



With financial support from the AGIS Programme
European Commission - Directorate General Justice, Freedom and Security
Contract nr. JAI/2004/AGIS/113 - December 2004

Raggruppamento Carabinieri Investigazioni Scientifiche
Reparto Investigazioni Scientifiche di Roma
Sezione Telematica

Seminario Internazionale – Roma, 23 e 24 maggio 2005

“Conferenza internazionale su strumenti, procedure, standard operativi e ricerca accademica (inerente aspetti tecnici e psicologici) nel settore delle investigazioni su Internet con speciale riferimento alla pedo-pornografia”

Investigazioni Tecniche: mezzi e problematiche

Cap. M. Mattiucci, Ten. D. Tricca, Mar.Ord. R. Olivieri, Mar. Ord. A. Natale, Mar. Ord. G. Finizia, Mar. Ord. A. Turco, Car. Sc. L. Giampieri, Car. Sc. S. G. Monfreda

La Sezione Telematica del RIS di RM si occupa, con competenza nazionale, di fare da supporto tecnico all'Arma territoriale per ogni aspetto inerente la criminalità ad alta tecnologia. Il presente lavoro presenta brevemente i maggiori campi forensi di indagine su sistemi digitali che la citata Sezione ha affrontato negli ultimi anni evidenziando statistiche, strumenti e metodi impiegati nonché alcune delle fondamentali problematiche tecnico/legali emerse.

Roma, 17 maggio 2005

1. Introduzione

La Sezione Telematica del RIS di Roma è unica nel suo genere tra i Reparti Investigazione Scientifica dell'Arma dei Carabinieri presenti in Italia nelle città di Roma, Parma, Messina e Cagliari. Proprio tale peculiarità le conferisce competenza su tutto il territorio nazionale in relazione a quelle attività investigative inerenti l'informatica, la telematica ed in generale i sistemi elettronici digitali. A tale settore, pedissequamente a quanto stabilito dal Gruppo per il Crimine ad Alta Tecnologia del G8, ci si riferirà, in questo lavoro, con il termine specifico di Crimine ad Alta Tecnologia (High Tech Crimes).

2. Le investigazioni tecniche

La Sezione Telematica del RIS di RM analizza ordinariamente dei reperti digitali a seguito della richiesta dell'Arma Territoriale, della Magistratura e raramente di altre FFPP. Gli esperti del repertamento dell'Arma territoriale prelevano i reperti digitali generalmente sulla scena del crimine per inviarli ai laboratori della Sezione.

Una prassi alternativa a quella evidenziata vede il personale tecnico della Sezione intervenire direttamente sulla scena del crimine assieme al personale repertatore al fine di supportarne l'attività quando questa divenisse di natura eccessivamente complessa dal punto di vista tecnico.

Eccezione alle citate procedure risulta ovviamente il fatto criminoso che avviene in ambiente virtuale (Internet). Può accadere che la Sezione stessa verifichi la presenza di un fatto illegale nella rete delle reti ed allora vengono prontamente interpellati gli investigatori della territoriale affinché si ristabilisca il normale flusso investigativo. Si può essere invece nella situazione in cui un utente comune individua il fatto-reato su Internet e ne dà comunicazione all'Arma territoriale (situazione assimilabile alla consuetudine). Per finire si può verificare che la stessa territoriale individui il reato su Internet per poi attivare le indagini e chiedere il necessario supporto alla Sezione Telematica e/o a specialisti esterni (quando siano stati disposti dalla magistratura).

In definitiva *l'investigazione tecnica* nasce sempre a seguito o in parallelo all'investigazione tradizionale e ne resta supporto evitando di assurgere a elemento autosufficiente.

3. Le aree di studio

Le aree di studio scientifico forense della Sezione sono molto aumentate negli ultimi 5 anni allargandosi dall'iniziale studio delle memorie di massa, che ad oggi è il settore più voluminoso ad Internet in diversi suoi aspetti fino a sofisticati e particolari sistemi elettronici.

Le seguenti categorizzazioni sono state fatte sulla base dell'esperienza e delle direttive e pubblicazioni internazionali nel settore:

6.1 L'analisi forense delle memorie di massa

Settore a cui ci si riferisce spesso con il termine *Forensic Computing (FC)* di cui sono state date diverse definizioni ma le seguenti due possono raccogliere sicuramente i concetti fondamentali inerenti: "...il processo di: Identificazione,

Conservazione, Analisi e Presentazione di ‘digital evidence’¹ in processo garantendone l’ammissibilità” [3] e/o “...la raccolta e l’analisi di dati secondo una prassi che ne garantisca la libertà da distorsioni e pregiudizi cercando di ricostruire dati ed azioni avvenuti nel passato all’interno del sistema informatico” [4]. In ogni caso, dato che le attività di FC tendono ad ottenere elementi atti a testimoniare un fatto accaduto-in o per-tramite-di un sistema informatico, la loro caratteristica principale è che intervengono sempre dopo il fatto stesso. Si noti che le due definizioni riportate tendono a completarsi e spiegarsi perché l’ammissibilità citata in [3], nella maggioranza degli ambiti legali è proprio la “libertà da distorsioni (volontarie/involontarie) e pregiudizi (di analisi)” di cui in [4].

Il termine memorie di massa raccoglie le memorie digitali di qualsiasi natura e principio, da quelle elettroniche a quelle magnetiche fino alle ottiche. La FC deve quindi tener conto delle peculiarità fisiche di ciascuno di questi supporti digitali al fine di garantire un’analisi accurata, completa e ripetibile (che non alteri in nessun modo il contenuto). A tale scopo i fattori predominanti nella procedura di laboratorio sono la copia iniziale e gli strumenti di analisi della copia.

In [5] viene sottolineato che “...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, nel FC, si impiegano delle funzioni di hash standard come DIVA [6] (proprietario della

¹ La traduzione brutale di “digital evidence” è “prova legale digitale” ma la legge italiana non ammette distinzioni tra “prove reali” e “prove digitali” quindi tale concetto è di difficile inquadramento formale (a meno di prossime modifiche della legge italiana inerenti le strutture e le informazioni digitali). Da adesso in avanti quindi si considererà la “digital evidence” come “prova legale ottenuta attraverso sistemi digitali” che, si badi bene è ben lungi da essere solo una “prova digitale” perché presume un processo interpretativo.

ditta Computer forensics ltd) o MD5² [7] (standard open largamente impiegato da diversi prodotti di punta nel FC 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).

Una nota molto importante deve poi essere riportata in relazione al tipo di copia dei dati di una memoria di massa o di una device digitale in genere. Si possono distinguere infatti almeno tre livelli di copia:

- a. *copia di livello fisico: o bitstream copy*, in cui il contenuto dell’unità fisica viene letto sequenzialmente (la sequenza è stabilita dall’indirizzamento fisico, in genere gestito dal controller dell’unità di memoria) caricando la minima quantità di memoria di volta in volta indirizzabile (ad es. negli hard disk il settore fisico, nelle ROM il byte, ecc.) per poi registrarla nella stessa sequenza su di un comune file binario (*immagine fisica dell’unità*);
- b. *copia di basso livello del file system: o 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 (ad es. il cluster in FATxx) per poi registrarla nella stessa sequenza su di un comune file binario (*immagine di basso livello del file system*);
- c. *copia del file system*: 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*) di particolare formato (dipendente dal tool impiegato).

Il classico comando *dd* dei sistemi operativi Unix-like può ad esempio effettuare delle copie sia di tipo a. che b. mentre il tool software *Ghost* svolge copie di tipo c.. Il *dd*, per la semplicità di impiego e per la disponibilità del codice sorgente (es. in Linux) è divenuto un punto di riferimento anche nel dump di sistemi digitali come ad esempio le smart-card. Sfortunatamente non fornisce

² *Hash MD5*: algoritmo, appartenente alla RSA Data Security Inc., sviluppato da Ronald L. Rivest nel 1991. Un’autorevole descrizione dell’algoritmo è riportata nel documento “RFC 1321”, pubblicato su Internet all’indirizzo <ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt>

nessuna garanzia di tipo forense, nel senso che non effettua controlli di aderenza o calcoli di hash-function, ecc..

Si sottolinea, infine, che i citati livelli di copia non sono affatto equivalenti se lo scopo è individuare elementi probatori di tipo forense. In [10] si asserisce che *“La persistenza dei dati è enorme. Contrariamente a quanto si possa pensare è molto difficile rimuovere dei dati da una memoria di massa, a prescindere dalla propria volontà...abbiamo impiegato un hard disk di discrete dimensioni per installare prima una copia di Windows, poi una di Solaris ed infine una di Linux ed il risultato è stato che con un opportuno software forense i file delle prime due installazioni erano facilmente recuperabili...”*. La ricerca dei dati cancellati (generalmente ricchissimi di informazioni sull’attività svolta) è un elemento fondamentale dal punto di vista legale e le tre copie di cui sopra non permettono parimenti la citata analisi. In particolare la copia fisica a. mantiene tutte le informazioni possibili anche sul partizionamento (ad es. coesistenza di più sistemi operativi, ecc.), quella b. contiene sia i file cancellati che quelli evidenti ma non i dati sulle partizioni includendo una sola di esse, per finire la c. mantiene solo il contenuto di file e directory evidenti. Ovviamente a tali fattori si contrappongono la velocità di svolgimento della copia che aumenta da a. fino a c.. La scelta del tipo di copia da svolgere dipende quindi molto dal tipo di prova digitale che si intende ottenere e dal tempo che si ha a disposizione.

6.2 L’analisi forense dei sistemi di comunicazione senza fili

Primeggia, in questo settore, l’analisi forense dei cellulari nei diversi protocolli attualmente presenti: ETACS, GSM, GPRS, UMTS. Tale analisi si esplica attraverso l’esplorazione del contenuto dell’hardware del cellulare, SIM esclusa e poi della memoria del chip di quest’ultima. Mentre per il FC la consolidata esperienza permette di selezionare procedure e tool validati in migliaia di casi lo stesso non può dirsi per il mondo dei telefoni cellulari in cui metodi e strumenti sono diversi a seconda degli studi tecnici e delle garanzie che il laboratorio forense garantisce.

La Sezione Telematica tende, come prassi, a garantire la minima alterazione del contenuto delle memorie del cellulare disconnettendolo dalla rete mediante l’analisi in condizioni di assenza di segnale radio.

Eccezioni a questo tipo quasi-ideale di approccio purtroppo esistono, soprattutto in relazione a quando bisogna superare le protezioni (PIN) della SIM. Il fatto viene superato dal punto di vista legale mediante una specifica disposizione della magistratura ma il fatto tecnico che l’inserimento ad esempio del PUK per superare il PIN porta ad un’alterazione irreversibile della memoria della SIM.

Altri sistemi “senza-fili” oggetto dell’analisi forense possono essere le cosiddette LAN-wireless in cui risorse di ogni tipo vengono a condividersi

attraverso segnali radio. Questo sub-settore è non solo rilevante quanto nuovo dal punto di vista puramente forense per cui sono in studio specifiche soluzioni mediante sistemi sperimentali realizzati dalla Sezione Telematica stessa.

Assieme allo studio forense dei telefoni cellulari la Sezione Telematica ha poi affrontato il mondo delle intercettazioni e della radiolocalizzazione per le quali è stata referente tecnico in materia normativa a livello nazionale.

6.3 L'analisi forense delle reti di computer

La Sezione svolge anche investigazioni in relazione ai crimini che vengono perpetrati mediante l'ausilio della Rete delle reti o esclusivamente in ambito virtuale su Internet.

Internet non determina solo un nuovo strumento di ausilio ai crimini ma genera proprio nuove categorie di crimini per i quali a volte è difficile anche trovare delle risposte legali efficaci (talvolta inesistenti). A ciò va aggiunto che Internet è anche e soprattutto un nuovo mezzo di comunicazione e coordinamento tra le forze della criminalità organizzata e comune.

La Sezione Telematica si propone come strumento di ausilio per i Reparti Territoriali dell'Arma dei Carabinieri in questo delicato settore fornendo una collaborazione continua che consente agli investigatori di rispondere a situazioni per le quali è necessaria una preparazione tecnica specifica.

Il trattamento dei casi investigativi avviene sia attraverso gli strumenti di laboratorio del RIS che mediante l'azione dei provider Internet (ISP) diretta da personale della stessa Sezione.

I casi maggiormente trattati riguardano: pedofilia, diffamazione, spionaggio industriale, terrorismo, frodi, ecc.. Di seguito si riportano alcuni generici riferimenti alle attività di indagine nel settore svolte dalla Sezione Telematica.

3.4.1 Remote control (controllo remoto)

L'uso sempre più frequente e massiccio della posta elettronica ha portato allo studio di sistemi software in grado di spostare tramite posta elettronica virus, cavalli di troia e programmi di controllo remoto nel destinatario senza che questo abbia la possibilità di filtrare i dati in ricezione.

In particolare i programmi di controllo remoto sono software originariamente pensati per il controllo ed il collaudo delle reti aziendali che permettevano all'amministratore di far svolgere ad un computer collegato tramite Internet o Intranet delle specifiche azioni senza che qualcuno lo manovrasse localmente. I programmi di controllo remoto possono avere scopi criminali rilevanti come, ad esempio, lo spionaggio industriale e l'intrusione.

3.4.2 Intrusion & Cracking

Per “intrusione” si intende l’accesso a delle risorse informatiche negate all’utente richiedente. La protezione delle risorse avviene attraverso dei meccanismi di autorizzazione che tengono conto di diversi elementi:

- *Password*: parola chiave privata conosciuta dal possessore e talvolta dall’amministratore del sistema che finisce per identificare le azioni del primo;
- *Priorità e livelli*: l’utente può essere abilitato o meno a sfruttare certe categorie di risorse a seguito della sua posizione gerarchica e funzionale all’interno dell’organizzazione cui appartiene da cui vengono stabiliti livelli di appartenenza e priorità degli stessi sulle risorse presenti;
- *Tempi*: certe risorse informatiche devono essere rese disponibili solo in determinati periodi di tempo (ad es. il classico lavoro d’ufficio 8.00-16.00) perché non è consono ai regolamenti dell’organizzazione sfruttarle in altri;
- *Accesso fisico*: se certe risorse non devono essere accedute di principio da una classe di utenti si fa in modo di renderle irraggiungibili fisicamente (nessun cavo di connessione) ma tale eventualità si è fatta sempre più remota causa la flessibilità di impiego di un sistema totalmente connesso.

Da tali vincoli di protezione scaturiscono studi su come aggirare i sistemi: ad esempio modificando l’orologio di riferimento della macchina protettrice delle risorse, oppure emulando l’identità di un utente abilitato dopo aver “ascoltato” in rete i messaggi di identificazione (sniffing), o ancora ingannando l’amministratore richiedendo via fax o telefono dati di identificazione fingendo di esserne i legittimi proprietari, ecc.

Le operazioni di intrusione su un sistema informatico protetto sono comunque una violazione di un’area privata in quanto internazionalmente una risorsa informatica la si ritiene privata ad una organizzazione se e solo se quest’ultima ha provveduto con ogni mezzo idoneo a proteggerla. Si noti che una informazione privata non protetta in Italia risulta comunque tutelata da una legge sulla privacy molto restrittiva ma nel resto del mondo ciò non è così comune.

Nelle operazioni di intrusione ha un ruolo fondamentale la procedura di “cracking”, ossia il sistema hardware/software per violare un meccanismo di protezione basato su password oppure per individuare una password ed avere così l’accesso a delle risorse protette non proprie.

3.4.3 Comunicazioni illegali

Internet rimane prima di tutto un potente e flessibile mezzo di comunicazione multimediale e quindi la maggioranza dei reati attualmente perseguiti sulla rete delle reti è di tipo comunicazione non legale. Di seguito si andranno ad esaminare delle tipologie di riferimento per i reati di tale classe:

- *Pedofilia e Pornografia su rete telematica*: argomento di grande attualità in Italia e nel mondo che ha fatto di Internet quasi un mezzo di comunicazione demoniaco. La possibilità di inviare anonimamente informazioni di tipo pedofilo come foto, testi, contatti ecc. è ben nota alle organizzazioni criminali operanti che talvolta creano anche siti di riferimento in cui espongono le ragioni della loro attività di scambio ed i principi di libertà cui tali scambi sono basati.
- *Diffamazione e minaccia*: in genere tramite e-mail.
- *E-mail Bombing*: la posta elettronica, da utente ad utente deve passare attraverso dei server di posta, computer dotati di poderose memorie di massa e specifici software in grado di mantenere e smistare i messaggi di posta elettronica. Esistono tecniche legate al protocollo di comunicazione della posta elettronica che consentono in poche ore di far arrivare migliaia di messaggi allo stesso server di posta da direzioni differenti fino a saturarne le capacità di gestione.
- *E-commerce frauds*: le comunicazioni alla base delle transazioni economiche del commercio elettronico devono risultare estremamente sicure pena l'impossibilità di svolgere transazioni corrette. Le frodi in questo settore sono diverse e molto sofisticate, prendono in considerazione lo sniffing (ascolto in rete) e la simulazione di identità. In questo modo si possono, per esempio ottenere numeri di carte di credito o accollare le transazioni ad altri utenti.

3.4.4 Hacker & Hacking

Dalle statistiche fornite dalla Cert-it (CERT italiano) le tecniche di attacco più usate sono:

- *Sniffing*: cattura dei dati che viaggiano in rete;
- *Spoofing*: falsificazione dei dati;
- *Denial of Service*: impedire ad un sistema informatico di fornire servizi;
- *Backdoor*: entrata segreta in un sistema informatico che lo stesso hacker riesce a crearsi;
- *E-mail bombing*: l'atto di bombardare con migliaia di messaggi di posta elettronica la casella di un utente causando un crash (malfunzionamento critico) del server.

6.5 L'analisi forense di sistemi elettronici

La Sezione Telematica del RIS di RM si occupa anche di analizzare una grande varietà di sistemi elettronici digitali non propriamente inquadrabili nelle categorie dei precedenti paragrafi. Si tratta spesso di moduli di difficile analisi per i quali la conoscenza procedurale deve essere studiata empiricamente o ricercata mediante collaborazioni esterne (università, ditte specializzate, ecc.).

Si riportano di seguito alcuni esempi:

- *Sistemi di clonazione delle carte magnetiche*: microtelecamere, microfoni, sistemi di trasmissione a media/corta distanza, lettori di bande magnetiche, ecc.. Il problema fondamentale è dimostrare l'operatività di questi strumenti evidenziandone il raggio d'azione e segnalando eventualmente nominativi e dati di utenti frodati. Diverse sono le frodi possibili ma quella più ricorrente in Italia è lo skimming, ossia la lettura e riproduzione di carte di credito magnetiche al fine di ottenere cloni rivendibili all'estero.
- *Sistemi di clonazione delle smartcard*: le smartcard, ossia le carte plastificate dotate di microprocessore (chip digitale con capacità di memoria ed elaborazione) costituiscono una nuova via di spostamento di denaro e dati all'interno di una società tecnologicamente avanzata. Ampio settore investigativo in fase di crescita, le "smartcard frauds" raggruppano tutte le frodi operabili mediante carte intelligenti (smartcard, molto diffuse nei paesi in cui la criminalità ha compiuto i maggiori passi avanti). Il campo di studio è molto ampio e si ricollega anche alle frodi tramite carte di credito su Internet.
- *Agende elettroniche*: campo di studio simile a quello della forensic computing da cui differisce a causa del particolare hardware che si va ad analizzare. Tali sistemi hanno protezioni elettroniche ed una complessità globale di qualità inferiori rispetto ai comuni personal computer. In tal senso, l'analisi ed il superamento delle protezioni (eliminazione delle password di protezione) possono essere compiute in maniera sistematica attraverso dei particolari strumenti hardware/software ad uso esclusivo delle polizie scientifiche.
- *Sistemi di videocontrollo*: i nuovi sistemi di ripresa adibiti al controllo nelle banche ed in altri luoghi pubblici sono ormai quasi tutti digitali e quindi memorizzano sequenze video digitali su hard disk invece che su VHS o altri standard video analogici. Da questo punto di vista tali sistemi possono essere considerati come computer special-purpose (specializzati) e quindi devono essere analizzati con criteri riconducibili a quelli del forensic computing.
- *Sistemi di innesco e di controllo delle armi*: sistemi digitali spesso controllabili a distanza che consentono di attivare armi, meccanismi esplosivi, ecc.
- *Altro...*

Questo settore, cui ci si riferisce quale *electronic-forensics* ha un volume di analisi tecniche limitato per quantità ma non per importanza e per impegno degli operatori di laboratorio in quanto ogni indagine tecnica sembra quasi essere un mondo a sé e difficilmente si arriva a riunirle in categorie di analisi.

6.6 L'analisi forense del software

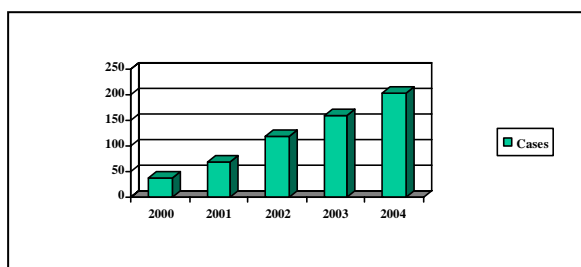
Le attività della Sezione in questo particolare ed esteso settore hanno riguardato:

- Individuazione di *software pirata*;
- Analisi di video-game a livello di programmazione e firmware;
- Analisi di software di protezione al fine di aggirarne le difese;
- Impiego di programmatori di EEPROM per l'alterazione delle memorie di smartcard.

4. Le statistiche

La Sezione impiega un database specializzato nel trattamento della documentazione inerente le indagini tecniche con gli attributi che le caratterizzano. Tale archivio elettronico consente di realizzare interessanti statistiche tra le quali:

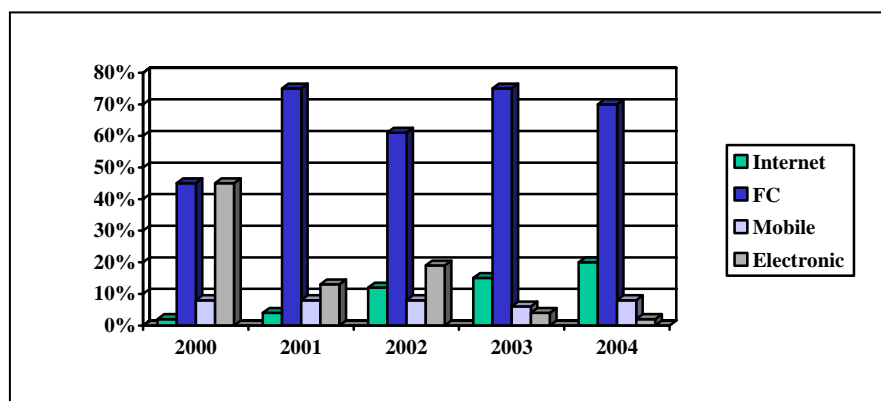
CASI INVESTIGATIVI TRATTATI NEGLI ANNI					
	2000	2001	2002	2003	2004
Nr. di casi	37	70	119	160	202



Come si può vedere l'incremento del volume di lavoro della Sezione è palesemente evidente. A tale incremento corrisponde un notevole problema di aggiornamento del personale e della strumentazione tecnico-forense da impiegare per le analisi di laboratorio. Ciò soprattutto alla luce dell'enorme velocità di cambiamento e progresso dei sistemi informatici e telematici.

Risulta poi molto interessante vedere come si sono distribuiti i casi in relazione alle varie categorie di analisi forense:

LE ANALISI FORENSI					
Settore	2000	2001	2002	2003	2004
Internet	2%	4%	12%	15%	20%
FC	45%	75%	61%	75%	70%
Mobile	8%	8%	8%	6%	8%
Electronic	45%	13%	19%	4%	2%



Come evidente le indagini tecniche su Internet, seppure limitate dato che la Sezione è nata principalmente per il forensic computing (settore ad oggi di punta nelle sue attività), sono andate incrementando percentualmente dal 2000 fino ad oggi mentre le analisi di sistemi elettronici speciali, pur essendo determinanti in casi di rilevanza nazionale sono numericamente andate scemando.

Bisogna poi tenere conto che di tutte le indagini tecniche più del 40% riguarda la pedopornografia. Anche tale percentuale è in continua ascesa dal 2000 fino ad oggi, con notevoli ripercussioni sul personale tecnico che, oltre ad avere una limitata preparazione nello specifico settore pedofilo, si è trovato ad operare in un argomento di difficile approccio umano che, secondo uno studio in corso, porterebbe a delle alterazioni nella personalità comunque da valutare periodicamente mediante test, colloqui, ecc..

5. Gli strumenti forensi

La Sezione Telematica svolge le sue attività di analisi forense basandosi su alcuni degli strumenti più diffusi e consolidati a livello nazionale ed europeo:

- *DIBS*: (Disk Image Backup System) uno dei primi sistemi di repertamento ed analisi dei dati nel forensic computing ormai in disuso dato l'enorme sviluppo della capacità delle memorie di massa;
- *EnCase*: software di repertamento dati ed analisi nel settore forensic computing impiegato da diversi anni dalla maggioranza delle FFPP al mondo;
- *Linux*: sistema operativo Unix-like la cui apertura a livello di sorgente consente di customizzarlo facilmente anche a livello forense (come già fatto con il comando “dd” per il dump delle memorie di massa).
- *Una serie di software di cracking, decryption, sniffing, tracing, ecc.* spesso artigianali o ricavato da alterazioni di software liberamente disponibili anche a livello di sorgente. Questi ultimi sono determinanti per alcune attività, soprattutto nelle Internet investigation ma non sono generalmente certificati né sono stati sottoposti ad una discreta casistica sperimentale.

6. Problematiche tecnico-investigative

Le investigazioni tecniche nel settore ad alta tecnologia nascondono diverse problematiche sia di natura tecnica che legale. Si riporta di seguito una carrellata di essi partendo da questioni comuni ad altre molto specifiche. Ciò al fine di sottolineare l'importanza di generare uno standard nel settore almeno a livello europeo.

6.1 Problematiche comuni

Al fine di garantire le parti processuali il procedimento di analisi tecnica dei reperti informatici/telematici deve rispondere ad uno standard di qualità totale ed in particolare bisogna ottenere *certificazione ed accreditamento* di:

- Strumenti di analisi;
- Procedure per l'impiego degli strumenti;
- Operatore che svolge le analisi;
- Strumenti per la creazione delle Relazioni Tecniche (reporting);
- Direttore di laboratorio responsabile per il reporting.

Data poi la citata velocità di evoluzione dello specifico settore vi è la necessità di un *continuo aggiornamento* degli:

- Strumenti impiegati;
- Conoscenze degli attori coinvolti.

Oltre a tali aspetti di garanzia bisogna poi stabilire delle metodologie ottimali di natura legale che consentano una *effettiva investigazione a livello almeno europeo* in relazione a crimini come quelli su Internet la cui natura transnazionale è fin troppo evidente e da anni impedisce di proseguire in un congruo numero di attività investigative.

Si arriva quindi alla problematica tecnica più evidente che è quella dell'incremento della capacità delle memorie di massa. Il processo di filtering che l'operatore si trova a dover applicare è sicuramente legato al suo acume investigativo ma la possibilità di tralasciare tracce importanti durante l'analisi di più di 10000 file (numero comune in un normale PC) diviene notevole. Ciò soprattutto considerando che le tipologie di file possono essere alterate mostrando un contenuto non rispondente alla realtà oppure si può far ricorso a crittazione, steganografia, ecc. che possono impedire con meccanismi, talvolta non superabili, la lettura dei dati.

Un'altra problematica di natura tecnica particolarmente sentita dagli operatori è relativa la loro possibilità di valutare correttamente il materiale in esame. Ad esempio il semplice fatto di stabilire se un'immagine porno vede coinvolto un minore o meno al suo interno non può essere delegata ad un tecnico informatico

forense che poco dovrebbe in assoluto sapere su come valutare tale fatto (non è sua specifica competenza). Tale problema si estende ovviamente a tanti altri settori della criminalità in cui si richiede erroneamente all'operatore di laboratorio di selezionare i file/dati di interesse quando quest'ultimo potrebbe non averne la competenza specifica.

L'ultima problematica cui si accennerà comune a diversi laboratori forensi "high tech" in Europa e nel mondo è l'influenza psicologica che attività quali le indagini pedo sui sistemi digitali hanno sugli operatori. Negli ultimi anni si è sollevato in tal senso un allarme non indifferente che ha portato diversi Dipartimenti scientifici ad imporre un controllo periodico del personale coinvolto mediante test scritti, colloqui, ecc..

6.2 Problematiche tecniche specifiche

La Sezione Telematica ha incontrato una grande varietà di problemi tecnici specifici durante le analisi svolte negli ultimi 5 anni da cui se ne riportano alcuni di rilevanza che possono fungere da base per ulteriori studi e soprattutto da metro di confronto con le altre realtà europee.

- *Decrittazione*: indagini che dovrebbero durare solo alcuni giorni spesso si protraggono per settimane a causa del problema di aprire archivi e/o documenti protetti mediante meccanismi di crittazione.

I tempi di decrittazione variano in funzione dell'algoritmo di cifratura impiegato, della quantità di informazioni presenti nell'archivio sottoposto alla procedura di "sfondamento" nonché della potenza di elaborazione disponibile.

Il formato compresso con password .zip impiega, ad esempio, un algoritmo relativamente debole e risulta suscettibile ad ogni tipo di attacco sia esso a forza bruta, basato su dizionario, su maschera, di tipo plain text o tendente a recuperare direttamente le chiavi di criptazione a prescindere dalla password. Uno qualsiasi dei suddetti metodi consente l'accesso all'archivio in tempi ragionevoli con una percentuale di successo di circa il 95%.

I formati .rar o .ace presentano delle difficoltà maggiori: l'algoritmo di cifratura che impiegano è nettamente più pesante di quello precedente e la loro intrinseca natura consente attacchi basati esclusivamente su forza bruta o dizionario, ovvero il tentativo di inserimento selettivo di password recuperate da un file di testo opportunamente preparato (dizionario) o generate mediante una combinazione progressiva di stringhe alfanumeriche. Tale metodo risulta dipendente ovviamente dalla dimensione dell'archivio e dal numero di file ivi presenti poiché ogni password generata o letta dal dizionario viene provata per ognuno dei file presenti in archivio. La velocità di decrittazione è quindi inversamente proporzionale al numero di file arrivando, in alcuni casi, ad attestarsi su un

valore di 8-10 password al secondo usando un elaboratore basato su Pentium 4 a 3 GHz, valore che determina tempi di elaborazione improponibili per il recupero delle chiavi d'accesso.

In tal caso si rende pertanto necessario sfruttare una potenza di calcolo maggiore di quella che può offrire un singolo elaboratore ad esempio mediante l'impiego di tools che supportino una decrittazione distribuita attraverso l'uso di un cluster di computer o, meglio ancora, di una intera rete di macchine.

Si noti, a tale proposito che la realtà dell'impiego di network di PC per la decrittazione è una realtà emergente in Europa come sottolineato dal resoconto sulla conferenza sul Cyber Crime tenuta a L'Aia il 19 aprile 2004, e che coinvolge le varie unità High Tech Europee. In tale meeting si è proposto infatti di gettare le basi verso la costituzione di una rete privata virtuale a livello europeo gestita dall'Europol (EU HTC VPN – già attivo e, almeno in parte, funzionale) che potrebbe, tra le altre importanti funzioni, divenire ausilio agli investigatori tecnici forensi per la decrittazione dei file.

- *Filtraggio delle informazioni*: l'incremento della capacità delle memorie di massa ha fatto divenire critico un problema che fino ad alcuni anni fa era risolvibile dal tecnico forense con un minimo di arguzia ed esperienza. Si tratta del come filtrare le informazioni di interesse ai fini delle indagini da una memoria di massa digitale.

Esistono problematiche di filtraggio ad almeno due livelli ma se ne potrebbero individuare diversi altri. In particolare:

- *Scelta delle informazioni evidenti*: anche ammettendo che tutte le informazioni contenute in una memoria di massa siano evidenti (cosa affatto scontata), l'onere di selezionarle è divenuto sempre maggiore negli ultimi anni perché innanzitutto la selezione non è brutalmente tecnica ma deve basarsi su diversi fattori non informatici quali: la personalità e le capacità tecniche dell'utente, il tipo di reato, ecc.. Ad esempio quando l'operatore High Tech deve selezionare delle immagini pedo tra tante immagini porno al fine di presentarle alla magistratura effettua un'attività di natura medica o psicologica ma certamente non coinvolge la sua competenza informatica. In questo senso risultano importanti nuovi studi che si stanno sempre più affacciando nel settore della criminologia, come il *profiling degli utenti di computer*. Tale affascinante settore di natura prettamente psicologico dovrebbe affiancarsi al forensic computing in fase di analisi al fine di consentire selezioni giustificate ma soprattutto corrette e quindi utili all'incriminazione e/o al prosieguo delle indagini.

Come esempio pratico, uno degli accertamenti tecnici informatici più ricorrenti è la ricerca, nelle memorie di massa di un PC posto in sequestro, di documenti contenenti immagini fotografiche di natura pedo-pornografica che quindi possano essere ricondotti ad un'attività delittuosa nell'ambito della pedofilia.

In un tale contesto, l'accertamento tecnico condotto con un prodotto forense come EnCase consente di analizzare tutti i file contenenti immagini fotografiche al fine di evidenziare l'eventuale presenza di documenti di interesse per le indagini. Tuttavia l'enorme mole di immagini solitamente rinvenibili rende estremamente lunga e tediosa la fase di individuazione preliminare dei possibili file di interesse. Ciò è ancor più vero se si tiene conto del fatto che di norma la maggioranza dei file contenenti immagini (grafiche o fotografiche) è costituita da materiale grafico facente parte del software del sistema operativo o dei vari pacchetti applicativi installati dall'utente.

L'esperienza acquisita nel corso dei numerosi accertamenti tecnici finora effettuati ha permesso di individuare dei criteri di selezione mediante i quali si può sensibilmente ridurre il numero dei file da analizzare.

Un primo criterio è basato sul confronto dei valori Hash MD5 tra i file rinvenuti sulla memoria di massa e le librerie di Hash a disposizione del tecnico. In tal modo è subito possibile evidenziare l'appartenenza di determinati file a specifici pacchetti software, siano essi sistemi operativi o applicazioni varie. Ciò consente quindi di escludere una parte più o meno significativa di file dalla successiva analisi individuale. Questo stesso criterio, del resto, consente anche l'immediata identificazione di eventuali file contenenti immagini fotografiche di natura pedo-pornografica, qualora risulti positivo il match dei valori Hash MD5 di tali file con quelli disponibili in apposite librerie. Può quindi essere di estrema utilità la costituzione di una ricca libreria di Hash MD5, generati a partire dai file contenenti immagini pedo-pornografiche individuati nel corso degli stessi accertamenti tecnici condotti in precedenza.

Un secondo criterio di selezione è poi basato sull'identificazione e successiva valutazione della risoluzione di ciascuna immagine grafica, con particolare attenzione ai file del formato JPEG i quali risultano di fatto quelli di gran lunga più utilizzati per la memorizzazione di immagini fotografiche. La valutazione della risoluzione delle singole immagini consente infatti di scartare dalla successiva analisi individuale tutte le immagini "troppo piccole", ovvero non sufficientemente grandi in termini di risoluzione da

poter essere di oggettivo interesse per le indagini. Tale criterio è stato messo in pratica mediante la scrittura di un'apposita script per EnCase (nelle sue versioni 3 e 4) che consente all'utente di specificare la risoluzione minima delle immagini JPEG da ricercare. I file così selezionati vengono segnalati tramite bookmark ed eventualmente estratti in un'apposita cartella. Della citata script sono state sviluppate due distinte versioni: la prima prende in considerazione i file JPEG rinvenuti da EnCase in area allocata e quindi mostrati in tabella; la seconda invece ricerca i file JPEG nell'intera area non allocata della memoria di massa in esame. Entrambe le versioni della script sviluppata consentono una riduzione in media del 60% del numero complessivo di file JPEG da destinare all'analisi visuale individuale.

- *Scelta delle informazioni non evidenti:* dalla crittazione al nascondere informazioni in file la cui estensione non corrisponde al contenuto fino a confondere piccoli file in cartelle enormi quali quelle del sistema operativo, ecc.. Si tratta di metodi molto fruibili che permettono di nascondere efficacemente le informazioni.

Si ponga il caso, ad esempio, che l'investigatore stia cercando in un Hard Disk delle foto digitali. Per prima cosa si tenterà di isolare tutti i file che verosimilmente possano contenere tali immagini. L'individuazione sarà basata fondamentalmente sull'analisi dell'estensione del file, concentrando l'attenzione su specifici formati (jpg, bmp, tif, png, ...) che comunemente sono destinati a contenere immagini. In questo modo, però, si escludono dalla ricerca quei file ai quali l'utente indiziato potrebbe aver modificato l'estensione, proprio al fine di sviare l'attenzione dell'investigatore dal contenuto particolarmente riservato.

Per evitare tali circostanze, l'investigatore potrebbe allora avvalersi di strumenti software capaci di confrontare l'estensione con l'*header* di ciascun file, al fine di evidenziarne eventuali anomalie. L'*header* di un file, infatti, costituisce una sequenza di particolari valori (stringa di byte) posti all'inizio del file, che identificano (spesso univocamente, ma non sempre) la tipologia dei dati contenuti. Utilizzando questa tecnica si riduce notevolmente la possibilità che particolari file sfuggano all'attenzione dell'investigatore forense, tuttavia potrebbero ancora rimanere esclusi taluni file nei quali sia stato appositamente inserito un header anomalo ma compatibile con la nuova estensione opportunamente assegnata.

A tal punto l'investigatore non dispone attualmente di collaudati strumenti di analisi, capaci di evidenziare la presenza di file così

profondamente alterati. Per questo motivo ci si spinge verso altre metodologie di analisi del contenuto delle memorie di massa, che possano prescindere dall'esame dell'estensione e dell'header, come lo scanning statistico.

La Sezione Telematica ha realizzato a tale scopo un software denominato "FileScanner", operante in ambiente Windows, grazie al quale è possibile evidenziare graficamente alcune proprietà statistiche che utilmente possono essere prese in considerazione al fine di caratterizzare automaticamente il formato del file partendo dalla sua analisi binaria.

È importante sottolineare, per finire, che l'ambito del filtraggio delle informazioni non è solo importante nel forensic computing ma la sua prima apparizione ed il settore di punta in cui si evidenzia la sua necessità è ovviamente nella supervisione dei canali dati (ad es. il controllo delle dorsali). *L'information filtering*, in questo caso, fa sue diverse tecniche mutuata dal consolidato settore del *data mining* (o più limitatamente *text mining*) che si occupa di "estrarre automaticamente non note ma valide ed utili informazioni da grandi sorgenti di dati quali ad esempio database per poi poter impiegare in processi decisionali"[16].

- *Immagini virtuali*: esistono almeno due tipologie di immagini digitali che possono essere utili nel settore delle indagini sul pedo-porno e che attualmente non possono essere considerate illegali in stretto riferimento allo specifico. La prima categoria racchiude le immagini ottenute come mistificazione di foto reali o composizione di parte di esse. La seconda quei disegni realizzati con strumenti generalmente software che richiamano situazioni pedo-porno o pedo-erotiche. La legge italiana, ad oggi, non consente di riferirsi a tali materiali come esplicitamente pedofili. Tali rappresentazioni, che tendono attualmente ad aggirare le norme vigenti, vanno comunque ad incrementare un mercato sempre crescente della pedo-pornografia, assemblando pezzi di corpi reali con parti disegnate o pezzi di veri e propri fumetti o cartoni animati.

Le condotte mirate alla trattazione del materiale di cui sopra, se riconosciute tali, consentono in base alla normativa vigente una riduzione della pena di un terzo rispetto alle sanzioni per le immagini di minori reali. Un fenomeno molto diffuso fra i procacciatori di tale materiale, stante ai dati relativi alle analisi finora trattate da questa Sezione, consiste nella ricerca, scambio etc., di materiale dai contenuti pornografici e pedopornografici sia sottoforma di fumetti o cartoni animati realizzati con tali contenuti (vds Manga) sia sottoforma di ritocchi di fumetti esistenti ed innocenti, ove i protagonisti (spesso miti per i bambini) vengono raffigurati in atti sessuali (vds Simpson, Pokemon etc.).

In data 7 novembre 2003 il Governo italiano, durante la riunione del Consiglio dei Ministri, ha approvato un disegno di legge per far fronte al preoccupante fenomeno della pornografia infantile e dello sfruttamento sessuale dei minori, mirata in particolar modo e quella realizzata e veicolata attraverso gli strumenti informatici.

La proposta di legge, frutto del lavoro del Comitato Interministeriale di Coordinamento per la lotta alla Pedofilia (CICLOPE), e suddivisa in 19 articoli organizzati in due Capi: “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo-pornografia” e “Norme contro la pornografia infantile a mezzo internet”, deriva dall’intenzione di:

(1) superare rapidamente quelle che si sono rivelate nel tempo delle gravi lacune dell’impianto normativo, sostanziale e processuale, realizzato dalla legge n. 269 del 1998, intitolata "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù", alla luce delle nuove tecnologie informatiche e dei nuovi mezzi di diffusione e commercializzazione del materiale pornografico realizzato attraverso lo sfruttamento di minori (vds programmi di file-sharing, diffusione a mezzo newsgroup con contenuti binari etc.);

(2) adeguare sostanzialmente la disciplina processuale vigente al contenuto della Decisione quadro **2004/68/GAI** del Consiglio Europeo, che induce gli Stati membri, tra le altre cose, ad incriminare anche la pornografia infantile c.d. “apparente” (anche se del problema delle immagini tipiche dei fumetti pedo-pornografici nulla è evidenziato direttamente).

– *Nuovi media digitali e nuovi aspetti investigativi*: la Sezione Telematica incontra continuamente nuovi problemi in relazione all’analisi di dispositivi digitali di rinnovata concezione. Un tipico esempio è costituito dai dispositivi wireless.

(1) Sono comunemente disponibili sul mercato dei prodotti che permettono di rendere di tipo wireless gli hard-disk e le informazioni in esso contenute. Vedasi il prodotto che l’Asus mette in vendita ampliando ulteriormente la propria gamma nell’ambito delle soluzioni WLAN, presentando il nuovo WL-HDD, un compatto dispositivo di memorizzazione unico nel suo genere. Si tratta di una nuova soluzione nata per rispondere alle esigenze di memorizzazione e condivisione dei dati anche attraverso un collegamento Wireless basato su protocollo IEEE 802.11g e compatibile con lo standard 802.11b. I problemi che si creano sono di natura sia tecnica che legale: (a) riuscire a trovare fisicamente i dispositivi durante l’intervento sulla scena del crimine, (b) avere la corrispondente autorizzazione formale della magistratura ad effettuare il

sequestro (ad es. un WL-HDD può trovarsi in un domicilio adiacente ma comunque diverso da quello dell'intervento).

(2) Con l'evoluzione di protocolli di comunicazione mobile quali ad esempio l'UMTS, che garantiscono un flusso dati paragonabile a quello degli ormai più comuni servizi su cavo, dispositivi portatili come i cellulari stanno divenendo sempre di più vere e proprie mini-workstation da tasca. Computer palmari o smartphone, che sino a pochi mesi fa consentivano esclusivamente di utilizzare servizi da organizer, attualmente integrano sistemi di comunicazione che spaziano dal BT al Wi-Fi, dal wap-gsm-gprs sino all'UMTS e utilizzano unità di memorizzazione che superano ormai le dimensioni del Gigabyte. In questo modo è possibile, oltre che a visualizzare immagini, riprodurre contenuti audio e video, prelevare o riversare in rete grandi quantità di dati senza aver necessariamente dover utilizzare un desktop o un notebook. Attraverso questi stessi dispositivi si possono effettuare riprese fotografiche o piccoli clip, utilizzando le camere ccd integrate, pronti per poter essere trasmessi in rete o attraverso i servizi di messaggistica avanzati come l'mms, il video-mms o l'e-mail. Tutto ciò porta a: (a) la difficoltà di monitoraggio del flusso dati tra questi sistemi che di fatto possono anche realizzare canali crittati "sicuri" e (b) difficoltà nel repertamento dei dati multimediali che contengono.

7. Conclusioni

Il Raggruppamento Carabinieri Investigazioni Scientifiche, con il presente progetto, si è proposto quanto segue:

- aggiornare ed allineare le proprie conoscenze relative alle investigazioni su Internet nel settore specifico della pedo-pornografia;
- incentivare, nell'ambito delle investigazioni telematiche, il ricorso a metodi e strumenti standard di investigazione tecnica al fine di fornire agli organi giudiziari referti inequivocabilmente interpretabili e sensibilizzare le competenti autorità nella direzione di realizzazione di uno standard per le analisi forensi High Tech in Europa;
- agevolare le procedure di cooperazione internazionale, attraverso l'approfondito esame delle normative vigenti e della diretta conoscenza interpersonale tra i funzionari che si occupano del settore nell'ambito dei Paesi destinatari del progetto proponendo utili modifiche inerenti le direttive europee nel settore della pedo-pornografia;
- ottenere documentazione valida da sottoporre all'attenzione di tutti i partecipanti la conferenza e dei reparti dell'Arma direttamente coinvolti nel contrasto al fenomeno pedo-pornografia su Internet.

La Sezione Telematica ha contribuito per l'aspetto tecnico/legale di stretta competenza provvedendo ad evidenziare sommariamente il proprio inquadramento operativo, i mezzi tecnici, le statistiche sulle indagini e le inevitabili problematiche affrontate e da affrontare nei prossimi anni per continuare la lotta alla criminalità nel settore Alta Tecnologia.

Bibliografia

- [1] Vlasti Broucek, Paul Turner (2001), *"Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare"*, School of Information Systems, University of Tasmania, Australia, Journal of Information Warfare.
- [2] Vlasti Broucek, Paul Turner (2001), *"Forensic Computing: Developing a Conceptual Approach for an emerging Academic Discipline"*, School of Information Systems, University of Tasmania, Australia, 5th Australian Security Research Symposium.
- [3] Mc Kemmish, R. (1999), *"What is Forensic Computing"*, Trends and Issues in Crime and Criminal Justice (118), Australian Institute of Criminology.
- [4] Farmer D., Venema W. (2000), *"Forensic Computer Analysis: an Introduction. Reconstructing past Events."*, Dr Dobb's Journal, 29, 70-75.
- [5] Bates J, (1997), *"Fundamentals of computer forensics"*, International Journal of Forensic Computing.
- [6] Bates, J. (2001). *"DIVA Computer Evidence (Digital Integrity Verification and Authentication)"*, International Journal of Forensic Computing, 26 March 2001.
- [7] R.Rivest (1992), RFC 1321 - *"The MD5 message digest algorithm"*, MIT laboratory for computer science and RSA Data Security, Inc., April 1992.
- [8] Vlasti Broucek, Paul Turner (2002), *"E-mail and WWW browsers: a forensic computing perspective on the need for improved user education for information systems security management"*, School of Information Systems, University of Tasmania, Australia.
- [9] Chet Hosmer (1998), *"Time-lining Computer Evidence"*, WetStone Technologies Inc.
- [10] Farmer D. (2001), *"Bring out your dead. The Ins and Out of Data recovery"*, Dr Dobb's Journal, 30(1).

- [11] ACPO (2000), "*Good Practice Guide for Computer Based Electronic Evidence*", The Association of Chief Police Officers (ACPO) Computer Crime Group.
- [12] T. Sammes, B. Jenkinson (2000), "*Forensic computing: a Practitioner's guide*", Springer Publications.
- [13] A.J. Marcella, R.S.Greenfield (2002), "*Cyber Forensics: a field manual for collecting, examining and preserving evidence of computer crimes*", Auerbach Publications.
- [14] M.M. Ferraro, E. Casey (2005), "*Investigating Child Exploitation and Pornography*", Elsevier Academic Press.
- [15] E. Casey (2004), "*Digital Evidence & Computer Crime*" 2° edition, Elsevier Academic Press.
- [16] P. Cabena, P. Hadjinian, R. Stadler, J. Verhess, A. Zanasi (1997), "*Discovering data mining: from concept to implementation*" IBM Redbooks, Prentice Hall.