

Indice generale

Autore e revisori	XV
Introduzione	xix
Ringraziamenti	xx
Capitolo 1 L'ambito della Digital Forensics	1
Obiettivi	1
Miti comuni sulla Computer Forensics	2
Mito 1: Computer Forensics e sicurezza informatica sono la stessa cosa	2
Mito 2: Computer Forensics è l'indagine sui computer	2
Mito 3: la Computer Forensics è l'indagine su crimini informatici	3
Mito 4: la Computer Forensics è usata in realtà per riesumare file cancellati	3
Tipi di prove forensi digitali recuperate	4
Posta elettronica (email)	4
Immagini	6
Video	7
Siti web visitati e ricerche in Internet	8
Cellphone Forensics	9
IoT Forensics	9
Quali competenze deve avere un investigatore forense?	9
Conoscenze di informatica	9
Conoscenze giuridiche	10
Capacità di comunicazione	10
Capacità linguistiche	11
Formazione continua	11
Programmazione	11
Riservatezza	11
L'importanza della Digital Forensics	12

Possibilità di lavoro.....	12
Storia della Digital Forensics	14
Anni Ottanta: l'arrivo del personal computer	14
Anni Novanta: l'impatto di Internet	15
Anni 2000: valute virtuali, IoT, crittografia ed effetto Edward Snowden.....	19
Training e istruzione	20
Training presso le forze dell'ordine.....	20
Formazione nelle scuole superiori.....	21
Formazione universitaria.....	21
Certificazioni professionali.....	21
Riepilogo	25
Glossario.....	27
Valutazione	28
Domande a risposta aperta	28
Domande a risposta multipla.....	28
Completa le frasi.....	30
Progetti	31

Capitolo 2 Windows e il suo file system.....33

Obiettivi.....	33
Memoria fisica e logica	35
Memorizzazione di file	35
Paginazione	38
Sistemi di numerazione e conversioni.....	41
Conversione da binario a decimale.....	41
Sistema esadecimale	41
Conversione da esadecimale a decimale.....	42
Conversione da esadecimale ad ASCII.....	43
Uso dell'esadecimale per identificare il tipo di file	46
Unicode	46
Sistemi operativi	46
Il processo di boot	46
File system di Windows.....	48
Registro di Windows	57
I tipi di dati del Registro.....	59
FTK Registry Viewer.....	60
Microsoft Office	60
Caratteristiche di Microsoft Windows.....	61
Windows Vista	61
Deframmentazione in Vista	61
Windows 7.....	66
Windows 8.1	77
Windows 10.....	79
Microsoft Office 365	80
Riepilogo	80

Valutazione	84
Domande a risposta aperta	84
Domande a risposta multipla	85
Completa le frasi	86
Progetti	87

Capitolo 3 Gestione dell'hardware dei computer89

Obiettivi	89
Unità disco	90
Small Computer System Interface (SCSI)	90
Integrated Drive Electronics (IDE)	91
Serial ATA (SATA)	92
Clonazione di un disco PATA o SATA	94
Clonazione di dispositivi	95
Memoria rimovibile	102
FireWire	102
Flash drive USB	103
Dischi esterni	104
MultiMedia Card (MMC)	105
Riepilogo	115
Glossario	116
Valutazione	117
Domande a risposta aperta	117
Domande a risposta multipla	118
Completa le frasi	119
Progetti	120
Bibliografia	120

Capitolo 4 Acquisire prove in un laboratorio di Computer Forensics121

Obiettivi	121
Requisiti per un laboratorio	122
American Society of Crime Laboratory Directors (ASCLD) ..	122
American Society of Crime Laboratory Directors/Lab Accreditation Board (ASCLD/LAB)	122
Linee guida dell'ASCLD/LAB per pratiche gestionali di laboratori forensi	123
ISO/IEC 17025:2017	124
Scientific Working Group on Digital Evidence (SWGDE)	124
Laboratori di Computer Forensics del settore privato	125
Laboratorio di acquisizione delle prove	126
Laboratorio di preparazione delle email	126
Controllo dell'inventario	126
Sistemi di gestione delle informazioni di laboratorio	126
Web hosting	127

Requisiti per un laboratorio di Computer Forensics.....	127
Layout del laboratorio.....	127
Gestione del laboratorio	148
Estrazione di evidenze da un dispositivo	151
Utilizzo dell'utility dd.....	151
Utilizzo di GREP (Global Regular Expressions Print)	152
Skimmer.....	158
Steganografia	161
Riepilogo	161
Valutazione	164
Domande a risposta aperta	164
Domande a risposta multipla.....	164
Completa le frasi.....	166
Progetti	167

Capitolo 5 Indagini online.....169

Obiettivi.....	169
Lavorare “sotto copertura”.....	170
Generazione di un'identità.....	171
Generazione di un account email.....	173
Mascheramento dell'identità	175
Indagini nel Dark Web	177
OSINT Framework.....	177
Tor	178
Invisible Internet Project.....	179
Freenet.....	179
SecureDrop	179
Marketplace del Dark Web.....	180
Valute virtuali	181
Bitcoin	182
Venmo e Vicemo	183
Prove da siti web.....	183
Archivi dei siti web.....	183
Statistiche sui siti web	184
Ricerche di base su un sospettato	185
Ricerca di informazioni personali	185
Interessi personali e gruppi di utenti	189
Ricerca di beni rubati.....	190
Crimini online.....	203
Furto di identità	204
Numeri di carte di credito in vendita.....	204
Cartelle mediche elettroniche	204
Contraffazioni e indagini di controproliferazione	205
Cyberbullismo	205
Social network.....	205
Cattura di comunicazioni online	206

	Cattura dello schermo	206
	Utilizzo del video	207
	Visualizzazione dei cookie	208
	Utilizzo del Registro di Windows	208
	Il browser Edge	209
	Riepilogo	209
	Glossario.....	210
	Valutazione	212
	Domande a risposta aperta	212
	Domande a risposta multipla.....	212
	Completa le frasi.....	214
	Progetti	214
Capitolo 6	Documentare l'indagine.....	217
	Obiettivi.....	217
	Ottenere evidenze da un fornitore di servizi.....	218
	Documentare una scena del crimine.....	219
	Sequestro delle prove	220
	Esame della scena del crimine	221
	Apparecchiature per l'investigatore della scena del crimine	221
	Documentazione delle prove.....	222
	Compilazione di un modulo per la catena di custodia	223
	Compilazione di un foglio di lavoro per computer	224
	Compilazione di un foglio di lavoro per disco rigido.....	225
	Compilazione di un foglio di lavoro per server.....	225
	Strumenti per documentare un'indagine	227
	FragView.....	227
	App utili per mobile	227
	Stesura di rapporti.....	228
	Fusi orari e ora legale.....	229
	Creazione di un rapporto comprensibile	230
	Testimonianza di esperti in tribunale	234
	Il testimone esperto	234
	Gli obiettivi del testimone esperto	235
	Preparazione di un testimone esperto per il processo	235
	Riepilogo	237
	Glossario.....	238
	Valutazione	238
	Domande a risposta aperta	238
	Domande a risposta multipla.....	238
	Completa le frasi.....	240
	Progetti	241
Capitolo 7	Network Forensics e risposta agli incidenti.....	243
	Obiettivi.....	243
	Gli strumenti	244

Dispositivi di rete.....	245
Server proxy	246
Server web	246
Server DHCP.....	249
Log DHCP.....	251
Hub	252
Switch.....	252
Server SMTP.....	252
Server DNS.....	254
Il file hosts.....	255
Protocollo DNS	256
Internet Corporation for Assigned Names and Numbers (ICANN)	256
Traceroute	256
Router	256
IDS	264
Firewall	266
Porte	267
Il modello OSI	267
Il livello fisico	268
Il livello del collegamento dati	268
Il livello di rete	269
Il livello del trasporto.....	269
Il livello di sessione	271
Il livello di presentazione	271
Il livello di applicazione	271
Introduzione a VoIP (Voice over Internet Protocol)	272
Svantaggi di VoIP	273
PBX (Private Branch Exchange)	273
Session Initiation Protocol (SIP).....	274
STUN (Simple Traversal of UDP Through NAT)	275
La risposta agli incidenti: Incident Response (IR)	275
STIX, TAXII e Cybox	276
Advanced persistent threat.....	276
APT10	277
Cyber Kill Chain.....	277
Indicatori di compromissione.....	281
Indagine sull'attacco a una rete.....	284
Random Access Memory (RAM)	284
AmCache	284
ShimCache.....	284
ShellBag	285
Volume Shadow Copy	285
Endpoint Detection and Response (EDR).....	285
Kibana.....	286
Log2Timeline/Plaso	286
SANS SIFT Workstation.....	286

Windows Registry.....	288
Riepilogo	290
Glossario.....	291
Valutazione	293
Donande a risposta aperta	293
Domande a risposta multipla.....	293
Completa le frasi.....	295
Progetti	296
Capitolo 8 Mobile Forensics	297
Obiettivi.....	297
La rete cellulare.....	299
Stazione ricetrasmittente base.....	300
Mobile Station.....	303
Tipi di telefoni cellulari	308
SIM card Forensics	310
Tipi di evidenze	313
Specifiche degli apparecchi	314
Memoria e capacità di elaborazione	314
Batteria.....	314
Altro hardware.....	314
Sistemi operativi per il mobile.....	315
Android.....	315
Symbian OS	324
BlackBerry 10	324
Windows Phone.....	324
Procedure operative standard per gestire prove da mobile.....	324
National Institute of Standards and Technology (NIST).....	324
Esame forense dell'apparecchio	329
Strumenti di Cellphone Forensics	329
Esame logico o fisico	331
Esami manuali dei cellulari.....	331
Flasher box	332
Global Satellite Service Provider	332
Servizi di comunicazione satellitari	333
Considerazioni legali.....	333
National Crime Information Center (NCIC)	333
Altri dispositivi mobili	335
Tablet	335
GPS tracking	336
Documentazione dell'indagine	337
Riepilogo	337
Glossario.....	338
Valutazione	342
Domande a risposta aperta	342
Domande a risposta multipla.....	342

Completa le frasi.....	344
Progetti	344

Capitolo 9 Indagini su app mobile.....347

Obiettivi.....	347
Analisi statica e analisi dinamica.....	348
Analisi statica	348
Analisi dinamica	353
Introduzione a Debookee	354
App di appuntamenti	362
Tinder.....	363
Grindr.....	366
App di ridesharing.....	371
Uber	372
App di comunicazione.....	374
Skype	374
Riepilogo	377
Glossario.....	377
Valutazione.....	378
Domande a risposta aperta	378
Domande a risposta multipla.....	378
Completa le frasi.....	378
Progetti	379

Capitolo 10 Photograph Forensics381

Obiettivi.....	381
National Center for Missing and Exploited Children (NCMEC).....	383
Project VIC.....	384
Casi	384
Selfie in Facebook	384
Cattura di un predatore.....	384
Estorsione.....	385
Introduzione alla fotografia digitale	385
File system.....	385
Applicazioni e servizi per la fotografia digitale.....	386
Esame di file di immagini	387
Exchangeable Image File Format (EXIF)	387
Ammissibilità come prove	390
Federal Rules of Evidence (FRE)	391
Fotografie analogiche e digitali	391
Casi.....	392
Caccia all'uomo a livello mondiale.....	392
NYPD Facial Recognition Unit.....	394
Riepilogo	394
Glossario.....	394

Valutazione	395
Domande a risposta aperta	395
Domande a risposta multipla	396
Completa le frasi	397
Progetti	398
Capitolo 11 Mac Forensics	399
Obiettivi	399
Un po' di storia	400
Macintosh	400
Mac mini con OS X Server	400
iPod	401
iPhone	402
iPad	403
iPad Pro	403
Apple Watch	404
Dispositivi Wi-Fi Apple	406
Apple TV	406
AirPort Express	407
AirPort Extreme	407
AirPort Time Capsule	407
Macintosh File System	408
Hierarchical File System (HFS)	408
HFS+	408
APFS	409
Esami forensi su un Mac	413
Epoch time	415
DMG	416
File PList	417
Database SQLite	418
File di email	419
File di ibernazione	419
I sistemi operativi Macintosh	419
macOS Catalina	420
FileVault	420
Disk Utility (Utilità disco)	421
macOS Keychain (Portachiavi)	421
iCloud Keychain (Portachiavi)	421
Display multipli	421
Notifiche	421
Tag	422
Safari	422
Target Disk Mode e la clonazione di dispositivi	424
Dispositivi mobili Apple	425
iOS	425
Configurazione di dispositivi Apple a livello d'impresa	442

Batteria.....	442
Esecuzione di un esame forense su un Mac	442
Casi	444
Trova il mio iPhone.....	445
Hacktivistà ricercato	445
Michael Jackson.....	445
iPhone rubato.....	445
Sequestro di droga	445
Processo per omicidio.....	446
Riepilogo	446
Glossario.....	446
Valutazione	449
Domande a risposta aperta	449
Domande a risposta multipla.....	450
Completa le frasi.....	451
Progetti	452

Capitolo 12 Casi di studio453

Obiettivi.....	453
Silk Road	454
Genesi di Silk Road.....	455
Minaccia di morte	457
La chiusura di Silk Road.....	458
La cattura di Ulbricht	458
Predibattimento.....	460
Ross Ulbricht a processo	461
Evidenze dal laptop	462
La sentenza.....	462
Il massacro di Las Vegas	464
Zacharias Moussaoui.....	466
Background.....	466
Evidenze digitali.....	467
Obiezioni dello Standby counsel.....	468
Dichiarazione giurata per l'accusa	468
Reperti.....	469
Il serial killer BTK (bind torture kill)	470
Profilo di un omicida.....	470
Evidenze	471
Cyberbullismo	472
Legislazione federale contro le molestie.....	472
Legislazione statale contro le molestie	472
Indizi di cyberbullismo	472
Che cos'è il cyberbullismo?.....	473
Phoebe Prince.....	473
Ryan Halligan	474
Megan Meier.....	474

Tyler Clementi	474
Sport	476
Riepilogo	477
Glossario.....	478
Valutazione	478
Domande a risposta aperta	478
Domande a risposta multipla	479
Completa le frasi.....	479
Progetto: analisi di un caso di cyberbullismo	480

Capitolo 13 Internet of Things (IoT) Forensics e tecnologie emergenti487

Obiettivi.....	487
5G.....	488
Wi-Fi 6	490
Reti mesh Wi-Fi.....	491
Shodan	491
Mirai Botnet.....	493
Mining di criptovalute	493
Alexa	493
Microchip.....	494
Fitness tracker	495
Apple Watch	496
Action camera	498
Sicurezza delle forze di polizia.....	498
Veicoli della polizia	500
Vehicle Forensics.....	500
Una soluzione low-tech per trovare dispositivi high-tech.....	501
Riepilogo	502
Glossario.....	502
Valutazione	503
Domande a risposta aperta	503
Domande a risposta multipla.....	504
Completa le frasi.....	505
Progetti	506

Appendice A Il panorama giuridico italiano507

Normative applicabili in Italia	507
La nozione di prova	511
La prova in sede civile	512
Cenni sui singoli mezzi di prova nel processo civile	516
La prova in sede penale	522
La prova in sede lavoristica	536
Focus: aspetti specifici del controllo sui lavoratori	538
Valenza della Digital Forensics a livello processuale	546

Profili giuridici dell'acquisizione, conservazione e analisi della prova informatica	552
Profili giuridici dei file di log	557
Profili giuridici della Network Forensics	567
Problematiche aperte	569

Appendice B Risposte573

Domande a risposta multipla	573
Completa le frasi	574

Indice analitico.....583