Capitolo 1

L'ambito della Digital Forensics

Obiettivi

Di seguito i temi principali che verranno affrontati nel corso di questo capitolo.

- Definizione e importanza della Digital Forensics.
- I diversi tipi di prove digitali e come vengono utilizzati.
- Le competenze, il training e i corsi di studio necessari per diventare un investigatore di informatica forense.
- Le possibilità di lavoro nel campo della Computer Forensics.
- La storia della Computer Forensics.
- Gli enti che, negli Stati Uniti e a livello internazionale, sono coinvolti nelle indagini di Computer Forensics.

L'espressione *Digital Forensics* indica il reperimento, l'analisi e l'uso di prove digitali in un'indagine civile o penale. La Digital Forensics (o Computer Forensics o informatica forense) non si limita ai computer come possibile fonte di prove; qualsiasi mezzo che possa memorizzare file digitali è una potenziale fonte di prove per un investigatore forense. La Digital Forensics coinvolge quindi l'esame di file digitali.
La Digital Forensics è una scienza, perché scientifiche sono le pratiche accettate utilizzate per acquisire ed esaminare le prove e stabilirne l'ammissibilità in tribunale. Inoltre, nel corso degli anni, gli strumenti utilizzati per reperire e analizzare prove digitali sono stati sottoposti a test scientifici. In effetti, il termine

In questo capitolo

- **Obiettivi**
- **Miti comuni sulla Computer Forensics**
- **Tipi di prove forensi digitali recuperate**
- **Quali competenze deve avere un investigatore forense?**
- **L'importanza della Digital Forensics**
- **Possibilità di lavoro**
- **Storia della Digital Forensics**
- **Training e istruzione**
- **Riepilogo**
- **Glossario**
- **Valutazione**

"forense" significa "adatto per l'attività giudiziaria". Da questa definizione si deduce che le prove digitali utilizzate in un'indagine devono essere acquisite, trattate e analizzate in modo corretto dal punto di vista forense: "corretto" significa che, durante l'acquisizione delle prove digitali e lungo tutto l'arco del processo investigativo, le prove devono rimanere nel loro stato originale. Inoltre, è necessario che sia registrato e documentato, nella forma della "catena di custodia", chiunque sia venuto in contatto con le prove.
A volte la Computer Forensics produce prove incriminanti utilizzate in casi penali; queste sono quindi prove a carico (incriminanti). Prove digitali possono anche essere prodotte a discarico, cioè per dimostrare l'innocenza di un accusato.

Miti comuni sulla Computer Forensics

Molti pensano che sicurezza informatica e Computer Forensics siano la stessa cosa, ma non è così. Questa è una delle tante convinzioni errate che circolano. La sicurezza informatica è proattiva e si concentra in particolare sulla protezione di sistemi informatici e dati sensibili, fra i quali possono rientrare proprietà intellettuali. La Computer Forensics è reattiva e la sua natura è investigativa, entra in gioco quando è possibile che sia stato commesso un crimine. Sicurezza e Computer Forensics si intersecano spesso nella risposta agli incidenti. Alcuni incidenti gravi, come la violazione di una rete, richiedono le competenze di un investigatore digitale forense, che cercherà di stabilire che cosa sia successo, quali danni siano stati provocati e, se possibile, identificherà chi abbia perpetrato quell'azione. Le competenze e le tecniche di Computer Forensics sono usate spesso per la raccolta di informazioni (*intelligence*), dove l'obiettivo può non essere un'incriminazione (per esempio: si esamina un dispositivo mobile per stabilire se una nazione usi un'app per profilare gli individui). Inoltre, le tecniche di Digital Forensics sono usate spesso per monitorare e raccogliere informazioni sull'uso di servizi di social media da parte di gruppi terroristici noti o potenziali. I paragrafi che seguono presentano alcune delle idee errate che circolano intorno alla Computer Forensics.

Mito 1: Computer Forensics e sicurezza informatica sono la stessa cosa

La sicurezza informatica è proattiva: mira a proteggere computer e dati da furti e da usi impropri. La Computer Forensics invece è reattiva e comporta la ricerca di prove digitali dopo che è stato commesso un crimine, per risolvere un caso e incriminare chi l'abbia commesso. La Computer Forensics può essere complementare alla sicurezza informatica, in particolare nel campo della risposta agli incidenti. Va notato però che la National Academy of Sciences ha classificato la Digital Forensics come un sottoinsieme della cybersecurity.

Mito 2: Computer Forensics è l'indagine sui computer

Capitoli successivi di questo libro dimostreranno che qualsiasi dispositivo in grado di memorizzare file può essere oggetto di esame da parte degli investigatori forensi. Per esempio, la SIM card di un telefono cellulare non è un computer, ma può contenere prove digitali importanti.

Mito 3: la Computer Forensics è l'indagine su crimini informatici

Una concezione erronea assai diffusa è che la Computer Forensics sia usata solo per risolvere crimini informatici, mentre in realtà è importante anche in indagini di omicidio, truffa, spionaggio industriale. Per esempio, il 16 aprile 2007 Seung-Hi Cho ha ucciso 32 persone e ne ha ferite molte altre nel campus del Virginia Polytechnic, poi si è suicidato. Gli investigatori forensi hanno esaminato il computer di Cho per ricostruire gli eventi che hanno portato al massacro. Hanno esaminato il suo account di email, `Blazers5505@hotmail.com` e la sua attività su eBay, sotto il nome di `blazers5505`. Gli investigatori di Computer Forensics hanno potuto stabilire con chi comunicava Cho e che cosa aveva cercato e acquistato online. Hanno anche esaminato il suo cellulare. Uno dei motivi della risposta rapida da parte degli esaminatori forensi è stata la necessità di stabilire se Cho avesse avuto dei complici.
Quando gli agenti federali hanno perquisito gli uffici della Enron verso la fine del 2001, hanno scoperto che i dipendenti avevano distrutto un gran numero di documenti. Gli esaminatori forensi hanno dovuto recuperare prove dai dischi dei computer. È stato stimato che la quantità di dati digitali recuperati fosse equivalente a 10 volte le dimensioni della Biblioteca del Congresso.

Mito 4: la Computer Forensics è usata in realtà per riesumare file cancellati

La finalità principale della Computer Forensics è recuperare e analizzare file con hardware e software di Computer Forensics e applicando una metodologia scientifica ammissibile in un tribunale. La Computer Forensics va ben oltre la capacità di riesumare file cancellati; con gli strumenti opportuni si possono recuperare anche altri file non facilmente accessibili. Inoltre, gli strumenti della Computer Forensics hanno capacità di ricerca e filtraggio estremamente efficaci. Molti strumenti offrono capacità di identificazione delle password e di decrittazione: tra questi strumenti rientrano, per esempio, FTK di AccessData e il suo Password Recovery Toolkit (PRTK).

Il principio di scambio di Locard

Edmond Locard (1877-1966), criminologo dell'Università di Lione, ha sviluppato una teoria che va sotto il nome di *Interscambio delle prove*, la cui premessa è che, ogniqualvolta un criminale entra in contatto con il suo ambiente, si ha un trasferimento incrociato di prove: "Dovunque passi, qualsiasi cosa tocchi, qualsiasi cosa lasci, anche inconsapevolmente, fungerà da testimonianza silenziosa contro di lui. Non solo le sue impronte digitali, o le impronte dei suoi passi, ma anche i suoi capelli, le fibre dei suoi vestiti, gli occhiali che rompe, i segni che lasciano i suoi attrezzi, la vernice che scalfisce, il sangue o lo sperma che deposita o raccoglie. Tutte queste cose e molte altre sono testimoni muti a suo carico. Queste sono prove che non dimenticano. Non si confondono per l'emozione del momento. Non sono assenti perché sono assenti testimoni umani. Si tratta di evidenze fattuali. Le prove fisiche non possono sbagliare, non possono giurare il falso, non possono essere totalmente assenti. Solo l'incapacità umana di trovarle, di studiarle e di comprenderle può diminuirne il valore"- Questa teoria vale anche per la Computer Forensics, dove l'investigatore deve essere consapevole di tutto l'ambiente con il quale il criminale può essere giunto in contatto. In altre parole, è importante che l'investigatore non si concentri solo su un laptop trovato in un appartamento, ma che pensi anche alle connessioni dal laptop, verso un router, verso dischi esterni e storage nel cloud.

Anche chiavette USB o CD nell'abitazione possono contenere prove importanti. Nomi e password di login possono essere scritti su foglietti di carta che si trovano nell'appartamento e possono essere fondamentali per accedere al sistema del sospettato, ai suoi file o a servizi Internet come la posta elettronica. Anche un DVR, usato per registrare trasmissioni televisive, è un mezzo di archiviazione che può contenere prove importanti. Il software EnCase di opentext supporta l'imaging e l'analisi di file memorizzati su un DVR. EnCase è uno strumento di imaging a bit-stream, che cioè produce una copia bit per bit dei supporti originali, compresi i file marcati per la cancellazione.

Tipi di prove forensi digitali recuperate

Mediante tecniche di Computer Forensics si può recuperare praticamente ogni tipo di file, da quelli di sistema a quelli creati dagli utenti, per esempio fogli di calcolo. La sezione seguente elenca alcuni dei file più importanti che possono essere recuperati e utilizzati nelle indagini; molti si possono recuperare anche se l'utente ha cercato di cancellarli.

Posta elettronica (email)

L'email è probabilmente il tipo più importante di evidenza digitale. È molto importante per vari motivi, fra cui i seguenti.

- Controllo, possesso, intenzioni.
- Catena degli eventi.
- Prevalenza.
- Inquinamento delle prove.
- Ammissibilità.
- Accessibilità.

Controllo, possesso, intenzioni

Nella Computer Forensics, stabilire controllo, possesso e intenzione è fondamentale perché le prove siano incriminanti. A volte non c'è nulla di più personale dell'email, che può mostrare le intenzioni del sospettato e della vittima. Nel caso di Sharon Lopatka, uccisa da Robert Glass, l'email è stata la prova più importante nella causa per omicidio. Glass e Lopatka si sono scambiati molte email prima di incontrarsi nella Carolina del Nord, dove Glass ha torturato e strangolato Lopatka. Le email andavano a sostegno delle dichiarazioni inquietanti, secondo cui tortura e omicidio sarebbero stati consensuali.
In casi che coinvolgono il possesso di pornografia infantile, l'accusato di solito sostiene di non avere saputo che quelle immagini erano presenti sul suo computer. L'accusa deve dimostrare che l'imputato sapeva della loro esistenza e che erano immagini di minori. Le email possono spesso dimostrare che le immagini erano state condivise dall'imputato con altri pedofili. Questo contribuisce a dimostrare la colpevolezza dell'imputato e consente di incriminarlo per possesso di immagini pedopornografiche e per l'uso di un computer per distribuire immagini illegali. Per stabilire che un'immagine che si trova su un computer è lo stesso file di immagine che si trova su un altro computer, si può utilizzare un procedimento che va sotto il nome di MD5 hashing.

Catena degli eventi

La ricostruzione degli eventi che hanno portato a un crimine è un aspetto importante della presentazione di un caso. Spesso un file di email contiene una catena di conversazioni, svoltesi nell'arco di vari giorni, e comprende ore, date, mittente e ricevente. Questo può contribuire a stabilire una catena di eventi.

Prevalenza

La posta elettronica è molto importante perché la usiamo molto per comunicare, perciò è molto presente nelle attività sia personali che di lavoro. Nell'indagine sulla Enron, sono state acquisite e indagate decine di migliaia di email. È possibile che una società di revisione dei conti dotata di una unità di Computer Forensics abbia anche una unità distinta con un gruppo di analisti che passano le proprie giornate soltanto esaminando l'evidenza fornita dall'email.

Inquinamento delle prove

L'inquinamento è l'occultamento, la distruzione, l'alterazione o la falsificazione delle prove ed è un reato grave. Nella causa *Mattel contro MGA Entertainment, Inc.,* il giudice distrettuale Stephen Larson ha stabilito che la giuria poteva ascoltare la testimonianza della Mattel secondo cui l'ex dipendente Carter Bryant aveva usato un'applicazione, chiamata Evidence Eliminator, per inquinare le prove prima di consegnare il suo computer agli avvocati nel 2004.
L'email è molto preziosa per gli investigatori perché, anche se l'accusato cerca di inquinarla sul proprio computer, rimane ancora accessibile da altre fonti. Per esempio, i messaggi si potrebbero trovare non solo sul computer del sospettato ma anche su quello del destinario. Inoltre è possibile emettere un mandato nei confronti di un servizio di posta elettronica perché consegni i file memorizzati sui suoi server. File di email si possono spesso acquisire anche da smartphone come gli iPhone e da altri dispositivi come un iPad o un MacBook.

Ammissibilità

Giudici e tribunali da anni accettano la posta elettronica come prova ammissibile. Cosa interessante, in un caso, *Rombom et al. contro Weberman et al.*, il giudice ha accettato come prova le stampe dei messaggi di posta; il querelante ha testimoniato di aver ricevuto le email dall'accusato e di averle stampate.

Accessibilità

A differenza di molte altre fonti di evidenza, per l'accesso alla posta elettronica di un individuo non è necessariamente richiesto un mandato di perquisizione. Il Dipartimento di Giustizia degli Stati Uniti ha sostenuto che, dopo che un'email è stata aperta, non è più protetta dallo Stored Communications Act (SCA). Anche se un giudice ha già respinto la petizione per una perquisizione senza mandato, il governo ha continuato a sostenere che quando l'email è nel cloud ha il diritto di accedervi liberamente. In base allo SCA, per le comunicazioni archiviate, come le email che risalgono a meno di 180 giorni prima, è necessario che le forze dell'ordine ottengano un mandato. Società come Yahoo!, Google e Microsoft hanno costituito un gruppo, denominato Electronic Frontier Foundation,

per opporsi con forza ai tentativi del governo in questo campo. Alcuni analisti pensano però che la legge potrebbe cambiare a favore del governo.
Comunque, quello che è chiaro è che l'email aziendale di un dipendente è proprietà del datore di lavoro. Un'azienda quindi può esaminare l'email di un dipendente senza il consenso di quest'ultimo. Nel 2009, nella causa *Stengart contro Loving Care Agency, Inc.*, la Divisione d'Appello della Corte Superiore del New Jersey ha ribadito che un datore di lavoro può accedere all'email di un dipendente e leggerla senza il consenso del dipendente, se quest'ultimo usa la tecnologia dell'azienda per accedere alla posta elettronica. Perciò, avere accesso alle comunicazioni via email spesso è più facile che avere accesso ad altri metodi di comunicazione.

Immagini

Esistono numerosi tipi di file di immagine. I formati più usati sono BMP (Windows bitmap), JPEG (Joint Photographic Experts Group), TIFF (Tagged Image File Format) e PNG (Portable Network Graphics). Le immagini sono particolarmente importanti nei casi di pedopornografia, sono anzi ancora più importanti oggi di quanto lo fossero 20 anni fa, perché le fotografie digitali presentano dettagli sul tipo di fotocamera utilizzata (dimostrando quindi il possesso) e spesso contentono dati GPS (Global Positioning System), che consentono di stabilire la posizione del dispositivo (per esempio, uno smartphone) e quando la fotografia è stata scattata. Questi metadati sono spesso associati alle fotografie scattate con uno smartphone. In generale i metadati di file di una fotografia digitale permettono di identificare marca e modello della fotocamera utilizzata, che sono informazioni preziose per gli investigatori. I metadati (Figura 1.1) sono informazioni su un file e possono includere le date di creazione, modifica e ultimo accesso, e a volte i particolari sull'utente che ha creato il file.

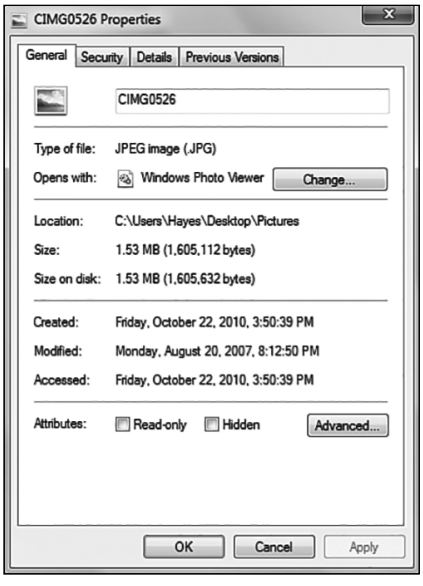

Figura 1.1 Metadati di un file.

La maggior parte dei software di imaging e analisi forense, fra cui l'applicazione FTK di AccessData, offre un'interfaccia utente che può filtrare le immagini per tipo e separarle. Questi file sono raggruppati e comprendono anche file di immagine estratti da altri file. Se, per esempio, un'email o un documento di Microsoft Word contengono un'immagine, l'applicazione può estrarla e raggrupparla con altre immagini che ha trovato.
Il software X-Ways Forensics e altri strumenti forensi consentono a un investigatore di filtrare tutte le immagini utilizzando come criterio una tonalità della pelle. Il risultato è che, dopo la ricerca, vengono presentate quasi esclusivamente immagini di persone. Le fotografie sono utilizzate da molti anni in tribunale, ma le immagini digitali oggi forniscono più informazioni delle immagini tradizionali su pellicola. Spesso, molti servizi online eliminano i metadati dalle fotografie digitali, perciò è possibile che un investigatore abbia bisogno di un mandato per ottenere le immagini che gli interessano nel formato originale (cioè complete di metadati). Nel Capitolo 10 parleremo più dettagliatamente dell'esame delle fotografie digitali.

Video

Prove video si possono trovare su molti tipi diversi di dispositivi, fra cui computer, fotocamere digitali, telefoni cellulari. Oggi i video di sorveglianza sono salvati in genere su computer e perciò ricadono nel campo dell'informatica forense. I video di sorveglianza spesso sono utili nel caso di furti a banche e negozi, ma vengono usati anche per molti altri tipi di attività criminali.
L'uso di skimmer ai bancomat ha reso possibili furti per milioni di dollari in tutto il mondo. Uno skimmer (Figura 1.2) è un dispositivo usato per catturare i dati memorizzati sulla banda magnetica di una carta bancomat, di una carta di credito o di debito. I video di sorveglianza possono essere fondamentali per catturare questo tipo di criminali.

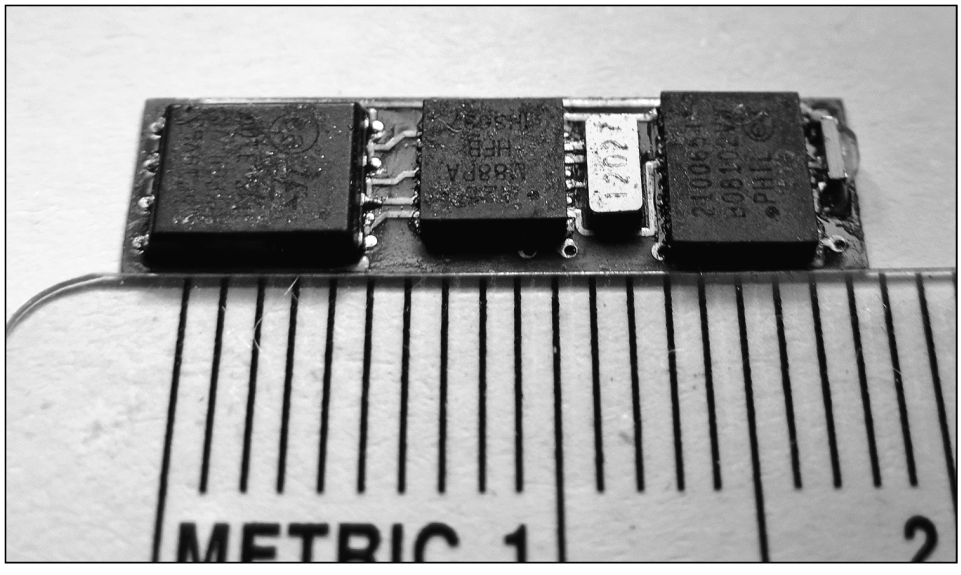

Figura 1.2 Dispositivo di skimming.

La televisione a circuito chiuso (CCTV, *Closed-Circuit TeleVision*) è l'uso di video trasmessi in una particolare sede. A Londra, per esempio, esistono oltre 600.000 videocamere CCTV, che sono state utilizzate per esempio nelle indagini su rapine ai danni di turisti e per casi di alto profilo come l'avvelenamento dell'ex spia russa Alexander Litvinenko nel 2006. Gli investigatori di Computer Forensics hanno a disposizione vari strumenti, fra cui alcuni che migliorano la qualità dei video da analizzare; altri creano fermi immagine personalizzabili in punti predeterminati di un video. Queste immagini sono preziose, perché possono essere incluse nei rapporti degli investigatori. Cosa ancora più importante, questi strumenti danno all'investigatore un metodo efficiente per identificare quando nel video compaiono evidenze incriminanti importanti, eliminando la necessità di guardare il video dall'inizio alla fine. Inoltre, se i contenuti video sono scioccanti, l'investigatore non è costretto a guardarli per intero. In tribunale, infine, i materiali video possono essere le prove più convincenti per la formulazione di una sentenza.

Siti web visitati e ricerche in Internet

È ancora viva, fra le forze dell'ordine, la discussione se si debba staccare la spina a un computer per conservare le evidenze nello stato originale o se un computer attivo debba rimanere acceso quando viene scoperto. Con i perfezionamenti delle tecniche crittografiche e la natura delle evidenze che si perdono se si toglie l'alimentazione, la maggior parte degli investigatori è convinta che un sistema attivo debba essere esaminato mentre è acceso. La cifratura è il processo per cui un testo in chiaro viene trasformato in un formato non leggibile, mediante l'applicazione di una formula matematica (un algoritmo). File che possono costituire evidenza e i dati relativi alle ricerche in Internet e ai siti web visitati sono più facilmente disponibili mentre il computer è acceso, poiché gran parte dell'attività corrente dell'utente, fra cui l'attività in Internet, è conservata in memoria ad accesso casuale (RAM, *Random Access Memory*). La RAM è chiamata anche memoria di breve termine o volatile, perché i suoi contenuti scompaiono quando viene tolta l'alimentazione. È importante sapere che, quando viene visitato un sito web, un computer client effettua una richiesta a un server web. Il client in effetti scarica un documento HTML e le relative risorse (come le immagini) dal sito web nella memoria del computer locale, come si vede nella Figura 1.3. La finalità principale di un server web è trasferire documenti HTML e le relative risorse in risposta alle richieste dei client. Si può pensare il client come un consumatore a cui il server fornisce un servizio. La maggior parte degli strumenti professionali di Computer Forensics possono creare effettivamente un'immagine dei contenuti della RAM mentre il computer è acceso. Sono disponibili anche vari strumenti open source di analisi della RAM.

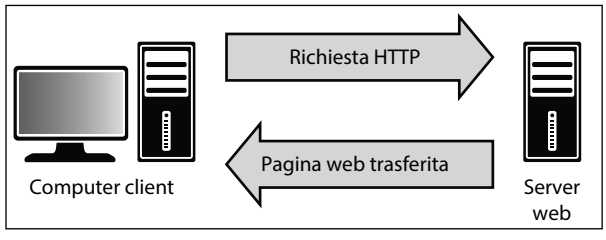

Figura 1.3 Comunicazioni fra un client e un server web.

Cellphone Forensics

Il campo dell'analisi forense per i telefoni cellulari, o Mobile Forensics, sta crescendo esponenzialmente, poiché le capacità dei dispositivi mobili continuano ad ampliarsi. Un telefono cellulare può dire quali persone il sospettato conosca (contatti), i suoi appuntamenti (calendario), con chi abbia parlato (tabulati delle chiamate) e che cosa abbia detto (messaggi di testo). Altri dispositivi possono fornire anche evidenze sotto forma di immagini e video (fotocamera incorporata), sui luoghi visitati (GPS), sugli acquisti effettuati online e sui siti web visitati (smartphone abilitati a Internet).
I telefoni cellulari sono usati spesso anche per tracciare i sospettati. Nel corso delle indagini sull'omicidio di Fred Jablin, il detective Coby Kelley ha ottenuto un mandato per la documentazione delle chiamate da cellulare della sospettata Piper Rountree. Poiché i ripetitori della telefonia cellulare tengono traccia del telefono di un utente mentre questi si sposta da una cella (un'area) all'altra, il detective è stato in grado di rintracciare la sospettata a Richmond, in Virginia, mentre si dirigeva a est sulla I-64 in direzione dell'aeroporto di Norfolk. In seguito, il cellulare è stato individuato mentre trasmetteva da Baltimore nel Maryland. Dopo ulteriori indagini, è stato scoperto che la Rountree aveva acquistato un biglietto aereo da Baltimore al Texas sotto il nome della sorella. Piper Rountree sosteneva di non essersi mai mossa da Houston nel Texas, ma la documentazione delle attività del cellulare dimostrava il contrario, e questa prova è stata determinante per stabilire la sua colpevolezza.
Trovate ulteriori informazioni sull'uso dei telefoni cellulari nelle indagini di Computer Forensics nel Capitolo 8.

IoT Forensics

Negli ultimi anni sono stati fatti significativi passi avanti nei sistemi di intelligenza artificiale (AI) per la casa. Inoltre, questi dispositivi abilitati dall'AI possono essere controllati da smartphone e integrati con dispositivi domotici (termostati, dispositivi di sorveglianza, illuminazione). Conoscere questi nuovi ecosistemi e le tracce digitali che questi dispositivi salvano localmente o nel cloud è fondamentale per gli investigatori. Parleremo più estesamente di IoT Forensics nel Capitolo 13.

Quali competenze deve avere un investigatore forense?

La Computer Forensics è un campo multidisciplinare, in cui sono richieste competenze in vari campi: informatica, diritto, procedura penale, matematica, scrittura, scienze forensi e linguistica.

Conoscenze di informatica

Per quanto riguarda l'informatica, è importante avere una buona conoscenza dei sistemi operativi e dei file system associati. Fondamenta solide in questo ambito consentiranno all'investigatore di sapere dove sono conservati i file e di stabilirne il valore per l'accusa in un caso penale. La conoscenza dei sistemi operativi permette di capire come interagiscono fra loro software e hardware. Queste informazioni sono fondamentali per ricostruire le

azioni di un utente su un computer. Per esempio, BitLocker, uno strumento di cifratura introdotto con le versioni Ultimate e Enterprise di Microsoft Windows Vista, consente di cifrare file, cartelle o intere unità disco. Se si toglie l'alimentazione a un computer su cui è attivato BitLocker, il processo crittografico si attiva. Un investigatore di Computer Forensics esperto che trovi questo sistema operativo (o uno più recente) su un computer acceso avrà ben chiari i potenziali rischi che lo spegnimento del computer potrebbe provocare.

Individuare e recuperare i file che possono costituire evidenza non è sufficiente. Un esaminatore forense esperto deve avere grandi capacità investigative, che gli consentiranno di associare quelle evidenze a una persona specifica; l'esaminatore deve essere in grado di usare le evidenze digitali per dimostrare controllo, possesso e intenzione. Per esempio, un investigatore deve poter dimostrare che un sospettato aveva il controllo del computer quando i file sono stati salvati nella memoria. Un esempio di controllo, in questo scenario, è se l'utente ha utilizzato un nome utente e una password per accedere al computer. Il possesso è un altro fattore importante, quando si cerca di dimostrare la colpevolezza. L'investigatore deve poter dimostrare che il sospettato ha creato un file, o lo ha modificato o lo ha spedito per posta elettronica a qualcuno. Infine, l'intenzione in generale è fondamentale per perseguire un criminale. Nel caso della Computer Forensics, gli accusati potrebbero sostenere di non aver avuto intenzione di visitare un particolare sito web o di avere scaricato certe immagini senza rendersene conto, ma di non averle mai guardate. Perciò l'investigatore di Computer Forensics, per poter dimostrare l'intenzione deve poter dimostrare che sia stato effettuato l'accesso a un determinato sito web varie volte, o magari che un'immagine è stata vista in più occasioni e quindi distribuita ad altri.

Conoscenze giuridiche

La conoscenza della legge è estremamente importante, in particolare per quanto riguarda la Computer Forensics. Poter accedere al computer di un sospettato può essere la prima difficoltà che un investigatore deve affrontare. Se il computer del sospettato si trova nella sua abitazione, è fondamentale conoscere le disposizioni di legge in materia di perquisizione e sequestro (il Quarto Emendamento, negli Stati Uniti). Per per accedere al computer, l'investigatore deve convincere un giudice che è stato commesso un crimine e che esistono fondati motivi per ritenere che in un luogo particolare esistano prove fondamentali: le forze dell'ordine devono dimostrare un "fondato motivo" per effettuare la perquisizione.

Capacità di comunicazione

Non si può sottovalutare l'importanza della scrittura nel campo della Computer Forensics. Alla fine, l'investigatore deve documentare il processo investigativo e quanto ha scoperto. Il rapporto inoltre deve essere scritto in maniera tale che quanti sono coinvolti nel caso e non possiedono le competenze tecniche dell'esaminatore forense possano comprendere ciò che è stato scoperto. Se il caso arriva in tribunale, l'investigatore forense potrebbe essere chiamato a testimoniare come esperto. In quel caso dovrà comunicare efficacemente quanto ha scoperto a giudice e giuria, che hanno competenze limitate di informatica o di Computer Forensics.

Capacità linguistiche

Le attività criminali oggi hanno una maggiore presenza internazionale, facilitata dalla diffusione di Internet. Con la crescita dei crimini informatici e l'adozione della tecnologia da parte dei terroristi internazionali, è cresciuto il bisogno di investigatori bilingui. Un investigatore di Computer Forensics bilingue ha perciò la possibilità di dare un contributo maggiore in determinate indagini.

Formazione continua

Un investigatore di Computer Forensics dovrà continuare ad acquisire nuove competenze. Ci saranno sempre comunque competenze fondamentali ma difficili da misurare. La capacità di astrazione, o di pensare fuori dagli schemi, è determinante, perché ogni crimine è diverso dagli altri e la natura delle prove varia. Perciò gli investigatori di Computer Forensics dovranno sviluppare continuamente nuove tattiche e nuove soluzioni. Saper essere flessibili e apprendere continuamente nuove competenze è particolarmente importante anche vista la rapidità con cui cambiano le tecnologie, e con queste anche la natura dei crimini. Un altro aspetto intangibile è legato alla psicologia. Essere in grado di comprendere il criminale consente di capire meglio le azioni della persona e può consentire di trovare rapidamente le risposte nel corso di un'indagine. Per questo motivo abbiamo bisogno di esperti in grado di profilare serial killer e altri criminali.

Programmazione

Anche se non è necessario che un investigatore forense abbia profonde conoscenze di programmazione, qualche capacità in questo campo è molto utile. Più specificamente, la conoscenza di Linux può aiutare nell'esame dei server Linux, nella clonazione di un volume, nell'esame di dispositivi Android, nell'analisi delle app Android e delle reti; si può usare AppleScripts per lo scraping di siti web o per individuare a forza bruta i PIN su un computer Mac; Python può essere usato per lo scraping automatizzato di siti Web; gli EnScripts sono script personalizzabili utilizzati con EnCase; i *cmdlet* e gli script di PowerShell si possono usare per recuperare evidenze fondamentali da diversi sistemi operativi, fra cui anche Windows.

Riservatezza

Infine, è fondamentale mantenere la riservatezza delle informazioni. Solo quanti devono sapere di un'indagine devono avere accesso alle informazioni; quanti meno sono, tanto meglio è. Se il sospettato scopre che sono in corso indagini, potrebbe fuggire o inquinare le prove, cioè cercare di nascondere, alterare o distruggere prove collegate alle indagini. Anche le fughe di notizie ai media sono fonte di preoccupazione, perché possono influire sulla percezione del caso da parte di chi è chiamato a decidere (sui membri della giuria, per esempio, negli ordinamenti in cui è una giuria a emettere un verdetto).

L'importanza della Digital Forensics

L'importanza della Digital Forensics continua ad aumentare, perché una parte sempre più ampia della nostra vita passa attraverso la tecnologia. Informazioni sulla nostra vita vengono registrate sui nostri computer, sui telefoni cellulari e nel Word Wide Web, in particolare attraverso i siti di social networking. Facebook, per esempio, ha circa due miliardi di utenti e offre agli investigatori una grande quantità di informazioni: fotografie, indizi sulle password, sulle possibili reti di amici e complici di un sospettato, per esempio. Agli investigatori criminali in genere è richiesta la ricostruzione degli eventi di un crimine e la tecnologia ha facilitato questo processo di ricostruzione. Gli spostamenti di un sospettato possono essere tracciati attraverso l'uso di abbonamenti collegati a una carta di credito, per esempio una MetroCard della metropolitana di New York, o attraverso il pagamento dei pedaggi ai caselli autostradali. Agli inizi del 2014, il pubblico ministero della Queens County a New York ha accusato un taxista, Rodolfo Sanchez, di furto aggravato, furto di servizio e possesso di proprietà rubata, perché il trasmettitore E-Z Pass (un tipo di telepass) e la relativa documentazione indicavano che aveva eluso il pagamento di molti pedaggi per i ponti e i tunnel della Metropolitan Transportation Authority (MTA). I movimenti di un sospettato possono essere tracciati anche attraverso l'uso del suo telefono cellulare.

Possibilità di lavoro

Il Bureau of Labor Statistics degli Stati Uniti ha riconosciuto l'importanza di Computer Forensics e sicurezza: stima che, dal 2018 al 2028, i posti di lavoro nell'IT aumenteranno del 12%, il che per i soli Stati Uniti significa circa 546.200 nuovi posti di lavoro. Le nuove possibilità di occupazione saranno legate in parte all'aumento delle attività criminali su Internet, come furto di identità, spamming, molestie via email e download illegale di materiali protetti da copyright.

Posti di lavoro nel campo della Computer Forensics esistono nelle forze dell'ordine a livello locale, statale, federale, internazionale, ma anche il settore privato offre molte possibilità per gli esaminatori forensi. La maggior parte delle società di revisione dei conti ha un laboratorio di Computer Forensics, le più grandi ne hanno anche più di uno. Le grandi aziende spesso si avvalgono, per le loro indagini, dei servizi di una divisione di Computer Forensics delle società di revisione dei conti. Gran parte delle loro attività riguardano l'eDiscovery, ovvero il recupero di dati memorizzati digitalmente. La necessità del recupero di dati può derivare dall'esistenza di un contenzioso con un'altra azienda o dall'esigenza di soddisfare una richiesta di informazioni da parte di un ente di controllo (come la SEC, Securities and Exchange Commission, negli Stati Uniti o la CONSOB in Italia). I servizi di eDiscovery in genere sono collegati a cause civili.

Esaminatori forensi esperti possono trovare lavoro anche in società private di investigazione. Queste società, come la CODEDETECTIVES LLC, vengono spesso consultate da persone coinvolte in cause civili, o da persone che stanno affrontando una causa di divorzio che comporta accordi contestati o accuse di infedeltà, in particolare quando non vi è accordo sulla custodia dei figli. Si potrebbe anche sostenere che la crescita della Mobile Forensics sia stata propiziata dalla richiesta di indagini da parte di persone che sospettavano un'infedeltà del coniuge.

Con il crescere dell'importanza della Computer Forensics e con la diffusione di nuove tecnologie, nasce continuamente l'esigenza di nuove soluzioni software e hardware. Aziende di software e hardware come AccessData, opentext, Cellebrite e Paraben assumono persone competenti sia in campo informatico sia in campo investigativo. Alcuni grandi studi legali di tutto il mondo hanno assunto investigatori forensi o hanno fatto ricorso ai servizi di investigatori forensi. In molti casi, inoltre, esaminatori forensi sono stati chiamani a testimoniare in tribunale come esperti.
Anche i sistemi finanziari di tutto il mondo si basano molto sulle comunicazioni elettroniche e sull'archiviazione digitale di informazioni sui conti dei clienti. Le frodi con carta di credito via Internet e altri casi di frodi finanziarie hanno spinto gli istituti finanziari a sviluppare e investire nel campo della Computer Forensics per identificare e far condannare i colpevoli. Questa capacità fornisce agli istituti finanziari una maggiore conoscenza delle attività criminali, delle strategie e delle tattiche, per migliorare la sicurezza informatica.
Altre organizzazioni che assumono investigatori forensi sono le agenzie del Dipartimento della Difesa, come l'Aeronautica, l'Esercito e la Marina. L'Internal Revenue Service (IRS) è una delle agenzie federali che da più tempo si interessa di Computer Forensics. Agenzie federali come Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Drug Enforcement Agency (DEA) e il Secret Service hanno laboratori di Computer Forensics. Per l'FBI queste competenze sono fondamentali, per le indagini per esempio su crimini da "colletti bianchi" che comportano il riciclaggio di denaro o magari per le comunicazioni elettroniche di terroristi di Al-Qaida. Anche i Secret Service usano sempre più la Computer Forensics nelle loro indagini, per esempio sulle contraffazioni.
Nell'ottobre 2001 l'allora presidente Bush ha firmato lo USA PATRIOT Act (H.R. 3162). Uno dei provvedimenti derivanti da questa legge è stata la creazione di una rete a livello nazionale di Electronic Crimes Task Force. La rete è costituita da forze dell'ordine a livello federale, statale e locale, oltre che da pubblici ministeri, accademici e rappresentanti delle industrie private. Questo gruppo ha la responsabilità di proteggere l'infrastruttura critica degli Stati Uniti. Le competenze degli esaminatori di Computer Forensics sono indispensabili anche per le indagini su attacchi a infrastrutture critiche, come il sistema finanziario e la rete elettrica.
Posti per investigatori forensi sono disponibili anche in molti settori dell'economia, vista la sempre maggiore digitalizzazione delle informazioni personali. Il furto di informazioni personali e gli attacchi alle infrastrutture critiche probabilmente aumenteranno, perciò ci sarà sempre più bisogno di competenze nel campo della Computer Forensics. Il raggio d'azione di questa disciplina si è tanto ampliato che hanno cominciato a emergere posizioni specializzate. Alcuni esaminatori sono specializzati nel prendere in carico dispositivi digitali e nel crearne immagini forensi, che poi vengono trasferite a un'altra area del laboratorio, dove vengono cercati i file collegati specificamente alle indagini in corso. In seguito, un altro team può avere la responsabilità di scrivere il rapporto e rendere disponibili le prove attraverso un sito web sicuro. Quest'ultima è la procedura definita di *discovery*, in cui sia l'accusa sia la difesa hanno accesso alle prove.
La specializzazione del settore è evidente anche per quanto riguarda i diversi tipi di dispositivi. Nella Mobile Forensics, per esempio, gli investigatori si concentrano sulle prove fornite dai telefoni cellulari; altri si specializzano in Mac Forensics (computer Apple e dispositivi come iPad e iPod).

Storia della Digital Forensics

La Computer Forensics è nata come ausilio nelle indagini sui crimini informatici. Negli anni Cinquanta, Sessanta e Settanta ci sono stati i *phone phreaker*, che usavano varie tecniche per fare telefonate in teleselezione e internazionali senza pagare. Steve Jobs e Steve Wozniak, i fondatori della Apple, a quanto pare avevano venduto un dispositivo che permetteva di fare telefonate senza pagare, sfruttando alcuni trucchi di telecomunicazione. I *phone phreaker* sono stati i primi *hacker*, da cui hanno preso ispirazione poi gli hacker informatici dagli anni Ottanta.

Anni Ottanta: l'arrivo del personal computer

Anche se forme di criminalità informatica esistevano già da tempo, si è verificata una forte espansione a partire da quando è stato disponibile il personal computer (PC) negli anni Ottanta. La IBM ha favorito inizialmente lo sviluppo del PC, a partire dal 1981, con l'introduzione del PC 5150. In quel decennio era in concorrenza con altre aziende, come Atari, Commodore, Tandy e Apple. Quest'ultima ha avuto un grande successo in questo mercato negli anni Ottanta. Nel 1984 ha introdotto il Macintosh 128K, con un piccolo schermo in bianco e nero incorporato, seguito quello stesso anno dal Macintosh 512K Personal Computer, che permetteva l'uso di software di produttività come Microsoft Excel. Il Macintosh SE è stato uno dei PC più diffusi, dal lancio nel 1987. In quello stesso periodo sono emerse le prime "bacheche elettroniche", che hanno facilitato le comunicazioni fra hacker. In seguito sono emersi gruppi di hacker come la Legion of Doom negli Stati Uniti. Nel 1983 il film *War Games* ha fatto conoscere a tutti l'idea dell'hacking con un personal computer per poter accedere ai computer del governo. Nel 1984 Eric Corley (con lo pseudonimo di Emmanuel Goldstein) ha iniziato a pubblicare *2600: The Hacker Quarterly*, che ha facilitato lo scambio di idee fra hacker. Kevin Mitnick, uno dei primi, fu condannato nel 1989 per furto di firmware (software) alla DEC e di codici di accesso alla MCI. Dopo numerose violazioni di alto profilo, nel 1986 il Congresso degli Stati Uniti ha approvato il Computer Fraud and Abuse Act, in seguito modificato più volte.

Federal Bureau of Investigation (FBI)

Nel 1984, l'FBI ha istituito il Magnetic Media Program, in seguito noto con il nome di Computer Analysis and Response Team (CART). Il gruppo ha avuto la responsabilità della Computer Forensics. L'agente speciale Michael Anderson della divisione indagini criminali dell'IRS è stato definito il "Padre della Computer Forensics".

National Center for Missing and Exploited Children (NCMEC)

Nelle forze dell'ordine a livello locale, gli investigatori forensi spesso devono dedicare una grande quantità di tempo a casi di abuso su minori, specialmente quelli che coinvolgono il possesso e la distribuzione di pornografia infantile. Nel 1984, il Congresso degli Stati Uniti ha istituito il National Center for Missing and Exploited Children (NCMEC), che ha il compito di aiutare a individuare bambini scomparsi e a combattere lo sfruttamento (sessuale) dei minori: funge da centro per la documentazione di crimini contro i minori, in particolare sulle vittime di abuso e sfruttamento sessuale.

Anni Novanta: l'impatto di Internet

Con la diffusione dei browser come Netscape, negli anni Novana l'accesso a Internet è diventato molto più facile: non era più necessario usare un'interfaccia a riga di comando per raggiungere le risorse in Internet, ma si poteva sfruttare un'interfaccia amichevole, addirittura esteticamente piacevole. I browser hanno favorito una migrazione di massa dei computer verso Internet. Altrettanto importante è stato il fatto che i computer, che in precedenza non comunicavano facilmente tra loro, a quel punto potevano comunicare con relativa semplicità, grazie all'adozione di un protocollo comune, l'HyperText Transfer Protocol (HTTP). Più o meno in quegli anni è stata creata la posta elettronica, anche se inizialmente era solo un metodo di comunicazione all'interno delle organizzazioni. Le aziende multinazionali potevano ridurre drasticamente i costi telefonici istituendo una rete di email. I nuovi usi della tecnologia per le comunicazioni hanno fatto sì che crescesse il valore delle evidenze digitali. Nel 1993 si è svolta (a Quantico in Virginia) la prima International Conference on Computer Evidence.

Dipartimento della Difesa (DoD)

Nel 1998, la Defense Reform Initiative Directive #27 ha imposto all'U.S. Air Force la costituzione del Department of Defense Computer Forensics Laboratory, con responsabilità per le indagini di controspionaggio, criminali e di prove informatiche. Contemporaneamente è stato creato un programma di training in Computer Forensics, denominato Defense Computer Investigations Training Program. Questo programma è diventato poi un'accademia, accreditata dall'American Council of Education. È stato creato il Department of Defense Cyber Crime Center, o DC3, formato dall'accademia, dal laboratorio e dal 2002 anche dal Department of Defense Cyber Crime Institute (DCCI). Il DC3 si è associato con il Center for Telecommunications and Network Security (CTANS) dell'Università statale dell'Oklahoma per sviluppare e gestire il National Repository for Digital Forensic Intelligence (NRDFI), che in seguito ha sviluppato numerosi strumenti per le indagini forensi.

U.S. Internal Revenue Service

La fondazione dell'IRS (l'equivalente dell'Agenzia delle entrate per gli Stati Uniti) risale alla Guerra civile americana, quando il presidente Lincoln creò la carica di Commissioner of Internal Revenue. Oggi l'IRS è una divisione del Department of the Treasury. Con la progressiva diffusione dell'uso dei computer, è cresciuta anche la necessità di Computer Forensics nelle indagini dell'IRS. L'Electronic Crimes Program della Criminal Investigation Division dell'IRS (IRS-CID) ha finanziato Elliott Spencer per lo sviluppo di uno strumento di Computer Forensics denominato ILook. L'IRS-CID ha iniziato a usare ILook nel 2000 come ausilio nelle indagini finanziarie. Storicamente, la ILook Suite è a disposizione, gratuitamente, delle forze dell'ordine locali e statali.

United States Secret Service (USSS)

Molti pensano che lo United States Secret Service (USSS) abbia solo il compito di proteggere il Commander in Chief, ovvero il Presidente degli Stati Uniti. Questa agenzia federale però ha anche una storia relativamente lunga e importante nel campo della Computer Forensics, perché l'USSS ha agenti che in tutti gli Stati Uniti conducono

indagini criminali, fra l'altro su crimini legati al riciclaggio e alla contraffazione di denaro. Nel Crime Bill del 1994, il Congresso ha affidato all'USSS anche il compito di applicare le proprie conoscenze in campo forense e tecnico alle indagini criminali collegate alla scomparsa e allo sfruttamento di minori. Il Servizio lavora quindi a stretto contatto con il NCMEC. Nel 1996, l'USSS ha costituito la New York Electronic Crimes Task Force (ECTF), un centro per la collaborazione nelle indagini sui crimini informatici.
Nel 2001, lo USA PATRIOT Act ha dato mandato all'USSS di ampliare la New York Electronic Crimes Task Force (ECTF) e di costituire ECTF a livello nazionale. L'anno successivo, preso atto della mancanza di coordinamento fra le agenzie delle forze dell'ordine prima degli eventi dell'11 settembre 2001, è stato costituito il Department of Homeland Security (DHS), la cui responsabilità primaria è la protezione degli Stati Uniti da attacchi terroristici e la risposta efficace ai disastri naturali. Il Secret service quindi è diventato un'agenzia all'interno del DHS. Nell'aprile del 2003, il PROTECT Act (noto anche come Amber Alert Bill) ha dato pieno mandato all'USSS di gestire le indagini sugli abusi su minori, dotandolo a questo fine di maggiori finanziamenti e maggiori risorse. Nel 2007, l'agenzia ha istituito il National Computer Forensics Institute (NCFI), una partnership fra USSS, DHS, la Alabama District Attorneys Association, lo stato dell'Alabama e la città di Hoover, Alabama. Il NCFI offre formazione nel campo della Computer Forensics a forze dell'ordine, pubblici ministeri e giudici. È dotato di aule tecnologiche, di un laboratorio di Computer Forensics e di un'aula di tribunale simulata. In realtà l'USSS in genere è meno coinvolto nei casi di sfruttamento di minori, dato che è maggiormente concentrato sui crimini finanziari. Nei casi di abuso su minori sono più coinvolti FBI, DHS-ICE e il Postal Inspector's Service.
La necessità di collaborazione a livello internazionale, in particolare con le forze dell'ordine in Europa, è diventata più impellente dopo l'11 settembre 2001. Per questo nel 2009 l'USSS ha costituito la prima European Electronic Crimes Task Force, con sede a Roma in Italia. L'anno successivo è stata costituita la Electronic Crimes Task Force del Regno Unito.

Collaborazione internazionale

La collaborazione internazionale nelle indagini è estremamente importante perché spesso il raggio d'azione della criminalità è molto esteso a livello geografico. I criminali usano spesso Internet per comunicare sia all'interno degli Stati Uniti, sia a livello internazionale. Nel 1995 è stata costituita la International Organization on Computer Evidence (IOCE). Questa organizzazione facilita lo scambio di informazioni fra le forze dell'ordine dei diversi paesi. Nel 1998, il G8 ha dato mandato all'IOCE di creare gli standard per la gestione delle prove digitali.

INTERPOL

Per quanto riguarda la collaborazione internazionale, l'INTERPOL ha assunto un ruolo centrale nell'applicazione delle prove digitali alle indagini criminali. L'INTERPOL è l'organizzazione di polizia internazionale più grande del mondo: rappresenta 188 nazioni. Nel 1989 il General Secretariat è stato trasferito a Lione, in Francia. Nel 2004 è stato istituito un ufficio di collegamento dell'INTERPOL presso le Nazioni Unite e nel 2009 è stato nominato un rappresentante speciale all'Unione Europea a Bruxelles.

L'Incident Response Team (IRT) dell'INTERPOL ha messo a disposizione le sue competenze di Computer Forensics in varie indagini internazionali di alto profilo. In un rapporto del 2008, su richiesta delle autorità colombiane, esaminatori forensi delle forze dell'ordine di Australia e Singapore hanno esaminato 609 GB di dati su otto laptop, due dischi esterni e tre chiavette USB. L'hardware e il software appartenevano alle *Fuerzas Armadas Revolucionarias de Colombia* (FARC), un'organizzazione terroristica antigovernativa della Colombia, ampiamente finanziata attraverso il controllo del traffico illegale di stupefacenti, in primo luogo traffico di cocaina. Gli investigatori colombiani hanno contattato l'INTERPOL per far esaminare i laptop sequestrati, perché investigatori imparziali potessero prendere visione delle prove digitali e confermare le affermazioni del governo, secondo le quali le prove digitali erano state gestite in modo corretto dal punto di vista forense.
All'Assemblea generale dell'ICPO-INTERPOL del 2008 a San Pietroburgo in Russia, è stata approvata la costituzione di una Computer Forensics Analysis Unit dell'INTERPOL. questa unità fornisce formazione e assistenza nelle indagini di Computer Forensics ed è stata investita della responsabilità di sviluppare standard internazionali per la ricerca, il sequestro e l'indagine di prove elettroniche.
L'INTERPOL lavora da molti anni nella lotta ai crimini contro i minori. Come il NCMEC, dal 2001 ha costituito un database di minori vittime di abusi, sotto il nome di INTERPOL Child Abuse Image Database (ICAID). Nel 2009, l'ICAID è stato sostituito dall'International Child Sexual Exploitation image database (ICSE DB). Questo database è accessibile in tempo reale alle forze dell'ordine di tutto il mondo e incorpora un software di confronto delle immagini che permette di collegare vittime e luoghi. L'INTERPOL lavora anche con altre agenzie in tutto il mondo per combattere gli abusi su minori, fra gli altri con il COSPOL Internet Related Child Abuse Material Project (CIRCAMP) e la Virtual Global Taskforce. CIRCAMP è una rete europea che effettua il monitoraggio di Internet per identificare casi di sfruttamento di minori. La Virtual Global Taskforce ha le stesse finalità, ma è una rete globale di agenzie di polizia che combattono gli abusi su minori online.
L'INTERPOL ha coordinato iniziative internazionali per la cattura di sospetti pedofili. Dopo che nel 2006 in Norvegia la polizia aveva effettuato una retata di predatori Internet, gli investigatori hanno scoperto un laptop contenente quasi 800 immagini orribili di ragazzi. Quasi 100 di quelle immagini mostravano un maschio bianco di mezza età che guardava mentre i ragazzi venivano abusati. Le autorità hanno chiesto l'assistenza dell'INTERPOL per identificare quel predatore sconosciuto. L'INTERPOL ha avviato una massiccia caccia all'uomo e ha chiesto aiuto al pubblico attraverso i media. Entro 48 ore dalla pubblicazione della richiesta di aiuto, l'INTERPOL e lo U.S. Immigration and Customs Enforcement (ICE) hanno arrestato Wayne Nelson Corliss, un sessantenne di Union, nel New Jersey.

Regional Computer Forensics Laboratory

Nel 1999, è stato istituito a San Diego in California il primo Regional Computer Forensics Laboratory (RCFL). Nel 2000 è stato aperto il secondo RCFL negli Stati Uniti a Dallas, in Texas. Un RCFL è un laboratorio sponsorizzato dall'FBI, utilizzato per addestrare rappresentanti delle forze dell'ordine all'uso degli strumenti di Computer Forensics. I laboratori sono usati anche dalle diverse agenzie di polizia per collaborare nelle indagini criminali. Le agenzie più piccole spesso non hanno né le disponibilità fi-

nanziarie né le risorse per creare un laboratorio di Computer Forensics e gli RCFL danno la possibilità alle forze di polizia di distaccare una o due persone presso un laboratorio a fini di formazione o per lavorare alle loro indagini. Fra i crimini su cui si indaga vi sono terrorismo, pornografia infantile, furto o distruzione di proprietà intellettuale, crimini Internet, frodi su proprietà e frodi finanziarie. Al momento in cui scriviamo, esistono 14 RFCL negli Stati Uniti e 2 in Europa.

Fusion center

Creati nel 2003, i *fusion center* negli Stati Uniti sono punti centrali per la raccolta di intelligence a livello statale e locale, al fine di prevenire attacchi terroristici. Il progetto è un'iniziativa congiunta del Department of Homeland Security (DHS) e del Department of Justice (DOJ). Nel paese sono attivi oltre 70 centri, la cui posizione dovrebbe essere segreta, ma un gruppo, denominato Public Intelligence, ha rivelato la localizzazione della maggior parte di questi centri. Gli edifici non hanno insegne né un indirizzo civico, ma sono associati solo a una casella postale (P.O. Box). Per esempio, l'indirizzo del fusion center di West Trenton, New Jersey, è P.O. Box 7068.

Le relazioni compilate dopo l'11 settembre indicavano la mancanza di condivisione delle informazioni fra agenzie governative (fra cui National Security Agency [NSA], Central Intelligence Agency [CIA] e Federal Bureau of Investigation [FBI]) come uno dei fattori principali che avevano impedito di prevenire gli attacchi terroristici. Per esempio, Ziad Jarrah ha dirottato il Volo 93 della United Airlines l'11 settembre 2011, mandandolo poi a schiantarsi in Pennsylvania. Jarrah era stato fermato dalla polizia locale, per eccesso di velocità, il 9 settembre, ma l'agente che lo aveva fermato non disponeva delle informazioni che si sarebbero potute usare per tenerlo in stato di arresto e non sapeva che Jarrah era indagato dall'FBI.

Le forze dell'ordine locali raccolgono informazioni e le convogliano verso i fusion center. Fra i tipi di informazioni raccolte vi sono video di sorveglianza, numeri di targa e segnalazioni di attività sospette (SAR, *suspicious activity report)*. Fra queste ultime vi sono segnalazioni di individui che scattano fotografie di edifici governativi, che disegnano mappe o che tengono incontri di gruppo non usuali.

I fusion center, a quanto si dice, conservano database di informazioni su quasi tutti gli americani, informazioni che comprendono numeri di cellulare non registrati, informazioni sulla patente di guida, richieste di risarcimento alle assicurazioni. I centri raccolgono informazioni anche da aziende di data mining relativamente sconosciute come la Entersect. Quest'ultima fornisce alle organizzazioni informazioni su potenziali dipendenti: fedina penale, cause, casi di bancarotta, istruzione, referenze di datori di lavoro. Fornisce alle forze dell'ordine anche un servizio denominato Entersect Police Online: in base a quanto riporta il sito web (`entersect.net`), può consentire l'accesso a miliardi di record online che coprono la maggior parte della popolazione degli Stati Uniti. I fusion center utilizzano anche altri fornitori commerciali di database. come Lexis-Nexis.

Per la segretezza che li circonda e la quantità di informazioni personali raccolte, ci sono state molte controversie sui fusion center. Organizzazioni per i diritti civili, come la American Civil Liberties Union (ACLU), hanno espresso contrarietà per lo zelo nella raccolta di informazioni personali e la mancanza di organi di controllo. Questi centri combinano personale aziendale e personale delle forze dell'ordine. C'è stato chi ha criticato il ruolo delle forze dell'ordine locali nel monitoraggio di attività sospette. Nel 2008, per esempio, la polizia dell'Amtrak [il sistema di trasporto ferroviario extraurbano

degli Stati Uniti] ha arrestato alla Penn Station di New York Duane Kerzic, che era stato visto scattare una foto a un treno. È stato trattenuto ammanettato in cella, poi è emerso che in realtà voleva solo partecipare all'annuale concorso fotografico dell'Amtrak.
Anche se il loro ruolo può essere classificato sotto la voce "antiterrorismo", i fusion center hanno un ruolo fondamentale anche in alcune indagini di Computer Forensics. Offrono comunque una chiara indicazione del tipo di informazioni digitali che attualmente vengono raccolte e conservate.

Anni 2000: valute virtuali, IoT, crittografia ed effetto Edward Snowden

Nel maggio 2010, Laszlo Hanyecz ha acquistato due pizze a Jacksonville per 10.000 Bitcoin (BTC). Il Bitcoin all'epoca valeva meno di 0,01 dollari. Dieci anni dopo, quei 10.000 BTC avrebbero avuto un valore pari a oltre 77 milioni di dollari. Anche se molti possessori di denaro virtuale sono persone rispettose della legge, queste valute senza dubbio hanno facilitato milioni di pagamenti a criminali. Particolarmente significativo è l'uso di criptovalute nei marketplace del Dark Web, fra cui Silk Road, AlphaBay, Honest-Cocaine e altri siti, dove le valute d'elezione per transazioni illecite sono state Bitcoin o Ethereum, dato l'anonimato che queste criptovalute offrono. Silk Road, gestito da Ross Ulbricht, era un marketplace del Dark Web, accessibile solo mediante il browser Tor. Anche nonostante lo smantellamento effettivo di Silk Road, il suo successo nel facilitare transazioni anonime nel mondo delle droghe ha portato alla creazione di altri marketplace nel Dark Web, gestiti da operatori criminali. Sono emersi altri marketplace nel Dark Web e negli anni 2000 sono stati perseguiti molti dei loro creatori, amministratori e vendor. Ciononostante, è probabile che questi tipi di marketplace continuino a fiorire. Le criptovalute sono le valute ideali per i trafficanti di droga, poiché eliminano la necessità di trasferire contanti da un paese all'altro e riducono le tracce cartacee collegate alle transazioni effettuate attraverso gli istituti finanziari tradizionali.
Come abbiamo già accennato, i dispositivi IoT e i dispositivi domotici abilitati dall'AI si sono rapidamente diffusi dopo il 2000. I dispositivi AI, come Alexa, o i sistemi di sorveglianza domestica, come The Ring, sono potenziali grandi fonti di ulteriori evidenze digitali.
Gli anni 2000 hanno segnato anche un'epoca in cui la crittografia è diventata la norma, anziché una scelta per i consumatori. Più specificamente, la cifratura dei dischi, anziché un'opzione, è diventata l'impostazione predefinita. Questo è particolarmente evidente nel caso degli sviluppatori per smartphone (sia Android che iPhone). Inoltre, i miglioramenti con l'autenticazione a due fattori (2FA) hanno aumentato l'adozione di questo protocollo di sicurezza in aziende come Apple e Microsoft; sempre più spesso le aziende richiedono un'ulteriore autenticazione via email o sms quando si registrano nuovi dispositivi o nel caso in cui si acceda a un'applicazione da un dispositivo o da un luogo che non vengono riconosciuti. Queste evoluzioni nel campo della crittografia e dell'autenticazione pongono sfide enormi per gli investigatori di Digital Forensics.
Nel maggio 2013, Edward Snowden ha improvvisamente lasciato la National Security Agency (NSA), portando con sé molti file segreti. Snowden ha reso pubbliche informazioni sul modo in cui grandi aziende di tecnologia trasmettevano grandi quantità di dati alla NSA, al GCHQ (Government Communications Headquarters) e in generale a Five Eyes, a sostegno dei programmi di sorveglianza; Five Eyes è una partnership collaborativa fra agenzie di intelligence di Stati Uniti, Regno Unito, Canada, Australia e

Nuova Zelanda. Si può pensare quello che si vuole delle azioni di Edward Snowden, ma certamente hanno inciso negativamente sulla capacità delle forze dell'ordine di raccogliere dati da servizi terzi, anche in presenza di un mandato o di un'ingiunzione. Per esempio, alcune aziende, come Twitter, ora hanno adottato la politica di informare i loro clienti se sono sottoposti a indagine, a meno che un giudice non lo proibisca espressamente. Sembra che altre aziende si siano affrettate ad adottare tecniche crittografiche su software e hardware per proteggere la privacy dei loro clienti dalla sorveglianza del governo e non semplicemente al fine di rafforzare la sicurezza.

Training e istruzione

Esistono molti modi per diventare investigatori di Computer Forensics. Per molti il percorso è stato indiretto, attraverso le forze dell'ordine. Molti di questi professionisti hanno iniziato la loro carriera come agenti di polizia e poi sono riusciti a diventare investigatori. In seguito, le loro capacità in campo informatico, unite alla necessità di investigare su casi con prove digitali, hanno offerto loro la possibilità di diventare esaminatori forensi esperti. Il training formale in Computer Forensics è ancora un fenomeno relativamente recente.

Training presso le forze dell'ordine

Come abbiamo notato in precedenza, le forze dell'ordine utilizzano i Regional Computer Forensic Laboratory (RCFL) per condividere risorse, collaborare nelle indagini e migliorare le proprie competenze come investigatori di Computer Forensics. Gli RCFL offrono anche corsi formali per la preparazione di esaminatori RCFL e FBI CART. Il training prevede istruzione in merito ad acquisizione e gestione delle prove, ma anche sui sistemi operativi e i relativi file system.

Il Computer Emergency Response Team (CERT) della Carnegie Mellon ha sviluppato vari strumenti di Computer Forensics esclusivamente per le forze dell'ordine. Il training su questi strumenti è fornito attraverso il Federal Virtual Training Environment (FedVTE) del CERT.

Il Federal Law Enforcement Training Center (FLETC), con sede a Glynco, in Georgia, è un'organizzazione di training interagenzia per le forze dell'ordine che serve oltre 80 agenzie federali negli Stati Uniti. Uno dei programmi che offre è quello per Seized Computer Evidence Recovery Specialist (SCERS). Il FLETC offre anche corsi su argomenti come la Mac Forensics e la Network Forensics.

Il National White Collar Crime Center (NW3C) è un'agenzia che fornisce training e supporto investigativo alle forze dell'ordine e ai pubblici ministeri. Organizza corsi per vari ambiti della Computer Forensics, fra cui analisi forense dei cellulari, indagini online, sistemi operativi, file system, acquisizione e gestione delle prove digitali. Uno dei più noti è il corso di Secure Techniques for Onsite Preview (STOP), rivolto a funzionari di sorveglianza per persone in libertà provvisoria, detective e agenti che eseguono controlli o visite domiciliari a sorpresa e devono poter controllare rapidamente un computer in modo corretto dal punto di vista forense. Per esempio, un agente di sorveglianza potrebbe aver bisogno di controllare se sul computer domestico di un molestatore sessuale in libertà vigilata siano presenti determinati tipi di immagini.

L'INTERPOL fornisce supporto investigativo in Computer Forensics per le forze dell'ordine a livello globale. Nell'aprile 2009, lo University College Dublin (UCD) e l'INTERPOL hanno avviato un'iniziativa di formazione per investigatori in e-crime. Questa iniziativa non solo offre formazione, ma facilita anche gli scambi accademici nel campo della Computer Forensics per rafforzare le competenze degli esaminatori forensi. Lo UCD organizza un prestigioso Master of Science in Forensic Computing and Cybercrime Investigation aperto esclusivamente alle forze dell'ordine di tutto il mondo. Un'altra organizzazione che ha la finalità di facilitare lo scambio di idee e pratiche nella Computer Forensics è la Computer Technology Investigators Network (CTIN), aperta a forze dell'ordine, professionisti di sicurezza aziendale e membri della comunità accademica. InfraGard, infine, è un'agenzia pubblica-privata dell'FBI che promuove lo scambio di informazioni fra i settori privato e pubblico su temi legati a terrorismo, intelligence e sicurezza. InfraGard ha costituito sezioni locali negli Stati Uniti; l'associazione è aperta a tutti i cittadini statunitensi; chi fa richiesta di adesione è sottoposto a un controllo dei precedenti da parte dell'FBI.

Formazione nelle scuole superiori

Molte scuole superiori negli Stati Uniti hanno adottato un curriculum in Computer Forensics per gli studenti che hanno scelto un indirizzo giuridico e tecnologico. Un esempio è il Department of Education della città di New York, con il quale ho collaborato per oltre un decennio, al fine di creare un curriculum in Computer Forensics e cybersicurezza per studenti delle scuole superiori. Un curriculum di questo tipo è un ottimo modo per presentare agli studenti le complessità delle indagini che coinvolgono prove digitali.

Formazione universitaria

Molte università hanno creato corsi di Computer Forensics nell'ambito di lauree di primo e secondo livello. Tre fra le prime istituzioni più prestigiose che hanno sviluppato corsi di laurea sono il Champlain College, la Purdue University e la Carnegie Mellon University. Le ultime due collaborano con le forze dell'ordine locali nel campo della Computer Forensics. Un altro corso di laurea in Computer Forensics degno di nota è offerto dalla Bloomsburg University. Indirizzi in Computer Forensics sono offerti anche da altre istituzioni accademiche, come la Pace University, che lavora a sua volta a stretto contatto con le forze dell'ordine.

Certificazioni professionali

Una laurea in Computer Forensics, informatica o sistemi informativi può offrire una base solida di Computer Forensics. Se alla laurea si affianca qualche certificazione si acquisiscono maggiori competenze nel settore e si diventa candidati ancora più attraenti per un potenziale datore di lavoro. Questo perché molti corsi di certificazione sono tenuti da professionisti del settore e prevedono un training pratico nell'uso degli strumenti professionali.

Le sezioni seguenti descrivono le certificazioni in Computer Forensics disponibili, che possono contribuire a legittimare le credenziali di un esaminatore forense. L'elenco però non è affatto esaustivo.

Certificazioni professionali per il pubblico generale

La International Association of Computer Investigative Specialists (IACIS) è un'organizzazione non profit che si dedica alla formazione del personale delle forze dell'ordine nel campo della Computer Forensics. Una delle certificazioni più apprezzate nel settore è quella di Certified Forensic Computer Examiner (CFCE), offerta dall'IACIS.
John Mellon è stato un membro attivo dell'IACIS prima di fondare la International Society of Forensic Computer Examiners (ISFCE). Ha sviluppato il programma di certificazione per Certified Computer Examiner (CCE), a partire dal 2003. L'ISFCE ha quattro centri di test e offre proficiency test per l'American Society of Crime Laboratories Directors/Laboratory Accreditation Board (ASCLD/LAB), riconosciuta come il vertice delle certificazioni per laboratori forensi. L'ASCLD è una società professionale non profit di direttori di laboratori e manager di scienza forense che cerca di promuovere l'eccellenza nel campo della scienza forense, inclusa la Computer Forensics. Lo United States Secret Service e molti altri laboratori di Computer Forensics delle forze dell'ordine sono accreditati dall'ASCLD/LAB, il che dimostra il prestigio che accompagna questa certificazione.
Sono disponibili per il pubblico generale molte altre certificazioni indipendenti. La certificazione Certified Computer Forensics Examiner (CCFE) è offerta dall' Information Assurance Certification Review Board (IACRB). Per ottenere la certificazione CCFE, il candidato deve dimostrare di possedere conoscenze adeguate nei campi seguenti.

- Giurisprudenza, etica e problemi legali.
- Il processo investigativo.
- Strumenti della Computer Forensics.
- Recupero di prove da dischi fissi e loro integrità.
- Recupero e integrità di dispositivi digitali.
- Analisi forense di file system.
- Analisi e correlazione delle prove.
- Acquisizione di prove in sistemi basati su Windows.
- Analisi forense di reti e memorie volatili.
- Compilazione di rapporti.

La certificazione Certified Forensic Consultant (CFC), conferita dall'American College of Forensics Examiners International (ACFEI), si concentra sugli aspetti legali della Computer Forensics negli Stati Uniti. Il programma forma gli studenti negli ambiti seguenti.

- Il procedimento giudiziario.
- Regole federali sulle prove.
- Il processo di scoperta.
- Come prendere appunti.
- Ispezione del sito.
- Il rapporto scritto.

- La lettera d'incarico.
- Tipi di testimoni.
- Il rapporto del testimone esperto.
- Preparazione per una deposizione.
- Che cosa aspettarsi in caso di deposizione.
- Preparazione per una causa.
- Testimonianza in una causa.
- Che cosa portare in tribunale.
- Il lavoro della consulenza forense.

L'ACFEI offre formazione e valutazione per la certificazione Certified Forensic Accountant (CrFA). Un contabile forense è una persona con una formazione nel campo della revisione dei conti, coinvolta nelle indagini finanziarie.
Da quando è stato costituito nel 1989, il SANS (SysAdmin, Audit, Network, Security) Institute ha offerto formazione per i professionisti della sicurezza sia nel settore pubblico che in quello privato. Offre anche formazione in Computer Forensics e organizza un corso intitolato Computer Forensic Investigations and Incident Response. Questo corso prepara alla certificazione GIAC Certified Forensic Analyst (GCFA). Fondata nel 1999, la Global Information Assurance Certification (GIAC) valuta le competenze dei professionisti della sicurezza.

Certificazioni professionali per professionisti della sicurezza

Sicurezza informatica e Computer Forensics sono due discipline diverse, ma complementari. Per questo molti esaminatori di Computer Forensics possiedono certificazioni nell'ambito della sicurezza. Sia i professionisti della sicurezza sia gli esperti di Computer Forensics possono essere coinvolti nella gestione di incidenti di sicurezza, per esempio intrusioni in reti. I professionisti della sicurezza possono fornire informazioni sul tipo di violazione che si è verificato e sull'estensione dell'attacco, mentre un esaminatore forense può spesso stabilire la traccia delle prove lasciate da chi ha compiuto l'attacco.
Il programma Certified Security Incident Handler (CSIH) è un corso eccellente per un investigatore di Computer Forensics. Il programma è offerto dal CERT (Computer Emergency Response Team) ed è una divisione del Software Engineering Institute (SEI) presso la Carnegie Mellon University. SEI è un centro di ricerca e sviluppo finanziato a livello federale, sponsorizzato dal Department of Defense (DoD). Il CERT offre training per amministratori di rete e altro staff di supporto tecnico, in particolare sull'identificazione di minacce in atto e potenziali alle reti. Inoltre, il CERT addestra i professionisti della sicurezza su come gestire le violazioni della sicurenza. Il CERT ha un team forense di fama, che lavora a stretto contatto con le forze dell'ordine su progetti di ricerca relativi alle aree lasciate scoperte dagli strumenti commerciali per gli investigatori forensi.
È abbastanza comune che un investigatore in Computer Forensics, in particolare nel settore privato, acquisisca la certificazione Certified Information Systems Security Professional (CISSP), offerta dall'International Information Systems Security Certification Consortium (ISC)[2]. La certificazione CISSP è stata approvata formalmente dal DoD fra le sue categorie di Information Assurance Technical and Managerial. Questa certificazione, importante e molto apprezzata, si ottiene superando un esame che verte sul

cosiddetto corpus di conoscenze comuni (Common Body of Knowledge, CBK), che copre i seguenti ambiti della sicurezza.

- Controllo degli accessi.
- Sicurezza dello sviluppo di applicazioni.
- Continuità aziendale e pianificazione del disaster recovery.
- Crittografia.
- Governance della sicurezza delle informazioni e gestione del rischio.
- Giurisprudenza, normativa, indagini e conformità.
- Sicurezza operativa.
- Sicurezza fisica.
- Architettura e progettazione della sicurezza.
- Sicurezza delle telecomunicazioni e delle reti.

Per superare l'esame CISSP, il candidato deve ottenere un punteggio non inferiore a 700 (su un totale possibile di 1000) punti rispondendo a 250 domande a risposta multipla. Il candidato deve dimostrare di avere un'esperienza di almeno cinque anni in due o più fra i dieci ambiti. Viene sottoposto a un controllo dei precedenti penali e deve osservare il codice etico del CISSP. Una volta ottenuta la certificazione, un CISSP deve ottenere continuamente dei crediti professionali (CPE, Continuing Professional Credits) per mantenerla.
Un'altra certificazione di sicurezza spesso ottenuta dagli esaminatori di Computer Forensics è quella di Certified Information Security Manager (CISM). Come quella di CISSP, anche questa è per professionisti della sicurezza, ma è diversa perché si rivolge a manager di sicurezza delle informazioni con esperienza nei settori seguenti.

- Governance della sicurezza delle informazioni.
- Gestione del rischio delle informazioni.
- Sviluppo di un programma di sicurezza delle informazioni.
- Gestione di un programma di sicurezza delle informazioni.
- Gestione e risposta degli incidenti.

Come per la CISSP, anche per la CISM è richiesta una formazione professionale permanente, per rimanere aggiornati sui problemi della gestione della sicurezza delle informazioni.

Certificazioni professionali offerte da società di software di Digital Forensics

La maggior parte delle aziende produttrici di software di Computer Forensics offre corsi di certificazione. Alcuni importanti produttori di software per l'imaging digitale forense sono Cellebrite/BlackBag, AccessData, opentext e X-Ways Forensics.

- BlackBag Technologies offre vari bootcamp forensi per Mac e Windows. Una delle sue certificazioni più diffuse è quella di BlackLight Certified Examiner (BCE).
- AccessData offre un AccessData Bootcamp e corsi di Windows Forensics, Mac Forensics, Internet Forensics e Mobile Forensics. La sua certificazione più nota è quella

di AccessData Certified Examiner (ACE). L'esame valuta le competenze degli utenti per quanto riguarda FTK Imager, Registry Viewer e gli strumenti PRTK.

- Anche opentext offre training e valutazione per esaminatori di Computer Forensics. Uno studente che può dimostrare la propria conoscenza di EnCase può diventare EnCase Certified Examiner (EnCE).
- X-Ways Forensics offre training e valutazione per lo strumento di imaging bit-stream X-Ways Forensics e per il prodotto WinHex. In genere, un istruttore di X-Ways tiene un corso di 5 giorni, in cui i primi due riguardano i file system, i successi si concentrano invece sugli strumenti forensi.

Le certificazioni BCE, ACE ed EnCE, così come i corsi di X-Ways Forensics, sono aperti a professionisti sia del settore privato che di quello pubblico.

Riepilogo

La Digital Forensics (o Computer Forensics) è l'uso di dati digitali per condurre indagini su crimini. È una disciplina scientifica e, come per ogni settore forense, richiede una stretta osservanza delle leggi. La Digital Forensics è stata utilizzata in molti tipi diversi di indagini criminali, ma può essere usata anche in procedimenti civili o nell'ambito di una risposta a una intrusione di rete. Un investigatore di Computer Forensics usa molti tipi diversi di hardware e software per estrarre e analizzare file, fra cui uno strumento di imaging bit-stream che produce una copia bit per bit dei dispositivi. Trovare prove spesso non è sufficiente: è importante stabilire anche controllo, possesso e intenzione del sospettato. Le prove digitali possono comprendere email, immagini, video, siti web visitati e ricerche in Internet.

Un bravo investigatore di Computer Forensics deve possedere competenze in molti ambiti diversi, fra cui informatica, procedimenti penali, giurisprudenza, matematica, scrittura, scienza forense e linguistica. Queste competenze si possono acquisire in vari modi, per esempio con un training on-the-job (frequente fra le forze dell'ordine), corsi di laurea presso università o college, o corsi di certificazione. Quanti volessero intraprendere una carriera nella Computer Forensics possono trovare molte occasioni nel settore privato come in quello pubblico.

L'introduzione del personal computer negli anni Ottanta ha reso possibile la diffusione dell'informatica nelle case e ha anche provocato un aumento dei crimini in quache modo legati all'informatica. Le agenzie governative hanno iniziato a dedicare risorse alla Computer Forensics, a partire dalla costituzione del Computer Analysis and Response Team (CART) presso l'FBI. L'introduzione dei browser web negli anni Novanta ha stimolato una migrazione degli utenti dei personal computer verso Internet e l'ha resa una risorsa preziosa per il riperimento di informazioni sui sospettati e anche una fonte di prove incriminanti. Molte agenzie del Department of Homeland Security (DHS) usano la Computer Forensics. Per esempio, Internet ha facilitato la creazione di reti internazionali con intenti criminosi e l'INTERPOL ha ampiamente rafforzato le proprie capacità di Computer Forensics. Esistono già forme di collaborazione fra DHS e altri paesi, ma la necessità di queste collaborazioni continuerà ad aumentare, in particolare proprio nell'ambito della Computer Forensics.

La Tabella 1.1 offre una breve panoramica storica sugli sviluppi della Computer Forensics e gli sviluppi tecnologici che hanno influito su questo campo.

Tabella 1.1 Una breve storia della Computer Forensics e delle tappe principali dell'IT.

Anno	Evento
1981	La IBM introduce il PC 5150.
1984	L'FBI istituisce il Magnetic Media Program, in seguito noto come CART.
1984	Viene fondato il National Center for Missing and Exploited Children (NCMEC).
1986	Lo USSS costituisce la Electronic Crimes Task Force (ECTF).
1986	Il Congresso degli USA approva il Computer Fraud and Abuse Act.
1993	Prima International Conference on Computer Evidence.
1994	Il Congresso aprova il Crime Bill e l'USSS inizia a lavorare sui crimini contro minori.
1994	Viene rilasciato Mosaic Netscape, primo browser web con interfaccia grafica.
1995	Viene costituita l'International Organization on Computer Evidence (IOCE).
1996	L'USSS fonda la New York Electronic Crimes Task Force (ECTF).
1998	Viene costituita l'Europol.
1999	A San Diego viene costituito il primo Regional Computer Forensics Laboratory (RCFL).
2000	La Criminal Investigation Division dell'IRS (IRS-CID) inizia a usare ILook.
2001	L'USA PATRIOT Act incarica l'USSS di costituire ECTF in tutti gli Stati Uniti.
2001	L'INTERPOL sviluppa un database di minori vittime di abusi (ICAID).
2002	Viene istituito il Department of Homeland Security (DHS).
2003	Viene approvato il PROTECT Act per combattere lo sfruttamento minorile.
2003	Vengono costituiti i fusion center.
2003	L'Europol costituisce lo European Cybercrime Centre (EC3)
2004	Viene costituito Facebook.
2007	Costituzione del National Computer Forensics Institute (NCFI).
2008	Viene approvata la formazione di una Computer Forensics Analysis Unit dell'INTERPOL.
2009	Viene costituita la prima ECTF europea (in Italia).
2009	Il Bitcoin Ledger inizia a registrare le transazioni.
2010	Viene costituita la seconda ECTF europea (nel Regno Unito).
2011	Entra in vigore il PATRIOT Sunsets Extension Act.
2013	Edward Snowden si rifugia in Russia dopo una fuga di dati classificati dalla NSA.
2015	La causa per The Silk Road si conclude con la condanna del suo creatore, Ross Ulbricht.
2015	Entra in vigore il Cybersecurity Information Sharing Act.
2016	Introduzione dell'Investigatory Powers Act nel Regno Unito.
2017	Apple introduce APFS con il sistema operativo iOS 10.3.
2018	Introduzione della General Data Protection Regulation (GDPR).

Glossario

Algoritmo. L'insieme dei passi utilizzati per risolvere un problema.

BitLocker. Uno strumento crittografico introdotto con le edizioni Ultimate ed Enterprise di Microsoft Windows Vista, che consente la cifratura a livello di file, cartella o unità disco.

Catena di custodia. Documentazione di tutte le persone che sono entrate in contatto con le prove, dalla loro acquisizione, alle indagini e fino alla presentazione in tribunale.

CCTV (Closed-Circuit TeleVision, televisione a circuito chiuso). Video registrati e trasmessi in una sede particolare.

Cifratura. Il processo di trasformazione di un testo in chiaro in un testo in formato non leggibile, mediante una formula matematica.

Client. Un computer che richiede una risorsa da un computer server.

Computer Analysis and Response Team (CART). Una unità dell' FBI che ha la responsabilità di fornire supporto alle indagini che richiedono esami esperti di Computer Forensics.

Computer Technology Investigators Network (CTIN). Un'organizzazione che facilita lo scambio di idee e pratiche nel campo della Computer Forensics.

Contabile forense (*forensic accountant*). Una persona con una formazione nel campo della revisione dei conti coinvolta in indagini finanziarie.

Digital Forensics. L'acquisizione, l'analisi e l'uso di prove digitali in indagini civili o penali.

eDiscovery. Il recupero di dati memorizzati in formato digitale.

Electronic Crimes Task Force (ECTF). Una rete di centri, diffusi in tutti gli Stati Uniti, che collaborano nelle indagini sui crimini informatici.

Federal Law Enforcement Training Center (FLETC). Una organizzazione interagenzia delle forze dell'ordine a cui partecipano oltre 80 agenzie federali di tutti gli Stati Uniti.

Five Eyes. Una partnership di collaborazione fra agenzie di intelligence di Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda.

Forense. Che riguarda l'attività giudiziaria.

GPS (Global Positioning System). Un dispositivo che riceve comunicazioni da satelliti orbitanti intorno alla Terra, per stabilire la posizione geografica.

Imaging bit-stream, strumenti. Strumenti che producono una copia bit per bit di media originali, compresi i file marcati per la cancellazione.

InfraGard. Un'agenzia pubblica-privata dell'FBI che promuove lo scambio di informazioni fra il settore privato e quello pubblico su questioni legate a terrorismo, intelligence e sicurezza.

Inquinamento delle prove. Occultamento, distruzione, alterazione o falsificazione delle prove.

INTERPOL. La maggiore organizzazione di polizia internazionale, che rappresenta 188 paesi membri.

Metadati. Informazioni su un file, che possono includere le date di creazione, modifica e ultimo accesso, nonché l'identificativo dell'utente che lo ha creato.

National Center for Missing and Exploited Children (NCMEC). Un'agenzia che ha il compito di contribuire all'individuazione di minori scomparsi e di combattere lo sfruttamento (sessuale) dei minori.

National White Collar Crime Center (NW3C). Un'agenzia che fornisce formazione e supporto investigativo al personale delle forze dell'ordine e ai pubblici ministeri.

Prove a carico. Prove incriminanti, spesso usate per condannare un criminale.

Prove a discarico. Prove utilizzate per dimostrare l'innocenza di un accusato.

RAM (Random Access Memory, memoria ad accesso casuale). Chiamata spesso anche memoria a breve termine o memoria volatile, perché i suoi contenuti si cancellano quando viene tolta l'alimentazione al computer. L'attività e i processi correnti di un utente, compresa l'attività in Internet, sono memorizzati in RAM.

Regional Computer Forensics Laboratory (RCFL). Un laboratorio sponsorizzato dall'FBI che addestra il personale delle forze dell'ordine all'uso di strumenti di Computer Forensics e collabora alle indagini criminali.

Sicurezza informatica (computer security). Prevenzione di accessi non autorizzati a computer e alle relative risorse.

Skimmer. Un dispositivo utilizzato per carpire informazioni memorizzate sulla banda magnetica di un bancomat, di una carta di credito o di debito.

Web server. Un computer che invia documenti HTML e risorse correlate, in risposta alle richieste di un computer client.

Valutazione

Domande a risposta aperta

1. Come si può diventare investigatori di Computer Forensics?
2. Che cos'è la Computer Forensics e come viene usata nelle indagini?
3. Quali tipi di attività criminali vengono svolti nei marketplace del Dark Web, e perché hanno avuto tanto successo?

Domande a risposta multipla

1. Quale delle affermazioni seguenti definisce meglio la Computer Forensics?
    A. La Computer Forensics è l'uso di prove per risolvere crimini informatici.
    B. La Computer Forensics è l'uso di prove digitali per risolvere un crimine.
    C. La Computer Forensics è utilizzata solo per recuperare file cancellati da un computer.
    D. La Computer Forensics è usata solo per esaminare computer desktop e laptop.

2. Un modulo di catena di custodia è utilizzato per documentare che cosa?
    A. Gli agenti di polizia che arrestano e incarcerano un sospetto criminale.
    B. Una catena di lettere o email utilizzata in un'indagine.
    C. Tutti coloro che sono stati in contatto con le prove di un caso.
    D. Nessuna delle risposte precedenti.

3. Quali fra le cose seguenti possono avere valore probatorio per un esaminatore di Computer Forensics?
    A. Una SIM card.
    B. Una Xbox.
    C. Una fotocamera digitale.
    D. Tutte le precedenti.

4. Quale fra le affermazioni seguenti descrive meglio uno strumento di imaging bit-stream?
    A. Uno strumento di imaging bit-stream produce una copia bit per bit dei contenuti del supporto originale.
    B. Uno strumento di imaging bit-stream spesso consente all'esaminatore di recuperare file cancellati.
    C. Né A né B sono corrette.
    D. Sia A sia B sono corrette.

5. Quali fra i seguenti sono vantaggi delle prove basate su email?
    A. Le prove in email di solito sono presenti in più luoghi.
    B. Si possono trovare più facilmente di altri tipi di prove.
    C. Sono state accettate come prove ammissibili in molti casi.
    D. Tutti i precedenti.

6. Quali fra le affermazioni seguenti sulle immagini fotografiche non sono vere?
    A. Le immagini possono fornire prove di dove sia stato il sospettato.
    B. Le immagini non si possono reperire facilmente utilizzando strumenti di imaging bit-stream come FTK.
    C. Un'immagine può identificare marca e modello della fotocamera digitale da cui è stata prodotta.
    D. Fondamentalmente oggi si usa un solo tipo di immagine digitale.

7. Quale dei termini seguenti descrive meglio l'occultamento, l'alterazione o la distruzione di prove legate a un'indagine?
    A. Inquinamento delle prove.
    B. Manipolazione delle prove.
    C. Prove a carico.
    D. Prove a discarico.

8. Il Computer Analysis and Response Team (CART) è un'unità di quale agenzia del governo degli Stati Uniti?
   A. USSS
   B. FBI
   C. CIA
   D. ICE

9. Quali fra le leggi seguenti ha istituito il Department of Homeland Security e ha incaricato lo United States Secret Service di costituire Electronic Crime Task Force a livello di tutti gli Stati Uniti?
   A. Health Insurance Portability and Accountability Act.
   B. Children's Online Privacy Protection Act.
   C. PROTECT Act.
   D. USA PATRIOT Act.

10. Quali fra le affermazioni seguenti sui Regional Computer Forensics Laboratory (RCFL) sono false?
    A. I RCFL possono essere usati dagli avvocati difensori in casi penali.
    B. La costituzione di RCFL è stata sponsorizzata dall'FBI.
    C. I RCFL non solo sono utilizzati per le indagini, ma forniscono anche formazione nel campo della Computer Forensics.
    D. Esistono RCFL sia negli Stati Uniti sia in Europa.

Completa le frasi

1. Un (una) _____ è un insieme di passi utilizzati per risolvere un problema.
2. La Computer _____ è l'uso di prove digitali in un'indagine criminale.
3. La _____ informatica è la prevenzione di accessi non autorizzati a computer e risorse associate.
4. Un accusato può dimostrare la propria innocenza con l'uso di prove _____.
5. Il procedimento di trasformazione di un testo in chiaro in un formato illeggibile con l'applicazione di una formula matematica si chiama _____.
6. L'organizzazione internazionale di polizia più grande del mondo si chiama _____.
7. La memoria volatile, a breve termine, i cui contenuti scompaiono quando viene tolata l'alimentazione a un computer, si chiama _____.
8. Un(o) _____ è un dispositivo utilizzato per estrarre le informazioni memorizzate nella banda magnetica di una carta bancomat o di una carta di credito di debito.
9. Un server _____ fornisce documenti HTML e le risorse relative, in risposta alle richieste di un computer client.

10. _____ è un'agenzia pubblica-privata dell'FBI, che promuove lo scambio di informazioni fra i settori privato e pubblico su questioni legate a terrorismo, intelligence e sicurezza.

Progetti

Indagare su un crimine

Siete investigatori di Computer Forensics in forza alla polizia locale e siete stati assegnati a un'indagine criminale. Il sospettato, Michael Murphy, lavorava come responsabile dello sviluppo di prodotto per una società di software. È stato interrogato in merito a una serie di costose telefonate internazionali. Un ulteriore esame dei tabulati telefonici ha permesso di appurare che telefonava a una società di software concorrente, con sede in Cina e uffici anche negli Stati Uniti. Di fronte a queste evidenze, ha chiesto di parlare con un avvocato e non ha voluto dire altro. Il giorno dopo non si è presentato al lavoro. Il giorno successivo sono state contattate le autorità locali e Murphy è stato arrestato mentre saliva a bordo di un aereo diretto a Beijing con un biglietto di sola andata, due giorni dopo essere stato interrogato. All'aeroporto, gli agenti della polizia aeroportuale hanno trovato una borsa contenente vari CD, tre dischi rigidi SATA e cinque chiavette USB. Indicate in dettaglio i potenziali tipi di prove digitali di cui avrete bisogno per questa indagine.

Ricerca sulle prospettive di impiego per investigatori di Computer Forensics

Descrivete perché la domanda di esaminatori di Computer Forensics è destinata a crescere nei prossimi anni. Includete nella risposta statistiche relative all'aumento di determinati tipi di crimini.

Ricerca sulle agenzie federali degli Stati Uniti

Create un organigramma che specifichi tutte le agenzie federali degli Stati Uniti che sono coinvolte nella Computer Forensics. Partite dal Department of Homeland Security, poi inserite il nome di ciascuna agenzia e, ove è il caso, il nome della relativa unità di Computer Forensics.

Silk Road

Esaminate i resoconti giornalistici e gli atti del processo per Silk Road. Scrivete una relazione che indichi in dettaglio l'uso di prove digitali da parte di FBI e DHS, che alla fine ha portato alla condanna di Ross Ulbricht.