

SOMMARIO

DEL VOLUME III

CAPITOLO 11 **QUALITY MANAGEMENT E DIGITAL FORENSICS INDUSTRIALE**

a cura di Marco MATTIUCCI

- | | |
|---|----|
| 1. Descrizione di un approccio sistemico alla produzione di servizi di <i>digital forensics</i> industriale | 3 |
| 2. <i>Digital forensics</i> “semplice” e <i>digital forensics</i> industriale | 10 |

CAPITOLO 12 **WINDOWS FORENSICS**

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

- | | |
|--|----|
| 1. Premessa | 15 |
| 2. Sistemi operativi Windows | 15 |
| 2.1 Microsoft Windows XP | 16 |
| 2.2 Microsoft Windows Vista | 18 |
| 2.3 Microsoft Windows 7 | 19 |
| 3. Analisi forense di un sistema operativo Windows | 20 |
| 3.1 File di installazione | 20 |
| 3.2 Registro di sistema | 23 |
| 3.3 Hive SOFTWARE | 27 |
| 3.4 Hive SYSTEM | 34 |
| 3.5 Hive SAM | 40 |
| 3.6 Hive NTUSER | 42 |

4. Strumenti per l'analisi del registro di sistema	46
5. Risorse online e articoli relativi all'analisi del registro	55
6. Profilo utente	57
6.1 Profilo utente nei sistemi operativi Windows 2000\XP	58
6.2 Profilo utente nei sistemi operativi Windows Vista\7	58
7. Collegamenti e file LNK	59
7.1 Strumenti per l'analisi dei file LNK	60
7.2 Risorse online e articoli relativi all'analisi dei collegamenti	65
8. Cestino	66
8.1 Cestino nei sistemi operativi 2000\XP	66
8.2 Cestino nei sistemi operativi Vista\7	67
8.3 Strumenti per l'analisi del cestino	68
8.4 Risorse online e articoli relativi all'analisi del cestino	72
9. Registro Eventi	72
9.1 Registro eventi nei sistemi operativi NT\2000\XP	73
9.2 Registro eventi nei sistemi operativi Vista\7	73
9.3 Strumenti per l'analisi del registro eventi	73
9.4 Risorse online e articoli relativi all'analisi del registro eventi	76
10. Prefetch	77
10.1 Strumenti per l'analisi del prefetch	79
10.2 Risorse online e articoli relativi all'analisi del prefetch	83
11. Thumbnails	84
11.1 Thumbnails nei sistemi operativi 2000\XP	84
11.2 Thumbnails nei sistemi operativi Vista\7	85
11.3 Strumenti per l'analisi delle thumbnails	86
11.4 Risorse online e articoli relativi all'analisi delle thumbnails	92
12. Spool di stampa	93
12.1 Strumenti per l'analisi dei file di spool	94
12.2 Risorse online e articoli relativi all'analisi degli spool di stampa	96
13. Analisi forense delle principali applicazioni per sistemi Windows	97
14. Navigazione su Internet	97
14.1 Internet Explorer	98
14.1.1 Informazioni di navigazione nei sistemi operativi XP\2003	98

14.1.2 Informazioni di navigazione nei sistemi operativi Vista\7	98
14.1.3 Informazioni di navigazione conservate all'interno del registro	99
14.1.4 Strumenti per l'analisi della navigazione con Internet Explorer	99
14.1.5 Risorse online e articoli relativi all'analisi dei file di Internet Explorer	107
14.2 Mozilla Firefox	108
14.2.1 Informazioni di navigazione nei sistemi operativi XP\2003	108
14.2.2 Informazioni di navigazione nei sistemi operativi Vista\7	109
14.2.3 Strumenti per l'analisi della navigazione con Mozilla Firefox	109
14.2.4 Risorse online e articoli relativi all'analisi dei file di Mozilla Firefox	117
14.3 Google Chrome	118
14.3.1 Informazioni di navigazione nei sistemi operativi XP\2003	118
14.3.2 Informazioni di navigazione nei sistemi operativi Vista\7	119
14.3.3 Strumenti per l'analisi della navigazione con Google Chrome	119
14.3.4 Risorse online e articoli relativi all'analisi dei file di Google Chrome	123
14.4 Apple Safari	124
14.4.1 Informazioni di navigazione nei sistemi operativi XP\2003	124
14.4.2 Informazioni di navigazione nei sistemi operativi Vista\7	125
14.4.3 Strumenti per l'analisi della navigazione con Apple Safari	125
14.4.4 Risorse online e articoli relativi all'analisi dei file di Apple Safari	127
15. Posta Elettronica	128
15.1 Microsoft Outlook	128
15.1.1 Strumenti per l'analisi della posta elettronica su Microsoft Outlook	129

15.1.2 Risorse online e articoli relativi all'analisi dei file di Microsoft Outlook	136
15.2 Microsoft Outlook Express	137
15.2.1 Strumenti per l'analisi della posta elettronica su Microsoft Outlook Express	139
15.2.2 Risorse online e articoli relativi all'analisi dei file di Microsoft Outlook Express	142
15.3 Windows Mail	143
15.3.1 Strumenti per l'analisi della posta elettronica su Windows Mail	143
16. File Sharing	145
16.1 Strumenti per l'analisi dei software di file sharing	145
17. Instant Messaging e Chat	157
17.1 Strumenti per l'analisi dei software di Instant Messaging	157
18. Altri elementi di interesse in fase di analisi	162
19. Software di analisi forense per Windows	162
19.1 Suite per l'analisi forense	163
19.2 Software di Acquisizione	172
19.3 Data Recovery	174
19.4 Password Cracking	183
19.5 Metadati	196
19.6 Strumenti per l'analisi dei metadati	198
19.7 Ricerca per parola chiave	207

CAPITOLO 13

MACINTOSH FORENSICS

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Premessa	212
2. Sistema Operativo Mac OS X	212
3. Partizionamento di un Macintosh	228
4. Macintosh Boot Process	230
5. Acquisizione forense di un Mac	233
6. Analisi forense di un Mac	240
6.1 Property List File	240
6.2 Database Sqlite3	241
6.3 Impostazioni generali del Sistema	243
6.3.1 Struttura delle cartelle	243

6.3.2 Versione del Sistema Operativo e data di installazione	244
6.3.3 Timezone	245
6.3.4 Informazioni di login e utenti cancellati	246
6.3.5 Aggiornamento del Software	247
6.3.6 Configurazioni di Rete	247
6.4 Profilo Utente	249
6.4.1 Account Utente e gruppi del Sistema	250
6.4.2 Password degli account Utente	252
6.4.3 Cartelle del Profilo Utente	254
6.4.4 Cartella Utente Library	256
6.5 Tracce di navigazione su Internet	259
6.5.1 Safari	259
6.5.2 Mozilla Firefox	263
6.6 Strumenti di Posta Elettronica, Chat e Calendario	264
6.6.1 Apple Mail	265
6.6.2 Rubrica Indirizzi	267
6.6.3 iChat, Skype e Microsoft Messenger	268
6.6.4 Apple iCal	272
6.7 Applicazioni Multimediali	273
6.7.1 iTunes	274
6.7.2 iPhoto	275
6.7.3 iMovie e iDVD	276
6.8 Strumenti di Office Automation	277
6.8.1 Microsoft Office	278
6.8.2 OpenOffice	282
6.9 File di Log	282
6.9.1 Log delle operazioni di logon/logoff	285
6.10 File Vault	285
6.10.1 Accesso ai dati senza protezione (analisi live)	287
6.11 Accesso ai dati protetti (password cracking)	288
6.12 Software di analisi forense per Mac	289
6.13 Toolkit Forensi	290
6.14 Software di visualizzazione file di sistema	295
6.15 Software di acquisizione e mounting	299
6.16 Software di data recovery	304

CAPITOLO 14
WINDOWS MEMORY FORENSICS

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Introduzione	311
2. Acquisizione della memoria principale	312
3. Problematiche e limiti nella fase di acquisizione della memoria	322
4. Perché acquisire la memoria principale	326
5. Metodologie di acquisizione della memoria	328
6. Strumenti di acquisizione della memoria	335
7. Introduzione all'analisi della memoria: esempi di analisi	348
8. Altri strumenti di acquisizione della memoria	365
9. Anti-Forensics nella fase di acquisizione della memoria	368

CAPITOLO 15
**CRIMEWARE FORENSICS. INTRODUZIONE
ALL'ANALISI DEI MALWARE E AL
FUNZIONAMENTO DEI CRIMEWARE IN UN
CONTESTO DI INFORMATION FORENSICS**

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Introduzione	375
2. <i>Malware</i> e <i>Crimeware</i>	376
3. Ciclo di Vita di un <i>Malware</i>	382
4. <i>Malware Forensics</i>	388

CAPITOLO 16
**TECNICHE DI ATTACCHI INFORMATICI A SITI WEB: ANALISI
DELLE CASISTICHE E LOG ANALYSIS**

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Premessa	409
2. Cenni teorici di base: Tipologie di sistemi coinvolti nell'erogazione di un servizio Web	410

3. Web server	411
4. IDS/IPS	412
5. Firewall	413
6. Reverse Proxy	414
7. Il concetto di “regular expression”	414
8. Utilizzo delle espressioni regolari	416
9. I log	416
10. Elementi generali sul log di traffico di rete	418
11. Elementi teorici per l’analisi dei log di un web server	419
12. Tecniche di attacco informatico “base”: la metodologia espositiva	422
13. Riferimenti a standard e metodologie	423
14. Open Web Application Security Project (OWASP)	423
15. Cenni alla metodologia DREAD per la valutazione dell’impatto di attacchi informatici	424
16. Le principali tipologie di attacco “base”	426
17. Attacchi abilitati da erronea validazione degli input	427
18. SQL Injection (e altre Injection Flaws)	427
19. Cross-site Scripting (XSS)	431
20. Hidden-Field Tampering	434
21. Attacchi al sistema di autenticazione	436
22. Brute Force	436
23. Failure to Restrict URL Access	438
24. Broken Authentication and Session Management	439
25. Cross Site Request Forgery (CSRF o XSRF)	443
26. Attacchi a elementi sul server	445
27. Information Leakage e Improper Error Handling	446
28. Malicious File Execution (abilitato da Remote File Inclusion)	448
29. Insecure Direct Object Reference	450
30. Denial of Service su applicazioni Web	451
31. Defacement	453
32. Scenari di attacco avanzati	455
32.1 Esempi di scenario di attacco	455
32.2 Creazione di shell PHP tramite SQL injection	455
32.3 Concetti preliminary	456
33. Scenario di attacco	457
34. “CRLF Injection” e alterazione di Header HTTP	459
35. CSRF e intercettazione di email	460
36. Approcci al rilevamento degli attacchi	462

37. Miglioramento delle tecniche manuali di analisi dei log	462
38. Le librerie di regular expression	463
39. Analisi e rilevamento tramite proxy	464
40. Strumenti per l'analisi automatica	465
40.1 Il plugin "SCALP"	466
40.2 OSSEC	466
40.3 Logwatch	467
40.4 Analog	468

CAPITOLO 17

MOBILE FORENSICS

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Premessa	475
2. I dispositivi mobili	475
3. Cenni alle architetture hardware e software	477
3.1 L'architettura hardware e software di un generico PDA	477
3.2 L'architettura hardware e software di un generico cellulare	479
4. Specificità sui dispositivi cellulari	482
5. Il Subscriber Identity Module (SIM)	484
6. Cenni all'architettura delle reti di telefonia mobile	486
6.1 Componenti fondamentali di una rete per telefonia mobile	487
6.2 Servizi offerti dalle reti di telefonia mobile	488
7. Cenni all'architettura dei servizi RIM (BlackBerry)	489
8. Cenni sulla connettività a corto raggio	490
9. Dispositivi potenzialmente sincronizzati	491
10. Periferiche di memorizzazione	493
11. Cablaggi e "docking station"	495
11.1 Cavi caricabatterie	496
11.2 Cavi per connessione dati	496
11.3 Docking station	498
12. La conservazione sicura del dispositivo fisico	500
12.1 PDA e dispositivi basati prevalentemente su memoria volatile	501
12.2 Cellulari e dispositivi basati prevalentemente su memorie allo stato solido	503

13. La conservazione sicura delle informazioni sul dispositivo	504
14. La gestione della connettività wireless	505
14.1 Connettività generica (a corto raggio e cellulare)	505
14.2 Connettività cellulare/GPRS/3G	507
14.3 Connettività RIM o altre connettività “push”	508
15. Le informazioni per la catena di custodia	508
16. Acquisizione forense dei dati ed analisi del dispositivo	511
16.1 Dispositivi “obstructed” o “unobstructed”	511
16.2 Acquisizione fisica o logica dei dati	512
16.3 Soluzioni e best practices a supporto dei processi di acquisizione	514
16.3.1 Calcolo di hash	515
16.3.2 Utilizzo di ambiente “sterile”	516
16.3.3 Tracciatura delle operazioni	518
16.3.4 Accesso in sola lettura ai dispositivi	520
16.3.5 Tipologie di file “frequenti” su tutti i device	521
17. Informazioni specifiche per i device mobili con funzionalità “cellulare”	523
18. Informazioni specifiche per i device con funzionalità “BlackBerry”	525
19. Analisi delle memorie (integrate o rimovibili)	526
19.1 Memoria integrata	527
19.2 Memoria sulla (U)SIM	528
19.3 Memoria rimovibile	529
19.4 Analisi dei dispositivi potenzialmente sincronizzati a quelli d’interesse	529
20. Analisi dei dispositivi mobili	530
20.1 Il problema del calcolo dell’hash	530
20.2 Approccio “manuale” tramite console di comando (locale o remota)	531
20.3 Approccio tramite software di connettività non forense	531
20.4 Tool di assistenza e riprogrammazione	533
20.5 Approccio tramite tool forensi specifici	533
20.6 Matrice di compatibilità	534
20.7 Elementi d’uso sui tool più diffusi	535
20.7.1 Tool specifici per l’analisi diretta della SIM/USIM	536
20.7.2 Forensic Card Reader	536
20.7.3 Forensic SIM Toolkit	537
20.7.4 SIMCon	538

20.7.5 SIMIS	538
20.7.6 USIMDetective	538
20.8 Strumenti per l'analisi di schede di memoria flash	538
20.9 Tool per analisi di dispositivi	539
20.9.1 Device Seizure	540
20.9.2 PocketPC forensic software	540
20.9.3 ABC Amber BlackBerry Converter	540
20.9.4 iPod Data Recovery	541
20.9.5 Lantern per iPhone/iPod Touch	541
20.10 Tool integrati	541
20.10.1 Oxygen Forensic Suite	542
20.10.2 Paraben Cell Seizure	543
20.10.3 Logicube CellDek	544
20.10.4 MicroSystemation Forensic Toolkit	544
20.10.5 MOBILedit! Forensic	545
20.10.6 Secure View	545
20.10.7 EnCase	546
20.11 Approccio tramite tool installati su memory card	547
21. Guida pratica per gli investigatori sulle attività "base di "mobile forensics"	549
21.1 Schema generale per l'analisi del dispositivo	551
22. Mappatura tra informazioni e obiettivi d'indagine	553
23. Analisi dei dispositivi	554
23.1 Analisi dei dispositivi iPhone	555
23.1.1 Caratteristiche tecniche dei sistemi iPhone	555
23.1.2 Architettura del sistema operativo	555
23.1.3 Comunicazioni	557
23.1.4 Meccanismi di salvataggio dei dati	557
23.1.5 Partizionamento della memoria	558
23.1.6 Salvataggio dei dati	559
23.1.7 Meccanismi di sicurezza	559
23.1.8 Kernel sicuro	560
23.1.9 Ripristino di fabbrica "rapido"	560
23.1.10 Strategie d'acquisizione e analisi	561
23.1.11 Acquisizione "fisica" della partizione dei dati dell'utente	561
23.1.12 Sostituzione del kernel e installazione del software agente	562
23.1.13 Attivazione del software agente	563

23.1.14 Trasmissione del contenuto della partizione dei dati dell'utente alla workstation	564
23.1.15 Analisi del contenuto della memoria	565
23.1.16 Analisi logica del file system	565
23.1.17 Analisi fisica del file immagine della partizione dei dati utente	569
23.1.18 Accesso a terminali bloccati	570
23.1.19 Estrazione dei dati sincronizzati sul PC associato	571
23.2 Analisi dei dispositivi BlackBerry	572
23.2.1 Caratteristiche tecniche dei sistemi BlackBerry	572
23.2.2 Comunicazioni e integrazione con altri sistemi	572
23.2.2.1 Messaggistica	574
23.2.2.2 Meccanismi di sicurezza	575
23.2.3 Aree d'acquisizione e analisi	577
23.2.3.1 Server centrale RIM	578
23.2.3.2 Server enterprise BES	578
23.2.3.3 Software di sincronizzazione BlackBerry Desktop	579
23.2.3.4 Utilizzo di un simulatore software	581
23.2.3.5 BlackBerry Diagnostic Report	583
23.3 Analisi dei dispositivi Android	584
23.3.1 Caratteristiche tecniche dei sistemi Android	584
23.3.1.1 Architettura del sistema operativo	585
23.3.1.2 Interfaccia di debug	586
23.3.1.3 Integrazione con i servizi Google	588
23.3.1.4 Meccanismi di salvataggio dei dati	591
23.3.1.5 Meccanismi di sicurezza	591
23.3.2 Strategie d'acquisizione e analisi	592
23.3.2.1 Accesso "amministrativo" al sistema	593
23.3.2.2 Analisi logica della memoria	594
23.3.2.3 Estrazione del contenuto fisico della memoria	595
23.3.2.4 Utilizzo di emulatori Android	596
23.4 Analisi dei dispositivi Symbian	597
23.4.1 Caratteristiche tecniche dei sistemi Symbian	598
23.4.1.1 Architettura del sistema operativo	598
23.4.1.2 Meccanismi di sicurezza con impatti sull'analisi forense	601
23.4.2 Strategie d'acquisizione e analisi	603
23.4.3 Estrazione "logica" attraverso software di sincronizzazione	604

23.4.4 Estrazione “logica” dei contenuti attraverso software agente	604
23.4.4.1 Disabilitazione delle protezioni di sicurezza	605
23.4.4.2 Installazione di software agente sul dispositivo	605
23.5 Analisi dei dispositivi Windows Mobile	606
23.5.1 Caratteristiche tecniche dei sistemi Windows Mobile	607
23.5.2 Comunicazioni	607
23.5.3 Meccanismi di salvataggio dei dati	607
23.5.4 Partizionamento della memoria	608
23.5.5 Salvataggio dei dati	609
23.5.6 Meccanismi di sicurezza con impatti sull’analisi forense	609
23.5.7 Strategie d’acquisizione e analisi	610
23.5.8 Acquisizione “fisica” della partizione dei dati dell’utente	610
23.5.8.1 Disabilitazione della policy per il controllo della certificazione delle applicazioni	611
23.5.8.2 Installazione del software agente	612
23.5.8.3 Copia “live” della partizione dei dati	612
23.5.9 Analisi del contenuto della memoria	613
23.5.9.1 Analisi logica del file system	613
23.5.9.2 Emulazione software dei dispositivi	615
23.5.9.3 Analisi “fisica” del file immagine della partizione dei dati utente	616
23.6 Analisi dei dispositivi Palm OS	617
23.6.1 Caratteristiche tecniche dei sistemi Palm OS	617
23.6.1.1 Comunicazioni	617
23.6.1.2 Meccanismi di salvataggio dei dati	618
23.6.2 Strategie d’acquisizione e analisi	620
23.6.3 Estrazione “fisica” del contenuto della memoria del dispositivo	620
23.6.3.1 Abilitazione della modalità di debug	621
23.6.3.2 Estrazione del contenuto della memoria RAM	622
23.6.4 Analisi del contenuto della memoria	623
24. Conclusioni	624
24.1 Strategie applicabili alle famiglie di dispositivi mobili	624
24.2 Mappatura delle strategie abilitate dalle possibilità d’intervento tecnologico	627

CAPITOLO 18
**CRITTOGRAFIA, STEGANOGRAFIA
E TECNICHE DI ANALISI FORENSE**

a cura di Gerardo COSTABILE, Marco MATTIUCCI
e Giuseppe MAZZARACO

1. Premessa	633
2. Steganografia	633
3. Principali metodi steganografici	633
4. Steganalisi	636
5. Identificazione della steganografia	637
6. Crittografia	641
7. La crittoanalisi	642
8. Possibili attacchi alla cifratura dei dati	643
9. Attacco alla cifratura di volumi di storage	647
10. Attacco alla cifratura di file e archivi di file	650
11. Attacco alla cifratura delle email	653
12. Esempio di un'acquisizione "live" e decifratura di un volume TrueCrypt	655

CAPITOLO 19
ELECTRONIC FORENSICS

a cura di Gerardo COSTABILE, Marco MATTIUCCI
e Giuseppe MAZZARACO

1. Premessa	661
2. Dispositivi <i>embedded general purpose</i>	661
3. Analisi dell' <i>hardware</i> e delle sue caratteristiche	663
4. Identificazione delle modalità d'interazione	666
5. Analisi del <i>software</i> e dei dati	669
6. <i>Skimmer analysis</i>	674
7. Alterazione di uno sportello bancario ATM	676
8. Alterazione di un terminale POS	677
9. Caratteristiche di un circuito pirata	678
10. Ulteriori considerazioni tecniche	681
11. Caratteristiche del sistema forense di lettura delle EEPROM	683
12. <i>Skimming</i> da sportello ATM mediante lettura audio della banda magnetica	687

13. Memorizzazione dei dati sulla banda magnetica	688
13.1. Dalla banda magnetica ai caratteri ASCII	688
13.2. La banda magnetica	688
13.3. Il segnale della testina di lettura	689
13.4. La codifica F2F o Aiken Biphase	689
13.5. Acquisizione di una banda magnetica mediante registrazione audio	690
13.6. Decodifica di una banda magnetica acquisita in formato audio	693
13.7. Il <i>software</i> MABdec per la decodifica Aiken Biphase	694
13.8. RFID <i>analysis</i>	696
14. Cenni al mondo RFID	696
14.1. Panoramica sull'analisi forense dei sistemi basati su RFID	699
14.2. Analisi dei <i>tag</i> RFID	699
14.3. Analisi dei sistemi dedicati al trattamento dei <i>tag</i> RFID	703

CAPITOLO 20

MEDIA FORENSICS

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. I supporti ottici e la loro analisi	707
2. Caratteristiche dei supporti ottici	707
2.1 Caratteristiche fisiche	707
3. Organizzazione fisica dei dati sui supporti ottici	709
4. Organizzazione logica dei dati sui supporti ottici	711
5. Acquisizione e analisi dei supporti ottici	713
6. Creazione dell'immagine del supporto	714
7. Analisi delle informazioni	715

CAPITOLO 21

CLOUD FORENSICS

a cura di Gerardo COSTABILE, Marco MATTIUCCI
e Giuseppe MAZZARACO

1. Premessa	719
2. Introduzione al cloud computing	719

3. Struttura di un <i>Cloud System</i>	721
4. La forensics applicata al cloud computing	722
5. Ricerca di evidenze lato <i>server</i>	725
6. Ricerca di evidenze lato <i>client</i>	726
7. Ricerca di evidenze relative a dati in transito	727
8. Cenni al <i>Cloud Computing</i> per finalit� di <i>digital forensics</i>	727

CAPITOLO 22

PRINTER AND SCANNER FORENSICS

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Premessa	733
2. Ambiti d'interesse della <i>printer and scanner forensics</i>	733
3. Analisi della stampa e identificazione della stampante	734
4. Analisi generale del documento	734
5. Analisi delle caratteristiche della stampa	736
6. Informazioni inserite nella stampa dal produttore	739
7. Profilazione delle stampanti	740
8. Preparazione del documento e profilazione della stampante	740
9. Analisi della scansione e identificazione dello <i>scanner</i>	743
10. Analisi della memoria interna dei dispositivi di stampa	745
11. Analisi delle evidenze generate dal processo di stampa sui sistemi collegati alla stampante	747

CAPITOLO 23

CASE STUDY ED ESERCIZI TECNICI

Caso 1. Esercizio: furto di informazioni tramite pen drive	753
Caso 2. Esercizio: password recovery	773
Caso 3. Esercizio: network traffic analysis	777
Caso 4. Esercizio: attacco terroristico	783
Caso 5. Esercizio: puzzle forensics	789
Caso 6. Esercizio: crypto analysis	799
Caso 7. Esercizio: analisi di un floppy disk	803
Caso 8. Esercizio: validazione di un write blocker (software)	849
Caso 9. Esercizio: validazione di un write blocker (hardware)	857
Caso 10. Case study: analisi di un computer vittima di frode informatica	867

Caso 11. Case study: analisi di un'email di phishing e di un sito clone	875
Caso 12. Case study: analisi tecnica del virus Anserin	883
Caso 13. Case study: tecnica di analisi di un sito di phishing – step by step	891
Caso 14. Relazione di consulenza tecnica informatica	899
BIBLIOGRAFIA E SITOGRAFIA	923
GLOSSARIO	961
APPENDICE DELLE IMMAGINI	997