Sequestri di materiale informatico
e Autodifesa informatica

Prerelease ver. 001.05

Capitolo 1 - Introduzione

Sempre più spesso il computer risulta al centro delle attenzioni della Polizia Giudiziaria (P.G.). Il motivo è facile da comprendere: i supporti magneto-ottici sono facilmente manipolabili, costruire prove risulta semplice, con un po' di abilità si riesce addirittura a non lasciare tracce, generalmente nessuno si attiva per contrastare la perizia informatica degli esperti incaricati dalle autorità (i cosidetti Forensic), inoltre quando si recupera il materiale informatico sottoposto a perquisizione, l'ultima cosa di cui ci si preoccupa è di realizzarne un controllo dettagliato.

In un periodo particolare come questo, dove le montature giudiziarie superano di gran lunga l'immaginabile e ogni prova "manipolabile" può essere di aiuto alla P.G. per dimostrare teoremi eversivi, il computer ha senz'altro un ruolo rilevante.
Il computer viene generalmente usato per realizzare documenti, manifesti e quindi per stamparli. Il passo successivo lo può fare la P.G. magari aggiungendone o nascondendone altri o modificandone i contenuti. Ma cosa possiamo fare per evitare che i mezzi che ci "agevolano" nello studio, nel lavoro o semplicemente nei nostri interessi, vengano usati contro di noi?

In realtà il sequestro di un computer non è mai così "giustificabile": tutta la giurisprudenza parla di "pirateria" e annessi, non di sequestri a "scopo politico" usati per spiare e controllare le attività degli oppositori. Tuttavia, in mancanza di una giurisprudenza specifica in merito, gli organi di controllo e repressione fanno ciò che vogliono.

Uno degli interventi più "pericolosi" effettuati dalla Polizia Scientifica potrebbe essere, ad esempio, la creazione, aggiunta o modifica anche parziale del contenuto degli Hard Disk.
Nessuno è in grado di garantire che eventuali prove "scottanti" riscontrate nei file dei vostri hard-disk, non siano stati "aggiunti" durante il sequestro, magari con qualche accorgimento ad esempio per farli sembrare cancellati in precedenza. Nessuno è in grado di provare che gli indirizzi trovati nelle agende elettroniche o nei telefoni cellulari non siano stati modificati appositamente per giustificare un'azione repressiva o determinare collegamenti con altre realtà o con realtà inesistenti? Assolutamente nessuno.

Quello appena ipotizzato sembrerebbe configurarsi come un caso eclatante, ma è probabile che molte volte le prove per giustificare le indagini e la repressione a livello nazionale e internazionale siano fondate su materiale informatico manomesso dopo il sequestro.
Cominciamo con il dire che:

- **LA POLIZIA GIUDIZIARIA PUO' PROCEDERE A PERQUISIZIONE E SEQUESTRO SOLO BASANDOSI SU DI UNA NOTIZIA DI REATO PREESISTENTE, E NON PIUTTOSTO PER ACQUISIRE LA NOTIZIA STESSA E LE RELATIVE PROVE.**

La P.G. non può sequestrare un computer per il reato ad esempio di imbrattamento col fine di ricercarvi prove diverse dal reato di imbrattamento, quali ad esempio il 270bis.

Inoltre:

- **E' NECESSARIO CHE IL CONTROLLO IN SEDE DI PERQUISIZIONE SIA EFFETTIATO DA UNA PERSONA ESPERTA QUALE AUSILIARIO (art. 348 c.p.p), IN MODO TALE CHE VENGA SOTTOPOSTO A SEQUESTRO SOLO CIO' CHE E' REALMENTE NECESSARIO**

Questo punto necessità di maggiori spiegazioni per le diverse interpretazioni a cui si presta.
Ci deve essere un tecnico che sappia distinguere fra computer, stampante, scanner e altro hardware per evitare che il sequestro comporti danni paragonabili alla pena relativa al reato contestato.

Una sentenza della corte di Cassazione di Roma (2003/03983) relativa ad un ricorso per il dissequestro di un computer completo di monitor, stampante e scanner dispone:

[...] la Corte annulla senza rinvio l'ordinanza impugnata relativamente a tutto il materiale informatico sequestrato, ad eccezione della memoria fissa del computer, disponendone il dissequestro e la restituzione agli aventi diritto. Così deciso in Roma, il 18 novembre 2003.

In pratica la Corte di Cassazione limita il sequestro solo ai cosiddetti supporti per la memorizzazione dei dati

Pertanto la P.G. si trova di fronte a due alternative:

1. **Sequestrare ESLUSIVAMENTE i supporti di memorizzazione (hard disk, dvd rw, cd rw, etc.)**
2. **Procedere a copia dei supporti in loco**

Inoltre va ricordato che secondo la legge italiana:

Un computer è uno strumento assolutamente comune e privo di caratteristiche tecniche o specificità che lo rendono unico (al contrario ad esempio di una pistola), è sufficiente quindi verbalizzare la configurazione senza procedere al sequestro.

Il computer NON può inoltre essere "Corpo del Reato" proprio per le sue caratteristiche neutre.

Si definiscono quindi come Corpo del reato:

"*Tutte le cose sulle quali o mediante le quali il reato è stato commesso, nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo."*

Relativamente al possibile contenuto e alla copia dei documenti presenti sul computer:

il **documento informatico** è definito come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. É quindi un insieme di bit che esiste solo in relazione ad un sistema in grado di leggerlo, e non di per sé stesso. L'informazione, quindi, è separata dal supporto che la contiene. Il documento informatico, a differenza di quello cartaceo, può essere trasferito da un supporto ad un altro, e di esso è possibile eseguire non semplicemente delle copie, ma degli esemplari esattamente identici all'originale e dotati della stessa efficacia. Il concetto di "originale" differente dalla sua "copia" in ambito di contenuti digitali non sussiste. Un Documento informatico può essere dunque riprodotto, trasmesso a distanza senza perdere la propria originalità, in quanto la sequenza di bit rimane inalterata.

Un altro caso relativo alle problematiche del sequestro di computer lo ritroviamo in una sentenza del 7 febbraio 2000 del tribunale di Torino dove:

"*il Pubblico Ministero aveva disposto il sequestro del solo hard disk e non di tutta la macchina. Si ribadisce la legittimità generale della sequestrabilità di un computer o di parte di esso, perché si rileva che fra il reato e il computer sussisterebbe un "vincolo pertinenziale" in quanto il software necessita dell'hard disk per funzionare, non rileva quindi che il software possa funzionare su un altro hard disk."*

Si ribadisce che per "mettere le mani" su un computer sospetto si può usare lo strumento del decreto di perquisizione e non quello dell'ispezione. La perquisizione (locale o personale) si usa per constatare se qualcuno porta su di sé o nasconde in qualche luogo il "corpo del reato" o elementi indizianti, mentre l'ispezione si effettua appunto sugli oggetti per rilevare elementi di fatto utili alle indagini. Secondo il giudice di Torino per le necessità di indagine sarebbe stato sufficiente effettuare una copia integrale del disco e affidarne l'analisi ad esperti e consulenti vari. Questo anche perché i dati contenuti nel computer avrebbero potuto appartenere a terzi che ne sarebbero stati ingiustamente privati. Ecco le parole del giudice:

"Pare invece accoglibile il motivo di riesame concernente la non necessità del sequestro dell'hard disk. Infatti nulla impediva agli agenti di P.G. , per di più appartenenti a Sezione specializzata nell'ambito dai reati informatici di procedere ad una copia integrale dell'hard disk, con specificazione verbale di ogni singola operazione."

Le prove del reato informatico sono spesso dei beni immateriali suscettibili di essere facilmente inquinati. É estremamente facile sia falsificare e cancellare le prove da esibire a dimostrazione di un reato informatico, sia modificare l'oggetto della prova: non è possibile, infatti, porre sui dati e sul software qualcosa di simile ad un sigillo che ne riveli in modo inequivocabile l'effrazione. I personal computer, per come sono strutturati oggi, non contengono solo dati pertinenti e rilevanti ai fini d'indagine. Spesso all'interno dell'Hard disk sono contenuti file molto personali. Basti pensare alla corrispondenza intrattenuta per posta elettronica e come la stessa sia tutelata dalla Costituzione Italiana (art. 15 Cost.). Un sequestro di tutti i componenti del personal computer lederebbe una serie di diritti fondamentali costituzionalmente protetti: riservatezza, segretezza, ma anche dello stesso diritto di difesa e persino del diritto di proprietà. Infatti il sequestro di tutto il personal computer - comprensivo cioè di schede audio, video e monitor (che tutto sono tranne che corpo del reato) - è lesivo anche di quel principio di pertinenza-rilevanza posto dal nostro legislatore all'art. 190 c.p.p. laddove afferma:
Le prove sono ammesse a richiesta di parte. Il giudice provvede senza ritardo con ordinanza escludendo le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti.
Il modo per essere sicuri che la P.G. non aggiunga, modifichi o in qualche modo danneggi il contenuto di un Hard disk è pretendere o eseguire personalmente la copia giudiziaria conforme e la "sigillazione" dell'hardware al momento del sequestro (non dopo). Inoltre apporre un sigillo "elettronico" tramite crittazione del file risultante con PGP.

Ma che cos'è questa fantomatica Copia Giudiziaria Conforme?

Tecnicamente una copia giudiziaria conforme è un copia esatta (byte a byte) del contenuto delle directory incriminate (o dell'intero disco) che vengono criptate e quindi copiate su un supporto immodificabile (DVDROM o CDROM). La giurisprudenza trattata nel DPCM 82/99 definisce tutte le caratteristiche della cifratura (criptazione) perché queste copie possano essere sicure e immodificabili.

In generale la giurisprudenza fa riferimento alle perquisizioni giudiziarie relative all'utilizzo di software pirata (copiato illegalmente) o ai reati informatici (hacking, ecc.) e indica specifiche copie relative a specifiche cartelle e/o a specifici programmi applicativi. Non fa alcun riferimento invece, e pare non ci sia normativa a riguardo, ai sequestri "generici" (esempio:"mi prendo il tuo PC per vedere cosa c'è dentro") effettuati nell'ambito di perquisizioni per contestazioni "generiche", come nel caso dei sequestri per la ricerca di generico "materiale" interessante.
In pratica quando si preveda il sequestro di PC o supporti ottico-magnetici, il motivo del sequestro e la destinazione delle ricerche dovrebbero essere specificati nel mandato di perquisizione. Già il fatto che si faccia riferimento a dati "generici" relativi a reati è contestabile.
La Copia Giudiziaria Conforme, come logico, deve riprodurre la situazione ESATTAMENTE al momento del sequestro e deve essere fatta in loco, nella data del sequestro o nell'immediato, non 20 giorni dopo. Per eseguire la copia giudiziaria conforme il computer NON deve essere acceso, o meglio i sistemi operativi presenti non devono essere avviati. Questo in quanto durante la procedura di avviamento, le date relative ad alcuni file di sistema in windows vengono modificate, mentre in sistemi "Unix-like" viene aggiornata tutta la relazionistica della macchina e quindi la situazione non è più quella del sequestro.
Per eseguire una copia conforme NON è necessaria la password di autenticazione in quanto viene semplicemente fatta la copia delle directory al completo e quindi letta o meglio "montata" da un'altro sistema e/o analizzata dai vari programmi per l'analisi dei dischi. Nel caso di criptazione delle cartelle il processo si fa leggermente più lungo e complesso, ma non rappresenta un grosso problema.
In questa procedura i sistemi operativi presenti sui computer sequestrati NON devono essere accesi. L'unico strumento/software valido (lo dice pure l'FBI…sic) per la copia giudiziaria conforme è il comando linux "dd" (per informazioni "man dd" sulla vostra linux box). Questo software fa la copia byte a byte del dispositivo da copiare, non si preoccupa di password o altro.
Inoltre alla fine della copia l'Hardware deve essere restituito immediatamente integro e funzionante (cosa che regolarmente NON avviene, di solito lo restituiscono rotto o con alcuni pezzi da aggiustare).
Per il controllo del checksum utilizzare "md5sum" e quindi per apporre la firma digitale utilizzare il comune PGP.
Una volta fatta la copia giudiziaria conforme a nostra volta, è necessario analizzarla e, se necessario, compararla.
Come veloce controprova, al momento del dissequestro per controllare i log (la così detta "relazionistica") dei sistemi operativi è sufficiente avviare il PC da CDROM utilizzando, ad esempio, una "linux live distro" (ad esempio una Knoppix) e quindi montare i filesystem degli Hard Disk in READ ONLY (sola lettura). Controllare le date dei file di sistema (se si usa, ahimè, windows) oppure se si usa linux, unix, BSD, ecc. i log di sistema (che di solito si trovano in /var/log).
Non dimentichiamo che la P.G. può modificare, con un semplice editor esadecimale (tipo WinHex) qualsiasi dato presente sul disco senza che ne venga modificata la data di creazione. In quel caso è necessaria un'analisi della superficie del disco abbastanza laboriosa e, di solito, distruttiva (ricerca tipica delle ditte che trattano il recupero dati in caso di crash fisico degli Hard Disk).
La prima cosa che solitamente fa la P.G. invece è accendere i PC e impuntarsi sulle password. Questo modifica la situazione del sistema al momento del sequestro e da quell'istante ogni prova è invalidata. Altro errore grossolano è quello di NON fornire copia giudiziaria conforme al momento del sequestro, all'indagato (o all'avvocato dell'indagato). Al momento del sequestro il PC va inoltre SIGILLATO (di modo che non vengano sostituiti i supporti ottico-magnetici con altri esattamente uguali con "quasi" lo stesso contenuto). In mancanza di sigilli qualsiasi "prova" è seriamente compromessa e quindi impugnabile.
In pratica, l'Hardware (il computer stesso) NON deve essere aperto.

IN CASO DI SEQUESTRO RICORDARSI QUINDI DI:

1. **Pretendere copia conforme in loco e farsene consegnare una copia.**
2. **Pretendere la "blindatura" dell'Hardware tramite sigilli.**
3. **In caso di rifiuto, farsi verbalizzare la mancata consegna e l'assenza di sigilli.**

Va ricordato che qualsiasi "lavoretto" dovesse fare la "Polizia Scientifica" o i "forensics", deve essere eseguito sulla COPIA, mai sull'originale. In pratica non possono lavorare con il vostro computer, bensì sui loro utilizzando la copia conforme eseguita al momento del sequestro e possibilmente non un mese dopo.
Logicamente la P.G. al momento del sequestro mette l'individuo in uno stato di forte prostrazione psicologica; spesso le perquisizioni vengono fatte alle sei del mattino oppure addirittura prima, mentre la giurisprudenza dice che:

la perquisizione in un'abitazione o in luoghi chiusi adiacenti ad essa non può essere iniziata prima delle ore sette e dopo le ore venti (in casi urgenti però l'autorità giudiziaria può disporre per iscritto che sia eseguita

anche in altra ora).

Inoltre le pressioni psicologiche si fanno sempre più forti dato "il vizietto" che la P.G. ultimamente ha di portare in caserma per la semplice firma dei verbali per poi notificare procedimenti di custodia cautelare in carcere e/o altro (ricordarsi che ci si può rifiutare, a firmare i verbali di sequestro ci si può recare anche più tardi). Inoltre la perquisizione o l'ispezione sono delle procedure umilianti; a chi fa piacere che un perfetto sconosciuto metta le mani nei propri cassetti, guardi la propria posta (anche se vietato, come cita il legislatore: in caso di sequestro della corrispondenza l'ufficiale di polizia giudiziaria deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati senza aprirli e senza prenderne altrimenti conoscenza del loro contenuto;).
Si tende quindi a far durare questa situazione il meno possibile e ci si dimenticano alcuni punti fermi sui quali è necessario NON transigere.

Forensic?

Vista l'ormai dimostrata inutilizzabilità delle prove acquisite tramite analisi dei computer, e viste le continue contestazioni (con relativi rimborsi) per la poca accuratezza nel trattare l'argomento, la P.G. si appoggia sempre più spesso a figure esterne, tecnicamente valide, il "forensics" è una persona esterna alla procura o alla P.G. abilitata alla consulenza per i materiali informatici. In pratica, il forensics" è un consulente che prende in consegna i computer, ne esegue copia giudiziaria conforme e ne analizza il contenuto in quanto abilitato dalla Procura al trattamento e all'analisi delle "prove" informatiche. La Procura o la P.G. si appoggia di solito a ditte che trattano di sicurezza informatica. Spesso si tratta di persone molto abili, quindi la nostra analisi di verifica dovrà essere ancora più puntigliosa. Ci si trova quindi davanti un "osso duro" che è motivato dal denaro più che dalla sua funzione isituzionale o dalla curiosità professionale e che può rappresentare un pericoloso protagonista del controllo e della repressione prossima futura. Ciononostante ogni prova acquisita tramite analisi a basso livello è, e rimarrà sempre, contestabile sia per l'approssimativa conduzione delle indagini della P.G., sia per la mancanza di una firma digitale o di un riferimento certo che attesti l'effettiva appartenenza della "prova inconfutabile" eventualmente trovata durante le analisi dei supporti ottici e magnetici all'effettivo proprietario del computer.
Cosa devo fare al momento del dissequestro?
Per spiegare esattamente cosa fare o non fare al momento del dissequestro è necessario entrare nello specifico capitolo delle informazioni tecniche (capitolo 2).
ASSOLUTAMENTE NON ACCENDERE I COMPUTER. Il dissequestro è un momento molto delicato qualsiasi "prova" può essere modificata, cancellata, compromessa. E' necessario capire se il materiale informatico sia stato danneggiato e se i documenti presenti nel computer siano stati aggiunti, cancellati o modificati, se la configurazione hardware (il computer) e software (i programmi, sistemi operativi ecc. ecc.) sia stata modificata. E' inoltre importante richiedere una perizia "di parte" che certifichi (stilando un verbale) la situazione del materiale informatico al momento del dissequestro a livello hardware e software. Questa può essere fatta da una qualsiasi persona che, con buone conoscenze informatiche, si assuma la responsabilità della perizia firmando il verbale che poi verrà consegnata all'eventuale avvocato difensore che procederà alla convocazione in caso di contestazioni, io preferirei suggerire un "esperto" con conoscenze specifiche che spiegherò nel capitolo relativo agli aspetti "tecnici". E' importante verificare la funzionalità dei computer (che DEVONO essere restituiti nelle medesime condizioni del sequestro). La funzionalità dei computer può essere anche verificata più tardi, a casa propria magari, e se si dovessero notare malfunzionamenti è possibile recarsi nuovamente dalla P.G. per richiedere una modifica al verbale di dissequestro.
E' importante capire l'importanza del momento del dissequestro. Va fatta, al momento, un analisi sull'aspetto HW (se il computer è stato seriamente manomesso). Per verificare la funzionalità software, appoggiarsi a una persona esperta. In generale, se si hanno dubbi sulla possibilità che la P.G. possa aver manomesso il contenuto dell'H.D., farsi accompagnare al dissequestro da un amico "esperto" che possa verificare il PC senza modificare la situazione. Diciamo comunque che più accurata sarà la fase di verbalizzazione del materiale durante il sequestro richiedendo anche di inserire numeri di serie dei supporti (HD e CDROM), delle schede madri, l'analisi visuale e l'apposizione di "sigilli" sulla viteria da parte nostra, più complicata sarà per la P.G. l'opera di falsificazione del contenuto del computer.

CHE COSA MI SERVE AL MOMENTO DEL DISSEQUESTRO?

Volendo fare i fiscali e per non mostrarsi impreparati le "cose" essenziali che servono sono:

1. **Video, tastiera e mouse vostri (è improbabile che in caserma o Questura ve ne prestino...).**
2. **Una distribuzione di linux LIVE (avviabile da CD, consiglio una Knoppix ver. da 3.7 in su per i pc o una Knoppix o Gentoo live ppc per MacIntosh).**
3. **Un hard disk Esterno USB o un masterizzatore DVD esterno.**

Ma chi glielo fa fare?

Analizzando bene la giurisprudenza notiamo che sono più gli articoli di legge che vengono violati dalle Procure che quelli eventualmente contestabili al singolo. Il resto lo fanno i media. Non è difficile avvedersi che i processi vengano svolti sui giornali dove non si parla mai di "indagini in corso" ma di "corda al collo" di qualsiasi persona entri nelle "grazie" delle Procure. Sapendo questo, le Procure sparano alto e si parla ormai sempre più di reati con nomi "altisonanti" o comunque che non permettano, grazie all'infame stampa, una qualsivoglia difesa. E così ci si può trovare in un indagine per "terrorismo" senza essere dei terroristi, ma con l'impossibilità di dimostrarlo.

Sembra un po' il conto della serva, ma la seguente lista di articoli può rendere l'idea dell'ignoranza delle Procure in materia legale relativamente al sequestro di materiale informatico.

Violazione di cinque articoli della Costituzione:

art.4 - Diritto al lavoro.
art.14 - Inviolabilità del domicilio (il concetto di domicilio informatico è definito dalla legge sui computer crime).
art.15 - Libertà e segretezza della corrispondenza (su un computer spesso si trova, oltre alla corrispondenza di chi lo possiede, anche quella di altri).
art.35 - Tutela del lavoro.
art.41 - Tutela della libera iniziativa privata. Violazione della convenzione per la salvaguardia dei diritti dell'uomo (protocollo addizionale):
art.1 - Ogni persona fisica o giuridica ha diritto al rispetto dei propri beni.

Violazione del codice di procedura penale:

Il sequestro di corrispondenza informatica (che avviene anche a carico di terzi non indagati) è in violazione degli Artt. 254-256-258 c.p.p. che tutelano la corrispondenza privata. Questo in particolare se sul sistema giace corrispondenza privata di altri utenti.

Capitolo 2 – Autodifesa Informatica

Note Tecniche

Senza voler fare il sapientino della situazione, questa parte è dedicata a chi ne vuole sapere un po' di più sui computer e come possono essere usati contro di noi. Logicamente non avendo una conoscenza infinita prego chiunque sia tecnicamente in grado di completare questo documento, di collaborarne ad una sestura quantomeno completa. I primitivisti possono tranquillamente sentirsi esentati dalla lettura di questo capitolo.
Tralasciando i devastanti effetti ambientali della produzione di Silicio per la costruzione di chip per l'informatica arriviamo alla domanda principe: “Perchè usare il computer?”. Le risposte possono essere molteplici, la più gettonata penso sia per alcuni il “lavoro”, per altri semplicemente la comodità, l'estetica nelle presentazioni, l'ordine dei documenti e la loro portabilità. Ci sono alcune cose che tutti, non solo chi è più esposto, dovrebbero sapere, che sono rappresentate dal livello di sicurezza che i nostri documenti hanno nel momento in cui vengono salvati su un computer. Queste brevi note sono infatti rivolte a tutti. Sempre più spesso l'oggetto più ricorrente in una casa è il PC, e non per niente sta diventando la cosa più sequestrata. E' anche da sfatare il fatto che solo i “cattivi” vengono perquisiti in quanto di questi tempi, dove il controllo e la repressione hanno la prevalsa sulla ragione, per la P.G. siamo tutti possibili “colpevoli”.
Logicamente questo è un capitolo che tratta “genericamente” un aspetto che non dovrebbe essere preso alla leggera, ma trattato nel dettaglio. Essendo un documento rivolto a tutti è preferibile, per la sua leggibilità, che ci si muova nella direzione dell'apprendimento.
Analizziamo ora il PC nella sua struttura:
Il computer è un insieme di schede, interfacce e supporti ottico magnetici riscrivibili e/o di sola lettura fissi e /o rimovibili (HD, ZIP, Floppy, CD-RW, DVD-RW, Compact Flash, chiavi USB, DAT, unità di Backup e chi più ne ha più ne metta) e di sola lettura (CD-ROM, DVD-ROM). L'interesse degli “inquirenti” è unicamente rivolta ai supporti magneto-ottici (di qualsiasi tipo). Sui supporti magneto-ottici fissi (Hard Disk) viene solitamente installato un Sistema Operativo. Il sistema operativo si occupa di “interfacciare” l'utente con le funzionalità proprie della macchina (schede, chip ecc. ecc.). Sul sistema operativo possono essere poi installati a loro volta degli applicativi (come ad esempio programmi per videoscrittura ecc. ecc.) che ne giustificano l'utilizzo. Una caratteristica “propria” del sistema operativo è il filesystem.
Per comodità, parleremo solo di alcuni sistemi operativi e della loro in-sicurezza. Parleremo quindi della famiglia felice di Windows, Linux, MacOSX (che è un BSD e quindi Unix).

Il filesystem

Il filesystem è, più semplicemente, il modo in cui il sistema operativo “ordina” i dati sull'Hard Disk. E' importante sapere almeno cos'è ed alcune sue caratteristiche. Il filesystem varia da sistema operativo a sistema operativo. Ad esempio, un PC con Windows XP, NT,2000 può avere come filsystem NTFS o FAT32, Windows95 (prima versione) può solo avere FAT16 mentre Windows95(Osr2), Windows98, WindowsME possono solo avere FAT32. Le caratteristiche di questi filesystem è quella di derivare (a parte NTFS) dal DOS. Una delle tristi caratteristiche del DOS è che i file, quando vengono cancellati (anche dal cestino) restano comunque residenti sul disco, finché qualche altro file non verrà salvato nella stessa posizione. In pratica, per non renderli visibili (e per farli sembrare cancellati), il sistema operativo aggiunge al nome un carattere “~” la tilde e quindi il “File manager” (l'esplora risorse tanto per capirci) semplicemente non li vede. Lo spazio occupato dal file rimane “disponibile” finché un'altro file gli verrà salvato sopra e così via. Dal punto di vista della sicurezza dei nostri dati, con questi sistemi operativi, siamo prossimi allo zero. Per ottenere la completa cancellazione del file è necessario riscrivere gli stessi settori almeno otto volte con dati a caso
Ad un analisi accurata, ad esempio con uno dei programmi commerciali per Windows usati dalla P.G. che si chiama “Active Uneraser” si possono tranquillamente recuperare documenti cancellati. Anche se poi questi

documenti potrebbero NON essere validi dal punto di vista processuale (vedi gli aspetti legali trattati nel precedente capitolo), non è proprio una bella cosa.
Come possiamo prevenire questo? Io suggerisco di NON usare Windows, primo perché sistema operativo proprietario e di una delle più grosse multinazionali sul pianeta, secondo perché fa prodotti decisamente scadenti, insicuri e inaffidabili. Rimane purtroppo il sistema operativo più utilizzato per la sua "reperibilità". In assenza di altro, usate floppy o gli ZIP il più possibile e non salvate mai niente su Hard Disk. Logicamente poi fateli sparire. In alternativa è possibile utilizzare la miriade di programmi e programmini commerciali per cancellare definitivamente i documenti. Uno fra tutti è il "wipe info" della Symantec, programma della suite Norton Utilities. Non ho accertato l'effetiva funzionalità di questo software e quindi non ho prova materiale della sua efficacia.
Un hard disk non è altro che un disco "magnetico" dove le informazioni vengono "impresse" temporaneamente. In questo campo, non si butta via niente. non esiste un settore del disco che non venga scritto e riscritto più volte. Come tutte le cose "magnetiche" presenta delle controindicazioni. Pensiamo a quando riregistriamo una musicassetta. Anche se l'esempio potrebbe far rabbrividire i più, in questo caso calza benissimo. Posso aver registrato su una musicassetta, un disco di Nikka Costa 12 anni fa e quindi riregistrato sopra l'ultimo album ruggente di King Diamond, ma analizzato attentamente questo nastro porterà ancora in leggero sottofondo le note della precedente vergogna musicale. Le tracce quindi della nostra giovanile passione potrebbero, ahimè, venire a galla. Lo stesso vale per un hard disk; cercando bene, qualcosa si trova sempre. Nel caso di Windows è molto più facile che in altri sistemi operativi. Inoltre, volendo avere la possibilità di cancellare definitivamente i file che ci interessano, dovremo sempre appoggiarci a programmi proprietari con vari sbattimenti. Prendiamo invece ad esempio Linux e FreeBSD. Quando noi cancelliamo un file con il comando "rm", effettivamente il sistema operativo mette a zero il file (lo cancella), ma la traccia su disco rimane. Ad un analisi approfondita il file, o parte di esso, potrebbe ricomparire. Io suggerisco il comando "wipe" quando si vuole cancellare definitivamente un file (la sintassi è la stessa del comando "rm"). il comando wipe, cancella il file e sovrascrive i settori precedentemente occupati dal file otto volte con dati a caso. Il file è definitivamente scomparso e ogni traccia, eliminata. Lo stesso su MacOSX. MacOSX presenta due possibilità di cancellazione: il nomale "empty trash" (che usa il comando "rm"), oppure il "secure empty trash" (che usa il comando simile al "wipe", che si trova nel menù del Finder e non è disponibile semplicemente cliccando con il tasto destro o facendo ctrl+click sul cestino). I sistemi unix sono decisamente più sicuri sia per la gestione dei file, sia per un eventuale connessione in rete.
Per mettere i nostri computer in "sicurezza" è necessario, al momento della formattazione del disco fisso, ricorrere ad alcune "furberie o stratagemmi" per eliminare definitivamente il contenuto precedente. Formattando semplicemente si rende disponibile tutta la superficie del disco alla scrittura, ma siamo molto lontani dalla cancellazione del contenuto precedente. Di alternative ce ne sono assai poche: sistemi operativi basati su Unix. Nel caso di Linux (o di *BSD) esiste un comando molto comodo: shred. Shred letteralmente "sporca" il disco sovrascrivendo dati a caso per 25 volte (questo è il valore predefinito, ma è possibile cambiarlo usando la sintassi riportata in seguito). La quantità dei passaggi la definirete voi in base a quanti giorni volete aspettare prima che finisca il processo di "insozzamento" ("shred –help" o man shred in consolle per avere dettagliate informazioni). Questo processo annienta qualsiasi contenuto dell'hard-disk (o disco fisso) preparandolo così a una nuova installazione più "sicura" (indifferentmente dal sistema operativo che si intenderà utilizzare). Tanto per darvi un riferimento sul tempo utilizzato dal comando shred per il suo "sporco" lavoro. Per "shreddare" una cartuccia ZIP (100MB) con le opzioni predefinite (quindi 25 passaggi) il mio PC (AthlonXP 1700 + 256MB RAM) ci ha messo circa 50minuti (!!!). Questo vuol dire che per "insozzare" un disco da 30GB (30.000MB) ci potrebbe anche mettere un tempo pari ad una10ina di giorni.... (magari proprio 25 passaggi no, però almeno 4 sarebbero consigliati).
Affrontata quindi la parte sul filesystem e delle precauzioni durante il salvataggio dei propri dati, cerchiamo di capire altre cose.
Quali sono le nostre possibiltà di contrastare un eventuale "intrusione" nel nostro computer? Si possono, ad esempio, criptare alcune cartelle dove noi desideriamo tenere dati più sensibili di altri. Cos'è quindi la criptazione? In pratica a quel particolare insieme di cartelle e di dati che noi abbiamo intenzione di rendere accessibili solo a noi, viene "codificata" da un algoritmo (una formula matematica) conosciuto. Logicamente a questo algoritmo manca un parametro che è la nostra chiave. La chiave è un'altra password che permette all'algoritmo di risolvere l'equazione che ci permetterà di avere accesso alle nostre cartelle.
Generalmente la cirptazione di cartelle non viene vista come semplice desiderio di privacy ma come vera e propria prova di un crimine in corso, non per questo in una degli ultimi tentativi di legge "antiterrorismo" veniva inserita l'eventuale proibizione di ogni algoritmo crittografico (nello specifico pgp o gpg) a protezione di documenti. Di fatto, grazie a questa "entità" (il terrorismo) viene vietata la possibilità di proteggere i propri dati sensibili e personali.

Alcuni Comandi Utili

Comandi per "sporcare" i dischi, per la criptazione di dispositivi, per la creazione di copia conforme, per la mappatura di dischi con filsystem UFS

```
shred -n 1 -v /dev/hdxx
```

creazione di directory criptate con cryptofs (linux – devono essere presenti alcuni moduli nel kernel)

```
cryptsetup -y create cryptofs /dev/hdx
mkfs /dev/mapper/cryptofs
```

copia conforme byte a byte

dd if=/dev/hdx of=/tmp/disco.raw

md5sum per generare o controllare il conteggio MD5, utile per controllare l'esatta provenienza del disco e per verificare che non sia stato manipolato

mount -t ufs -o ufstype=openstep,ro /dev/hdcX /mnt/macosx