Strumenti e Metodi della Computer Forensics

N. Bassetti

Abstract. *Descriveremo i metodi e gli strumenti usati nella disciplina della digital forensics. Il focus è sul metodo scientifico e le abilità necessarie per lavorare sui reperti digitali.*

Keywords: Computer forensics, Scientific method, Open source tools

1. Introduzione

La digital forensics è una disciplina relativamente giovane e quindi in constante divenire e legata all'evoluzione dell'hardware e del software.

Si pensi a quanto è cambiato negli ultimi dieci anni, i computer sono diventati sempre più potenti, i sistemi operativi più complessi e differenziati, il mobile (smartphone, tablet, ecc.) ricopre una fetta importantissima, tutto questo implica una condizione di corsa tra gli investigatori digitali e la tecnologia.

Regolare le metodologie da applicare nella fase di acquisizione ed analisi è cosa ardua, poiché non esiste una ricetta, un protocollo definito e definitivo, quindi l'unica via è quella di applicare il metodo scientifico.

2 Il metodo scientifico nella computer forensics

Come per ogni attività forense, anche il repertamento e l'analisi dei dispositivi digitali, deve seguire i dettami della scienza, ossia la verificabilità, la ripetibilità, la misurabilità, la falsificabilità di una tesi e l'uso di strumenti comprovati dalla comunità dei *peers*.

Spesso si pensa che l'informatica sia una mera applicazione di qualche colpo di mouse e di azioni di copia ed incolla, ma non è così, l'informatica forense deve seguire delle regole al fine di garantire e giustificare la *fonte di prova digitale*.

Al fine di raccogliere le fonti di prova informatiche in modo rigoroso, si deve optare per una metodologia che utilizzi che permetta la giustificazione di ogni azione compiuta.

2.1 Le fasi

2.1.1. L'acquisizione

In questa fase lo scopo è quello di rendere un reperto informatico acquisibile il più possibile fedele all'originale, laddove possibile.

Nel caso degli hard disk si adotterà la copia bit a bit, ossia il disco sarà riprodotto su un file immagine, partendo dal suo primo bit sino all'ultimo, questo procedimento garantirà la copia esatta del disco, infine si dovrà applicare una o più funzioni di hash (MD5, SHA1, ecc.), che generano un codice univoco e non invertibile, allo scopo di verificare se la copia sia identica all'originale.

Nel caso dei dispositivi mobili, telefoni, tablet, ecc. Si agirà utilizzando i prodotti, generalmente commerciali, che possono "entrare" nel dispositivo ed effettuare una copia binaria del dispositivo; chiaramente per loro natura, l'acquisizione di questi dispositivi è sempre da effettuare in regime di irripetibilità, poiché sono soggetti a modificazioni, sia pure per il livello di carica della batteria, quindi nel caso dei apparati mobili, il metodo è abbastanza limitato, perché non c'è una tecnologia standard uguale per tutti, perciò ci si deve affidare agli strumenti che sono sul mercato (UFED, Oxygen, XRY,ecc.)

Nel caso di un sistema live, ossia acceso, l'irripetibilità è d'obbligo, quindi si procederà ad una copia forense del disco, da sistema acceso, alla fine della copia, tutti lavoreranno su quella, ma prima di effettuare la copia del disco, si deve procedere con l'acquisire tutti i *dati volatili*, come il dump della RAM, i processi, le connessioni di rete, ecc. seguendo un ordine ben preciso.

La fase d'acquisizione deve garantire che il reperto originale non sia alterato da eventuali scritture, quindi si adottano sistemi hardware come i write blocker e/o sistemi Gnu/Linux come C.A.IN.E. che permette un boot sul sistema indagato, senza "toccare" minimamente il disco originale.

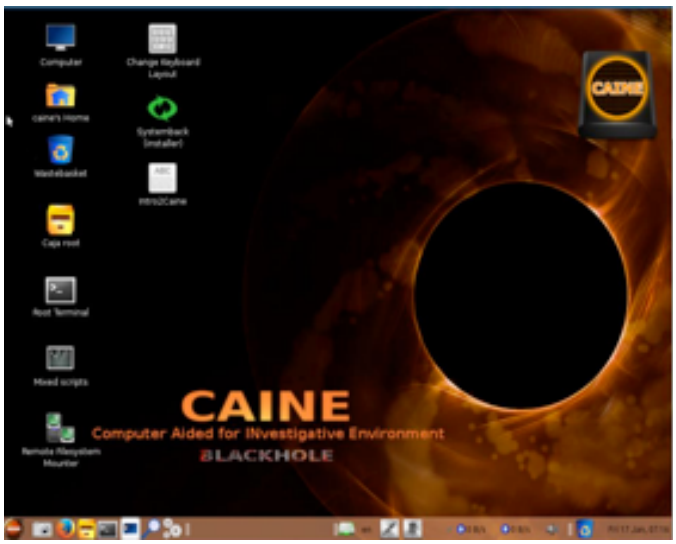

Figura 1 - Live distro forense CAINE

Figura 2 - Write blocker (Wikipedia)

2.1.2. L'analisi

Una volta acquisito il reperto, la fase d'analisi implica l'uso degli strumenti software più disparati, da quelli commerciali, ai freeware ed open source, chiaramente ogni scelta va giustificata e va dichiarato lo strumento adottato, sempre al fine della ripetibilità da parte di terzi che potrebbero voler verificare le evidenze trovate.

Nel caso si usino strumenti commerciali, l'importante è che siano accettati de facto dalla comunità scientifica internazionale, mentre su strumenti open source, sia sviluppati ad hoc dall'analista sia presi da fonti terze, va indicata la sorgente del software o allegato il codice sorgente laddove non fosse pubblicato.

A volte, nella fase d'analisi, è altresì importante, effettuare ricerche, reverse engineering, confrontarsi con esperti internazionali, e riportare anche i loro pareri, la bibliografia e la metodologia utilizzata per raggiungere il risultato.

Ultimo, ma non meno importante aspetto, è quello dedicato al tentativo da parte dell'analista di confutare se stesso, così da poter blindare i risultati ottenuti o prepararsi delle risposte a domande che potrebbero considerare aspetti meno probabili, ma comunque possibili che contestino l'analisi condotta o le risultanze.

2.1.3. Preservazione e reporting

Dopo la fase d'acquisizione, bisogna preservare il reperto con delle metodologie ben precise, prima di tutto la catena di custodia, ossia tener sempre traccia degli spostamenti del reperto e poi effettuare sempre una copia della copia, sulla quale si andrà a lavorare.

Il reporting è la fase in cui si deve stilare la relazione tecnica, che deve esser scritta in maniera semplice e comprensibile, giustificando ogni passaggio e spostando le parti più "tecniche" negli allegati.

Conclusioni

Sarebbe auspicabile possedere una cultura tecnica informatica o ingegneristica, per il semplice fatto che un consulente tecnico di digital forensics è sostanzialmente un tecnico appunto.

In questa materia si affrontano varie branche dell'informatica, file system, database, reti, linguaggi di programmazione, web, social networks, malware, sistemi mobili, insomma un po' di tutto, quindi qualcuno che viene da una lunga gavetta magari da programmatore, poi sistemista, navigatore del web, sempre aggiornato sui nuovi fenomeni e sistemi informativi sarebbe l'optimum, inoltre anche qualche nozione legale come la conoscenza degli articoli 359 c.p.p e 360 c.p.p., la legge 48/2008 oltre che del DPR 115/2002 non sarebbe male, ricordando sempre che un consulente tecnico è un tecnico non è un legale, non è uno criminologo, non è uno psicologo, non è un investigatore nel senso classico, ma una persona che deve dimostrare il come ed il perché ha trovato delle evidenze o fonti di prova digitali, preservando il reperto originale da alterazioni, utilizzando tecniche e strumenti approvati o riutilizzabili da terzi, non inventando nulla che non sia dimostrabile scientificamente e, laddove possibile, ripetibile.

Tutto questo è affrontabile anche da chi non ha una cultura di base, a patto che si impegni molto nello studiare, sperimentare, confrontarsi ed avere la tenacia di affrontare nuove sfide intellettuali, specialmente nell'aggiornarsi costantemente, vista la velocità del progresso tecnologico.

In sostanza, non bisogna accontentarsi di una certificazione privata, di un corsetto, di qualche software *friendly* e saper solo premere qualche pulsante, ma a volte anche scontrarsi con materie ostiche come la matematica, la crittografia, la logica, cose che potrebbero ostacolare qualcuno che magari le aveva lasciate sui libri del liceo e non più bazzicate per anni ed anni finché non ha deciso di essere preda del demone della digital forensics.

Queste considerazioni sono state ispirate dall'osservazione dalla costante crescita di chi si avvicina alla materia in oggetto e di ci lavora; molti bravi lavorano su casi importanti altri bravi sono relegati a ruoli minori, molti blasonati non si sa nemmeno perché lo siano e spesso si sentono di errori pazzeschi da parte di consulenti tecnici, che nonostante queste cialtronate, continuano ad essere ingaggiati da Procure e/o privati, non c'è un protocollo ben definito, non c'è un albo, una certificazione riconosciuta da chi "ingaggia", non c'è unione ,ed a volte stima, anche tra i singoli o i gruppi che si occupano di questo, insomma tutto normale, tutto italico, però colpisce il vedere o sentire di gente che fino ad un paio di anni fa a malapena sapeva cosa fosse un byte e poi si è ritrovata a lavorare su di una disciplina così complessa e così ricca di cultura tecnico/informatica, perciò e per anni di letture e discussioni su CFI (Computer Forensics Italy, una grandissima community dedicata alla digital forensics), abbiamo voluto stilare questi requirements non sufficienti ma sicuramente necessari ad iniziare un percorso da indagatori del bit.

Bibliografia

[Bassetti, 2011] Indagini Digitali – Nanni Bassetti – 2011 Lulu.com.

[AICA 2013] Congresso Nazionale AICA 2013.

[Brian Carrier 2005] File System Forensics Analysis – Addison Wesley Professional

[Cory Altheide,Harlan Carvey] Digital Forensics with Open Source Tools – Syngress Elsevier - 2011.

Biografia

Nanni Bassetti è Laureato in Scienze dell'Informazione a Bari ed è libero professionista specializzato in informatica forense. Ha collaborato come free-lance con molte riviste informatiche nazionali e internazionali e come docente per molti corsi presso enti, scuole e università, ha inoltre scritto articoli divulgativi di programmazione, web usability, sicurezza informatica e computer forensics. Ha lavorato come ausiliario di Polizia Giudiziaria e per alcune Procure della Repubblica oltre che come CTU/CTP per molte analisi forensi informatiche civili e penali. Iscritto all'albo dei C.T.U. presso il Tribunale di Bari, è consulente di parte civile per alcuni casi di risonanza nazionale. Fondatore di CFI - Computer Forensics Italy - la più grande community di computer forensics italiana. Membro fondatore di ONIF (Osservatorio Nazionale Informatica Forense) www.onif.it. Project manager di Caine Linux Live Distro forense. Curatore del sito Scripts4cf dedicato a software per la computer forensics. Ha pubblicato "Internet Web Security – tutta la verità sulla sicurezza del web" nel 2004 con la Duke Editrice e il libro "Indagini Digitali".

Email: nannib@libero.it