

I Crimini ad Alta Tecnologia e l'Arma dei Carabinieri

RIS di Roma – Sezione Telematica

Il Comandante Cap. tlm. Ing. Marco Mattiucci

www.marcomattiucci.it (sito web in continuo aggiornamento)

L'attività della Sezione Telematica del RIS di Roma è principalmente l'analisi di sistemi software ed hardware al fine di individuare indizi investigativi e/o elementi che possano condurre alla formazione delle prove nell'ambito delle indagini dei Reparti territoriali e speciali dell'Arma. La scienza emergente del digital forensics, cui tale Sezione basa studi ed attività, presenta peculiarità tecnico/legali e problematiche che devono essere poste all'attenzione degli specialisti come degli appartenenti al framework legale destinato a trattarne i risultati fuori e dentro il dibattimento.

SOMMARIO

1. Introduzione

- a. Cosa sono i crimini ad alta tecnologia ed il perché di questa strana definizione.**
- b. La Polizia Postale e delle Comunicazioni**
- c. La Guardia di Finanza – Nucleo Speciale Anticrimine Tecnologico**
- d. L'Arma dei Carabinieri**
 - *Struttura RaCIS – RIS RM – Sezione Telematica – post reato*
 - *Struttura ROS – Sezione Telematica – pre reato*
 - *La territoriale e le squadre telematica*
- e. La nascita della Sezione Telematica del RIS**
- f. Accertamenti tecnici, Consulenze tecniche e Perizie**

2. Elementi di principio

- a. Settori:**
 - *Forensic Computing*
 - *Network Forensics*
 - *Mobile Forensics*
 - *Software forensics*
 - *Embedded System Forensics*
- b. Dato ed informazione**
- c. Memoria volatile e memoria semi-permanente**
- d. Reperto fisico e reperto dati**
 - *Il problema dell'originale e la copia sulla scena del crimine*
- e. La copia e la ripetibilità dell'accertamento**

3. Forensic computing

a. Il sequestro, la problematica delle metodiche di repertamento fisico

b. Tipologie di copia = REPERTAMENTO DEI DATI

- *copia di basso livello – bitstream copy*
- *copia a livello di File system – cluster copy*
- *copia a livello di file – backup*

c. L'analisi delle copie:

- *ricerca per stringa*
- *file evidenti*
- *file cancellati*
- *cluster persi*
- *date ed orari: il problema dell'attendibilità*
- *dati nascosti – il cracking:*
 - . *steganografia*
 - . *crittografia*
 - . *compressione*
 - . *dati incoerenti*

4. Network forensics

a. Network investigation: interventi in ambienti di rete privati

a. L'Internet investigation:

- *intercettazione digitale*
- *tracciamento e localizzazione digitale*
- *siti esca*
- *nuovi reati non previsti dal codice*

b. Repertamento ed analisi su Internet

- *il problema della copia dei siti*
- *il problema dell'analisi dei siti*
- *la posta elettronica: autenticità dei contenuti e del mittente*
- *FTP: trasferimento file*
- *Chat rooms: comunicazione in tempo reale tramite messaggistica a contesti.*
- *tanti altri servizi magari realizzati alla bisogna...*

c. Azioni preventive e repressive su Internet: ipotesi sull'uso legittimo della “forza”

d. Information warfare: cenni alle attività militari e dei servizi su Internet

f. Il peer to peer, le VPN, il telnet, il VoIP ed il modem to modem

5. Mobile Forensics

a. Mobile investigation

- *intercettazione*
- *radiolocalizzazione*

b. Repertamento dei cellulari: isolamento e movimento dei sistemi

c. Analisi di SIM e Telefonini:

- *isolamento e riesumazione dei dati cancellati*

6. Software forensics

- a. *Software illegalmente acquisito, detenuto ed impiegato*
- b. *Strumenti di cracking*
- c. *Software dichiarati illeciti: i videogame ed i sistemi di crittazione...*
- d. *Un nuovo trend nei giochi elettronici illeciti: il remote-game.*

7. Embedded system forensics

a. Repertamento ed analisi di sistemi speciali:

- *inneschi di ordigni esplosivi*
- *palmtop*
- *sistemi di clonazione delle carte di credito e frodi on-line*
- *sistemi di videosorveglianza digitali*
- *sistemi GPS*

b. la nascita dell'Electronic Forensics

8. Le garanzie

a. La necessità di definizione delle tecniche di contrasto al crimine ad alta tecnologia

b. Gruppo di lavoro accademici in Italia

c. L'importanza della qualità totale del processo di produzione delle fonti di prova:

- *Certificazione del personale (selezione/aggiornamento/test)*
- *Certificazione degli strumenti (selezione/aggiornamento/comparazione)*
- *Molteplicità degli strumenti impiegati per una stessa indagine*
- *Certificazione e standardizzazione delle procedure (repertamento/analisi)*
- *Standardizzazione dei termini impiegati nelle relazioni tecniche finali*
- *Standardizzazione del reporting*

d. La Sezione Telematica del RIS di RM e la struttura di una relazione Tecnica

TRATTAZIONE SINTETICA

1. Introduzione

a. Cosa sono i crimini ad alta tecnologia ed il perché di questa strana definizione.

High Tech Crime

“the use of information and communications technology to commit or further a criminal act, against a person, property, organisation or a networked computer system” [Europol 2003], diverso dal più ristretto *cyber crime*, ossia, *“the criminal use of any computer network or system on the Internet; attacks or abuse against the systems and networks for criminal purposes; crimes and abuse from either existing criminals using new technology or new crimes that have developed with the growth of the Internet”* [Europol 2003].

Cos'hanno di diverso i crimini ad alta tecnologia dai crimini comuni? solo il fatto che coinvolgono elementi ad alta tecnologia in genere digitali? No! Il trend è che nei prossimi anni esisteranno solo crimini ad alta tecnologia perchè non ci sarà reato che non coinvolgerà almeno uno strumento digitale... il cellulare ne è un esempio evidente...

Il termine "Crimini ad alta tecnologia" (HTC), traduzione del più famoso High Tech Crime, proviene dall'omonimo gruppo di lavoro del G8 con il quale ebbi occasione di interagire in una splendida ed enorme conferenza a Londra nell'ottobre del 1999. A quei tempi la mia esperienza nel settore scientifico forense si limitava a qualche centinaio di casi affrontati con molto criterio ma effettivamente con limitatezza di veduta.

In quel frangente mi resi conto di quanto ampio fosse il settore di cui mi stavo andando ad occupare con sempre maggior vigore ed individuai quello che già da allora si configurava come un settore di punta della IT che in Italia sarebbe stato notato per bene almeno 6 anni dopo.

Forensics & Investigation: approcci, teorie e strumenti inclusi nel HTC

“...Strictly speaking, forensic science is the application of science to law and is ultimately defined by use in court... Investigation can benefit from the influence of forensic science”

“In 2001 the first annual Digital Forensic Research Workgroup (DFRWS www.dfrws.org) recognized the need for a revision in terminology and proposed – digital forensic science – to describe the field as whole. The terms forensic computer analysis and forensic computing have also become widely used. ”

[Digital Evidence and Computer Crime, 2° edition, 2004]

La scienza forense nasce come attività post-reato, ossia dopo il fatto, mentre l'indagine spesso si applica in maniera preventiva. In Italia diversi Reparti delle Forze di Polizia (FFPP) operano, nel settore del digital forensics, in maniera preventiva e/o forense.

b. La Polizia Postale e delle Comunicazioni

c. La Guardia di Finanza – Nucleo Speciale Anticrimine Tecnologico

d. L'Arma dei Carabinieri

- *Struttura RaCIS – RIS RM – Sezione Telematica – post reato*

In Italia, il RaCIS è organizzato su quattro Reparti investigazioni scientifiche (RIS) con sede a Roma, Parma, Messina e Cagliari. Ogni reparto ha competenza

specifica su una fetta di territorio (Parma per il Nord, Roma per il Centro-Sud, Messina per il Sud e Cagliari per la Sardegna). Ogni RIS è articolato in diverse sezioni che rispondono a branche specifiche della criminalistica (chimica forense, biologia forense, balistica, dattiloscopia e fotografia giudiziaria, fonica e grafica ed informatica). In stretto contatto con i quattro Reparti ci sono 29 Sezioni investigazioni scientifiche (SIS) che costituiscono, sul piano interprovinciale, il braccio tecnologico specializzato nelle attività di sopralluogo e repertamento sulla scena del crimine oltre che nelle analisi delle sostanze stupefacenti.

Il RaCIS è membro fondatore dell'ENFSI (European network of forensic science institutes), l'organismo che riunisce gli istituti forensi di 18 Paesi europei. Inoltre è membro dell'ASCLD (American society of crime laboratory), l'associazione internazionale che collega i direttori delle principali strutture forensi mondiali e che ha sede negli Stati Uniti. Per finire il RaCIS è collegato con le maggiori università italiane per ricerche e progetti ed il suo personale ufficiale svolge un incredibile numero di conferenze e lezioni presso corsi di master e di laurea.

- *Struttura ROS – Sezione Telematica – pre reato*

- *La territoriale e le squadre telematica*

e. La nascita della Sezione Telematica del RIS

f. Accertamenti tecnici, Consulenze tecniche e Perizie

2. Elementi di principio

a. Settori:

- *Forensic Computing*

...contrasto ai crimini di qualsiasi natura attraverso indagini che si svolgono sulle memorie di massa (hard disk, floppy disk, ecc.) di computer.

Ricordo ancora quando, in una delle prime indagini informatiche che affrontavo, mi fu detto: "ma che problema hai? attiva quel PC e cerca quello che ti serve sull'hard disk..." Inutile dire che non feci quell'errore idiota che sfortunatamente ancora in molti oggi fanno ma piuttosto mi procurai le mie prime conoscenze tecniche di Forensic Computing e realizzai un software ed una procedura per il repertamento dei dati.

- *Network Forensics*

...e quando l'evidenza di un crimine è 'distribuito' su una rete di computer?!

Una delle più grosse superficialità di un tecnico informatico forense è pensare di poter esaurire l'indagine tecnica sui dati di una rete di computer analizzando le singole macchine componenti. E' davvero il caso di dire che in questi frangenti i

dati della rete sono "maggiori" di quelli dovuti alla somma dei dati nei singoli nodi componenti.

- *Mobile Forensics*

... il cellulare è attualmente il dispositivo elettronico più diffuso a livello personale in Italia!

Non vi è omicidio o suicidio in cui il cellulare non rivesta un ruolo determinante per le indagini e sfortunatamente il cellulare è il primo sistema con il quale l'investigatore arrivato sulla scena del crimine tende ad avere interazione diretta. Il terminale UMTS che presto soppianderà tutti gli altri protocolli è un computer a tutti gli effetti, ecco perché si vanno definendo procedure molto simili di principio a quelle del forensic computing con strumentazioni però molto differenti.

- *Software forensics*

...qualcuno mi disse, il software e le informazioni dovrebbero essere di tutti ed io risposi: bello e valido di principio, peccato che sia illegale!

La proliferazione di software illegale è una delle più grandi piaghe italiane dal punto di vista dell'informatica criminale. Siamo in assoluto la nazione con il più alto tasso di clonazione di software in Europa. Nello stesso modo amiamo il gioco d'azzardo software che ha aperto nuove frontiere a questo settore tra cui il gioco delocalizzato, on-line, su Internet.

- *Embedded System Forensics*

...talvolta non si sa che fare dal punto di vista tecnico e questo capita proprio quando il sistema da analizzare è artigianale!

Sistemi elettronici artigianali realizzati a scopo illegale sono frequentissimi. Uno dei target maggiormente remunerativi e quindi trattati è ovviamente quello della clonazione delle carte di credito e dei bancomat ma non mancano gli inneschi elettronici, comandi a distanza robotizzati, ecc.

b. Dato ed informazione

L'art. 1 del DPR 513/97 fornisce una definizione di base, che poi verrà ripresa fino ad oggi nelle diverse leggi e regolamenti inerenti l'informatica e le telecomunicazioni, secondo la quale si intende "per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Il concetto legale di base dal quale si parte è quindi quello del documento; in questo lavoro si propone un passo indietro estremamente importante dal punto di vista forense: prima di definire il documento informatico è necessario stabilire cos'è un dato digitale e cosa significhi trattarlo. È inevitabile quindi affrontare la differenza tra dato ed informazione nell'ambito informatico.

Fermo restando che un sistema informatico si limita sempre a rappresentare la realtà mediante simboli memorizzabili in una memoria digitale e che in particolare quei simboli si riassumono nei due opposti binari 0 ed 1, la diversità tra dato ed informazione si esplica ovviamente attraverso la ricchezza dei contenuti e la loro interpretazione. La minima quantità di informazione che un sistema digitale è in grado di impiegare è un bit ossia una variabile matematica che può assumere i valori 0 ed 1. Una sequenza di bit che non sia soggetta a nessuna forma interpretativa è considerabile dato digitale (elementare). Non appena una regola interpretativa agisse sulla stessa sequenza (es. un protocollo di rappresentazione dei caratteri come ASCII o UNICODE) si “costruirebbe” una informazione più complessa.

Dal punto di vista legale la differenziazione fatta è fondamentale e la sua inosservanza conduce spesso ad errori grossolani. Si consideri, ad esempio, una pagina web su Internet: attribuire alla stampa della pagina risultanze dibattimentali significa svolgere la propria disamina su una interpretazione dei dati (informazione complessa) e non sui dati costituiti dalla sequenza di bit che formano il codice HTML (o ancora più evoluto) che realizza effettivamente la visualizzazione. Se il codice della pagina realizzasse funzioni articolate di connessione e pubblicazioni di informazioni innestate non sarebbe possibile determinarlo sulla scorta della citata stampa.

c. Memoria volatile e memoria semi-permanente

Il problema di cosa analizzare

Ad oggi la maggior enfasi nelle indagini informatiche è data all’analisi delle memorie di massa ed io stesso non avvalorerei minimamente l’analisi, ad esempio, del contenuto di una RAM di un PC a fini forensi. Non vi è a mio avviso la necessaria garanzia né per l’investigatore e tanto meno per l’indagato perché i mutamenti della RAM possono essere veloci (es. mancanza di corrente) e non lasciare la minima traccia.

Mentre per il repertamento ed analisi di un sistema stand-alone tale rigido approccio può risultare valido è assolutamente proibitivo per sistemi di rete e per palmtop o sistemi elettronici speciali che talvolta hanno esclusivamente la RAM (magari alimentata perennemente). Da questo si sta affacciando oggi il problema della “*live analysis*” ossia dell’analisi dei sistemi durante il loro funzionamento che implica l’analisi sia dello stato delle memorie di massa, che della memoria volatile che delle loro evoluzioni temporali...

d. Reperto fisico e reperto dati

Il problema dell’originale e la copia sulla scena del crimine

“...la speciale natura delle prove digitali richiede considerazioni aggiuntive ed alcuni cambiamenti rispetto le prove reali” ed in particolare il fatto che le informazioni memorizzate su un sistema digitale sono per loro natura indipendenti da quest’ultimo. In pratica, senza la necessaria e forzata caratterizzazione esterna (fisica), le prove digitali non sono associabili ad un apparato o ad un istante di tempo. Questo determina il fatto fondamentale che la differenziazione tra copia ed originale, quando si opera su memorie digitali ed in mancanza di specifiche direttive dell’operatore è impossibile. Ecco quindi un principio di indistinguibilità che ha condotto la preservazione dei dati utili (anche chiamata repertamento dei dati) ad essere un’attività equivalente alla copia degli stessi

su supporti di memoria particolarmente affidabili (ottici e/o nastri magnetici con “blindatura”).

La caratterizzazione delle copie avviene includendo in esse informazioni ausiliarie come: data ed ora in cui avviene la copia, ID dell’operatore, commenti, ecc.. Tali elementi vengono sottoposti ad un processo di hashing assieme ai dati utili ed i valori calcolati rimangono definitivamente storicizzati in supporti ausiliari a quelli di destinazione della copia. A questo proposito, si impiegano delle funzioni di hash standard come DIVA (proprietario della ditta Computer forensics ltd) o MD5 (standard open largamente impiegato da diversi prodotti di punta come EnCase, Ilook, ecc.). I valori di hash calcolati durante la copia sono utili per garantire due fatti essenziali:

- Data la possibilità di calcolare l’hash sia sui dati di partenza che su quelli copiati e fermo restando le proprietà di univocità degli algoritmi che implementano la funzione di hash, è possibile verificare l’aderenza “assoluta” della copia ai dati di partenza durante il processo di clonazione, impiegando tale metodo come un pesante (computazionalmente) e rigoroso sistema di controllo errore.
- Successivamente alla copia, la disponibilità del valore(i) di hash, consente di stabilire se la copia è ancora valida e se sono intervenute delle alterazioni (volontarie e/o involontarie).

e. La copia e la ripetibilità dell’accertamento

Considerando due possibilità molto comuni:

- (1) PC su una scena del crimine;
- (2) intercettazione di dati su un canale di trasmissione digitale;

si può agire in entrambi i casi copiando i dati di interesse su di un supporto di memoria di massa affidabile. Trattandosi di copia e quindi in linea di principio di azione di lettura sul sistema analizzato, non c’è pericolo di alterazione o inquinamento. Dal punto di vista dell’inquadramento del sequestro e del relativo corpo di reato vi è qualche riflessione da fare. Nel caso (1) il corpo di reato è il PC o la copia integrale dei dati in esso contenuti? o che è la stessa cosa qual’è l’originale dei dati, quelli sul PC o quelli copiati sul supporto affidabile? ed ancora, in relazione al (2), l’originale esiste solo nella copia in quanto il flusso dati sul canale è temporaneo.

Le questioni evidenziate non sono di così semplice trattazione. La (1) si può risolvere ferreamente depositando sia il PC che il supporto che contiene la copia come corpo di reato evidenziando la precisa azione di copia sul verbale. In questo modo, nell’ipotesi di non riaccedere ulteriormente al PC (inutile dato che si ha la copia integrale) e che la copia fatta sia certificata in maniera forense (impiego di un sistema di copia forense, presenza di personale specializzato ed attuazione di procedure riconosciute internazionalmente) e sigillata (presenza di un codice di validazione es. HASH MD5) si può (fittiziamente) considerare che l’originale sia unico e coincidente nel supporto contenente la copia. Sfortunatamente nel momento in cui PC e copia dei dati si dividono (es. restituzione del reperto al possessore) non vi è più modo di dimostrare che la copia è perfettamente conforme all’originale che è il PC. In un modo ancora più subdolo e

sfortunato se (situazione non rara) i contenuti del PC andassero casualmente ad alterarsi o a perdersi parzialmente o totalmente la copia resterebbe l'unico originale...!!!

Su questo fatto che la copia forense dei dati è in realtà il vero originale, caso automaticamente verificato in (2) e cui spesso ci si riconduce in (1), lascio il lettore alle dovute riflessioni. Un'ottima via d'uscita potrebbe essere il considerare l'atto della copia come un atto "irripetibile" (art. 359, 360 CPP) [21,22] e quindi il risultato, cioè la copia stessa su un ben determinato supporto, come un nuovo corpo di reato distinto da quello da cui provengono i dati e ad esso legato tramite un apposito verbale di attività tecnica firmato da ognuna delle parti processuali ed eventualmente dai rispettivi periti.

3. Forensic computing

a. Il sequestro, la problematica delle metodiche di repertamento fisico

Attivare un PC senza i previsti strumenti hardware/software di natura forense significa svolgere un'attività tecnica che è di per sua natura altera il contenuto dati della macchina in maniera irreversibile.

Interagire sul PC rilevato come attivo sulla scena del crimine senza i necessari presupposti di natura informatico-forense (personale specializzato) significa con buona certezza svolgere un'attività tecnica che è di per sua natura può alterare il contenuto dati della macchina in maniera irreversibile.

Ho avuto occasione di incontrare obiezioni a questi ferrei punti di vista che corrispondono allo stato dell'arte nel settore a livello internazionale. Ad esempio qualcuno ha osservato che riattivando il PC si vanno a modificare dei dati ma che questi sono generalmente ininfluenti rispetto allo specifico, ristretto contesto delle indagini. Questo è vero solo ad un approccio superficiale del problema! Vediamo perché...

Al momento dell'attivazione è vero che il sistema operativo (es. windows) della macchina scrive dei dati sulla memoria di massa che possono risultare marginali in se stessi ma la scrittura di tali dati va indirettamente ad incidere su quelli cancellati in quanto potenzialmente (fatto estremamente verosimile) le aree marcate come cancellate tendono in breve ad essere sovrascritte dai nuovi dati. In breve riattivando senza i necessari criteri il PC si limita la possibilità di recupero dei file cancellati, attività questa di fondamentale importanza nelle indagini.

Lo stesso problema può essere evidenziato nel caso in cui ci si limita ad interagire sul PC già attivo. Più si opera su di esso minore diviene la probabilità di ritrovare file o in generale dati cancellati di recente.

b. Tipologie di copia = REPERTAMENTO DEI DATI

- copia di basso livello – bitstream copy

in cui il contenuto dell'unità fisica viene letto sequenzialmente caricando la minima quantità di memoria di volta in volta indirizzabile per poi registrarla nella stessa sequenza su di un comune file binario (immagine fisica dell'unità);

- *copia a livello di File system – cluster copy*

in cui il contenuto di una partizione logica (strutturata a seguito di una formattazione correlata ad un preciso file system) viene letto sequenzialmente caricando la minima quantità di memoria che il file system consente di indirizzare di volta in volta per poi registrarla nella stessa sequenza su di un comune file binario (immagine di basso livello del file system);

- *copia a livello di file – backup*

in cui parte o tutto il contenuto di alto livello di una partizione logica (strutturata a seguito di una formattazione correlata ad un preciso file system), ivi intendendo i contenuti di file e directory evidenti (non cancellati), viene sottoposto a backup su di un file (file di backup).

c. L'analisi delle copie:

- *ricerca per stringa*

I tool forensi per la ricerca stringhe su immagini di memorie di massa sono lo strumento più assodato e frequente per l'individuazione di elementi di interesse. Gli algoritmi di ricerca sono divenuti negli ultimi anni di una efficienza notevole e possono agire su diverse codifiche (ASCII, UNICODE, ecc.).

"The most common technique is to encode the characters using ASCII or Unicode... ASCII is nice and simple if you use American English, but it's quite limited for the rest of the world because their native symbols cannot be represented. Unicode helps solve this problem by using more the one byte to store the numerical version of a symbol (www.unicode.org)." [File System Forensic Analysis, Wesley 2005]

- *file evidenti*

Vedere ed interpretare correttamente i contenuti della maggioranza dei file normalmente presenti su un PC è un target fondamentale del tecnico forense. I software "viewer" permettono di aprire in "sola lettura" centinaia di tipologie di file senza la necessità di avere installato il software "creator".

- *file cancellati*

"...it's necessary to extract data that have been deleted, hidden, camouflaged or that are otherwise unavailable for viewing using the native operative system and/or resident file system..." [Digital Evidence & Computer Crime, 2° edition, Casey 2004]

Nei fortunati casi in cui è possibile recuperare per intero dei file cancellati, quest'ultima è un'attività di estremo interesse perché è verosimile sia l'attendibilità dei risultati che la correlazione temporale tra la cancellazione ed il fatto reato in studio.

- *Orphan cluster & Slack space*

"...in short, once a cluster contains data, the entire cluster is reserved... the extra sectors in a cluster are called file slack space." [Digital Evidence & Computer Crime, 2° edition, Casey 2004]

"When a file is deleted, its entry in the file system is updated to indicate it's deleted status and the clusters that were previously allocated to storing are unallocated and can be reused to store a new file. However the data are left on the disk and it's often possible to retrieve a file immediately after it has been deleted. The data will remain on the disk until a new file overwrites them...." [Digital Evidence & Computer Crime, 2° edition, Casey 2004]

Quando l'analisi semplice dei file cancellati non è sufficiente e considerando file system come FAT e NTFS, si deve passare a quella dei cluster persi (deallocati e non puntati da nessun indice di direttorio) e/o degli slack che possono contenere dati dello stesso file appena cancellati o dati di un precedente file cancellato e soprascritto.

- *date ed orari: il problema dell'attendibilità*

Time stamps is a recorded representation of the computer clock related to a specific action. Time stamps are very important evidence items that may be erroneous due to:

- *Midadjusted clock or clock-drift*
- *Purposeful maladjusted clock*
- *Non-synchronization of different clock sources*
- *Malicious or non-malicious tampering of time stamps*

[ENFSI-FITWG, Netherlands Sept 2005]

Le date e gli orari (creazione, modifica, accesso, cancellazione, ecc.) sono elementi di primaria importanza nel settore forense e sfortunatamente hanno un'attendibilità molto limitata, basata essenzialmente sulla loro coerenza in una moltitudine di file presenti sulla stessa partizione.

- *dati nascosti – il cracking:*

In alcuni casi i dati sono nascosti volontariamente dall'indagato e quindi si devono individuare e poi impiegare delle tecniche di cracking per abbatterne le protezioni.

. *steganografia*

“La steganografia è l'arte di nascondere informazioni nelle informazioni così da non destare sospetti nonché il processo di introdurre informazioni in un canale nascosto così da celare le informazioni stesse. È uno strumento utile per la protezione delle informazioni personali, e le organizzazioni stanno investendo ingenti risorse nell'analisi delle tecniche steganografiche al fine di proteggere l'integrità dei propri dati.” [Prof. Maioli, Child Pornography Conference, Rome May 2005]

Le informazioni vengono nascoste codificandole generalmente nel “rumore” dei file multimediali (video e/o suoni) in quanto tale scelta complica terribilmente il processo di attacco. Talvolta sono steganografate informazioni già crittate e/o compresse in quanto tali procedure tendono ad aumentare l'entropia informativa e quindi rendere il flusso da nascondere molto simile al rumore nel quale lo si nasconde (spesso ipotizzato come bianco).

. *crittografia*

“Encryption is a process by which a readable digital object (plain text) is converted into an unreadable digital object (cipher text) using a mathematical function...” [Digital Evidence & Computer Crime, 2° edition, Casey 2004]

“Encryption is the primary means for providing confidentiality services for information sent over the Internet. Encryption can be used to protect any electronic traffic, such as mail messages or the contents of a file being downloaded. Encryption can also protect information in storage, such as in databases or stored on computer systems where physical security is difficult or impossible” [B. Guttman, R. Bagwill, IT Lab Computer Security Division of NIST, 1997]

La crittografia, nelle sue forme simmetriche ed asimmetriche, costituisce ad oggi una delle maggiori problematiche tecnico investigative nel recupero delle informazioni digitali ed allo stesso tempo rimane una delle garanzie

essenziali allo svolgimento di azioni “sicure” su Internet (es. le transazioni economiche).

. *compressione*

*“When data is compressed, the goal is to reduce redundancy, leaving only the informational content”
[D. A. Lelewer and D. S. Hirschberg, University of California, Irvine]*

La compressione come processo di codificazione delle informazioni è strettamente legato alla crittazione anche se ovviamente il suo obiettivo primario non è rendere illeggibile le informazioni quanto limitarne lo spazio occupato in memoria. In particolare la compressione senza perdita con password è in molti casi una buona forma di crittazione ed in ogni caso le informazioni compresse non risentono della ricerca tramite stringa.

. *dati incoerenti*

“Data mining: the process of extracting previously unknown, valid, and actionable information from large databases and then using the information to make crucial decisions....” [Discovering Data Mining, IBM Prentice Hall 1998]

A volte ci si chiede quale necessità ci sia di crittare i dati quando un PC medio contiene decine di migliaia di file ed analizzarli tutti uno per uno è impossibile! L’information filtering a scopo forense è un data mining a tutti gli effetti ed esistono comunque diversi metodi per rendere incoerenti i dati di un file in modo che si confonda tra migliaia di altri e non venga mai notato.

4. Network forensics

“The network security process involves:

- *Security: the process of maintaining an acceptable level of perceived risk...*
- *Assessment: consists in enumerating resources, assigning value to them, identifying their vulnerabilities and devising policies...*
- *Prevention: is the application of countermeasures to reduce the likelihood of compromise...*
- *Detection: is the process of identifying intrusions...*
- *Response: is the process of validating the findings of the detection process and taking steps to remediate intrusions.*

Intrusions are policy violations or computer security incidents.

An incident is any unlawful, unauthorized, or unacceptable action that involves a computer system or network.

Incident response is the process of containing, investigating and remediating an intrusion.

Network forensics is the art of collecting, protecting, analysing and presenting network traffic to support remediation or prosecution.”

[Extrusion Detection, Wesley 2006]

a. Network investigation: interventi in ambienti di rete privati

Il termine "Network Forensics" (NF) si riferisce all'analisi di sistemi di rete, ivi inclusa la Rete delle reti ossia Internet, al fine di determinare, congelare e presentare in dibattimento o agli investigatori elementi inerenti un determinato caso investigativo. Da questo punto di vista è bene sottolineare una differenza notevole tra il NF e la Network Security (NS). La prima opera in ambito legale e quindi si occupa di violazioni delle leggi mentre la seconda si può trovare ad operare in ambiti non necessariamente penali o civili come quelli in cui si viola un regolamento interno di una struttura. Dal punto di

vista delle autorizzazioni necessarie a svolgere determinare attività tecniche si crea un divario enorme. Questo non toglie che diversi strumenti hardware/software impiegati nella sicurezza informatica trovano vasta applicazione in ambito di NF. Un'altra differenza di natura questa volta più tecnica è che il NF interviene sempre dopo il fatto mentre la NS può agire prima e nel mentre. Ad esempio lo studio, l'installazione e l'impostazione dei parametri di un Intrusion Detection System (IDS) è NS mentre l'analisi di una intrusione che ha causato un danneggiamento al sistema informatico attraverso i LOG dello stesso IDS rappresenta attività di NF.

a. L'Internet investigation:

- intercettazione digitale

Lo scopo dell'intercettazione è prelevare in tempo reale dei dati durante il loro fluire su di un canale di trasmissione e ricostruirne i contenuti in modo da renderli fruibili agli investigatori, all'AG, ecc.. Mentre queste fasi erano pressoché banali per le intercettazioni telefoniche su linea analogica divengono complesse e difficili da inquadrare nel digitale.

Esistono diversi livelli di intercettazione digitale proprio perché la Rete delle reti opera in maniera stratificata, ossia impiega layer che sono il più possibile impermeabili tra loro per ragioni di convenienza economica e tecnica.

Attraversando i diversi livelli si può avere quindi: (1) intercettazione su cavo del segnale di basso livello e ricostruzione completa dei protocolli; (2) intercettazione presso il Provider di servizi Internet ossia l'ente privato o pubblico che permette la particolare connessione (spesso gli Internet Service Provider = ISP); (3) intercettazione sulle dorsali (backbone) di comunicazione con separazione e filtraggio dei dati.

Esistono poi diversi servizi che si possono intercettare e la loro intercettazione può corrispondere ad azioni legali di natura differente. L'intercettazione delle email, che avviene ricevendo in un'apposita casella clone tutto quello che riceve o invia un soggetto, riguarda la corrispondenza o no? Si possono poi intercettare i movimenti dati su un sito web (uploading & downloading), le comunicazioni tramite chat, in linea di principio il VoIP, ecc.

- tracciamento e localizzazione digitale

Il tracciamento riguarda invece l'inseguire un dato su Internet cercando di ricollegarlo ad un ente fisico o legale. Si tracciano le email alla ricerca del mittente (che non necessariamente è quello segnalato sul campo mittente della posta elettronica). Si tracciano i siti web alla ricerca del server su Internet che li ospita e di colui che li aggiorna, mantiene o crea, ecc..

- siti esca

Attività tipicamente delegata alla Polizia delle comunicazioni in cui si realizzano dietro autorizzazione della AG particolari siti di contenuto generalmente illegale al fine di entrare nelle maglie di un'organizzazione criminale (azione sotto copertura in ambito virtuale).

- nuovi reati non previsti dal codice

Bisogna considerare che Internet non è semplicemente un nuovo strumento informatico al pari di un PC o di un cellulare con il quale svolgere funzioni che comunque avremmo svolto nella realtà con altri mezzi differenti. La Rete delle reti determina una nuova realtà e soprattutto delle possibilità di interazione tra le persone neanche concepibili prima da cui si presentano talvolta delle fattispecie di reato neanche preventivabili.

b. Repertamento ed analisi su Internet

...il crimine sulla più grande delle reti: la Rete delle reti, Internet!

Una volta si pensava che la propria rete aziendale o privata potesse essere resa sicura semplicemente chiudendola o impiegando strumenti proprietari. Da questo punto di vista le indagini di eventuali crimini connessi a tali reti si risolvevano in un'attività circoscritta e limitata. Oggi l'apertura verso Internet è la chiave principale del business (o del tempo libero) sia personale che aziendale da cui le indagini si sono dovute aprire su un panorama immenso, spesso di natura mondiale...

- il problema della copia dei siti

“...some of these tools (web-copier) will not copy subpages of a web site if links to these subpages are encoded in a scripting language that the tool does not understand...” [Digital Evidence & Computer Crime, 2° edition, Casey 2004]

Si torna di nuovo al problema del repertamento dei dati. Un sito web è un insieme strutturato di dati ma il problema è che sempre più spesso tale strutturazione non si può circoscrivere facilmente. In pratica, ad oggi, bisogna ammettere che non esiste una metodologia sicura e completa per repertare qualsiasi sito web a meno che questi non sia talmente semplice da avere scarsi legami con il suo esterno e non fornisca variegati e complessi servizi aggiuntivi.

Il web non è solo innestato dal punto di vista hardware dei collegamenti ma soprattutto dei contenuti. Un sito che non ha collegamenti con il suo esterno è praticamente un sito fuori mercato da cui estremamente raro. Il sito è una pubblicazione per cui nasce con l'intenzione di comunicare qualcosa a tanti da cui la ricchezza dei suoi contenuti e delle sue interazioni con altri siti è fortemente desiderata.

- il problema dell'analisi dei siti

Fermo restando che la copia di un sito è difficile se non in alcuni casi impossibile da ottenere in maniera completa rimane il grande problema dell'analisi dei suoi dati. La grande interazione tra i dati del sito e quelli su Internet al suo esterno determina un fatto importantissimo, l'analisi dipende dal momento in cui viene svolta dato che Internet è tempo-variante con un livello di dinamicità enorme.

L'unica possibilità, vera solo da un punto di vista teorico-tecnico potrebbe essere quella di avere una “immagine congelata di Internet” nell'attimo in cui siamo interessati all'analisi o almeno avere una “immagine congelata di Internet

limitatamente a quello che possiamo dimostrare essere il campo di azione del sito sottoposto a sequestro”.

- la posta elettronica: autenticità dei contenuti e del mittente

L’email è sicuramente uno dei servizi Internet più impiegati in assoluto. Bisogna ricordare che di principio la posta elettronica è un servizio aperto, ossia non prevede nativamente particolari accorgimenti di protezione dei contenuti né dalla loro visione e tantomeno dalla loro alterazione. Neanche prevede metodi per garantire l’identità del mittente e/o dei dati quali l’orario, la data, la ricezione, ecc.. Si rifletta sul fatto che il messaggio email, dal punto di vista del server che lo ricetrasmette su Internet è una “cartolina” mentre sul computer del mittente e del destinatario si può ben considerare come corrispondenza chiusa!

- FTP: trasferimento file

Il classico servizio impiegato per lo scambio di file. Tipica la sua importanza in relazione allo scaricamento o caricamento dati da/verso siti web. È ovviamente un normale target dell’intercettazione digitale.

- Chat rooms: comunicazione in tempo reale tramite messaggistica a contesti.

- tanto altri servizi magari realizzati alla bisogna...

c. Azioni preventive e repressive su Internet: ipotesi sull’uso legittimo della “forza”

Le Forze di Polizia impiegano da tempo le armi al fine legittimo secondo quanto previsto dalle vigenti leggi. Qualcuno ipotizza quindi la realizzazione di particolari strumenti, molto simili a quelli impiegati dai pirati informatici, per colpire determinati servizi su Internet che sono palesemente illegali.

Se ad esempio si determinasse un sito web atto allo scambio ed al coordinamento nella produzione di materiale pedopornografico lo si potrebbe “affondare” andando a “colpire” il gestore di servizi Internet che lo ospita ma si lasciano alle ovvie riflessioni del lettore le possibili difficoltà nel gestire i limiti ed influenze di un tale approccio.

d. Information warfare: cenni alle attività militari e dei servizi su Internet

“The growing reliance on computer networks makes the networks themselves likely sites for attack. What is more, civilian and military networks are becoming increasingly intertwined and so the US military’s focus have shifted from protecting every network to securing mission critical systems. Current efforts include software agent based systems (for real time detection and recovery from cyber attacks) and network level early warning systems (for monitoring suspicious on-line activity)...

...the prospect of cyberwarfare or information warfare is a deadly serious matter...”

[Computer Forensics, Charles River 2002]

f. Il peer to peer, le VPN, il telnet, il VoIP ed il modem to modem

Il peer to peer (P2P) è salito alla ribalta ultimamente per lo scambio (sharing) illegale di musica, software e per le comunicazioni sicure tra soggetti criminali. Una rete P2P si può considerare come una serie di “legami” su Internet che permettono di identificare una sorta di comunità virtuale costruita essenzialmente sulla necessità di scambiare file.

Tale sistema di connessione tende a garantire downloading (un host - nodo - preleva il file dalla rete) ed uploading (un host deposita il file nella rete) di file in maniera tale che si determini una condivisione e diffusione dei dati. Uno dei sistemi antesignani per il P2P attuale fu ovviamente Napster. Sistemi oggi famosi, anche per ragioni investigative, sono KaZaA e Gnutella i quali si basano sul protocollo HTTP (Hypertext Transfer Protocol - uno dei principali protocolli alla base delle trasmissioni delle informazioni nei comuni siti web), estremamente diffuso e disponibile.

Una delle principali necessità investigative nel settore P2P è ovviamente il tracciamento delle operazioni di downloading e uploading. Sfortunatamente, molti dei sistemi P2P attualmente operativi sono nativamente limitati dal punto di vista delle informazioni utili che potrebbero fornire all'investigatore che cerca di determinare provenienza e destinazione dei file scambiati.

Il telnet è un servizio molto particolare che consente di impiegare macchine remote su Internet come se fossero realmente a propria disposizione sul momento e posto in cui ci si trova. Prettamente impiegato da tecnici specializzati ed ovviamente dagli hacker.

Il VoIP (Voice Over Internet Protocol) è un servizio che si è scoperto commercialmente negli ultimi anni ossia la possibilità di fare telefonate o video-telefonate (non è molto diverso dato che tutto viene comunque digitalizzato) su Internet. Può impiegare nativamente la crittazione e presenta grandi problemi nella procedura di intercettazione.

Le VPN (reti private virtuali) sono sistemi hardware/software di connessione tra nodi su Internet che, impiegando crittazione spinta permettono di realizzare sulla Rete delle reti una sotto rete che abbia alte caratteristiche di sicurezza, protezione ed impermeabilità alle intercettazioni.

Modem to modem, sistema oramai obsoleto che consente di collegare più computer remoti bypassando Internet ed impiegando solo la linea telefonica analogica. Talvolta impiegato per il controllo a distanza di meccanismi computerizzati è di semplice implementazione e presenta l'unico punto debole del numero telefonico fisso necessario al collegamento.

5. Mobile Forensics

Grazie ad una tecnologia tipica del GSM, GPRS, UMTS, non è il radiotelefono a contenere i dati dell'abbonato, bensì una smartcard (“carta intelligente”) denominata SIM-Card (Subscriber Identity Module), da inserire nell'apparecchio che si desidera utilizzare.

L'abbonamento fa quindi riferimento alla carta e non al radiotelefono. La SIM-Card, estraibile dal terminale radiomobile, contiene un circuito integrato dotato di memorie volatili e non volatili, e si presenta strutturalmente in due possibili soluzioni opportunamente standardizzate:

(1) IC-Card (formato Card) avente le dimensioni di una carta di credito e (2) PLUG-IN di dimensioni particolarmente ridotte (2.5 x 1.5 cm).

I dati permanenti che caratterizzano l'utente sono registrati dal gestore radiomobile in aree di memoria "read-only" della SIM protette in modo da non essere accessibili ai normali utenti. Tali dati riguardano l'identità "IMSI" (International Mobile Subscriber Identity) dell'abbonato radiomobile, la chiave di autenticazione del cliente "KI" (Key Identity), gli algoritmi di calcolo utilizzati per quest'ultima attività ed anche per la cifratura della conversazione. All'utente, come noto, rimangono accessibili i campi per l'inserimento dei codici PIN e PUK.

a. Mobile investigation

- intercettazione

Non solo voce, si devono trattare sempre più spesso le immagini (videochiamate), gli SMS, le email, ecc. la migrazione del sistema cellulare verso una rete Internet-like è inesorabile e tutt'altro che lenta.

- radiolocalizzazione

La posizione della cella che connette un cellulare con la sua SIM alla rete di telecomunicazioni del provider è individuale a carico di quest'ultimo. In un'area cittadina questo equivale ad individuare spostamenti con approssimazioni di alcune centinaia di metri mentre in un'area extraurbana ci si può portare anche ad arrotondamenti di km.

b. Repertamento dei cellulari: isolamento e movimento dei sistemi

Un telefono cellulare attivo presenta diversi elementi problematici nel suo repertamento e successiva analisi. Innanzitutto la movimentazione di un tale dispositivo collegato alla rete di telecomunicazione vuole dire quasi con certezza alterarne il contenuto al momento del cambio di cella. In secondo luogo il dispositivo attivo può continuare a ricevere chiamate e messaggi che possono determinare ulteriori alterazioni (a prescindere dal fatto che investigativamente tali ricezioni possano essere utili o meno. A causa di tali fattori il primo elemento del sequestro di un cellulare è l'isolamento elettromagnetico o se questo non è possibile lo spegnimento.

c. Analisi di SIM e Telefonini:

- isolamento e riesumazione dei dati cancellati

Il procedimento di repertamento ed analisi dei dati interni ad un cellulare segue parallelamente quello dei PC. Sono di recente realizzazione infatti dei sistemi che consentono di operare separatamente su hardware radiomobile e su SIM. Spento il cellulare si estrae la SIM e se ne inserisce una forense che non permette nessuna di collegamento alla cella e previene ogni azione di scrittura in memoria. A questo punto il terminale radiomobile viene opportunamente collegato ad un PC ed inizia lo scaricamento dei dati (messaggi, video, registrazioni sonore, ecc.).

Nel frattempo la SIM viene clonata integralmente su SIM scrivibili una sola volta (garanzia e traccia) e queste potranno rispettivamente essere: (1) depositata

all'ufficio corpi di reato quale reperto, (2) impiegata per l'analisi dei dati, (3) consegnata alle parti processuali per consentire accertamenti, riscontri, ecc..

Tutti i processi di clonazione devono ovviamente essere soggetti a validazione mediante codice di controllo (MD5).

Questa metodologia permette di avere in copia tutto quello che è reperibile dal cellulare sia nella SIM che nel terminale radiomobile ivi comprese le aree di memorie dichiarate cancellate ma ancora leggibile (rubrica, SMS, MMS, ecc.), ossia non sovrascritte parzialmente o totalmente.

6. Software forensics

a. Software illegalmente acquisito, detenuto ed impiegato

b. Strumenti di cracking

Si tratta di studiare e realizzare hardware/software per il recupero di password di archivi o aree protette e/o per abbatterne le relative protezioni.

c. Software dichiarati illeciti: i videogame ed i sistemi di crittazione...

d. Un nuovo trend nei giochi elettronici illeciti: il remote-game.

Il gambling online, ad oggi, rappresenta l'evoluzione tecnologica dei giochi elettronici, quali ad esempio le slot machines o i videopoker, ai quali, unitamente all'aspetto ludico e all'intrattenimento, si affianca la possibilità di veder corrisposto un premio in denaro in funzione dei risultati conseguiti durante le manche di gioco.

Diversamente da quanto avviene, ad esempio, con l'utilizzo delle console dei videopoker, il gambling on line, permette all'utente di effettuare sessioni di gioco virtualmente da qualunque personal computer connesso alla rete Internet, e di utilizzare, in sostituzione del classico gettone da bar o moneta, veri fondi monetari per via telematica come il proprio conto bancario o la propria carta di credito.

Il Casinò on-line

In rete esistono diversi tipi di gambling online, che permettono scommesse di vario genere, tra cui ad esempio quelle sportive o le lotterie, ma i servizi che raccolgono il maggior numero di frequentatori sono quelli che riproducono in maniera virtuale le ambientazioni e giochi tipici dei grandi casinò. Tra i giochi messi a disposizione vi sono, ad esempio, la Roulette, il Black Jack, il Baccarat, le Slot Machines ed il Poker.

Attraverso operazioni generalmente di bonifico, il giocatore apre un "conto virtuale" presso i server del casinò selezionato, trasferendo i fondi da un conto bancario o una carta di credito. Questo conto rappresenterà il bacino monetario utilizzabile dall'utente per effettuare le puntate nelle varie manche di gioco, e per accumulare le eventuali somme vinte. Per poter riscuotere in parte o totalmente le somme presenti sul proprio conto, la maggior parte dei "casinò online" consente di effettuare accrediti su carta di credito, bonifici su conti bancari e in alcuni casi, l'invio di assegni direttamente al domicilio.

7. Embedded system forensics

a. Repertamento ed analisi di sistemi speciali:

- *inneschi di ordigni esplosivi*

- *palmtop*

“handheld devices are designed to make efficient use of their limited amount of memory. For instance Palm OS divides its memory into partitions called heaps and further divides some of these heaps into chunks for storing the equivalent of files (called databases on Palm OS)...some devices use FAT file system too...”
[Digital Evidence & Computer Crime, 2° edition, Casey 2004]

Le agende elettroniche, dette anche “organizer”, “data bank” o “digital diary”, sono apparecchi elettronici disponibili in una vasta gamma, da molto piccoli ed economici che possono contenere alcuni numeri telefonici, a quelli più costosi e sofisticati, detti anche PDA, che hanno potenze di calcolo elevate e che possono memorizzare grosse quantità di dati (testo, suoni ed immagini digitali).

Attualmente manca uno standard costruttivo unico per le agende elettroniche in quanto ogni produttore ha messo a punto strutture hardware particolari e proprietarie. Esistono circa 70 costruttori di data bank e diverse tipologie di prodotti che differiscono l'uno dall'altro per struttura e funzionamento.

Nell'analisi delle agende elettroniche, si deve porre particolare cautela allo stato delle batterie di alimentazione, questo perché i dati contenuti nella memoria, se venisse a mancare l'alimentazione interna, andrebbero irrimediabilmente persi.

- *sistemi di clonazione delle carte di credito e frodi on-line*

Le carte di credito, debito e prepagate sono usualmente, a livello italiano, un sistema di memorizzazione dati basato su una banda magnetica quindi una memoria che conserva dati digitali di modesta quantità e di natura alfanumerica. Tali dati, attraverso la combinazione dei sistemi bancari e talvolta di specifiche password (si pensi al bancomat) realizzano sostanzialmente transazioni economiche. Dal punto di vista fisico copiare tali dati è estremamente semplice. Si possono impiegare dei dispositivi di ridotta dimensione e grande flessibilità di impiego (perfettamente legali) denominati skimmer. Essi vanno poi collegati ad un PC sia per lo scaricamento dei dati che eventualmente per il loro impiego per transazioni o clonazioni (realizzazione di carte clonate).

Nell'ambito dell'impiego delle carte di credito va poi segnalato un filone molto flessibile, dinamico e carico di transazioni che spesso viene individuato con il termine MTIO (Mail, Telephone and Internet Orders). Anche prima del massiccio avvento di Internet con l'E-commerce ed i movimenti elettronici di denaro la carta di credito aveva aperto la porta alla virtualizzazione degli ordini mediante posta e telefono. Ad oggi la virtualizzazione è così spinta che sono state determinate specifiche carte ricaricabili la cui destinazione precipua è la Rete delle reti ed il cui impiego crescente ed anonimo spinge a pensare che presto soppianteranno la moneta cartacea.

Per le FFPP la tracciabilità di una carta o in genere di una transazione elettronica si riconduce all'individuazione di un numero di telefono, un IP address o nel migliore dei casi di dati fisici (es. indirizzo, identità, ecc.). Usualmente l'attività di indagine coinvolge gli Istituti bancari ed i provider di servizi telematici su Internet. Entrambi forniscono LOG (file report di attività), i primi sulle transazioni ed i secondi sulle comunicazioni ed i collegamenti. Tali tipologie di dati devono essere incrociate dall'investigatore tecnico al fine di determinare validi dati di tracciamento. Alcune osservazioni a questo proposito sono importanti: (1) il tracciamento come processo complesso ha un serio costo in termini di uomini, mezzi, preparazione tecnica e ditte/Enti coinvolti per cui spesso si tende a tracciare solo nei casi di maggiore importanza (che coinvolgono grosse transazioni o serie di transazioni) o paradossalmente in quelli più banali che si possono risolvere con relativa facilità perchè il responsabile non ha posto in atto validi meccanismi per nascondere la sua identità; (2) il tracciamento non è sempre possibile sia a seguito della non disponibilità dei LOG (tecnica in quanto potrebbero non esistere o legale in quanto gli istituti coinvolti - es. esteri o fraudolenti - potrebbero non volerli fornire) che per l'implementazione da parte del responsabile di forti meccanismi di anonimizzazione come l'impiego di PROXY, anonymizer ed intermediari finanziari elettronici che forniscono come servizio proprio l'impossibilità di risalire al richiedente di esso.

- sistemi di videosorveglianza digitali

I sistemi di videosorveglianza erano originariamente basati su sistemi VHS a cassette magnetiche analogiche. Ad oggi si sono orientati verso la digitalizzazione ed in definitiva uno di tali sistemi è semplicemente un particolare PC in cui l'ingresso dati privilegiato è la telecamera e non la tastiera o il mouse. I video ed i suoni sono quindi memorizzati in formato generalmente proprietario su hard disk. Tali supporti vengono sfruttati fino al riempimento per poi dare avvio alla sovrascrittura ciclica (primo memorizzato – primo sovrascritto).

In questo senso può dover essere necessario recuperare aree di memoria cancellate, mettere a fuoco o ingrandire fotogrammi, esaltare suoni, ecc. ma il tutto si risolve in attività di un software e non più, come avveniva un tempo, in operazioni su di un banco di lavoro per VHS. Questo ha determinato un allargamento delle possibilità di indagine. E per il sequestro del video? Andrebbero prese le stesse cautele di cui al capitolo sul forensic computing...

- sistemi GPS

Il sistema di localizzazione satellitare GPS (Global Positioning System), noto anche con il nome di Navstar, fu concepito dal Ministero della Difesa statunitense come mezzo universale per determinare con estrema precisione le coordinate di un punto dislocato sulla terra attraverso un sistema di satelliti artificiali e particolari ricevitori, consentendo inoltre di ottenere un'indicazione oraria molto precisa. Le applicazioni del sistema GPS non sono limitate al campo militare, ma sono disponibili anche per uso civile, seppure con qualche limitazione nella precisione ottenibile nelle misure.

L'attività forense sul GPS si limita all'individuazione di dati posizionali ed alterazioni di essi in corrispondenza di fatti criminosi.

b. la nascita dell'Electronic Forensics

L'electronic forensics è un'altra delle numerose branche del digital forensics. La sua ragion d'essere nasce dal fatto che spesso si devono affrontare indagini tecniche su sistemi praticamente ignoti basati però su componentistica elettronica standard di facile reperibilità (si pensi ai controlli elettronici dei giochi elettronici illegali, agli inneschi, a sistemi elettronici modificati al fine di svolgere particolari attività criminali, ecc.). Vi è quindi la necessità di capire quale risultato produca una strumentazione elettronica al fine forense e questa potrebbe essere una delle definizioni (da dare) dell'elettronica legale o investigativa.

8. Le garanzie

Lo scopo degli organi scientifici delle Forze di Polizia non dovrebbe essere quello di determinare la colpevolezza di un soggetto quanto l'individuazione di tutti quegli elementi, che solo l'indagine scientifica può determinare e/o avvalorare, atti a dimostrare l'effettivo svolgimento dei fatti.

In questo senso l'Arma dei Carabinieri ed in particolare la Sezione Telematica del RIS di Roma si è sempre mossa al fine di garantire al meglio delle sue possibilità tutte le parti processuali. Lo dimostrano le innumerevoli relazioni tecniche che in dibattimento hanno scagionato l'indagato. Il nostro successo non è misurato in base al numero di condanne ma in base alla possibilità di rendere chiari fatti che non lo sono. Questo determina la nostra mancanza assoluta di protagonismo televisivo o mediatico.

a. La necessità di definizione delle tecniche di contrasto al crimine ad alta tecnologia

L'attività tecnica nel settore è enorme in Italia ma vi è ancora una grande difficoltà nel coglierne le linee guida, questo per la mancanza di definizioni accademiche di natura squisitamente tecnica che dovrebbero essere poi avvalorate: (a) dall'esperienza accumulata negli ultimi anni dai vari organi tecnico-investigativi e periti, (b) dalla magistratura e dagli avvocati.

b. Gruppo di lavoro accademici in Italia

Ci sono diverse realtà universitarie che hanno provato e stanno provando a determinare i confini e le definizioni del crimine ad alta tecnologia. Vorrei citare l'Università di Messina che sta preparando per settembre 2006 una laurea specifica nel settore informatico ed elettronico forense e l'Università di Milano con il LEFT (Legal Electronic Forensic Team) gruppo di ricerca legale che si propone lo scopo, tra gli altri, di scrivere le linee guida uniformi per l'Italia nel settore delle indagini informatiche.

c. L'importanza della qualità totale del processo di produzione delle fonti di prova:

- *Certificazione del personale (selezione/aggiornamento/test)*
- *Certificazione degli strumenti (selezione/aggiornamento/comparazione)*
- *Molteplicità degli strumenti impiegati per una stessa indagine*
- *Certificazione e standardizzazione delle procedure (repertamento/analisi)*

- *Standardizzazione dei termini impiegati nelle relazioni tecniche finali*
- *Standardizzazione del reporting*

d. La Sezione Telematica del RIS di RM e la struttura di una relazione Tecnica

Una degli obiettivi fondamentali di un laboratorio forense è la standardizzazione delle relazioni tecniche a causa dei seguenti motivi:

- (1) bisogna impiegare un linguaggio semplice e preciso per descrivere i risultati delle analisi onde evitare contrasti in dibattimento;
- (2) bisogna impiegare un linguaggio tecnico approfondito ed avvalorato accademicamente per descrivere i passi del processo di repertamento ed analisi;
- (3) bisogna evitare errori procedurali a tutti i costi (l'attività è spesso ripetitiva).