

SOMMARIO

DEL VOLUME II

CAPITOLO 5

IDENTIFICAZIONE, ACQUISIZIONE ED ANALISI DELLE *DIGITAL EVIDENCE*: APPROFONDIMENTI TECNICI

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO

1. Premessa	3
2. Identificazione/Riconoscimento	4
2.1 Supporti magnetici	5
2.2 Supporti ottici	5
2.3 Supporti alternativi	6
2.4 Altri supporti (atipici)	7
2.5 Possibili fonti di elementi informativi e interfacce di connessione	8
2.6 Tipologia di sistema	9
2.7 BIOS	10
2.8 Sistema operativo	11
2.9 <i>File system</i>	12
2.10 Tipologie di <i>file</i>	12
2.11 Altre possibili fonti di informazione su <i>storage</i>	14
2.12 Interfacce	15
3. Acquisizione	18
3.1 Modalità di acquisizione del dato: primi cenni	19
3.2 <i>Order of Volatility</i>	20
3.3 Intercettazione	20
3.4 Sequestro del supporto informatico	22
3.5 Acquisizione <i>live</i> e <i>post-mortem</i> : primi cenni	22

3.6 Elementi specifici in funzione dello stato del sistema (accesso, spento, <i>stand-by</i>)	22
3.7 Le opportunità derivanti dall'operare su un sistema acceso	25
3.8 Rischi legati al mantenimento dello stato di "acceso" su un sistema	27
4. Stato del sistema - Schema sintetico	28
5. Acquisizione <i>live</i> dei sistemi: approfondimenti	29
5.1 L'impatto dell'anti-forensics sull'acquisizione <i>live</i>	31
5.2 Acquisizione <i>live</i> dei sistemi <i>Windows</i> (cenni)	33
5.3 Acquisizione <i>live</i> dei sistemi <i>Macintosh</i> (cenni)	35
5.4 Acquisizione mediante "duplicazione" del dato su sistemi accesi	37
5.5 Acquisizione <i>post-mortem</i> dei sistemi	40
5.6 Tecniche generali per l'acquisizione <i>post-mortem</i>	42
5.7 La strumentazione per l'acquisizione <i>post-mortem</i>	45
5.8 Acquisizione <i>post-mortem</i> con strumenti <i>software</i> commerciali	48
5.9 Acquisizione forense con <i>tools</i> commerciali: <i>Encase</i>	48
5.10 Acquisizione forense con <i>tools</i> commerciali: FTK	54
5.11 Acquisizione forense con <i>tools open source</i>	61
5.12 Acquisizione forense con <i>tools open source: dd</i>	61
5.13 Acquisizione forense con <i>tools open source: dcfldd</i>	64
5.14 Acquisizione forense con <i>tools open source: altri tool</i>	66
5.15 Acquisizione forense con <i>tools open source: dc3dd</i>	70
5.16 Acquisizione forense con <i>tools open source: ddrescue</i>	73
5.17 Acquisizione forense con <i>tools open source: dd_rescue</i>	77
5.18 L'acquisizione da supporti danneggiati	78
6. Elementi tecnici sull'acquisizione dei dati	79
6.1 <i>Data Wiping</i>	79
6.2 Validazione	79
6.3 Elementi di natura temporale	81
6.3.1 <i>Timestamp</i>	81
6.3.2 Rilevazione scostamento temporale	81
6.3.3 <i>Time Server</i>	82
7. Conservazione e protezione	83
7.1 Protezione del supporto di memorizzazione	83
7.2 Restrizioni all'accesso al dato	84
7.3 La Catena di custodia	85
7.3.1 Caratteristiche del sistema	86

7.3.2 Caratteristiche della <i>digital evidence</i>	87
7.3.3 <i>Chain of Custody</i> e Restituzione	88
7.4 Redazione dei verbali/report	88
8. Analisi delle evidenze acquisite	90
8.1 Cenni sull'analisi dei dati acquisiti in <i>live</i>	90
8.2 Cenni sull'analisi dei dati acquisiti <i>post-mortem</i>	95
8.2.1 Le possibilità della <i>disk forensics</i>	97
9. Tecnologia proprietaria a supporto della <i>Computer Forensics</i>	99
9.1 Strumenti a supporto dell'acquisizione del dato	99
9.1.1 Strumenti di copia <i>Hardware</i> : alcuni esempi	100
9.2 Gli strumenti di analisi	102
9.2.1 Un caso particolare: lo <i>Shadow Copy Volume</i>	102
9.2.2 FRED SR	103
9.2.3 FTK, <i>Encase</i>	104
9.4 Gli strumenti di supporto	104

CAPITOLO 6

LA RETE INTERNET E “DINTORNI”

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO
(parte I, II, III, V) e di Francesco CAJANI (parte IV)

PARTE I - ASPETTI TECNICI ED INVESTIGATIVI DI BASE

1. <i>Internet Protocol</i> : gli indirizzi IP	109
2. Indirizzi IP pubblici e privati	110
3. IP statico/ IP dinamico	112
4. Le reti NAT	113
5. <i>Wireless</i> aperte o punti di rete non controllati	115
6. Anonimizzazione	117
7. Il servizio DNS	119
7.1 <i>Dynamic DNS</i>	122
8. La <i>cache</i> del <i>browser</i>	123
8.1 I “ <i>cookie</i> ”	123
8.2 <i>Web browser</i>	125
9. <i>Whois</i> o similari	128
10. <i>Traceroute</i>	130
11. <i>Network Forensics</i>	132
12. L'indagine su una rete “locale”	133

**PARTE II - PEER TO PEER E DIGITAL FORENSICS:
IL CASO EMULE**

1. Le reti <i>Peer-to-peer</i> : funzionamento tecnico	137
2. Applicazioni delle reti <i>peer-to-peer</i>	138
3. Tipologie di reti <i>peer-to-peer</i>	139
4. <i>Client peer-to-peer</i> per <i>File-sharing</i> : <i>eMule</i>	141
5. <i>eMuleForensic</i> : analisi forense del <i>file sharing</i> con <i>eMule</i>	141
5.1 Analisi forense su un singolo sistema	143
5.1.1 Il file <i>AC_SearchString.dat</i>	143
5.1.2 Il file <i>known.met</i>	144
5.2 Analisi forense condotta parallelamente su più sistemi	144
5.2.1 Il file <i>preferences.dat</i>	144
5.2.2 Il file <i>clients.met</i>	146
5.3 Un <i>tool</i> per la conversione automatica dei <i>file di config</i> : <i>eMuleForensic</i>	147
5.4 L'incrocio dei dati	148
5.5 Limiti della <i>link analysis</i> nell'approccio <i>post-mortem</i>	149
5.6 Analisi di un sistema in seguito alla cancellazione di <i>eMule</i>	150

**PARTE III - INTELLIGENCE SULLA RETE INTERNET:
MOTORI DI RICERCA E SOCIAL NETWORK**

1. L'evoluzione dei "blog" e delle reti "sociali"	151
2. Motori di ricerca	153
3. Siti per la condivisione di contenuti multimediali	154
4. <i>Blog</i> e <i>Social network</i>	154
5. Analisi e correlazione delle informazioni	158
6. Utilizzo avanzato dei motori di ricerca	158
7. Reperimento di informazioni personali sui siti "social"	161

**PARTE IV - SEQUESTRO PROBATORIO E PREVENTIVO
DI PAGINE E SITI WEB: ASPETTI GIURIDICI**

1. Principi generali	164
2. Ipotesi particolari alla luce della recente giurisprudenza	166
2.1 Il sequestro preventivo di siti web allocati all'estero	166
2.2 Il sequestro preventivo d'urgenza del sito <i>Coolstreaming.it</i>	167
2.2.1 Il caso specifico analizzato nel 2005: un sistema di <i>peer to peer</i> TV	170
2.3 Il ricorso al sequestro preventivo nel caso <i>PirateBay</i> e la decisione della Corte di Cassazione	181
2.3.1 Inibitoria <i>ex d.lgs. 70/ 2003</i> e sequestro preventivo	190

2.4 Il necessario rapporto di pertinenzialità fra la <i>res</i> e il reato	193
2.5 Le differenti ipotesi <i>ex 14-quater</i> legge 3 agosto 1998 (pedopornografia <i>online</i>)	195
3. Il sequestro dei <i>forum online</i> e dei <i>blog</i>	200
3.1 <i>Case study</i> : una recente ordinanza del Tribunale del Riesame di Milano sul sequestro preventivo di una pagina di un <i>blog</i> e la non applicabilità ad esso delle garanzie costituzionali in materia di stampa (e la conferma della Suprema Corte sul punto)	203

PARTE V - INTERNET 3.0 IL FUTURO DELLA COMPUTER FORENSICS

1. Premessa	219
2. Internet degli oggetti: le definizioni	220
3. Gli oggetti “ <i>smart</i> ”	222
4. L'interconnessione di oggetti “ <i>smart</i> ”	223
5. Alcune applicazioni di Internet delle cose	224
6. Il “ <i>tagging</i> ”	225
6.1 RFID	226
6.2 NFC e utilizzo di <i>gateway</i>	227
6.3 <i>Tagging</i> 2D o altri <i>tag</i> passivi	229
7. Standard e protocolli specifici	230
7.1 <i>Digital Object Identifier</i>	230
7.2 Cenni a <i>Internet Protocol for Smart Objects Alliance</i>	232
8. Affidabilità e sicurezza delle <i>digital evidence</i> “negli” oggetti	233

CAPITOLO 7

LA POSTA ELETTRONICA

a cura di Gerardo COSTABILE e Giuseppe MAZZARACO
(parte I) e di Francesco CAJANI (parte II)

PARTE I - ASPETTI TECNICI ED INVESTIGATIVI

1. Nozioni di base	239
2. L'invio di <i>e-mail</i> anonime	241
3. L' <i>header</i> dei protocolli	243
3.1 Incapsulamento	243
3.2 <i>Header</i> IP	245
3.3 <i>Header</i> TCP/UDP	246
3.4 <i>Header</i> HTTP	249

3.5 <i>Header</i> SMTP	251
4. Estrazione degli <i>Header</i> dai maggiori <i>software</i> di posta elettronica ed analisi di alcuni casi	255
4.1 Istruzioni operative per l'estrapolazione degli <i>header</i>	263

PARTE II - L'ACQUISIZIONE E IL SEQUESTRO DELLA POSTA ELETTRONICA: ASPETTI GIURIDICI

1. L'acquisizione e sequestro di corrispondenza in generale (artt. 353 e 254 c.p.p)	272
2. La nozione di "corrispondenza" oggetto di tutela costituzionale	274
3. Il messaggio di posta elettronica (<i>e-mail</i>): comunicazione "aperta" o "chiusa"	275
3.1 I tre "luoghi" ove di regola pu� essere acquisita una <i>e-mail</i> : A) il <i>client</i> del mittente, B) il <i>client</i> del destinatario, C) il <i>server</i> del gestore di posta elettronica	279
4. L'acquisizione degli SMS	282
5. La nuova disciplina prevista dalla legge 48/2008 e i suoi riflessi sulla acquisizione delle <i>e-mail</i>	284

CAPITOLO 8

ACQUISIZIONE DATI DEL TRAFFICO ED INTERCETTAZIONI TELEMATICHE

a cura di Francesco CAJANI (parte I, II sez. III, III),
Gerardo COSTABILE, Marco MATTIUCCI e Giuseppe MAZZARACO
(parte II sez. I) e di Stefano ATERNO (parte II sez. II)

PARTE I - TABULATI TELEFONICI E LOG FILES

1. Tabulati telefonici e <i>log files</i> come irrinunciabili spunti investigativi ed importanti fonti di prova	289
1.1 Le richieste della Autorit� Giudiziaria	294
2. La normativa attualmente vigente in materia: artt. 123 e 132 Codice Privacy	294
2.1 Il regime per i dati relativi al traffico telefonico	298
2.1.1 Il provvedimento necessario per l'acquisizione dei c.d. tabulati	298
2.1.2 Il periodo di conservazione dei dati relativi ai traffico telefonico, oggi pari a 24 mesi (30 giorni per le chiamate senza risposta)	301
2.1.3 Richieste di dati del traffico telefonico per periodi superiori ai 24 mesi: lo stato attuale	304

2.2 Il regime per i dati relativi al traffico telematico (cd. <i>log files</i>)	305
2.2.1 Acquisizione e periodo di conservazione	306
3. L'acquisizione di dati del traffico telefonico e/o telematico presso gli <i>Internet Service Providers</i> italiani	308
3.1 Una ipotesi concreta	308
3.2 Le recenti innovazioni della l. 48/2008 in materia di sequestro ed acquisizione dei dati del traffico	315
3.3 Le linee guida di cooperazione tra le Forze di Polizia e gli <i>Internet Service Providers</i>	316
4. Le piattaforme informatiche messe a disposizione dei gestori telefonici alla Polizia Giudiziaria al fine di consentire un pi rapido accesso ai dati del traffico	317
4.1 AG WEB Vodafone	317
4.2 LAW PORTAL Wind	318
4.3 AG SERVICE Telecom Italia Mobile	319
5. Le prestazioni obbligatorie e il pagamento dei dati del traffico telefonico	320
6. Le richieste dei dati attinenti al traffico telematico relativi ai gestori americani (in particolare: <i>Yahoo</i> , <i>Google</i> e <i>Microsoft</i>)	323
7. Le <i>Data request guidelines</i> di <i>Facebook</i>	323

PARTE II - LE INTERCETTAZIONI TELEMATICHE

SEZIONE I – NOZIONI TECNICHE DI BASE

1. Classificazione delle intercettazioni telematiche	324
1.1 Tecniche ed architettura delle intercettazioni telematiche	329
2. L'intercettazione di posta elettronica e la c.d. duplicazione (o re-indirizzamento)	333
2.1 L'intercettazione di posta elettronica all'estero (aspetti tecnico-operativi)	339
3. La microspia telematica	341

SEZIONE II - ANALISI DELLA NORMATIVA APPLICABILE

1. L'ambito applicativo dell'art. 266- <i>bis</i> c.p.p. e l'oggetto delle intercettazioni telematiche	344
2. Presupposti procedurali ed esecuzione delle operazioni (artt. 267-271 c.p.p.)	351
3. Le intercettazioni preventive telematiche (art. 25- <i>ter</i> legge 356/1992, oggi art. 266 disp. att. c.p.p.)	355

4. La giurisprudenza in materia di instradamento e la potenziale attinenza alle intercettazioni telematiche	359
-------------------------------------------------------------------------------------------------------------	-----

SEZIONE III - I DATI RELATIVI ALLE CHIAMATE VOIP
(*VOICE OVER IP*) E L'INTERCETTAZIONE DELLE
RELATIVE COMUNICAZIONI: QUALE REGIME
NORMATIVO È APPLICABILE?

1. Il dibattito sul regime normativo applicabile	363
2. Le intercettazioni di comunicazioni su sistemi VoIP crittografati	368
2.1 Il "caso <i>Skype</i> "	368
2.2 Le vicende dell'omicidio Roveraro	370
2.3 Lo stato attuale delle intercettazioni di comunicazioni tramite sistemi VoIP con protocolli di crittografia	372

**PARTE III - L'INTERCONNESSIONE DEI SISTEMI DI
COMUNICAZIONE: PROBLEMI DI GIURISDIZIONE
IN MATERIA DI INTERCETTAZIONE TELEMATICA E
DI *DATA RETENTION***

1. "La Legge è per il mondo reale e non certo per il <i>cyberspazio</i> "	374
2. "No <i>server no law opinion</i> " vs. "No <i>server but law opinion</i> "	376
2.1 I sistemi di comunicazione VoIP	376
2.2 L'intercettazione di caselle di posta elettronica <i>@.com</i>	377
2.3 Le richieste relative alla c.d. "posta in giacenza"	379
2.4 La conservazione dei dati relativi al traffico telematico	381
3. La giurisprudenza americana sulla legge applicabile al mondo Internet	382
4. Di quali obblighi, derivanti da leggi nazionali già esistenti, possiamo ragionevolmente pretendere l'osservanza	389
4.1 La normativa in materia di comunicazioni elettroniche	390
4.2 La normativa in materia di conservazione dei dati (<i>data retention</i>)	391
4.3 Le contraddizioni degli ISP americani in tema di <i>data retention</i> : quando non si vuole conservare...	394
5. Gli obblighi di mutua assistenza con gli Stati Uniti derivanti dalla Convenzione sul <i>Cybercrime</i>	395
6. Intercettazioni ed indagini penali: le recenti posizioni del Governo USA	399
7. La forza del mercato e la forza del Diritto	400
8. Quali previsioni per un futuro incerto?	402

CAPITOLO 9
**“LE OPERAZIONI DIGITALI SOTTO COPERTURA”: L’AGENTE
PROVOCATORE E L’ATTIVITÀ DI CONTRASTO
NELLE INDAGINI INFORMATICHE**

a cura di Francesco CAJANI

1. Le previsioni normative: in particolare l’art. 14 comma 2 l. 269/1998 in materia di pedopornografia <i>online</i>	411
1.1 Investigazioni “sotto copertura” effettuate in assenza dei presupposti normativi: la responsabilità dell’agente provocatore a titolo di concorso e profili di utilizzabilità delle risultanze acquisite anche per diverse fattispecie di reato	417
1.2 Utilizzabilità dei risultati legittimamente acquisiti “sotto copertura” ma riferiti a reati diversi o meno gravi	419

CAPITOLO 10
**I “NUOVI” MEZZI DI RICERCA DELLA PROVA: VIDEORIPRESE
INVESTIGATIVE, AGENTE SEGRETO ATTREZZATO PER IL SUO-
NO, PEDINAMENTO ELETTRONICO ED APPOSTAMENTI IN-
FORMATICI, INSTALLAZIONE DI CAPTATORI INFORMATICI**

a cura di Francesco CAJANI

1. Introduzione	427
2. Le intercettazioni processuali: una definizione normativa	427
3. Le c.d. “intercettazioni “di immagini” (video-riprese investigative) nella elaborazione giurisprudenziale	429
4. Il c.d. agente segreto attrezzato per il suono	436
5. Il c.d. “pedinamento elettronico” (<i>positioning</i> tramite GPS o localizzazione delle celle interessate)	442
5.1 <i>Case study</i> : utilizzo di reti <i>wireless</i> bucate a fini illeciti e localizzazione del possibile autore tramite celle UMTS	449
6. Il c.d. “appostamento informatico” come precipua forma di localizzazione sul web	462
6.1 Le <i>e-mail</i> traccianti: aspetti tecnici e utilizzo per finalità investigative	464
6.2 Un primo riconoscimento giurisprudenziale della legittimità dell’utilizzo delle <i>e-mail</i> traccianti a fini investigativi	468
7. L’installazione di “captatori informatici” alla luce della recente pronuncia della Suprema Corte	483