



Digital Forensics – B.P.

Di Nanni Bassetti

18/06/2008

Definizione

La Digital Forensics è la disciplina scientifica che serve per identificare, acquisire ed analizzare una prova digitale, preservandola da eventuali alterazioni.

Scientifica: ripetibile (Galileo Galilei)

è la modalità tipica con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile. Esso consiste, da una parte, nella raccolta di evidenza empirica e misurabile attraverso l'osservazione e l'esperimento; dall'altra, nella formulazione di ipotesi e teorie da sottoporre nuovamente al vaglio dell'esperimento.

Prova: deve garantire il suo uso in tribunale

Definizione

I campi d'azione della Digital Forensics sono:

- 1) Indagini interne ad una azienda
- 2) Supporto alla Polizia Giudiziaria ed ai PM (CTU)
- 3) Supporto ai privati indagati (CTP)
- 4) Valutazione danni
- 5) Spionaggio
- 6) Frode
- 7) Pedopornografia
- 8) Violazione policy
- 9) Ricatto
- 10) Terrorismo

Definizione

Le fasi principali sono 4:

- 1) Identificazione
- 2) Acquisizione
- 3) Analisi e valutazione
- 4) Presentazione

L'identificazione ed acquisizione

Sulla scena del crimine bisogna, innanzi tutto, identificare ogni dispositivo che possa contenere prove (digital evidences), per poi acquisirlo.

L'identificazione ed acquisizione

Attualmente i dispositivi digitali che possono contenere le prove sono tantissimi e spesso sono così, inseriti nel nostro habitat da non farci più caso.

Esempi:

- 1) Computers
- 2) Memory cards
- 3) Nastri digitali

L'identificazione ed acquisizione

- 5) SIM cards
- 6) Cd-DVD rom
- 7) Smart printers
- 8) Smart Fax
- 9) Lettori MP3/AVI
- 10) Playstation et similia
- 11) ecc.

L'identificazione ed acquisizione

Al momento dell'analisi della scena si dovrà capire cosa prendere per poi analizzarlo.

Durante i sequestri si potrebbero ignorare o tralasciare alcuni dispositivi che potrebbero contenere informazioni preziose.

L'identificazione ed acquisizione

Non è detto che la prova, la cosiddetta
“*smoking gun*” sia sul computer di casa....

Anzi potrebbe essere su un DVD con la
copertina degli “Aristogatti” di Walt Disney

L'identificazione ed acquisizione

- Nella fase di sequestro si **potrebbero** commettere degli errori.
- Questo perché la D.F. è ancora una scienza senza protocollo comune.
- Non ci si preoccupa della ripetibilità del metodo utilizzato

L'identificazione ed acquisizione

- Non ci si preoccupa della preservazione della prova
- Non ci si preoccupa della catena di custodia e del corretto modo di presentare i risultati delle indagini informatiche (reporting)

L'identificazione ed acquisizione

La D.F. si divide in 2 branche la *live analysis* e la *post mortem*

Ognuna di esse ha regole diverse, dato che la live è un'analisi su un sistema acceso ed in funzione

La post mortem è su un sistema spento

L'identificazione ed acquisizione

Non ci soffermeremo molto sulle regole dell'analisi live perché è legata ad un evento in fieri ed è meno frequente...

Si ricordino dei semplici principi:

L'identificazione ed acquisizione

- 1) Non spegnere il sistema con la procedura di spegnimento
- 2) Non usare programmi della macchina sospetta
- 3) Dump della RAM (quando e se possibile)
- 4) Cercare di copiare i media bit a bit
- 5) Lanciare un programma di listing dei processi, utenti, insomma salvare tutte le informazioni di runtime
- 6) Scollegarlo dalla rete se non serve essere connessi
- 7) Documentare tutto quello che si sta facendo
- 8) Eseguire tutti i tools (esterni) di Live Analysis
- 9) Principio di indeterminazione di Heisenberg (gatto di Schroedinger)

L'identificazione ed acquisizione

Analisi Post Mortem

Il dispositivo è spento quindi è necessario acquisire tutti i dati presenti sul disco rigido in maniera *raw* o *bit a bit*.

Così da avere un clone perfetto dell'hard disk, compresi i files cancellati e lo slack space su un supporto esterno previamente sterilizzato (wiping) oppure un file immagine.

Verificare tutto con i codici di *hash* MD5 e SHA1

L'Analisi

1. L'analisi va effettuata sempre sulle copie e MAI sull'originale.
2. Si usino tools accettati de facto dalla comunità scientifica
3. Open Source Vs Closed Source
4. L'esperienza e la fantasia
5. Il profiling

L'Analisi

Tutte le analisi e ricerche devono essere eseguite sulla copia (meglio se copia della copia)

In ambiente virtuale (VMWare, Qemu, ecc.)
Questo per il fine della *ripetibilità*

L'Analisi

I tools possono essere commerciali o open source, l'importante che siano accettati dalla comunità dei C.F. experts, al fine di fugare dubbi sull'affidabilità dello strumento usato.

In caso di sviluppo di strumenti nuovi, è utile fornire il codice sorgente.

L'Analisi

I tools commerciali potrebbero avere varie problematiche, come tutto ciò di cui non si conosce il sorgente:

- 1) *Bugs*
- 2) *Formati troppo proprietari*
- 3) *Fine dello sviluppo del sw*

L'Analisi

I tools Open Source hanno dei vantaggi indiscutibili:

- 1) *Controllo dei Bugs da parte della community degli sviluppatori*
- 2) *Formati aperti e compatibili*
- 3) *Sorgenti aperti a tutti -> Si sa cosa fanno*

L'Analisi

La scelta NON deve essere radicale, ci sono sw commerciali che fanno cose che gli open source non fanno e viceversa

L'Analisi

TOOLS OPEN SOURCE:

Live distro Linux:

1. Helix
2. FCCU
3. IRItaly
4. F.I.R.E.
5. DEFT

L'Analisi

TOOLS CLOSED SOURCE:

1. ENCASE
2. UTK e FTK
3. XWAYS Forensic
4. ProDiscover
5. Ecc.

L'Analisi

Non bastano solo i tools a scoprire le prove
ci vuole anche:

- Esperienza
- Fantasia
- Arte
- Magia ;-)

A volte le prove sono in posti introvabili, protette da password, dentro le immagini (steganografia), nelle thumbnails, in files con headers modificati, su server internet, ecc. ecc.

L'Analisi

PROFILING

Per risparmiare tempo è utile dedicare un po' di tempo a studiare il *suspect* ed il suo profilo psicologico....magari così basterà aprire la cartella IMMAGINI ed abbiamo la prova che cercavamo....

Approcci

Deduttivo: idea generale scendo nel particolare.

Induttivo: dal particolare vado al generale

Reporting e Presentazione

Dall'acquisizione sino alla consegna delle prove il tutto deve essere documentato con i moduli della CATENA DI CUSTODIA (verbali), in modo da avere sempre la tracciabilità della prova.

Alla fine dell'analisi, bisognerà ricostruire gli eventi accaduti sul dispositivo analizzato e tutti i passi eseguiti per l'analisi, per poi spiegarli nel report finale da consegnare a chi di competenza (PM, Avvocati, P.G., ecc.)

Reporting e Presentazione

Il report non deve essere scritto in linguaggio “stregonesco informatico”, ma deve essere il più semplice e chiaro possibile, per ovvie ragioni....

Le prove vanno registrate su supporti ottici/magnetici e codificate con hash MD5, SHA1 e poi creare un file che contiene i codici che a sua volta dovrà essere criptato al fine di non dare la possibilità di alterare le prove con ri-masterizzazioni ...

Personalmente firmo anche col pennarello i supporti consegnati 😊

LA FORENSICS STATION

- Un computer abbastanza potente
- Hard disk esterni firewire/usb2/ata/sata
- Write blocker HW o SW
- Software O.S. / C.S.
- Scheda di rete (alta velocità)
- Masterizzatore DVD

Links interessanti:

- <http://www.cfitaly.net>
- <http://www.nannibassetti.com/cf> (Digital Sherlock Forum)
- <http://forensicsbypila.blogspot.com/> (Blog di Andrea Ghirardini)
- <http://www.cybercrimes.it>
- <http://www.denisfrati.it>
- <http://www.ictlex.com>
- <http://www.iritally-livecd.org/> (IRItaly)
- <http://www.iisfa.it/index.html> (IISFA)
- <http://forensics.typepad.com/> (Ziccardi)
- <http://www.marcomattiucci.it/>
- <http://www.ossblog.it/>

- www.guidancesoftware.com/ (ENCASE)
- www.accessdata.com/products/ (UTK)
- <http://www.techpathways.com/ProDiscoverDFT.htm> (PRODISCOVER)
- <http://www.e-fense.com/helix/forum/index.php> (HELIX)
- www.winhex.com/ (X-Ways)

Varie

1. Carving da Thumbs.db con foremost e DMThumbs
2. Carving con HexEditor
3. Carving immagine iso
4. Usi di Tridnet per identificare i files, file (linux) e ftype windows
5. Eliminazione header e upx
6. Steganografia
7. Helix in VMWare e VirtualBox, navigazione da VMWare o da Live disk, non lascia traccia
8. Autopsy in cygwin
9. UPX, AXCrypt, cambio headers
10. Entropia per formati sconosciuti
11. Intercettazione Voip (Skype) con trojan
12. DD, DD_Rescue (md5 diverso) e clonazione (stessa geometria dischi)
13. Casi di irripetibilità (360 c.p.p.) flussi di rete, live analysis, dischi rovinati, dischi con virus, supporti obsoleti e strani.
14. Photorec e Testdisk
15. Rainbow tables, collisione MD5



Conclusioni

- Arrivederci e buona caccia! 😊



CONTATTI

NBS di Nanni Bassetti
Consulente Information Security

<http://www.nannibassetti.com/>

E-Mail: nannib@libero.it

Cell. +39-3476587097