

# Panoramica generale

## Che cos'è la Computer Forensics?

È difficile dare una semplice e univoca risposta a questa domanda, perché “Computer Forensics” è un'espressione diffusamente impiegata, ma la sua definizione non è ancora del tutto standardizzata. La materia è approdata da poco nelle aule di tribunale ed è in continuo sviluppo. Gli stessi addetti ai lavori, in Italia, hanno al proposito opinioni poco concordi se non, per certi versi, del tutto opposte.

Una possibile definizione sufficientemente universale di “Computer Forensics” potrebbe essere:

“La disciplina che si occupa della preservazione, dell'identificazione, dello studio, delle informazioni contenute nei computer, o nei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigativa”.

Tenendo come riferimento questa definizione generica, nel presente volume si cercherà di esaminare approfonditamente l'argomento per vederne le applicazioni pratiche.

Innanzitutto si ha a che fare, senza dubbio, con una nuova specializzazione dell'attività di polizia scientifica – al pari della balistica, della genetica, dell'entomologia applicate –, che entra in gioco nel momento in cui le evidenze dell'azione criminosa sono reperibili “nel mondo digitale”.

Il concetto, espresso in questo modo, potrebbe anche sembrare una frase di Morpheus in Matrix (“Questo è Struttura, il nostro programma di caricamento”),

## In questo capitolo

- **Che cos'è la Computer Forensics?**
- **Applicazioni della Computer Forensics**
- **Una metodologia forense**
- **Una filosofia di lavoro**

una cosa da relegare alla fantascienza o nella vita di qualche hacker; una disciplina, quindi, che trova la sua dimensione nell'individuazione dell'ennesimo diffusore di virus, del cracker che ha violato una celebre banca online, o di qualche altro aleatorio personaggio "abitante" la rete Internet. Tuttavia si sarebbe lontani dalla realtà. Non è difficile capirlo, basta guardarsi attorno. Siamo letteralmente contornati dalla tecnologia. Oramai si trovano computer ovunque. Certo, non sempre hanno una forma canonica che li rende immediatamente riconoscibili, ma la loro diffusione è molto più pervasiva di quanto si possa pensare.

Si esaminino alcuni esempi volti a chiarire il concetto.

Le moderne console per videogiochi sono diffusissime. Sony ha dichiarato di aver venduto, oltre 200 milioni di PS2. Xbox di Microsoft non ha certo raggiunto risultati molto diversi. Le nuove console, Xbox360 e PS3, promettono di abbandonare il solo scopo video-ludico per diventare strumenti molto più potenti: è l'avverarsi della previsione di Bill Gates ("un PC in ogni casa"), realizzata sotto mentite spoglie.

Lo stesso può dirsi del mondo della telefonia mobile. Definire semplice *cellulare* uno smartphone basato su un sistema operativo Symbian, Windows Mobile, Mac OS X o Palm OS è quantomeno riduttivo. Tutti questi oggetti sono dei veri e propri computer nei quali finiscono le informazioni più disparate.

Il recentissimo fenomeno dei netbook è un ulteriore esempio di quanto esposto sinora. Asus, con la serie EEE PC, sembra essere riuscita sorprendentemente a trovare una nuova branca dell'informatica. L'entusiasmo con cui il netbook è stato accolto dalla clientela e la velocità con cui i concorrenti si sono lanciati nella progettazione di nuovi dispositivi di questo genere fa ben pensare che non si tratti di una moda passeggera, ma un fenomeno destinato a durare e, probabilmente, a soppiantare i palmari.

Anche le moderne automobili dispongono spesso di sistemi di intrattenimento molto sofisticati che, in definitiva, altro non sono che PC adibiti a uno scopo preciso.

Ritornando al computer nella sua forma più tradizionale, si pensi a quanto Apple ha spinto sul concetto di "digital hub" con la sua suite di programmi iLife, creati allo scopo di gestire in modo digitale i ricordi più cari delle persone. Oppure si pensi con quale velocità la fotografia digitale, nel momento in cui è diventata matura, ha soppiantato quella tradizionale su pellicola, specialmente tra gli utenti amatoriali.

Che cosa comporta tutto ciò? Comporta il fatto che da molto tempo la tecnologia non è più appannaggio degli hacker. "L'uomo della strada" usa la tecnologia in molti ambiti della propria vita personale. Nonostante l'uso di un personal computer rimanga più complesso di quello di un qualunque altro elettrodomestico, alcune sue diverse incarnazioni, come un mediacenter, uno smartphone o un hard disk recorder per la televisione sono tranquillamente accettate nella vita comune.

Viene quindi naturale pensare al fatto che se in una *scena criminis* si rinviene un qualunque dispositivo tecnologico, esso debba essere analizzato come tutto il resto del materiale presente, indipendentemente dal tipo di crimine che è stato perpetrato. I legami tra un qualsiasi dispositivo hardware e un crimine possono sfuggire nell'immediato, ma possono rivelarsi evidenti al momento dell'analisi.

Come appena osservato, oramai qualunque scena del crimine pullula di dispositivi high-tech. Nasce quindi il problema, oltre ovviamente a quello della loro identificazione (cioè del loro pronto riconoscimento, non sempre banale), di una corretta gestione delle informazioni che questi oggetti possono contenere.

E qui il divario tra quanto normalmente accade con gli oggetti di uso comune è tragicamente enorme. Negli ultimi anni, note serie televisive aventi come protagonista la polizia scientifica, quali “C.S.I.” o l’italianissimo “R.I.S.”, hanno tenuto milioni di telespettatori incollati agli schermi. Per la prima volta i “topi di laboratorio” sono stati presentati come personaggi accattivanti e dinamici e non solo come scienziati chini a esaminare cose incomprensibili. Ebbene, tutti avranno notato la cura con la quale le prove vengono collezionate, preservate e ispezionate. Il granellino di sabbia, l’impronta digitale, la scritta a matita su un foglietto, il liquido organico sono gelosamente custoditi per evitare la benché minima alterazione, nella speranza che portino a una svolta determinante nelle indagini.

Eppure, anche in queste serie, per lo più precise in campi come genetica, fisica o entomologia, si vedono i protagonisti accendere con consumata leggerezza i computer degli indagati o delle vittime, alla ricerca di prove. Tutto ciò non è per nulla strano: ogni giorno molti appartenenti alle forze di polizia, in diversi Paesi, si comportano in maniera analoga nei confronti delle apparecchiature tecnologiche rinvenute sulla scena di un crimine. Questo comportamento è errato e deleterio, e spesso ha causato un arresto o una compromissione dell’indagine.

## Applicazioni della Computer Forensics

Qualunque dispositivo tecnologico possieda un sistema di memorizzazione di informazione, sia esso una macchina fotografica digitale, un computer, un palmare o una console per videogiochi, va gestito e controllato come se intersecasse due realtà ben distinte. In effetti, esso è costituito da una parte fisica e una parte logica, che sono ambedue importanti (spesso la seconda più della prima) e necessitano della dovuta attenzione.

La parte fisica è semplice da comprendere. La si può vedere, toccare con mano, percepire con i sensi. È facile, quindi, comprendere come vi si possano trovare impronte digitali, residui organici (una ricerca ha dimostrato che in una comune tastiera usata in ufficio si possono trovare più batteri e particelle di sporco che in un bagno pubblico).

La parte logica, digitale è la ragione di vita di un *computer forensics expert*. Si pensi a una prova fisica aleatoria, come un’impronta. Rovinarla esaminandola è estremamente semplice nonché disastroso. Richiede una cautela quasi maniacale.

Ora si pensi a un file. Un file non è un concetto materiale. È una semplice astrazione logica. Non ha una sua natura fisica. Un file può essere copiato, esistendo quindi su più supporti fisici diversi. Un file non può essere rubato, almeno non nel senso classico del termine: se ne prendo la copia e lascio l’originale al suo posto non ho sottratto nulla al suo legittimo proprietario. Un file può essere alterato, ma come si può dimostrare l’alterazione di qualcosa che esiste solo a livello logico? Anche riportandosi alla sua rappresentazione su un supporto magnetico, è impossibile riuscire ad arrivare a un livello così dettagliato da dimostrare che, per esempio, una particella di materiale magnetico ha cambiato il suo orientamento. Questo diventa ancora più aleatorio nel momento in cui il file risiede su un supporto come un chip di memoria RAM. Esso viene continuamente modificato dal refresh della memoria, dal fatto che il sistema operativo decide di spostarlo in un’altra locazione di memoria o sul file di swap. Un calo di tensione lo può irrimediabilmente distruggere o alterare.

**NOTA**

Un file di swap, detto anche file di scambio, è una porzione di disco fisso utilizzata come memoria quando il sistema operativo esaurisce la memoria di lavoro fisica; il file può essere permanente, nel qual caso viene utilizzato uno spazio contiguo dell'hard disk, o temporaneo, cioè viene utilizzato lo spazio su disco solo se questo è disponibile.

Si potrebbe continuare all'infinito con esempi sulla stessa falsariga, ma una cosa dovrebbe ora apparire lampante. Un dispositivo elettronico non può essere acceso e gestito con leggerezza da parte del computer forensics expert. Vista l'immaterialità della prova, la sua distruzione o alterazione può avvenire per una miriade di motivazioni diverse.

La nostra società si basa quasi esclusivamente su informazioni digitali. Il nostro mondo reale ha fortissimi legami con quello digitale. Banalmente, si provi a effettuare un'operazione bancaria nel momento in cui il sistema informativo ha deciso di non funzionare: i nostri soldi reali non risultano disponibili, perché la loro rappresentazione digitale non è utilizzabile.

Per tale motivo è quindi evidente che molte prove riguardanti crimini del tutto reali, compresi omicidi, attentati terroristici, frodi o rapimenti, possono risiedere su apparati digitali. Si pensi a titolo di esempio alle webcam o alle telecamere di sorveglianza che registrano dati su hard disk.

Questo è il compito principale della Computer Forensics; ovvero, riprendendo la definizione citata all'inizio del capitolo: "occuparsi della preservazione, dell'identificazione, dello studio della documentazione contenuta nei computer, o nei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigativa".

Ora il concetto dovrebbe essere più chiaro, così come un po' più evidenti dovrebbero già essere gli errori grossolani commessi dagli investigatori delle serie televisive e, purtroppo, delle forze di polizia di molti Stati.

## Una metodologia forense

Come dichiarato in precedenza, la Computer Forensics è una nuova branca della polizia scientifica. Il suo fascino e il suo limite massimo risiedono nel fatto di essere, appunto, "nuova". È un fascino, sicuramente, per il fatto che a ogni nuovo caso si scoprono nuovi metodi di analisi e di approccio alla situazione; è un limite perché la stessa evidenza, affidata a periti diversi o addirittura allo stesso forensics expert in due tempi diversi, potrebbe produrre risultati totalmente opposti.

Tutto questo è ovvio. L'esperienza aiuta a migliorare e a progredire nella materia specifica. Chi scrive è assolutamente convinto che se potesse ritornare ora su alcuni dei casi affrontati qualche anno fa otterrebbe risultati di gran lunga migliori.

Sfortunatamente, non è un problema solo di efficienza o di efficacia. In molti casi si evidenziano dei comportamenti palesemente sbagliati che inevitabilmente si traducono, in fase di dibattimento, nell'invalidazione della prova. Si immagini il danno che questo può arrecare, specialmente se l'errore è avvenuto già nella fase di acquisizione della prova stessa.

Ciò che è assolutamente necessario è un metodo di lavoro che permetta di evitare a ogni forensics expert di passare il tempo a reinventare le stesse cose o di rifare gli stessi

errori che altri suoi colleghi hanno già compiuto. In questo modo si potrebbe ottenere una serie di vantaggi.

- *Normalizzazione dei risultati.* Applicando la stessa metodologia sarebbe possibile ottenere risultati molto simili pur rivolgendosi a periti diversi, almeno per le fasi più di routine, come l'acquisizione delle evidenze.
- *Minore dispersione di energie.* La mancanza di comunicazione e una legislazione assolutamente assente fanno sì che ogni singolo forensics expert debba affrontare gli stessi problemi già affrontati da altri e debba trovarvi soluzione. Ciò, inevitabilmente, complica il lavoro e ruba tempo ed energie all'unica fase in cui la personalità del perito può davvero esprimersi, ovvero quella dell'analisi delle evidenze.
- *Minori possibilità alla controparte.* Applicare un metodo che abbia già superato più volte le forche caudine del dibattito eviterebbe di dare agio agli avvocati di parte avversa di trovare un vizio di forma o un cavillo legale che possa invalidare tutto il lavoro svolto.
- *Verificabilità dei risultati.* Come si avrà più volte modo di sottolineare, l'uso di un metodo comune permetterebbe inoltre ai periti di parte avversa di controllare in maniera più semplice e incontrovertibile i risultati ottenuti dagli investigatori.

In questo testo si cercherà, per quanto possibile, di fornire un metodo di lavoro che si possa applicare a ogni singolo caso e che risulti indipendente sia dagli strumenti (*tool*) di analisi utilizzati, sia dalla tipologia di prova in esame.

Fissare un metodo non deve essere interpretato come un tentativo di "industrializzare" il lavoro. La variabilità delle situazioni è tale che ogni forensics expert potrà trovare spazio per esprimersi e dimostrare la sua competenza a ogni nuovo caso. Il metodo permette semplicemente di sveltire le fasi più noiose e ripetitive e di porre una base comune su cui cominciare l'analisi.

## Una filosofia di lavoro

In tutto il testo sarà possibile trovare ben più di un riferimento a strumenti di lavoro Open Source. Da molto tempo si trascina a questo proposito una diatriba, ovvero se sia meglio rivolgersi a strumenti commerciali oppure a software disponibili liberamente.

Tutto questo merita una riflessione. Non è possibile riuscire a gestire un ampio ventaglio di situazioni senza essere un minimo pragmatici. Invariabilmente, i limiti di una delle due scelte si faranno presto sentire. È quindi indubbio che si debba ricorrere a un approccio misto che tenda a trovare il meglio in quanto disponibile in entrambi i mondi.

Fissato questo concetto, è bene fare alcune precisazioni. Esistono infatti delle situazioni in cui è possibile scegliere liberamente fra un tool commerciale e un tool Open Source senza che ci sia una manifesta superiorità di uno o dell'altro. In questo caso verrebbe da considerare la scelta come del tutto arbitraria. Tuttavia, il software Open Source, in campo forense, ha dei vantaggi evidenti su quello commerciale.

Innanzitutto è disponibile in formato sorgente. Può sembrare un particolare scontato o irrilevante, ma potrebbe essere vitale in dibattito. Le funzioni del software sono infatti come una scatola nera: prendono in pasto dei dati e forniscono dei risultati. Non è possibile capire esattamente i meccanismi interni preposti a questo processo se il programma è compilato, ovvero intelligibile solo dalla macchina. Specialmente nel caso

di software atti a validare una prova, ovvero a calcolare l'algoritmo di hash usato per la verifica, sia esso MD5 o una variante dello SHA, un avvocato potrebbe insinuare che tale software sia *tampered*, ovvero compromesso *ad hoc* per mostrare il risultato voluto. Con un software Open Source è semplice replicare: si scarica un'altra versione, si ricompila al volo e si dimostra che il software non è stato alterato.

Un altro vantaggio evidente è la possibilità di esaminare il formato dei file che sono utilizzati. Molti software commerciali utilizzano dei tag proprietari durante il salvataggio delle evidenze. Per quanto ciò possa consentire evidenti vantaggi, complica notevolmente le cose nel caso si voglia usare, per l'analisi, un software differente da quello usato per l'acquisizione. Questo, in parte, è uno dei motivi per cui alcune software house nel campo forense regalano la parte del loro software atta all'acquisizione: semplicemente sanno che la scelta del software di analisi sarà poi quasi obbligata. Detto per inciso, questa politica basata su considerazioni di marketing non è sicuramente molto utile per chi ha a cuore l'efficienza professionale. Legare un'indagine all'uso di un particolare strumento significa anche legare i risultati ai limiti di tale strumento. Non è una riflessione da trascurare.

Con il software Open Source questo non è un problema: è sufficiente vedere il codice per capire come sono strutturati i dati e potersi scrivere un convertitore nel momento in cui ciò si rendesse necessario.

Il software Open Source è inoltre distribuito senza vincoli. Nel caso specifico dell'analisi forense questo è un vantaggio enorme, perché il perito accorto ha la libertà di accludere ai risultati della propria analisi tutto il software utilizzato per arrivare al risultato evidenziato nella propria relazione, a tutto vantaggio della trasparenza e della verificabilità dei risultati dalla parte avversa.

Un ulteriore vantaggio è che il software Open Source è disponibile in Rete per periodi di tempo molto prolungati. Non sempre un procedimento si risolve nel giro di pochi mesi; anzi, un tempo molto più lungo è la norma. Che cosa succederebbe se la software house che ha scritto il programma che è stato utilizzato per l'analisi dovesse chiudere, nel frattempo? Oppure, più semplicemente, se dismettesse quel particolare prodotto per passare a un programma più evoluto? Sarebbe possibile ripetere l'analisi a distanza di anni? La maggioranza dei software Open Source è conservata in particolari repository gestiti da un software di versionamento. È quindi possibile ottenere non solo l'ultima versione del programma, ma anche tutte le versioni precedenti, ivi compresa quella usata per la specifica indagine. Inoltre, essendo disponibile sotto forma di codice sorgente, potrà essere ricompilata (magari con qualche minimo adattamento) per la particolare architettura hardware posseduta anni dopo.

Per questi motivi, e per altri che si discuteranno nei prossimi capitoli, l'approccio scelto è semplicemente quello di utilizzare software commerciale esclusivamente nel caso in cui non vi sia un software Open Source di pari livello che possa assolvere alla stessa funzione.

A ogni modo, per accogliere le obiezioni portate alla prima edizione di questo libro su un eccessivo sbilanciamento a favore dell'Open Source, in questa edizione sarà dato molto più spazio anche ai pacchetti commerciali integrati per questa attività, primo fra tutti X-Ways Forensics, che abbiamo avuto modo di apprezzare grandemente durante alcuni casi usati come test per la seconda edizione.