

# Indice generale

<b>Prefazione .....</b>	<b>xiii</b>
<b>Introduzione .....</b>	<b>xvii</b>
I dati non sono più dove ci si aspettava che fossero .....	xvii
<b>Struttura del libro .....</b>	<b>xxi</b>
Requisiti per la lettura .....	xxi
Convenzioni utilizzate nel testo.....	xxii
Contatti .....	xxii
<b>Ringraziamenti .....</b>	<b>xxiii</b>
<b>Capitolo 1   Panoramica generale.....</b>	<b>1</b>
Che cos'è la Digital Forensics? .....	1
Applicazioni della Digital Forensics .....	4
Una metodologia forense .....	6
Una filosofia di lavoro .....	7
<b>Capitolo 2   Il panorama giuridico italiano .....</b>	<b>9</b>
Normative applicabili in Italia .....	9
La nozione di prova .....	12
La prova in sede civile .....	13
Cenni sui singoli mezzi di prova nel processo civile .....	16
La prova in sede penale .....	22
La prova in sede lavoristica .....	33
Focus: aspetti specifici del controllo sui lavoratori .....	35
Valenza della Digital Forensics a livello processuale .....	44
Profili giuridici dell'acquisizione, conservazione e analisi della prova informatica .....	49

Profili giuridici dei file di log .....	53
Profili giuridici della Network Forensics .....	62
Problematiche aperte .....	64

### **Capitolo 3    Acquisizione del dato: sequestro e duplicazione.....67**

Modalità di acquisizione .....	67
Ricerca.....	68
Sequestro .....	70
Alcune considerazioni.....	71
Preservare lo stato della prova.....	72
Personal computer.....	74
Sistemi mobili.....	77
Chromebook.....	78
Tastiera e mouse .....	79
Duplicazione .....	79
Alcune considerazioni.....	80
Software da utilizzare .....	83
Il problema dei RAID (vale anche per gli storage).....	86
Il write blocker.....	89
Copie di sistemi complessi .....	94
Mettere in sicurezza la scena .....	95
Identificare le fonti di prova digitali presenti.....	96
Preparare una checklist per ogni singolo sistema presente .....	96
Definire una lista di priorità .....	96

### **Capitolo 4    Intercettazione del dato.....99**

Premessa.....	99
Network Forensics: tipi e problematiche.....	100
Governativa .....	101
Privata.....	102
Come si usano? .....	106
Conservazione .....	108

### **Capitolo 5    Il laboratorio di analisi .....109**

Premessa.....	109
Concetti generali .....	110
NAS e SAN: un po' di definizioni.....	112
NAS.....	113
Block storage.....	114
OpenAFS .....	114
Architettura del laboratorio di analisi .....	117
Laboratori personali o di dimensioni contenute.....	117
Laboratori di dimensioni medio-grandi.....	118
Macchina da analisi/acquisizione .....	119
Cabinet capiente ma facilmente trasportabile .....	119

	Elevata velocità di I/O.....	120
	Reparto dischi efficiente e di grande capacità .....	121
	NAS back-end.....	121
	Sistema RAID .....	121
	Grande adattabilità nei collegamenti.....	122
	Macchine da analisi/test .....	123
	File/application server.....	124
	Backup .....	124
	Software .....	125
	Sistema operativo.....	126
	LiveCD .....	128
	Distribuzione general purpose .....	128
	Scegliere la distribuzione.....	129
<b>Capitolo 6</b>	<b>Media, partizioni e volumi .....</b>	<b>131</b>
	Premessa.....	131
	Comandi e funzioni Unix.....	132
	Gestione delle immagini disco .....	132
	Sistemi di partizionamento.....	136
	Il mondo non è mai semplice.....	145
	Linux LVM .....	145
	Linux Software RAID .....	146
	Windows Dynamic Disk (LDM) e software RAID.....	147
	Analisi preliminare .....	148
<b>Capitolo 7</b>	<b>File system .....</b>	<b>153</b>
	Premessa.....	153
	Tipologie di file system.....	153
	Caratteristiche comuni ai file system .....	155
	Dati, metadati e altre strutture .....	155
	Logica di funzionamento .....	157
	File system non journaled .....	157
	Principali file system .....	160
	FAT.....	160
	Considerazioni a livello di analisi.....	164
	NTFS.....	164
	Allocazione dei cluster.....	170
	Runlist .....	171
	Principali attributi nelle entry MFT .....	174
	Caratteristiche avanzate.....	183
	VSC .....	185
	Ext2,Ext3 ed Ext4 .....	187
	Ext4 .....	187
	Il superblock.....	189
	Group description table .....	189
	Block bitmap e inode bitmap.....	189

Inode .....	189
Attributi estesi .....	193
Directory entry.....	195
Link simbolici.....	196
Journal .....	196
OCFS2.....	198
Cluster .....	199
HFS+ .....	203
Struttura di HFS+ .....	204
ZFS.....	206
Concetti chiave.....	207
zpool e device .....	208
Boot block .....	211
Puntatori ai blocchi, diretti e indiretti.....	212
Gestione degli oggetti, metadati e relazioni.....	213
Gestione di snapshot e dataset .....	216
Oggetti ZAP .....	221
ZFS e ZPL .....	224
Intent log .....	226
Conclusioni su ZFS.....	226
BtrFS (Butter File System) .....	227
Introduzione e principi di funzionamento.....	227
Conclusioni .....	233

## **Capitolo 8 Tool e programmi di analisi.....235**

Premessa .....	235
Categorie .....	236
Sistemi di virtualizzazione .....	238
VMware .....	238
Parallels .....	240
Xen.....	240
KVM.....	240
VirtualBox.....	241
Programmi di hacking e cracking.....	242
Casi possibili.....	242
Password resetting .....	243
Reset password .....	243
BIOS password .....	244
Linux su x86 root password reset.....	245
Mac OS X Administrator password reset .....	245
Windows (da 2000 in poi) Administrator password reset .....	246
Password cracking .....	247
Wordlist.....	248
Password cracker.....	248
Debugger, decompiler e disassembler.....	250
Network dissector.....	250

Programmi di conversione .....	252
Scenari comuni .....	253
Posta elettronica.....	253
Microsoft Exchange.....	253
Lotus Notes.....	254
Audio, video e immagini .....	255
Player video.....	256
Editor video .....	257
Converter video .....	257
Player audio.....	258
Analisi di file e dischi .....	260
File viewer.....	260
Editor esadecimale .....	260
Programmi per il recupero dati.....	262
Windows.....	262
OS X .....	263
Linux .....	263
Programmi di ricerca sequenziale.....	263

## **Capitolo 9 Pacchetti integrati per la Digital Forensics .....265**

Premessa .....	265
X-Way Forensics.....	266
Funzioni principali .....	266
Il pacchetto X-Ways Forensics.....	268
Uso del pacchetto.....	273
Filtri.....	278
Log, report table, annotazioni e tag.....	279
Autopsy Browser v. 3.x .....	281
OSForensics.....	283
Conclusioni .....	289

## **Capitolo 10 Ambienti Live per analisi forense .....291**

Premessa .....	291
La situazione attuale.....	292
CAINE 4.....	292
Ambiente Windows .....	292
Ambiente Linux .....	293
Impressioni.....	296
DEFT 8.....	296
Ambiente Windows .....	297
Ambiente Linux .....	297
Impressioni.....	300
WINFE .....	300
PortableApps .....	301
Acquisizione .....	301
Analisi .....	301

**Capitolo 11 Una metodologia forense .....303**

Premessa.....	303
Formare una squadra.....	304
Rispetto totale per la prova .....	305
Effettuare un accertamento che possa essere ripetibile.....	306
Agire in modo da documentare ogni azione eseguita.....	306
Porre la controparte in condizione di replicare quanto fatto ...	309
Cercare di trovare la soluzione più semplice .....	310
Profiling .....	310
Analisi .....	311
Ottimizzare i tempi.....	312
Cercare di osservare la situazione da un punto di vista diverso .....	313
Non essere legati a uno specifico ambiente.....	314
Sviluppare un software secondo necessità.....	315
Garantire l'inalterabilità dei risultati.....	317
Invocare l'articolo 360 c.p.p.....	318

**Capitolo 12 Analisi di sistemi Windows .....321**

Premessa.....	321
Il problema Windows 8/8.1 .....	322
Vantaggi e svantaggi di Windows.....	324
I volumi.....	326
Registry .....	328
Thumbs.db.....	330
Shell bag.....	331
BagMRU .....	332
MRUListEx.....	333
Interpretare le shell bag.....	334
Quali dati si possono ottenere .....	334
Event viewer.....	334
Dati applicazioni e Impostazioni locali oppure Appdata .....	335
File di swap.....	336
Hiberfil.sys.....	337
Principali programmi in dotazione .....	337
Internet Explorer.....	338
Servizi cloud.....	338

**Capitolo 13 Analisi di sistemi OS X .....339**

Premessa.....	339
L'idea di fondo.....	340
Il sistema.....	342
Particolarità del sistema.....	342
Configurazioni .....	342
Analisi di un Mac.....	347

<b>Capitolo 14</b>	<b>Analisi di sistemi Linux.....</b>	<b>349</b>
	Premessa.....	349
	LSB (Linux Standard Base).....	350
	Distribuzioni.....	350
	Distribuzioni commerciali o di derivazione commerciale.....	351
	Distribuzioni free.....	352
	Il sistema.....	352
	Analisi.....	355
	Log.....	356
	Configurazione del sistema.....	358
	Home directory.....	360
	Swap.....	361
	Var.....	361
	Condivisione dati.....	362
	Peculiarità di una workstation.....	363
	Peculiarità degli ambienti server.....	363
<b>Capitolo 15</b>	<b>Gestione dei file di log.....</b>	<b>367</b>
	Premessa.....	367
	File di log: acquisizione.....	369
	Diversi scenari.....	370
	Acquisire i file di log.....	372
	File di log: analisi.....	374
<b>Capitolo 16</b>	<b>Cloud e Virtual Forensics.....</b>	<b>381</b>
	Premessa.....	381
	I servizi cloud.....	382
	Cloud Forensics.....	383
	Analisi degli artifact.....	384
	Google Drive.....	384
	Prezi.....	386
	Citrix Receiver.....	388
	Facebook.....	388
	Network Forensics.....	389
	Collaborazione con il fornitore di servizi.....	390
	Virtual Forensics.....	392
	Acquisizione.....	392
	Analisi.....	395
<b>Capitolo 17</b>	<b>Enterprise Digital Forensics.....</b>	<b>397</b>
	Design di un datacenter.....	398
	Tecnologie enterprise.....	399
	Storage.....	399
	SAN.....	401

Fibre Channel.....	401
iSCSI.....	403
Una metodologia di analisi.....	404
Premessa.....	404
Un possibile approccio.....	404
Il problema NAS.....	406
Attenzione agli snapshot.....	406

**Capitolo 18 Mobile Forensics .....407**

Premessa.....	407
Smartphone e cloud.....	408
Il mercato degli smartphone.....	409
Analisi di uno smartphone.....	410
Android.....	412
Architettura e sicurezza.....	412
Acquisizione.....	414
iOS.....	415
Architettura e sicurezza.....	415
Acquisizione.....	416
Analisi.....	416
Conclusioni.....	418

**Indice analitico.....419**