IL FUTURO DELLA DIGITAL FORENSICS

di Nanni Bassetti

❶ *Introduzione*

La Digital Forensics è quella disciplina scientifica che regola l'identificazione, l'acquisizione, la preservazione, l'analisi ed il *reporting* di fonti di prova digitali al fine di renderle utilizzabili in un processo giuridico. L'unico protocollo applicabile è il metodo scientifico, ovvero la modalità tipica con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile (da Wikipedia). 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. Le fasi della Digital Forensics sono: identificazione, acquisizione, preservazione, analisi, reporting. Le copie *post mortem* di un dispositivo di memorizzazione di massa, laddove possibile, vanno effettuate *bit-a-bit* con verifica di codice *hash*, una funzione matematica che genera un codice univoco e non reversibile.

Tutto questo è il presente, ma probabilmente potrà diventare presto il passato, perché nel futuro della Digital Forensics si cominciano a intravedere scure nubi, formate da ostacoli di non piccolo cabotaggio. Durante le vostre ricerche potrete imbattervi in alcuni di questi *baubau* della Digital Forensics, vere e proprie innovazioni tecnologiche e culturali, che potrebbero spazzar via tutto quello che finora si è cercato di consolidare.

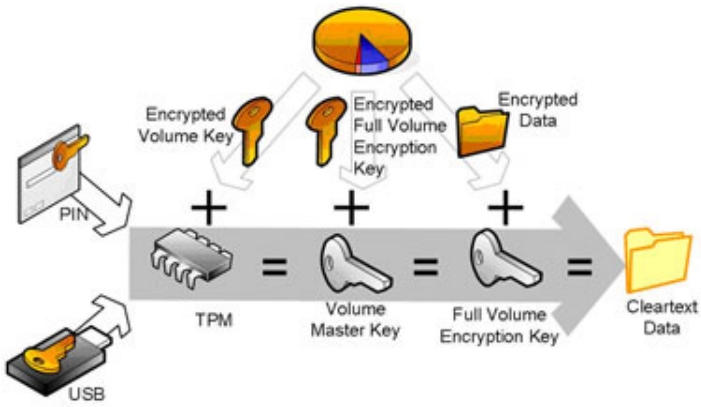
❷ *I dischi auto-criptanti e auto-cancellanti*

Al giorno oggi dobbiamo constatare la presenza sul mercato di particolari *hard disk* che, una volta inizializzati su un computer tramite dei microcodici nei loro *firmware*, raccolgono alcune informazioni sul sistema ospite, sicché nel momento in cui dovessero esser spostati su un altro sistema, anche solo ai fini di effettuare una copia forense ed anche con l'uso del *write blocker*, questi potrebbero far partire una procedura interna di *self-crypting* o *self-wiping*, il che significherebbe perdere irrimediabilmente i loro contenuto.
Nel caso in cui un modello di *hard disk* con il *self-encryptig* sia rubato e tenti di connettersi a un sistema non-familiare, il disco rigido e l'*host* iniziano un processo di autenticazione. Se il tentativo di autenticazione ha esito negativo, il disco può essere configurato per negare l'accesso o cripto/cancellare i dati sensibili.

Self-Encrypting Drives (SED) equipaggiati con *Toshiba Wipe Technology*

❸ *BitLocker Drive Encryption*

I vostri dati sono protetti con crittografia dell'intero volume del sistema operativo Windows. Se il computer è dotato di un TPM compatibile, BitLocker utilizza il TPM per bloccare le chiavi di crittografia che proteggono i dati. Di conseguenza, le chiavi non sono accessibili finché il TPM ha verificato lo stato del *computer*. La crittografia dell'intero volume protegge tutti i dati, compreso il sistema operativo, il registro di Windows, i *files* temporanei, e il *files* di ibernazione.
Le chiavi necessarie per decriptare i dati rimangono bloccati dal TPM, quindi un attaccante non può leggere i dati semplicemente rimuovendo il disco rigido e installandolo in un altro computer. Il TPM è un *microchip* progettato per fornire funzioni relative alla sicurezza di base, che coinvolgono principalmente le chiavi di crittografia. Il TPM è di solito installato sulla scheda madre di un *computer desktop* o portatile, e comunica con il resto del sistema usando un *bus hardware*.
Computer che incorporano un TPM hanno la capacità di creare chiavi crittografiche e crittografare loro in modo che possano essere decifrati solo dal TPM. Se anche si riuscisse a ricavare una *key* per il *decrypting* poi servirebbe anche l'eventuale *password* per l'*unlock* del disco.



Fonte: *http://lacy.hu/windows_vista/biztonsagi_ujdonsagok*

"Se durante l'avvio del computer viene rilevata una condizione che potrebbe rappresentare un rischio per la protezione, ad esempio errori del disco, una modifica al BIOS o a un qualsiasi file di avvio, BitLocker blocca l'unità e richiede una password di ripristino speciale per sbloccarla. Assicurarsi di creare la password di ripristino quando si attiva BitLocker per la prima volta, altrimenti potrebbe non essere più possibile accedere ai file.
BitLocker utilizza in genere il chip Trusted Platform Module (TPM) nel computer per archiviare le chiavi utilizzate per sbloccare il disco rigido crittografato. Quando si accede al computer, BitLocker richiede a TPM le chiavi per il disco rigido e lo sblocca. Poiché TPM invia le chiavi a BitLocker immediatamente dopo che è stato eseguito l'accesso al computer, la protezione del computer dipende dalla complessità della password di accesso. Se è stata creata una

password complessa che impedisce l'accesso agli utenti non autorizzati, il disco rigido protetto tramite BitLocker resterà bloccato" (da http://windows.microsoft.com/it-it/windows-vista/help-protect-your-files-using-bitlocker-drive-encryption).

"*Con Windows 8.1 la crittografia del disco è sempre attiva. Microsoft ha infatti deciso di applicare la protezione crittografica ai tablet o ai PC usando la funzione "device encryption" in modo automatico - in passato invece era l'utente a dover attivare la crittografia manualmente*" (da http://www.tomshw.it/cont/news/windows-8-1-crittografia-e-sicurezza-facile-per-tutti/50108/1.html).

❹ *SSD e l'auto corrosione*

I dischi allo stato solido subiscono il fenomeno dell'"auto-corrosione", ossia quando si cancella un *file*, il comando TRIM del sistema operativo dice al *controller* del disco di cancellarlo, quindi il *file* va nella *garbage collection*. Poichè gli SSD seguono la regola del *wear leveling* e per cancellare un *file* devono prima scrivere, le operazioni di cancellazione non sono in tempo reale, ma in *background* e gestite dal *controller*, poi una volta cancellati i blocchi, non si recupera più il *file*, poiché sovrascritto.
Quindi, quando si stacca un SSD e lo si attacca ad un altro computer, il *write blocker* non blocca l'auto-corrosione, dato che il fenomeno si attiva dall'interno, appena il *controller* riceve corrente elettrica. L'unico sistema per *bypassare* questo problema è quello di effettuare il *chip-off*, ossia il dissaldamento dei *chip* di memoria del disco ed il conseguente *dump*, con tutta la difficoltà che ne deriva, sia tecnica sia di ricostruzione dei dati.

❺ *Altro*

A questa lista si aggiungono altre difficoltà: i dispositivi mobili (cellulari, *tablet*, ecc.) sono tanti e in differenti modelli, i sw/hw per il dump e le analisi sono pochi, limitati e costosi e con aggiornamenti lenti rispetto all'uscita impetuosa di nuovi modelli e sistemi operativi. Inoltre, molti dati sono attualmente sui *Cloud*, quindi sparsi su più *server* nel mondo.

- ***Investigator weakness*** – sempre più Gb/Tb da gestire, costi, complessità, si parla di dischi di parecchi gigabyte o terabyte, Raid, usare tecniche di *data hiding* e a quel punto le analisi da condurre porterebbero via moltissime risorse in termini di tempo e denaro, costringendo l'investigatore a lavorare con serie difficoltà.

- ***Awareness*** – Aumentano le competenze e la consapevolezza tecnica degli utenti: oggi criptano, cancellano in maniera sicura, usano pw, *data storare online*, macchine virtuali, TOR, TrueCrypt, PGP, AxCrypt, Bitlocker, Live distro, Secure Eraser, Wipe, Ccleaner, Disk Eraser, UPX, ecc.

- ***ATA HDD PW*** – una banalità anche se vecchia ma ancora un bell'ostacolo. Ci sono due modalità di ATA Password security, HIGH e MAXIMUM, se la security è HIGH si può sbloccare il disco con la password USER o quella MASTER (di fabbrica), se è MAXIMUM solo con la password USER.

❻ *Esempi e conseguenze*

Una conseguenza dell'uso di questi strumenti è che la regola del *pull-the-plug* (staccare la spina) su apparati accesi, va rivista e meditata, visto che dopo lo spegnimento ci si potrebbe trovare di fronte ad un sistema completamente criptato o inaccessibile.

Usare TOR su un *computer* implica render le proprie navigazioni ed iscrizioni a siti completamente anonime, infatti, la navigazione con TOR attivato non lascia tracce sul computer, si possono raggiungere siti che esistono solo nella *anonymity network* e non raggiungibili dal normale *web*, ma presenti solo sul *deep web o dark web*, una serie di servizi (*hidden services*) e siti funzionanti solo sui *computer* degli utenti e non registrati su alcun DNS e ogni collegamento è criptato. La moneta utilizzata è il bitcoin o il litecoin, cripto-valute virtuali peer-to-peer, senza intermediari appunto, che rendono pressoché impossibile la tracciatura.
Dulcis in fundo, esiste anche una *gnu/linux distro* chiamata TAILS, che permette un *bootstrap* da pendrive o dvd-rom, già configurata per l'utilizzo di TOR e altri servizi di anonimizzazione e che non lascia alcuna traccia su *hard disk* o su *pendrive*, considerando che all'uscita opera un *wiping* (cancellazione sicura) di ogni residuo d'informazione (questo per la versione su *pendrive usb*).

❼ *Conclusioni*

La nostra L. 48/2008 recita in più articoli:
"*...quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.*".

Inoltre: "*... In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti*".

Di fronte a tali tecnologie e mutamenti culturali, va da sè che l'operatività dell'investigatore informatico sarà sempre più limitata e difficoltosa; molti dati andranno dispersi o non saranno recuperabili e quello descritto in questo contesto è solo la punta dell'*iceberg*, perché sicuramente nasceranno nuove tecnologie e sistemi di difficile approccio, mentre la tecnologia a disposizione dell'investigatore ha un andamento molto più lento, considerando che molti strumenti *software* sono ricavati da *reverse engineering* e che non riescono ad aggiornarsi così velocemente.
L'unica costante nell'evoluzione e nella *race condition* tra strumenti forensi e mondo informatico in veloce divenire e mutamento è l'uso del nostro cervello, della metodologia scientifica e del *problem solving*. Gli operatori dovranno cercare di adattare i loro mezzi e le loro conoscenze al fine di trarre il massimo delle informazioni possibili, anche se non si utilizzeranno i metodi finora conosciuti, il viaggio è cominciato, le nubi si avvicinano, apriamo gli ombrelli dunque! ©