antona sono state individuate le utenze rilevanti per stringere il cerchio attorno ai presunti brigatisti Broccatelli, Proietti, Mezzasalma, Banelli, Morandi e Costa. "Se le società di telefonia avessero cancellato quei dati, l'indagine non sarebbe stata possibile", ha affermato Saviotti a poche ora dalla votazione del decreto in Consiglio dei ministri.

Bisogna dare atto che i dati che permisero ai magistrati romani di lavorare sulle rivendicazioni del delitto Biagi e della bomba a via Brunetti sono stati proprio il mittente, il destinatario, l'ora e la durata della comunicazione, l'utenza telefonica, il sistema operativo usato per e il tipo di connessione.

Saviotti riteneva che fosse preminente rendere sicura la conservazione dei dati.

Le soluzioni di conservazione dei file di log consentono di estrarre solo le informazioni di interesse, che includono: il *timestamp*, cioè ora e data dell'evento, l'indirizzo IP cui era attestato il cliente nell' effettuare l'operazione e gli indirizzi di mittente e destinatari delle e-mail.

I contenuti dei messaggi di posta vengono invece regolarmente archiviati su supporto un fisico temporaneo, a solo fine di back-up.

[46] All'interno del gruppo interministeriale per la sicurezza delle reti e le intercettazioni telefoniche

Ciò avviene su sistemi fisicamente separati, per il ripristino dei dati in caso di danneggiamento o perdita e non a fini di ricerca.

L'inscindibilità dei dati dal contenuto è una questione ancora aperta, ma, secondo alcuni Internet Service Provider, la legge costringe sicuramente ad investimenti in termini tecnici e di risorse umane molto elevati.

Maggiori costi discenderebbero dall'eventuale obbligo di conservazione di dati sulle community dei portali.

2. GLI INDIRIZZI GIURISPRUDENZIALI E IL CODICE DELLA PRIVACY

La localizzazione mediante sistema satellitare (GPS) degli spostamenti di una persona indagata è stata considerata non soggetta ad autorizzazione preventiva da parte del giudice per le indagini preliminari, e nemmeno del pubblico ministero, in quanto rappresenterebbe una sorta di pedinamento a distanza , non assimilabile all'attività di intercettazione di conversazioni o comunicazioni, pur se realizzato con modalità e tecnologie similari, e sarebbe compreso tra i mezzi atipici di ricerca della prova attribuiti alla competenza della polizia giudiziaria[47].

Anche il c.d. "tracciamento delle comunicazioni", consistente nel sottoporre a controllo l'utenza intercettata per rilevarne gli spostamenti nello spazio è stato ridotto dalla giurisprudenza a mero accertamento di fatto, riconducibile alla generica attività di assicurazione delle fonti di prova ed esperibile anche di propria iniziativa dalla polizia giudiziaria[48].

[47] Cass., sez. V, 10 marzo 2010, Zenele , in Guida dir., 2010 , n. 16, p. 95; Cass., sez. IV, 29 gennaio 2007, Navarro, in Giur. it., 2007, p. 2549; Cass., sez. V, 7 maggio 2004, M., in Cess. pen., 2005, p. 3036; Cass., sez. V, 2 maggio 2002, Bresciani , in Dir. pen. proc., 2003, p. 93.
[48] Cass., sez. II, 24 ottobre 1998, Gurrieri, 1999, p. 1687

Queste interpretazioni, tuttavia , non tengono minimamente conto di quanto dispone l'art. 126 del Codice della *privacy,* il quale prescrive che «i dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso , revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto».

Solo, dunque, se tale consenso sia stato prestato, l'autorità giudiziaria può richiedere al gestore del pubblico servizio di telecomunicazioni di effettuare per il futuro il "tracciamento" dell'utenza, verificandone gli spostamenti sul territorio, ai sensi dell'art. 132 stesso Codice[49], che ha risolto in via normativa il problema dell'acquisizione dei tabulati di flussi telematici, subordinandola, per qualsiasi reato e in assenza di qualsivoglia *standard* probatorio, ad un decreto motivato del pubblico ministero per i dati risalenti agli ultimi dodici mesi (il termine è aumentato a ventiquattro mesi per i dati relativi al traffico telefonico e ridotto a trenta giorni per le chiamate senza risposta), emesso anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private: al difensore dell'imputato o della persona sottoposta alle indagini è riconosciuto un autonomo potere di richiedere direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito, con le modalità indicate nell'art . *391-quater* c.p.p., ferma restando, per il traffico entrante, la condizione che possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive.

[49] L'art . 132 ha subito altalenanti modifiche, in senso repressivo garantista, le ultime delle quali sono state introdotte dagli artt. 2 e 10 del d.lgs. 30 maggio2008, n. 109: sulla successione delle disposizioni si veda la pregevole ricostruzione critica di C. Conti, *Attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova,* in AA.VV., *Le nuove norme sulla sicurezza pubblica,* a cura di S. Lorusso, Padova, 2008, pp. 6 ss. e 14 ss.

La Corte di Cassazione ha ritenuto utilizzabili senza necessità del decreto di autorizzazione del giudice per le indagini preliminari i dati segnalati sul *display* di un apparecchio di telefonia mobile, poiché tali elementi non sarebbero assimilabili al contenuto di conversazioni o comunicazioni telefoniche e l'acquisizione del cellulare rientrerebbe tra gli atti urgenti di polizia giudiziaria:

La Corte di Cassazione ha pure affermato essere acquisibile ai sensi dell'art. 234 c.p.p. il frutto della stampa di *files* di un *computer,* in quanto la norma ricomprende genericamente nella nozione di documento tutto ciò che è caratterizzato dal requisito della scrittura e, dunque, anche la riproduzione su carta (stampa) del *file* del *computer,* rappresentativo del fatto di annotazione eseguita dall'operatore.

E da ciò è desumibile che i medesimi principi dovrebbero essere applicabili anche alla lettura di messaggi telefonici, scritti (cosiddetti SMS, cioè *short messaging system)* o visivi (cosiddetti MMS, cioè *multimedial messaging system),* e di posta elettronica, scaricabili da telefoni o computer.

Relativamente a queste ipotesi, lungi dal potersi configurare una prova documentale o atipica , la disciplina di siffatti rilevamenti deve essere ricondotta alla normativa dettata dagli artt. 121, 126 e 132 del Codice della *privacy,* prima citati, che, in assonanza con la previsione dell'art. 15 Cost., consentono l'acquisizione dei dati in esame, specie se si tratta di messaggi o di posta elettronica o se riferibili alle chiamate in entrata e in uscita (assimilabili in tutto ai tabulati conservati dagli enti gestori dei servizi di telefonia), ad un preventivo atto motivato dell'autorità giudiziaria.

Appare pertanto profilabile l'integrazione della inutilizzabilità sancita dall'art. 11, comma 2 stesso Codice.

Particolarmente interessante è il caso delle c.d. perquisizioni elettroniche, che consentono intrusioni in un sistema informatico, ovviamente all'insaputa dell'interessato, attraverso l'inserimento di un programma *ad hoc* in grado di captare dati e trasmetterli in tempo reale o ad intervalli prestabiliti agli organi investigativi o di leggerli durante la trasmissione tramite uno *sniffer,* secondo un ampio ventaglio di possibilità tecniche, dipendenti dalla sofisticatezza del programma o dello stesso *sniffer:* si possono così accertare e registrare nel tempo i siti *web* visitati e gli *account* di accesso nonché decifrare quel che viene digitato sulle tastiere di collegamento al sistema.

Tali perquisizioni, gravemente lesive della riservatezza e normalmente esperite nella fase delle indagini preliminari, non potrebbero essere considerate prove atipiche o documentali e devono essere piuttosto ascritte alla categoria dei flussi comunicativi, soggetti alla disciplina dell'art 15 Cost. e del Codice della *privacy.*

3. GLI OBBLIGHI STATUITI DAL GARANTE DELLA PRIVACY PER I CONSULENTI

Con la deliberazione n. 46 del 26 giugno 2008 il Garante per la protezione dei dati personali ha emanato le "Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero", regole che riguardano sia i consulenti tecnici di ufficio che quelli di parte nei procedimenti civili, penali ed amministrativi e rendono loro applicabili le disposizioni del "Codice in materia di protezione dei dati personali" (d.lgs. 196/2003).

I consulenti nell'espletamento dell'incarico conferito, vengono a contatto con una moltitudine di informazioni e di dati personali riferiti sia alle parti processuali sia a soggetti che a vario titolo partecipano al processo. Di conseguenza, costoro sono

chiamati all'osservanza delle regole poste a presidio della sicurezza dell'integrità di detti dati.

Ai trattamenti effettuati dai consulenti, in quanto direttamente correlati alla trattazione giudiziaria di affari e di controversie, si applicano le norme del Codice relative ai trattamenti effettuati presso uffici giudiziari di ogni ordine e grado "per ragioni di giustizia", in particolare l'art.47 del d.lgs. 196/2003 che rende espressamente non applicabili alcune disposizioni del Codice stesso.

Tali deroghe riguardano:

- le modalità di esercizio dei diritti da parte dell'interessato (art. 9);
- il riscontro da fornire al medesimo (art.10);
- l'informativa agli interessati (art. 13);
- la cessazione del trattamento (art. 16);
- il trattamento svolto da soggetti pubblici (artt. da 18 a 22);
- la notificazione al Garante (artt. 37 e 38 , commi da l a 5);
- determinati obblighi di comunicazione all'Autorità, le autorizzazioni e il trasferimento dei dati all'estero (artt . da 39 a 45);
- i ricorsi al Garante (artt . da 145 a 151).

Valgono però per tutti i consulenti le regole generali sulle modalità di trattamento (art. 11) e sull'osservanza delle misure idonee e preventive (art. 31) e minime (artt. da 33 a 35).

La raccolta ed il trattamento dei dati personali sono leciti nei limiti in cui ciò sia necessario per l'adempimento dell'incarico ricevuto e solo nell'ambito dell'accertamento assegnato .

Le informazioni personali e le modalità di trattamento devono essere proporzionate alla finalità perseguita, nel rispetto scrupoloso delle prescrizioni impartite dall'autorità giudiziaria.

Le relazioni di consulenza non devono riportare dati (sensibili, giudiziari o comunque delicati) non pertinenti all'oggetto dell'incarico, né contenere immotivatamente informazioni personali riferite a soggetti estranei al procedimento.

L'eventuale utilizzo incrociato di dati, poi, può avvenire solo se strettamente correlato alle indagini che sono state delegate e se autorizzato dalle singole autorità giudiziarie preposte.

Nella delibera del Garante viene ribadito l'obbligo per ciascun professionista di mantenere il segreto sulle operazioni peritali e su ogni altra informazione appresa durante o in ragione dell'incarico, nel rispetto delle norme civili, penali e deontologiche applicabili.

Eventuali comunicazioni di dati a terzi, anche attraverso i consulenti di parte, possono avvenire nel rispetto delle predette norme, nonché delle istruzioni ed autorizzazioni preventive rilasciate di volta in volta dall'autorità giudiziaria .

Per quanto concerne la conservazione dei dati, va detto che l'art. 16 del d.lgs. 196/2003 non si applica ai trattamenti per fini di giustizia.

Nel caso dei consulenti è previsto, infatti, che tutti i dati raccolti nell'espletamento dell'incarico oppure ricevuti dal magistrato devono essere riconsegnati al termine dell'attività, una volta che l'incarico possa considerarsi esaurito.

Possono essere eccezionalmente conservate alcune informazioni solo se previsto dalla legge o dietro autorizzazione del magistrato .

Inoltre il professionista può legittimamente conservare alcuni dati solo se necessario per adempiere ad un obbligo in materia fiscale , contabile o tributaria.

Sui consulenti ricade l'onere di provvedere alla tutela dei dati personali utilizzati ed è loro la responsabilità in caso di indebita divulgazione , perdita o distruzione.

Vige pertanto l'obbligo di adottare tutte le misure di sicurezza, generali e minime, che il Codice in materia di protezione dei dati personali prevede agli articoli 31, 33, 34, 35, nonché nel Disciplinare tecnico "Allegato B".

Quando si avvale di collaboratori, vi deve essere un preventivo incarico scritto con cui il perito o il consulente, rivestendo la qualità di titolare del trattamento, fornisce tutte le istruzioni necessarie sulle corrette modalità di utilizzazione, conservazione, custodia dei dati e l'ambito di trattamento consentito (art. 30).

Tutto quanto sopra detto vale anche per i professionisti incaricati dalle parti private.

V. LA PROVA SCIENTIFICA

1. SCIENZA E GIURISDIZIONE

Negli ultimi tempi il tema della prova scientifica sia diventato di gran moda per ragioni per molti aspetti paradossali.

Ragioni paradossali perché da una parte il ruolo della scienza e l'importanza delle conoscenze scientifiche sono cresciute a dismisura negli ultimi anni; dall'altra parte è diventata sempre più diffusa, sempre maggiore la consapevolezza che la scienza è anche un'istituzione sociale ed ha in qualche misura a che fare con il potere: con il potere, per esempio, che esercita colui che distingue ciò che può essere considerato "scienza" da ciò che non deve essere così qualificato.

Ad esempio il protocollo Di Bella sulla cura del cancro o il più recente metodo Stamina del Prof. Vannoni per la cura con cellule staminali.

Si è discusso a lungo se si trattasse o meno di scienza. E il problema, in entrambi i casi, è stato risolto dalle istituzioni pubbliche.

Questa istituzionalizzazione avvicina in qualche misura la scienza alla giurisdizione, perché anche la giurisdizione è una conoscenza istituzionalizzata, anche la giurisdizione è un metodo istituzionalizzato di conoscenza.

Tanto che viene da domandarsi quale sia il rapporto tra queste due conoscenze istituzionalizzate. Ed è in questa domanda il punto di partenza fondamentale per comprendere i limiti di utilizzazione della scienza da parte del giudice.

Lo scienziato utilizza esperienze particolari e ripetibili, per produrre enunciati di carattere generale.

La giurisdizione opera, invece, in senso esattamente opposto, perché il giudice utilizza le conoscenze, gli enunciati generali, prodotti dalla scienza, per affermare qualcosa su fatti particolari e irripetibili, non riproducibili in laboratorio.

Questa constatazione ha implicazioni importantissime, perché nessuna legge scientifica, nessun enunciato universale, per quanto sia certo nelle sue implicazioni, potrà dirci tutto sul caso particolare che si richiede di risolvere in un'aula di giustizia. Infatti quel caso particolare è appunto un *unicum;* mentre la legge scientifica parla di una classe di fatti, e quindi quella legge potrà essere solo uno degli elementi di giudizio, non potrà mai essere l'unico elemento di giudizio.

2. PROBABILITA' STATISICA E PROBABILITA' LOGICA

In realtà le leggi scientifiche che sono più utili al giudice sono quelle che non si limitano a constatare la frequenza del verificarsi di un fenomeno, ma quelle che lo spiegano; sono utili le leggi che ci dicono anche perché, dato il fatto "A" ne segue il fatto "B".

Una legge scientifica per cui nel 99% dei casi dato "A" ne segue "B", al giudice non basta, perché il giudice non può condannare al 99%.

Le leggi più utili per il giudice non sono dunque le cosiddette leggi statistiche, con probabilità frequenziale, che dicono solo qual è la ricorrenza di un certo fenomeno, ma sono le leggi che si inseriscono in un sistema di conoscenze scientifiche già esistenti e sperimentate, e si ricollegano a queste conoscenze appunto per offrire una spiegazione del fenomeno, per dirci perché quel fenomeno si manifesta.

Tuttavia anche queste leggi non sono da sole sufficienti a ricostruire la concreta vicenda umana che il giudice deve vagliare, perché sono tanti gli elementi

circostanziali, tanti gli elementi di disturbo coinvolti, che nessuna vicenda rientrerà mai integralmente ed esclusivamente nell'ambito esplicativo di una sola legge.

La probabilità logica è il grado di plausibilità della storia che, anche sulla base delle conoscenze scientifiche, si riesce a ricostruire per dare un senso accettabile a quella vicenda; la storia che spieghi il perché nella società in cui il giudice opera quel fatto deve avere un certo significato, che non dipende solo dalle leggi scientifiche, ma dipende anche da abitudini, tecnologie, istituzioni, morali, che a quella vicenda danno un senso comunicabile discorsivamente; dipende da una infinità di fattori, che vanno tutti considerati in una particolare prospettiva ricostruttiva.

Le conoscenze scientifiche sono dunque solo una parte delle conoscenze che il giudice deve utilizzare per ricostruire i fatti.

3. USO PROCESSUALE DELLA PROVA SCIENTIFICA

D'altro canto il problema dell'utilizzazione della conoscenza scientifica può porsi in due prospettive diverse nel processo.

In ogni processo si dibattono, si discutono, sempre, immancabilmente, due pretese: una pretesa di verità, relativa alle affermazioni sui fatti e una pretesa di validità, relativa alle qualificazioni che di quei fatti che vengono proposti.

L'attore che promuove il giudizio, nel processo penale il pubblico ministero, afferma dei fatti e ne propone una qualificazione, postulando che quei fatti debbano avere un certo effetto giuridico previsto dalla legge. Vi sono sempre, in ogni processo, una pretesa di verità e una pretesa di validità.

La pretesa di validità si riferisce a una qualificazione che e sempre giuridica, anche quando dipenda da qualificazioni sociali. Vengono infatti rese “giuridiche” le stesse

norme sociali o anche morali cui la legge rimanda per assegnare un determinato significato a un fatto.

Quando si dice che uccidere un uomo è un delitto, il concetto di uomo è definito dalla cultura sociale di un determinato momento storico e può accadere che includa piuttosto che escludere l'uomo di colore o l'ebreo.

Se dunque la risposta alla pretesa di validità è sempre una risposta giuridica, essa presuppone però una preesistente risposta alla pretesa di verità: vale a dire alla pretesa di corrispondenza alla realtà delle affermazioni sui fatti poste a base della decisione.

Infatti non è possibile porsi seriamente il problema della qualificazione di un fatto che non sia stato seriamente accertato.

E l'idea della verità come corrispondenza non è affatto incompatibile con l'idea che la verifica delle affermazioni sui fatti proposte dall'attore debba avvenire nel contraddittorio delle parti.

Occorre, infatti, distinguere il problema dei criteri di verità, del metodo di accertamento della verità, dal problema della definizione logica della verità, come rapporto di un enunciato descrittivo con il modo che pretende di descrivere.

Il modo in cui si verifica questo presunto rapporto di corrispondenza non mette affatto in discussione la definizione della verità.

Analogamente avviene quando un problema di qualificazione, un problema di validità, si pone in termini causali.

Nel processo accade frequentemente che ci siano due distinti modi di usare la categoria della causalità.

Ad esempio possiamo domandarci perché un aereo con ottanta passeggeri è caduto a Ustica.

Ci troviamo di fronte a un evento, la caduta dell'aereo, e dobbiamo ricostruirne la cause. Questa è la pretesa di verità del processo.

Altre volte ci troviamo a ragionare pur sempre in termini di causalità, ma in una prospettiva completamente diversa. I fatti non sono in discussione, perché la pretesa di verità ha ricevuto una risposta soddisfacente.

Posto ad esempio che un operaio è stato lasciato lavorare a contatto con l'amianto, possiamo dire che c'è un rapporto di causalità tra questo fatto e la morte dell'operaio? Qui la risposta attesa non è più a una pretesa di verità, ma dobbiamo rispondere a una domanda sulla possibilità di qualificare un fatto come causa di un altro. Ci si domanda, stando all'esempio, se possiamo dire che l'esposizione all'amianto è stata la causa della malattia.

E questo è un problema di qualificazione.

4. TEORIE DELLA CAUSALITÀ E SCHEMI ARGOMENTATIVI DEL GIUDICE.

La "condicio sine qua non", come la teoria della corrispondenza per la verità, è una teoria solo logica , vuota di contenuti. Come la teoria della verità di Tarsky, anche la teoria condizionalistica della causalità è una teoria tautologica, perciò necessariamente vera.

E' tautologica perché la teoria condizionalistica ci dice solo che, se un fatto è condizione necessaria di un altro, ne è causa; se invece ne è condizione sufficiente, non ci sono altre condizioni necessarie.

È un gioco di parole: se una condizione è necessaria, significa che non ce ne sono altre sufficienti; se è sufficiente significa che non ce ne sono altre necessarie.

Ma è un gioco di parole fondamentale, perché ci chiarisce cosa noi intendiamo per "causalità"; stabilisce le condizioni per un uso corretto di questa qualificazione.

Rimane però il problema di stabilire come noi accertiamo se una condizione è necessaria o sufficiente. E qui entra in gioco certamente la scienza; ma entrano in gioco anche le peculiarità dell'accertamento giudiziario.

Sia la risposta alla pretesa di verità sia la risposta alla pretesa di validità rispondono infatti nel processo a un medesimo schema argomentativo. Si parte da un dato, per esempio una prova, e si argomenta una conclusione, in ragione di una regola di inferenza, ad esempio una legge scientifica, che giustifica il passaggio da quel dato di partenza a quella conclusione.

Quando si tratta di rispondere ad una pretesa di verità, la regola di inferenza, esibita a garanzia dell'argomentazione sui fatti , viene fondata su una base di esperienze ricorrenti, secondo il principio di induzione.

Quando, invece, si tratta di rispondere alla pretesa di validità di un criterio di qualificazione, la fondazione della regola di inferenza può essere riferita alla supposta condivisione di valori, di interessi , di bisogni, di convenzioni sociali.

5. IL PROBLEMA DEL DUBBIO RAGIONEVOLE

Se la conoscenza scientifica è istituzionalizzata, a maggior ragione la giurisdizione deve rispondere a regole certe su tempi, modalità e occasioni di argomentazione.

E questa regolamentazione deve consentirci di rispondere anche al problema del dubbio ragionevole, che si porrà certamente in termini perentori, dopo la recente riforma dell'art. 533 c.p.p.

Ogni dubbio ragionevole è un 'ipotesi alternativa; è l'ipotesi che si possa spiegare, si possa dare una risposta alternativa, a una delle pretese di verità o a una delle pretese di validità, che si agitano nel processo.

Ragionevole significa innanzitutto compatibile con le regole del processo. E non sembri questa una banalità.

Esiste ad esempio una norma per cui una prova sopravvenuta può giustificare la revisione del giudicato. Sappiamo però che nel giudizio di cassazione non si può chiedere l'ammissione di una prova. Non è possibile che in Cassazione il difensore tiri fuori una fotografia e pretenda di esibirla come prova. Quella fotografia potrebbe giustificare qualsiasi ipotesi, anche plausibilissima, ma non è ragionevole, perché è incompatibile con le regole del processo. Se sarà il caso, il difensore potrà farla valere in sede di revisione. Altrimenti si violano le stesse regole del contraddittorio.

Con il codice Rocco era la parte a dover dimostrare la rilevanza della prova, per ottenerne l'ammissione a opera del giudice. Con il codice vigente è il giudice che, per negare l'ammissione della prova richiesta dalle parti, deve dimostrare che essa è manifestamente irrilevante, in quanto non pertinente al *thema decidendum,* ovvero è manifestamente superflua, in quanto tendente a un risultato conoscitivo già acquisito.

Sicché, per il solo fatto che una prova sia stata richiesta da una parte, se ne presume l'ammissibilita sino a dimostrazione del contrario; ed è in questa presunzione che si manifesta il potere dispositivo delle parti in ordine alla prova.

La plausibilità delle ipotesi ricostruttive del fatto va allora commisurata alle diverse storie che si sono effettivamente confrontate nel processo. Non può il giudice inseguire tutte le possibili storie , in astratto formulabili rispetto a un avvenimento;

non può il giudice inseguire l'astrattezza di ogni dubbio possibile. Il principio del contraddittorio esige che il giudice faccia riferimento a ciò che le parti hanno effettivamente proposto e prospettato.

Ed è solo rispetto a queste prospettive concrete che può porsi un dubbio ragionevole; non è ragionevole il dubbio astratto. Il criterio della ragionevolezza evoca la plausibilità dell'accertamento, non la cogenza dimostrativa dell'astratta razionalità, che legittimerebbe, e renderebbe insuperabile, qualsiasi dubbio inteso in senso propriamente logico.

Questo dà ovviamente il senso della relatività delle nostre certezze; ma la consapevolezza della debolezza delle nostre conoscenze è certamente preferibile alla pretesa di una verità assoluta attestata da un solitario costruttore di ipotesi anche astratte.

Spesso diamo risposte che sono sempre condizionate dal nostro punto di vista, dai nostri criteri di ragionevolezza.

E la grande conquista della nostra civiltà sta nell'avere individuato il confronto quale criterio di selezione delle prospettive più adeguate.

È il contraddittorio dunque il solo criterio della nostra certezza. Solo dal confronto reale può nascere un ragionevole dubbio, perché è ragionevole solo l'ipotesi alternati va che effettivamente sia venuta fuori dal contraddittorio tra le parti.

6. IL FATTORE TEMPO NEI RAPPORTI TRA SCIENZA E DIRITTO

Per altro verso, merita di essere sottolineato, nella dimensione delle coordinate epistemologiche e logiche del ragionamento probatorio, che sta mutando il quadro assiologico del fattore "*tempo*" nei rapporti tra scienza e diritto.

È stato rimarcato, quale significativo elemento di differenziazione fra i due sistemi formali di indagine, che « poiché il diritto deve giungere a una conclusione in un tempo finito, l'accertamento dei fatti a fini legali è sempre condizionato dal tempo»[50]; il giudice deve comunque concludere il processo in base agli elementi probatori di cui dispone, per quanto prematura e revocabile possa apparire la decisione giudiziale agli occhi degli scienziati .

Insomma, la limitatezza spazio-temporale del processo che si chiude col giudicato *vs.* la riproducibilità del fenomeno ad opera dello scienziato.

E però, l'idea che l'accertamento dei fatti , ai fini della conferma o falsificazione dell'ipotesi di accusa, sia condizionato e limitato nel tempo, nella sua assolutezza, non sembra più sostenibile in un contesto segnato in profondità dalle implicazioni gnoseologiche insite nella costituzionalizzazione del contraddittorio in senso "forte" e nel riconoscimento legislativo del criterio del '"al di là di ogni ragionevole dubbio".

Anche la Corte di Strasburgo, nell'affidare ai giudici nazionali il compito di «interpretare la legislazione esistente alla luce del processo scientifico e delle conseguenti ripercussioni sociali », mette in luce l'esigenza di conformare la regolamentazione della dinamica processuale all'evoluzione dei saperi extra giuridici incidenti sul fenomeno probatorio, facendone scaturire precise indicazioni

[50] S. JASANOFF, *La scienza davanti ai giudici,* Milano, 2001, pp. 355-392. Più in generale, sui rapporti fra scienza e diritto, M. T. ALLACCHINI, *La costruzione giuridica della scienza come costruzione giuridica della scienza come co-produzione tra scienza e diritto* in *Politeia,* 2002, n. 65, p. 126.

ermeneutiche destinate a consolidare il processo di graduale estensione dell'area di operatività della revisione.

Di talché, sarebbe incompatibile con i principi convenzionali una disciplina nazionale che facesse, sempre e in ogni caso, prevalere l'esigenza di certezza e stabilità dei rapporti giuridici rispetto alla tutela di un diritto fondamentale , che potrebbe essere invece assicurata mediante il ricorso a una (nuova) prova resa possibile dal progresso tecnico-scientifico.

Risulta invece coerente con questa impostazione il più recente indirizzo giurisprudenziale della Corte di cassazione per il quale, in tema di revisione, la perizia ben può costituire "prova nuova", laddove si basi su "nuovi" metodi e acquisizioni scientifiche idonei a superare i criteri di valutazione di elementi fattuali, pure già noti ai periti e al giudice e adottati nel precedente giudizio.

Ciò che rileva, tuttavia, non è tanto la potenziale ricorribilità a un metodo di indagine nuovo, quanto la concreta idoneità del mezzo di prova a pervenire, per effetto del progresso scientifico, a risultati probatori sostanzialmente diversi e suscettibili di mutare il contenuto dell'accertamento espletato nel precedente giudizio. Ciò che conta non è la metodologia d'indagine (che potrebbe anche essere la stessa, benché aggiornata e perfezionata alla luce di nuove scoperte) bensì il probabile risultato della "nuova" prova tecnico-scientifica[51].

[51] Sembra coerente con questo tipo di ragionamento la valutazione prognostica che è affidata al giudice della revisione della condanna nella fase introduttiva del relativo giudizio, laddove la prova "nuova" sia caratterizzata dalla novità del metodo impiegato o dei principi tecnico- scientifici applicati nella fattispecie. In tal caso, il preliminare apprezzamento critico del grado di affidabilità, rilevanza e idoneità dimostrativa di siffatta prova a ribaltare l'originario costrutto accusatorio - che non si traduca tuttavia in un'approfondita e indebita anticipazione del giudizio di merito -, in funzione del probabile esito positivo della revisione e del conseguente proscioglimento dell'imputato, anche mediante l'introduzione di un "dubbio" ragionevole sulla colpevolezza del condannato, condiziona non solo l'ingresso della prova nel processo bensì, addirittura e più radicalmente, la t a ammissibilità della domanda di revisione e del relativo giudizio (artt. 630 lett, *c, 631* e 634, comma 1 c.p.p.).

L'accertamento della "verità", in termini di corrispondenza dell'enunciato di accusa ai fatti, pur stabilizzatosi nel giudicato, rimane così aperto alla potenziale, futura revisione, sullo sfondo epistemologico del razionalismo critico imperniato sul metodo "falsificazionista", ovvero sulla "eliminazione induttiva" delle spiegazioni alternative, che caratterizza la ricerca scientifica.

La valutazione delle prove e il giudizio conclusivo, essendo influenzati dall'incessante divenire della conoscenza scientifica e dal più elevato *standard* decisorio del ragionevole dubbio, sono chiamati costantemente a misurarsi con un punto di vista "esterno", per sua natura mutevole, dettato dall'evoluzione delle conoscenze scientifiche, cui possa conseguire, nel caso concreto , il ragionevole dubbio circa la colpevolezza dell'imputato.

D'altra parte, occorre convenire che, in un sistema ispirato alla concezione "aperta" della prova e alla costante interazione tra scienza e diritto, il dinamico adeguamento della certezza e della stabilità processuale all'evoluzione scientifica si pone come necessaria condizione di legittimazione "esterna", sul piano etico-politico, della stessa attività giurisdizionale.

VI. DIRITTO DI DIFESA E PROVA SCIENTIFICA

1. PRINCIPI COSTITUZIONALI

Nel processo penale si assiste alla progressiva adozione di modelli scientifici nelle tecniche di ricostruzione dei fatti e al corrispondente assottigliarsi del repertorio di conoscenze dell'uomo medio, come serbatoio delle regole di inferenza da utilizzare nel ragionamento probatorio[52].

II fenomeno, tuttavia, non è scevro di conseguenze, poiché lo spostamento della linea di confine tra sapere comune e conoscenze specialistiche rende le decisioni più difficilmente controllabili dal giudice e dalle parti.

Oreste Dominioni ha rilevato in proposito che si tratta di operazioni probatorie per le quali, al momento dell'ammissione, dell'assunzione e della valutazione, si usano strumenti di conoscenza attinti alla scienza e alla tecnica, vale a dire princìpi e metodologie scientifiche, metodiche tecnologiche ed apparati tecnici , il cui uso richiede competenze esperte[53].

II problema di fondo è verificare come il ricorso alle leggi scientifiche, sempre mutevoli in virtù del continuo progresso tecnologico, possa avvenire nel rispetto dei principi del giusto processo e segnatamente del diritto di difesa, dai quali non si può prescindere.

In particolare la presunzione di non colpevolezza, al riconoscimento della inviolabilità del diritto di difesa in ogni stato e grado del procedimento, alla formazione della prova nel dibattimento nel contraddittorio delle parti, ai diritti dell'accusato di essere informato nel più breve tempo possibile della natura e dei

[52] G. CANZIO. Prova scientifica, ricerca della ”verità" e decisione giudiziaria nel processo penale, in AA.Vv., Quaderno n. 8 della Riu. trim. dir. proc. civ., 2005. p. 71
[53] O. DOMINIONI, La prova penale scientifica. Milano. 2005. p. 12.

motivi dell'accusa elevata a suo carico , di disporre del tempo necessario e delle condizioni necessarie per preparare la propria difesa, di ottenere la convocazione di persone a sua difesa.

Logico corollario di tali enunciazioni è che lo stesso accusato possa difendersi provando, anche attraverso l'individuazione di fonti di prova e la successiva loro raccolta da parte del difensore.

Va ancora rimarcato che la condanna può venire inflitta soltanto se l'imputato risulti colpevole oltre ogni ragionevole dubbio.

In una recente decisione[54], la Corte suprema ha affermato in proposito che la regola dell'oltre il ragionevole dubbio formalizzata nell'art. 533, comma 1 c.p.p., impone di pronunciare condanna, quando il dato probatorio acquisito lascia fuori solo eventualità remote, ma la cui realizzazione nella fattispecie concreta non trova il benché minimo riscontro nelle emergenze processuali, ponendosi al di fuori dell'ordine naturale delle cose e della normale razionalità umana: pretende, pertanto, percorsi epistemiologicamente corretti, argomentazioni motivate circa le opzioni valutative della prova, giustificazione razionale della decisione, standard conclusivi di alta probabilità logica in termini di certezza processuale, essendo indiscutibile che il diritto alla prova, come espressione del diritto di difesa, estende il suo ambito fino a comprendere il diritto delle parti ad una valutazione legale, completa e razionale della prova.

È evidente, in tale prospettiva, la stretta correlazione, dinamica e strutturale esistente tra la regola in esame e le coesistenti garanzie, proprie del processo penale, rappresentate:

[54] Cass., sez. I, 26 maggio 2010, Erardi, in Dir. Pen.proc., 2010, p. 203

a) dalla presunzione di innocenza dell'imputato, regola probatoria e di giudizio collegata alla struttura del processo e alle metodiche di accertamento del fatto ;

b) dall'onere della prova a carico dell'accusa;

c) dalla regola di giudizio stabilita per la sentenza di assoluzione in caso di "insufficienza", "contraddittorietà" e "incertezza " della prova d'accusa (art. 530, commi 2 e 3 c.p.p.), secondo il classico canone di garanzia in *dubio pro reo;*

d) dall'obbligo di motivazione delle decisioni giudiziarie e dalla necessaria giustificazione razionale delle stesse.

In tema di prova scientifica, dunque, il giudice dovrebbe dar conto in motivazione di aver valutato criticamente il grado di controllabilità e attendibilità del metodo scientifico, l'esistenza di revisioni critiche di esperti del settore, l'indicazione dei margini di errore conosciuto.

2. IL CONTROLLO NELL'ASSUNZIONE DELLA PROVA SCIENTIFICA

In questo quadro, è inevitabile osservare che la specificità della materia esige sofisticate conoscenze tecniche in possesso di soggetti altamente specializzati, per cui le problematiche in materia non involgono soltanto l'applicazione dei tipici istituti previsti dal codice di procedura penale (e segnatamente le disposizioni in materia di rilievi, operazioni tecniche , accertamenti tecnici ripetibili e non, perizie ed ispezioni), ma sconfinano nel labile e scivoloso terreno delle prove atipiche.

Ora, è certamente vero che l'art. 189 c.p.p. è stato introdotto nel nostro ordinamento proprio per « evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive », quindi il giudice deve vagliare che

le prove non disciplinate dalla legge siano affidabili sul piano della genuinità dell'accertamento e non lesive della libertà morale della persona[55].

E', tuttavia, altrettanto indiscutibile come atipico sia ciò che esula da cataloghi nei quali potrebbe astrattamente rientrare e soprattutto che la norma fissa regole alle quali non dovrebbe essere consentito derogare, vale a dire che tratti di una prova non disciplinata dalla legge, che risulti idonea ad assicurare accertamento dei fatti, che non pregiudichi la libertà morale della persona e specialmente che il giudice proceda all'ammissione sentite le parti sulle modalità di assunzione.

Da ciò deriva la sussidiarietà della prova atipica e la necessità di un preventivo contraddittorio tra le parti davanti al giudice per le modalità di assunzione: il che esclude la sua applicazione nella fase delle indagini preliminari, dove, per di più, gli atti suscettibili di assumere rilievo probatorio sono ben definiti e tipici (dai sequestri, alle perquisizioni, alle ispezioni, agli accertamenti tecnici).

Indubbiamente gli strumenti probatori di questo tipo, specie se innovativi, tendono a sfuggire al catalogo legale ed è difficile elaborare per essi un repertorio cristallizzato, poiché derivano dal mondo indefinito e costantemente mutevole degli studi che scienza teorica, scienza applicata e tecnologia conducono, con risultati mai definitivi e irreversibili.

La scoperta di nuove e attendibili tecniche non è sufficiente per eludere le disposizioni sulla perizia[56] ed è evidente che « o sono reperibili risorse di cui giudice e parti possono giovarsi per il controllo dello strumento scientifico-tecnico, e allora esso è ammissibile nel processo; oppure tali risorse mancano a causa della sua natura nuova o controversa e dell'elevata specializzazione, e allora non è ammissibile poiché

[55] Relazione al progetto preliminare, in Doc. giust., 1988, p. 125

[56] M. NOBILI, La nuova procedura penale. Lezioni agli studenti, Bologna, 1989, p. 120.

non è consentito che nella funzione probatoria si usino apparati conoscitivi insuscettibili di controllo ad opera del giudice e delle parti » [57].

Se venisse a mancare una effettiva possibilità di valutazione dell'operato dell'esperto, verrebbe, infatti, vanificato il principio della formazione della prova nel contraddittorio e si creerebbe il paradosso che un giudice ovviamente "inesperto" aderirebbe acriticamente alle conclusioni proposte da un esperto.

Appare, perciò, condivisibile l'opinione per cui il giudice deve verificare la validità scientifica dei criteri e dei metodi d'indagine utilizzati dal perito, allorché essi si presentino nuovi e sperimentali, e perciò non sottoposti al vaglio di una pluralità di casi ed al confronto critico tra gli esperti del settore, così da non potersi considerare acquisiti al patrimonio della comunità scientifica, mentre se la perizia si fonda su cognizioni di comune dominio tra gli esperti e su tecniche di indagine consolidate, tale verifica concerne soltanto la loro corretta applicazione[58].

Al riguardo, è opportuno notare che l'art. 220 c.p.p. sembra riflettere proprio le situazioni rappresentate, laddove dispone che si debba procedere a perizia allorquando «occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche ».

La scoperta di nuove e attendibili tecniche non giustifica dunque la disapplicazione delle disposizioni sulla perizia e sugli accertamenti tecnici nelle indagini preliminari, con le correlative garanzie.

---

[57] O. DOMINIONI , La prova penale scientifica , cit., p. 69.

[58] Cass., sez. V, 9 luglio 1993, Ietto, in Ardr. n. proc. pen., 1994, p. 226: il caso esaminato riguardava una perizia nella quale era stato applicato un metodo di ricerca definito "parametrico", dotato di una elevatissima capacità di identificazione della voce. In applicazione di questo principio, Cass., sez. II , 17 ottobre 2003, T., in CED 227854, ha ritenuto utilizzabile un metodo computerizzato di identificazione dei volti travisati degli autori di una rapina , ripresi da una telecamera a circuito chiuso ; cfr. anche Cass., sez. II , 11 Agosto 1997, p.m. in c. Vezzoni , in CED208464.

3. GLI ACCERTAMENTI TECNICI IRRIPETIBILI

L'esigenza del rispetto rigoroso del diritto di difesa è ulteriormente rafforzata dalla estrema delicatezza della fase di individuazione, raccolta, conservazione e valutazione dei dati, che richiedono un'alta specializzazione e presentano il rischio che una parte del materiale si deteriori o si disperda, impedendo o rendendo difficile contestare la valenza probatoria dell'accertamento.

Non sembra risolutiva al riguardo l'emanazione di protocolli operativi da parte del legislatore, che non potrebbero essere tassativi (si vedano, ad esempio, gli artt. 354, comma 2, e 359-bis c.p.p.) e comunque sarebbero rapidamente superati dal tumultuoso e costante sviluppo tecnologico, essendo illusorio immaginare costanti interventi di aggiornamento: d'altro canto, anche se essi fossero elaborati dalla comunità scientifica specializzata, avrebbero sì un maggior grado di affidabilità, ma sarebbero ugualmente soggetti ad obsolescenza e a continui adeguamenti.

Inoltre, siffatte prassi consentirebbero solo un contraddittorio differito, certamente insufficiente, specie laddove l'indagine importi un forte contenuto valutativo.

È allora indispensabile che il difensore e il consulente tecnico di parte siano posti in grado di partecipare attivamente a questa prima fase e trovino applicazione le norme in materia di accertamenti tecnici non ripetibili, tra i quali sono esattamente inquadrabili le attività in discussione, non sembrando discutibile che esse riguardino «persone, cose e luoghi il cui stato è soggetto a modificazione» (art. 360 c.p.p.) ovvero «le cose, le tracce e i luoghi» suscettibili di alterarsi, disperdersi o modificarsi (art. 354, comma 2 c.p.p.).

Va anche rilevato come la presenza dello stesso difensore agli accertamenti, rilievi ed operazioni tecniche della polizia giudiziaria non richieda alcuna autorizzazione (con

la facoltà di avvalersi di persone idonee: artt. 348 e 354 c.p.p.) a norma dell'art. 391-sexies c.p.p., e comunque egli, può effettuare propri accertamenti non ripetibili ai sensi dell'art.391-decies c.p.p., dandone avviso al pubblico ministero per l'esercizio delle facoltà a questi riconosciute dall'art.360 c.p.p., ovvero altri atti non ripetibili (cui il pubblico ministero può decidere di partecipare personalmente o per delega alla polizia giudiziaria), con allegazione della relativa documentazione al fascicolo per il dibattimento.

In proposito, appare opportuno osservare che il richiamo all'art. 360 c.p.p. rende evidente che gli accertamenti tecnici irripetibili sono soltanto quelli riguardanti «persone, cose o luoghi il cui stato è soggetto a modificazione»: per converso, gli altri atti non ripetibili consentiti al difensore non devono essere suscettibili di provocare mutamenti dello stato dei luoghi e delle cose.

I primi, dunque, esigono un'attività implicante un grado di conoscenza tecnico-scientifica, nella quale l'elemento giudizio prevale sull'elemento osservazione; gli altri, invece, regolamentati nell'art. *391-sexies* c.p.p., si esauriscono in una mera attività di esame e descrizione, senza alcuna valutazione critica del dato raccolto, come emerge dal contenuto della norma, che nella prima parte parla di accessi diretti a « prendere visione» o a procedere alla «descrizione» dello stato dei luoghi e delle cose, e autorizza poi l'esecuzione di rilevi «grafici, descrittivi, fotografici e audiovisivi», attività tutte che escludono ogni possibilità di interventi che comportino l'alterazione dello stato dei luoghi e delle cose[59].

[59] Cfr., volendo, P. GUALTIERI, Le investigazioni del difensore, Padova, 2002, pp. 188 ., anche per una confutazione critica delle contrarie opinioni, nonché, sull'ambiguità del termine rilievo e sulla distinzione con l'accertamento tecnico, P. GUALTIERI, Perquisizioni ed ispezioni di polizia. Milano, 1979, pp. 62 ss..

La differenza fra le due tipologie di atti spiega pure perché il pubblico ministero debba essere avvertito solo quando si tratti di accertamenti tecnici non ripetibili, riguardanti, appunto, persone, cose e luoghi il cui stato è soggetto a modificazione.

E in proposito sono configurabili diverse situazioni.

La parte pubblica può, infatti:

a) disinteressarsi completamente della formazione dell'atto;

b) rivendicare il diritto di assistere, unitamente al proprio consulente tecnico eventualmente nominato, al conferimento dell'incarico al consulente tecnico del difensore, partecipare agli accertamenti e avanzare osservazioni e riserve (art. 360, *comma 3 c.p.p.);*

c) formulare, prima del conferimento di tale incarico, riserva di promuovere incidente probatorio, in modo che non si possa procedere agli accertamenti, salvo non siano successivamente utilmente esperibili (art . 360, comma 4 c.p.p.);

d) disporre a sua volta un accertamento tecnico irripetibile, non necessariamente identico come oggetto, ma coincidente con quello deciso dal difensore.

Tutte queste opzioni non sono in contrasto con le disposizioni contenute nell'art. 360 c.p.p., che devono intendersi applicabili nella loro interezza, salvo non risultino incompatibili: e non pare proprio che questa evenienza si realizzi, considerato anche che la volontà del legislatore è stata quella di realizzare una regolamentazione speculare degli obblighi e dei diritti previsti nelle due norme (artt. 360 e 391-decies, comma 3 c.p.p.), rispettivamente per il pubblico ministero e per il difensore[60].

[60] Come emerge dalla Relazione alla legge n. 397/2000 del sen. Follieri , pubblicata in R BRICCHETTI E.RANDAZZO, Le indagini della difesa dopo la legge 7 dicembre «2000 n. 397, Milano, 2001, p. 27 1,Ia intenzione del legislatore era proprio quella « che anche l'art. 391 decies comma 2 c.p.p., dovesse specularmente stabilire l'obbligo del difensore di avvisare senza ritardo il pubblico ministero circa il compimento di atti non ripetibili compiuti in occasione dell'accesso ai luoghi

Il problema è dunque di armonizzarle fra di loro. La prima eventualità sopra prospettata, appare estremamente improbabile, attesa la rilevanza probatoria che l'atto raccolto dalla difesa può assumere, ed accadrà anche raramente che il pubblico ministero si adatti a subire le conclusioni della parte privata e del suo consulente tecnico. Non è da escludere la formulazione della riserva di incidente probatorio, la quale, però, non fornisce certezze in ordine all'effettiva sospensione degli accertamenti e alla loro utilizzabilità al dibattimento, poiché il difensore potrebbe procedervi e il giudice ritenere a sua volta sussistenti le condizioni di indifferibilità.

L'ipotesi più verosimile sembra pertanto l'ultima, vale a dire che il pubblico ministero decida di esperire un accertamento tecnico irripetibile, in qualche misura sovrapponibile a quello del difensore.

Gli inevitabili interferenze e conflitti lo vedrebbero soccombente dinanzi ai poteri autoritativi e coercitivi del pubblico ministero e della polizia giudiziaria, che possono porre subito sotto sequestro le cose pertinenti al reato ed assicurare la conservazione dello stato dei luoghi.

4. GLI ACCERTAMENTI RIPETIBILI.

Per gli atti non ripetibili, il terzo comma dell'art. 391-*decies* c.p.p. si limita a riconoscere alla parte pubblica la facoltà di assistervi, personalmente o per delega alla polizia giudiziaria, senza alcuna disposizione in ordine ad obblighi di comunicazioni a carico della difesa. Tale silenzio della norma sul punto e la natura meramente descrittiva delle attività da eseguirsi inducono a ritenere non necessari gli avvisi, tanto da evitare al difensore un'anticipata esibizione, se non relativamente al contenuto dell'atto (del quale può comunque essere omesso il deposito), quantomeno al suo espletamento.

La facoltà di partecipazione degli organi inquirenti troverà pertanto una marginale attuazione nelle sole ipotesi in cui essi vengano casualmente, o per scelta dei soggetti della difesa, a conoscenza del suo compimento.

E anche importante rammentare che l'art. 366 c.p.p. permette l'accesso del difensore alle cose sequestrate: e tale facoltà può essere temporaneamente sospesa in presenza di gravi motivi, che devono essere resi espliciti nell'eventuale provvedimento di diniego, ma non tollera altre restrizioni .

II potere di esaminare le cose sequestrate anche fuori dei casi in cui è disposta perizia (art . 233, comma 1 c.p.p.), è riconosciuto pure ai consulenti tecnici di parte: a tal fine è però necessaria un'autorizzazione rilasciata, su istanza del difensore, dal giudice o, prima dell'esercizio dell'azione penale, dal pubblico ministero.

La regolamentazione crea una discutibile disparità fra l'intervento dell'avvocato, non soggetto a condizioni, e quello del suo esperto, subordinato invece ad una apposita autorizzazione dell'autorità giudiziaria: e ciò potrebbe incidere negativamente sul diritto di difendersi provando, che non è limitato ai soli aspetti giuridici, ma implica spesso profonde e specialistiche conoscenze tecniche[61]. E, in effetti, un esame, cioè una osservazione visiva e tattile, senza manipolazioni (realizzabile anche attraverso fotografie, riprese cinematografiche, misurazioni dimensionali o ponderali) non può certo esporre i beni assoggettati a cautela ad una irreversibile alterazione, per cui l'autorizzazione avrebbe dovuto essere limitata alle sole ipotesi nelle quali fossero ritenute necessarie e richieste indagini più penetranti, suscettibili di mettere a repentaglio le esigenze di conservazione.

[61] Non sembra dubbio che un ingiustificato diniego di accesso al materiale sequestrato, che integra la chiara violazione del diritto di difesa, risulterebbe sanzionabile ex art. 178, lett. c, c.p.p.

Si aggiunga che l'art. 233, comma 1 c.p.p. limita il numero massimo di esperti nominabili a due: la disposizione, peraltro, dovrebbe essere interpretata in senso restrittivo, vale a dire con riferimento a singoli temi di indagine scientifica, in quanto potrebbe sorgere la necessità di accertamenti che richiedano conoscenze specialistiche in diversi settori (medico-legale, informatico, chimico, balistico), e in tal caso non sembra possa negarsi il ricorso, contestuale o in tempi successivi, a più consulenti tecnici .

È inoltre previsto che «l' autorità giudiziaria impartisce le prescrizioni necessarie per la conservazione dello stato originario delle cose e dei luoghi e per il rispetto delle persone ».

5. LA PROVA ATIPICA E LA PROVA DOCUMENTALE.

Questo ventaglio di possibilità di intervento del difensore nelle fasi acquisitiva e valutativa della prova scientifica rischia tuttavia di essere puramente teorico, poiché tanto più sarà specialistica l'indagine da svolgere, tanto maggiori saranno i costi necessari per assicurare la partecipazione di esperti di alta qualificazione: sicché una efficace assistenza sarà riservata soltanto a chi disponga di rilevanti risorse .

L'espansione della prova scientifica amplifica, così, il divario di poteri tra la polizia giudiziaria e il pubblico ministero da un lato e le parti private dall'altro, in quanto gli organi inquirenti pubblici non subiscono nei loro interventi limitazioni operative o economiche.

In questo contesto, il difensore riuscirà quindi difficilmente ad assumere un ruolo attivo, ma dovrà limitarsi ad una azione di critica e contrasto alle iniziative degli organi pubblici di investigazione.

Sarebbe dunque necessario che la raccolta e la valutazione della prova scientifica avvenisse attraverso i più garantisti istituti tipici già esistenti nel codice di rito .

Invece il ricorso all'atipicità probatoria è molto frequente nelle applicazioni giurisprudenziali.

E addirittura, per la fase delle indagini preliminari, si assiste ad una progressiva espansione del concetto di prova documentale.

In una decisione in materia di videoregistrazioni (estese dall'avvento dei "videofonini", alle comunicazioni video), le sezioni unite, tra alcuni princìpi corretti , hanno affermato che quelle eseguite dalla polizia giudiziaria nell'ambito del processo, anche d'iniziativa, devono considerarsi prove atipiche, soggette alla disciplina dettata dall'art. 189 c.p.p. e, trattandosi di documentazione di attività investigativa non ripetibile, possono essere allegate al relativo verbale e inserite nel fascicolo per il dibattimento: parimenti, sarebbero inquadrabili tra le prove atipiche, subordinate ad autorizzazione motivata dell'autorità giudiziaria e alla disciplina dell'art. 189 c.p.p., le videoregistrazioni in ambienti in cui è garantita l'intimità e la riservatezza, ma non riconducibili alla nozione di domicilio[62].

Tuttavia l'art. 189 c.p.p. è riferibile soltanto alla fase dibattimentale e comunque non pare applicabile ai mezzi di ricerca della prova, in quanto richiede , come rilevato , l'intervento del giudice.

Rappresenta, quindi, un aggiramento delle regole sostenere che l'esecuzione delle riprese visive lascia impregiudicata la questione sull'ammissibilità della prova (sulla

[62] Cass., sez. un., 28 marzo 2006, Prisco, in Cm. *pen.,* 2006, p. 3937: nella decisione si è anche ritenuto che le videoregistrazioni in luoghi pubblici ovvero aperti o esposti al pubblico, non effettuate nell'ambito del procedimento penale, vanno incluse nella categoria dei documenti di cui all'art 234 c.p.p. e che le riprese video di comportamenti non comunicativi non sono ammesse nel domicilio, in quanto lesive dell'art.14 Cost.,e non possono quindi venire utilizzate, poiché, essendo prove illecite, non trova applicazione la disciplina prevista dall'art.189 c.p.p.. Si veda in materia il disegno di legge AS 1512, approvato dalla Camera il 17 luglio 2007.

quale dovrà pronunciarsi il giudice del dibattimento) e sulla determinazione dello strumento (perizia o mera riproduzione) che dovrà essere utilizzato per visionare le immagini acquisite.

Inoltre, la asserita inclusione tra le prove atipiche delle videoregistrazioni in ambienti in cui è garantita la intimità e la riservatezza si pone in contrasto con i princìpi affermati dalla Corte costituzionale, secondo i quali questa ipotesi può essere disciplinata soltanto dal legislatore, nel rispetto delle garanzie stabilite dall'art. 14 Cost.

Successivamente è stato anche deciso che le video riprese in luoghi pubblici effettuate al di fuori delle indagini preliminari non possono essere classificate come prove atipiche *ex* art . 189 c.p.p., ma devono essere qualificate documenti e possono diventare prove documentali da utilizzare come tali nel processo.

VII. LE CTU E LE ANALISI INFORMATICHE

1. IL CONSULENTE TECNICO

Il codice di procedura penale dedica alla perizia ed alla consulenza tecnica un limitato numero di norme, per lo più contenute negli artt. 220 e seguenti (Libro III, dedicato alle Prove, Titolo II dedicato ai Mezzi di prova ed infine Capo VI, intitolato semplicemente "Perizia").

Bisogna fare distinzione fra i termini 'perizia' e 'consulenza'. Entrambi si riferiscono al medesimo mezzo di prova, consistente in indagini, accertamenti e valutazioni di natura tecnica.

Il Giudice, il Pubblico Ministero e le altre parti del processo penale possono disporne discrezionalmente quando ciò appaia loro necessario, in ambiti nei quali siano richieste *specifiche competenze tecniche, scientifiche o artistiche*. (come si legge nell'art. 220 c.p.p.)

Tuttavia, mentre il perito è nominato dal Giudice (e, dunque, tale nomina si collocherà, sovente, nella fase del giudizio, che è successiva a quella delle indagini preliminari), il consulente è nominato dalle parti del processo penale, cioè dal Pubblico Ministero, dall'imputato o dalla persona offesa dal reato (parte civile, successivamente all'esercizio dell'azione penale).

Il consulente tecnico è definito organo giudiziario, ma si distingue dal giudice perché la sua non è mai attività decisoria, limitandosi ad esprimere pareri, a raccogliere notizie, ad effettuare verifiche.

La denominazione adottata dal legislatore nel 1942 ha voluto porre in risalto due concetti:

a) la persona designata quale ausiliare del giudice non è chiamata a decidere al posto del giudice o insieme al giudice, ma deve soltanto consigliarlo adoperando le conoscenze, le nozioni, la dottrina di cui è particolarmente fornita ed in relazione e per le quali è stata inserita nel processo;

b) la persona designata deve essere una persona fornita di particolari cognizioni tecniche nella materia di cui si discute.

Per il C.T.U. il rapporto con il processo è originato da un provvedimento giudiziario . Ecco perché questi ausiliari vengono anche definiti incaricati giudiziari: a seguito e per effetto del provvedimento dell'organo giudiziario, il privato cittadino viene incaricato temporaneamente di un pubblico ufficio.

La funzione specifica e naturale della consulenza è quella di fornire al giudice valutazioni o apprezzamenti per questioni che comportino specifiche conoscenze in materie extragiuridiche[63], di aiutare il giudice nella valutazione degli elementi acquisiti o nella soluzione di questioni che comportino specifiche conoscenze[64] e di sciogliere dubbi di natura tecnica[65].

[63] Cass. sez. I, 8.3.1977, n. 945; Cass. sez. Il, 30.1.2003, n. 1512

[64] Cass. sez. IIl, 26.2.2003 , n. 2887; Cass.sez.II. 30.5.2007, n. 12695

[65] È viziata la sentenza di merito che ponga a fondamento della decisione unicamente le rìsultanze della perizia d'ufficio, facendo proprie le conclusioni del consulente che, avvenendo a questioni giuridiche e all'esistenza di usi e consuetudini, non possono formare oggetto di indagine tecnica. (Cass. sez. Il, 16.1.1995, n. 405, FP, 1995, I, 167).

Il C.T.U. ha la qualità di pubblico ufficiale e, pertanto, l'atto da lui redatto, il quale attesta che a lui sono state rese informazioni, fa fede fino a querela di falso[66] .

Più precisamente riguardo alla parte cronistica il documento redatto dal consulente fa fede fino a querela di falso, mentre vanno distinti tutti gli aspetti valutativi, generali o particolari, implicanti l'attività intellettiva dello stesso, oggetto di libero convincimento da parte del giudice.

Non può prestare l'ufficio di perito, a pena di nullità, chi versa in particolari condizioni espressamente elencate dalla legge.

Sono esclusi il minorenne, l'interdetto, l'inabilitato e chi è affetto da infermità di mente; analogamente è escluso chi è interdetto anche temporaneamente dai pubblici uffici ovvero è interdetto o sospeso dall'esercizio di una professione o di un'arte .

Questa serie di casi configura una sorta di incapacità legale, che è comprensiva del caso di chi è sottoposto a misure di sicurezza personali o a misure di prevenzione.

Ancora, è escluso chi ha la facoltà di astenersi dal testimoniare o chi è chiamato a prestare ufficio di testimone o di interprete.

Queste esclusioni rinnovano il principio generale della netta separazione tra le funzioni di tecnico e di testimone, già esistente nel passato regime giudiziario.

Una precisa norma di legge stabilisce che non può prestare l'ufficio di perito e di C.T.U. chi non può essere assunto come testimone.

La scelta del perito è riservata all'apprezzamento del giudice e non è sindacabile in sede di legittimità[67].

[66] Cass. sez. III, 10.8 .2004, n. 15411
[67] Cass. sez. III, 30.3.2010, n. 7622

Tale discrezionalità del giudice di merito si estende anche alla categoria professionale di appartenenza del consulente e alla competenza del medesimo a svolgere le indagini richieste[68] .

2. LA SCELTA DEL CONSULENTE TECNICO

2.1 L'ALBO DEI PERITI E C.T.U.

I consulenti tecnici di ufficio vengono scelti normalmente tra quelli iscritti negli appositi albi istituiti presso ogni Tribunale.

L'albo è tenuto dal presidente del Tribunale ed è costituito da un comitato presieduto dal medesimo e formato dal procuratore della Repubblica e da delegati degli ordini e collegi professionali.

L'albo è suddiviso, per lo meno, nelle seguenti categorie ancorché possa contenere ulteriori sottocategorie corrispondenti a diverse specializzazioni: medico/chirurgica, industriale, commerciale, agricola, bancaria e assicurativa.

Il comitato, come riconosciuto dalla Suprema Corte di Cassazione, pur operando in ambito giurisdizionale, ha funzioni meramente amministrative[69].

Possono ottenere l'iscrizione nell'albo i possessori di specifiche competenze tecniche in una determinata materia, sono di specchiata condotta morale e sono iscritti alle rispettive associazioni professionali.

Sulle domande di iscrizione decide il comitato sopra menzionato.

---

[68] La decisione di affidare l'incarico ad un professionista (nella specie, geometra) iscritto ad un albo diverso da quello competente per la materia al quale si riferisce la consulenza (nella specie , ingegneri), ovvero non iscritto in alcun albo professionale, non è censurabile in sede di legittimità e non richiede specifica motivazione. (Cass. sez. III, 12.3.2010, n. 6050).

[69] I comitati previsti dagli artt.. 14 e 15 disp. atti c.p.c. hanno natura di organi amministrativi e non giurisdizionali e, pertanto, avverso le loro deliberazioni non è proponibile il ricorso per Cassazione ex art.111. (Cass. sez. U., 21.5.1998, n. 460).

La competenza tecnica, per poter essere considerata "speciale", deve derivare non solo dal titolo di studio acquisito, dall'appartenenza a una categoria o dallo svolgimento di un'attività professionale, ma soprattutto dall'acquisizione di titoli di specializzazione specifica e da percorsi di formazione particolari.

Maggiori restrizioni vengono poste relativamente alla condotta morale: il riferimento della norma è da leggersi come generale condotta morale e quindi costituiscono condizioni limitanti non solo i casi di condanne penali, ma anche l'irrogazione di sanzioni disciplinari e amministrative per fatti non inerenti l'incarico di C.T.U., ma che possono comunque incidere sull'esercizio della professione e che denotano spregio della legalità o mancanza di senso civico. È in ogni caso compito del comitato valutare la situazione particolare in relazione alle singole circostanze .

Il requisito dell'iscrizione nell'albo professionale vale ovviamente solo per quelle categorie organizzate in ordini e collegi (architetti, ingegneri, commercialisti, geometri, periti industriali ecc.). Al consulente non è consentito essere iscritto in più di un albo.

Per richiedere l'iscrizione è necessario presentare domanda al presidente del Tribunale corredata da alcuni documenti che, a titolo esemplificativo, sono: estratto dell'atto di nascita, certificato generale del casellario giudiziario, certificato di residenza, certificato di iscrizione all'ordine, titoli e/o documenti che il richiedente intende esibire per dimostrare la propria competenza nella materia.

Alcuni di questi documenti possono oggi essere autocertificati (D.P.R. 28.12.2000 n. 445).

2.2 LA VIGILANZA SUI CONSULENTI TECNICI

Sui consulenti tecnici e periti nell'adempimento delle proprie funzioni gravano tre tipi di responsabilità: disciplinare, penale e civile. In questa sede ci si sofferma soltanto sulla prima.

La vigilanza sui consulenti tecnici è esercitata dal presidente del Tribunale, il quale, d'ufficio o su istanza del procuratore della Repubblica o del presidente dell'associazione professionale, può promuovere procedimento disciplinare.

L'attività di vigilanza è esercitata sui seguenti aspetti:

1) il consulente non ha tenuto una "condotta morale specchiata", e si fa riferimento alle condanne penali o civili, nonché all'irrogazione di sanzioni disciplinari e amministrative per fatti anche non inerenti l'incarico di C.T.U., ma che possono incidere sull 'esercizio della professione o comunque denotare in chi le ha subite spregio della legalità o mancanza di senso civico;

2) il consulente non ha ottemperato agli obblighi derivanti dall'incarico ricevuto, come per esempio: rifiuto ingiustificato di prestare il proprio ufficio, mancata comparizione all'udienza per il giuramento senza giustificato motivo, mancato deposito della relazione nel termine assegnato e senza giustificato motivo, mancato avviso alle parti dell'inizio delle operazioni peritali, aggravato dalla necessità del rinnovo della consulenza, negligenza o imperizia nell'espletamento dell'incarico.

In tema di consulenza tecnica d'ufficio, se il giudice affida al consulente il semplice incarico di valutare fatti già accertati o dati preesistenti, la funzione del consulente è deducente e la sua attività non produrrà prova.

Se invece al consulente è conferito l'incarico di accertare fatti non altrimenti accertabili che con l'impiego di tecniche particolari, il consulente è percipiente, e la

consulenza costituisce fonte diretta di prova ed è utilizzabile al pari di ogni altra prova ritualmente acquisita al processo (Cass. sez Il, 12.1.2011, n. 518 , *Dejure-Giuffrè).*

2.3 NOMINA DEL C.T.U.

Il giudice ha un'assoluta discrezionalità nel disporre la consulenza tecnica d'ufficio[70]. Di regola il C.T.U. viene nominato durante la fase istruttoria.

Non di rado, tuttavia, si verifica che, pur essendo ancora in corso le indagini preliminari, si renda necessario ricorrere alla perizia.

Ciò avviene nelle forme dell'*incidente probatorio* (disciplinato dagli artt. 392 e seguenti c.p.p.), con nomina di un perito, da parte del Giudice per le indagini preliminari.

Questo comporta un'eccezionale anticipazione dell'istruttoria processuale, non essendosi ancora concluse le indagini dirette dal Pubblico Ministero e si verifica soltanto se l'accertamento di natura tecnica riguardi persone, cose o luoghi soggetti a modificazione non evitabile (ad esempio una autopsia)

La formulazione corretta e precisa dei quesiti da sottoporre al C.T.U. risulta essere fondamentale per avere una consulenza che risponda in modo idoneo ed approfondito alle problematiche tecniche sottese al procedimento.

[70] In materia di procedimento civile, la consulenza tecnica d'ufficio non costituisce normalmente un mezzo di prova, ma è finalizzata all'acquisizione, da pane del giudice, di un parere tecnico necessario , o quanto meno utile, per la valutazione di elementi probatori già acquisiti o per la soluzione di questioni che comportino specifiche conoscenze. La nomina del consulente rientra quindi nel potere discrezionale del giudice , che può provvedervi anche senza alcuna richiesta delle parti, sicché ove la pane ne faccia richiesta non si tratta di un'istanza istruttoria in senso tecnico ma di una mera sollecitazione rivolta al giudice affinché questi , avvalendosi dei suoi poteri discrezionali , provveda al riguardo; ne consegue che una tale richiesta non può mai considerarsi tardiva, ancorché formulata dalla pane tardivamente costituitasi in giudizio (Cass. sez. lav., 21.4.2010, n. 9461, GeM , 2010,4, 574).

Quesiti posti scorrettamente possono condurre a C.T.U. insoddisfacenti, idonee a loro volta a condizionare la sentenza.

Anche un'ampiezza eccessiva dei quesiti può essere deleteria, esponendo le parti a costi spropositati di C.T.U..

In casi particolari può essere nominato più di un consulente soltanto.

Il C.T.U. ha l'obbligo di essere presente all'udienza fissata per il giuramento.

Sempre alla stessa udienza il giudice fissa il termine entro il quale la consulenza tecnica deve essere depositata.

Nell'udienza civile durante l'assegnazione dell'incarico il giudice può assegnare al C.T.U. un fondo spese che pone a carico di una delle parti, di tutte le parti in quote uguali, oppure a carico solidale delle parti. (ciascuna parte è tenuta a garantire l'intero pagamento)

Le parti hanno la facoltà (non l'obbligo) di nominare un proprio consulente tecnico che affiancherà il C.T.U. durante le operazioni peritali.

Il C.T.P. può essere nominato dai legali in udienza oppure prima dell'inizio delle operazioni peritali nei termini stabiliti dal giudice.

Ricevuto l'incarico, il C.T.U. consulta il fascicolo dei legali e firma il verbale per accettazione dell'incarico.

Per quanto attiene il numero dei periti che il Giudice può nominare, l'art. 221 c.p.p. non prevede un limite.

Un limite numerico, invece, è imposto alle parti del processo penale dagli artt. 225 e 233 c.p.p..

In particolare l'art. 225 c.p.p. presuppone che vi sia stata la nomina di uno o più periti da parte del Giudice e, in tal caso, il Pubblico Ministero e le parti private potranno nominare propri consulenti, in numero non superiore a quello dei periti.

L'art. 233 c.p.p., invece, nell'ipotesi che il Giudice non abbia disposto alcuna perizia, impone al Pubblico Ministero ed alle altre parti di non nominare più di due consulenti tecnici.

Le norme richiamate sembrano riferirsi, esclusivamente, alla fase del giudizio e non anche a quella delle indagini preliminari.

L'art. 227 c.p.p. prevede che il perito, appena nominato, proceda immediatamente ai necessari accertamenti e risponda ai quesiti postigli altrettanto celermente, fornendo un parere che verrà raccolto nello stesso verbale con il quale gli è stato conferito l'incarico.

Tuttavia, nella prassi ciò non accade, poiché, anche per accertamenti tecnici non particolarmente complessi, i Giudici ed i Pubblici Ministeri concedono al perito od al consulente tecnico un termine, non superiore a novanta giorni (limite imposto dal codice e prorogabile), per rispondere, con una relazione, ai quesiti posti.

3. LA COMPETENZA DEL C.T.U.

Il giudice deve in primo luogo tener conto della competenza specifica del consulente, in relazione alla questione oggetto della consulenza[71].

Quando le indagini e le valutazioni risultano di notevole complessità ovvero richiedono distinte conoscenze in differenti discipline, il giudice affida l'espletamento della perizia a due o più consulenti.

Alcuni casi di nomina di un *collegio peritale* potrebbero essere necessari:

[71] Cass. 24 .2.1983, n. 1428

- quando vi sia una particolare complessità del caso da analizzare
- quando vi sia un'enorme mole di dati da elaborare
- laddove sia necessario, nell'ambito della medesima materia di competenza, coinvolgere soggetti con un elevatissimo livello di specializzazione

Frequentemente i C.T.U., nello svolgimento del proprio mandato, sono costretti ad avvalersi dell'opera di collaboratori; costoro sono chiamati a svolgere ordinariamente incombenze materiali in veste di ausiliari, ma la loro attività deve svolgersi comunque e sempre sotto il controllo del consulente, in quanto unico titolare della perizia e unico responsabile nei confronti del giudice.

Nell'eventualità che il C.T.U. si renda conto che per l'espletamento dell'incarico sono richieste attività specialistiche che esulano dalle proprie competenze, chiede al giudice l'autorizzazione ad avvalersi di un ausiliario e alla conseguente spesa.

Recenti decisioni hanno confermato che il consulente tecnico d'ufficio può comunque avvalersi dell'opera di specialisti al fine di acquisire, mediante gli opportuni e necessari sussidi tecnici, tutti gli elementi di giudizio, senza che sia necessaria una preventiva autorizzazione del giudice, né una nomina formale, purché egli assuma la responsabilità morale e giuridica dell'accertamento e delle conclusioni raggiunte dal collaboratore[72].

L'autorizzazione all'ausilio di terzi esperti è necessaria ai soli fini del rimborso delle spese sostenute dal C.T.U., mentre egli resta libero di servirsi di ausiliari, ove se ne assuma l'onere.

Possono partecipare alle operazioni peritali solo i C.T.P. nominati, i legali e le parti coinvolte.

[72] Cass. sez. lll, 29.3.2006 , n. 7243

Il C.T.U. non può fondare le proprie conclusioni su fatti o circostanze non ritualmente dedotti e provati nel giudizio: gli elementi sui quali fonda il proprio giudizio debbono essere i medesimi sui quali il giudice potrebbe fondare la propria sentenza[73].

I difensori e i consulenti di parte possono sottoporre al C.T.U. osservazioni e istanze che, pur non dovendo essere necessariamente trascritti nella relazione, devono costituire oggetto di adeguata valutazione da parte del consulente d'ufficio[74].

Documenti eventualmente prodotti dalle parti al di fuori dei canali tipici non possono essere utilizzati dal giudice, e quindi neanche dal C.T.U.

Deve perciò ritenersi errata la prassi di alcuni C.T.U. di accettare, esaminare e porre a fondamento della relazione la documentazione che l'avvocato, o talora la stessa parte sostanziale del processo, consegni loro *brevi mani,* al momento delle indagini peritali.

Tale prassi è scorretta perché impedisce la possibilità di un effettivo contraddittorio sul documento consegnato al C.T.U.

La Cassazione recentemente ha statuito:

Nell'ambito della consulenza tecnica si deve escludere, a prescindere dal consenso della controparte, l'ammissibilità della produzione tardiva di prove documentali concernenti fatti e situazioni poste direttamente a fondamento della domanda e delle eccezioni di merito. potendo il consulente tecnico esaminare documenti ulteriori solo se meramente accessori, cioè utili a consentire una risposta più esauriente ed approfondita al quesito posto dal giudice[75].

---

[73] Cass. sez. III, 10.5.2001, n. 6502
[74] Cass. sez. Il , 14.2.1994, n. 1459
[75] Cass. sez, I, 2.12.2010, n. 24549

Il C.T.U., quando svolge le sue indagini da solo, cioè senza presenza del giudice , può compiere tutti gli accertamenti che siano collegati con l'oggetto della perizia e, conseguentemente, legittimamente utilizzare i documenti cosi acquisiti.

L'assunzione di informazioni da terzi da parte del consulente è subordinata all'autorizzazione del giudice e l 'esercizio di questa facoltà incontra soltanto tre condizioni:

a) le notizie acquisite da terzi debbono concernere fatti e situazioni relativi all'oggetto della relazione;

b) l'acquisizione presso terzi deve essere necessaria per espletare convenientemente il compito affidato al C.T.U.[76];

c) nella relazione il C.T.U. deve indicare le fonti del proprio accertamento[77].

la Cassazione ha stabilito che il C.T.U. possa acquisire da terzi non già qualsiasi informazione, ma soltanto le informazioni "strettamente necessarie per rispondere al quesito tecnico postogli dal giudice, per le quali, peraltro, parte della giurisprudenza ritiene che non sia neppure necessaria un'espressa autorizzazione del giudice, dovendo detta autorizzazione ritenersi ricompresa implicitamente nel mandato"[78].

4. IL PROCESSO VERBALE

Il C.T.U. redige di regola processo verbale delle proprie attività di sopralluogo, di accesso presso gli uffici e in generale delle operazioni peritali.

[76] Cass. Sez, I, 7.11.1989, n. 4644
[77] Cass. sez. lll , 6.11 .2001 , n. 13686
[78] Cass. sez. Ill, 10.5.2001 , n. 6502

Nella pratica il giudice demanda costantemente al consulente ogni attività d'indagine e di sopralluogo con la conseguenza formale che il C.T.U. potrebbe omettere la redazione del processo verbale delle operazioni.

In realtà, la prassi ha suggerito comunque la compilazione del verbale, il quale normalmente ha il seguente contenuto:

1) ora, data e luogo dello svolgimento delle operazioni;

2) soggetti presenti;

3) eventuale autorizzazione ricevuta per l'accesso ai luoghi;

4) attività compiute;

5) documenti acquisiti;

6) osservazioni ed istanze delle parti;

7) conclusioni ed esito al quesito posto.

La redazione del processo verbale permette dunque l'esplicarsi del pieno contraddittorio fra le parti, l'ammissione alle attività dei soli soggetti autorizzati, la correttezza dell'acquisizione documentale e l'eventuale registrazione delle istanze e delle osservazioni delle parti, nonché la fissazione del prosieguo delle attività peritali.

Inoltre, il processo verbale, soprattutto per gli incarichi più complessi e che si sviluppano su un ampio arco temporale, è utile per programmare gli accertamenti e le ispezioni che si intendono compiere, registrare le diverse operazioni e le verifiche svolte e per riportane le risultanze.

Rappresenta, quindi, un documento mediante il quale si illustra la cronologia delle attività condotte con allegazione alla relazione e richiamo nell'apposito paragrafo delle operazioni peritali.

Tuttavia non è consigliabile che il processo verbale diventi una vera e propria «relazione peritale» con commenti, analisi degli accertamenti, scambi di osservazioni articolate e, magari , risposte, seppur sintetiche, in ordine ai quesiti posti , in quanto non sarebbe funzionale al compimento corretto dell'incarico.

Il processo verbale è un atto pubblico ed essendo redatto da un pubblico ufficiale fa piena prova fino a querela di falso e deve essere sottoscritto da tutti i presenti e l'eventuale rifiuto di firma va segnalato dal consulente mediante specifica indicazione. Così non è per la relazione di consulenza[79].

Se il C.T.U. si rende conto che le operazioni peritali non possono essere concluse nei termini stabiliti, prima della scadenza deposita motivata istanza al giudice per richiedere la proroga del termine di deposito della relazione di consulenza tecnica, proroga che in genere il giudice concede.

Il c.t.u . deve avere cura di non compiere valutazioni di tipo giuridico e di non interpretare e valutare prove documentali, in quanto giudizio riservato esclusivamente al giudice[80].

Viceversa, tra gli esami che il C.T.U. non può assolutamente omettere rientra l'esame dei luoghi o delle persone[81].

---

[79] La querela di falso è necessaria, a tutela della pubblica fede, solo per togliere a un documento l'idoneità a far fede e servire quale prova di determinati atti o rapporti, per cui essa non è ammissibile né necessaria in relazione a un ano, quale la relazione del C.T.U . ai sensi dell'art. 195 c.p.c., in cui vengono soltanto trasfusi i risultati delle indagini tecniche dallo stesso compiute. Tale relazione non fa pubblica fede riguardo agli apprezzamenti, rilievi e accertamenti in essa contenuti, non rivestendo affatto alcun carattere di prova assoluta o privilegiata, ma anzi essendo soggetta, come tutti gli altri mezzi di prova, al libero e discrezionale apprezzamento da pane del giudice. Mentre il verbale redatto dal C.T.U. , in relazione alla qualità di pubblico ufficiale da questi rivestita, costituisce atto pubblico anche riguardo ai fatti che il consulente asserisce essersi verificati in sua presenza, per cui nei suoi confronti deve ritenersi astrattamente esperibile il rimedio della querela di falso, questa invece non è ammissibile contro il contenuto della consulenza tecnica, che non fa pubblica fede delle affermazioni o constatazioni o giudizi in essa contenuti. (Cass. sez. Il, 24.5.2007, n. 12086, GDir, 2007, 38, 59).

[80] Cass. sez. IIl, 22.7.1993, n. 8206

[81] Cass. sez. lav., 28.7.1994, n. 7036

Il C.T.U. non è tenuto a eseguire gli accertamenti sollecitati dal consulente di parte , in quanto egli è vincolato unicamente ai quesiti postigli dal giudice.

La consulenza redatta dal C.T.U. deve attenersi strettamente ai quesiti, evitando:

1) da un lato, di dilungarsi su questioni irrilevanti ai fini della risposta al quesito.

2) dall'altro, il silenzio, vale a dire il non affrontare questioni essenziali ai fini della risposta al quesito. Ove al C.T.U. sia chiesto di descrivere luoghi, cose o persone, la descrizione deve essere sempre accurata e dettagliata, e corredata da adeguata documentazione fotografica o da riprese video. La parte descrittiva deve essere sempre graficamente ben evidenziata e separata dalla eventuale parte valutativa. Ove la relazione contenga una pane valutativa, il c.t.u, avrà cura di motivare sempre le proprie conclusioni, descrivendo *l'iter* logico seguito.

Idealmente, ogni relazione di consulenza va divisa in quattro parti:

a) una parte epigrafica, nella quale il C.T.U. indica gli estremi della causa, del giudice e riassume le operazioni compiute: inizio operazioni, sopralluoghi, accessi, proroghe concesse, esito del tentativo di conciliazione ove previsto;

b) una parte descrittiva, nella quale il C.T.U. illustra gli accertamenti o le ricostruzioni in fatto da lui personalmente compiuti;

c) una parte valutativa, nella quale il C.T.U. risponde ai quesiti motivando adeguatamente le proprie scelte.

d) una pane riassuntiva, nella quale il C.T.U. espone in forma sintetica la risposta ad ogni quesito affidatogli.

E' molto importante che la relazione di consulenza sia redatta in modo intelligibile evitando l'abuso di espressioni tecniche. Ove possa aiutare nell'esposizione dei fatti o delle valutazioni, è raccomandato l'impiego di grafici, illustrazioni, tabelle, ovvero

qualsiasi accorgimento in grado di meglio illustrare il contenuto della relazione stessa .

5. LA RILEVANZA DELLA C.T.U. NELLA SENTENZA DEL GIUDICE

Nel nostro ordinamento vige il principio *judex peritus peritorum,* in virtù del quale è consentito al giudice disattendere le argomentazioni tecniche svolte nella propria relazione dal C.T.U.: e ciò sia quando le argomentazioni stesse siano intimamente contraddittorie, sia quando il giudice le sostituisca con altre argomentazioni, tratte da proprie personali cognizioni tecniche ; in ambedue i casi, l'unico onere incontrato dal giudice è quello di un'adeguata motivazione, esente da vizi logici ed errori di diritto[82].

Ove il giudice, ritenendole valide, aderisca alle conclusioni del C.T.U., non avrà l'obbligo di motivare la propria adesione a tali conclusioni, essendo sufficiente che indichi le fonti del proprio convincimento.

Nell'ipotesi in cui il giudice intenda invece disattendere le conclusioni del C.T.U., ha l'obbligo di motivare il proprio dissenso.

Deve, cioè, contrapporre nozioni ed apprezzamenti tecnici a quelli affermati dal C.T.U., per dimostrarne l'inattendibilità sul piano scientifico.

Il giudice di legittimità ha tuttavia affermato l'opportunità che il giudice di merito, in questi casi, provveda innanzitutto a chiedere chiarimenti al consulente, oppure a rinnovare le indagini[83].

[82] Il giudice del merito, in virtù del principio del libero convincimento, ha facoltà di apprezzare in piena autonomia rutti gli elementi presi in esame dal consulente tecnico e le considerazioni da lui espresse che ritenga utili ai fini della decisione. (Cass. sez. III, 9.3.20 10, n. 5658).

[83] Cass. 6.6.1985, n. 3384

Il dissenso dall'operato del C.T.U. è stato ritenuto adeguatamente motivato quando, nella sentenza:

a) viene posta in luce una manifesta discordanza, sul piano della logica, tra gli accertamenti eseguiti e le conseguenze che il consulente intende trarne;

b) viene dimostrato, con convincente motivazione, che alle indagini del C.T.U. non può essere riconosciuta sicura efficacia scientifica[84] .

Motivare il dissenso in modo convincente ed adeguato vuol dire pertanto che il giudice deve far emergere l'errore logico compiuto indicandone il vizio metodologico e fornendo per contro i dati dai quali abbia tratto il proprio diverso convincimento. Inoltre il giudice ha l'onere di dimostrare, in motivazione, di aver tenuto in debito conto pur nel suo contrario apprezzamento - gli accertamenti e le valutazioni tecniche compiuti dal C.T.U.

6. IL RAPPORTO TRA CTU E AUTORITA' GIUDIZIARIA

Il rapporto che si instaura fra il consulente tecnico ed il Pubblico Ministero, all'apparenza semplice, si rivela, in realtà, il più delle volte, particolarmente complesso.

Deve considerarsi, innanzitutto, che il P.M. procede alla nomina del consulente, nel corso delle indagini preliminari, cioè in una fase nella quale poco o nulla è dato sapere, inizialmente, in ordine ai fatti oggetto di investigazione (è possibile, ad

[84] Le valutazioni espresse dal C.T.U. non hanno efficacia vincolante per il giudice, il quale può legittimamente dissuaderle attraverso una valutazione critica che, tuttavia, deve necessariamente essere ancorata alle risultanze processuali e risultare congruamente e logicamente motivata, dovendo indicare in particolare gli elementi di cui si è avvalso per ritenere erronei gli argomenti sui quali il consulente si è basato, ovvero gli elementi probatori , i criteri di valutazione e gli argomenti logico-giuridici per addivenire alla decisione contrastante con il parere dell'ausiliario (App . Roma sez. ili , 6.4.2010, n. 1433, GDir, 20 10, 22, 72) .

esempio, che manchino dei potenziali testimoni, o che questi, pur essendoci, non sia stato – ancora - possibile identificarli o reperirli).

Non di rado, quindi, il P.M. dovrà, per così dire, resistere alla forte tentazione di trasformare il proprio consulente tecnico in un – sia pur qualificatissimo – ufficiale di polizia giudiziaria, al quale, in sostanza, delegare lo svolgimento delle prime (e non solo le *prime*) indagini.

I consulenti non sono – e, dunque, non devono mai diventare – organi di polizia giudiziaria.

Ciò anche perché essi sono chiamati a compiere accertamenti, all'esito dei quali dovranno esprimere delle valutazioni (al contrario degli appartenenti alla polizia giudiziaria, i quali possono compiere i necessari accertamenti su tracce e cose che potrebbero subire alterazioni, ma non devono mai esprimere valutazioni tecnico-scientifiche: si pensi alle analisi ricognitive, e non valutative, che la polizia giudiziaria può effettuare in ordine alla natura della sostanza che si ritenga stupefacente).

E' tale profilo valutativo (soprattutto) che, in senso squisitamente tecnico-giuridico, avuto riguardo alla disciplina del processo penale (specialmente nella prospettiva dell'esame che avrà luogo nel dibattimento), distingue il consulente sia dall'appartenente alla polizia giudiziaria che dai testimoni.

I termini stessi con i quali il P.M. (lo stesso, per il vero, vale per il Giudice ed i suoi periti) formula i quesiti che verranno affidati ai consulenti tecnici dovranno essere precisi e, quel che più conta, dovranno porre quegli esperti in condizione di rispondere ad essi, attraverso valutazioni esclusivamente tecniche.

E' possibile (e *lecito*), invece, che al consulente venga richiesto di richiamare ed interpretare norme tecniche o, al limite, norme giuridiche dal prevalente contenuto tecnico (si pensi, ad esempio, alla definizione di esposizione quotidiana personale di un lavoratore al rumore, contenuta nell'art. 39 del D.L.vo n. 277/91, espressa con una formula matematica piuttosto complessa).

Il consulente, dal canto suo, dovrà resistere (anch'egli) alla tentazione di *trasformarsi in Pubblico Ministero* (o Giudice) od agente/ufficiale di polizia giudiziaria.

Non di rado, infatti, coloro che vengono incaricati di compiere accertamenti tecnici, non limitandosi ad esplicare un'attività di consulenza, culminante, quindi, in una valutazione critica, tendono a suggerire soluzioni propriamente giuridiche, indicando, ad esempio, più o meno *perentoriamente*, le norme che dovrebbero trovare applicazione nel caso da essi trattato.

7. LIQUIDAZIONE DEI COMPENSI

La liquidazione del compenso al C.T.U. è oggi disciplinata dagli artt. 49 e ss. d.p.r. 30.5.2002 n . 115 , i quali statuiscono i criteri generali di liquidazione e dal d .m . 30.5.2002 (pubblicato in G.U. 5.8.2002, n. 182), il quale fissa la misura degli onorari[85].

Gli onorari spettanti ai C.T.U. possono essere computati secondo tre modalità diverse:

a) onorari fissi: in questo caso, la misura del compenso è prevista in modo rigido dal regolamento, indipendentemente dal valore della controversia;

[85] La natura pubblicistica dell'incarico affidato al consulente tecnico di ufficio, esclude in ordine alla determinazione del compenso il rinvio ricettizio alle tariffe professionali, dettate per regolare i rapporti fra i professionisti ed i privati, sia pur compatibilmente con l'interesse generale. (Cass. sez. l, 23.9.1994, n. 7837, GeM, 1994, 1141).

b) onorari variabili: in questo caso , la misura del compenso è proporzionale al valore della controversia;

c) onorari a tempo (c.d. vacazionì): in questo caso, la misura del compenso è commisurata al tempo ragionevolmente occorrente per lo svolgimento dell'incarico.

Gli onorari fissi e quelli variabili sono previsti dal regolamento con riferimento alla consulenza in determinate materie, espressamente elencate.

Nella liquidazione a percentuale per scaglioni resta comunque insuperabile lo scaglione massimo previsto dal decreto, quand'anche il valore della causa sia superiore.

Il criterio di liquidazione a tempo, invece, è un criterio residuale: esso trova applicazione in tutte le ipotesi in cui per la materia oggetto della consulenza non è previsto dal regolamento un onorario *ad hoc,* ovvero quando sia "impossibile" l'applicazione dell'onorario fisso o variabile[86] (art . 1 alI. al d.m. 30.5.2002).

Nulla esclude che i compensi a tempo siano applicati anche quando la materia oggetto della consulenza sia prevista dal d.m. 30.5.2002, in tutti i casi in cui l'applicazione degli altri criteri porterebbe ad una liquidazione manifestamente iniqua per eccesso o per difetto rispetto all'impegno effettivamente profuso dal C.T.U. va ricordato che, ai sensi dell'ano29 d.m. 30.5.2002 , tutti gli onorari, se non diversamente stabilito , sono comprensivi sia della redazione della relazione, sia della partecipazione alle udienze, sia di ogni altra attività concernente ì quesiti. Per ottenere la liquidazione dei compensi, il C.T.U. ha l'obbligo di documentare tutti gli

[86] *La liquidazione a vacazioni è residuale : essa, cioè, può trovare applicazione* soltanto nei casi in cui la materia oggetto della consulenza non rientri in alcuna delle previsioni di cui al d.m. 30.5.2002.(Cass. su. II, 23.9.2010, n. 20088, 2010, 11,23).

esborsi sostenuti, allegando la documentazione relativa alla richiesta di liquidazione[87].

Sia gli onorari a tempo che quelli fissi o variabili, possono essere aumentati o ridotti. In particolare:

a) per i soli onorari fissi o variabili è consentita una variazione in aumento sino al 20%, nel caso di urgenza, a prescindere dalla difficoltà dell'incarico (art. 51,20 co., d.p.r. *115/2002);*

b) per tutti gli onorari è consentita una variazione in aumento sino al 100%, per le prestazioni di eccezionale importanza, complessità e difficoltà (an. 52, 10co., d.p.r. *11512002);*

c) per i soli onorari fissi e variabili è prevista la riduzione del 25% nel caso in cui il C.LU. ritardi ingiustificatamente il deposito della relazione; per i soli onorari a tempo non si tiene conto del tempo successivo alla scadenza del termine fissato dal giudice per il deposito della relazione, nel caso di ingiustificato ritardo del C.T.U.

La possibilità di aumentare fino al doppio i compensi liquidati al consulente tecnico d'ufficio costituisce oggetto di un potere discrezionale attribuito al giudice, che lo esercita mediante il prudente apprezzamento di pertinenti elementi di giudizio, quali la natura e l'importanza dei compiti di accertamento in fatto, il tempo e l'impegno profusi dall'ausiliare giudiziale.

[87] In tema di liquidazione del compenso al consulente tecnico d'ufficio, il principio di onnicomprensività dell'onorario sancito dal d.m. 30 maggio 2002 riguarda le attività complementari ed accessorie che, pur non essendo specificamente previste in sede di conferimento dell'incarico, risultano tutta via strumentali all'accertamento tecnico, e non trova applicazione in presenza di una pluralità di indagini non interdipendenti, che presuppongono necessariamente una pluralità di incarichi di natura differente, come nel caso di richiesta di rilievi topografici e planimetrici da un lato, e di attività di stima dei beni dall'altro che, in quanto previsti distintamente dagli art.12 e 13, comportano una liquidazione autonoma del compenso. (Cass. sez. lII, 25.3.2010 , n. 7174, GCM, 3, 433).

Peraltro, la semplice circostanza che il giudice abbia attribuito particolare rilevanza a livello quantitativo e qualitativo dell'opera di tale ausiliare al predetto specifico fine, non implica, di per sé, che della rilevanza debba anche considerarsi necessariamente di livello cosi elevato da giustificare, altresì. il superamento dei massimi già riconosciuti fino al raddoppio degli stessi.

In materia di compenso spettante al C.T.U., si tengano anche presenti gli ulteriori principi giurisprudenziali: non spetta al C.T.U. alcun compenso aggiuntivo per aver effettuato, dopo il deposito della relazione, un supplemento di indagini se tale supplemento è stato reso necessario dalle carenze della prima relazione[88].

Le spese sostenute dal C.T.U. nell'espletamento dell'incarico affidatogli dal giudice sono rimborsabili a prescindere da una specifica preventiva autorizzazione, quando secondo il prudente apprezzamento del giudice di merito siano necessarie ai fini delle indagini e dell'adempimento dell'incarico[89].

Nel caso in cui il consulente tecnico sia stato autorizzato dal giudice ad avvalersi dell'ausilio di altri prestatori d'opera per attività strumentale rispetto ai quesiti posti, la spesa relativa va inclusa tra quelle di cui il giudice dispone il rimborso a favore del consulente tecnico, potendosi procedere alla liquidazione di un autonomo compenso a favore dell'ausiliare solo quando il giudice abbia conferito a quest'ultimo uno specifico incarico, in considerazione dell'autonomia delle prestazioni al medesimo richieste.

Si ricorda, infine, che, avverso il decreto di pagamento emesso a favore dell'ausiliario del magistrato, il beneficiario e le parti processuali, compreso il pubblico ministero ,

[88] Cass. Sez. I,8.10.1997, n. 9761
[89] Cass. sez. II, 5.8.1992, n. 9293

possono proporre opposizione, entro venti giorni dall'avvenuta comunicazione, al presidente dell'ufficio giudiziario competente.

8. C.T.U E SPESE DI GIUSTIZIA NELLE INDAGINI PENALI

Un recente caso, di una controversia tra gli uffici di una Procura ed il consulente informatico del P.M., propone delle riflessioni sulla disciplina della liquidazione delle "spese di giustizia", quando la consulenza tecnica ha avuto come oggetto la estrapolazione di dati da supporti informatici mediante complesse operazioni, finalizzate a produrre delle "prove" da allegare al fascicolo, che risultino poi leggibili e valutabili dal giudice.

Accade ormai di frequente che, soprattutto in indagini su fenomeni ed organizzazioni di pedo-pornografia informatica e telematica (ma può accadere anche per altre tematiche), i magistrati richiedano al consulente tecnico una attività di estrapolazione di voluminosi files di dati e la loro interpretazione (conversione dei formati grafici dei files, loro "pulizia" dal c.d. rumore di fondo, ingrandimento delle immagini, rendering, ecc.), operazione che si svolge con totale compenetrazione tra *attività intellettuale* ed *attività tecnica-materiale*, come è tipico dei lavori informatici, cosicché viene meno la vecchia distinzione tra attività intellettuale svolta dal consulente ed operazioni materiali che egli può far svolgere da ausiliari e laboratori esterni, distinzione invece tipica delle consuete consulenze di ingegneria delle costruzioni, geologia, ecc.

In pratica risulta in tali "casi informatici" (ed anche in talune indagini in materia di terrorismo) indispensabile che il consulente disponga personalmente di materiali tecnici aggiuntivi (rispetto a quelli in dotazione alle Procura ovvero ai reparti di

Polizia Giudiziaria) ed in particolare di *hard disk* di eccezionale capienza, peraltro ormai di normale vendita e di costi molto più contenuti che nel recente passato, o addirittura di computer dotati di CPU di eccezionale velocità e di enorme RAM.

L'art. 56 del D.P.R. 115/2002 (nuovo T.U. sulle spese di giustizia) prevede la liquidazione al consulente – sulla base di fattura emessa dal terzo fornitore verso la persona fisica del consulente - del rimborso delle *spese sostenute* per l' adempimento dell' incarico, e al riguardo la prassi portava al pacifico riconoscimento delle indennità di viaggio, della stampa di fotografie, un tempo della battitura dattilografica della finale relazione (oggi scritta al computer dal consulente stesso) e di quant' altro rientrante nella normalità.

In tal caso un unico mandato di pagamento prevede l'erogazione della somma complessiva al consulente (onorario e rimborsi spese).

Quando esigenze tecniche specifiche di quell'incarico richiedano che il consulente disponga di *materiali di rilevante valore* (non rientranti tra i materiali di consumo tradizionalmente intesi) diviene difficile pretendere che il consulente *anticipi di tasca propria* i costi per l' acquisto di detti materiali, ovvero che riesca ad ottenerli con pagamento differito nel tempo ed emissione di fattura pro-forma da parte del venditore, che sarà pagato soltanto con la finale liquidazione del consulente, e proprio da quest' ultimo, al quale il P.M. riconoscerà il rimborso della spesa sostenuta.

Il rischio concreto per il P.M. è che, volendosi imporre al consulente *onerose anticipazioni di tasca propria*, talvolta di parecchie migliaia di euro (insomma: parecchi milioni di vecchie lire, per intenderci meglio), divenga impossibile ottenere con

urgenza la prestazione intellettuale del consulente specialistico ed anche impossibile ottenere poi – per l' allegazione al fascicolo – la disponibilità di quei costosi supporti magnetici di massa (hard disk da 1000-2000 Gb) che resteranno per sempre nel procedimento, e che quindi – a stretto rigore – non possono essere considerati materiali di consumo fungibili.

Ancor più rilevante può apparire, in pratica, il problema di ottenere la costosa fornitura di servizi da un ente di ricerca che disponga di un potentissimo super-calcolatore, servizi che prevedono un costo commisurato alle ore di utilizzo dell' apparato e degli addetti.

La soluzione del problema, per casi analoghi, ma non ovviamente in materia informatica, tradizionalmente escogitata ed applicata nella concreta prassi giudiziaria e non assoggettata a rilievi contabili (autorizzare la liquidazione sul Mod. 12 delle somme necessarie per l'acquisto dei detti materiali col titolo di *spese di somministrazione, con erogazione della somma direttamente al terzo fornitore*) trova una apposita testuale previsione nell' art. 70 del citato T.U. n. 115/2002, che – quale norma elastica di chiusura del sistema - prevede le *spese straordinarie*, affidando opportunamente al magistrato che procede uno strumento duttile ed atipico, nel senso che, con *provvedimento motivato*, adottato con le modalità degli artt. 61 e segg., *per quanto compatibili*, potranno risolversi quei problemi pratici sopra descritti, modulando la soluzione più appropriata, assicurando così al *servizio giustizia* le competenze tecniche indispensabili.

Resta evidente che *i materiali acquistati* – sulla base delle caratteristiche tecniche precisate dal consulente e con procedura a trattativa diretta, poiché per materiali di alta specializzazione tecnologica e con taluni limiti di importo non è obbligatorio

espletare gara di appalto (cfr. d.p.r. 18.4.1994, n. 573 e art. 13, lett.c) del d.lgs. 17.3.1995, n. 158)), i cui tempi procedurali, del resto, mai si conciliano con la speditezza delle indagini penali – *entrano nella proprietà della amministrazione giudiziaria*, così come lo sono le copertine dei fascicoli.

E' però evidente che, di regola, l'utilizzo di tali materiali (hard disk) si esaurirà con quel procedimento, a cui resteranno allegati per sempre, come supporto documentale informatico.

Il caso ipotetico e residuale, della possibilità – quando il procedimento sia definito - di un riutilizzo successivo dei materiali, si pensi ad es. a moduli di memoria aggiuntiva RAM, per finalità di servizio dell' Ufficio Giudiziario, potrà essere disciplinato con opportuni provvedimenti del magistrato, che al caso disporrà anche il loro inserimento nell' inventario degli strumenti informatici in dotazione, escludendo di conseguenza la ripetizione del relativo costo di acquisto a carico dell' imputato.

Dall' esame di questo nuovo tema di attualità, si ricava che, nella pratica giudiziaria, magistrati, funzionari e soggetti esterni chiamati a collaborare, dovranno aver maggior fiducia nella logica intrinseca dell' ordinamento e maggiore conoscenza delle disposizioni normative ed organizzative, in particolare di quelle che si collegano all' organizzazione amministrativa e contabile degli uffici giudiziari.

Tale fiducia e tale conoscenza sono i presupposti indispensabili per trovare nelle norme la soluzione ai "problemi", che sono più spesso apparenti che reali.

9. SPESE DI GIUSTIZIA PER CTU INFORMATICHE

La Procura Generale di Venezia, così come le Procure di Forlì e Ferrara, hanno gentilmente accolto la richiesta di collaborazione alla stesura della presente progetto di ricerca per affrontare il tema dei costi sostenuti per le consulenze tecniche di tipo informatico.

Nello specifico le singole procure del Veneto hanno fornito dati aggregati ed anonimi relativi al numero di consulenze tecniche informatiche e al totale delle somme liquidate per le stesse negli anni 2010 (Tab.1), 2011 (Tab.2) e 2012 (Tab.3).

Tab.1

	ANNO 2010	
	INCARICHI	LIQUIDAZIONI (€)
VENEZIA	29	28328,99
BELLUNO	6	2382,33
VICENZA	8	11811,52
TREVISO	6	31254,73
PADOVA	22	45505,55
BASSANO	1	1433,95
MINORI VE	0	0

Tab.2

	ANNO 2011	
	INCARICHI	LIQUIDAZIONI (€)
VENEZIA	35	74944,77
BELLUNO	2	907,14
VICENZA	14	19552,14
TREVISO	4	4947,68
PADOVA	19	51293,96
BASSANO	1	3748,17
MINORI VE	0	0

Tab. 3	ANNO 2012	
	INCARICHI	LIQUIDAZIONI (€)
VENEZIA	29	66585,55
BELLUNO	1	520,87
VICENZA	11	12289,61
TREVISO	4	9908,69
PADOVA	40	99017,23
BASSANO	0	0
MINORI VE	1	169,53

Dai dati emergono dati che potrebbero apparire scontati quali: il progressivo aumento dei conferimenti d'incarico per analisi informatiche (72 nel 2010, 75 nel 2011 e 86 nel 2012) un altrettanto progressivo aumento della spese liquidate nel totale (€ 120.717 nel 2010, € 155.393 nel 2011, € 188.491 nel 2012)

Nel corso del triennio considerato si è passati da un costo medio per CT di 1.676 euro nel 2010 ai 2.191 euro del 2012 passando per i 2.071 euro del 2011.

La Procura della Repubblica di Forlì ha risposto positivamente alla richiesta alla pari delle Procure venete e, nonostante il sistema d'inserimento delle prestazioni sia notevolmente diverso, emerge il dato di un totale liquidato nei tre anni studiati di 88.718 euro per 41 consulenze di natura informatica.

Da questa informazione emerge che a Forlì la spesa media per CT informatica è di € 2.164 importo assolutamente in linea con il dato emerso, in maniera aggregata, in Veneto.

Si elencano di seguito i dati forniti dalla Procura della Repubblica di Ferrara:

- nell'anno 2010 sono stati liquidati 13.965,24 euro per CT informatiche a fronte di una spesa totale per CT di 388.967,92 euro;

- nell'anno 2011 sono stati liquidati 4.790,74 euro per CT informatiche a fronte di una spesa totale per CT di 498.378,31 euro;
- nell'anno 2012 sono stati liquidati 10.630,40 euro per CT informatiche a fronte di una spesa totale per CT di 334.671,31 euro;

Deve far riflettere il fatto che le spese per Consulenze Tecniche Informatiche rappresentano solo l'1-2 % della spesa totale.

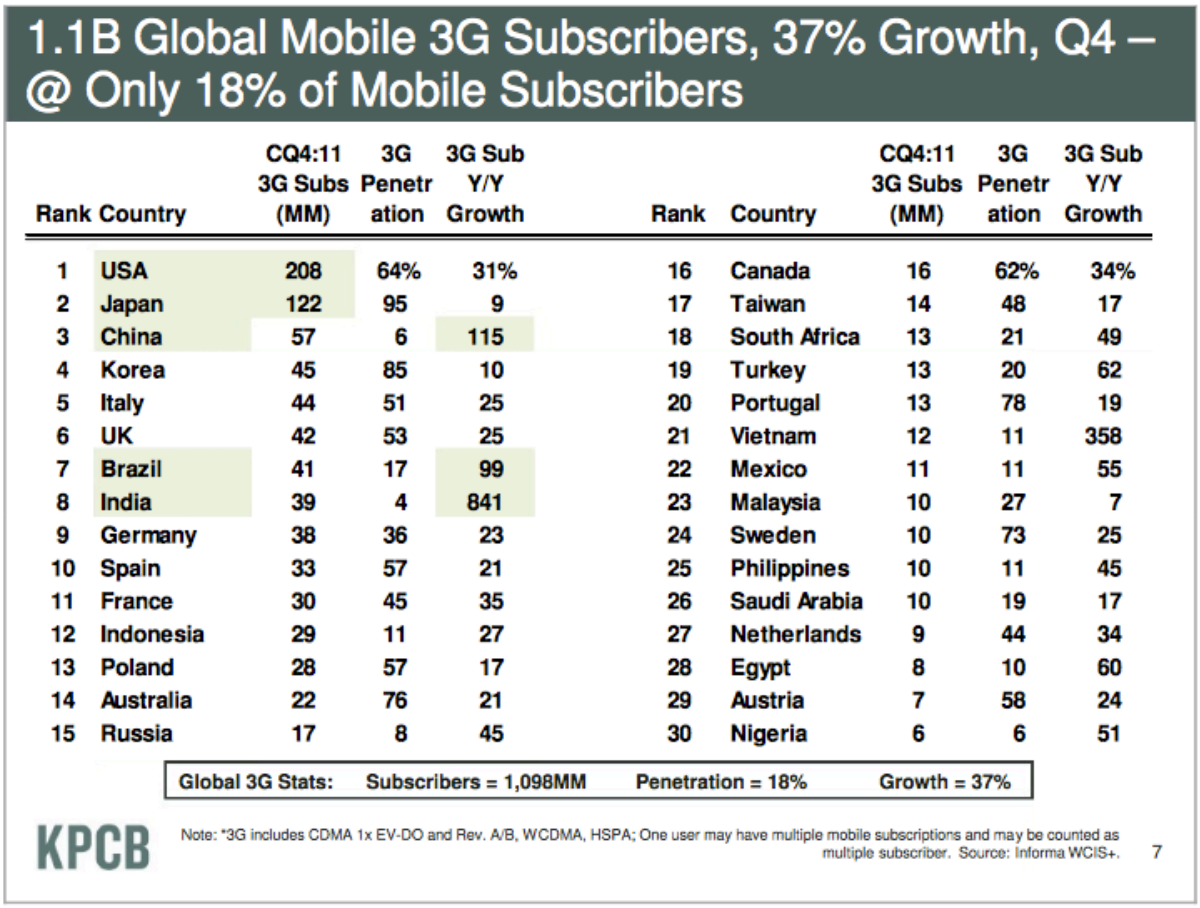
In un'epoca dove 41 milioni di italiani trascorrono in media da 1 a 2 ore al giorno su internet (Tab.4), 44 milioni di italiani posseggono un contratto di navigazione mobile in 3G (l'Italia è il 5° Paese al mondo come fruitori di questa tecnologia, Tab.5) è anacronistico pensare che le analisi informatico forensi debbano essere richieste solo "in casi eccezionali".

Utenti attivi, pagine viste e tempo speso nel giorno medio, per fasce d'età

Fonte: Audiweb Database, dati Settembre 2012 - Audiweb powered by Nielsen

	2-10 anni	11-17 anni	18-24 anni	25-34 anni	35-54 anni	55-74 anni	Oltre 74 anni
Utenti attivi nel giorno medio (000)	286	872	1,364	2,743	6,805	2,149	80
% sugli utenti attivi nel giorno medio	2.0%	6.1%	9.5%	19.2%	47.6%	15.0%	0.6%
Pagine viste nel giorno medio (000)	18,076	104,213	253,835	435,457	966,988	229,180	5,672
Pagine viste nel giorno medio per persona	63	120	186	159	142	107	71
Tempo speso nel giorno medio per persona (h:m)	0:49	1:06	1:40	1:32	1:23	1:10	0:53

Tab.4



1.1B Global Mobile 3G Subscribers, 37% Growth, Q4 – @ Only 18% of Mobile Subscribers

Rank	Country	CQ4:11 3G Subs (MM)	3G Penetration	3G Sub Y/Y Growth	Rank	Country	CQ4:11 3G Subs (MM)	3G Penetration	3G Sub Y/Y Growth
1	USA	208	64%	31%	16	Canada	16	62%	34%
2	Japan	122	95	9	17	Taiwan	14	48	17
3	China	57	6	115	18	South Africa	13	21	49
4	Korea	45	85	10	19	Turkey	13	20	62
5	Italy	44	51	25	20	Portugal	13	78	19
6	UK	42	53	25	21	Vietnam	12	11	358
7	Brazil	41	17	99	22	Mexico	11	11	55
8	India	39	4	841	23	Malaysia	10	27	7
9	Germany	38	36	23	24	Sweden	10	73	25
10	Spain	33	57	21	25	Philippines	10	11	45
11	France	30	45	35	26	Saudi Arabia	10	19	17
12	Indonesia	29	11	27	27	Netherlands	9	44	34
13	Poland	28	57	17	28	Egypt	8	10	60
14	Australia	22	76	21	29	Austria	7	58	24
15	Russia	17	8	45	30	Nigeria	6	6	51

Global 3G Stats: Subscribers = 1,098MM Penetration = 18% Growth = 37%

KPCB

Note: *3G includes CDMA 1x EV-DO and Rev. A/B, WCDMA, HSPA; One user may have multiple mobile subscriptions and may be counted as multiple subscriber. Source: Informa WCIS+. 7

Tab.5

Ovviamente non è possibile desumere i tempi medi di realizzazione delle CT, ma vi è la convinzione che il fattore tempo rappresenti un limite al numero di conferimento d'incarico.

I conferimenti d'incarico per realizzare una CT informatica sono veramente esigui se rapportati alle decine di migliaia di procedimenti penali instaurati in regione.

Difficile pensare che solo in 86 casi nel 2012 siano stati sequestrati supporti informatici. (si ribadisce che anche gli smartphone ormai somigliano per caratteristiche e struttura più ad un computer che ad un telefono)

La riluttanza da parte dell'Autorità Giudiziaria nel cercare un esperto che possa ricavare elementi utili ai fini d'indagine non può essere imputabile solo ad un problema di costi e di competenza, ma è chiaro che, se solo in pochissimi casi si

ricorre a questo strumento, ci deve per forza essere una diffusa convinzione di una scarsa utilità della CT informatica.

Un ultimo costo, ma non meno importante, è quello dei diritti di cancelleria per copie di CD o DVD[90].

L'importo dovuto per una copia di CD o DVD è di 295,16 euro e sul piano normativo non vi sono altre fonti per dettagliare altre forme di copia digitale.

Per il legislatore viene considerata la sola possibilità di copiare CD o DVD che hanno rispettivamente una capienza di 700 Mb e 4700 Mb quando allo stato attuale i PC montano dischi di almeno 500.000 Mb (500 Gb).

Normalmente ad una CT informatica vengono allegati dati digitali su supporti idonei: CD, DVD ma anche hard disk o memorie Flash.

Se esiguo in termini assoluti il numero di CT informatiche richieste dall'accusa, che ha costi fissi e prestabiliti, è presumibile che le CT di parte lo siano ancor meno perché, oltre ad avere costi maggiori, è ostacolata dagli oneri di cancelleria necessari per ottenere una copia del lavoro svolto dalla CT di controparte.

[90] Come ribadito dalla CIRCOLARE 18 MARZO 2010 del MINISTERO DELLA GIUSTIZIA.

CONSIDERAZIONI CONCLUSIVE

Attraverso questo progetto si è inteso definire le possibilità tecniche di realizzare uno strumento versatile e di facile utilizzo da mettere a disposizione dell'A.G. e della P.G. finalizzato a consentire il proseguo dell'attività d'indagine in tempi molto rapidi e con un notevole contenimento dei costi di giustizia rispetto ad una normale CTU .

Si è voluto creare un ambiente di lavoro favorevole a chiunque, anche ai giuristi più scettici, dandogli la possibilità di visionare contenuti di supporti digitali, acquisiti e memorizzati conformemente a quanto imposto dalle norme, con interfacce intuitive.

La virtualizzazione dei dischi e delle macchine e la visualizzazione delle stesse dalla propria postazione di lavoro comporta notevoli vantaggi di comprensione e la possibilità di accedere da qualunque postazione connessa ad internet e ne avvantaggia la fruibilità in ogni dove.

Potranno così essere superati i tipici ostacoli posti dalla capacità tecnica e comunicativa dell'esperto affidatario dell'incarico di consulente e ridotte le distorsioni interpretative su questioni scientifiche.

Particolare attenzione è stata posta sui vantaggi in termini di garanzia del diritto di difesa, il miglioramento di tempi e costi e la capacità di riuscire a implementare il sistema a seguito di eventuali richieste di integrazione da parte dei fruitori.

Tuttavia non sono stati tralasciati i limiti tecnici, i limiti dettati dalle norme vigenti e gli ambiti di applicabilità.

Lo studio e la ricerca scientifica si è concentrata su sperimentazioni tecniche effettuate in laboratorio riproducendo un modello che possa trovare applicazione in

termini di performance e sicurezza presso singole Procure della Repubblica e/o Tribunali Ordinari, ma scalabile fino al punto di poter essere applicato al servizio di una rete regionale, nazionale o addirittura trasnazionale.

Sono stati verificati i livelli di sicurezza più idonei per la conservazione e la trasmissione delle informazioni acquisite e trattate.

L'attenzione è stata anche rivolta alla quantificazione dei costi di messa in opera del progetto e alla comparazione degli stessi con le spese di liquidazione sostenute da un campione significativo di Procure, da cui emerge la concreta possibilità di raggiungere un dimezzamento della spesa lorda per CT informatiche.

Gli aspetti giuridici trattati maggiormente sono quelli legati al valore della prova scientifica, alla conservazione del dato, alle modalità di analisi delle copie forensi e all'ubicazione fisica da cui gestire una delicata fase procedimentale.

Altro argomento menzionato in allegato alla D.Lgs. 196/2003 riguarda gli aspetti legati alla riservatezza di alcune informazioni contenute nei supporti assolutamente estranee ai fatti per cui si procede di cui si dovrà perdere traccia.

Si spera che questo lavoro possa reppresentare, quantomeno, uno stimolo per un adeguamento della giustizia alla non più nuova realtà digitale che la nostra società sta vivendo.

BIBLIOGRAFIA DI RIFERIMENTO

Referenze

- Kruse W. G. e J.G. Heiser, *Computer Forensics, Incident Response Essentials*, Addison-Wesley, 2002

- NIJ Guide, *Electronic crime scene investigation: a guide for first responders*, Department of Justice, 2001

-Casey E. (editor), *Handbook of Computer Crime Investigation*, Academic Press, 2002

-Marcella A. J. e R. Greenfield (editor), *Cyber Forensics*, Auerbach, 2002

-Maioli C., *Introduzione all'informatica forense*, in: La sicurezza preventiva dell'informazione e della comunicazione, MILANO, Franco Angeli, 2004

RICOGNIZIONE BIBLIOGRAFICA

Computer forensics: tra giudizio e businness, Filippo Novario – Torino: Liberia Cortina, 2012

Investigazione penale e tecnologia informatica, L. Luparia e G. Ziccardi – Milano, Giuffré, 2007.

Sicurezza dell'informazione : fondamenti, buone pratiche e laboratorio virtuale, R. Laschi, R. Montanari, A. Riccioni. - Bologna : Progetto Leonardo, 2008.

Informatica: arte e mestiere, Dino Mandrioli ... [et al.]. - 3. ed. - Milano : McGraw-Hill, [2008]. - XXII, 508 p. ;

L'attività del C.T.U. e del perito, [aggiornato al D. lgs. n. 104/2010 e alla L. n. 69/2009] / Giampaolo Di Marco, Maria Sichetti. - Milano : Giuffrè, 2010.

La devianza informatica tra crimini e diritti: un'analisi sociogiuridica, Cecilia Biengino – Roma: Carrocci, 2009.

Le dinamiche probatorie e gli strumenti per l'accertamento giudiziale, contributi di Alfredo Bargi ... [et al.]. - Torino : UTET giuridica, ©2008.

Le nuove norme sulla sicurezza pubblica : emergenza in materia ambientale, misure di contrasto all'immigrazione illegale e alla criminalità organizzata, misure di prevenzione, prova penale informatica e tutela della privacy, sospensione del processo penale nei confronti delle alte cariche dello Stato, tutela della sicurezza nella circolazione stradale : d.lgs. 30 maggio 2008, n. 109; legge 14 luglio 2008, n. 123; legge 23 luglio 2008, n. 124; legge 24 luglio 2008, n. 125, [scritti di] F. Albano ... [et al.] ; a cura di Sergio Lorusso. - Padova : CEDAM, 2008.

I reati informatici: nuova disciplina e tecniche processuali di accertamento, Giuseppe Amato ... [et al.] ; CD-ROM con formulario. - [Assago] : CEDAM.

Le prove, a cura di Adolfo Scalfati. - Torino : UTET giuridica, 2009

Sistema penale e criminalità informatica : profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48), a cura di Luca Lupària. - Milano : Giuffrè, 2009.

La prova tra processo, scienza e verità. Quel rapporto giudice-accertamento, in D&G, 2006.

Cenni sul computer come strumento di prova nel processo penale, F. Sbisà, in Il Foro ambr., 2000

I costi della giustizia, Marchesi Daniela. - Bologna : Il mulino, 2003

Computer Forensics, A. Ghirardini e G. Faggioli - Roma: Apogeo, 2007

Documento informatico e giusto processo, P. Tonini, in Dir. pen. proc., 2009

Scienza e processo penale : linee guida per l'acquisizione della prova scientifica, a cura di Luisella de Cataldo Neuburger. - Padova : CEDAM, 2010.

Il sequestro nel processo penale, Mario Garavelli. - Torino : UTET, 2002

Tutele e procedure giudiziarie europee: principi fondamentali e applicazioni pratiche, a cura di Michele Angelo Lupoi. - Santarcangelo di Romagna : Maggioli, 2011

L'arte del dubbio, G. Carofiglio – Palermo, 2007.

Contrasto al terrorismo interno e internazionale, R. E. Kostoris e R. Orlandi, Torino, 2007

Apparenze : accertamento giudiziale e prova scientifica, Stefano Fuselli. - Milano : Franco Angeli, 2008.

Nuove tecnologie e processo penale : giustizia e scienza: saperi diversi a confronto, a cura di Mario Chiavario. - Torino : G. Giappichelli, 2006.

La prova penale scientifica: gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione, Oreste Dominioni. - Milano: Giuffrè, 2005

Le investigazioni del difensore, P. Gualtieri – Padova: CEDAM, 2002

APPENDICE

VIRTUAL FORENSIC AMBIENT
- Manuale d'installazione -

Table of Contents

Introduzione

Per la realizzazione dell'intero sistema ci avvarremo di diverse tecnologie. Ogni tecnologia, spesso, viene già completamente implementata in software, applicative, distribuzioni Linux e/o BSD.

ZFS

La scelta su questo genere di file system è ricaduta sia per la capacità di indirizzare uno spazio di memoria elevato[1] sia per i sistemi di sicurezza in esso integrati (metodo transazionale ad oggetti copy-on-write; snapshot; compressione; blocchi a dimensione variabile; Priorità I/O con scheduling di tipo deadline; ecc.) . Questo filesystem permette inoltre la realizzazione di oggetti denominati "Dataset" (un dataset è come una directory su di un volume ma si comporta come un filesystem e quindi supporta snapshot, quote e compressione), e degli "Snapshots" (copia read-only del filesystem al momento) nonchè dei Device virtuali (virtual devices).

iSCSI - Internet SCSI (Small Computer System Interface)

Si tratta di una tecnologia che permette di collegare un dispositivo a blocchi residente su di un'altra macchina (target) attraverso lo stack IP (porte 860 e 3260), permettendo alla macchina che lo monta (initiator) di usarlo come un dispositivo connesso ad essa fisicamente. iSCSI permette l'applicazione di politiche di sicurezza (autenticazione CHAP) nonchè di indirizzamento a livello IP delle risorse permettendo, dunque, il routing e l'uso del sistema DNS.

FreeNAS

Per implementare uno storage con file system ZFS abbiamo utilizzato la distribuzione BSD[2] : FreeNAS (64bit)[3]. Quest'ultima permette non solo la realizzazione di un NAS/SAN basato su file system ZFS ma anche di gestirlo direttamente in tutte le sue proprietà. FreeNAS permette, inoltre, sia la gestione sia la configurazione di ulteriori strumenti come iSCSI (target ed initiator). In particolare, è possibile generare e presentare con facilità tutte le operazioni tipiche di un filesystem ZFS (snapshots, creazione di dataset e volumi, ecc.).

Virtualizzazione

La virtualizzazione permette di emulare alcuni dispositive hardware (hard disk, scheda grafica, scheda di rete, ecc.) in tal modo, in concorso con opportune tecniche, è possibile ricreare un intero sistema informatico.

---

[1] ZFS è un file system a 128 bit: può quindi fornire uno spazio di 16 miliardi di miliardi di volte la capacità dei file system attuali a 64 bit. I limiti del ZFS sono stati progettati per essere così ampi da non essere mai raggiunti in una qualsiasi operazione pratica. Bonwick affermò che "per riempire un file system a 128 bit non sarebbero bastati tutti i dischi della terra". (Wikipedia)

[2] http://it.wikipedia.org/wiki/Berkeley_Software_Distribution

[3] http://www.freenas.org

VirtualBox

Per implementare un sistema di virtualizzazione che sia in grado di offrire ottime performance ma anche elevate opportunità di configurazione è stato scelto Oracle VirtualBox. Esso permette di essere configurato anche attraverso una interfaccia CLI, semplificando l'esecuzione di script di automatizzazione. Questo progetto ha inotre una VirtualBox Main API che comprende tutte le interfacce COM pubbliche ed i componenti messi a disposizione da VirtualBox server e VirtualBox client library

The Sleuth Kit (TSK)

The Sleuth Kit è una libreria ed un insieme di comandi che permettono di investigare su dispositivi di memorizzazione ovvero su immagini di dischi. La funzionalità più importante di TSK è la capacità di analizzare volumi e dati a livello di filesystem.

DEBIAN Linux

Per realizzare l'intera piattaforma, necessaria a coordinare ed a realizzare le diverse risorse, è stato scelto come S.O. DEBIAN Linux, sia per la sua rinomata stabilità (specie nel brench STABLE) sia per la sua ottima aderenza allo standard POSIX oltrechè la sua predisposizione ad integrare diverse tecnologie e novità grazie alla sua enorme comunità di sviluppatori.

PHP

PHP (acronimo ricorsivo per *PHP: Hypertext Preprocessor* fu realizzato da Rasmus Lerdorf nei primi anni novanta) è un linguaggio di scripting general-purpose open source orientato al web, come altri linguaggi di scripting può essere integrato direttamente nel codice HTML che compone una pagina. Esso infatti trova la sua massima applicazione nella realizzazione (anche con metodologie OOP) di siti web ed interfacce grafiche offerte attraverso i relativi server. Deve la sua notorietà anche alla facile integrazione con sistemi database quali MySQL e alla totale integrazione con il server http Apache grazie al relativo modulo libapache2-mod-php5.

MySQL

MySQL è un motore di database relazionale molto diffuso. La sua notorietà è dovuta alle sue ottime performance ed alla sua semplicità di gestione, nonchè per la sua velocità, flessibilità ed affidabilità.

INFRASTRUTTURA

FreeNAS + ZFS + iSCSI

VirtualBox + iSCSI

Debian MySQL server

Debian Apache + PHP

PRESENTAZIONE / REGISTRAZIONE

Debian Apache + PHP + MySql

ACQUISIZIONE

Forlex + iSCSI
DEBIAN LAMP

ELABORAZIONE

DEBIAN LAMP

RICERCA

DEBIAN LAMP + TSK

FREENAS + ZFS

Terminologia

ZFS Volume : un Volume con file system ZFS. In genere si tratta dello storage generato aggregando più dischi fisici. Tra i diversi tipi di aggregazione vi è il RAID-Z. Questo è un tipo di raid software che eredita gli aspetti positivi del RAID5 eliminando il problema del "write hole" usando il sistema del copy-on-write (anzichè sovrascrivere un dato, esso viene scritto in una nuova locazione e ne viene sovrascritto il puntatore alla vecchia locazione).

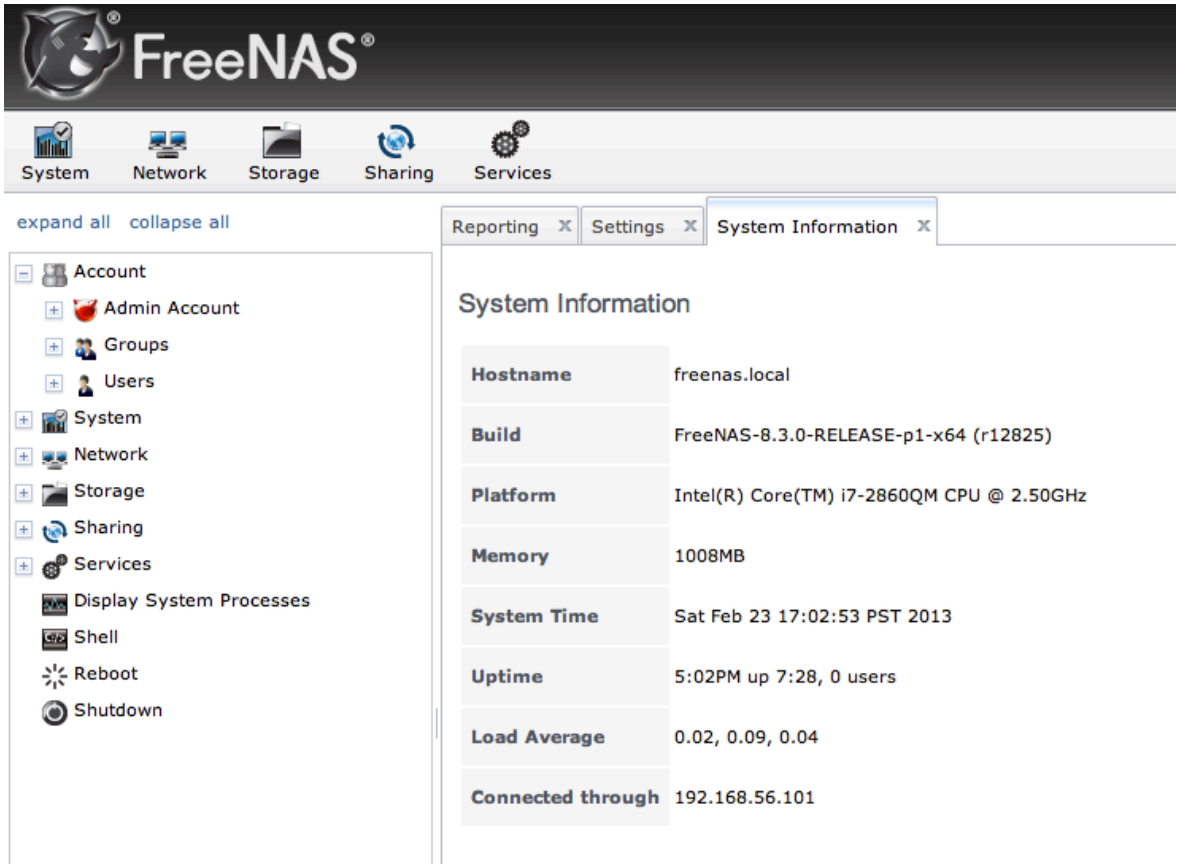
ZVOL **:** un dispositivo a blocchi all'interno di un Volume ZFS.

ZFS Dataset : un oggetto simile ad una directory ma che permette la gestione delle quote e l'applicazione di Snapshot, si comporta quindi come un file system a se stante.

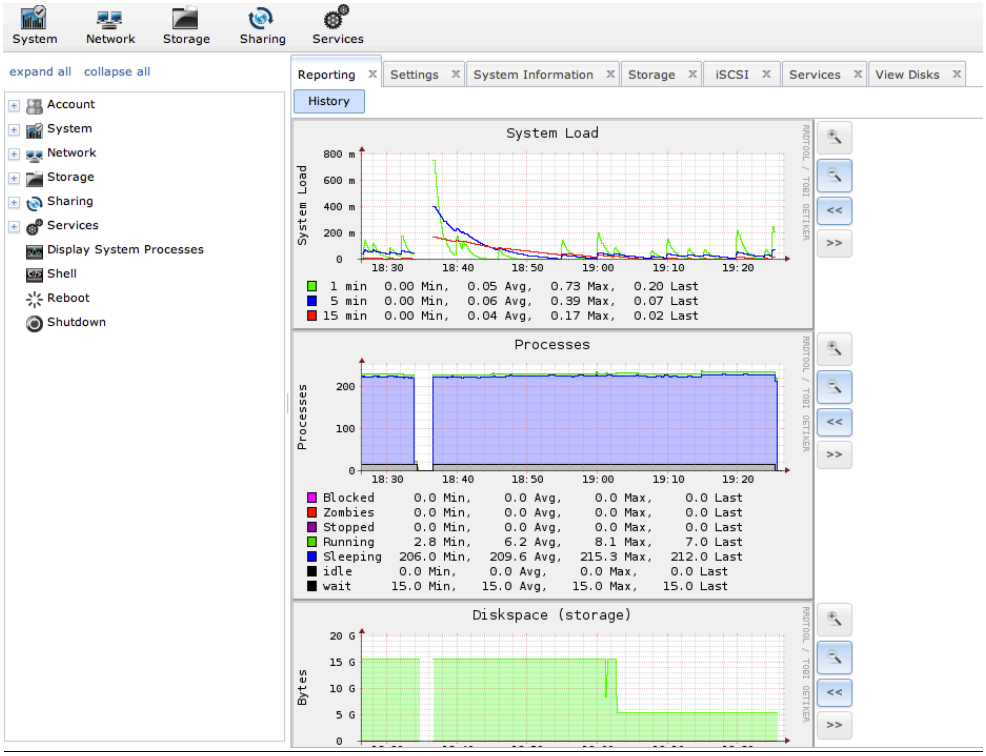
Esempio di indirizzo iSCSI

Type		Date		Naming Aut		Name defined by authority
iqn	.	2013-03	.	com.example	:	mylun

Al termine dell'installazione di FreeNAS versione 8.3 avremo un sistema gestibile attraverso intefaccia web all'indirizzo IP della macchina appena configurata.

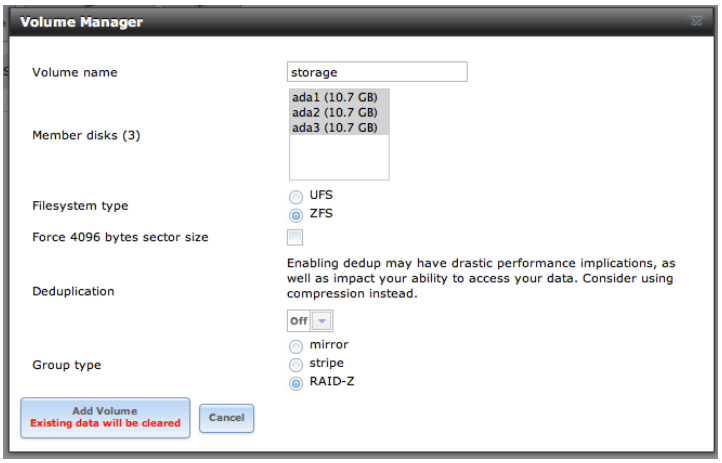


si possono anche leggere le statistiche di sistema :



Creazione dello Storage (Volume ZFS)

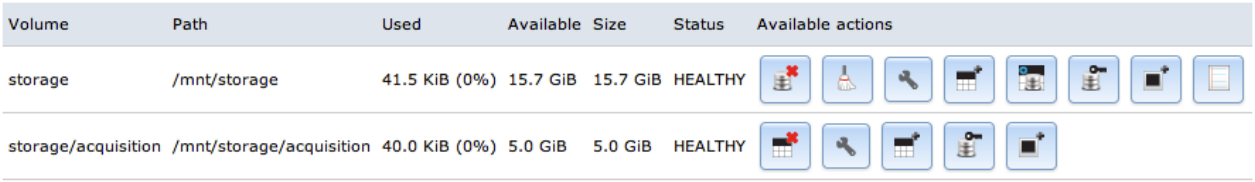
Ora si deve creare un volume ZFS con i dischi che abbiamo aggiunto al sistema . Il volume lo creiamo in ZFS con RAID-Z : click su **STORAGE** -> **Create Volume** Inseriamo il nome di volume es. "storage" selezioniamo i dischi (almeno tre per questo tipo di raid) ada1, ada2 ed ada3 (ada0 è il sistema operativo) scegliamo ZFS e RAID-Z[4] e quindi clicchiamo su **Add Volume**.



[4] *RAID-Z* is not actually a kind of RAID, but a higher-level software solution that implements an integrated redundancy scheme similar to RAID 5, using ZFS.[15] RAID-Z avoids the RAID 5 "write hole"[16] using copy-on-write: rather than overwriting data, it writes to a new location and then automatically overwrites the pointer to the old data. It avoids the need for read-modify-write operations for small writes by only ever performing full-stripe writes. Small blocks are mirrored instead of parity protected, which is possible because the file system is aware of the underlying storage structure and can allocate extra space if necessary. *RAID-Z2* doubles the parity structure to achieve results similar to RAID 6: the ability to sustain up to two drive failures without losing data.

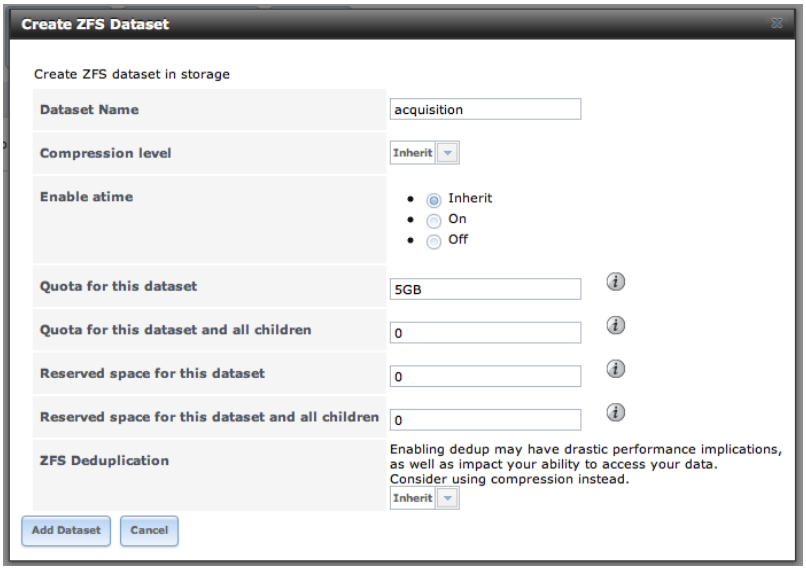
Creazione di un Dataset

Dopo aver selezionato **Volumes -> View Volumes** abbiamo la lista dei volumi ZFS generati.



Per ogni volume possiamo realizzare diverse operazioni tra cui generare un Dataset attraverso l'apposita icona (**Create ZFS Dataset**).

Questo ci permette di definire un Dataset con la relativa quota (lasciando 0 resta quota infinita) nel nostro esempio sarà di 5GB.

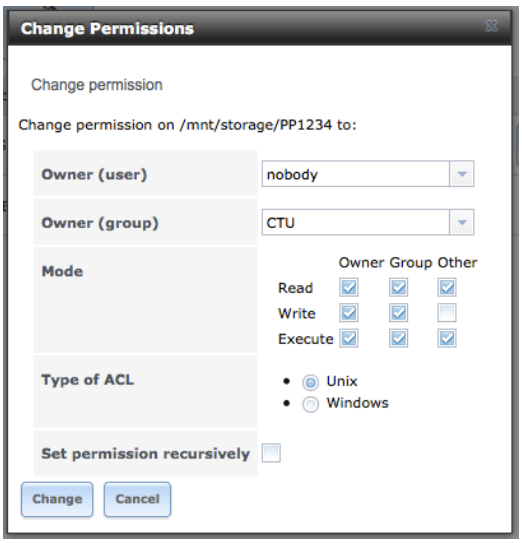


Snapshot
to do

Rolling back snapshot
to do

Creazione di un Dataset con permessi

Creazione di un Gruppo
Creazione di un Utente
Abbinamento dell'utete al gruppo
Creazione del Dataset
Assegnazione del Gruppo al Dataset con aggiunta di W anche al Gruppo

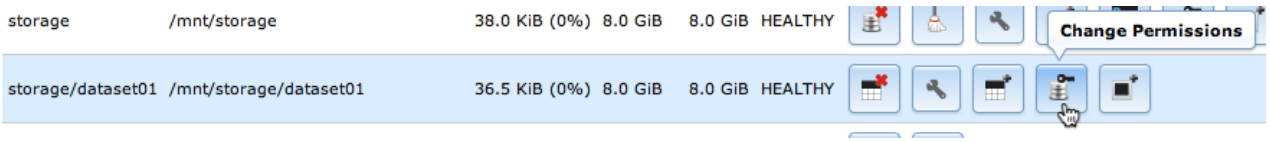


FREENAS Shares

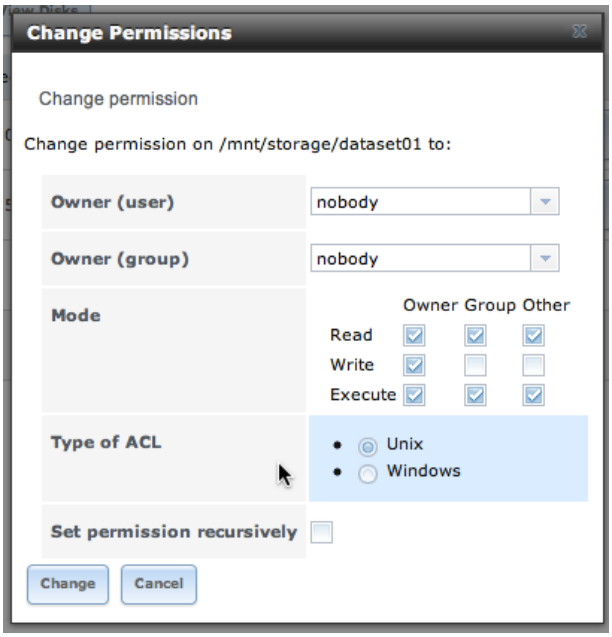
NFS - Condivisione di un Dataset

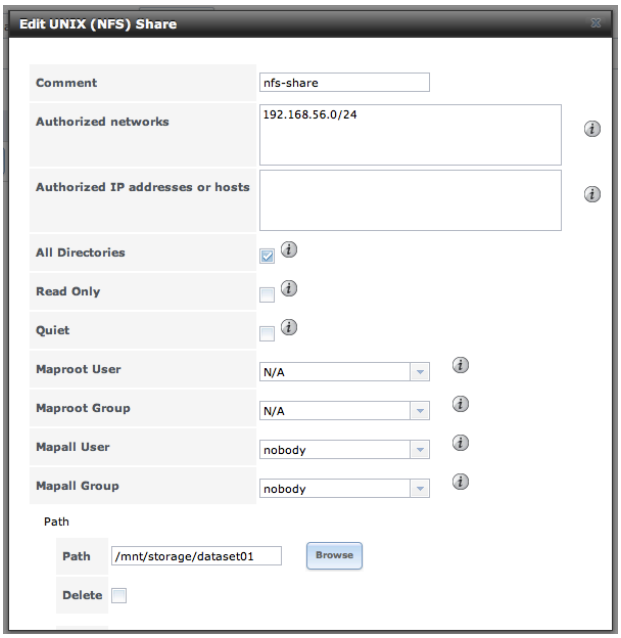
L'accesso ad un Dataset può essere eseguito con diverse modalità. Una, che potrebbe essere scelta perchè flessibile nella configurazione e con sufficienti principi di sicurezza è il NFS (Network File System). Grazie ad esso è possibile montare via rete un Dataset come se fosse un dispositivo a blocchi locale. I vantaggi sono, ovviamente, quelli di poter accedere ad una locazione di memoria in rete e dunque essere multi-utente.

Dopo aver creato un Dataset (es.:dataset01) sarà possibile definirne gli utenti ed i diritti attraverso la relativa interfaccia :



Si noti come sia possibile definire un Utente ed un Gruppo con i relativi diritti RWE per OGO. Questo permette di definire, in modo sufficientemente granulare, i diritti di accesso al Dataset. In fine definiamo i parametri della condivisione NFS.





Nella definisione dei parametri della condivisione NFS vi è la possbilità di "autorizzare intere classi di IP" oppure, puntualmente, solo alcuni hosts. Inoltre si noti come anche in questo caso è possibile scegliere gli utenti ed i relativi gruppi.

La connessione ad una condivivisione NFS, nel caso di S.O. Linux sarà simile all'operazione di mounting di un dispositivo a blocchi locale:

```
mount -t nfs 192.168.56.101:/mnt/storage/dataset01 /media/nfs-dataset01
```

ATTENZIONE: per eseguire il mount si deve inserire TUTTO il percorso del dataset (/mnt/storage/etc)

N.B.: per semplicità implementativa è stato scelto l'utente Nobody del gruppo Nobody.

NFS - creazione di una share NFS autenticata

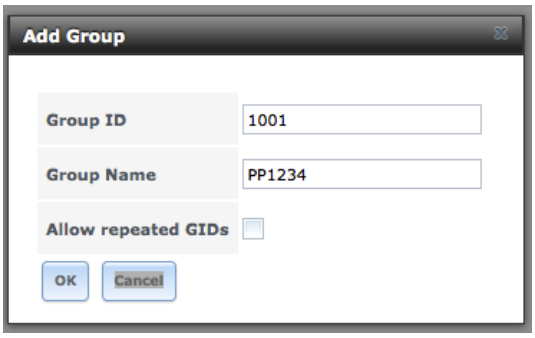
Si può realizzare questa tipologia di share solo implementando Kerberos ed usando NFSv4, ma sin'ora la stabilità e la sicurezza di tale sistema è alquanto discutibile, perciò non sarà analizzata.

CIFS - condividisione un Dataset

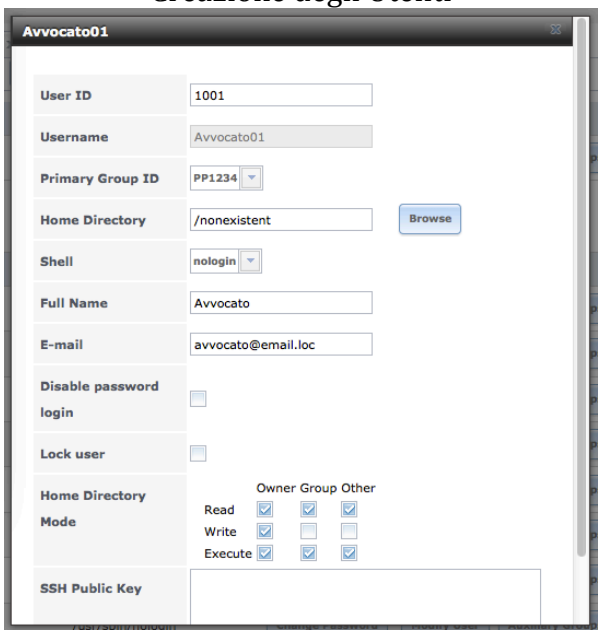
Al fine di avere una condivisione autenticata si può optare per il protocollo CIFS. In questo modo sarà possibile definire i gruppi di utenti abilitati ed in seguito tutti gli utenti con i relativi diritti operativi (questa scelta permette inoltre d'interfacciare facilmente anche ad un directory server LDAP). Di seguito i passi per la corretta implementazione :

In particolare creeremo un Dataset e lo proteggeremo assegnandogli un Gruppo (il Procedimento Penale oppure il numero di caso). In seguito vi aggregheremo degli Utenti che potranno così usare la connessione CIFS per accedere al Dataset

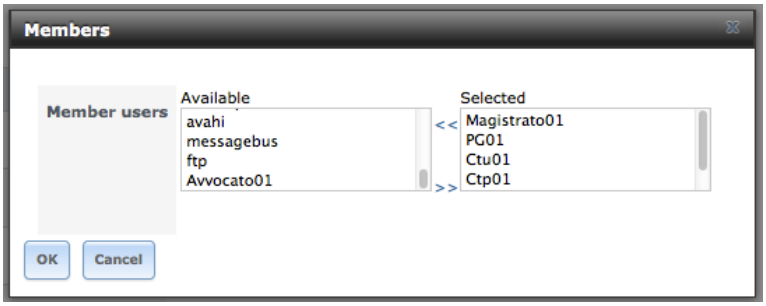
Creazione del Gruppo di utenti
(il numero di caso)



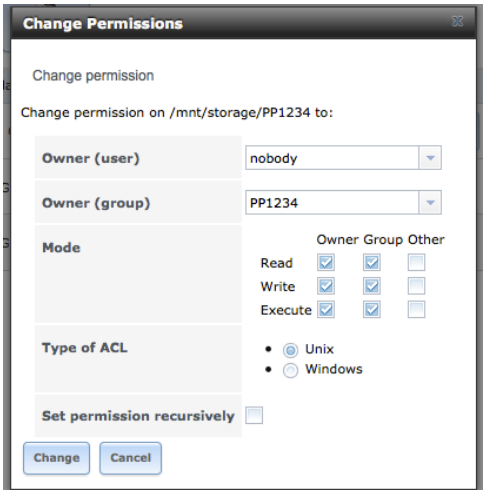
Creazione degli Utenti



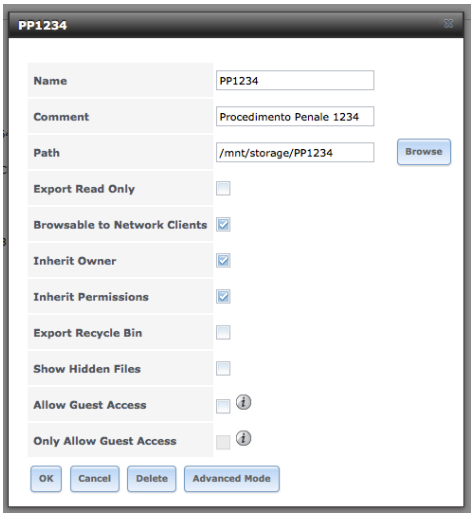
Assegnazione degli Utenti al Gruppo



Creazione del Dataset ed Assegnazione del Gruppo al Dataset con diritti di Lettura Scrittura



Creazione di una condivisione CIFS con path al Dataset e con Gruppo di Utenti definito precedentemente



In tal modo ogni utente potrà accedere alle condivisioni a lui assegnate in base al gruppo (caso) di appartenenza e potrà interagire con il materiale in esso contenute.

iSCSI - creazione di un Target

Terminologia

Initiator: un client autorizzato all'accesso allo storage.

Target: una risorsa che offre un data storage (server).

Portal : indirizzo IP e numero di porta (default 3260) del server

Discovery : Discovery, oppure auto-discovery, è il processo di richiesta, da parte di un Initiator ad un Portal Target (oppure Discovery Portal), per ottenere l'elenco dei suoi targets e renderli disponibili all'Initiator.

iSNS (the Internet Storage Name Service) : Anzichè consttatre direttamente un Portal si può usare questo metodo per il Discovery. Si può paragonare iSNS ad un sistema DNS per network storage devices.

Multi-pathing : In iSCSI il multi-pathing è la possibilità di offrire la stessa risorsa (device) su più target portal così chè, per implementare un sistema di fault-tollerance, in caso una dei due utilizzatori (server) dovesse avere problemi l'altro utilizzatore continuerebbe ad un asare il target device senza problemi.

CHAP(Challenge Handshake Authentication Protocol): metodo di autenticazione basato su una password condivisa ed un three-way authentication per determinare se un sistema è autorizzato ad accedere allo storage device. Il metodo CHAP verifica periodicamente la sessione per evitare gli attacchi a sessione (hijacked di sessione). In iSCSI, l'autenticazione CHAP viene eseguita dal client (initiator).

Mutual CHAP: un superset del CHAP nel quale sia Initiator sia il Target si autenticano mutualmente.

Extent: l'unità da condividere, può essere

Device Extent : un dispositivo raw come un hard disk, una partizione, ecc

File Extent : un file, un volume di tipo ZVOL.

LUN (Logical Unit Number) : identifica un dispositivo logico SCSI. Un initiator negozia con un target la connessione verso una LUN, l'esito è una connessione iSCSI che emula la connessione con un disco SCSI. l'Initiators gestisce la iSCSI LUN come se fosse un disco SCSI/IDE accedendovi direttamente e gestendone il filesystem.

LUC (Logical Unit Controller) :

NB.:

- Avviando una connessione al solo Portal potrò ricevere la lista dei device;
- Porre attenzione alla lunghezza delle password fra 12 e 16 caratteri

Premessa

Per la corretta implementazione di questo servizio si deve ricordare che :

Autenticazione CHAP :	permette di autenticarsi, fornendo credenziali create sul Target.
Mutual CHAP :	permette di autenticarsi, fornendo dapprima initiator-username e initiator-password che identificano l'Initiator e poi la target-username e target-password presenti sul Target.

Ovviamente un Initiator non potrà usare più initiator-username e initiator-password inquanto il software client è uno solo come anche lo stesso initiator. Nel caso volessimo fornire più target per lo stesso Initiators sfruttando la sicurezza del MutualChap, la configurazione del Target sarà stessa username e password per l'Initiator da abilitare e diversa coppia di credenziali per i diversi target da offrire.

Procedura di implementazione

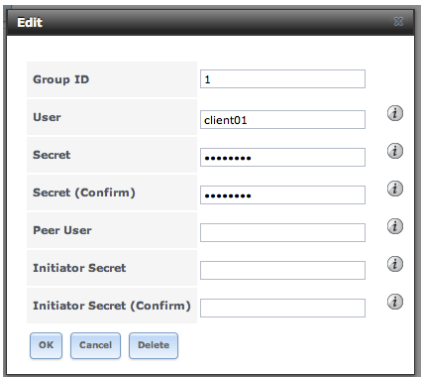
1. Decidere il tipo di autenticazione : CHAP oppure Mutual CHAP. Impostare le autorizzazioni per l'accesso
2. Creare un Device Extent / File Extent
3. Abilitare gli hosts, che usano iSCSI Initiator, alla connessione.
4. Creare un Portal (indirizzo IP e numero di porta da usare per connessioni iSCSI)
5. Impostare i parametri per la configurazione globale dei Target.
6. Creare unTarget
7. Associare i Targets alle Extents.
8. Avviare il servizio iSCSI

Autenticazione ed accessi

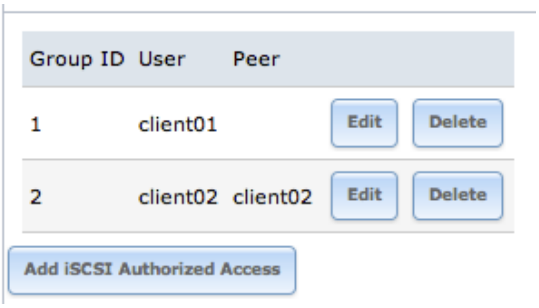
Per impostare questi parametri dobbiamo selezionare :

Services → ISCSI → Authorized Accesses → Add Authorized Access

quindi compilare il seguente form :

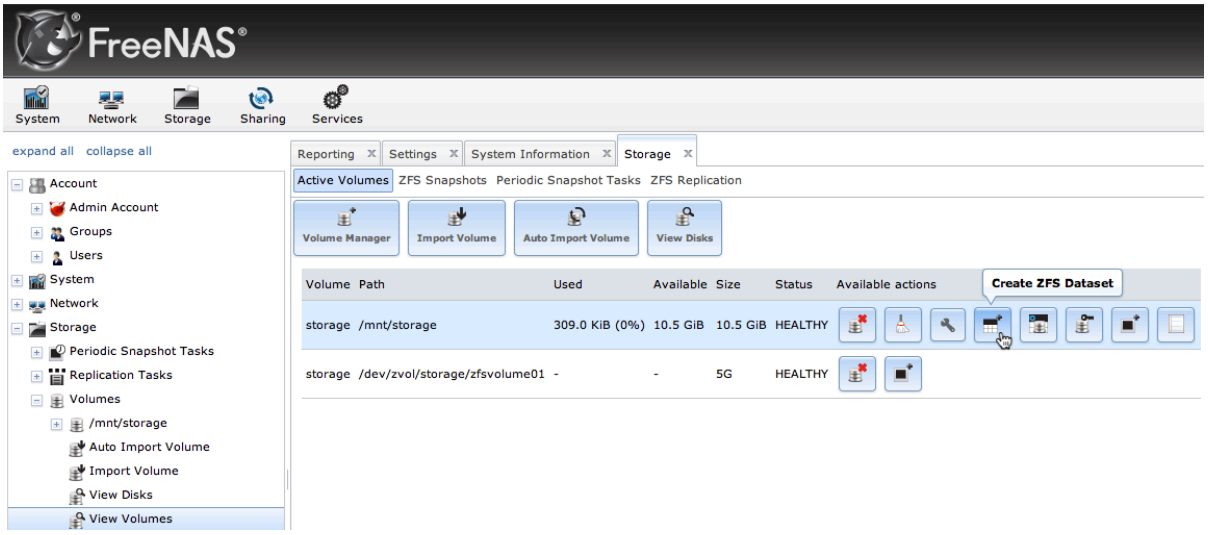


Form per Accessi autorizzati

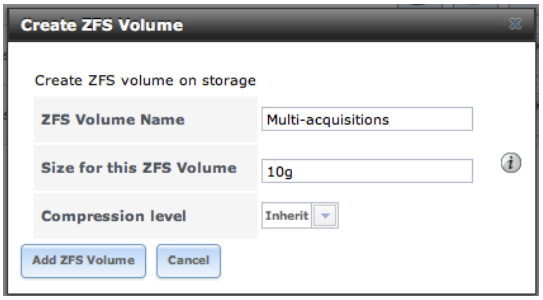


Lista di utenti autorizzati , CHAP e Mutual Chap.

Prima di creare un Device Extent dobbiamo ricordarci di creare un ZVOL dalla relativa icona in corrispondenza del Volume ZFS

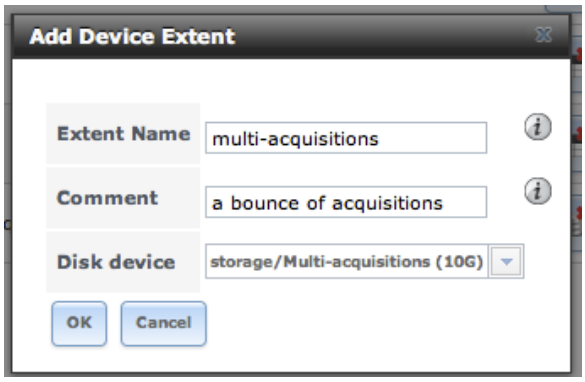


ed in seguito compilare il relativo form



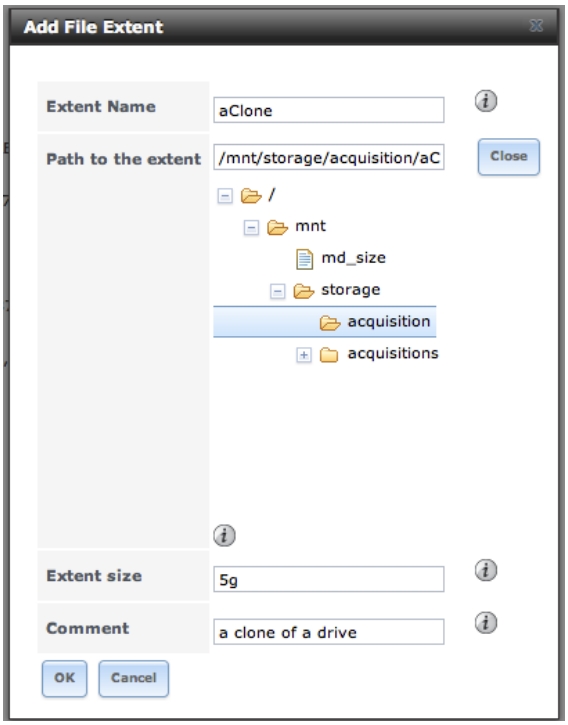
Generiamo ora sia un Device Extent sia un File Extent (serviranno rispettivamente per riversare un insieme di acquisizioni e per effettuare una acquisizione).

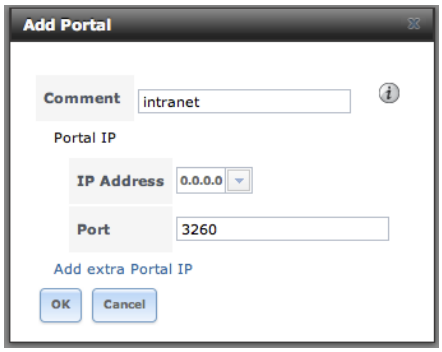
Services → ISCSI → Device Extents → Add Device Extent



in questo modo avremo un volume ZFS, raggiungibile via iSCSI all'interno del quale ad esempio salvare le nostre acquisizioni.

Services → ISCSI → File Extents → Add File Extent

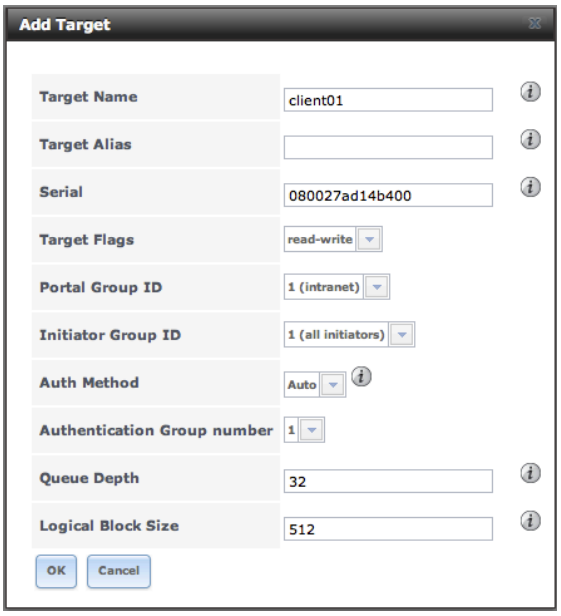


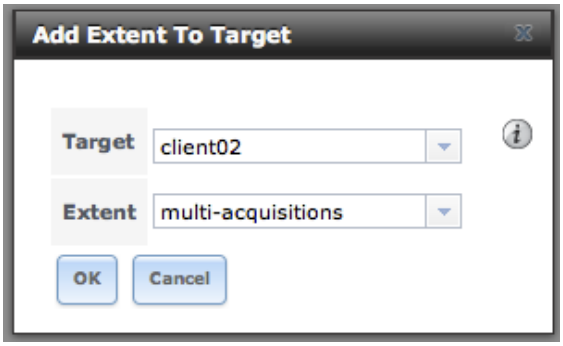


Al termine dovremo configurare un Portal al fine di abilitare l'elenco degli hosts che potranno acedere alle risorse iSCSI e la classe di Initiators

in questo caso abbiamo abilitato tutti gl'indirizzi IP sulla porta 3260 e tutti gl'Initiators.

Ed in seguito abbiamo creato i Targets e poi associati ai relativi Extent .

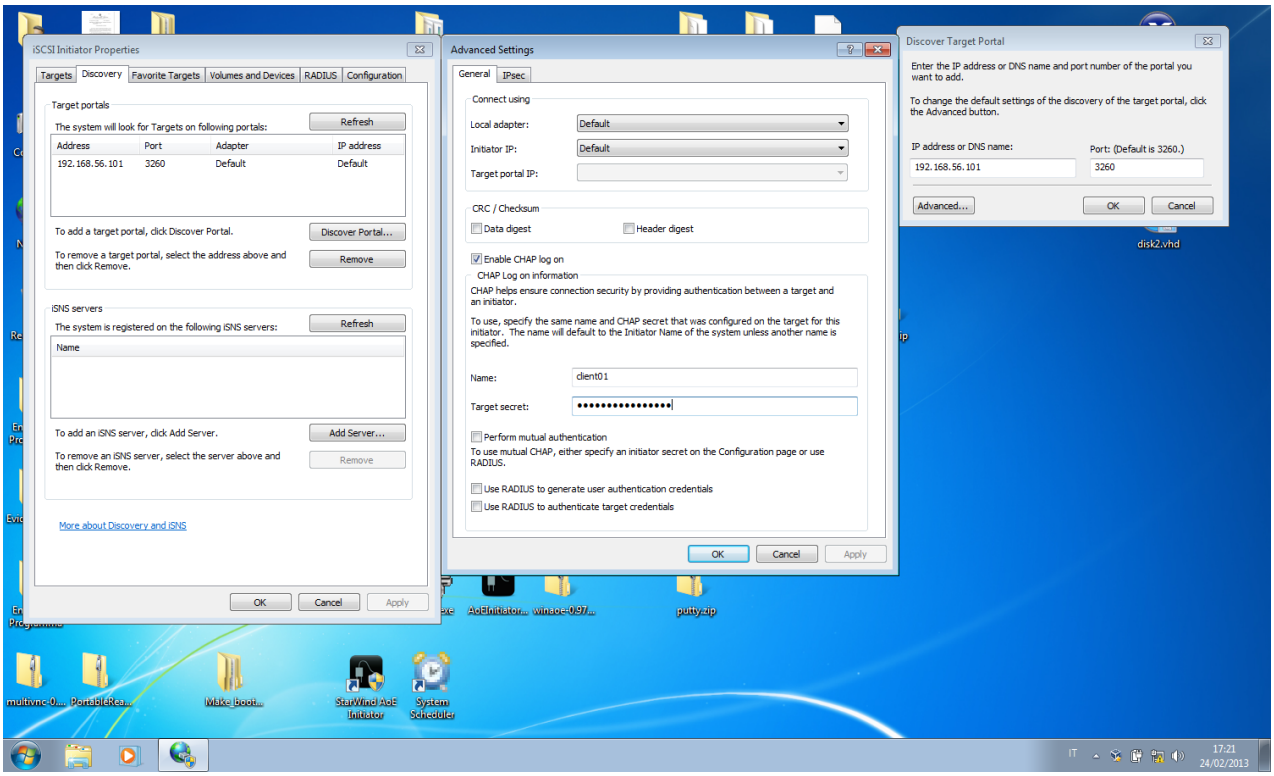




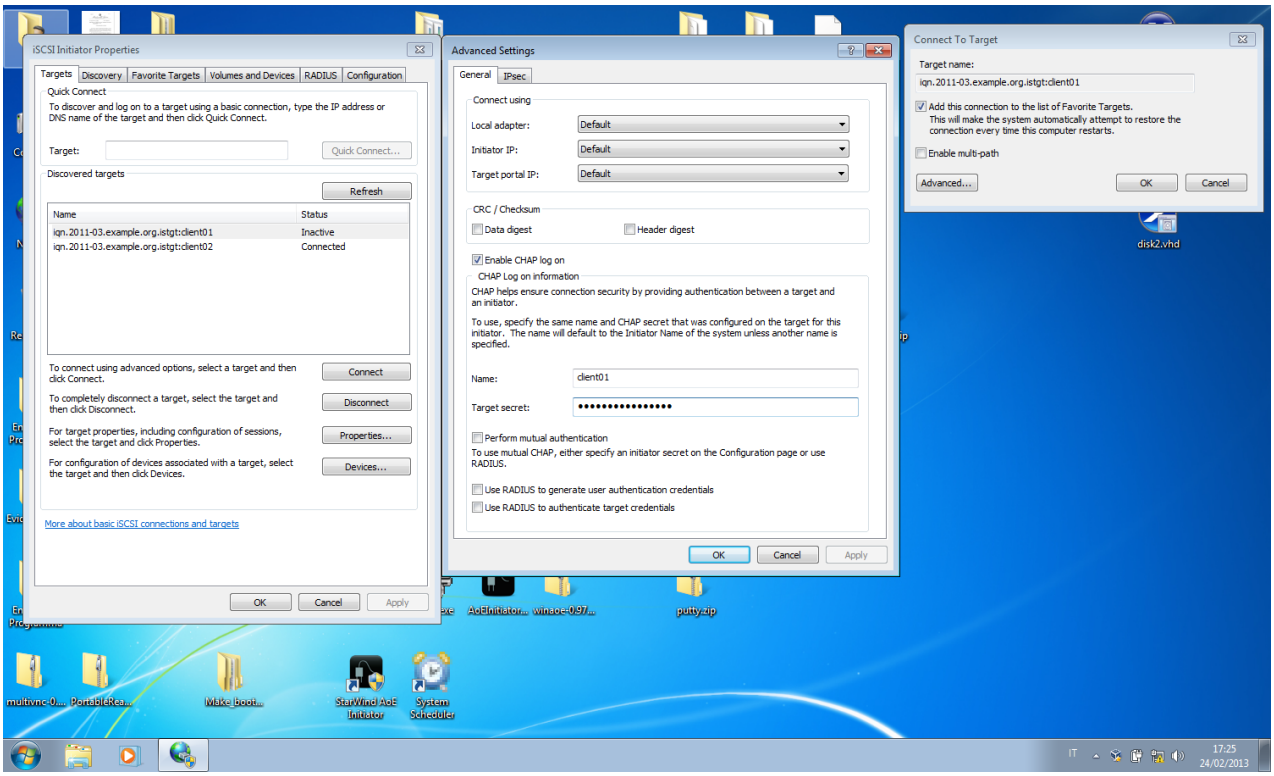
Windows 7 iSCSI Initiator

Questo S.O. è già fornito di un Initiator iSCSI la configurazione risulta abbastanza semplice. Si deve ricordare che nel caso in cui le impostazioni globali del target (Target Global Configuration) siano state impostate come segue:

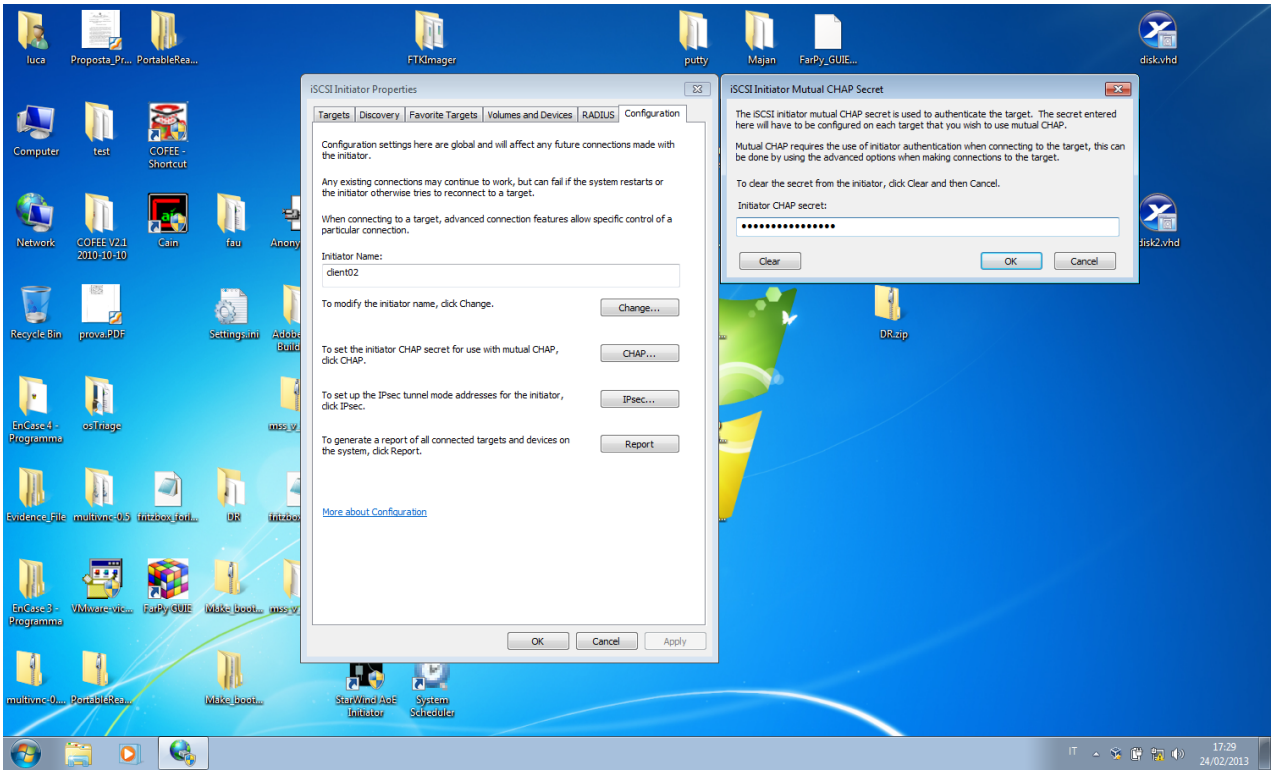
A seguito di questo, sull'Initiator si dovranno impostare le credenziali di accesso relative al Discovery per poter visualizzare l'elenco dei Target.



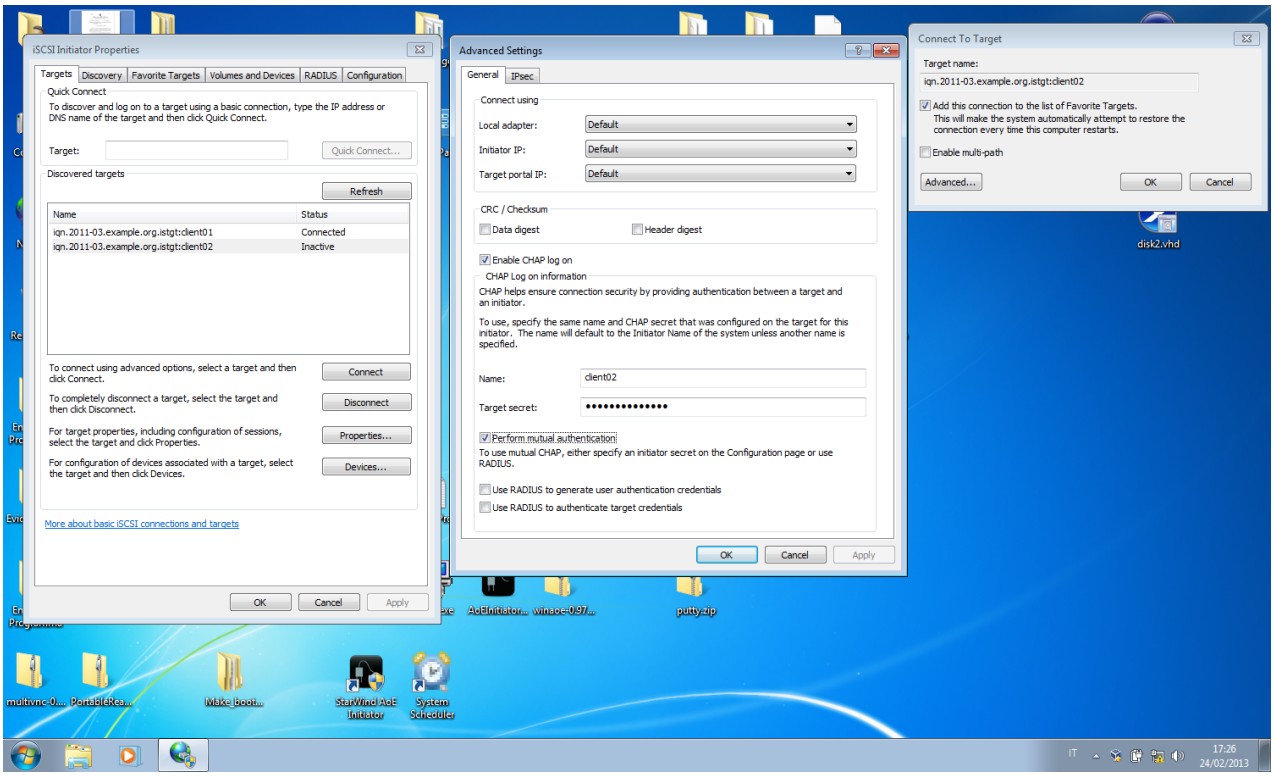
in seguito, in caso di semplice autenticazione CHAP, per una risorsa, potremo connetterci ad essa previo inserimento delle credenziali



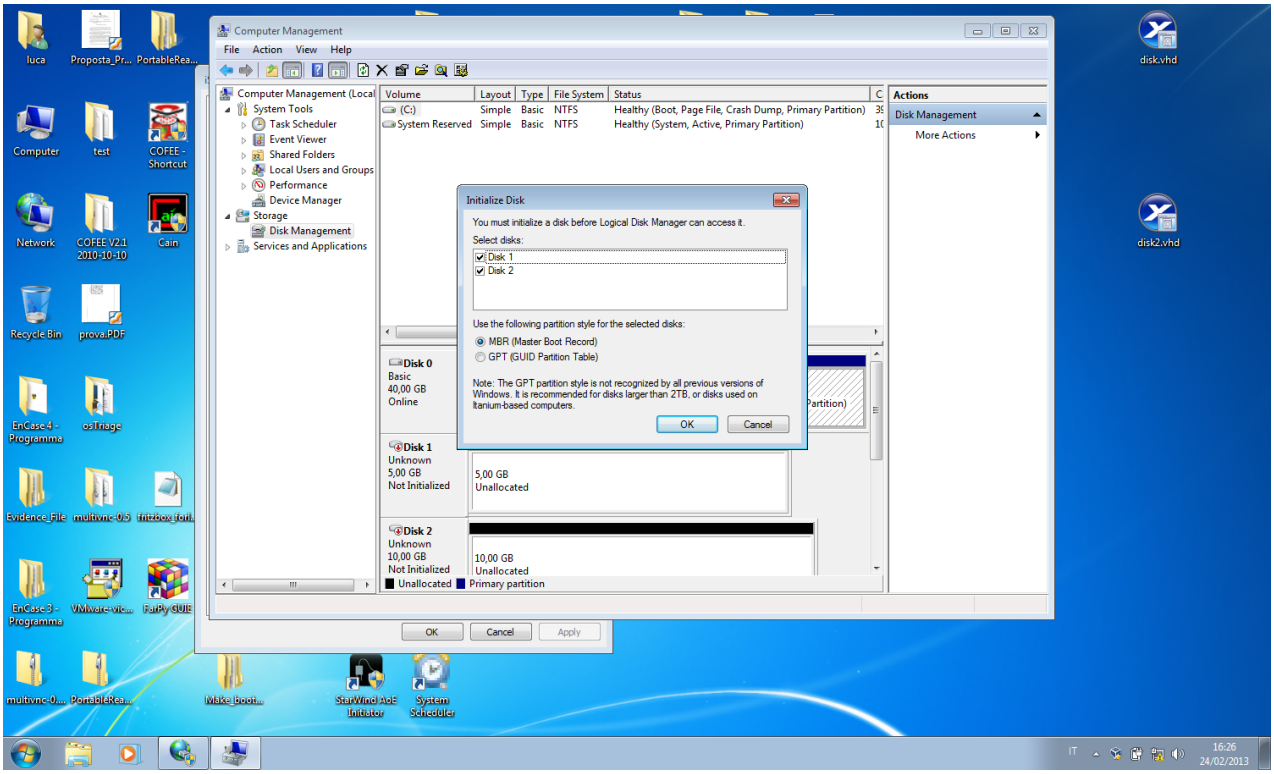
nell'ipotesi di autenticazione MutualCHAP, dovremo inserire nella finestra Configuration le apposite credenziali Initiator



e quindi potremo connetterci al target iSCSI che richiede tale tipo di autenticazione



Dopo queste operazioni saremo in grado di usare i dispositivi connessi come se fossero dei normali hard disk locali



Linux iSCSI Initiator

Di seguito un esempio di connessione su sistema operativo Debian Linux.

Innanzitutto installiamo quanto necessario per l'Initiator, il tool Open-iSCSI

```
apt-get install open-iscsi
```

L'accesso alle risorse avverà secondo due modalità diverse di autenticazione : CHAP e Mutual CHAP. In entrambi i casi chi richiede la connessione avrà le sue credenziali di accesso come istituito durante l'installazione del target.

Il server necessita di credenziali sia per il Discovery delle risorse sia per la connessione al dispositivo. Il discovery può essere, anche in questo caso sia in CHAP sia in Mutual CHAP. Nel caso di specie abbiamo provveduto a configurare come segue :

Discovery	Tipo isorsa	Mutual Chap
Risorse	File per clonare un disco ZVol per riversare acquisizioni	client01 -> CHAP client02 -> Mutual CHAP

Credenziali	Tipologia
discovery	username : discovery password : FreeNAS_ discovery username initiator : inidiscovery password initiator : FreeNAS_inidiscovery
client01	username : client01 password : FreeNAS_client01
client02	username : tgtclient02 password : FreeNAS_tgtclient02 username initiator : iniclient02 password initiator : FreeNAS_iniclient02

Si provvede a modificare il file /etc/iscsi/iscsi.conf nelle seguenti voci :

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = discovery
discovery.sendtargets.auth.password = FreeNAS_ discovery
discovery.sendtargets.auth.username_in = inidiscovery
discovery.sendtargets.auth.password_in = FreeNAS_inidiscovery
```

in questo modo saremo in grado di eseguire il comando

```
iscsiadm -m discovery -t st -p <IP portal> (es.: 192.168.56.101)
```

-m: determina la modalità -t: specifica il tipo -p: indica l'indirizzo IP del target

ricevendo una lista di risorse

```
192.168.56.101:3260,1 iqn.2011-03.example.org.istgt:client02
192.168.56.101:3260,1 iqn.2011-03.example.org.istgt:client01
```

si noti come dopo l'identificativo (dopo i due punti) di ogni risorsa vi sia il nome del target. (es.: client01)

Adesso possiamo impostare le opzioni, per l'Initiator, per connettersi al target specificato a seconda del tipo di autenticazione:

NULLA

Casi di connessione (login) ove non è richiesta l'autenticazione.

```
iscsiadm –m node --targetname 192.168.56.101:3260,1 iqn.2011-03.example.org.istgt:client02 --login
```

CHAP

```
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client01" --portal "192.168.56.101:3260" --op=update --name node.session.auth.authmethod --value=CHAP
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client01" --portal "192.168.56.101:3260" --op=update --name node.session.auth.username --value=client01
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client01" --portal "192.168.56.101:3260" --op=update --name node.session.auth.password --value=FreeNAS_client01
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client01" --portal "192.168.56.101:3260" --login
```

Mutual CHAP

```
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client02" --portal "192.168.56.101:3260" --op=update --name node.session.auth.authmethod --value=CHAP
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client02" --portal "192.168.56.101:3260" --op=update --name node.session.auth.username --value=tgtclient02
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client02" --portal "192.168.56.101:3260" --op=update --name node.session.auth.password --value=FreeNAS_tgtclient02
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client02" --portal "192.168.56.101:3260" --op=update --name node.session.auth.username_in --value=initclient02
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client02" --portal "192.168.56.101:3260" --op=update --name node.session.auth.password_in --value=FreeNAS_initclient02
iscsiadm -m node --targetname "iqn.2011-03.example.org.istgt:client02" --portal "192.168.56.101:3260" --login
```

In entrambi i casi riceveremo un messaggio di conferma dell'avvenuta connessione alla risorsa.

```
Logging in to [iface: default, target: iqn.2011-03.example.org.istgt:client02, portal: 192.168.56.101,3260] (multiple)
Login to [iface: default, target: iqn.2011-03.example.org.istgt:client02, portal: 192.168.56.101,3260] successful.
```

Se si volesse elencare tutte le risorse presenti sulla macchina potremmo usare il seguente comando :

```
find /sys/devices/platform/host* -name block\* -exec ls -la '{}' \; | sed s#^.*../block/#/dev/#g
```

lanciando il comando : fdsik -lu avremo una lista di tutti i device di memorizzazione che

potranno essere formattati e partizionati a nostro piacimento.

Logout

Per iconnetersi da una risorsa invece si potrà eseguire il logout

```
iscsiadm –m node --targetname 192.168.56.101:3260,1 iqn.2011-03.example.org.istgt:client02 --logout
```

VirtualBox + iSCSI proprietario

Il sistema di virtualizzazione VirtualBox permette di montare direttamente uno storage come se fosse un proprio dispositivo a blocchi. In particolare è possibile connettere nativamente una risorsa iSCSI come hard disk e dunque utilizzarla. Dapprima creiamo una macchina virtuale con le differenti opzioni. Per effettuare questa operazione utilizzeremola sola interfaccia CLI di VirtualBOX:

Creazione Virtual Machine

```
VBoxManage createvm --name "MyWin" --ostype "WindowsXP" --register
```

aggiunta RAM ACPI e Video RAM

```
VBoxManage modifyvm "MyWin" --memory 1024 --acpi on --vram 128
```

aggiunta controller SATA con 10 porte SATA

```
VBoxManage storagectl "MyWin" --name "SATA Controller" --add sata --controller IntelAHCI --sataportcount 10
```

aggiunta di un hard disk

```
VBoxManage storageattach MyWin --storagectl "SATA Controller" --port 0 --device 0 --type hdd --medium winxp
```

aggiunta controller IDE

```
VBoxManage storagectl "MyWin" --name "IDE Controller" --add ide
```

Aggiunta lettore DVD vuoto

```
VBoxManage storageattach "MyWin" --storagectl "IDE Controller" --port 1 --device 0 --type dvddrive --medium emptydrive
```

Inserimento del DVD

```
VBoxManage storageattach "MyWin" --storagectl "IDE Controller" --port 0 --device 0 --type dvddrive --medium /root/Documents/WINXPSP3/WINXP_IT_SP3.iso
```

Definizione sequenza di boot

```
VBoxManage modifyvm "MyWin" --boot1 dvd --boot2 disk --boot3 none --boot4 none
```

Abilitazione IOAPIC

```
VBoxManage modifyvm "MyWin" --ioapic on
```

Aggiunta della scheda di rete ed aggregazione ad una rete Host-Only

```
VBoxManage modifyvm "MyWin" --nic1 hostonly
```

Definizione della rete Host-Only di riferimento

```
VBoxManage modifyvm "MyWin" --hostonlyadapter1 vboxnet0
```

Associazione della scheda di rete in bridge

```
VBoxManage modifyvm PP12345 --bridgeadapter1 eth0
```

Connessione di un Hard disk iSCSI (con autenticazione CHAP) alla macchina

```
VBoxManage storageattach MyWin --storagectl "SATA Controller" --port 0 --device 0 --type hdd --medium iscsi --server 192.168.56.104 --target "iqn.2011-03.example.org.istgt:client01" --tport 3260 --username client01 --password FreeNAS_client01

iSCSI disk created. UUID: b8d89a36-d0ce-4cef-9cd1-1c54ef8763da
```

Avvio della macchina virtuale in modalità Headless

```
VBoxHeadless --startvm MyWin
```

Ulteriori comandi per gestire la macchina virtuale

```
VBoxHeadless --startvm MyWin --vrde off

VBoxManage controlvm MyWin pause

VBoxManage controlvm MyWin resume

VBoxManage controlvm MyWin reset

VBoxManage controlvm MyWin poweroff

VBoxManage controlvm MyWin acpipowerbutton
```

Creazione ed aggregazione ad una rete Host-Only con DHCP server attivo

```
VBoxManage hostonlyif create ipconfig vboxnet0 --ip 192.168.50.1

VBoxManage dhcpserver add --ifname vboxnet0 --ip 192.168.50.1 --netmask 255.255.255.0 --lowerip 192.168.50.100 --upperip 192.168.50.110

VBoxManage dhcpserver modify --ifname vboxnet0 --enable
```

IMPORTANTE : Se vogliamo avere VRDE attivo si deve installare l'extension pack.

Installazione dell' Extension Pack di riferimento

```
VBoxManage --version (otterremo la versione ad es.: 4.1.18_Debianr78361 )

wget http://download.virtualbox.org/virtualbox/4.1.18/Oracle_VM_VirtualBox_Extension_Pack-4.1.18-78361.vbox-extpack

VBoxManage extpack install Oracle_VM_VirtualBox_Extension_Pack-4.1.18-78361.vbox-extpack
```

Una volta avviata la macchina sarà possibile vederne il monitor attraverso un qualsiasi client RDP. Questa configurazione non imposta alcuna policy di sicurezza (metodo Null) ma è possibile definirne diverse:

1) External - definizione di una libreria esterna di autenticazione (VBoxAuth.so) che s'integra come modulo PAM e quindi autentica gli utenti del sistema host.

Vi è anche una ulteriore libreria (VBoxAuthSimple) che permette l'autenticazione agli utenti che hanno le loro credenziali definite nella sezione **extradata** del file XML di definizione della Macchina Virtuale. (Questo metodo potrebbe essere il preferito, non dipendendo da altri sistemi di autenticazione)

Abilitare VBoxAuthSimple

```
VBoxManage setproperty vrdeauthlibrary "VBoxAuthSimple"
```

Impostare ad external l'autenticazione

```
VBoxManage modifyvm MyWin --vrdeauthtype external
```

Calcoliamo l'hash della password

```
VBoxManage internalcommands passwordhash "miapassword"
Password hash: 368301ce55166eb3b6bad6aee0beb6b6baa35542bd11f57c5977dd6c8b038df6
oppure
VBoxManage internalcommands passwordhash "miapassword" > pwdhash
```

Impostiamo l'utente "miouser" e relativa password nel sistema

```
VBoxManage setextradata MyWin "VBoxAuthSimple/users/miouser" 368...df6
oppure
VBoxManage setextradata MyWin "VBoxAuthSimple/users/miouser" 'cat pwdhash'
```

Troveremo quindi nel file XML di configurazione i seguenti elementi nella sezione Extradata

```
<ExtraData>
<ExtraDataItem name="VBoxAuthSimple/users/miouser" value="368301ce55166..... 7dd6c8b038df6"/>
</ExtraData>
```

2) Guest - ancora in fase di test

HARD DISKS VIRTUALI

Nel caso in cui volessimo convertire un disco virtuale vdi in un altro formato possiamo usare clonehd, quindi da vdi a vmdk basterà :

```
VBoxManage clonehd source.vdi target.vmdk --format VMDK
```

Pigrizia

Ecco una sequenza di comandi per realizzare velocemente un macchina virtuale con un disco virtuale già generato :

$ VBoxManage createvm --name “Name of VM Here” --register

$ VBoxManage modifyvm “Windows7” --memory 1024 --acpi on --boot1 dvd --nic1 bridged --bridgeadapter1 eth0

$ VBoxManage createhd --filename Windows7.vdi --size 10000

$ VBoxManage storagectl “Windows7” --name “IDE Controller” --add ide

$ VBoxManage storageattach “Windows7” --storagectl “IDE Controller” --port 0 --device 0 --type hdd --medium Windows7.vdi

$ VBoxManage storageattach “Windows7” --storagectl “IDE Controller” --port 1 --device 0 --type dvddrive --medium Windows7.iso

Comando per vedere l'elenco delle macchine virtuali in esecuzione

```
$ VBoxManage list runningvms
```

Comando per vedere l'elenco dei dischi virtuali in esecuzione

```
$VBoxManage list hdds
```

Comando per disconnettere un disco da una macchina

```
$VBoxManage storageattach "Windows7" --storagecontrol "SATA Controller" --port 0 --device 0 --type hdd --medium none
```

Comando per rimuovere un disco dalla lista dei dichi disponibili

```
$VboxManage closemedium disk <uuid>
```

VirtualBox + iSCSI da Sistema

Nel caso si volesse connetere un target iSCSI ed in seguito renderlo accessibile ad una macchina virtuale in VirtualBox, potremo eseguire le operazioni elencate nel capitolo Linux iSCSI Initiator e poi definirlo cone un dispositivo di tipo RAW.
Quindi una volta connessa la nostra LUN basterà sapere l'identificativo del Block device (es.: /dev/sdc) e lanciare il comando con il relativo nome del device che sivuole creare (es.: mydisk.vmdk) :

```
VBoxManage internalcommands createrawvmdk -filename mydisk.vmdk -rawdisk /dev/sdc
```

a questo punto si potrà aggiungere il nuovo disco alla nostra macchina virtuale

```
VBoxManage storageattach MyWin --storagectl "SATA Controller" --port 0 --device 0 --type hdd --medium mydisk.vmdk
```

Script

Nell'ipotesi si volessero estrarre ulteriori informazioni, da shell, sulle macchine/hard disk/porte e device/controller dovremo fare riferimento sia ai comandi VBoxManage sia al file XML (con estensione vbox) che definisce una macchina virtuale ed è presente all'interno della di directory che la ospita. In realtà saremo costretti a combinare il comando con ulteriori comandi e tools. Alcuni molto utili saranno AWK, SED,GREP ed XPATH(per l'xml). Di seguito una raccolta di combinazioni utili ai diversi scopi realizzati su macchina Ubuntu.

Conoscere la lista degli UUID degli hard disks presenti nella Media Libary

```
VBoxManage list hdds | grep "^UUID:" |awk '{print $2}'
```

Conoscere la lista delle macchine

```
vboxmanage list vms
```

Conoscere la lista degli UUID delle macchine presenti nel sistema

```
vboxmanage list vms | awk '{print $2}'
```

Conoscere il nome di ogni macchina

```
vboxmanage list vms | awk '{print $1}'
```

Conoscere UUID macchina per ogni UUID hard disk

```
vboxmanage list hdds | grep "^Usage:" | awk '{print $2 " " $4}'| sed 's/)//g/'
```

Conoscere info macchina per ogni hard disk

```
vboxmanage showvminfo $(vboxmanage list hdds | grep "^Usage:" | awk '{print $4}'| sed 's/)//g')
```

XPATH

Conoscere UUID macchina che usa un hard disk

```
//Machine[MediaRegistry[HardDisks[HardDisk[@uuid="{<UUID disco>}"]]]]/@uuid <pathtofile>.vbox | grep -P -o '[0-9a-z]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}'
```

Lista degli UUID dei dischi connessi ad una macchina

```
xpath -q -e ' //HardDisk/@uuid' <pathtofile>.vbox | grep -P -o '[0-9a-z]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}'
```

Conoscere il numero di porta alla quale è connesso un disco

```
xpath -q -e ' //AttachedDevice[Image[@uuid="{< UUID Disco>}"]]/@port' <pathtofile>.vbox | grep -P -o '(?<=\")[0-9](?=\")'
```

Conoscere il numero di device al quale è connesso un disco

```
xpath -q -e ' //AttachedDevice[Image[@uuid="{< UUID Disco>}"]]/@device' <pathtofile>.vbox | grep -P -o '(?<=\")[0-9](?=\")'
```

Conoscere il Controller al quale è connesso un disco

```
xpath -q -e ' //StorageController[AttachedDevice[Image[@uuid="{< UUID Disco>}"]]]/@name | grep -P -o '(?<=\").*(?=\")'
```

FREEBSD Installazione

Uno dei tanti vantaggi di FreeBSD è la disponibilità del file system ZFS. Al contrario dei sistemi già preconfezionati, una installazione "pulita" permette una maggiore flessibilità in caso di personalizzazioni. Di seguito i passaggi per installare un S.O. FreeBSD con ZFS, iSCSI e share NFS.

http://zfsguru.com/doc/bsd/setup http://people.freebsd.org/~rse/iscsi/iscsi.txt

SSH - Root login

Per poter eseguire login come root via ssh si deve modificare il file di configurazione del demone come segue :
vi /etc/ssh/sshd_config
e decommentare e porre a "yes" le seguenti voci :

```
#Authentication:
#..
PermitRootLogin yes
#..

PasswordAuthentication yes
#...
```

riavviare il demone

```
/etc/rc.d/sshd restart
```

Cambio indirizzo IP

Editiamo il file /etc/rc.conf ed aggiungiamo la seguente configurazione:

```
ifconfig_em0="inet 192.168.56.101 netmask 255.255.255.0"
```

quindi riavviamo la rete

```
/etc/rc.d/netif restart
```

Installazione dei sorgenti

Nel caso di alcuni ports è necessario avere i sorgenti in locale. Per poterli scaricare dovremo:

```
#cp /usr/share/example/cvsup/stable-supfile /root/stable-sup
```

configurare il repository

```
#vi /root/stable-sup
```

```
*default host=cvsup1.FreeBSD.org
*default base=/var/db
*default prefix=/usr
*default release=cvs tag=RELENG_9
*default delete use-rel-suffix
src-all
```

```
#csup /root/stable-sup
```

Ricompilare Kernel e tools

1. make buildworld

This first compiles the new compiler and a few related tools, then uses the new compiler to compile the rest of the new world. The result ends up in /usr/obj.

2. make buildkernel

   This uses the new compiler residing in /usr/obj in order to protect against compiler-kernel mismatches.

3. make installkernel

   Place the new kernel and kernel modules onto the disk, making it possible to boot with the newly updated kernel.

4. Reboot into single user mode.

   Single user mode minimizes problems from updating software that is already running. It also minimizes any problems from running the old world on a new kernel.

5. mergemaster -p

   This does some initial configuration file updates in preparation for the new world. For instance, it may add new user groups to the system, or new user names to the password database. This is often necessary when new groups or special system-user accounts have been added since the last update, so that the installworld step will be able to use the newly installed system user or system group names without problems.

6. make installworld

   Copies the world from /usr/obj. The new kernel and new world are now installed on disk.

7. mergemaster

   Repeated to update the remaining configuration files, now that the new world is on disk.

8. Reboot.

   A full machine reboot is needed now to load the new kernel and new world with new configuration files.

http://www.freebsd.org/doc/handbook/makeworld.html

Afflib

Per installare le AFFlib ed i relativi tools possiamo usare il sistema dei ports ma con l'utility pkg *. Quindi

pkg_add -r afflib

al termine del download e dell'installazione ci verrà chiesto d'installare il modulo del kernel per i filesystems FUSE e quindi daremo :

pkg_add -r fusefs-kmod

al temine dell'installazione aggiungeemo i seguenti parametri di abilitazione :

echo "fusefs_enable="YES""">>/etc/rc.conf
poi eseguiremo
/usr/local/etc/rc.d/fusefs start
e dunque
sysctl vfs.usermount=1

ora avremo AFFlib ed i tools installati.

AoE - ATA over Ethernet

Target (server)

Il target è di reale semplice installazione, nel caso di FreeBSD, che supporta AoE dal 2006, basterà lanciare compilare il giusto port :

```
#cd /usr/ports/net/vblade
```

```
#make install
```

ed avremo il nostro target compilato, per usarlo basterà :

```
#vblade 0 1 em0 <device>
```

Initiator (client)

Come nel caso dell'iSCSI l'Initiator è il dispositivo che utilizzerà il device a blocchi offerto. Innanzitutto controlliamo che il kernel in uso abbia il modulo precaricato :

```
#grep ATA_OVER /boot/config-`uname -r`
```

se leggiamo :

```
CONFIG_ATA_OVER_ETH=m
```

significa che il modulo è presente ora installiamo i tools

in caso contrario lo configuriamo :

```
Device Drivers -->
        |- Block Devices --->
                |-  <m> ATA over Ethernet support
```

quindi carichiamo il modulo ed assicuriamoci che venga caricato ogni avvio

```
#modprobe aoe
```

```
#echo "aoe" >> /etc/modules
```

Passiamo ora alla vera e propria installzione :

```
#apt-get install aoetools
```

```
#vi /etc/udev/rules.d/25-aoe.rules
```

aggiugiamo le seguenti regole

```
/etc/udev/rules.d/udev.rules:SUBSYSTEM=="aoe",            KERNEL=="discover",           NAME="etherd/%k"
/etc/udev/rules.d/udev.rules:SUBSYSTEM=="aoe",              KERNEL=="err",              NAME="etherd/%k"
/etc/udev/rules.d/udev.rules:SUBSYSTEM=="aoe",          KERNEL=="interfaces",           NAME="etherd/%k"
/etc/udev/rules.d/udev.rules:SUBSYSTEM=="aoe", KERNEL=="revalidate", NAME="etherd/%k"
```

riavviamo Udev

```
#/etc/init.d/udev restart
```

ora potremo realizzare il discovery delle risorse

```
#aoe-discover
```

e poi potremo visualizzare tutte le risorse presenti su quel ramo di rete :

```
#aoe-stat
        e0.1      1GB      eth0 up
```

ora potremo usare il dispositivo identificato come un normale dispositivo a blocchi:

```
#mkfs.ext3 /dev/etherd/e0.1
```

ZFS

http://docs.huihoo.com/opensolaris/solaris-zfs-administration-guide/html/ch06s03.html

Setup ZFS

Per impostare un file system di tipo ZFS, in realtà non sono richieste molte operazioni. Il tutto si riduce a pochi comandi da console. Assicuriamoci che nel file rc.conf sia presente il flag di abilitazione, altrimenti lo inseriamo:

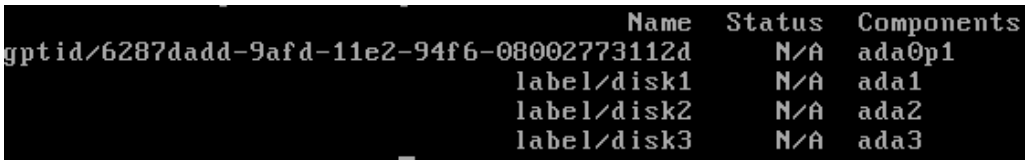
```
#echo 'zfs_enable="YES"' >> /etc/rc.conf
```

Per poter creare il nostro zpool iniziamo con l'identificare i dischi che vorremo usare per comporlo assegnando, inoltre, le label ad ognuno di essi :

```
#glabel label disk1 /dev/ada1
#glabel label disk2 /dev/ada2
#glabel label disk3 /dev/ada3
```

per visualizzare quanto impostato

#glabel status



ora potremo creare il pool (nome= storage) con il seguente comando:

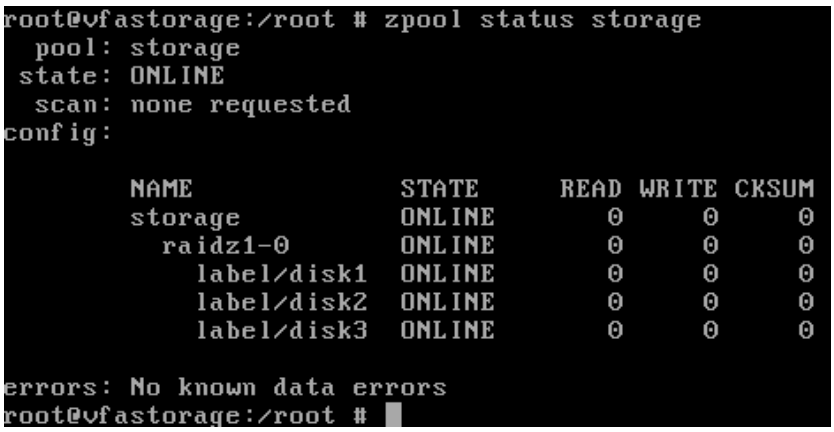
#zpool create storage label/disk1 label/disk2 label/disk3

oppure

#zpool create storage ada1 ada2 ... adan

per visualizzare quanto creato

#zpool status storage



se volessimo vedere le statistiche di uso del pool basterà :

#zpool iostat -v 5 5

Creare un Dataset

Per creare un dataset è necessario il comando :

#zfs create storage/<dataset name>

possiamo abilitare la compressione (gzip) su questo dataset, in questo modo occuperà meno spazio e si comporterà come se fosse un archivio.

#zfs set compression=gzip storage/<dataset name>

ma volendo disabilitare, invece, la compressione su di un'altro dataset, contenuto al suo interno potremo fare :

#zfs set compression=off storage/<dataset name>/<sub dataset>

Quota

Zfs permette di impostare una "quota" con

#zfs set quota=<nr>GB storage/dataset01

#zfs get quota storage/dataset01

Reservation

La funzionalità di Reservation assicura la quota necessaria ad un dataset

#zfs set reservation=<nr>G storage/dataset01

#zfs get reservation storage/dataset01

Snapshot

Nel caso volessimo preservare l'integrità di questo contenitore potremo usare la funzionalità di snapshot. Lo snapshot è una copia read-only di un file syset o di un volume. Il tempo di realizzazione è immediato ed all'inizio non occupa spazio. Lo spazio che lo snapshot può occupare è la differenza fra i dati originali ed i nuovi.

Per eseguire uno snapshot si usa l'apposito comando aggiungendo al termine del nome del dataset il simbolo '@' ed una stringa che lo identifica (di norma un riferimento temporale come la data+ora)

eseguiamo uno snapshot:

#zfs snapshot storage/dataset01@<data time>

elenchiamo tutti gli snapshot presenti :

#zfs list -t snapshot

oppure per elencare tutti gli snapshot di un particolare file system

#zfs list -r -t snapshot -o name,creation storage/dataset01

rinominiamo uno snapshot :

#zfs rename storage/dataset01@<vecchio nome> storage/dataset01@<nuovo nome>

tutti gli snapshots vengono salvati in una directory all'interno del punto di mount del filesystem. Quindi, se storage è montato su /storage, avremo :

/storage/.zfs/snapshot

Rollback

Il rollback è la funzionalità che permette di eliminare tutti i cambiamenti eseguiti su di uno specifico snapshot. Per eseguire il rollback :

#zfs rollback storage/dataset01@<nome snapshot>

in caso di più snapshots è possibile eseguire il rollback contemporaneo di snapshots consecutivi specificando con -r lo snapshot di destinazione, cioè se dovessimo avere :

#zfs list -r -t snapshot -o name,creation storage/dataset01

NAME CREATION

```
storage/dataset01@primo          Mon Mar 13 10:10 2013
storage/dataset01@secondo        Mon Mar 13 10:20 2013
storage/dataset01@terzo          Mon Mar 13 10:30 2013
storage/dataset01@quarto         Mon Mar 13 10:40 2013
```

indicando lo snapshot dataset01@secondo realizzeremo il rollback distruggendo il quarto ed il terzo.

```
#zfs rollback -r storage/dataset01@secondo
```

Clone

Un clone è un volume scrivibile (al contrario dello snapshot) di un file system. La creazione è immediata ed occupa spazio zero, rispetto all'originale. Un clone viene realizzato da, e solo da, uno snapshot. Si instaura una dipendenza da snapshot e clone. Non è possibile distruggere uno snapshot senza aver distrutto il clone.

```
#zfs snapshot storage/dataset01@primo
#zfs clone storage/dataset01@primo storage/nuovadir/altradir/dataset01_primo_clone
```

per impostare proprietà sul clone (share, quota, ecc) :

```
#zfs set sharenfs=on storage/nuovadir/altradir/dataset01_primo_clone
#zfs set quota=<nr>G storage/nuovadir/altradir/dataset01_primo_clone
```

per distruggere un clone :

```
#zfs destroy storage/nuovadir/altradir/dataset01_primo_clone
```

Una delle peculiarità della shell di Zfs è la possibilità di attivare direttamente alcune forme di condivisione (guardare in FreeBSD Shares - Dataset Sharing)

Mount

Zfs esegue automaticamente il mount di un file system e per questo basterà seguire direttamente il path ove è stato creato : cd /storage/dataset01. Nel caso di uno snapshot e quindi di un clone basterà visitare il percorso : /storage/dataset-clone. In caso contrario il comando

```
#zfs mount
```

mostrerà quanto ci serve.

Creare uno ZVOL

```
zfs create -V 1g storage/image0          //un volume di 1GB denominato image0 nello zpool denominato storage
diskinfo -v /dev/zvol/storage/image0
```

```
root@vfastorage:/root # diskinfo -v /dev/zvol/storage/image01
/dev/zvol/storage/image01
        512             # sectorsize
        1073741824      # mediasize in bytes (1.0G)
        2097152         # mediasize in sectors
        0               # stripesize
        0               # stripeoffset
```

Snapshot di ZVOL

Lo snapshot è una istantanea del volume ad un certo istante, questo ci permette di effettuare diverse operazioni evitando di perdere dati per noi importanti.

zfs snapshot storage/image01@20122012
zfs clone storage/image01@201202012 storage/image01_201202013_clone

ora possiamo montarla

mount /dev/zvol/storage/image01_201202013_clone /media/image

ZFS - Command line

ZFS oltre ad essere una tipologia di file-system è anche il nome della utility per gestire quest'ultimo. Di seguito alcuni comandi utili e relative spiegazioni:

creazione di un Dataset

```
#zfs create storage/dataset01
```

creazione di un ZVOL

```
#zfs create -V 10g storage/dataset01/volume01
```

mostra la lista delle condivisioni NFS

#showmount -e

zfs get share rpool/fs1

http://breden.org.uk/2009/05/10/home-fileserver-zfs-file-systems/

http://lildude.co.uk/zfs-cheatsheet

http://docs.oracle.com/cd/E23824_01/html/821-1448/gayne.html

FreeBSD Shares

Dataset Sharing

La shell di gestione di Zfs permette, al momento della creazione di un dataset, di attivarne anche la relativa condivisione in NFS oppure in CIFS (smb). Questo permette di non preoccuparsi a più alto livello di servizi di condivisione oltrechè di condividere puntualmente e secondo regole che decidiamo di volta in volta ogni singolo dataset creato.
Per avviare la condivisione dapprima creiamo il dataset :

```
#zfs create storage/dataset01
```

ora lo condividiamo in NFS
pubblico per tutti

```
#zfs sharenfs="on" storage/dataset01
```

protetto e ristretto alla sola rete

```
#zfs create storage/dataset01/protetta
#zfs sharenfs="-network 10.0.0.0 -mask 255.255.255.0" storage/dataset01/protetta
```

protetto e ristretto al solo client

```
#zfs create storage/dataset01/privata
#zfs sharenfs="-network 10.0.0.67 -mask 255.255.255.255" storage/dataset01/privata
```

le condivisioni vengono registrate in /etc/zfs/exports

```
#zfs get sharenfs
```

visualizza tutte le condivisioni NFS abilitate sui singoli dataset e rispettivi cloni.

NFS

Per installare il server NFS su FreeBSD si devono eseguire poche semplici operazioni, innanzitutto si deve aggiungere ad rc.conf alcune voci, in modo da assicurarci l'avvio al momento del boot :

```
#echo 'nfs_server_enable="YES"' >> /etc/rc.conf
#echo 'nfs_server_flags="-u -t -n 4"' >> /etc/rc.conf
#echo 'rpcbind_enable="YES"' >> /etc/rc.conf
#echo 'rpc_lockd_enable="YES"' >> /etc/rc.conf
#echo 'rpc_statd_enable="YES"' >> /etc/rc.conf
#echo 'mountd_flags="-r"' >> /etc/rc.conf
#echo 'mountd_enable="YES"' >> /etc/rc.conf
```

aggiungiamo al file exports le directory con relativi path, che vogliamo condividere :

```
#vi /etc/exports
```

nel nostro caso

```
/storage -maproot=vfa-analisi  -network 192.168.56 -mask 255.255.255.0
```

ora avviamo il server

```
rpcbind
nfsd -u -t -n 4
mountd -r
```

nel caso volessimo caricare qualsiasi cambiamento al file exports possiamo eseguire :

```
/etc/rc.d/mountd onereload
```

mentre se volessimo listare tutte le shares :

```
showmount -e
```

Lato client (linux), invece ci basterà lanciare il comando mount seguito da indirizzo ip del server:path alla share oltre al mountpoint locale:

```
mount 192.168.56.101:/storage /vfastorage
```

CIFS

Installare samba
cd /usr/ports/net/samba36
make install

http://www.us-webmasters.com/FreeBSD/Install/Samba/

```
echo 'samba_enable="YES"' >> /etc/rc.conf
```

dopo l'installazione personalizziamo smb.conf

```
vi /usr/local/etc/smb.conf
```

ad esempio

```
[global]
        server string = VFA Storage
        netbios name = VFA
        security = user
        interfaces = em0
        log level = 3
        log file = /var/log/samba/log.%m
        max log size = 50
        load printers = No
        os level = 39
        dns proxy = No
        socket options = TCP_NODELAY
        allow hosts = 192.168.56.0/24
        idmap config * : range = 9999 - 99999
        idmap config * : backend = tdb
```

creaiamo una share

aggiungiamo un dataset

```
zfs create storage/dataset01
```

gruppo di utenti che avranno accesso a questo dataset

```
pw groupadd <nome gruppo >
```

ora creiamo gli utenti che accederanno al dataset

```
pw useradd <nome utente > -s /bin/sh
echo "<password >" | pw usermod <nome utente > -h 0
pw groupadd <dataset> -M <utente>,<utente>,..,<utente>
chgrp <nome gruppo> /storage/<dataset>
chmod 770 /storage/<dataset>
```

```
[dataset01]
        comment = ZFS <dataset>
        path = /storage/<dataset>
        guest ok = no
        browseable = yes
        public = no
        writable = yes
        read list = @<groupname>
        valid users = @vfa, @<groupname>
        write list = @vfa
        create mask = 0770
        force create mode = 0770
        security mask = 0770
        force security mode = 0770
        directory mask = 2770
        force directory mode = 2770
        directory security mask = 2770
        force directory security mode = 2770
```

Ricordarsi di abilitare a 777 la root dello storage e poi a 777 il dataset altrimento all'interno di quest'ultio sarà impossibile operare.
In merito ai proprietari : la root dello storage roo:wheel il datatset roo:<groupname> così che tutti gli appartenenti al gruppo potranno leggere.

ora abilitiamo SWAT de-commentando la relativa riga in inetd.conf

```
vi /etc/inetd.conf
```

```
swat    stream  tcp     nowait/400      root    /usr/local/sbin/swat    swat
```

e poi ricarichiamo

```
/etc/rc.d/inetd onereload
```

ora possiamo visitare la pagina di configurazione di swat

https://<server ip> :901

http://doub.home.xs4all.nl/samba-ldap/index.html

Aggiungere un utente a samba :

smbpasswd -a <nome utente> ed alla richiesta di password inserirla, oppure

$(echo "password"; echo "password") | smbpasswd -s -a <nome utente>

Elencare tutti gli utenti samba

pdbedit -L oppure più verboso pdbedit -L -v

Cancellare un utente

pdbedit -x -u <nome utente>

http://www.samba.org/samba/docs/man/manpages-3/pdbedit.8.html

iSCSI

Per implementare un iSCSI target dobbiamo installare il port istgt

```
cd /usr/ports/net/istgt
```

quindi compiliamo il port

```
make install
```

ora passiamo alla configurazione, copiando e personalizzando i tre file di configurazione di esempio:

```
cd /usr/local/etc/istgt
cp /usr/local/etc/istgt/auth.conf.sample  /usr/local/etc/istgt/auth.conf
cp /usr/local/etc/istgt/istgt.conf.sample  /usr/local/etc/istgt/istgt.conf
cp /usr/local/etc/istgt/istgtcontrol.conf.sample  /usr/local/etc/istgt/istgtcontrol.conf
```

editiamo i predetti files come segue :

Auth.conf (registra le credenziali di accesso - CHAP - MutualCHAP -)

In questo file vengono memorizzate le credenziali per l'autenticazione. Si definiscono dei gruppi di autenticazione (AuthGroup) all'interno dei quali s'inseriscono le credenziali.
#[AuthGroupName]
Auth "<chap target username>" "<chap target password>" "<mutualchap initiator username>" "<mutualchap initiator password>"

Esempio di autenticazione CHAP
[AuthGroup1]
Auth "client01" "client01password" "" ""

Esempio di autenticazione MutualCHAP
[AuthGroup2]
Auth "targetclient01" "targetclient01password" "initclient01" "initclient01password"

[AuthGroup10000]
 Comment "Group for unit controller"

Auth "ctluser" "test" "mutualuser" "mutualsecret"

istgt.conf (file delle impostazioni)

In questo file sono registrate le impostazioni globali del target tra cui :

```
[Global]
  Comment "Global section"
  # node name (not include optional part)
  NodeBase "iqn.2013-01.vfa.istgt"                                  nome del nodo
  # files
  PidFile /var/run/istgt.pid
  AuthFile /usr/local/etc/istgt/auth.conf                           file delle credenziali
  # directories
  # for removable media (virtual DVD/virtual Tape)
  # MediaDirectory /var/istgt
  # syslog facility
  LogFacility "local7"
  # socket I/O timeout sec. (polling is infinity)
  Timeout 30
  # NOPIN sending interval sec.
  NopInInterval 20
  # authentication information for discovery session
  DiscoveryAuthMethod Auto
  DiscoveryAuthGroup AuthGroup10000                                 tipo di autenticazione
  #DiscoveryAuthGroup AuthGroup9999                                 Auto = CHAP + MultiCHAP
  # reserved maximum connections and sessions
  # NOTE: iSCSI boot is 2 or more sessions required
  MaxSessions 16
  MaxConnections 12
  # maximum number of sending R2T in each connection
  # actual number is limited to QueueDepth and MaxCmdSN and ExpCmdSN
  # 0=disabled, 1-256=improves large writing
  MaxR2T 32
  # iSCSI initial parameters negotiate with initiators
  # NOTE: incorrect values might crash
  MaxOutstandingR2T 16
  DefaultTime2Wait 2
  DefaultTime2Retain 60
  FirstBurstLength 262144
  MaxBurstLength 1048576
  MaxRecvDataSegmentLength 262144
  # NOTE: not supported
  InitialR2T Yes
  ImmediateData Yes
  DataPDUInOrder Yes
  DataSequenceInOrder Yes
  ErrorRecoveryLevel 0

[UnitControl]
  Comment "Internal Logical Unit Controller"
  #AuthMethod Auto
  AuthMethod CHAP Mutual
  AuthGroup AuthGroup10000
  # this portal is only used as controller (by istgtcontrol)
  # if it's not necessary, no portal is valid
  #Portal UC1 [::1]:3261
  Portal UC1 127.0.0.1:3261
```

```
  # accept IP netmask
  #Netmask [::1]
  Netmask 127.0.0.1

# You should set IPs in /etc/rc.conf for physical I/F
[PortalGroup1]
  Comment "SINGLE PORT TEST"
  # Portal Label(not used) IP(IPv6 or IPv4):Port
  #Portal DA1 [2001:03e0:06cf:0003:021b:21ff:fe04:f405]:3260
  Portal DA1 192.168.56.102:3260                          IP + port del Portal
                                                          se 0.0.0.0 tutti gl'ip
[InitiatorGroup1]
  Comment "Initiator Group1"
  # name with ! deny login/discovery
  #InitiatorName "!iqn.1991-05.com.microsoft:moon"
  # specified name allow login/discovery
  #InitiatorName "iqn.1991-05.com.microsoft:saturn"
  # special word "ALL" match all of initiators
  InitiatorName "ALL"                                     Any Initiator Name
  Netmask 192.168.56.0/24                                 from this network

# TargetName, Mapping, UnitType, LUN0 are minimum required
[LogicalUnit1]
  Comment "iSCSI Disk"
  # full specified iqn (same as below)
  #TargetName iqn.2007-09.jp.ne.peach.istgt:disk1
  # short specified non iqn (will add NodeBase)
  TargetName idisk1
  TargetAlias "Data Disk1"
  # use initiators in tag1 via portals in tag1
  Mapping PortalGroup1 InitiatorGroup1
  # accept both CHAP and None
  #AuthMethod Auto
  AuthMethod CHAP
  AuthGroup AuthGroup1
  #UseDigest Header Data
  UseDigest Auto
  UnitType Disk
  # SCSI INQUIRY - Vendor(8) Product(16) Revision(4) Serial(16)
  #UnitInquiry "FreeBSD" "iSCSI Disk" "0123" "10000001"
  # Queuing 0=disabled, 1-255=enabled with specified depth.
  #QueueDepth 32

  # override global setting if need
  #MaxOutstandingR2T 16
  #DefaultTime2Wait 2
  #DefaultTime2Retain 60
  #FirstBurstLength 262144
  #MaxBurstLength 1048576
  #MaxRecvDataSegmentLength 262144
  #InitialR2T Yes
  #ImmediateData Yes
  #DataPDUInOrder Yes
  #DataSequenceInOrder Yes
  #ErrorRecoveryLevel 0

  # LogicalVolume for this unit on LUN0
  # for file extent
  #LUN0 Storage /tank/iscsi/istgt-disk1 10GB
  # for raw device extent
```

```
#LUN0 Storage /dev/ad4 Auto
# for ZFS volume extent
#LUN0 Storage /dev/zvol/tank/istgt-vol1 Auto
LUN0 Storage /dev/zvol/storage/PP1234/idisk1 Auto

# override the serial of LUN0 specified with UnitInquiry
#LUN0 Option Serial "10000001"

# for 3.5inch, 7200rpm HDD
# RPM 0=not reported, 1=non-rotating(SSD), n>1024 rpm
#LUN0 Option RPM 7200
# FormFactor 0=not reported, 1=5.25, 2=3.5, 3=2.5, 4=1.8, 5=less 1.8 inch
#LUN0 Option FormFactor 2

# for 2.5inch, SSD
#LUN0 Option RPM 1
#LUN0 Option FormFactor 3

# for future use (enabled by default)
#LUN0 Option ReadCache Disable

# control WCE(mode page 8) and O_FSYNC/O_SYNC on the backing store (enabled by default)
#LUN0 Option WriteCache Disable
```

istgtcontrol.conf

The istgtcontrol is a remote program to operate removable media, and to get information and to reset some conditions. The istgt can provide virtual tape device based on LTO/DLT, and CD/DVD device. (still experimental)

```
[Global]
  Comment "Sample Configuration"
  Timeout 60

  AuthMethod CHAP Mutual
  Auth "ctluser" "test" "mutualuser" "mutualsecret"

  Host localhost
  Port 3261

  TargetName "iqn.2011-06.net.example.tests:testdisk"
  Lun 0

  Flags "ro"
  Size "auto"
```

UBUNTU

Root Access

Per abilitare l'accesso come root basta

```
sudo passwd root
```

ed alla successiva richiesta di password inserire il valore desiderato (due volte) al termine potremo eseguire logout - login come root.

ZFS

```
sudo -i

apt-get install linux-headers-`uname -r` linux-headers-generic build-essential
```

apt-get install python-software-properties

```
apt-add-repository ppa:zfs-native/stable
apt-get update
apt-get install ubuntu-zfs
```

iSCSI

sudo aptitude install iscsitarget iscsitarget-source iscsitarget-dkms

vi /etc/default/iscsitarget.

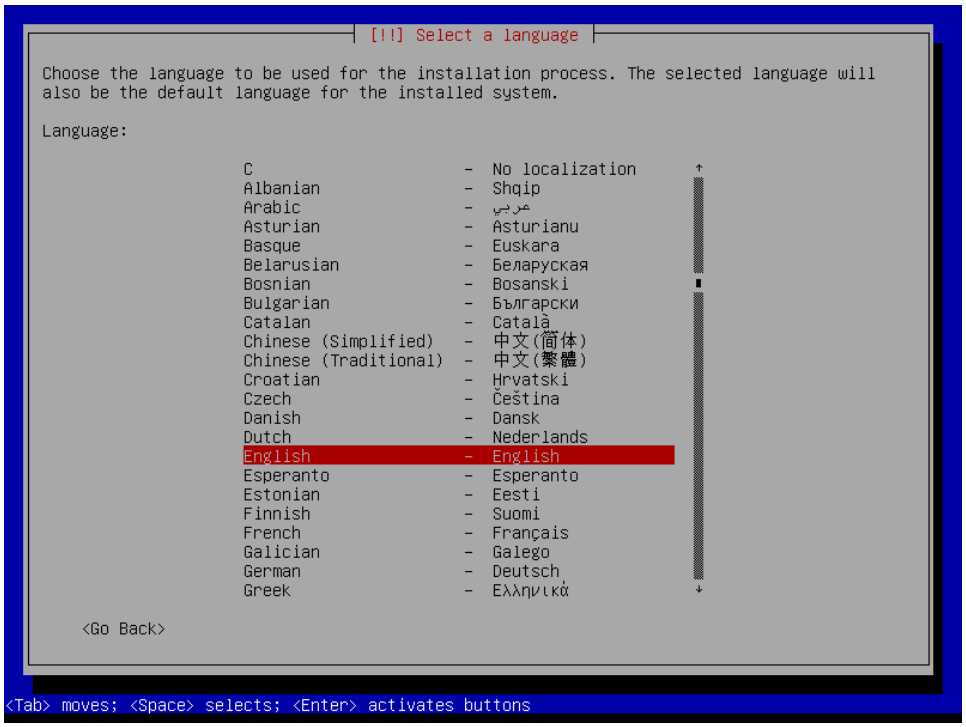
cambiamo da fale a true il valore di ISCSITARGET_ENABLE

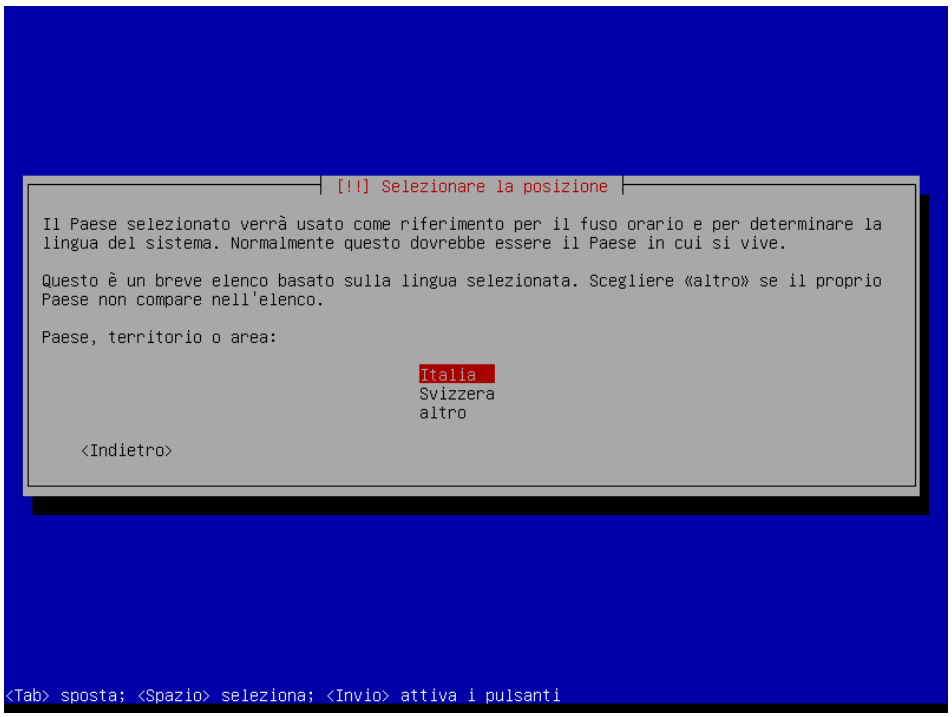
Samba

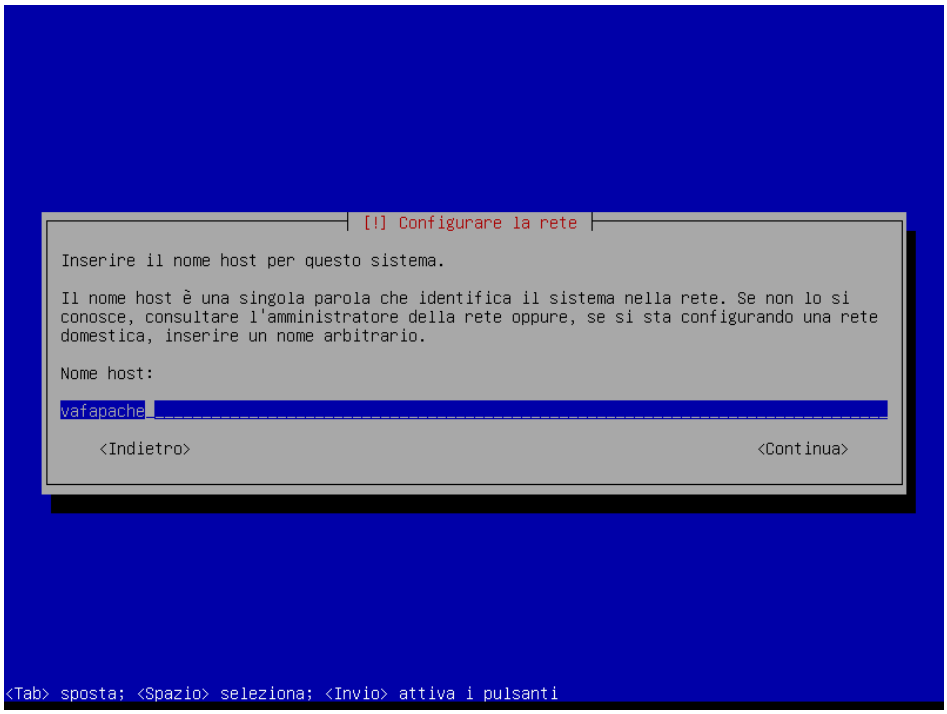
VirtualBox

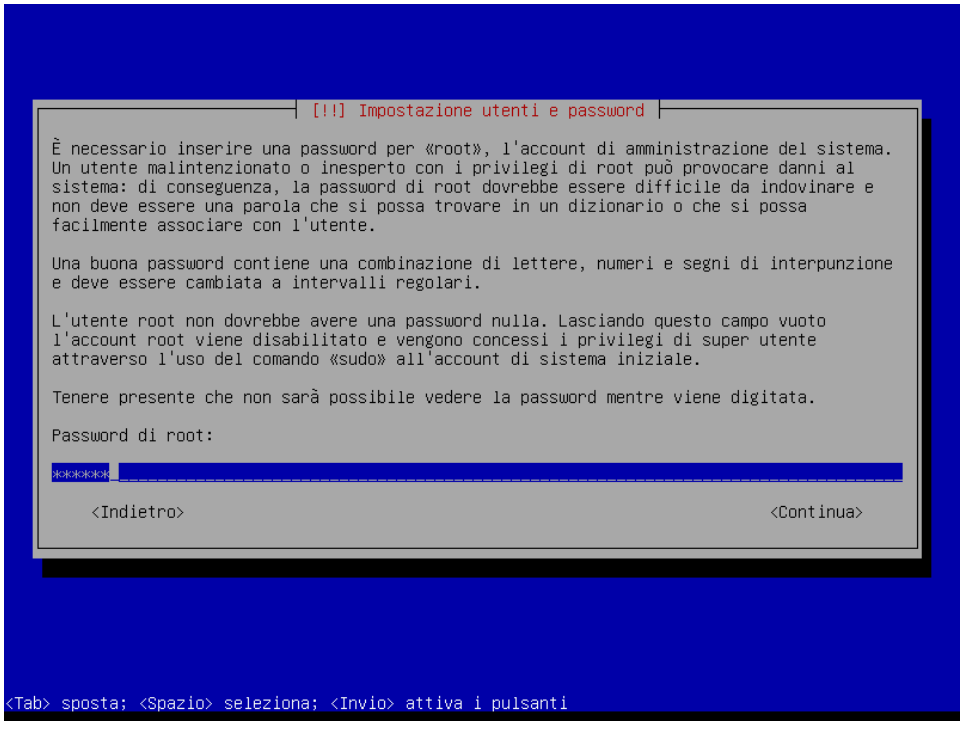
```
echo "deb http://download.virtualbox.org/virtualbox/debian $(lsb_release -sc)
contrib" | sudo tee /etc/apt/sources.list.d/virtualbox.list
wget -q
http://download.virtualbox.org/virtualbox/debian/oracle_vbox.asc -O- | sudo
apt-key add -
sudo apt-get update
sudo apt-get install virtualbox-4.1
```

DEBIAN Installazione base


[!!] Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
C - No localization
Albanian - Shqip
Arabic - عربي
Asturian - Asturianu
Basque - Euskara
Belarusian - Беларуская
Bosnian - Bosanski
Bulgarian - Български
Catalan - Català
Chinese (Simplified) - 中文(简体)
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
German - Deutsch
Greek - Ελληνικά
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

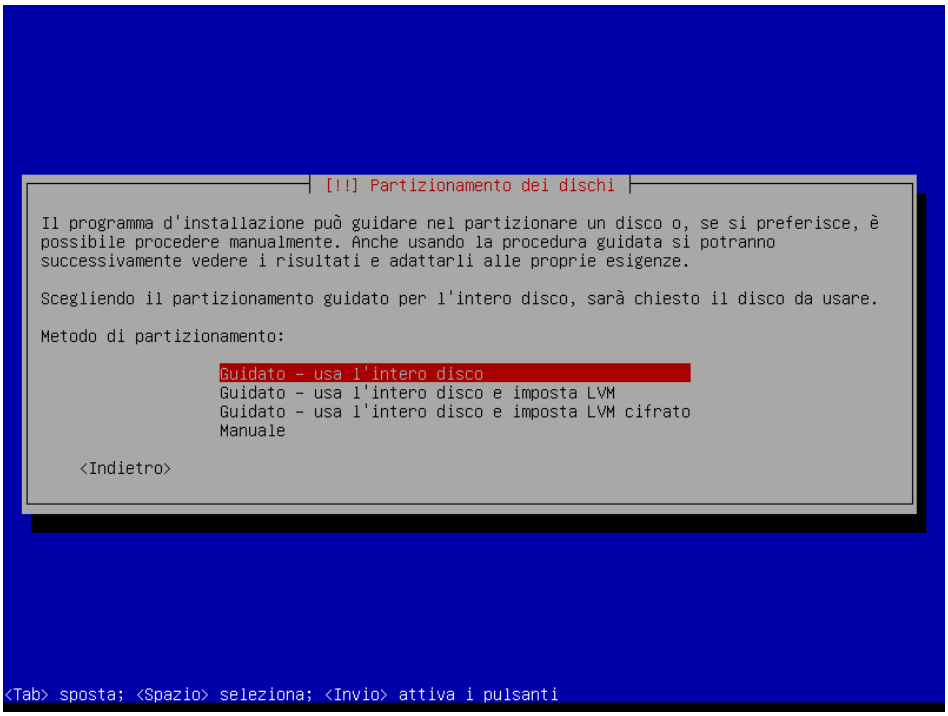

[!!] Selezionare la posizione
Il Paese selezionato verrà usato come riferimento per il fuso orario e per determinare la lingua del sistema. Normalmente questo dovrebbe essere il Paese in cui si vive.
Questo è un breve elenco basato sulla lingua selezionata. Scegliere «altro» se il proprio Paese non compare nell'elenco.
Paese, territorio o area:
Italia
Svizzera
altro
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

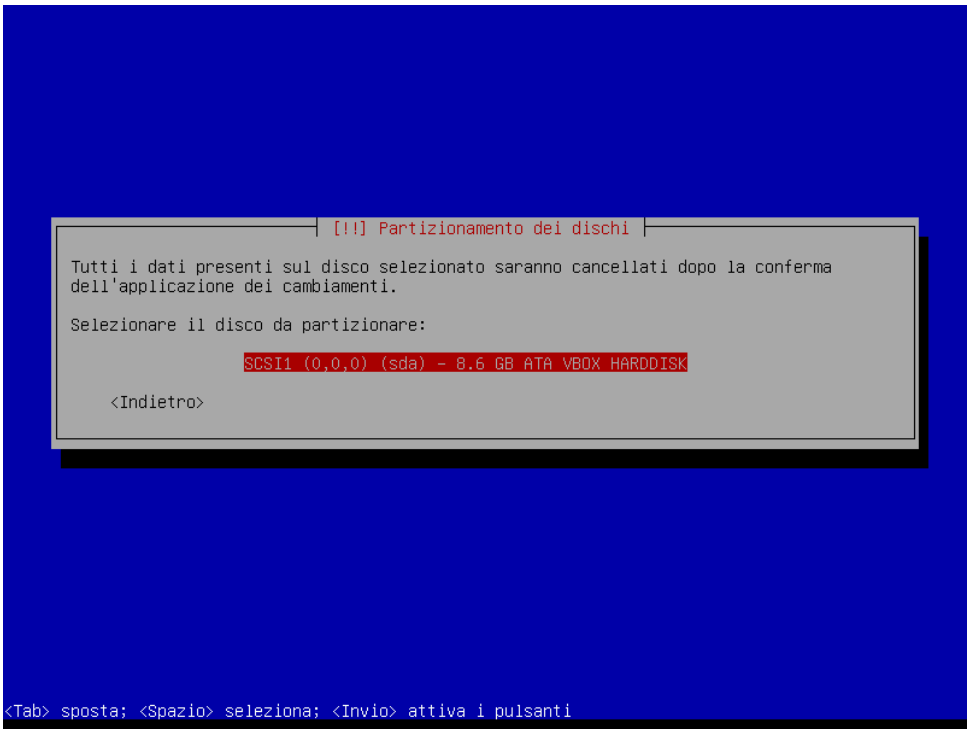

[!] Configurare la rete
Inserire il nome host per questo sistema.
Il nome host è una singola parola che identifica il sistema nella rete. Se non lo si conosce, consultare l'amministratore della rete oppure, se si sta configurando una rete domestica, inserire un nome arbitrario.
Nome host:
vafapache
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

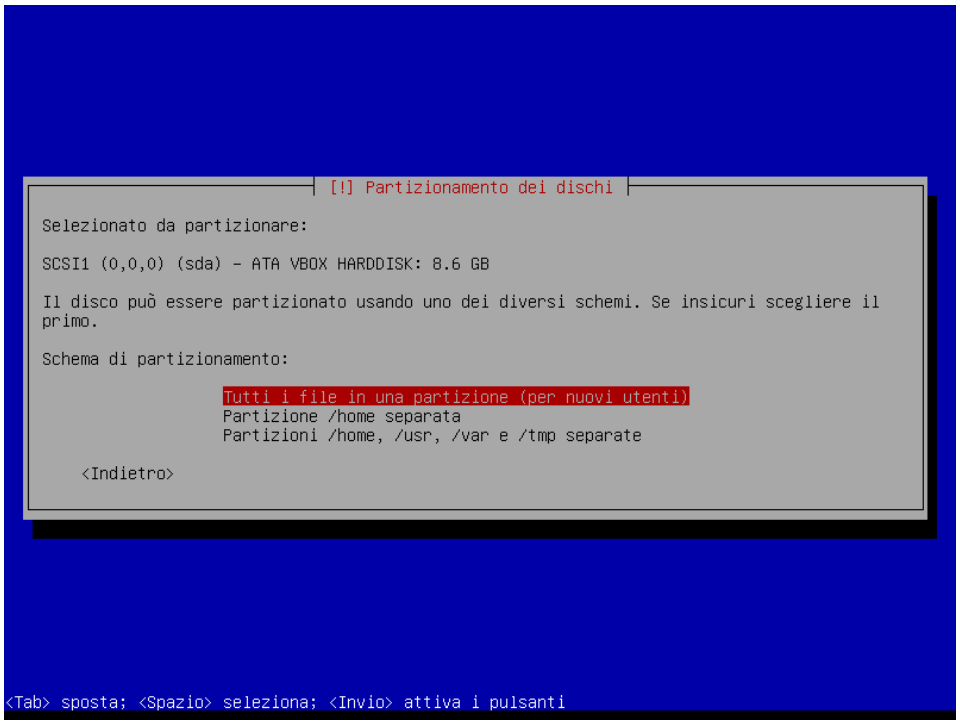

[!!] Impostazione utenti e password
È necessario inserire una password per «root», l'account di amministrazione del sistema. Un utente malintenzionato o inesperto con i privilegi di root può provocare danni al sistema: di conseguenza, la password di root dovrebbe essere difficile da indovinare e non deve essere una parola che si possa trovare in un dizionario o che si possa facilmente associare con l'utente.
Una buona password contiene una combinazione di lettere, numeri e segni di interpunzione e deve essere cambiata a intervalli regolari.
L'utente root non dovrebbe avere una password nulla. Lasciando questo campo vuoto l'account root viene disabilitato e vengono concessi i privilegi di super utente attraverso l'uso del comando «sudo» all'account di sistema iniziale.
Tenere presente che non sarà possibile vedere la password mentre viene digitata.
Password di root:
******
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

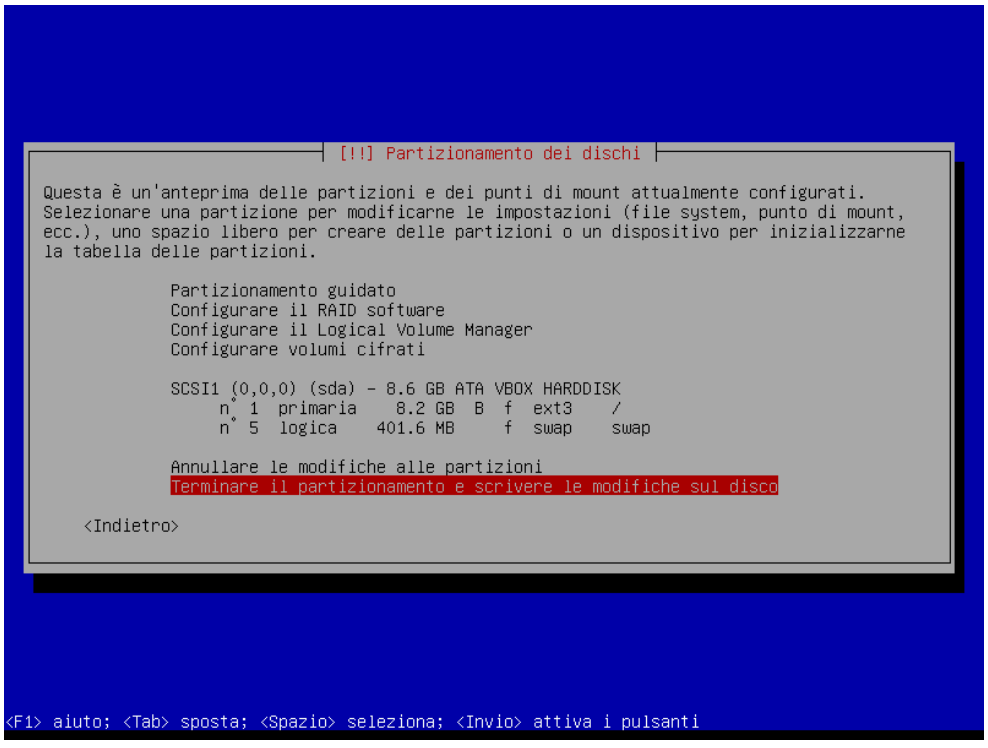

[!!] Impostazione utenti e password
Verrà ora creato un account utente da usare al posto dell'account di root per le attività normali, che non riguardano l'amministrazione del sistema.
Inserire il vero nome di questo utente, per esempio nome e cognome. Questa informazione viene usata per indicare il mittente delle email e da altri programmi che mostrano o usano il nome completo dell'utente.
Nome completo del nuovo utente:
vafapache
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

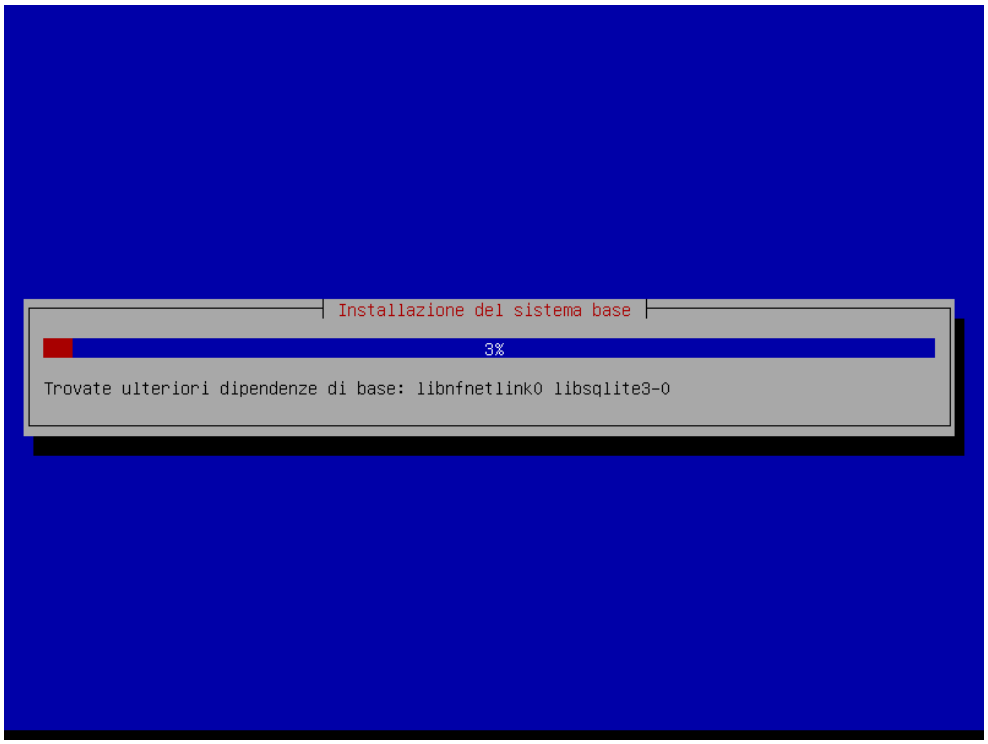
[!!] Impostazione utenti e password
Una buona password contiene una combinazione di lettere, numeri e segni di interpunzione e deve essere cambiata a intervalli regolari.
Scegliere una password per il nuovo utente:
******
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

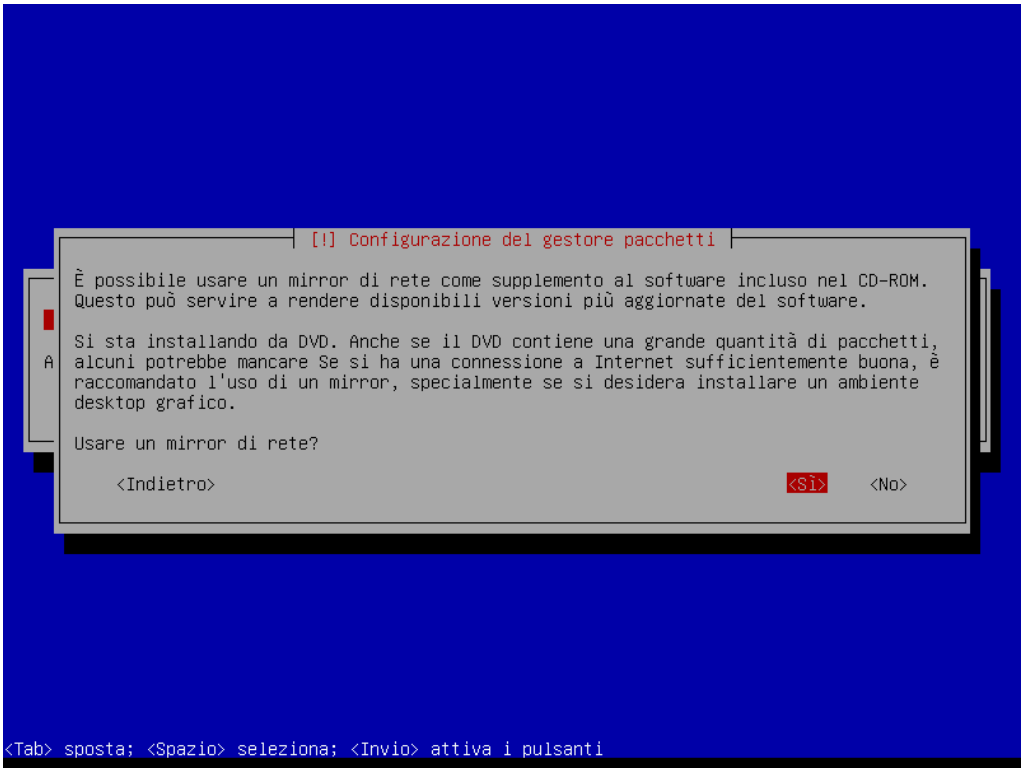

[!!] Partizionamento dei dischi
Il programma d'installazione può guidare nel partizionare un disco o, se si preferisce, è possibile procedere manualmente. Anche usando la procedura guidata si potranno successivamente vedere i risultati e adattarli alle proprie esigenze.
Scegliendo il partizionamento guidato per l'intero disco, sarà chiesto il disco da usare.
Metodo di partizionamento:
Guidato - usa l'intero disco
Guidato - usa l'intero disco e imposta LVM
Guidato - usa l'intero disco e imposta LVM cifrato
Manuale
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

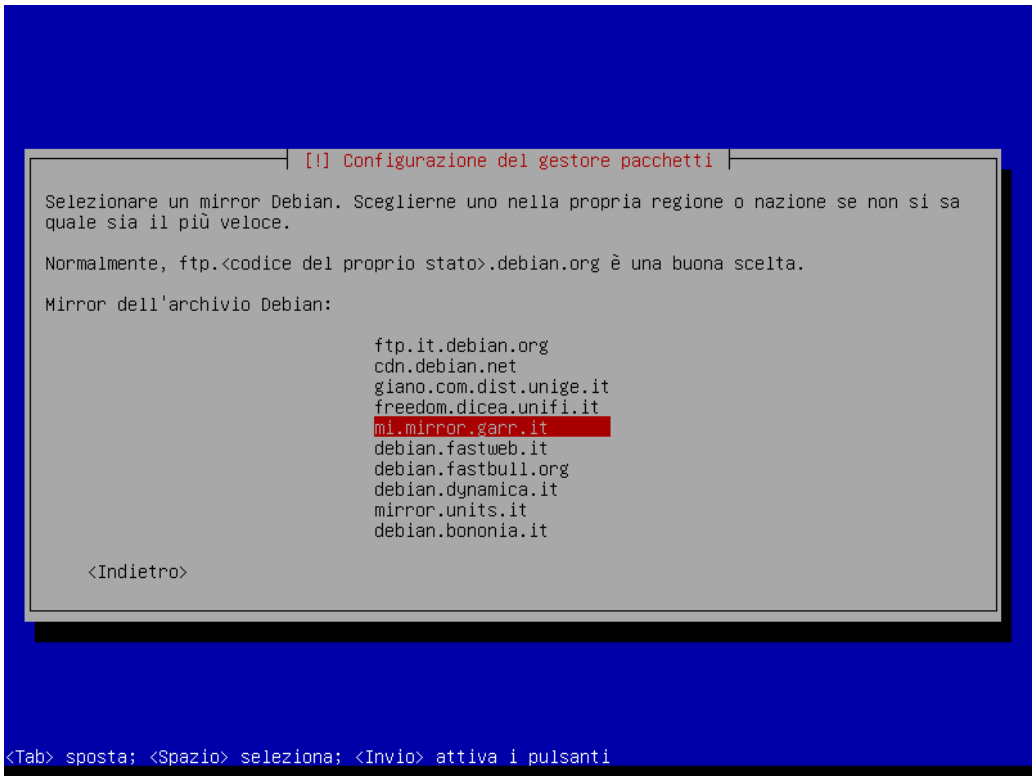

[!!] Partizionamento dei dischi
Tutti i dati presenti sul disco selezionato saranno cancellati dopo la conferma dell'applicazione dei cambiamenti.
Selezionare il disco da partizionare:
SCSI1 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

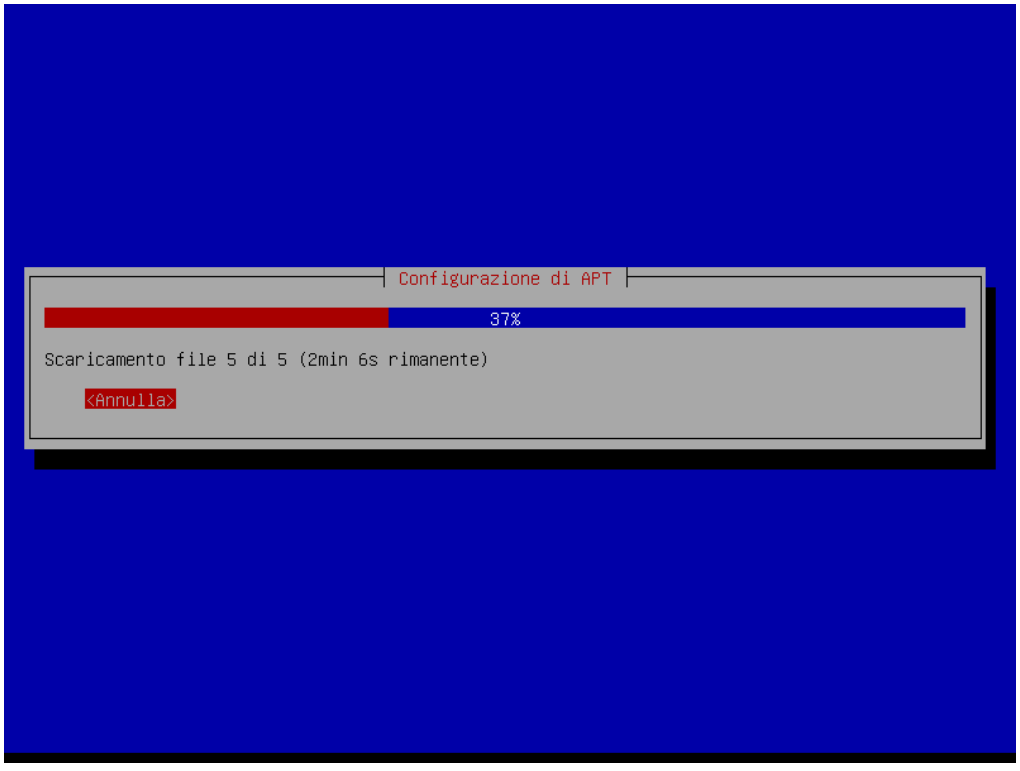

[!] Partizionamento dei dischi
Selezionato da partizionare:
SCSI1 (0,0,0) (sda) - ATA VBOX HARDDISK: 8.6 GB
Il disco può essere partizionato usando uno dei diversi schemi. Se insicuri scegliere il primo.
Schema di partizionamento:
Tutti i file in una partizione (per nuovi utenti)
Partizione /home separata
Partizioni /home, /usr, /var e /tmp separate
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

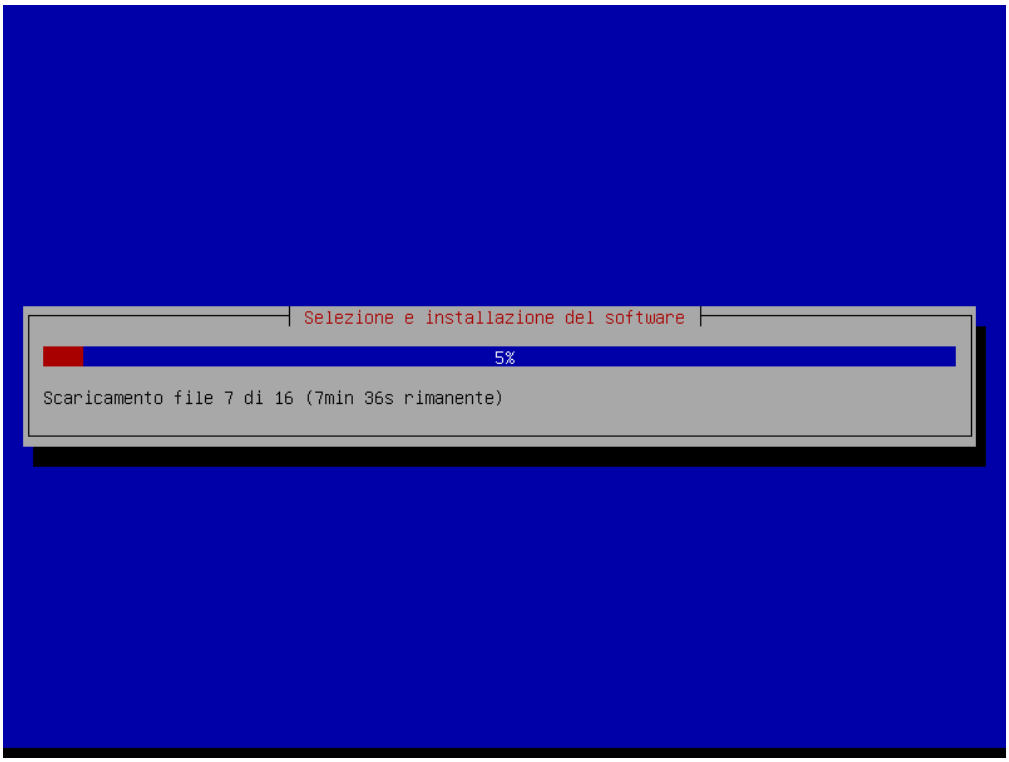

[!!] Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati. Selezionare una partizione per modificarne le impostazioni (file system, punto di mount, ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne la tabella delle partizioni.
Partizionamento guidato
Configurare il RAID software
Configurare il Logical Volume Manager
Configurare volumi cifrati
SCSI1 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
n° 1 primaria 8.2 GB B f ext3 /
n° 5 logica 401.6 MB f swap swap
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

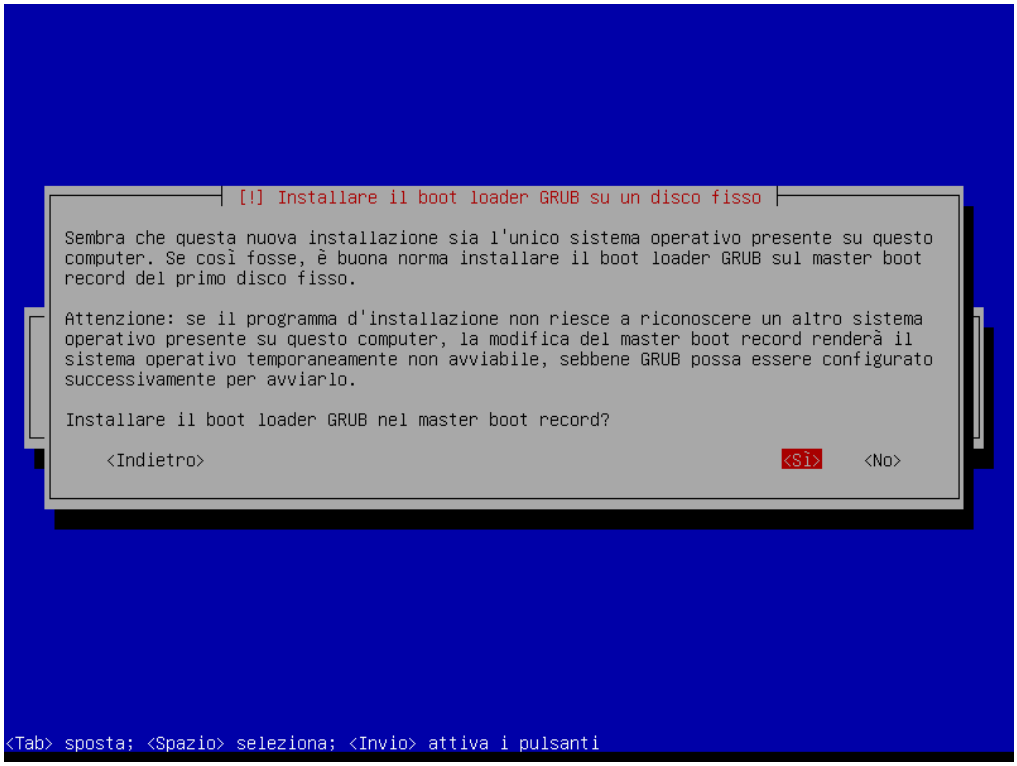

Installazione del sistema base
3%
Trovate ulteriori dipendenze di base: libnfnetlink0 libsqlite3-0

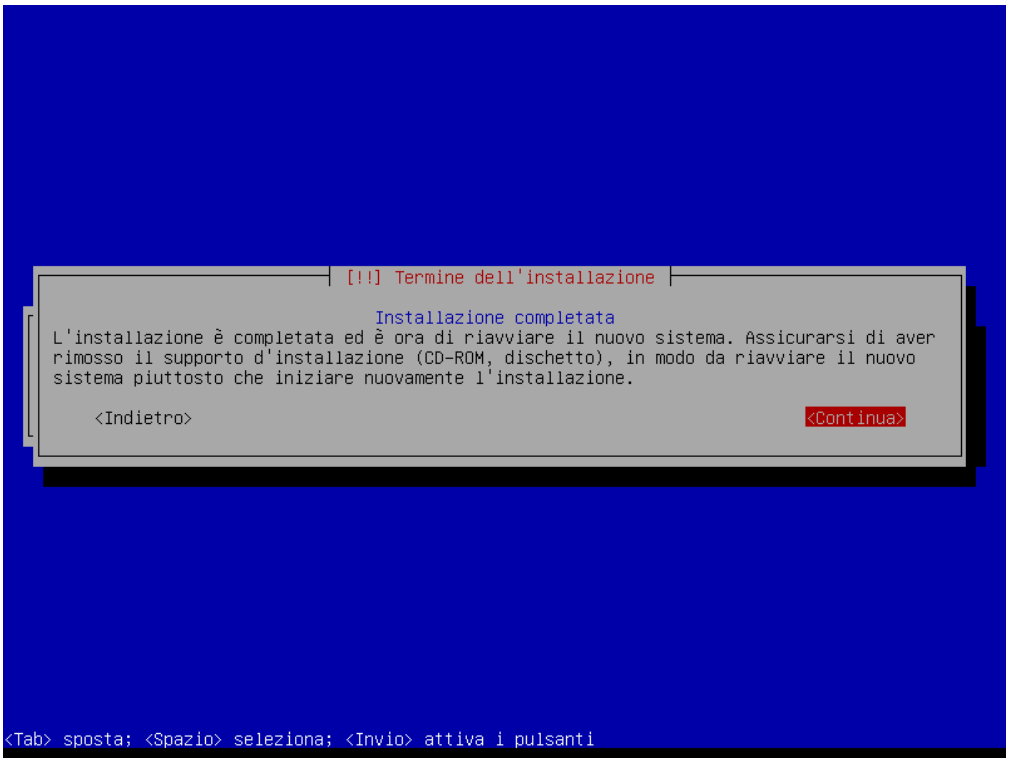

[!] Configurazione del gestore pacchetti
È possibile usare un mirror di rete come supplemento al software incluso nel CD-ROM.
Questo può servire a rendere disponibili versioni più aggiornate del software.
Si sta installando da DVD. Anche se il DVD contiene una grande quantità di pacchetti,
alcuni potrebbe mancare Se si ha una connessione a Internet sufficientemente buona, è
raccomandato l'uso di un mirror, specialmente se si desidera installare un ambiente
desktop grafico.
Usare un mirror di rete?
<Indietro>
<Sì>
<No>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


[!] Configurazione del gestore pacchetti
Selezionare un mirror Debian. Sceglierne uno nella propria regione o nazione se non si sa quale sia il più veloce.
Normalmente, ftp.<codice del proprio stato>.debian.org è una buona scelta.
Mirror dell'archivio Debian:
ftp.it.debian.org
cdn.debian.net
giano.com.dist.unige.it
freedom.dicea.unifi.it
mi.mirror.garr.it
debian.fastweb.it
debian.fastbull.org
debian.dynamica.it
mirror.units.it
debian.bononia.it
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


Configurazione di APT
37%
Scaricamento file 5 di 5 (2min 6s rimanente)
<Annulla>


Selezione e installazione del software
5%
Scaricamento file 7 di 16 (7min 36s rimanente)


[!] Installare il boot loader GRUB su un disco fisso
Sembra che questa nuova installazione sia l'unico sistema operativo presente su questo computer. Se così fosse, è buona norma installare il boot loader GRUB sul master boot record del primo disco fisso.
Attenzione: se il programma d'installazione non riesce a riconoscere un altro sistema operativo presente su questo computer, la modifica del master boot record renderà il sistema operativo temporaneamente non avviabile, sebbene GRUB possa essere configurato successivamente per avviarlo.
Installare il boot loader GRUB nel master boot record?
<Indietro>
<Sì>
<No>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


[!!] Termine dell'installazione
Installazione completata
L'installazione è completata ed è ora di riavviare il nuovo sistema. Assicurarsi di aver rimosso il supporto d'installazione (CD-ROM, dischetto), in modo da riavviare il nuovo sistema piuttosto che iniziare nuovamente l'installazione.
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

Per la realizzazione dei diversi database di appoggio è stato scelta la combinazione Apache + MySQL + PHP. Per ovvie ragioni di sicurezza nonchè per diminuire l'incidenza dei tempi di downtime si è optato per separare il database dall'interfaccia web.

MySQL

L'installazione e la configurazione del database, grazie ai sistemi di packet-managing ad oggi presenti in tutte le distribuzioni resta molto semplice ed affidabile (la nostra sarà Debian).

In realtà vi saranno due server MySQL indipendenti,
1) gestione dell'intero sistema, Autenticazione, Gestione supporti , Gestione del caso in generale, ecc.
2) memorizzazione esiti attività di Computer Forensic e relativa gestione del singolo caso oltre ad essere sorgente del sistema di Reporting.

L'installazione seguirà le impostazioni di default sino ad avere l'interfaccia a riga di comando ed il prompt.

```
apt-get update
apt-get install mysql-server mysql-client
```

durante l'installazione potremo inserire la password di amministratore. (es.: forlex)

Inoltre, per semplicità configuriamo il server per essere gestito attraverso interfaccia grafica (PHPMyAdmin) residente su un'altro server (server di front-end).
Quindi impartiremo i seguenti comandi :

```
mysql -u root -p
Enter password : <password >
```

creiamo un utente "pmaroot" e lo accreditiamo presso il server concedendogli tutti i privilegi su tutte le tabelle (segno %).

```
mysql> CREATE USER 'pmaroot'@'%' IDENTIFIED BY 'forlex';
mysql> GRANT ALL PRIVILEGES ON *.* TO pmaroot@'%';
```

quindi commentiamo all'interno del file /etc/mysql/my.conf le seguenti righe :

```
#bind-address=192.168.56.105
#bind-address=localhost
```

così da aprire il sql server alla gestione da altri indirizzi IP.

In seguito testeremo la buona riuscita della configurazione provando a collegarci da un'altra macchina con client mysql impartendo il seguente comando :

```
mysql -u pmaroot -h 192.168.56.105 -p
```

se dopo aver inserito la password, riceveremo un feedback positivo, significa che il server potrà essere amministrato anche da altre macchine.

Apache + PHP (over SSL)

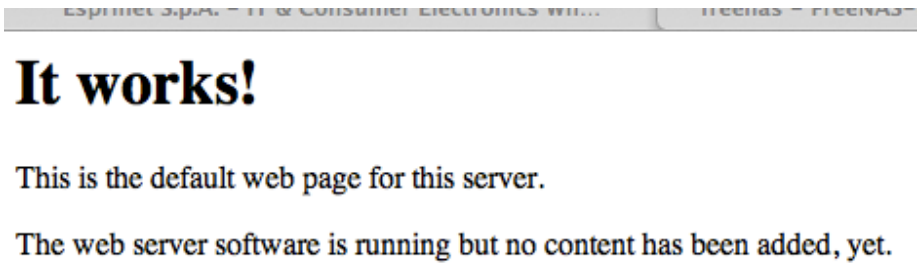
L'installazione del server web e del relativo modulo per l'interprete PHP verrà eseguita su una macchina con S.O: Debian la quale avrà funzioni d'interfaccia alle diverse opzioni offerte dal sistema.

Installiamo il server http (Apache 2) e l'interprete PHP oltre al relativo modulo per il server web (libapache2-mod-php5).

```
apt-get install apache2 php5 libapache2-mod-php5 mysql-server
```

```
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti saranno inoltre installati:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common file
  libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libcap2
  libdb4.7 libgnutls26 libldap-2.4-2 libmagic1 libonig2 libpcre3 libqdbm14
  libsasl2-2 libsasl2-modules libtasn1-3 libxml2 mime-support openssl perl
  perl-modules php5-cli php5-common php5-suhosin sgml-base ssl-cert xml-core
Pacchetti suggeriti:
  www-browser apache2-doc apache2-suexec apache2-suexec-custom php-pear
  gnutls-bin libsasl2-modules-otp libsasl2-modules-ldap libsasl2-modules-sql
  libsasl2-modules-gssapi-mit libsasl2-modules-gssapi-heimdal ca-certificates
  perl-doc libterm-readline-gnu-perl libterm-readline-perl-perl sgml-base-doc
  openssl-blacklist debhelper
I seguenti pacchetti NUOVI saranno installati:
  apache2 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common
  file libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libcap2 libdb4.7 libgnutls26 libldap-2.4-2 libmagic1
  libonig2 libpcre3 libqdbm14 libsasl2-2 libsasl2-modules libtasn1-3 libxml2
  mime-support openssl perl perl-modules php5 php5-cli php5-common
  php5-suhosin sgml-base ssl-cert xml-core
0 aggiornati, 34 installati, 0 da rimuovere e 0 non aggiornati.
È necessario scaricare 18,5 MB/21,3 MB di archivi.
Dopo quest'operazione, verranno occupati 71,7 MB di spazio su disco.
Continuare [S/n]? _
```

Testiamo il funzionamento visitando l'indirizzo IP sul quale il server offre la relativa pagina di conferma



successivamente, non usufruendo di un sistema DNS, configuriamo il file hosts per associare gl'indirizzi IP ai relativi server MySQL precedentemente installati e comunque ricordiamo la seguente associazione :

192.168.56.105()	vafmysqlauth
192.168.56.106()	vafmysqlcase
192.168.56.107()	vafmysqlanalisys

```
vi /etc/hosts
```

ed aggiungiamo le seguenti righe

```
192.168.56.105  vafmysqlauth
192.168.56.106  vafmysqlcase
192.168.56.107  vafmysqlanalisys
```

Installazione di OpenSSL

Iniziamo con installare OpenSSL

```
apt-get install openssl
```

Ora dobbiamo creare un certificato digitale per il server che ne garantisca l'identità.

Il certificato deve contenere:

- Una chiave pubblica
- Le informazioni riguardanti la propria identità
- Una firma digitale di una organizzazione che certifica il legame tra informazioni identificative e chiave pubblica

quindi creiamo innanzitutto una directory che contenga i certificati :

```
mkdir /root/certificates
```

creiamo il file che utilizzerà openssl per generare i propri certificati, openssl.cnf

```
vi /root/certificates/openssl.cnf
```

ed inseriamogli il seguente testo :

```
[ req ]
default_md = sha1
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
countryName = Country
countryName_default = IT
countryName_min = 2
countryName_max = 2
localityName = Locality
localityName_default = Bologna
organizationName = Organization
organizationName_default = VFA
commonName = Common Name
commonName_max = 64

[ certauth ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints = CA:true
crlDistributionPoints = @crl

[ server ]
```

```
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
nsCertType = server
crlDistributionPoints = @crl

[ client ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = clientAuth
nsCertType = client
crlDistributionPoints = @crl

[ crl ]
URI=http://192.168.56.104/ca.crl
```

generiamo il certificato della CA

```
openssl req -config ./openssl.cnf -newkey rsa:4096 -nodes -keyform PEM -keyout ca.key -x509 -days 3650 -extensions certauth -outform PEM -out ca.cer
```

generiamo la chiave privata del server

```
openssl genrsa -out server.key 4096
```

e quindi generiamo il Certificate Signing Request in formato PKCS#10 dovremo usare il seguente comando, alla voce Common Name defineremo l'hostname (localhost oppure home ecc.)

```
openssl req -config ./openssl.cnf -new -key server.key -out server.req
```

con certificato auto-firmato della CA, generiamo il certificato con numero seriale 100 (ad esempio)

```
openssl x509 -req -in server.req -CA ca.cer -CAkey ca.key -set_serial 100 -extfile openssl.cnf -extensions server -days 365 -outform PEM -out server.cer
```

leggeremo l'esito :

```
Signature ok
subject=/C=IT/L=Bologna/O=VFA/CN=localhost
Getting CA Private Key
```

il nuovo file server.key, ora contiene la chiave privata del server mentre il fiel server.cer è un certificato auto-firmato. A questo punto il file server.req non sarà più necessario

```
rm server.req
```

passiamo alla generazione della chiave privata per il client (sempre a 4096 bit)

```
openssl genrsa -out client.key 4096
```

generiamo nuovamente il CSR

```
openssl req -config ./openssl.cnf -new -key client.key -out client.req
```

ed alla richiesta del Common Name inserisco il mio nome "Luca Guerrieri". Anche ora con certificato auto-firmato della CA, generiamo il certificato con numero seriale 101

```
openssl x509 -req -in client.req -CA ca.cer -CAkey ca.key -set_serial 101 -extfile openssl.cnf -extensions client -days 365 -outform PEM -out client.cer
```

e leggiamo l'esito

```
Signature ok
subject=/C=IT/L=Bologna/O=VFA/CN=Luca Guerrieri
Getting CA Private Key
```

NB.: il client verrà identificato con un certificato che avrà validità 365 giorni ma questo valore è, ovviamente, personalizzabile.

salviamo ora la chiave privata ed il certificato in formato PKCS#12 in modo che possa essere importato nel browser. Proteggeremo il certificato con una password che verrà utilizzata dal giusto proprietario per l'operazione d'importazione. (password = MD5 ("forlex") -> 3dfea430c9ea20a3b6ad60fa5cdac2a d)

```
openssl pkcs12 -export -inkey client.key -in client.cer -out client.p12
```

Attenzione : alla richiesta di password quando la inseriremo non avremo feedback visivi (no * no password)

ora il nostro client.p12 è l'unione di tutto ciò che serve per il client quindi, per maggiore sicurezza cancelliamo i file

```
rm client.key client.cer client.req
```

Configurazione del server Apache 2 (mod_ssl)

Passiamo ora alla configurazione del server web (Apache 2).

abilitiamo il modulo su apache

```
a2enmod ssl
```

e riavviamo il server

```
/etc/init.d/apache restart
```

La configurazione avviene personalizzando il file default-ssl :

```
vi /etc/apache2/sites-enabled/default-ssl
```

qui potremo definire tutto ciò che occorre per la realizzazione della sessione criptata

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin administrator@vfa.loc

    DocumentRoot /var/www/vfa
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/vfa>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log

    # Possible values include: debug, info, notice, warn, error, crit,
    # alert, emerg.
    LogLevel warn

    CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on

    #   A self-signed (snakeoil) certificate can be created by installing
    #   the ssl-cert package. See
    #   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
    #   If both key and certificate are stored in the same file, only the
    #   SSLCertificateFile directive is needed.
    SSLCertificateFile    /etc/apache2/ssl/server.cer
    SSLCertificateKeyFile /etc/apache2/ssl/server.key
....
```

ora copiamo i file generati precedentemente nella directory /etc/apache2/ssl

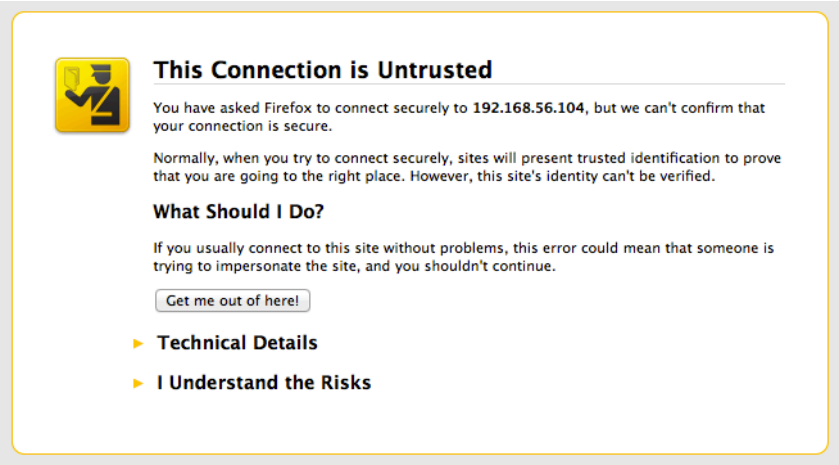
```
cp /root/certificates/server.* /etc/apache2/ssl
```

e riavviamo il server

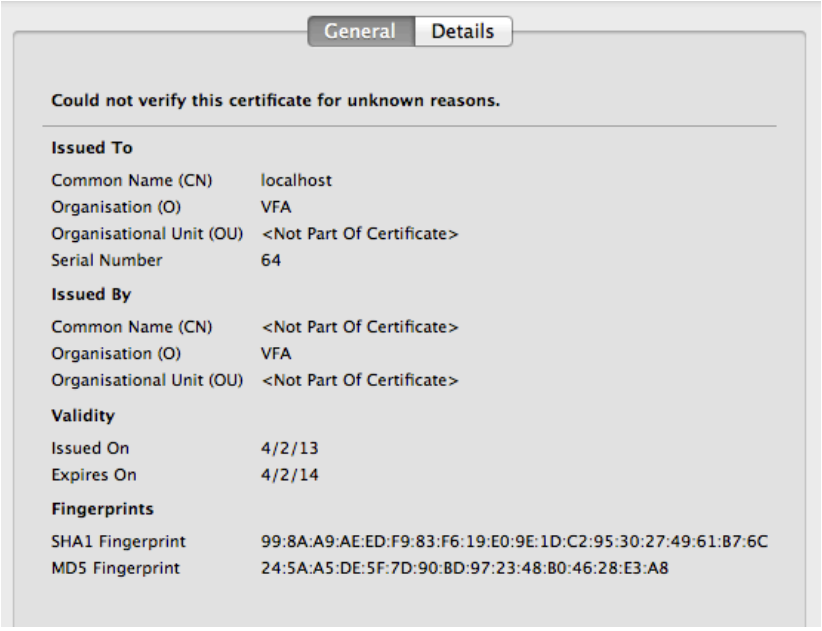
```
/etc/init.d/apache2 restart
```

a questo punto testiamo la connessione ssl atraverso una chiamata con protocollo https.

La pagina in risposta ci confermerà la correttezza dell operazioni sin'ora realizzate.



ed ecco i particolari del certificato :



Apache 2 SSL mutual authentication

Questo tipo di autenticazione nota anche come "two-way SSL authentication", consiste nell'uso dei certificati digitali per identificare sia il server web sia il client (mutual authentication). In tal modo è possibile fornire al client tempi e risorse di cui fruire mentre per il sever si riducono al minimo i client non autorizzati e l'uso di risorse non destinate puntualmente a gruppi di utenti, precedentemente censiti.

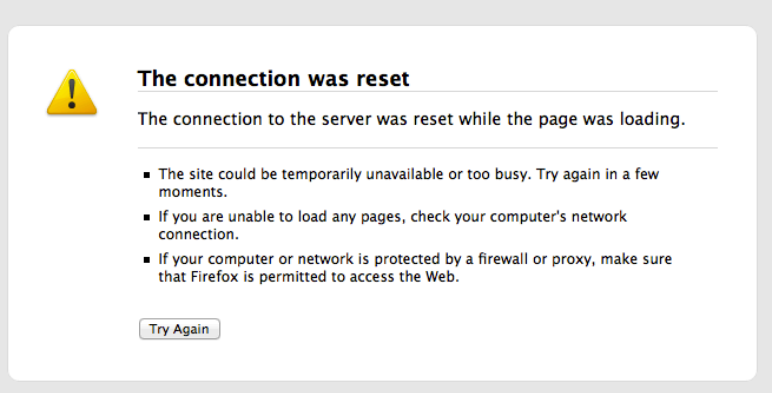
L'abilitazione di questo metodo di autenticazione passa per il file di configurazione del relativo Virtualhost, abilitando le seguenti direttive :

```
SSLCACertificateFile /etc/apache2/ssl/ca.cer
SSLVerifyClient                                    require
SSLVerifyDepth 1
```

dopo aver copiato il file ca.cer in quella directory

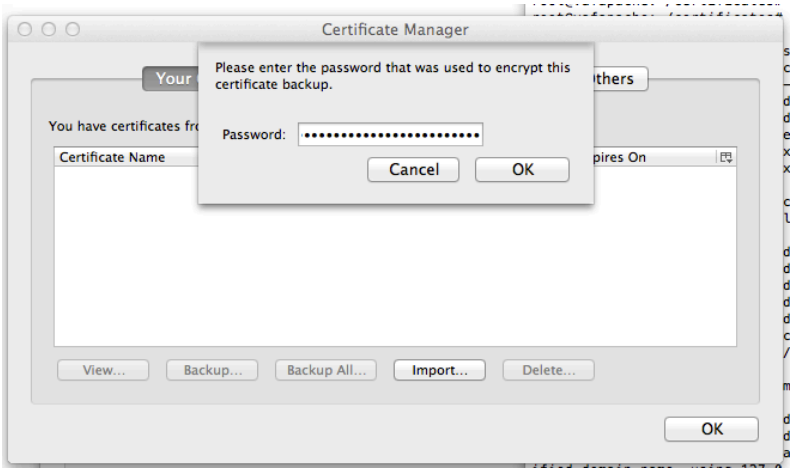
Per la precisione : SSLVerifyClient require ci assicura che un client con un certificato generato da una CA non affidabile non potrà fruire della sessione SSL e quindi del servizio; la direttiva SSLVerifyDepth 1 specifica la profondità delle CA affidabili (certificato generato da un CA affidabile la quale ha generato il proprio da un'altra CA ecc.). In questo caso mettendo 1 vogliamo forzare la lettura di un certificatogenerato da una sola CA - la nostra -.

Dopo il riavvio del server proviamo a visitare la nostra pagina (https://ecc.):



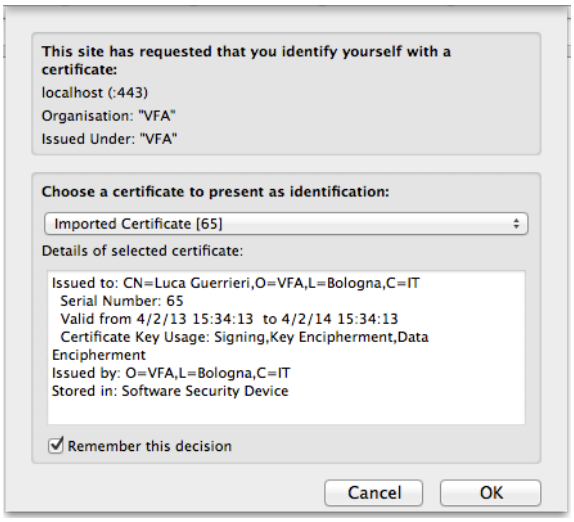
questa risposta (Connection reset) ci fa comprendere che il server non non trovando il certificato nel browser ha resettato la connessione.

Installiamo il certificato:



inserendo la password utilizzata durante la generazione. (3dfea430c9ea20a3b6ad60fa5cd ac2ad) ed ecco che al termine dell'importazione potremo vedere le proprietà del nostro certificato.

Da notare Issued by Organisation e Validity Issued On ed Expires On.
La notifica, da parte del browser che il sito da noi visitato richiede la fornitura di un certificato non può che renderci felici.



Definizione della Directory

```
<Directory /var/www/vfa/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        allow from all
        SSLVerifyClient Require
        SSLVerifyDepth 1
```

```
        SSLRequire %{SSL_CLIENT_S_DN_O} eq "VFA"
</Directory>
```

Revocation List (todo)

Attraverso questo strumento possiamo definire una lista dei certificati revocati così che Apache sia in grado di sapere subito quali sono i certificati revocati (revocati e non scaduti)e rigettare quindi la connessione.

Aggiungiamo la direttiva

```
SSLCARevocationFile /etc/apache2/ssl/revocation.crl
```

al file di configurazione del nostro Virtualhost

http://www.cafesoft.com/products/cams/ps/docs30/admin/ConfiguringApache2ForSSLTLSMutualAuthentication.html#Creating_a_Certificate_Authority_using_OpenSSL

PHP SSH2 extension

Questa estensione è necessaria per poter eseguire shell remote attraverso uno script PHP.

L'installazione procede come segue:

```
aptitude install libssh2-1-dev libssh2-php
```

ora sarà possibile controllare se il modulo è stato installato

```
php -m |grep ssh2
```

se l'esito sarà "ssh2" vuol dire che l'installazione è andata a buon fine.

Ora dobbiamo installare l'estensione, editando il file php.ini

```
vi /etc/php5/apache2/php.ini
```

ed aggiungendo alla fine del file :

```
extension=ssh2.so
```

a questo punto, dopo aver riavviato apache

```
/etc/init.d/apache2 restart
```

basterà controllarela presenza della stringa ssh2 all'interno della pagina risultante da

```
<?php phpinfo(); ?>
```

Ora si passa alla configurazione per l'esecuzione di ssh2_connect. Creazione della directory che conterrà le chiavi generate (capitolo Autenticazione SSH a scambio di chiavi)

```
mkdir /var/www/.ssh
```

copiamo le chiavi :

```
cp /root/.ssh/* /var/www/.ssh
```

assegniamo la proprietà all'utente www-data (Apache)

```
chown www-data:www-data -R /var/www/.ssh
```

proteggiamo la directory inserendo un'apposita direttiva nel file di configurazione di Apache

```
vi /etc/apache2/sites-enabled/000-default

<Directory /var/www/.ssh2>
        Order allow,deny
</Directory>
```

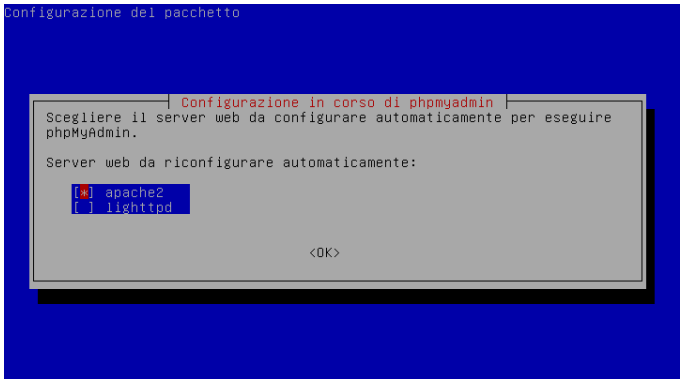
Qundi testiamo il funzionamento:

```
        $connection = ssh2_connect($server,22,array('hostkey'=>'ssh-rsa'));
        if (ssh2_auth_pubkey_file($connection,'root','/var/www/.ssh/id_rsa.pub','/var/www/.ssh/id_rsa')) {
                echo "success!";
        } else {
                echo "no success :-(";
        }
```

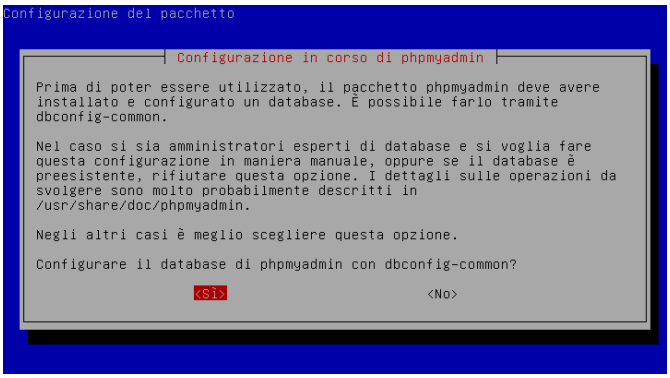
http://phpmaster.com/using-ssh-and-sftp-with-php/

Installazione PHPMyAdmin

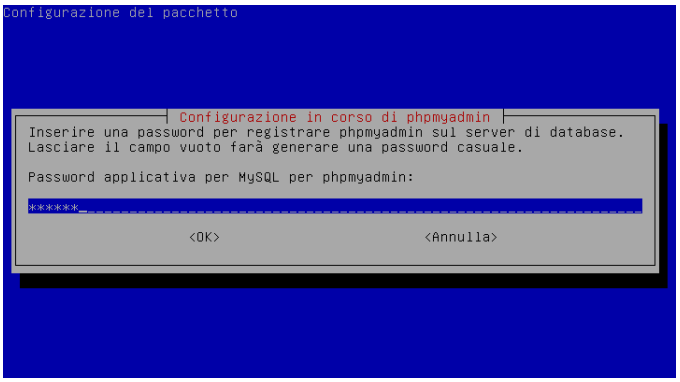
```
apt-get install phpmyadmin
```



lo configuriamo per utilizzare Apache



possiamo anche procedere alla configurazione per poi modificarla nelle parti in cui c'interessa (PHPMyAdmin fa uso di MySQL per le sue configurazioni utente):



La home page offrirà la possibilità del login

Ora, per motivi di sicurezza, cambiamo l'alias con il quale richiamiamo questo manager, quindi :

```
vi /etc/apache2/conf.d/phpmyadmin.conf
```

e poi

```
Alias /pma /usr/share/phpmyadmin
```

Configurazione Multiple Servers su PhpMyAdmin

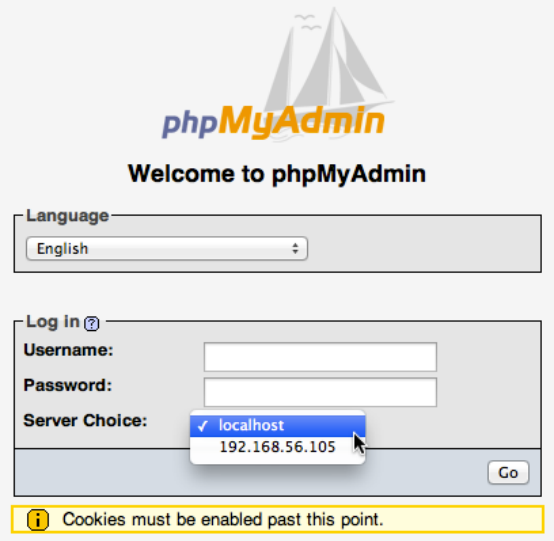
ora si può procedere con la modifica del file di configurazione al fine di poter fare login su diversi server MySQL, inserendo i seguenti parametri .

```
cd /etc/phpmyadmin
```

editiamo il file **config.inc.php** ed aggiungiamo quindi le caratteristiche dei diversi server all'interno di questo file

```
/*
 * primo server
 */
/* Authentication type */
$cfg['Servers'][$i]['auth_type'] = 'cookie';
/* Server parameters */
$cfg['Servers'][$i]['host'] = '192.168.56.105';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['compress'] = false;
/* Select mysqli if your server has it */
$cfg['Servers'][$i]['extension'] = 'mysqli';
$i++;
/*
 * secondo server
 */
/* Authentication type */
$cfg['Servers'][$i]['auth_type'] = 'cookie';
/* Server parameters */
$cfg['Servers'][$i]['host'] = '192.168.56.106';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['compress'] = false;
/* Select mysqli if your server has it */
$cfg['Servers'][$i]['extension'] = 'mysqli';
$i++;
 /*
 * terzo server
 */
$i=3;
/* Authentication type */
$cfg['Servers'][$i]['auth_type'] = 'cookie';
/* Server parameters */
$cfg['Servers'][$i]['host'] = '192.168.56.107'';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['compress'] = false;
/* Select mysqli if your server has it */
$cfg['Servers'][$i]['extension'] = 'mysqli';
$i++;
```

avremo dunque sulla pagina web di riferimento di PHPMyAdmin la voce "Server Choiche:" popolata con la lista dei server MySQL amministrabili.



Si precisa che all'interno del file
/var/lib/phpmyadmin/blowfish_secret.inc.php
viene memorizzato l'hash della password di accesso all'interfaccia

Apache WebDav - Autenticazione con MySQL

Web-based Distributed Authoring and Versioning - WebDav -
Questo protocollo ha lo scopo di rendere il WWW un mezzo di lettura e scrittura come se fosse una directory remota - web share - la sua realizzazione avviene dunque impiegando server web (es.: Apache). All'interno di tale condivisione possiamo dunque creare, modificare, spostare i file in essa contenuti. Il protocollo offre anche un sistema di protezione da sovrascrittura dei file, di gestione della proprietà (creazione, rimozione, modifica, ecc.), oltre ad innumerevoli altre funzionalità.
Per implementare questo genere di server ci avvarremo di Apache ma nel caso dell'autenticazione useremo un server MySQL il quale avrà una tabella utenti che sarà utile al momento della richiesta di autenticazione alla web share.

```
apt-get install apache2 mysql-client libapache2-mod-auth-mysql
```

abilitiamo i moduli per il dav e per l'autnticazione via Mysql

```
a2enmod dav_fs
a2enmod dav
a2enmod auth_mysql
```

creiamo il database e la relativa tabella utenti oltre ad abilitare il nostro server web (webdav) ad accedervi sul server MySql

```
mysqladmin -u root -p create webdav
mysql -u root -p
mysql> CREATE USER 'webdav'@'%' IDENTIFIED BY 'forlex';
mysql> GRANT ALL PRIVILEGES ON *.* TO webdav@'%';
FLUSH PRIVILEGES;
```

quindi commentiamo all'interno del file /etc/mysql/my.conf le seguenti righe :

```
#bind-address=192.168.56.105
#bind-address=localhost
```

così da permettere l'accesso al server mysql da parte dell'host del server web.

Passiamo ora al server web e configuriamo la web-share, innanzi tutto proviamo ad accedere al server MySql atraverso il client mysql:

mysql -h <ip server mysql> -u webdav -p

se dopo aver inserito la password avremo la console di mysql, significa che tutto è andato bene e quindi possiamo procedere con la configurazione di apache.
Creiamo nella directory /etc/apache2/sites-available il nostro file di configurazione es: webdavdisk :

```
vi /etc/apache2/sites-available/webdavdisk
```

Inseriamo le seguenti direttive

```
NameVirtualHost *
<VirtualHost *>
ServerAdmin webamster@mail.loc

DocumentRoot /var/www/share
<Directory /var/www/share>
        Options Indexes MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
</Directory>

Alias /webdav /var/www/share
<Location /webdav>
DAV On
AuthBasicAuthoritative Off
AuthUserFile /dev/null
AuthMySQL On
AuthName “webdav”
AuthType Basic
Auth_MySQL_Host <IP SERVER MYSQL>
Auth_MySQL_User webdav
Auth_MySQL_Password password
AuthMySQL_DB webdav
AuthMySQL_Password_Table <TABELLA CREDENZIALI>
Auth_MySQL_Username_Field username
Auth_MySQL_Password_Field passwd
Auth_MySQL_Password_Clause "AND active=1"
Auth_MySQL_Empty_Passwords Off
Auth_MySQL_Encryption_Types PHP_MD5
Auth_MySQL_Authoritative On
require valid-user
</Location>
</VirtualHost>
```

abilitiamo il virtualhost

```
a2ensite webdavdisk
```

riavviamo il server (oppure ricarichiamo)

```
/etc/init.d/apache2 reload
```

in caso di errori : tail -f /var/log/apache2/error.log

ricordiamo che la directory sulla quale monteremo la condivisione dovrà essere dell'utente www-data quindi :

```
chmod www-data /var/www/share
```

ora provvediamo a montare un disco iscsi

```
iscsiadm -m discovery -t sendtargets -p <ip iscsi target>
```

ed in seguito al discovery provvediamo a montare il target d'interesse

```
iscsiadm -m node --targetname "1.2.3.4:volume" --portal <ip iscsi target>
```

a questo punto dovremmo avere il messaggio di "success". Adesso possiamo associalro alla nosta share con il comando di mount :

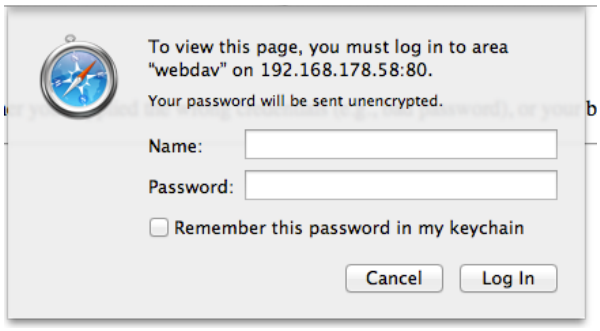
```
mount /dev/sdb1 /var/www/webdav
```

Montare una share webdav

Innanzitutto ricordiamo che il nostro nome utente e la password sono memorizate all'interno del DB indicato in fase di configurazione e che le password sono salvate in maniera criptata (MD5) .
Per montare una share webdav occore visitare la url compresa di nome share quindi :

```
http://<ip server>/webdavdisk
```

immediatamente riceveremo una richiesta di credenziali



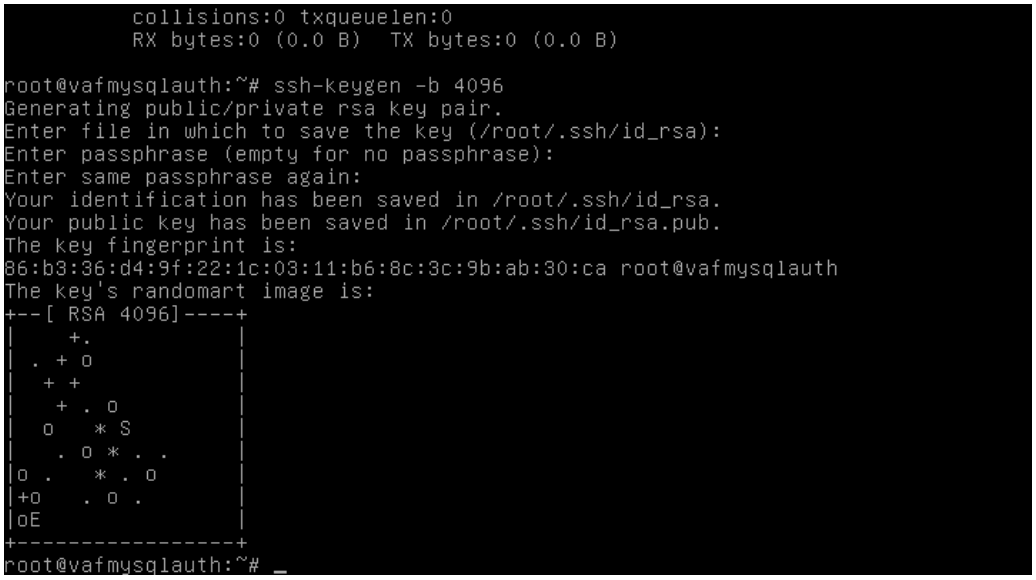
Inserendo le corrette credenziali potremo vedere il contenuto della share. Occorre precisare che questa share è configurata in sola-lettura.

SSH Server - autenticazione a scambio di chiavi

Al fine di poter gestire tutti i processi, nonchè tutte le funzionalità del sistema, si è proceduto alla configurazione di una autenticazione SSH con scambio di chiavi frai due server Presentazione e Storage. Questa impostazione permette di accedere alla shell dei comandi del server remoto senza l'utilizzo della procedura di autenticazione standard, d'altra parte la sicurezza viene preservata (anche maggiormente di un normale accesso con username e password) inquanto solo i client in possesso della "chiave giusta" sono in grado accedere al promp dei comandi remoto.

Generiamo una coppia di chiavi :

ssh-keygen -b 4096 (-b 4096 imposta la lunghezza a 4096 anzichè i canonici 2048)



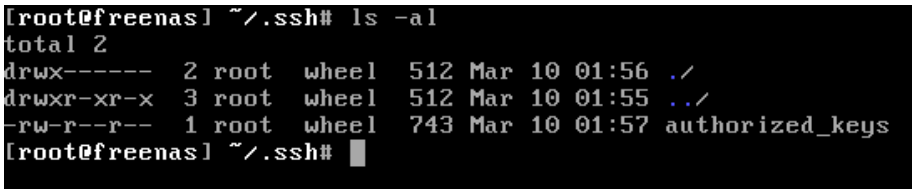
prima di eseguire la copia della chiave pubblica dovremo abilitare e creare su FreeNAS il file Authorized_keys e la directory /root/.ssh

```
# mount -uw /
# mkdir -p /root/.ssh/
# chmod 700 /root/.ssh
# touch /root/.ssh/authorized_keys
```

ora procediamo alla copia della chiave pubblica all'interno della lista delle chiavi autorizzate presso il server

```
scp /root/.ssh/id_rsa.pub root@192.168.56.101:/root/.ssh/authorized_keys
```

controllare che i permessi sul file authorized_keys siano :



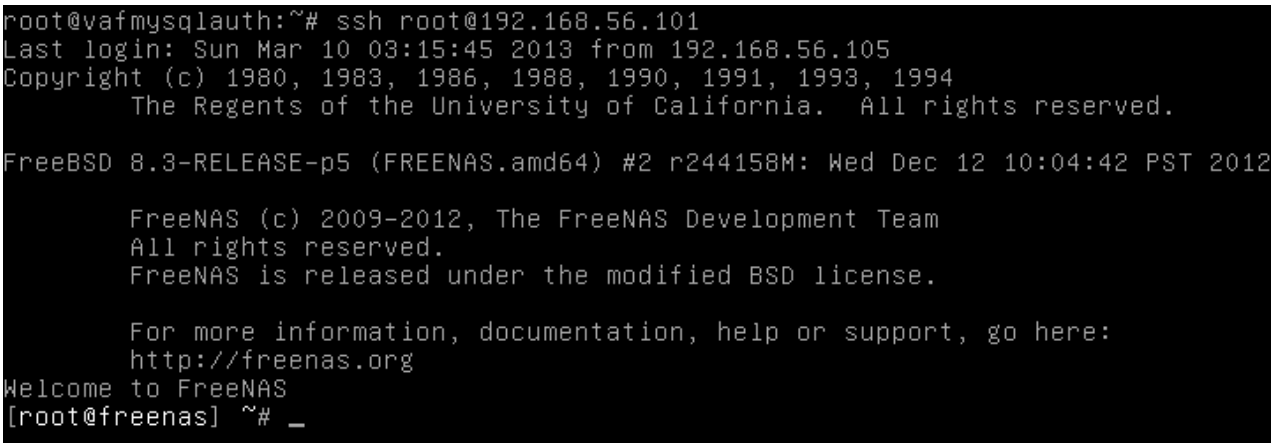
ora aggiungere al file di configurazione /etc/ssh/sshd_config le seguenti voci di configurazione:

```
HostbasedAuthentication yes
RSAAuthentication yes
PubkeyAuthentication yes
PasswordAuthentication no
```

ed inseguito riavviamo il servizio

```
/etc/rc.d/sshd restart
```

proviamo ora la connessione dal client certificato e vedremo apparire la console del server storage remoto senza richiesta di password



PiXA Framework

PHP - XML - Ajax Framework

Il PiXA Framework, è il framework alla base di tutto il sistema, un insieme di classi e funzioni che permettono l'implementazione di tutte le funzionalità dell'interfaccia di gestione nonchè il relativo ulteriore sviluppo. Per la realizzazione sono state impiegate le tecniche dell' OOP, oltre ad utilizzare funzionalità specifiche per la connesse a risorse realizzate con altri linguaggi come XML[5]. La scelta è ricaduta su PHP anche per la semplicità e la velocità del ciclo di sviluppo nonchè per l'ampia documentazione.

[5] **XML** (sigla di **eXtensible Markup Language**) è un linguaggio di markup, basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.

SAS (Secure Authentication System)

SISTEMA DI AUTENTICAZIONE

Il SAS è un sistema di autenticazione che permette la gestione dell'accesso a servizi offerti attraverso la piattaforma web.
Le tecnologie impiegate sono il linguaggio PHP ed Actionscript 3.0 mentre per l'esecuzione la collaudata coppia Apache - MySQL.

In particolare funziona come segue :

In merito a quest'ultima funzionalità si tratta di un controllo basato sugl'identificativi di Sessione[6], in modo da avere sotto controllo sia il tipo di accessi sia l'associazione fra credenziali ed appunto l'identificativo di Sessione. In pratica, la visualizzazione dei contenuti è permessa solo se sono presenti, contemporaneamente, diverse condizioni. **Resta importante specificare che il sistema di login ha la peculiarità di effettuare la fusione e criptazione delle credenziali di accesso, inserite dall'utente, direttamente**

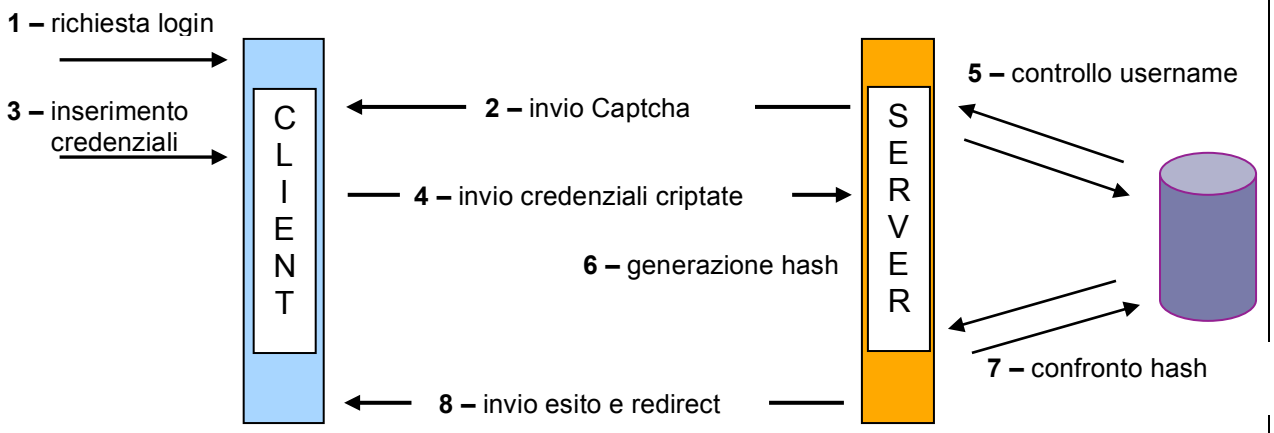
lato client. Il client, infatti, realizza l'hashing md5 di : username, password e di una stringa di caratteri in formato immagine, generata casualmente dal sistema e visualizzata direttamente a video (sistema CAPTCHA). L'hash di queste informazioni viene poi inviato al server di autenticazione. Quest'ultimo, ricevuta tale informazione, innanzitutto controlla che l'utente esista (in caso negativo non prosegue e rilancia la pagina di login), in quel caso prova a generare la stessa stringa hash con le informazioni in suo possesso. Se l'esito è positivo vuol dire che non c'è stato nessuno che ha alterato i dati, altrimenti non consente le successive operazioni.e rimanda immediatamente alla pagina di login.

1) richiesta di login
2) visualizzazione pagina di Login con avvio del client grafico per il successivo invio della stringa CAPTCHA per criptare le credenziali di accesso;
3) inserimento da parte dell'utente delle credenziali di accesso criptate;
4) invio delle credenziali di accesso al server
5) il server controlla l'esistenza della username in caso affermativo procede altrimenti si ritorna al punto 2

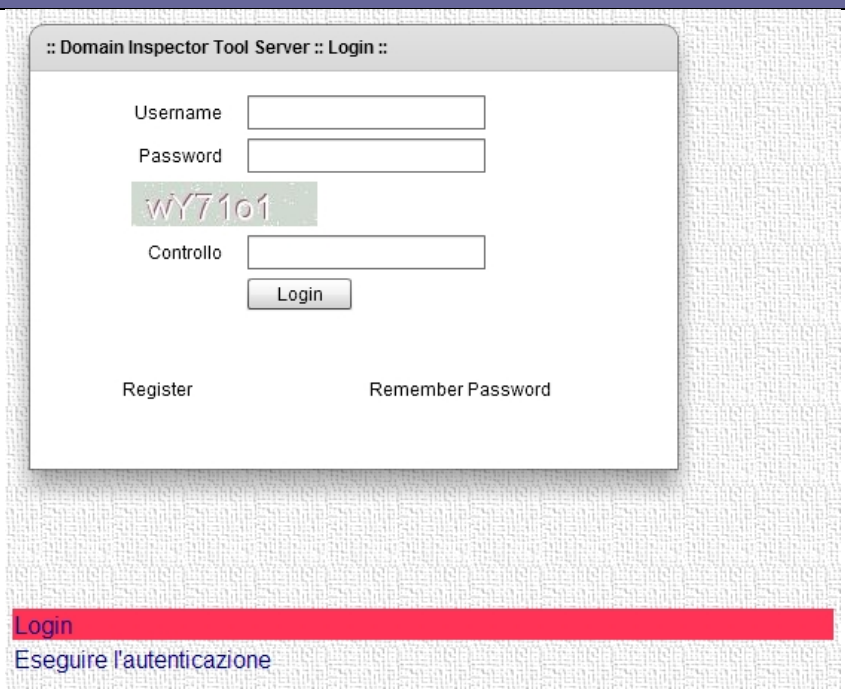
[6] Nel caso delle comunicazioni fra computer basate sul protocollo HTTP, un identificativo di sessione è una informazione che identifica una serie di messaggi che verranno scambiati fra le macchine.

6) il server genera una stringa di hash composta dagli stessi dati inviati al client (Captcha + username + password)
7) il server confronta le due stringhe hash (ricevuta e generata) nel caso siano uguali procede, altrimenti rimanda al punto 2;
8) invio esito delle operazioni di login e successivo redirect all'area privata.

SCHEMA DELL' OPERAZIONE DI LOGIN



IL CLIENT GRAFICO PER LE OPERAZIONI DI LOGIN



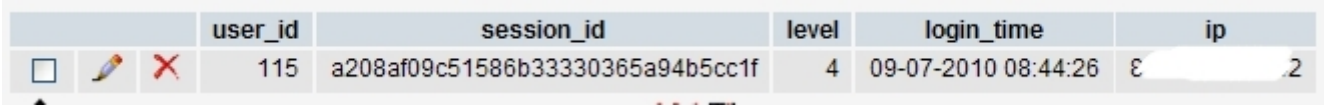
In pratica il sistema di login ha le seguenti proprietà :

1) Trasmissione sicura delle credenziali d'accesso (criptate) da un **client in esecuzione sulla macchina** (peculiarità della tecnologia Flex) senza in realtà costringere l'utente ad installare un apposito software sul proprio computer ed inoltre usufruendo delle caratteristiche di **multi-piattaforma**.
2) Invio asincrono delle credenziali. **Il sistema, di fatto, implementa una logica di autenticazione a chiave pubblica/chiave privata, ove la chiave pubblica è la combinazione di username e password e la chiave privata è di fatto la stringa casuale generata ed inviata al client sotto forma d'immagine (CAPTCHA)**. In questo modo un malintenzionato che intercetta il traffico sin dall'inizio, per scoprire le credenziali d'accesso, non sarebbe in grado di identificarle in quanto: nonostante venisse in possesso della stringa casuale non potrebbe scoprire la username, la password e la OTP con cui è stata generata in quanto viaggiano, verso il server, in forma criptata. Nell'ipotesi in cui riuscisse a conoscere username e password (per evitare di lasciare tracce nel sistema di logging) dovrebbe ogni volta intercettare la stringa casuale generata perché, funzionando come una OTP viene "bruciata" ad ogni login. *Inoltre se il malintenzionato, riuscisse a scoprire la username e la password e quindi la stringa OTP non potrebbe portare a termine un attacco di Hjacking di Sessione poiché la sessione viene rigenerata al termine della procedura di login.* In tal modo il sistema provvede autonomamente a controllare la congruità delle informazioni. In fine l'utente, nel caso di quest'ultimo tipo di attacco, riceverebbe l'informazione che "qualcun altro" sta utilizzando le sue credenziali.
3) Sicurezza a vari livelli, se l'utente non esiste non si procede ad ulteriori operazioni fra client e server, riducendo sia il carico di lavoro del server sia le possibilità di riuscita di un attacco.
4) Unicità delle credenziali d'accesso, l'utente usa sempre quelle assegnategli ma il sistema riceve un'insieme diverso ogni volta, come in un sistema O.T.P. (One Time Password) in caso non corrispondano l'utente viene informato da un apposito messaggio.

5) Elaborazione delle informazioni lato client completamente invisibile ad un malintenzionato che potrebbe accedere fisicamente alla macchina della vittima. **La criptazione viene effettuata con un applicativo compilato e residente sul client, quindi non direttamente interpretabile** (applicazione Flex su pagina html). In questo modo, il malintenzionato, non può sapere come viene composta la stringa di login.
6) Possibilità di applicare algoritmi proprietari di criptazione per aumentarne la segretezza (basta conoscere Javascript o mxml).
7) Delega della segretezza delle credenziali all'utente ed al gestore del sistema informatico.
8) Redirezionamento dell'utente, sin dalla fase di login, ad una comunicazione con protocollo **https**, per raggiungere una completa segretezza della comunicazione ed una sicura identificazione dell'utente sin dalle prime fasi di autenticazione.
9) Controllo della **validità della Sessione** ad ogni richiesta di una pagina,. L'autenticazione, infatti, è basata sulle sessioni e non su IP, credenziali, ecc. in

questo modo, se ci si dovesse accorgere che le sessioni sono cambiate il sistema obbliga nuovamente al login registrando l'accaduto (protezioni da attacchi basati su Sessioni).

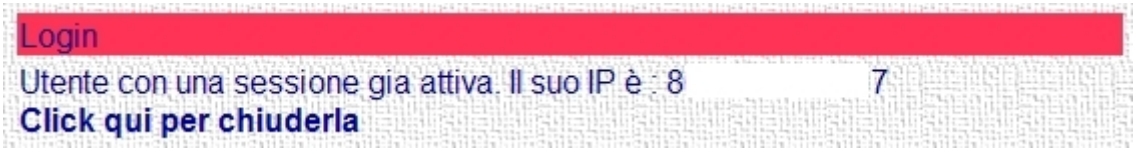
10) Memorizzazione della sessione su database e non nel Cookie o in variabili d'ambiente accessibili ad ignoti, infatti si usa il cookie generato al login come se fosse un certificato, al solo fine di avere certezza che il client sia quello registrato.



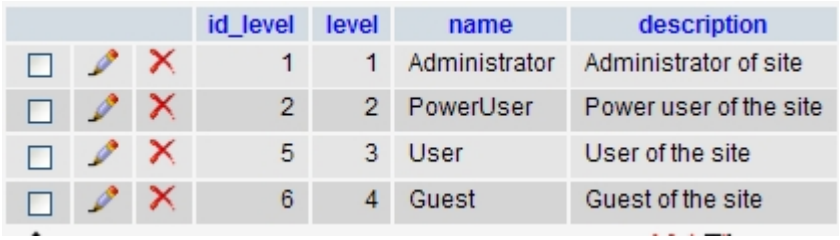
			user_id	session_id	level	login_time	ip
☐	✎	✕	115	a208af09c51586b33330365a94b5cc1f	4	09-07-2010 08:44:26	ε .2

11) Controllo dell'esistenza di sessioni multiple, in quell'ipotesi i relativi utenti vengono costretti nuovamente al login.

12) Impossibilità dell'uso contemporaneo delle stesse credenziali, solo un utente alla volta può usare la sua username e password, se qualcun'altro le utilizza il legittimo proprietario viene informato e l'informazione viene registrata in un file di log



13) Possibilità di sospendere una sessione attiva, causando il logout forzato di quell'utente.
14) Gestione dei livelli di accesso (amministratore / power user / user / guest) completamente personalizzabili.



	id_level	level	name	description
	1	1	Administrator	Administrator of site
	2	2	PowerUser	Power user of the site
	5	3	User	User of the site
	6	4	Guest	Guest of the site

15) Registrazione / Ricorda password / Cambia password . Tipiche funzionalità per effettuare la registrazione di un utente (con relativo controllo dell'informazione inserita), sistema per cambiare autonomamente la password, sistema per ricordare la

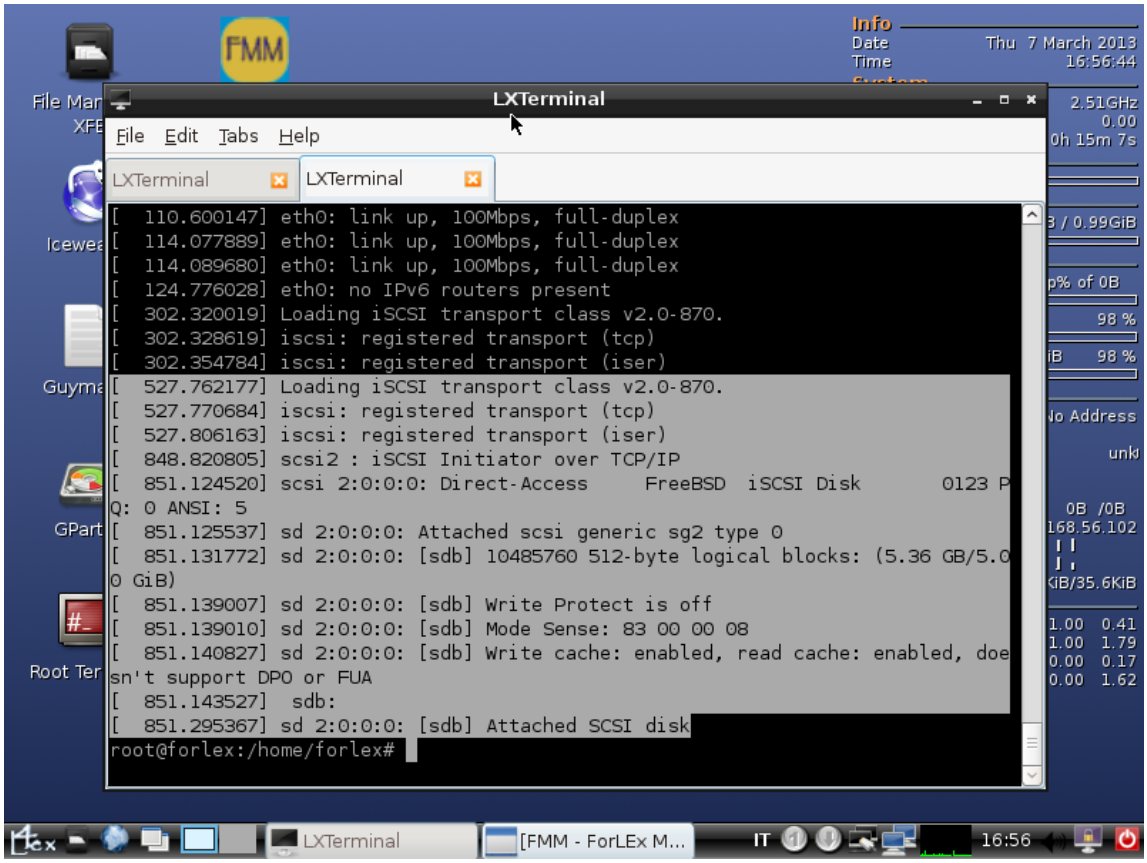
password rinviandola dopo un controllo sulla identità dell'utente (risposta a domanda segreta)

Acquisizione di supporti orginali

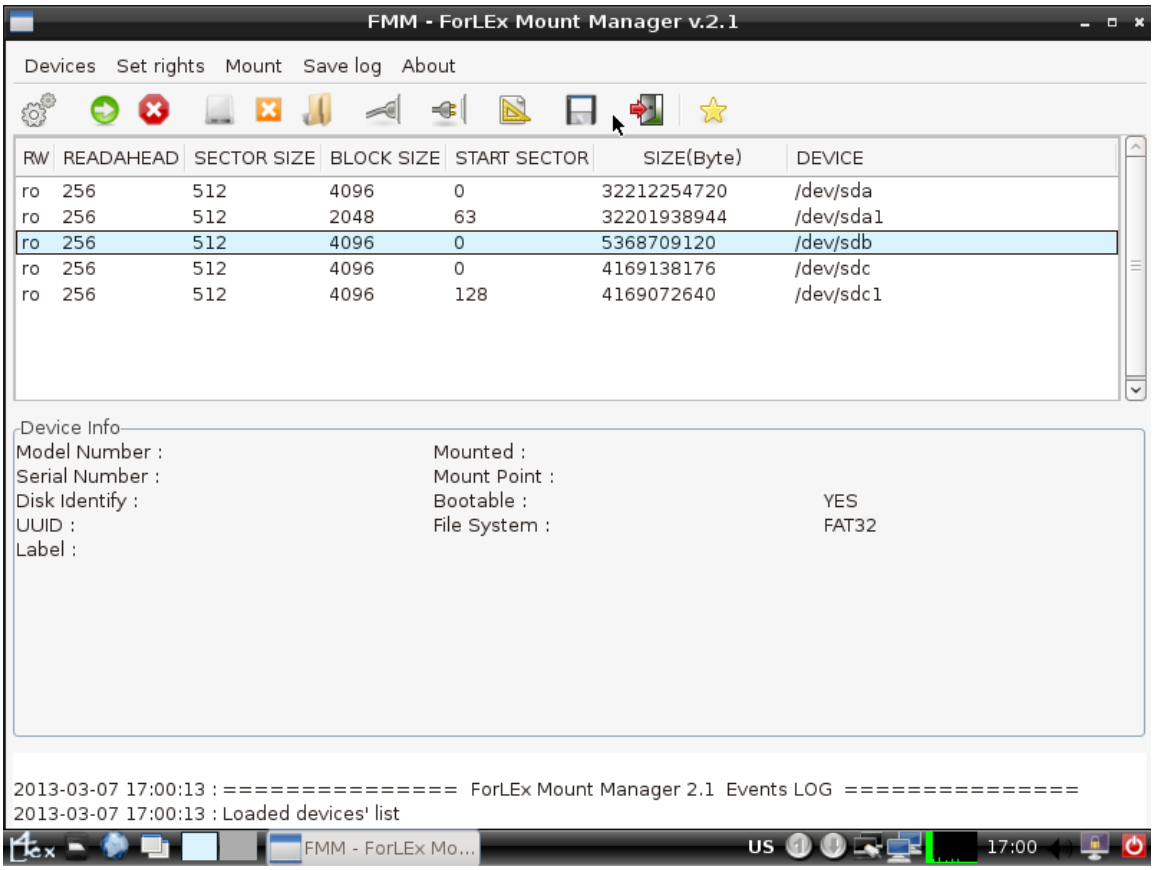
ForLEX Live CD

In questa fase utilizzeremo il live-cd ForLEX 2.0.5 (Armando) per acquisire i dispositivi di nostro interesse. L'acquisizione la eseguiremo in modo da poter avere una immagine DD(disk dump) del dispositivo da analizzare. Al termine ne verà calcolato l'hash così da poter convalidare l'acquisizione. I file che verranno generati durante l'acquisizione verranno memorizzati direttamente all'interno dello storage del VFA così da poter essere direttamente avviati all'analisi. Il protocollo di collegamento sarà iSCSI.

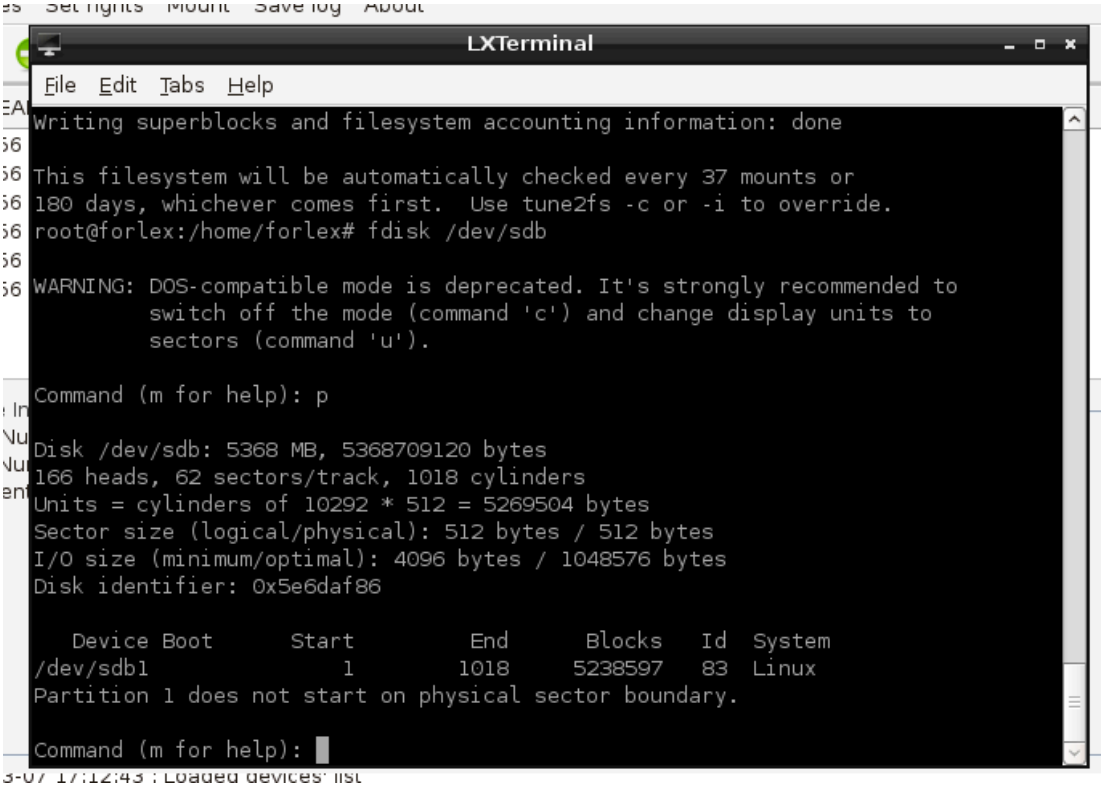
Dopo la necessaria configurazione del file iscsi.conf per poter inserire i parametri utili all'autenticazione MutualCHAP inerente il Discovery delle risorse, si è proceduto al collegamento del target al fine di riversare un'acquisizione tipo (Ubuntu on usb).



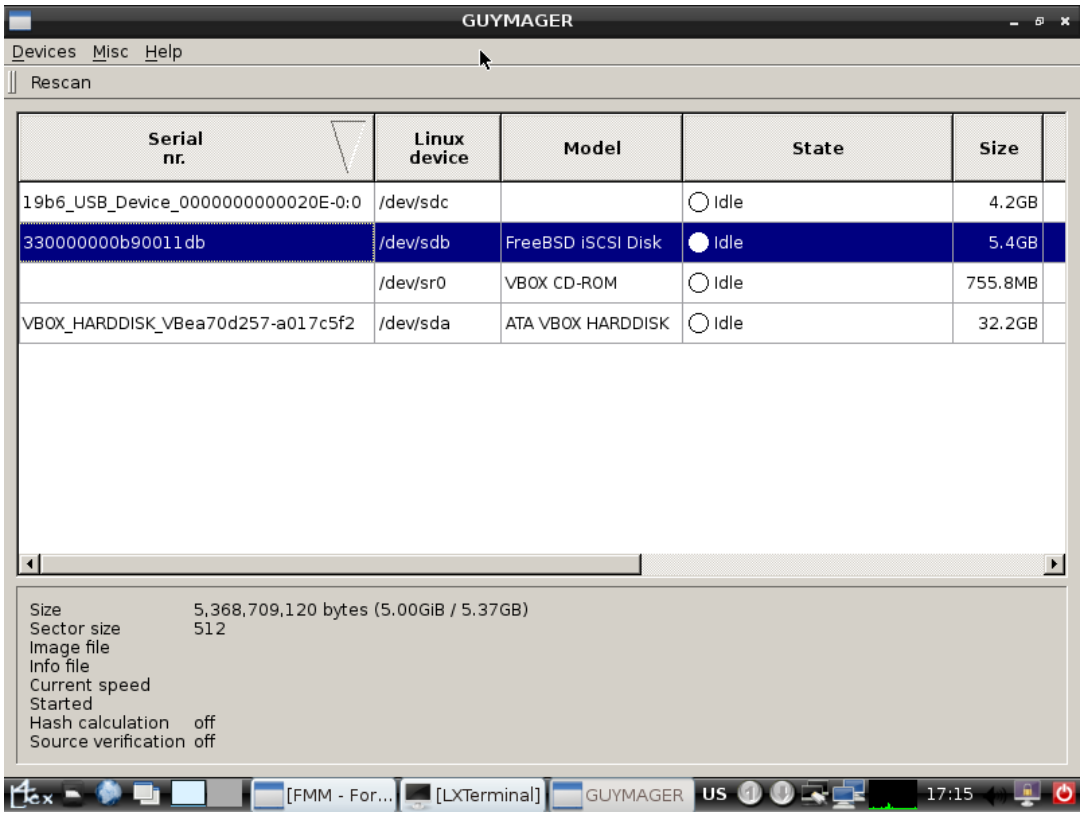
A seguito della connessione al target si crea un nuovo block device (/dev/sdb)



Forlex Mount Manager mostra sia il disco USB d'acquisire sia il disco iSCSI appena connesso.

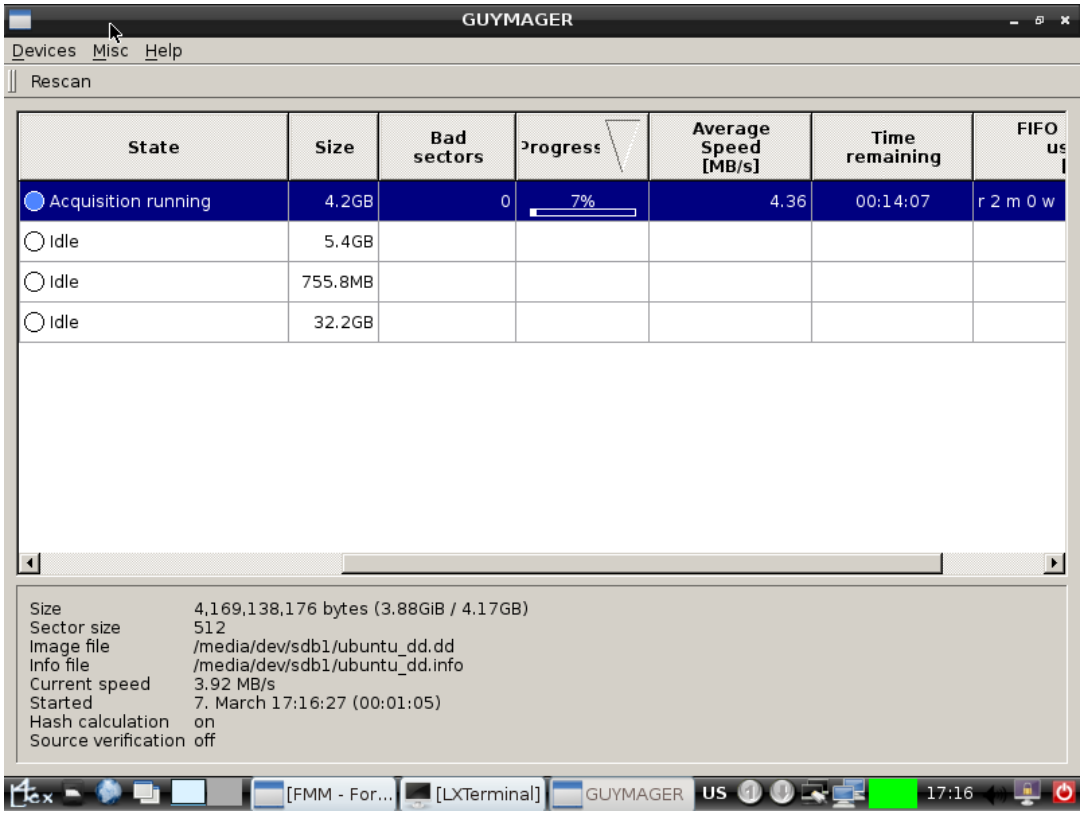


partizionento del disco connesso



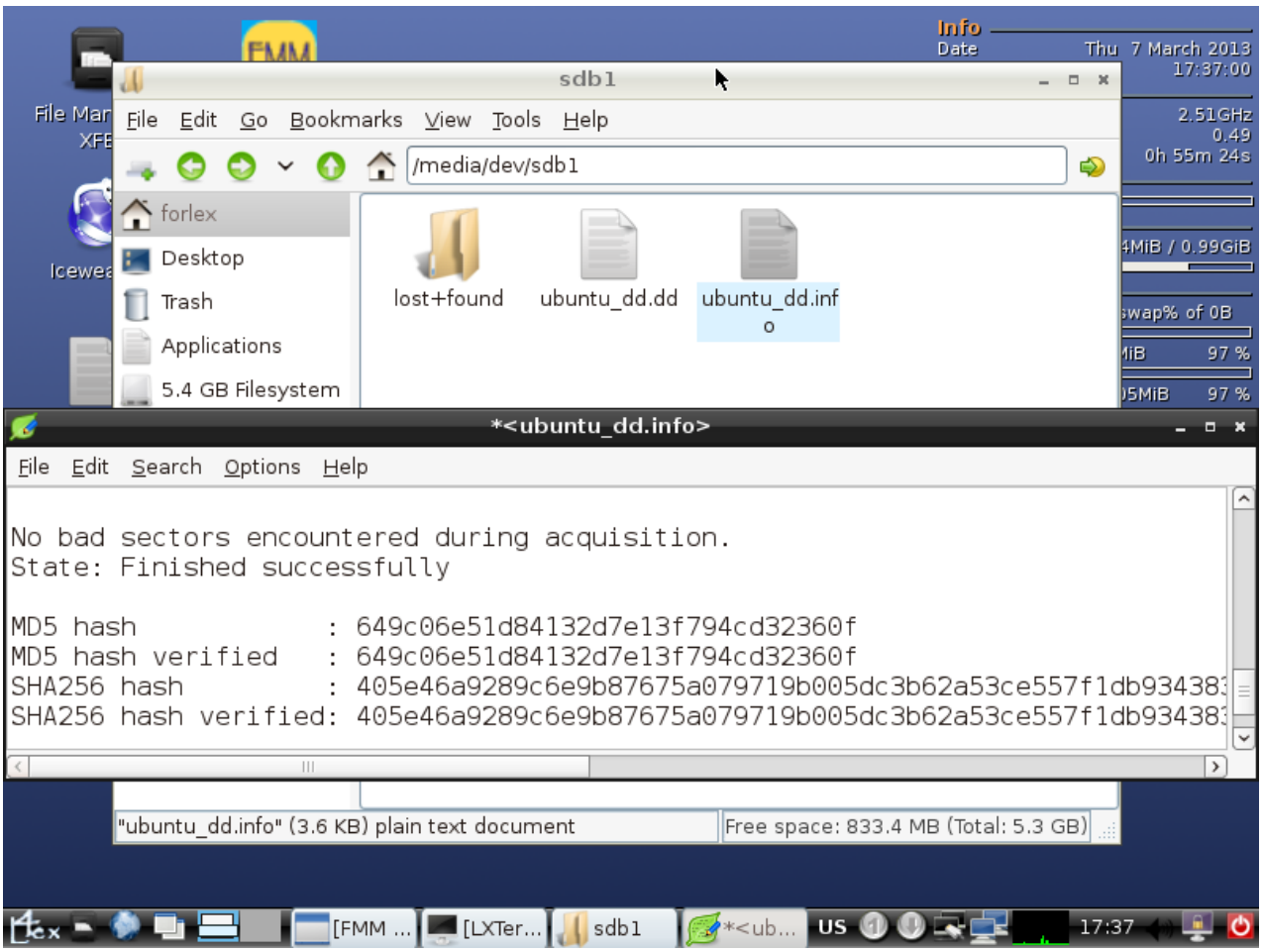
Guymager mostra sia il disco da acquisire (/dev/dsc) sia il disco su cui riversare (/dev/sdb)

Dopo il partizionamento avremo /dev/db1 che una volta montato ci permetterà di salvare l'immagine della periferica acquisita. Giova ricordare che il disco iSCSI montato è in realtà un File Extent su ZFS.



L'acquisizione in progresso, si noti la velocità (3.92 MB/s) e la destinazione (/media/dev/sdb1/ubuntu_dd.dd)

Al termine dell'acquisizione avremo i file generati e completi di hash direttamente sul nostro storage iSCSI.



APPUNTI

Abilitiamo SSL:

```
mysql -u root -p
show variables like '%ssl%';
```

```
Server version: 5.1.66-0+squeeze1 (Debian)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show variables like '%ssl%';
+---------------+----------+
| Variable_name | Value    |
+---------------+----------+
| have_openssl  | DISABLED |
| have_ssl      | DISABLED |
| ssl_ca        |          |
| ssl_capath    |          |
| ssl_cert      |          |
| ssl_cipher    |          |
| ssl_key       |          |
+---------------+----------+
7 rows in set (0.00 sec)

mysql> _
```

questo significa che MySQL supporta SSL.
Aggiungiamo, nella sezione Security Features un nuova riga e scriviamo "ssl" (senza apici), riavviamo e controlliamo che che ssl si sia abilitato.

```
Server version: 5.1.66-0+squeeze1 (Debian)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show variables like '%ssl%';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| have_openssl  | YES   |
| have_ssl      | YES   |
| ssl_ca        |       |
| ssl_capath    |       |
| ssl_cert      |       |
| ssl_cipher    |       |
| ssl_key       |       |
+---------------+-------+
7 rows in set (0.00 sec)

mysql> _
```

installiamo OpenSSl

```
apt-get install openssl
```

MOUNTING

Ricostruzione dell'immagine

In caso di acquisizioni divise in più files (ddfile.001, ddfile.002 ... ddfile.00n), per poter vedere il contenuto dell'intera immagine del disco senza dover eseguire il *cat* di tutti i file che la compongono (quindi rigenerare un file della grandezza della somma dei file) possiamo dunque seguire diverse strade :

- mount con Device Mapper
- mount con Affuse (da Afflib)
- mount con Xmount

Device Mapper

Affuse

Xmount

EWFMount

http://hexstr-morgan.blogspot.it/2012/10/libewf-installation.html

Al termine dell'operazione di ricostruzione possiamo passare alle operazioni di mount

Mount locale

Mount iSCSI

ANALISI

Sleuthkit

In Sleuthkit vi sono diversi comandi utili, tutti, o quasi, prendono immagini raw, ewf e raw split.

MMLS

Questo comando permette di leggere il layout delle partizioni di un disco/immagine
mmls -i raw|ewf|split image
grazei a questo comando possiamo leggere qual'è il settore dal quale parte una partizione - offset - il tipo di file system ed altre informazioni. Utilizzeremo queste informazioni in seguito per eseguire le nostre ricerche.

Sorter

Questo comando in realtà è uno script perl che segue la ricerca di tutti i file immagini (jpeg, gif, png, ecc.) all'inerno delle immagini degli hard disks. In particolare Sorter permette non

solo di effettuare una canonica ricerca ma anche di identificare tutte le immagini cancellate. Il comando, inoltre, restituiche sia tutte le immagini identificate (che avranno come parte del nome l'inode/settore ove erano memorizzate) sia un report in formato html con le relative thumbnails.
Ecco un esempio :

sorter ...

un modo per personalizzare la ricerca è quello di fornire a Sorter un file di configurazione. Al suo interno potremo definire : Categoria,

SCRIPTS

```
#!/bin/sh
#Creates new project
#ver. 0.1 from 26.12.2009
### user ###
echo "Enter projectname to create:"
read PROJECT if [ -z $PROJECT ];
then
exit
fi
USERPASS=`< /dev/urandom tr -dc A-Za-z0-9 | head -c8`
SQLPASS=`< /dev/urandom tr -dc A-Za-z0-9 | head -c8`
pw groupadd $PROJECT
pw user add $PROJECT -d /home/$PROJECT -m -s /bin/sh -G $PROJECT
echo '$USERPASS' |pw usermod $PROJECT  -h 0
### directories ###
mkdir /home/$PROJECT/htdocs
mkdir /home/$PROJECT/logs
chmod -R 755 /home/$PROJECT
chown -R $PROJECT /home/$PROJECT
### MySQL ###
mysql -t <<STOP
CREATE DATABASE $PROJECT default character set utf8 collate utf8_general_ci;
CREATE USER '$PROJECT'@'localhost' Identified by '$SQLPASS';
GRANT ALL ON $PROJECT.* TO '$PROJECT'@'localhost';
\q
STOP
echo "User name: $PROJECT"
echo "User password: $USERPASS"
echo "MySQL password: $SQLPASS"
```

XMLStartlet

apt-get install xmlstartlet

elenca tutti i nodi
xmlstartlet el -u file.xml

elenca tutti gli attributi
xmlstartlet el -a file.xml

elenca tutti i valori per ogni attributo

xmlstartlet el -v file.xml

xmlstartlet sel -T

VFAStorage

Il servizio offerto da questo dispositivo è la conservazione/preservazione delle immagini disco acquisite nonchè la condivisione.

Creazione caso

La creazione di un caso è in realtà :

- Creazione di un gruppo di utenti assegnando il nome di un case (es.: PP0001)
- Aggiunta di un primo utente a tale gruppo
- Creazione di un Dataset ed assegnazione al gruppo con diritti di file system
- Creazione di una share CIFS con lo stesso nome del gruppo e con target il Dataset appena creato.
- Assegnazione del gruppo in modalità sola lettura
- Assegnazione del gruppo di amministrazione (vfa) con diritti di scrittura/lettura.
- Creazione di un volume ZVol da condividere via iSCSI per la memorizzazione dell'esito analisi.

A seguito della creazione del caso l'utente "vfa" che appartiene al gruppo "vfa" potrà caricare le immagini disco acquisite.

Ogni immagine disco (composta da n file si atipo E01 sia tipo DD) sarà posizionata all'interno della propria directory che avrà lo stesso nome.

Es.: *Win7dd.dd* sarà nella directory *Win7dd*.
Win7casa.E01 ... Win7casa.E02 ... Win7casa.E0n andrà nella directory *Win7casa*

La creazione avviene con lo script *addcaseusers.sh* :

```
#!/usr/local/bin/bash
##     This script creates a dataset, assign it to a group and add a user to this last.
##     Also create volume for storaging analisys results.
##
## Admin group : vfa                                                    (there is always the
group vfawhich is an administrative-internal group)
## Dataset group : input group (eg.: PP1234)
## TODO : manage users on group


### Variables

user=$1                             # New user name
pass=$2                             # New user password
group=$3
admin_user=$4                       # Supervisor's account name
dataset=$5
samba_config=/usr/local/etc/smb.conf   # Path to Samba config file (smb.conf)
pathtostorage=storage/
pathtolog=/var/log/vfa/
size=2
LOG=$pathtolog$group.log

### Functions

## Usage ##
usage ()
{
       if [ "$1" -ne "3" ]; then
              echo
              echo -e "\tUsage : $0 username password group\n"
```

```
             exit 1
        fi
}
## Check for root access
root_check ()
{
     if [ $(id -u) != "0" ]
          then echo "`date +%s` - Need to be root"; exit 1
     fi
}
## Create the dataset
create_dataset()
{
       zfs create $pathtostorage$group
       chgrp $group /$pathtostorage$group
       chmod 777 /$pathtostorage$group
}
## Create volume analisi for the group
create_volume()
{
       zfs create -V "$1"G $pathtostorage$group/$group-analisys
       #chgrp $group /dev/zvol/$pathtostorage/$group
}

## Create the group
add_group()
{
       pw groupadd $group
}
## Create log file
add_log(){
    touch $pathtolog$group.log
    echo "`date +%s` - Starting Log file per Gruppo : $group" >> $LOG
}

# Add user to the group (case) then set encrypted password
add_user ()
{
       pw useradd $user -m -g $group -s /dev/null
       echo "$pass" | pw usermod $user -h 0
}

# Add supervisor to the group for administration
admin2group ()
{
       pw usermod $admin_user -g $group
}

# Add user and password to Samba
add_user_samba ()
{
       (echo "$pass"; echo "$pass") | smbpasswd -s -a $user
}

# Add a share
add_share ()
{
       echo -e "\n## $group begin ##\n[$group]\n \tpath = /$pathtostorage$group\n
\tcomment = $group's Folder\n \tguest ok = no\n \tbrowseable = yes\n \tpublic = no\n
\twritable = yes\n \tread list = @$group\n \twrite list = @vfa\n \tvalid users = @vfa,
@$group\n \tcreate mask = 0770\n \tforce create mode = 0770\n \tsecurity mask = 0770\n
\tforce security mode = 0770\n \tdirectory mask = 2770\n \tforce directory mode =
2770\n \tdirectory security mask = 2770\n \tforce directory security mode = 2770 \n##
$group end ##" >> $samba_config
}

# Reload Samba server
smbd_reload ()
{
       service samba reload
}
```

```
# Restart Samba server
smbd_restart ()
{
       service samba restart
}

### Main Routine

## Redirection output salvo file descrittori
usage $#
root_check
add_log
exec 3>&1 4>&2
exec 1>$LOG 2>&1
# Create system and samba user with home directory
#echo "`date +%s` - Creating user"
    add_group && add_user && add_user_samba
    if [ "$?" = "0" ]; then
        echo "`date +%s` - Creazione gruppo ed utente completata"
    else
        echo "`date +%s` - Creazione gruppo ed utente fallita"; exit 1
    fi
# Create shares in smb.conf and add supervisor to user's group
#echo "`date +%s` - Aggiunta share e gestione permessi in smb.conf"
    #add_share && admin2group
    add_share
    if [ "$?" = "0" ]; then
        echo "`date +%s` - Aggiunta share e permessi completata"
    else
        echo "`date +%s` - Aggiunta share e permessi fallita"; exit 1
    fi
# Create shares add supervisor to user's group
#echo "`date +%s` - Creazione dataset e gestione permessi"
    create_dataset
    if [ "$?" = "0" ]; then
        echo "`date +%s` - Creazione dataset e gestione permessi completata"
    else
        echo "`date +%s` - Creazione dataset e gestione permessi fallita"; exit 1
    fi
# Create volume add to group
#echo "`date +%s` - Creazione dataset e gestione permessi"
    create_volume $size
    if [ "$?" = "0" ]; then
        echo "`date +%s` - Creazione volume Analisi e permessi completata"
    else
        echo "`date +%s` - Creazione volume Analisi e permessi fallita"; exit 1
    fi
# Restart/Reload samba
#echo "`date +%s` - Reloading Samba sharing service"
    #smbd_restart
    smbd_reload
    if [ "$?" = "0" ]; then
        echo "`date +%s` - Reloading Samba sharing service completato"
    else
        echo "`date +%s` - Reloading Samba sharing service fallito"; exit 1
    fi
exit
#restore file descrittori
exec 1>&3 3>&-
exec 2>&4 4>&-
```

Rimozione share

La rimozione di una share avviene utilizzando lo script *rmcaseshare.sh*

```
#!/usr/local/bin/bash

##     This script removes a cifs share

### Variables

share=$1
samba_config=/usr/local/etc/smb.conf   # Path to Samba config file (smb.conf)
pathtolog=/var/log/vfa/
LOG=$pathtolog$group.log

### Functions

## Usage ##
usage ()
{
       if [ "$1" -ne "1" ]; then
              echo
              echo -e "\tUsage : $0 share\n"
              exit 1
        fi
}
## Check for root access
root_check ()
{
     if [ $(id -u) != "0" ]
          then echo "`date +%s` - Need to be root"; exit 1
     fi
}
## Remove the share making a backup copy
remove_share (){
       cp /usr/local/etc/smb.conf /usr/local/etc/smb.conf.$group
       sed -e '/## '$share' begin ##/,/## '$share' end ##/d' /usr/local/etc/smb.conf >
/usr/local/etc/smb.conf.new
       mv /usr/local/etc/smb.conf.new /usr/local/etc/smb.conf
}
#########################
usage $#
root_check
exec 3>&1 4>&2
exec 1>>$LOG 2>&1
remove_share
exec 1>&3 3>&-
exec 2>&4 4>&-
```

Aggiunta di una LUN iSCSI

Durante la creazione di un caso si crea anche un volume che servirà a memorizzare l'esito di una prima analisi condotta sull'immagine disco montata. Tale volume (zvol) sarà condiviso attraverso iSCSI. L'aggiunta dell'apposita LUN avviene attraverso lo script *addlun.sh*

```
#!/usr/local/bin/bash
##     This script adds a LUN

###Variables
lun=$1                              # lunname
authgroup=$2                        # authgroup (group in auth.conf
group=$3                            # group

istgt_conf=/usr/local/etc/istgt/istgt.conf   # Path to istgt config file (istgt.conf)
pathtovolumes=/dev/zvol/storage/
pathtolog=/var/log/vfa/
LOG=$pathtolog$group.log
random=`jot -r 1 10 1000`

###Functions
## Usage ##
usage ()
{
       if [ "$1" -ne "3" ]; then
              echo
              echo -e "\tUsage : $0 <lun name> <authorized group> <group>\n"
              exit 1
        fi
}
## Check for root access
root_check ()
{
     if [ $(id -u) != "0" ]
          then echo "`date +%s` - Need to be root"; exit 1
     fi
}
## Test if a file exists ##
testfile ()
{
   [-e "$1"]
   return $?
}
## Add the LUN definition into ISTGT config file
add_lun(){
# TargetName, Mapping, UnitType, LUN0 are minimum required
       echo   -e   "\n##   $lun   begin   ##\n[LogicalUnit$lun]\n\tComment   Hard   disk
$lun\n\tTargetName  $lun-analisys\n\tTargetAlias  Analisys  Disk\n\tMapping  PortalGroup1
InitiatorGroup1\n\tAuthMethod          Auto\n\tAuthGroup          $authgroup\n\tUseDigest
Auto\n\tUnitType  Disk\n\tLUN0  Storage  $pathtovolumes$group/$lun-analisys  Auto\n\tLUN0
Option  Serial  10000$random\n\tLUN0  Option  RPM  1\n\tLUN0  Option  FormFactor  2  \n## $lun
end ##" >> $istgt_conf
}
## Reload service
istgt_reload(){
       service istgt reload
}

### Main Routine
## Redirection output salvo file descrittori
usage $#
root_check
exec 3>&1 4>&2
exec 1>>$LOG 2>&1
testfile "$LOG"
if [ "$?" = "1" ]; then
        echo "`date +%s` - File log not esists"; exit 1
fi
testfile $pathtovolumes$group/$lun-analisys
if [ "$?" = "1" ]; then
```

```
        echo "`date +%s` - LUN creation $lun failed, target file does not exist"; exit
1
fi
add_lun
if [ "$?" = "0" ]; then
        echo "`date +%s` - LUN creation $lun completed"
    else
        echo "`date +%s` - LUN creation $lun failed"; exit 1
    fi
istgt_reload
if [ "$?" = "0" ]; then
        echo "`date +%s` - Reloading iSCSI target service completed"
    else
        echo "`date +%s` - Reloading iSCSI target service failed"; exit 1
    fi
exit
#restore file descrittori
exec 1>&3 3>&-
exec 2>&4 4>&-
```

Rimozione di una LUN

Al termine delle attività sarà possibile rimuovere la condivisione del volume usando *rmlun.sh*

```
#!/usr/local/bin/bash
## This script removes a LUN

###Variables
lun=$1                              # lun name
istgt_conf=/usr/local/etc/istgt/istgt.conf   # Path to istgt config file (istgt.conf)
pathtovolumes=/dev/zvol/storage/
pathtolog=/var/log/vfa/
LOG=$pathtolog$lun.log
###Functions
## Usage ##
usage ()
{
       if [ "$1" -ne "1" ]; then
              echo
              echo -e "\tUsage : $0 <lun name>\n"
              exit 1
        fi
}
## Check for root access
root_check ()
{
     if [ $(id -u) != "0" ]
          then echo "`date +%s` - Need to be root"; exit 1
     fi
}

testfile()
{
  [ -e "$1" ]
  return $?
}

remove_lun ()
{
 cp $istgt_conf $istgt_conf.$lun
 sed -e '/## '$lun' begin ##/,/## '$lun' end ##/d' $istgt_conf > $istgt_conf.new
 mv $istgt_conf.new $istgt_conf
}
istgt_reload(){
       service istgt reload
}
```

```
### Main Routine
usage $#
root_check
exec 3>&1 4>&2
exec 1>>$LOG 2>&1
testfile "$pathtovolumes$lun/$lun-analisys"
if [ "$?" = "1" ]; then
       echo "`date +%s` - I'm not able to remove the LUN, the file does not exist";
       exit 1
fi
remove_lun $lun
istgt_reload
echo "`date +%s` - Lun $lun removed"
exec 1>&3 3>&-
exec 2>&4 4>&-
```

VFAVirtual

Questo dispositivo offre un servizio di virtualizzazione "on-demand" cioè esegue la connessione al caso indicato e virtualizza i dischi immagine indicati. La virtualizzazione passa per diversi steps che sono :

Montaggio e creazione di un Virtual Drive (hard disk virtuale)

- Monta la condivisione CIFS del caso
- Controlla che siano presenti file utili al successivo mounting
- Monta i file immagine (non è necessario riversarli in un solo unico file) affuse o xmount
- Crea un file di cache apposito per evitare la scrittura/modifica dei files immagine originali
- Converte il file immagine così montato in disco virtuale (VDI)

- Adattamento del disco immagine e del S.O. in esso contenuto all'avvio in ambiente virtuale

  In questo caso è possibile ottimizzare il S.O. per essere eseguito in ambiente virtuale. Questa operazione viene eseguita attraverso un'apposita macchina virtuale che, avviandosi con un apposito livecd, esegue delle operazioni automatizzate. L'utente amministratore potrà gestire tale operazione collegandosi alla porta 6500, del sistema di virtualizzazione, via RDP.

  Nel caso di macchine Windows con profili utenti protetti da password è possibile utilizzare la stessa procedura per "cancellarle".

  Al termine di questa procedura si potrà spegnere e cancellare questa macchina virtuale denominata "open" lasciando di fatto il disco virtuale nella nuova condizione con S.O. virtualizzabile ed utenti senza password.

Creazione di una macchina virtuale

- Controlla che esistano e sia raggiungibili le risorse per creare la macchina
- Crea una macchina con risorse standard con nome/porta vrde assegnato
- Crea un file di log apposito della macchina
- Aggiunge il disco virtuale appena creato nella fase precedente

Uso/controllo della macchina

- Controlo della macchina come accensione / spegnimento / reset / poweroff / acpipowerbutton / loadcd / unloadcd / ecc.
- Visualizzazione dello schermo della macchina attraverso client RDP sulla porta 5000-5020

Montaggio e creazione di un Virtual Drive (vdi) *virtmount.sh*

Creazione macchina virtuale *createvm.sh*

```
#!/bin/bash

configfile='/etc/vfa/vfa.conf'
configfile_secured='/tmp/vfa.conf'

# check if there is malicious code
if egrep -q -v '^#|^[^ ]*=[^;]*' "$configfile"; then
  echo "Config file is unclean, cleaning it..." >&2
  # purge original source and create new clean config file
  egrep '^#|^[^ ]*=[^;&]*'  "$configfile" > "$configfile_secured"
  configfile="$configfile_secured"
fi

# now we can source it
source "$configfile"

###Variables
vmname=$1            # Virtual machine's name
ostype=$2           # os type: WindowsXP Windows7 Linux
image=$3            # hard disk image file complete of path
logfile=$5          # logfile name
LOG=$pathtolog$logfile.log

###Functions
## Usage ##
usage ()
{
       if [ "$1" -ne "4" ]; then
              echo
              echo   -e   "\tUsage   :   $0   vmname   ostype   path-to-image   vrdeport
logfile\n\n\t\ttype $0 oslist for listing all the OS types (very long list)"
              exit 1
       fi
}

## Check for root access
root_check ()
{
    if [ $(id -u) != "0" ]
       then echo "`date +%s` - Need to be root"; return 1
    fi
}

oslist()
{
       if [ "$1" = "oslist" ]; then
              vboxmanage list ostypes
              return 0
       else
              return 1
       fi
}

# cretae virtual machine
create_vm()
{
       if [ ! -e "$image" ]; then
              echo "`date +%s` - The virtual hard disk $image does not exist"
              return 1
       else
              echo "`date +%s` - The virtual hard disk exists"
```

```
              vdimountpoint=$image
       fi
       VBoxManage setproperty machinefolder "$vmsfolder"
       echo "Creating VM $vmname"
       VBoxManage createvm --name "$vmname" --ostype "$ostype" --register
       echo "Addind and customizing $vmname with mem $vmmem"
       VBoxManage modifyvm "$vmname" --memory $vmmem --acpi on --vram 128 --boot1 dvd --
nic1 bridged --bridgeadapter1 eth0
       echo "Addind SATA Controller with 4 ports"
       VBoxManage storagectl "$vmname" --name "SATA Controller" --add sata --controller
IntelAHCI --sataportcount 4
       echo "Attaching a virtual disk $image"
       VBoxManage storageattach "$vmname" --storagectl "SATA Controller" --port 0 --
device 0 --type hdd --medium $image
       echo "Addind IDE Controller with 4 ports"
       VBoxManage storagectl "$vmname" --name "IDE Controller" --add ide
       echo "Attaching dvddrive to IDE1\/0"
       VBoxManage storageattach "$vmname" --storagectl "IDE Controller" --port 1 --
device 0 --type dvddrive --medium emptydrive
       echo "Defining boot sequence"
       VBoxManage modifyvm "$vmname" --boot1 dvd --boot2 disk --boot3 none --boot4 none
       VBoxManage modifyvm "$vmname" --vrde on
       VBoxManage modifyvm "$vmname" --vrdeport $vrdeport
}

### Main Routine
usage $#
#Conf
if [ -z $4 ]; then
       echo "`date +%s` - VRDE port undefined"
       exit 1
elif [ $4 -ge $MIN_VRDE_PORT -a $4 -le $MAX_VRDE_PORT ]; then
       vrdeport=$4
else
       echo "`date +%s` - The VRDE port number inserted is not valid for this system"
       exit 1
fi
if [ -z $5 ]; then
       logfile=$1
fi
root_check
oslist $1
exec 3>&1 4>&2
exec 1>>$LOG 2>&1
create_vm
exec 1>&3 3>&-
exec 2>&4 4>&-
exit
```

Creazione macchina virtuale "OPEN"

```
#!/bin/bash

configfile='/etc/vfa/vfa.conf'
configfile_secured='/tmp/vfa.conf'

# check if there is malicious code
if egrep -q -v '^#|^[^ ]*=[^;]*' "$configfile"; then
  echo "Config file is unclean, cleaning it..." >&2
  # purge original source and create new clean config file
  egrep '^#|^[^ ]*=[^;&]*'  "$configfile" > "$configfile_secured"
  configfile="$configfile_secured"
fi

# now we can source it
source "$configfile"

############
###Variables
############
```

```
vmname=$1           # Virtual machine's name
image=$2            # Virtual Drive vdi

LOG=$pathtolog$1.log

############
###Functions
############

## Usage ##
usage ()
{
       if [ "$1" -ne "2" ]; then
              echo
              echo -e "\tUsage : $0 vmname image(path to)"
              exit 1
       fi
}

## Check for root access
root_check ()
{
    if [ $(id -u) != "0" ]
       then echo "`date +%s` - Need to be root"; return 1
    fi
}

# cretae virtual machine
create_vm()
{
       if [ ! -e "$image" ]; then
              echo "`date +%s` - The virtual hard disk $image does not exist"
              return 1
       else
              echo "`date +%s` - The virtual hard disk exists"
              vdimountpoint=$image
       fi
       VBoxManage setproperty machinefolder "$vmsfolder"
       echo "Creating VM $vmname"
       VBoxManage createvm --name "$vmname" --ostype Windows7 --register
       echo "Addind and customizing $vmname with mem $vmmem"
       VBoxManage modifyvm "$vmname" --memory $vmmem --acpi on --vram 4 --boot1 dvd --
nic1 bridged --bridgeadapter1 eth0
       echo "Addind IDE Controller with 4 ports"
       VBoxManage storagectl "$vmname" --name "IDE Controller" --add ide
       echo "Attaching a virtual disk $image"
       VBoxManage storageattach "$vmname" --storagectl "IDE Controller" --port 1 --
device 0 --type hdd --medium "$image"
       echo "Attaching dvddrive to IDE1\/0"
       VBoxManage storageattach "$vmname" --storagectl "IDE Controller" --port 0 --
device 0 --type dvddrive --medium /root/opengates.iso
       echo "Defining boot sequence"
       VBoxManage modifyvm "$vmname" --boot1 dvd --boot2 disk --boot3 none --boot4 none
       VBoxManage modifyvm "$vmname" --vrde on
       VBoxManage modifyvm "$vmname" --vrdeport 6500
}


################
### Main Routine
################
## Redirection output salvo file descrittori
usage $#
#Conf
#if [ -z $4 ]; then
       #echo "`date +%s` - VRDE port undefined"
       #exit 1
#elif [ $4 -ge $MIN_VRDE_PORT -a $4 -le $MAX_VRDE_PORT ]; then
#      vrdeport=$4
#else
#      echo "`date +%s` - The VRDE port number inserted is not valid for this system"
```

```
#      exit 1
#fi
#if [ -z $5 ]; then
#      logfile=$1
#fi
root_check
exec 3>&1 4>&2
exec 1>>$LOG 2>&1
create_vm
#restore file descrittori
exec 1>&3 3>&-
exec 2>&4 4>&-
exit
```

Creazione macchina virtuale *controlvm.sh*