

Alcuni aspetti operativi di digital forensics

Poste Italiane
Sicurezza Telematica
G. Costabile

*COMPUTER FORENSICS, INVESTIGAZIONE PENALE E CRIMINALITÀ
TECNOLOGICA - L.E.F.T. (Legal Electronic Forensics Team)*
<http://www.avanzata.it/left> - Milano, 28 marzo 2007

Sintesi dell'intervento

A cura del Magg. CC Ing. Marco Mattiucci - Roma, 12 aprile 2007

Il Dr. Costabile ha presentato innanzitutto l'International Information System Forensics Association (IISFA) associazione americana senza fini di lucro atta alla divulgazione, training e certificazione in relazione al mondo del forensic IT. Il Comitato Tecnico Scientifico dell'IISFA è in corso di costituzione mentre il board direttivo è già stato creato. L'obiettivo è realizzare una certificazione tecnica nei settori del forensic computing e del network forensics che funzioni anche in Italia. I soci includono elementi dell'autorità giudiziaria, delle forze di polizia, dei periti e consulenti tecnici, di professori universitari, ricercatori, ecc.. Da sottolineare che l'iscrizione ai corsi IISFA per le forze di polizia è gratuita.

Sono stati quindi mostrati alcuni filmati tecnici (USA) inerenti il repertamento informatico sulla scena del crimine ed il trashing a scopo investigativo. Ciò evidenziando come lo spegnimento o meno del sistema computerizzato in maniera forzata (stacco dell'alimentazione elettrica), sebbene consigliato da tutti come standard, presenti anche qualche inconveniente.

Altre slide della presentazione hanno illustrato le attività di analisi di una SIM ed il relativo recupero di informazioni cancellate nonché diverse forme di cracking ottenuto mediante l'applicazione di dizionari intelligenti che vanno ad indicizzare i contenuti delle memorie di massa oggetto di indagine, di pagine web correlate, di informazioni personali dell'indagato, ecc..

L'interessante argomento successivo è stato poi quello della probabilità in ambito digital forensics (date le discussioni avute negli incontri precedenti del LEFT). Valori di probabilità a priori per accertamenti in quest'area sono molto difficili da valutare proprio a causa della variabilità delle condizioni al contorno. Si sottolinea che il forensics in ambito High Tech è un processo e non solo un prodotto o un servizio. In tale senso ci si sta avviando a compiere lo stesso errore che si è fatto all'affacciarsi prepotente, di alcuni anni fa, della sicurezza informatica sul mondo del grande business aziendale. Oggi tutti sanno bene che la sicurezza di un sistema informatico non è solo il firewall o il potente sistema di crittazione ma soprattutto la politica di sicurezza impostata dall'azienda su dipendenti e direttivo.

A titolo indicativo, sempre riguardo le probabilità, si è discusso del problema "collisione" per MD5 e del fatto che le slide dei precedenti incontri del LEFT siano addirittura state usate in dibattito contro alcuni periti per mettere in discussione la bontà della loro attività. Come più volte evidenziato nel corso degli incontri LEFT un fatto è quello puramente teorico della collisione ed un altro è applicare tale aspetto al caso concreto, ad esempio, della copia di un hard disk. Anche lo SHA-1, spesso indicato come valida alternativa allo MD5 è stato attaccato e teoricamente superato dal punto di vista matematico. Praticamente, però, l'attacco non è ancora stato portato a termine e se anche questo accadesse (fatto che i ricercatori danno per certo nel giro di alcuni anni) non sarebbe neanche plausibile pensare a due hard disk diversi di poco (con presumibile alterazione di informazioni critiche) e lo stesso valore di SHA-1 proprio perché, ad oggi, non c'è la possibilità di modificare di una piccola percentuale di contenuto un file preesistente lasciandone inalterato lo SHA-1 (o l'MD5) mentre è possibile costruire due file ad-hoc diversi che abbiano lo stesso MD5.

A tale proposito è stato sottolineato che il NIST ha indetto una competizione per una nuova funzione di hash standard, da impiegare per il futuro, che goda di particolare resistenza agli attacchi.

Di seguito sono state discusse brevemente alcune sentenze della Cassazione inerenti Internet e le informazioni digitali.

La sentenza della Cassazione, sezione lavoro, n. 2912/04 del 2 dicembre 2003 (rif. <http://www.interlex.it/docdigit/amonti73.htm>) evidenzia quanto segue:

“Si deve soltanto evidenziare che non è corretto il richiamo dei principi relativi alla produzione in appello di documenti precostituiti, in relazione ad una pagina Web depositata dall'A. nel corso del giudizio di rinvio, poiché le informazioni tratte da una rete telematica sono per natura volatili e suscettibili di continua trasformazione e, a prescindere dalla ritualità della produzione, va esclusa la qualità di documento in una copia su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento”.

In definitiva si sancisce **l'irripetibilità legale del repertamento di una pagina web** (fatto peraltro già evidenziato da diversi specialisti nel settore ma raramente ascoltato).

La sentenza, Corte di Cassazione Penale 13 novembre 2003 - 29 gennaio 2004, n. 3449 (02110/2003) evidenzia quanto segue:

“Ora, nella concreta fattispecie dedotta in procedimento, si contesta al ricorrente di aver sottratto dei files al presunto, legittimo detentore, e che l'impossessamento (con spossessamento di quel soggetto) si avvenuto mediante la "copia" dei files.

Indipendentemente da ogni altra argomentazione, è inevitabile considerare che la copiatura dei files da CD o da HD (compact-disk o hard-disk) in altro non consiste se non in una "duplicazione" di tali files (analoga al risultato di un procedimento fotografico, se pure tecnicamente cosa ben diversa), tanto che i files in possesso del detentore del CD o del computer sul quale sia installato l'hard-disk contenenti i files (nel caso, dei progetti e degli studi elaborati per conto del committente) rimangono memorizzati sul medesimo supporto sul quale si trovavano, mentre di essi il soggetto, presunto agente nel reato di furto, entra in possesso di un copia, senza che la precedente situazione di fatto (e giuridica) venga modificata a danno del soggetto già possessore di tali files.

E così come non può certo affermarsi che mediante processo fotografico si possa spossessare il titolare di un bene materiale corporeo (o di una res), così, allo stesso modo, non può affermarsi che lo spossessamento avvenga mediante il processo di copiatura dei files informatici.

Ne consegue, per la non configurabilità del reato di furto dei files mediante duplicazione (o copiatura), la mancata configurazione del fumus commissi delicti, necessario presupposto del disposto sequestro.

La non compiuta spiegazione, in provvedimento impugnato, della modalità concreta dell'affermato spossessamento ad opera dell'indagato, implica il lamentato difetto di motivazione, ed esige annullamento con rinvio del provvedimento impugnato per nuovo esame sul punto.”

La discussione è continuata sull'art. 220 C.P.P. (oggetto della perizia) che lascia al patrimonio della scienza e della tecnica il metodo e non lo cristallizza in legge proprio per ottenere una notevole flessibilità ed adattabilità ai continui aggiornamenti di tali settori. Si presenta quindi come poco valida l'idea di adattare la legge ai continui cambiamenti soprattutto dell'informatica e della telematica in quanto risulterebbe vano e si rimarrebbe sempre un passo indietro. Semmai bisognerebbe garantire un ulteriore livello di flessibilità al framework legale così da aumentarne la possibilità di impiego futura.

L'utilità delle “best practices” è stato il concetto affrontato successivamente. Esse aiutano per la standardizzazione ma non devono essere troppo stringenti in quanto finirebbero per costituire un problema serio per i tecnici competenti ed un cavillo interessante per invalidare il recupero di determinati elementi di prova. L'approccio delle best practice è tipicamente anglosassone e sfortunatamente tale punto di vista poco si adatterebbe alla nostra filosofia del diritto.

Si è quindi parlato del Computer Forensics e della ripetibilità degli accertamenti informatici. In dibattito spesso si sentono paragoni assurdi tra computer e beni fisici di vario tipo (come la mozzarella...) e nello stesso modo la fonte di prova digitale viene avvicinata a elementi volatili come i residui dello sparo, ecc.

Un'altra questione aperta è ovviamente quella dei “sistemi appropriati” con i quali svolgere le indagini tecniche. Cosa vorrebbe dire “appropriato”? chi lo stabilisce? Ad oggi nessuno. Ci si potrebbe affidare al NIST ed ai suoi test oppure agli strumenti open source ma sono solo direzioni che il singolo consulente può decidere o meno di adottare senza obblighi alcuni.

Lo IACIS dice, tra le sue linee guida, che:

- I tool vanno adattati dall'investigatore tecnico esclusivamente in casi particolari (non di prassi) o per i quali non si è specificamente preparati e bisogna darne atto.
- Il sistema operativo per l'attività andrebbe scelto adeguatamente, in ogni caso i write-blocker andrebbero sempre usati.
- Gli esami sugli originali dovrebbero essere sempre evitati. Lavorare sugli originali comporta infatti che si tratti di un accertamento irripetibile quasi con certezza.
- Impiegare più di un tool per svolgere un accertamento è indicato ed ottiene risultati ottimali ed in media maggiormente esaustivi.

Ad esempio FTK è molto lento in acquisizione ma indicizza in maniera ottimale il contenuto consentendo delle ricerche dati altamente performanti. EnCase è più rapido nella prima fase e consente l'impiego di un grande numero di script per la ricerca (che comunque è lenta), ecc..

Il NIST ha realizzato e svolge un Computer Forensics Tool testing che sta avendo diversi esiti. Uno dei più rilevanti riguarda proprio i write-blocker. Alcuni di essi, infatti, hanno dimostrato completa affidabilità (come FastBlock), altri meno.

Si è sottolineato poi che le perizie e consulenze tecniche in Italia sono piene di "dovrebbe, potrebbe, ecc." questo per non essere smentiti in dibattito e per mostrare una certa competenza. In questa maniera spesso si lasciano spiragli alla controparte non indifferenti.

Ultimi argomenti che lo scrivente ha seguito sono stati: l'importanza delle politiche di sicurezza aziendali per il supporto al forensics nello stesso ambiente (tracciamento degli eventi) e l'impiego dei dati temporali in LOG, comunicazioni, ecc. (integrità, consequenzialità, genuinità e corretta interpretazione della timeline).

Gli ultimi minuti della conferenza non sono stati seguiti dallo scrivente per cui potrebbe essere stati evidenziati argomenti non riportanti nemmeno sommariamente in questo lavoro.