

Indice generale

Introduzione	xv
Ringraziamenti	xix
Capitolo 1	Panoramica generale.....	1
	Che cos'è la Computer Forensics?.....	1
	Applicazioni della Computer Forensics.....	3
	Una metodologia forense	4
	Una filosofia di lavoro	5
Capitolo 2	Il panorama giuridico italiano	7
	Normative applicabili in Italia	7
	La nozione di prova	10
	La prova in sede civile	11
	Cenni sui singoli mezzi di prova nel processo civile	13
	La prova in sede penale	18
	La prova in sede lavoristica	28
	Focus: aspetti specifici del controllo sui lavoratori	30
	Valenza della Computer Forensics a livello processuale.....	39
	Profili giuridici dell'acquisizione, conservazione e analisi della prova informatica	42
	Profili giuridici dei file di log	46
	Profili giuridici della Network Forensics	51
	Problematiche aperte	53
	Giurisprudenza rilevante	55
Capitolo 3	Acquisizione del dato: sequestro e duplicazione	59
	Modalità di acquisizione	59
	Ricerca.....	60
	Sequestro	61

	Alcune considerazioni.....	62
	Preservare lo stato della prova.....	63
	Personal computer.....	65
	Personal digital assistant (PDA).....	68
	Netbook.....	69
	Tastiera e mouse.....	70
	Duplicazione.....	70
	Alcune considerazioni.....	71
	Software da utilizzare.....	73
	Il problema dei RAID.....	75
	Il write blocker.....	77
	Copia di un sistema Live.....	83
Capitolo 4	Intercettazione del dato.....	85
	Premessa.....	85
	Una questione di trasparenza.....	85
	Hardware.....	89
	Software.....	90
	Configurazione.....	91
	tcpdump.....	93
	tshark.....	94
	Conservazione e analisi.....	95
Capitolo 5	Il laboratorio di analisi.....	97
	Premessa.....	97
	Concetti generali.....	98
	OpenAFS.....	99
	Architettura del laboratorio di analisi.....	101
	Connessioni di rete.....	102
	Macchina da analisi/acquisizione.....	102
	Cabinet capiente ma facilmente trasportabile.....	102
	Elevata velocità di I/O.....	103
	Reparto dischi efficiente e di grande capacità.....	103
	Sistema RAID.....	104
	Grande adattabilità nei collegamenti.....	104
	Macchine da analisi/test.....	106
	File/application server.....	106
	Backup.....	107
	Software.....	107
	Sistema operativo.....	109
	LiveCD.....	111
	Distribuzione general purpose.....	112
	Scegliere la distribuzione.....	112
Capitolo 6	Media, partizioni e volumi.....	115
	Premessa.....	115
	Comandi e funzioni Unix.....	116

Gestione delle immagini disco	116
Sistemi di partizionamento.....	120
Il mondo non è mai semplice.....	129
Linux LVM	130
Linux Software RAID	131
Windows Dynamic Disk (LDM) e Software RAID.....	132
Analisi preliminare	133
Capitolo 7	
File system.....	139
Premessa	139
Caratteristiche comuni ai file system	139
Dati, metadati e altre strutture	140
Logica di funzionamento	141
Principali file system	143
FAT.....	143
Considerazioni a livello di analisi.....	147
NTFS.....	147
Allocazione dei cluster.....	153
Runlist.....	154
Principali attributi nelle entry MFT.....	157
Indici.....	159
Strutture metadati esterne	162
Novità introdotte nella nuova release (informalmente NTFS v. 6.0).....	166
Ext2 ed Ext3	167
Il superblock.....	168
Group description table	170
Block bitmap e inode bitmap.....	170
Inode	170
Attributi estesi	172
Directory entry.....	174
Link simbolici.....	175
Journal	175
ReiserFS.....	177
Struttura di ReiserFS	178
HFS+	184
Struttura di HFS+	184
ZFS	187
Concetti chiave.....	188
zpool e device	190
Boot block	192
Puntatori ai blocchi, diretti e indiretti.....	193
Gestione degli oggetti, metadati e relazioni.....	195
Gestione di snapshot e dataset.....	198
Oggetti ZAP	202
ZFS, ZPL	206
Intent log	207
Conclusioni su ZFS.....	208

Capitolo 8	Tool e programmi di analisi	209
	Premessa	209
	Categorie	210
	Sistemi di virtualizzazione	212
	VMware	212
	Parallels	214
	XEN	214
	QEMU	215
	KVM.....	215
	Programmi di hacking e cracking.....	216
	Casi possibili.....	216
	Password resetting.....	218
	Password cracking.....	221
	Debugger, decompiler, disassembler.....	225
	Network dissector.....	225
	Programmi di conversione	227
	Scenari comuni	227
	Posta elettronica.....	228
	Audio, video e immagini	231
	Analisi di file e dischi	236
	File viewer.....	236
	Editor esadecimale	237
	Analisi tramite strumenti Open Source	238
	Data recovery	250
Capitolo 9	X-Ways Forensics	253
	Premessa	253
	Principali funzioni	254
	Il pacchetto X-Ways Forensics.....	255
	Conclusioni	264
Capitolo 10	Linux forensics live distribution.....	265
	Premessa	265
	La situazione attuale.....	265
	Acquisizione	266
	Analisi	267
	Le distribuzioni Live	268
	Helix.....	268
	DEFT.....	276
	CAINE	282
Capitolo 11	Metodologia di analisi generale	285
	Premessa	285
	Formare una squadra.....	286
	Rispetto totale per la prova	287
	Effettuare un accertamento che possa essere ripetibile.....	288

	Agire in modo da documentare ogni azione eseguita.....	288
	Porre la controparte in condizione di replicare quanto fatto	291
	Cercare di trovare la soluzione più semplice	292
	Profiling	292
	Analisi	293
	Ottimizzare i tempi.....	294
	Cercare di osservare la situazione da un punto di vista diverso	295
	Non essere legati a uno specifico ambiente.....	296
	Sviluppare un software secondo necessità.....	298
	Garantire l'inalterabilità dei risultati.....	299
	Invocare l'articolo 360 c.p.p.....	300
Capitolo 12	Analisi di un sistema Windows.....	303
	Premessa	303
	Vantaggi e svantaggi di Windows.....	303
	Inizio dell'analisi	305
	Registry	306
	Thumbs.db.....	308
	Event viewer.....	309
	Dati applicazioni e Impostazioni locali	310
	File di swap.....	311
	Hiberfil.sys.....	311
	Caching delle password.....	311
	Principali programmi in dotazione	313
	Internet Explorer.....	313
	Outlook Express.....	314
	Windows LiveCD.....	315
	Data hiding.....	316
Capitolo 13	Analisi di un sistema Mac OS X	317
	Premessa	317
	L'idea di fondo.....	317
	Il sistema.....	319
	Particolarità del sistema.....	319
	Configurazioni	319
	Data hiding.....	327
Capitolo 14	Analisi di un sistema Linux.....	331
	Premessa	331
	LSB (Linux Standard Base).....	332
	Distribuzioni	332
	Il sistema.....	334
	Analisi	337
	Log.....	337
	Configurazione del sistema	340
	Home directory.....	341
	Swap	343

	Var	343
	Condivisione dati	343
	Data hiding.....	344
Capitolo 15	File di log.....	347
	Premessa.....	347
	File di log: acquisizione	348
	File di log: analisi.....	349
Capitolo 16	Network Forensics	359
	Premessa.....	359
	Sistemi ad appannaggio delle forze dell'ordine.....	360
	Intrusion Detection System.....	362
	Validazione dei dati.....	363
	Decodifica dei dati.....	364
	Wireshark in azione	365
	Xplico	369
	P2P Marshall	370
	Uno sguardo al futuro.....	372
Capitolo 17	Media non convenzionali	373
	Premessa.....	373
	Apple iPod.....	373
	Sony PSP.....	377
	Dispositivi Archos	377
	Lettori mp3 e macchine fotografiche digitali	379
Capitolo 18	Mobile Forensics.....	381
	Premessa.....	381
	Telefoni cellulari e crimini	382
	Componenti di un sistema mobile	386
	SIM.....	386
	Memory card.....	388
	Telefono	388
	Metodologia di analisi.....	389
	Ambiente	389
	Analisi	390
	Tool di analisi	392
	Ufed Cellebrite	393
	Oxygen Forensics Suite 2	396
Capitolo 19	CD e DVD	401
	Premessa.....	401
	Formati e struttura dei supporti ottici.....	402
	Formati di un CD	402
	Struttura di un CD	403

	Formati di un DVD	403
	Tipi di supporti DVD	404
	Struttura di un DVD	405
	Modalità di scrittura delle tracce DVD	405
	Masterizzazioni single session e multisession	406
	Multisession e analisi forense	407
	Packet writing	408
	File system	409
	File system: ISO 9660, UDF, HFS	409
	Visione logica di un CD e di un DVD	410
	Analisi multilivello	411
	Livello fisico: analisi visiva del supporto e verifica dell'integrità fisica	411
	Livello fisico: identificazione del tipo di supporto	412
	Livello sessione e livello file system	414
	Un caso di studio reale	414
	Metodologia di copia e verifica di un supporto ottico	423
	Creazione di un file di immagine	424
	Disaster recovery di un supporto ottico	425
	Conclusioni	426
Appendice A	Limiti e ostacoli	429
	Premessa	429
	Crittografia	429
	Steganografia	430
	Data hiding	431
	Macchine virtuali	432
	Multimedia	434
Appendice B	Esempi di casi reali	435
	Premessa	435
	Casi	435
	Furto di un portatile	435
	Spionaggio industriale	436
	Cacciatore di teste	437
	Intercettazione su Skype	437
	Rivendicazione	438
	Estrazione file da un DAT	439
	FileVault	439
Appendice C	Associazioni e certificazioni	441
	Premessa	441
	IISFA Italian Chapter	441
	Formazione e convegni	442
	Centro di competenza	444
Indice analitico	445