

Introduzione

“... Quando qualche anno fa parlai per la prima volta di Computer Forensics a una conferenza italiana, notai delle espressioni di compatimento, tipo quelle che di solito si riservano a parente noto per non essere troppo sano di mente e che, nel mezzo di un matrimonio, si lancia in una delle sue filippiche. Un magistrato mi disse che se mi interessava questo campo avrei dovuto ‘andarmene in America’. Inutile dire che quella conferenza non va annoverata tra i miei successi...”

La pubblicazione della prima edizione di questo volume fu una scommessa, per Apogeo. Il settore non solo era nuovo, ma era anche di nicchia. Alla fine rimanemmo tutti piacevolmente sorpresi non solo per il numero assoluto di copie vendute che il libro aveva raggiunto, ma anche il fatto che per diversi mesi rimase in testa nella classifica dei libri più venduti della casa editrice.

È un segno dei tempi. L'informatica si fa sempre più pervasiva e i crimini in cui è necessario esaminare delle evidenze digitali sono oggi un numero incalcolabile.

Inoltre, la gamma dei dispositivi da analizzare si è ampliata enormemente nel tempo, al punto che già la dizione “Computer Forensics” non è quasi più corretta. Ha senso piuttosto di parlare di “Digital Forensics”, comprendendo infatti non solo computer in senso stretto, ma sistemi digitali di ogni genere, quali telefoni cellulari, lettori multimediali, sistemi per la domotica, il car entertainment, sistemi informativi in generale e molto altro.

Anche la cultura generale si è innalzata grazie a convegni, manifestazioni e articoli. Siamo ben lungi da un risultato anche solo accettabile, comunque. In particolare, la nostra classe politica continua a peccare di ignoranza e saccenza. Non si parla di proposte assurde effettuate da onorevoli ex divi dello spettacolo, che sventolano lo spauracchio della pedofilia per cercare ulteriori inasprimenti sul copyright (quale relazione vi sia tra le due cose solo loro lo sanno), ma piuttosto di persone come qualche ex ministro di grazia e giustizia che in televisione cade dalle nuvole su argomenti come Skype o sul fatto che un civile possa essere nominato ausiliario di polizia giudiziaria. Oppure possiamo pensare al fatto che ogni legislatura “si dimentica” che i professionisti che lavorano in questo campo lo fanno più che altro per passione visto che la tariffa oraria pagata (poco più di 4 – dicasi quattro – euro l'ora) si ottenga più facilmente andando a chiedere l'elemosina in stazione o ai semafori. Quindi per raggiungere almeno le spese si devono chiedere incarichi fino a tre mesi. Basterebbe gestire la cosa a trattativa privata per poter snellire non poco le operazioni e lavorare con persone decisamente più motivate.

Arrivano ancora in laboratorio PC presi letteralmente sottobraccio senza alcun metodo di gestione della prova (reale se non digitale), in aula i giudici ridicolizzano l'hash md5 come fosse una pietanza per la mensa dei poveri ma qualcosa sta funzionando. Queste situazioni si fanno meno comuni (per il "rare" ci stiamo lavorando), la legge 48/2008 ha ratificato la convenzione di Budapest (con *solì* 7 anni di ritardo, ma non vogliamo fare i pignoli) e c'è una richiesta sempre maggiore di corsi in merito sia da parte di privati sia da parte delle forze di polizia.

IISFA (si veda l'Appendice C) cresce, e non solo. Si sta rifacendo la certificazione CIFI per adattarla ai tempi e si fanno incontri di approfondimento almeno una volta al mese, oltre a organizzare corsi e manifestazioni di interesse generale.

Anche questo testo, giocoforza, doveva ammodernarsi. Chi ha letto la prima edizione noterà come gli autori abbiano cercato di lavorare ora sugli argomenti più caldi, tentando di non stravolgere il formato iniziale che ha riscosso un certo successo.

Il volume rimane un *compendium* di Computer Forensics, non un *how-to* su come svolgere le diverse operazioni. L'idea base rimane quella di fornire un metodo prima che un riferimento su quanto esiste sul mercato e sul suo utilizzo.

Qualcuno ha criticato la prima edizione sottolineando che era troppo orientata all'Open Source. Si è cercato di recepire in parte questa critica, senza stravolgere la filosofia sottostante, introducendo un intero capitolo dedicato a un tool commerciale, oltre che inserendo molti riferimenti ai principali sistemi presenti sul mercato.

Si è migliorato il capitolo sul Network Forensics, si è aggiunto un intero capitolo sulla Mobile Forensics, oltre a una disamina a livello di byte level di ZFS. Per ora questo file system non è molto diffuso, ma tra poco approderà su Linux a kernel level, oltre che su Snow Leopard. ZFS ha innovato completamente il mondo dei file system e il suo impatto si potrà notare nel corso dei prossimi anni. Probabilmente questo è l'unico testo attuale che contenga una disamina così completa sull'argomento.

In generale, comunque, ogni pagina è stata oggetto di aggiustamenti qui e là. La speranza è quella di replicare il successo della prima edizione. Non solo per una soddisfazione degli autori, ma anche perché questo significherebbe che, nel suo piccolo, questo libro aiuterà a diffondere la cultura della Computer Forensics.

I nostri obiettivi rimangono dunque inalterati. Li elenchiamo di seguito.

Trasferire esperienza

Chi scrive ha affrontato oramai qualche centinaio di casi, muovendosi nell'attuale marasma legislativo italiano. Tale esperienza può rivelarsi utile sia per chi si affaccia per la prima volta a questo settore, sia per l'esperto che voglia confrontare la propria esperienza con quanto accaduto ad altri. È noto infatti che, mancando una regolamentazione precisa del settore, lavorare con procure diverse o, talvolta, anche solamente con magistrati diversi può portare a esperienze diametralmente opposte.

Allargare l'ambito della disciplina

Riservare la Computer Forensics ai soli reati informatici, quelli per intenderci connessi con la violazione delle reti, è riduttivo. Analisi informatiche di natura forense sono state utili nelle più svariate situazioni, dal traffico di droga ai movimenti eversivi, dall'evasione fiscale a frodi avvenute nel settore dell'allevamento del bestiame.

Sviluppare una metodologia

Dalla ricerca delle evidenze durante il sequestro, alla corretta gestione del dato in fase di acquisizione fino a giungere, dopo opportuna analisi, al banco del tribunale. L'idea è di fornire un metodo di lavoro che offra le dovute garanzie, la corretta gestione delle evidenze, la ripetibilità e la più consona presentazione ai non addetti ai lavori. Tale metodologia si è raffinata, in chi scrive, sia grazie ai preziosi consigli di magistrati esperti, sia correggendo gli inevitabili errori commessi.

Provvedere un compendio tecnico

Questo libro fornisce una serie di spunti, di idee, di scoperte derivanti da quanto accaduto nei nostri laboratori nel corso degli anni. L'idea è di raccogliere le conoscenze derivate da anni di esperienza diretta nella risoluzione di casi di varia natura, ma tutti connessi in qualche maniera al mondo digitale. Se ci si aspetta, però, una guida all'uso dei singoli tool, probabilmente si rimarrà in parte delusi. Il lettore che affronta questa tematica non può essere digiuno in materia informatica, pertanto non si è ritenuto utile scendere nel dettaglio, per esempio, nella sintassi dei comandi Unix utilizzati.

Fornire uno scenario legale di riferimento

Un intero capitolo, il secondo, è dedicato esclusivamente a fare il punto della situazione sulla legislazione vigente in Italia. Sparsi in alcuni capitoli si troveranno poi dei box di approfondimento, specifici per le implicazioni giuridiche degli argomenti analizzati: la Computer Forensics vive necessariamente in simbiosi con la giurisprudenza che di fatto condiziona e limita la pratica investigativa.

Organizzazione dell'opera

Il volume si compone di 19 capitoli e 3 appendici. La lettura sequenziale è consigliata ma non obbligatoria: essendo il volume pensato non tanto come la "Bibbia della Computer Forensics", quanto come uno strumento per valorizzare le proprie competenze informatiche nella prassi investigativa, ogni lettore è libero di focalizzarsi sulle parti del libro più attinenti alle sue necessità che, come ogni computer forensics expert sa bene, variano da caso a caso.

Dopo il Capitolo 1, scritto per fare luce su alcuni concetti base, con il Capitolo 2 si presenta una panoramica giuridico italiano inerente la materia.

I Capitoli 3 e 4 sono quindi dedicati all'importante fase dell'acquisizione del dato, mentre il Capitolo 5 apre le porte del laboratorio del computer forensics expert, argomento che viene approfondito nel Capitolo 6.

Nel Capitolo 7 si apre invece un'ampia parentesi sull'analisi dei file system, su cui si concentra buona parte della prassi investigativa.

Con i Capitoli 8, 9 e 10 si ritorna invece all'illustrazione di importati strumenti di lavoro.

Giunti a questo punto, il Capitolo 11 propone una metodologia di analisi generale. Quindi i Capitoli 12, 13 e 14 sono rispettivamente dedicati all'analisi dei sistemi Windows, Mac OS X e Linux.

Il Capitolo 15 tratta la gestione e l'analisi dei file di log, mentre il Capitolo 16 affronta le problematiche connesse con la cosiddetta Network Forensics.

In conclusione, i Capitoli 17, 18 e 19 affrontano le specificità dei media non convenzionali, con cui ogni investigatore prima o poi è destinato a misurarsi, della Mobile Forensics e infine dei CD, DVD e supporti rimovibili in genere.

Le appendici conclusive spendono quindi qualche pagina per fissare alcune problematiche, per illustrare velocemente qualche caso esemplare di quanto precedentemente detto e per presentare l'operato di IISFA.

Requisiti per la lettura

Questo volume è stato pensato per chi si avvicina alla pratica investigativa sui sistemi informatici e informativi. Nozioni di programmazione e robuste esperienze di navigazione in Rete sono pertanto assolutamente necessarie, così come una buona confidenza con i principali protocolli di comunicazione e una solida conoscenza delle architetture dei più diffusi sistemi operativi (specialmente Unix). A monte di tutto questo vi è, imprescindibile, la curiosità e un reale interesse verso la scienza nota come Computer Forensics.

Convenzioni utilizzate nel testo

Leggendo questo volume vi capiterà di incontrare due particolari box di approfondimento.

Diario di un computer forensics expert

Qui Andrea Ghirardini apre le porte dei suoi archivi, integrando quanto in discussione con esempi tratti dai casi di cui si compone la sua esperienza investigativa.

Cosa dice la legge

Qui Gabriele Faggioli fissa l'attenzione su quanto previsto dalla normativa in merito al tema trattato: perché la giurisprudenza gioca sempre un ruolo importante.

Contatti

È possibile contattare gli autori presso i seguenti indirizzi di posta elettronica:

darkpila@gmail.com (Andrea Ghirardini)

gf@gabrielefaggioli.it (Gabriele Faggioli)