L'AUDIT DI INFORMATICA FORENSE : UNO STRUMENTO FONDAMENTALE PER UNA PERIZIA DI QUALITA'

Vito Santarcangelo[1°], Giuseppe Lamacchia[2], Nancy Santarcangelo[3]

[1] *Centro Studi S.r.l. , Zona Industriale Loc. Sant' Antuono - 84035 Polla (SA)*
[2] *Studio Legale Avv. Lamacchia – Via Dante, 13D - Matera*
[3] *BNG S.r.l. – Via Ravenna, 2 - 75015 Ferrandina (MT)*

° *autore di riferimento - email: info@iinformatica.it*

Riassunto

Il lavoro presenta un'analisi dettagliata di una indagine informatica, sia per richiamare l'attenzione sui rischi connessi anche ad un uso del tutto lecito di uno strumento informatico, sia per cercare di comunicare agli esperti *alcuni possibili gravi errori procedurali assolutamente da evitare, sia, infine, per sensibilizzare coloro che, eventualmente, fossero coinvolti in episodi spiacevoli di questo tipo, di curare che il perito di parte sia ben consapevole delle cose che sono dette in questo articolo. L'idea è nata a seguito del crescente numero di reati informatici* [1] *che negli ultimi anni hanno monopolizzato l'attenzione dei mass media e, nel contempo, hanno persino modificato le previsioni normative e regolamentari e, soprattutto dal fatto che l'Italia è certamente tra le nazioni europee più colpite da attacchi informatici: il 36 per cento in più solo nel 2011; mentre resta desolatamente agli ultimi posti in ordine alla prevenzione ed alla sicurezza informatica (...Ultimo Paese in Europa per investimenti e applicazioni dell'ICT Security...)*[1].

1. INTRODUZIONE

Da circa un decennio, informatici e giuristi (esperti della materia) si sono prodigati nell'organizzazione di convegni, corsi, seminari e master di vari livelli, finalizzati a sensibilizzare gli italiani sulla *informatic security*, purtroppo però con scarsi risultati. I concetti dell'informatica forense restano, tuttora, come sfondo indistinto della disciplina e nell'uso della informatica.

Non sembra, quindi, superfluo, presentare le tecniche di ricerca ed acquisizione del dato informatico, ai fini della realtà del processo penale, con l'ausilio di casi pratici, a

[1] *www.tomshw.it/cont/...**sicurezza-informatica**...**italia**/.../1.html*

beneficio del 58,7% della popolazione, che, da dati del dicembre 2011, costituisce la percentuale di utenti internet in Italia.

Il lavoro è sviluppato in 4 paragrafi; nel primo si fa vedere come sia possibile incorrere in procedimenti penali, senza aver messo in atto alcun comportamento fraudolento; nel secondo è indicata la metodologia di tutela del dato informatico; e nei successivi viene mostrato come, nella realtà, viene effettuata una analisi forense.

2. PROFILI GIURIDICI E PROCESSUALI DELLA DIGITAL FORENSIC: IL DATO INFORMATICO COME PROVA GIUDIZIARIA

L'analisi di cui ci occuperemo è indicata come *Digital Forensic*, ed è definita come *l'analisi completa di sistema informatico digitale, finalizzata alla ricerca di elementi probatori che saranno oggetto della necessaria attività investigativa, essenziali per il Pubblico Ministero e/o per il difensore dell'indagato/imputato in un processo penale*.

Questa attività si colloca nella fase di investigazione; nel processo penale questa fase rientra nelle indagini preliminari e rappresenta la fase iniziale dell'intero procedimento penale. L'obiettivo è, a seconda di chi ne chiede l'acquisizione, di preservare elementi probatori per provare l'estraneità ai fatti ascritti all'imputato o per provare la sua responsabilità penale.

A titolo di esempio, si riporta qui di seguito il caso di un signore, appassionato della rete internet e frequente utilizzatore di social network, raggiunto presso la sua abitazione da due carabinieri in borghese che lo invitavano a recarsi presso la locale caserma, dove, durante l'interrogatorio, gli fu richiesto se avesse mai dato un ordine di bonifico in favore di un soggetto X, utilizzando il conto corrente della signora Y.

Invitato a cercarsi un avvocato di fiducia, gli fu notificata una ipotesi di reato di truffa informatica.

Cosa era successo? La signora Y aveva sporto denuncia verso ignoti per truffa telematica depositando la denuncia/querela presso la Procura competente, che provvedeva alla predetta iscrizione e successivamente delegava i carabinieri di zona competenti a svolgere interrogatorio dell'indagato.

Ritornando alla generalità del discorso, e seguendo il normale iter procedurale vi è una fase, segnata dall'avviso di conclusione delle indagini preliminari, in cui entra in gioco l'operato del team composto dall'avvocato e dal perito informatico che, non di rado, si accorge di grossolane carenze nell'indagine informatica eseguita.

Basti pensare che la motivazione del rinvio a giudizio dell'individuo dell'esempio precedente era avvenuta sulla scorta del semplice indirizzo IP comunicato dal Provider alla Procura richiedente, perché l'indirizzo IP dell'utente a quell'ora di quel giorno risultante nella denuncia/querela sporta dalla signora Y era connesso con la banca ordinante del bonifico, e senza considerare che utilizzando un semplice virus *Trojan* installato sul Pc della vittima, questa operazione poteva essere eseguita da terzi.

3. TUTELA DELL'INTEGRITA' DEL DATO

L'attività di ricerca della prova svolta dall'esperto di digital forensic, conduce, quindi, ad una relazione peritale che viene utilizzata nella fase dibattimentale del processo come

prova. Tuttavia è di fondamentale importanza assicurare e garantire una valida attività di ricerca probatoria caratterizzata dalla "tutela dell'integrità del dato informatico".

In questo paragrafo si intendono mostrare alcune delle "best practices" in merito alla salvaguardia dei dati presenti sui supporti di archiviazione posti sotto il vincolo del sequestro.

L'argomento è trattato in modo tecnico, per cui per coloro che non hanno familiarità informatica, è sufficiente sapere che si sta descrivendo una procedura operativa in grado di assicurare la correttezza del dato.

L'evidenza informatica non deve essere alterata, perciò è necessario prevedere a priori una "copia forense" del dispositivo in modo da non alterarne lo stato e il contenuto. Per effettuare l'analisi di un hard disk è necessario adoperare dispositivi hardware di sola lettura (write blocker) o distribuzioni live di linux (che effettuano il mount dell'hard disk in modalità "read" senza alterarne così il contenuto) [2]. Per la memorizzazione, oltre all'utilizzo di supporti di sola lettura (come CD / DVD), nella forensics vengono utilizzati anche algoritmi di hash (come l'MD5 o l'SHA1), il cui scopo è quello di generare una impronta del file permettendo così di verificarne l'integrità in un qualsiasi momento. Una qualsiasi modifica del file produrrebbe un'hash corrispondente differente. Per poter analizzare i dati di un hard disk è quindi sufficiente procurarsi una distribuzione di linux (come ad es. Helix) ed utilizzare il programma "dd" presente per effettuare così la copia forense su un supporto esterno.

Pur esistendo una serie di varianti all'algoritmo base dd (dcfldd, ddrescue, dd_rescue, sdd, etc.), si privilegia l'utilizzo di "dd" in quanto studi di complessità computazionale mostrano che la complessità asintotica O(g(n)) di un algoritmo g(n) è proporzionale al margine d'errore dell'algoritmo stesso [3]. Considerando che nell'analisi informatica forense fra i vincoli vi è la minimizzazione del margine d'errore, la scelta deve ricadere sull'algoritmo con complessità asintotica minore ossia "dd". Il comando dd è altamente personalizzabile tramite i suoi parametri, di conseguenza è lo standard de facto per la duplicazione delle prove binarie in ambito forense. Infatti, il metodo di duplicazione byte a byte è quello che consente di ottenere i risultati migliori nel tentativo di creare copie identiche all'originale e perciò di rispettare il principio d'inalterabilità della prova.

Supponiamo di dover creare un'immagine "copia.dd" dell'hard disk di sola lettura /dev/hda1/ nell'hard disk montato in scrittura in /media/sdb1/.

Il comando dd da eseguire sarà:

```
dd if=/dev/hda1 of=/media/sdb1/copia.dd conv=noerror,sync bs=32K
```

L'attributo "if" rappresenta l'input, "of" l'output . L'utilizzo del parametro "noerror" consente al processo, nella eventualità di un errore, di riportare l'errore nello "standard error" ma di non arrestarsi. Questo comporterà che gli indirizzi e la dimensione dell'immagine del disco rigido non corrisponderanno. Per ovviare a questo inconveniente si usano in contemporanea i parametri "noerror" e "sync". Il "sync" completerà con byte nulli lo spazio rimanente fino alla blocksize (bs), consentendo di preservare gli indirizzi. La dimensione, invece, risulterà sempre un multiplo della blocksize (bs).

Al termine è comunque necessario calcolare l'*md5* hash del file copia.dd ottenuto mediante il comando "md5sum"

```
md5sum copia.dd > copiadd.md5
```

4. ANALISI FORENSE DELLE ATTIVITA' DI UNA POSTAZIONE PC

Dopo aver concentrato la nostra attenzione sulla tutela del dato, passiamo a descrivere in modo pratico cosa sia la "computer forensics" con l'intento di mostrare al lettore come le attività effettuate da un utente su una postazione pc vengano registrate in opportuni file di sistema e possano essere utilizzati per mostrare un'evidenza informatica in ambito forense. L'analisi forense di un computer (computer forensics) può essere effettuata "live" (il pc da analizzare è acceso) e "post mortem" (il pc da analizzare è spento). L'analisi live riguarda principalmente i dati presenti in memoria RAM (memoria volatile del pc). In RAM infatti risiedono molte informazioni non recuperabili diversamente (comprese le credenziali di accesso a siti internet e il contenuto delle mail). In tale paragrafo per comodità si mostrerà una semplice analisi "post mortem" di una postazione pc con sistema operativo Windows 7. Supponiamo di aver effettuato le seguenti operazioni su un pc:

1. Accensione del pc alle ore 21.30
2. Apertura di Microsoft Word
3. Creazione del file "riservato.doc" e salvataggio all'interno di una cartella di nome "file riservati"
4. Cancellazione della cartella "file riservati"
5. Svuotamento del cestino
6. Spegnimento del pc alle ore 21.40

La maggior parte degli utenti penserebbe di non aver lasciato alcuna traccia di tali operazioni. In realtà è tutto fin troppo chiaro.

Utilizzando, infatti, un tool forense di analisi delle attività recenti come "OS Forensics" è possibile estrarre una timeline delle attività effettuate su tale macchina, che per comodità del lettore numeriamo al fine di dargli riscontro delle attività eseguite:

1)

System boot
Activity Type: System Event (System)
Record ID: 364131, Type ID: 6009
User:
Event Time: 07/06/2013, 21:30

2)

{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office12\WINWORD.EXE
Activity Type: Autorun command
UserAssist entry: {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office12\WINWORD.EXE, **User: Utente**
Date: 07/06/2013, 21:33, Count: 3

3)

riservato.doc
Activity Type: Office MRU
Path: C:\Users\Utente\Desktop
User: Utente, Location:
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1
Last Access: 07/06/2013, 21:35

6)

Shutdown
Activity Type: System Event (System)
Record ID: 364266, Type ID: 1074
User:
Event Time: 07/06/2013, 21:40

Dalla lista delle attività recenti non abbiamo alcuna informazione in merito alle cancellazioni. Per recuperare tali informazioni ci vengono in aiuto le utility di ricerca dei file cancellati.

$I6G2XH2 (Recycle bin meta data for: file riservati)
C:\$Recycle.Bin\S-1-5-21-340941697-3009836483-3621836857-1000\
Estimated restoration quality: 99%, Attributes: A-
Size: 544 Bytes, Created: 07/06/2013, 21:38, Modified: 07/06/2013, 21:38, Accessed: 07-Jun-2013 20:12

Questo record si riferisce al file $I###### creato per la cartella file riservati al momento dello spostamento nel cestino. Infatti, il cestino di Windows è la cartella $Recycle.bin di ciascun disco logico. Per ogni file cancellato dal sistema ci sono due file nel cestino [4]. Il primo contiene le informazioni su nome del file, cartella e data di cancellazione mentre il secondo contiene i dati veri e propri:

- $I###### Nome,percorso,data di cancellazione
- $R###### Contenuto del file originale

Perciò abbiamo traccia del fatto che alle ore 21:38 la cartella "file riservati" veniva spostata nel cestino, e quindi eliminata. Recuperando il file $I###### si scopre il contenuto del path "C:\Users\Utente\Desktop\file riservati".
Ecco che le attività 4 e 5 della lista sono emerse.

5. ANALISI FORENSE DI RETE (NETWORK FORENSICS)

Internet ha rivoluzionato il modo di vivere, lavorare e relazionarci, aprendo anche nuovi scenari di responsabilità civili e penali. La maggior parte delle attività svolte nella Computer Forensics (CF) conduce verso un ambito di rete (es. navigazione internet, e-mail, utilizzo di chat, software P2P, sistemi VoIP), quindi verso attività della NF (Network Forensics). Molte attività della NF hanno come conclusione il sequestro di una o più memorie di massa e quindi si ricade di nuovo nella CF. L'identificazione dei

dati utili per un'indagine su una rete consiste nella verifica dei sistemi e supporti interessati (switch, router,ISP), nella ricerca degli elementi che testimoniano una determinata attività sulla rete (LOG, report IDS), nell'individuazione di dispositivi e relativi supporti di memoria da analizzare mediante "computer forensics" per ottenere maggiori dettagli in merito alle attività svolte [5].

La rete è una struttura complessa formata da tanti nodi, che sono dispositivi di rete e host (computer). Se il problema è rappresentato da un singolo nodo, la soluzione più semplice sarebbe quella di fare lo shutdown della macchina, sequestrarla e agire secondo la CF. Tuttavia lo shutdown di un nodo della rete può compromettere definitivamente informazioni e processi che viaggiano sulla rete stessa. In questo caso l'unica via d'uscita è l'analisi a "runtime", ossia durante la normale attività del nodo e della rete.

Per mostrare meglio al lettore nel concreto cosa sia la NF consideriamo due casi classici di Network Forensics: analisi di una rete wifi e l'analisi del traffico di una macchina affetta da trojan-proxy.

Con l'avvento del wifi la connessione ha superato il confine dell'area circoscritta e delimitata da un impianto cablato, rendendo così possibile l'accesso ad utenti non autorizzati anche a distanza che ne sfruttano le vulnerabilità dei sistemi di autenticazione.

Il pericolo non è però rappresentato solo dal wifi, ma anche dai trojan proxy, software che colonizzano i pc soprattutto se sprovvisti di antivirus. Queste tipologie di trojan mettono il computer e la rete della vittima a disposizione dell'aggressore, in maniera silente, e quindi senza alterare il normale funzionamento del dispositivo della vittima.

Tali Trojan rendono l'attaccante completamente anonimo offrendogli la possibilità di fare qualsiasi cosa dal computer della vittima in gran sicurezza, inclusa la possibilità di lanciare attacchi dalla rete della vittima. I trojan proxy possono quindi essere utilizzati per operazioni in totale anonimato, per effettuare acquisti con carte di credito rubate e per altre attività illegali.

Le evidenze informatiche delle attività dell'attaccante (che ha agito mediante wifi o trojan-proxy) conducono alla rete della vittima, danneggiando così quest'ultima dal punto di vista delle responsabilità delle azioni effettuate dall'attaccante.

Per spiegare più semplicemente questi aspetti, presentiamo quindi al lettore due casi di analisi forense di rete: il caso in cui qualche "intruso" è collegato alla rete wifi e il caso in cui si è vittima di un trojan-proxy. Entrambe le operazioni vanno effettuate in modalità "runtime" ovvero analizzando lo stato della rete e il traffico del pc a connessione attiva.

Per renderci conto di quali dispositivi sono attivi all'interno della rete intranet (wifi e cablata) è sufficiente utilizzare un programma gratuito chiamato "fing" della Overlook Soft. Si tratta di un software multipiattaforma, disponibile anche per Iphone. E' sufficiente richiamarlo dalla shell per ottenere la rappresentazione tabellare completa dei dispositivi connessi e dei relativi indirizzi MAC. Se un intruso è presente sarà visibile all'interno di tale report. Nel caso in cui si riscontra la presenza di un dispositivo non autorizzato, oltre ad ottenere ulteriori informazioni in merito sul dispositivo,sfruttando il MAC address ricavato e utilizzando protocolli canonici, è possibile effettuare un'analisi realtime del suo traffico mediante la tecnica del "Man in the middle". Per effettuare tale analisi è possibile utilizzare un analizzatore chiamato "Cain" che permette di visualizzare in chiaro i pacchetti scambiati dal dispositivo non

autorizzato al router e ottenere una evidenza informatica del suo traffico, comprese informazioni a lui direttamente riconducibili.

Supponiamo di aver lanciato “fing” nella rete e di aver riscontrato nella tabella di output che oltre al nostro pc che chiamiamo per semplicità “V” (192.168.1.9) e al router (192.168.1.1) che chiamiamo per semplicità “R” vi sia un dispositivo non autorizzato (192.168.1.6) che chiamiamo per semplicità “A”.

State	Host	MAC Address
UP	192.168.1.1	00:13:2C:28:BA:71
UP	192.168.1.6	9C:EE:EB:54:E6:FC
UP	192.168.1.9	28:CA:EE:9C:04:EB

Supponiamo di voler analizzare a “runtime” il traffico web di “A”. Per poterlo fare è necessario effettuare un’operazione di “sniffing”, effettuabile con la tecnica del “MAN IN THE MIDDLE” [6] verso il dispositivo “A”. Tale tipo di attacco consiste nel trasformare il path A-R in A-V-R , facendo fingere a V di essere R (tecnicamente “arp spoofing”), in modo da intercettare tutto il traffico di A. Supponiamo che l’utente A effettui le seguenti azioni mediante browser:

1) Ricerca su www.bing.com della parola “Matera”
2) Accesso a facebook con credenziali info@iinformatica.it e password test

Dall’analisi effettuata mediante “CAIN” sulla macchina V è possibile ottenere in tempo reale la traccia di tutto il traffico web originato da A.

195.22.200.155	192.168.1.6	0231B6B6EBD1625A05BFB...	-1	http://www.bing.com/search?q=matera&for
31.13.86.17	192.168.1.6	info@iinformatica.it	test	http://m.facebook.com/?refsrc=http%3A%

Da tale analisi otteniamo un’evidenza informatica del traffico di A, mediante cui non solo provare la presenza di A nella nostra rete, ma esaminarne il suo traffico e cercare di individuare la sua identità reale a partire dal traffico da lui generato.

Nel caso di presenza di “trojan-proxy” all’interno del pc, è necessario analizzare tutto il traffico di rete generato dal dispositivo infetto. Il software per Windows “CurrPorts” permette di visualizzare in tempo reale il traffico generato da ciascun processo. E’ possibile perciò individuare quale processo fra quelli in esecuzione origina del traffico non autorizzato. Tale analisi e tale reportistica costituiscono un’evidenza informatica in merito. Un’alternativa avanzata è rappresentata da “Wireshark” che permette un’analisi “runtime” del traffico di rete anche da altra postazione sfruttando il servizio Remote Packet Capture Protocol da attivare sulla macchina target.

Altri casi frequenti che richiedono una analisi di NF sono l’analisi di un header di una e-mail e l’analisi realtime una conversazione effettuata tramite un sistema di messaggistica istantanea (es. Skype). Nell’header di una e-mail e durante una conversazione Skype si ha la chiara evidenza informatica dei nodi di rete (indirizzi ip pubblici) coinvolti. Tale argomento sarà oggetto di un prossimo lavoro in cui tratteremo nel dettaglio la social engineering (ingegneria sociale).

6. CONCLUSIONI E SVILUPPI

Il presente lavoro ha cercato di evidenziare un aspetto collegato al mondo dell'informatica non noto ai più. La tematica trattata non viene neanche sufficientemente comunicata ed è essenzialmente sviluppata su un piano esclusivamente accademico, in modo da limitarne, non diciamo, il know – how, ma, anche la contezza della sua esistenza. Anche se ci rendiamo conto che le procedure indicate possono essere seguite soltanto da esperti, abbiamo, nondimeno voluto trattarle, sia per iniziare a socchiudere una finestra su un argomento che, quando sarà noto ai più, potrebbe avere risvolti del tutto positivi, sia sugli utilizzatori di sistemi informatici, che su esperti del settore, sia per dare concretezza ad un argomento che finora è noto soltanto in linea di principio. Mentre invitiamo il lettore interessato a contattarci per eventuali approfondimenti, e mentre cerchiamo di organizzare un seminario per spiegare in modo puntuale le cose dette, ci riserviamo di fornire esempi concreti in un prossimo lavoro.

THE AUDIT OF COMPUTER FORENSIC: AN ESSENTIAL TOOL FOR A QUALITY SURVEY

Summary

The work deals with a detailed analysis of the problems encountered in a forensics analysis. The purposes are to make aware the practitioners of the risks associated to the use of the informatics tools as well a to suggest some precautions in developing the analysis. The idea of the article born from the consideration that Italy is the worst Country in Europe from ICT Security viewpoint

BIBLIOGRAFIA

[1] **Symantec Corporation,** Internet Security Threat Report 2013

[2] **A. De Sanctis,** Digital Forensic, Corso di Sicurezza c/o Università di Salerno, 2011

[3] **D. Scalea,** DD Analisi funzionale,forense e algoritmica, Cybercrimes

[4] **M.Epifani,** Introduzione all'analisi forense di Microsoft Windows 7, 2010

[5] **F.Mignogna,** Network Forensics, Università degli Studi di Perugia, 2010

[6] **R.Russell,** Hack Proofing, McGraw-Hill, 2003