

## INDICE

	<i>pag.</i>
Introduzione	XXI
Introduzione alla edizione del 2011	XXIII
Il futuro ci ha raggiunto, di <i>Giorgio Spangher</i>	XXV
Cybercrime, l'ultima frontiera, di <i>Filippo Spiezia</i>	XXVII

### Capitolo 1

#### DIGITAL FORENSICS & DIGITAL INVESTIGATION: CLASSIFICAZIONE, TECNICHE E LINEE GUIDA NAZIONALI ED INTERNAZIONALI

*Gerardo Costabile*

1. Digital forensics & digital investigation: definizioni e punti di attenzione	1
2. Digital evidence: cenni tecnici di base	5
3. Classificazione delle "evidenze digitali"	6
4. Dati e log sui sistemi coinvolti: cenni	6
5. Log e informazioni degli elementi infrastrutturali della rete o di sistemi di supporto: cenni	7
6. Le fasi del processo di digital forensics: gli standard internazionali	8
7. Digital forensics: le classificazioni tipiche	10
8. La c.d. preview	12
9. Le best practices sulla digital forensics in Italia	13
10. Le linee guida della digital forensics: l'esempio della Guardia di finanza	20
11. Le nuove frontiere della digital investigation e forensics	23
12. Prevedere i crimini: l'Intelligenza Artificiale e le reti neurali a supporto del comparto sicurezza ed investigazioni	27

## Capitolo 2

### RETE INTERNET E “DINTORNI”: ASPETTI TECNICI DI BASE

*Gerardo Costabile*

1. Internet Protocol: gli indirizzi IP	33
2. Indirizzi IP pubblici e privati	34
3. IP statico/IP dinamico	36
4. Le reti NAT	37
5. Wireless aperte o punti di rete non controllati	38
6. Anonimizzazione	40
7. Il servizio DNS	42
7.1. <i>Segue</i> : Dynamic DNS	45
8. La cache del browser	46
8.1. <i>Segue</i> : i “cookie”	46
8.2. <i>Segue</i> : Web browser	48
9. Whois o similari	51
10. Traceroute	55
11. Network Forensics	56
12. L’indagine su una rete “locale”	57

## Capitolo 3

### LE INDAGINI DIGITALI

*Gerardo Costabile*

1. La complementarità tra le indagini tradizionali e le indagini 2.0: complessità e opportunità	61
2. Metodologie investigative	62
3. Mobile Forensics & Investigation	63
4. Cloud Forensics & Investigation	67
5. La Cyber Intelligence	76
5.1. <i>Segue</i> : l’Open Source Intelligence (OSINT)	85
6. Social Network Analysis (SNA)	87
6.1. <i>Segue</i> : casi pratici di applicazione della SNA	96
6.2. <i>Segue</i> : criticità e limiti degli strumenti SNA	101
7. Deep & Dark web Intelligence	103
7.1. <i>Segue</i> : i Dark Net Markets	109
7.2. <i>Segue</i> : terrorismo e propaganda nel Dark Web	113

	<i>pag.</i>
7.3. <i>Segue</i> : anonimato nel Dark Web e indagini di polizia giudiziaria	114
8. Big Data Intelligence e strumenti a supporto	115
9. Bitcoin Intelligence ed attività investigativa	124
9.1. <i>Segue</i> : utilizzo di Bitcoin nelle attività illecite	124
9.2. <i>Segue</i> : Bitcoin Investigation	125
9.3. <i>Segue</i> : i sequestri di Bitcoin dal punto di vista tecnico-operativo	127

## Capitolo 4

### LA RICEZIONE DELLA *NOTITIA CRIMINIS* E I PRIMI ATTI D'INDAGINE

*Francesco Cajani*

1. La nozione giuridica di digital evidence (prova elettronica o digitale)	129
2. La classificazione dei reati informatici	132
3. L'acquisizione della <i>notitia criminis</i>	137
4. L'acquisizione della denuncia e della denuncia/querela ad opera della polizia giudiziaria	138
4.1. <i>Segue</i> : la "ragionevole tempestività" nella trasmissione della comunicazione di notizia di reato e la necessità di individuare dei protocolli di polizia giudiziaria volti alla corretta acquisizione della denuncia/querela	139
5. Informazioni della persona offesa in sede di denuncia/querela	141
6. Gli atti di indagine in assenza (attesa) della querela	143
7. La remissione della querela	143
8. Arresto in flagranza e fermo nei reati informatici	145
8.1. <i>Segue</i> : l'utilizzo indebito di carte di credito e altri strumenti di pagamento; l'illecito possesso e/o falsificazione	147
8.2. <i>Segue</i> : il phishing e le ipotesi di cyber riciclaggio	149
9. Gli allegati alla denuncia/querela o alla comunicazione di notizia di reato: in particolare, la produzione di una pagina web su supporto cartaceo	150
10. Aspetti tecnici per la corretta acquisizione di informazioni presenti in rete	153
10.1. <i>Segue</i> : acquisizione di sito web	154
11. Furto di identità sul web	157
11.1. <i>Segue</i> : informazioni della persona offesa in caso di truffa e-commerce	161
11.2. <i>Segue</i> : i primi accertamenti di polizia giudiziaria sull'analisi dei movimenti dei conti correnti relativi alle banche on line	162
11.3. <i>Segue</i> : gli altri strumenti di pagamento utilizzabili per conseguire l'illecito profitto e, in particolare, il vaglia on line e le operazioni di money transfert	163

	<i>pag.</i>
11.4. <i>Segue</i> : la pericolosità del truffatore seriale e la possibilità di applicazione di una misura di prevenzione. Il caso M.	165
12. Le (altre) indagini scientifiche in ausilio alla cyber forensics	167
13. I supporti di memorizzazione utilizzati	172

## Capitolo 5

### GIURISDIZIONE E COMPETENZA NELLE INDAGINI INFORMATICHE

*Francesco Cajani*

1. Le regole di giurisdizione nell'attività di individuazione e raccolta delle evidenze digitali	175
1.1. <i>Segue</i> : 2001/2008 Odissea nel cyber spazio	177
2. Problemi di giurisdizione in materia di siti e/o pagine web allocate su server esteri	181
2.1. <i>Segue</i> : il sequestro preventivo di siti web allocati all'estero	182
2.2. <i>Segue</i> : il sequestro preventivo d'urgenza del sito Coolstreaming.it	183
2.3. <i>Segue</i> : il ricorso al sequestro preventivo nel caso PirateBay e la decisione della Corte di Cassazione n. 49437/2009	185
2.4. <i>Segue</i> : l'intervento delle Sezioni Unite nel 2015	192
2.5. <i>Segue</i> : inibitoria ex d.lgs. n. 70/2003 e sequestro preventivo	194
3. La competenza territoriale in relazione alle indagini digitali	196
4. L'individuazione del "domicilio informatico" come criterio generalmente idoneo a radicare la competenza territoriale nelle ipotesi ex art. 615-ter c.p.	197
4.1. <i>Segue</i> : il diverso criterio in caso di sistemi informatici interconnessi (c.d. client/server)	199
5. Il <i>locus commissi delicti</i> nei casi di diffamazione on line	201
6. Individuazione del <i>locus commissi delicti</i> nelle truffe su piattaforma e-commerce	209
6.1. <i>Segue</i> : l'impostazione della Corte di Cassazione (pagamenti verso carte Postepay; pagamenti tramite bonifici su conti correnti; pagamenti tramite carte di credito ricaricabili e alle c.d. banche on line)	210
6.2. <i>Segue</i> : considerazioni finali sui criteri di individuazione della competenza territoriale	216
7. La competenza territoriale nei casi di frode informatica	220
7.1. <i>Segue</i> : nei casi di phishing e cyber riciclaggio	222
7.2. <i>Segue</i> : nei reati di pedopornografia on line	224
8. La competenza funzionale in materia di cyber crime: i lavori parlamentari della legge n. 48/2008	225

pag.

8.1. <i>Segue</i> : l'assenza di indicazioni, nel testo della Convenzione di Budapest, quanto alle questioni di competenza	226
8.2. <i>Segue</i> : il catalogo di reati di cui all'art. 51, comma 3- <i>quinquies</i> , c.p.p. rientranti nella competenza c.d. distrettuale	227
8.3. <i>Segue</i> : la <i>vis attractiva</i> dei procedimenti relativi ai reati c.d. distrettuali rispetto ai procedimenti relativi ad altri reati ad essi connessi	228
8.4. <i>Segue</i> : osservazioni critiche	229

## Capitolo 6

### LA COOPERAZIONE INTERNAZIONALE NELLE INDAGINI DIGITALI

*Francesco Cajani*

1. Un nuovo concetto di cooperazione internazionale	233
2. Organismi di coordinamento giudiziario ed investigativo a livello europeo	241
2.1. <i>Segue</i> : l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale – Eurojust	242
2.2. <i>Segue</i> : Europol	246
2.3. <i>Segue</i> : Interpol	247
2.4. <i>Segue</i> : Olaf	248
3. Organismi di cooperazione internazionale	249
3.1. <i>Segue</i> : il Consiglio d'Europa e l'azione del Cybercrime Convention Committee (T-CY)	249
3.2. <i>Segue</i> : i punti di contatto nazionali (Rete 24/7)	252
3.3. <i>Segue</i> : l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine (UNODC)	253
4. Le squadre investigative comuni	254
5. Ipotesi di collaborazione tra le forze di polizia e il c.d. settore privato: le Task Force in materia di computer crimes	257
6. Cooperazione e coordinamento investigativo nei reati transnazionali: il sequestro (anche per equivalente) di beni all'estero	259

## Capitolo 7

### L'ACQUISIZIONE DEI DATI DEL TRAFFICO

*Stefano Aterno e Francesco Cajani*

#### PARTE I – LA DISCIPLINA IN TEMA DI CONSERVAZIONE DEI DATI – DATA RETENTION

1. Elenco normativo e cronologia delle fonti in materia	270
---------------------------------------------------------	-----

	<i>pag.</i>
2. Le fonti nazionali e le fonti europee	277
2.1. <i>Segue:</i> le Direttive 95/46/CE e 97/66/CE e la Direttiva 2002/58/CE	277
2.2. <i>Segue:</i> il c.d. decreto Pisanu (d.l. n. 144/2005, convertito in legge n. 155/2005)	279
2.3. <i>Segue:</i> la Direttiva 2006/24/CE	279
3. Le modifiche della normativa sulla data retention in seguito all'attuazione della Direttiva 2006/24/CE con il d.lgs. n. 109/2008: come è cambiato l'art. 132 del Codice privacy	283
3.1. <i>Segue:</i> i "dati relativi al traffico" e le altre definizioni normative	284
3.2. <i>Segue:</i> il lungo "calvario" della normativa in materia di data retention	287
3.3. <i>Segue:</i> l'art. 132 Codice privacy	289
3.4. <i>Segue:</i> le chiamate senza risposta	300
4. Indirizzo di Internet protocol: cosa conservare e cosa cancellare?	302
5. Il freezing dei dati telematici previsto dai commi 4- <i>ter</i> ss. dell'art. 132 Codice privacy	306
6. La storia del WI-FI in Italia	309
7. Le modifiche del luglio 2017 e la legge n. 167 del novembre 2017	314
8. Il d.lgs n. 101/2018 e il suo piccolo contributo alla data retention	317
9. L'art. 234- <i>bis</i> c.p.p.: acquisizione di dati informatici all'estero	317
<b>PARTE II – TABULATI TELEFONICI E LOG FILES</b>	
1. Tabulati telefonici e log files come irrinunciabili spunti investigativi ed importanti fonti di prova	320
1.1. <i>Segue:</i> le richieste della autorità giudiziaria ai gestori telefonici/telematici	322
2. La normativa attualmente vigente in materia: artt. 123 e 132 Codice privacy	323
2.1. <i>Segue:</i> il regime per i dati relativi al traffico telefonico	326
2.1.1. <i>Segue:</i> il periodo di conservazione dei dati relativi al traffico telefonico, oggi pari a 24 mesi (30 giorni per le chiamate senza risposta)	328
2.1.2. <i>Segue:</i> richieste di dati del traffico telefonico per periodi superiori ai 24 mesi: lo stato attuale e la normativa antiterroristica	331
2.2. <i>Segue:</i> il regime per i dati relativi al traffico telematico (c.d. log files)	333
2.2.1. <i>Segue:</i> acquisizione e periodo di conservazione	334
3. L'acquisizione di dati del traffico telefonico e/o telematico presso gli Internet Service Providers italiani: le ripercussioni della legge n. 48/2008 in materia di sequestro ed acquisizione dei dati del traffico	336
3.1. <i>Segue:</i> le linee guida di cooperazione tra le forze di polizia e gli Internet Service Providers. Le piattaforme informatiche messe a disposizione di molti gestori di telefonia italiani al fine di ottenere le informazioni richieste	337

	<i>pag.</i>
4. Le prestazioni obbligatorie a fini di giustizia	339
5. Le richieste dei dati attinenti al traffico telematico relativi ai gestori americani: rinvio	340

## Capitolo 8

### LE INTERCETTAZIONI DIGITALI

*Gerardo Costabile e Stefano Aterno*

#### PARTE I – ASPETTI TECNICO-INVESTIGATIVI DELLE INTERCETTAZIONI DIGITALI

1. Tipologia e classificazione delle intercettazioni telematiche	341
1.1. <i>Segue</i> : tecniche ed architettura delle intercettazioni telematiche	344
2. L'intercettazione di posta elettronica e la c.d. duplicazione (o re-indirizzamento)	345
2.1. <i>Segue</i> : l'intercettazione di posta elettronica all'estero (aspetti tecnico-operativi)	348
3. Intercettazione attiva: il c.d. captatore informatico	349

#### PARTE II – ASPETTI NORMATIVI

1. Il captatore informatico: le nuove tecniche di intercettazione, perquisizione e acquisizione da remoto	354
1.1. <i>Segue</i> : il captatore informatico e la Corte di Cassazione n. 16556/2010 (c.d. Virruso)	355
1.2. <i>Segue</i> : il tema delle intercettazioni tra presenti. La sentenza Scurato delle Sezioni Unite della Corte di Cassazione	361
2. La sentenza della Corte di Cassazione sul caso Occhionero e sul caso Romeo	366
2.1. <i>Segue</i> : l'uso del captatore informatico in modalità "screen shot" è qualcosa di diverso da una intercettazione telematica <i>ex art. 266-bis c.p.p.</i>	368
3. Dalle prime ipotesi legislative alla legge Spazzacorrotti	378
3.1. <i>Segue</i> : la proposta c.d. Quintarelli	378
3.2. <i>Segue</i> : l'art. 1, comma 84, lett. e) della legge di riforma Orlando recante modifiche al Codice di procedura penale	383
3.3. <i>Segue</i> : i contenuti della delega c.d. Orlando (legge 23 giugno 2017, n. 103)	383
3.4. <i>Segue</i> : la disciplina delle intercettazioni mediante captatore informatico: dal d.lgs. n. 216/2017 al d.l. n. 161/2019	385
3.4.1. <i>Segue</i> : i contenuti delle riforme	390

	<i>pag.</i>
3.4.2. <i>Segue</i> : le anomalie delle riforme: ciò che il decreto non dice ma presuppone	394
3.5. <i>Segue</i> : la legge c.d. Spazzacorrotti e le modifiche riguardanti l'art. 266, comma 2, c.p.p. sull'intercettazione c.d. itinerante	402

## Capitolo 9

### LE RICHIESTE PER FINALITÀ DI GIUSTIZIA RIVOLTE AGLI INTERNET PROVIDERS ESTERI

*Francesco Cajani*

1. I dati	407
2. “La legge è per il mondo reale e non certo per il cyber spazio”	408
3. Rogatoria sì, rogatoria no	410
4. La Voluntary disclosure	412
5. La classificazione internazionale delle tipologie di dati informatici in possesso del ISP	413
5.1. <i>Segue</i> : le c.d. Emergency Disclosure Requests e il caso “WhatsApp”	417
5.2. <i>Segue</i> : le ulteriori problematiche in caso di procedimenti relativi a casi di diffamazione on line	418
6. C’era una volta il problema delle chiamate VOIP e dell’intercettazione delle relative comunicazioni	418
7. Le intercettazioni delle caselle di posta elettronica @.com	422
8. “No server, no law” vs “No server, but law” opinion	423
9. La giurisprudenza americana sulla legge applicabile al mondo Internet	429
10. Quale futuro, dunque, si attende?	435

## Capitolo 10

### ATTIVITÀ DI ACQUISIZIONE DELLA DIGITAL EVIDENCE: ISPEZIONI, PERQUISIZIONI E ACCERTAMENTI TECNICI

*Donatella Curtotti*

1. Le forme di acquisizione della prova digitale: uno sguardo di insieme	439
2. L’acquisizione degli elementi di prova di natura digitale: attività irripetibile o ripetibile?	442
3. Mezzi di ricerca della prova: l’ispezione informatica	445
4. La perquisizione informatica. L’art. 247, comma 2- <i>bis</i> e l’art. 352 c.p.p. Differenze applicative dei due strumenti investigativi	447



	<i>pag.</i>
4.1. <i>Segue</i> : le perquisizioni on line	450
5. Gli accertamenti urgenti <i>ex art.</i> 354 c.p.p.	453
6. La “duplicazione su supporti”. La garanzia della conformità della copia all’originale e la sua immutabilità	454

## Capitolo 11

### IL SEQUESTRO

*Donatella Curtotti*

1. Il sequestro di sistemi informatici e telematici e di supporti digitali	457
1.1. <i>Segue</i> : la restituzione del materiale informatico sequestrato	459
2. La richiesta di consegna dei dati informatici in alternativa al sequestro	461
3. Il sequestro urgente dei dati informatici	463
3.1. <i>Segue</i> : il sequestro in seguito ad accertamenti urgenti “inutilizzabili”	464
4. L’acquisizione dei dati informatici tra sequestro di corrispondenza e intercettazione telematica	468
4.1. <i>Segue</i> : l’acquisizione dei dati custoditi nel Cloud	472
5. L’acquisizione dei dati e i sigilli informatici	474

## Capitolo 12

### I “NUOVI” STRUMENTI DI INDAGINE

*Francesco Cajani*

1. Introduzione	477
2. Le c.d. “intercettazioni di immagini” (le video-riprese investigative) nell’elaborazione giurisprudenziale	479
3. Il c.d. agente attrezzato per il suono	486
4. Il c.d. pedinamento elettronico (positioning tramite GPS o localizzazione delle celle interessate)	490
4.1. <i>Segue</i> : l’acquisizione dei risultati dell’attività di rilevamento satellitare tramite GPS	493
5. L’acquisizione di riprese e/o la geolocalizzazione di un soggetto effettuata tramite captatore informatico	494
6. Il c.d. appostamento informatico come precipua forma di localizzazione sul web	496
6.1. <i>Segue</i> : le e-mail traccianti: aspetti tecnici e utilizzo per finalità investigative	497
6.2. <i>Segue</i> : un primo riconoscimento giurisprudenziale	501

## Capitolo 13

**“LE OPERAZIONI DIGITALI SOTTO COPERTURA”:  
L’AGENTE PROVOCATORE E L’ATTIVITÀ DI CONTRASTO**

*Donatella Curtotti*

1.	Definizione, inquadramento sistematico, problematiche culturali e giuridiche	505
2.	Le previsioni normative: l’art. 14, comma 2, legge n. 269/1998 in materia di pedopornografia on line	508
3.	Investigazioni “sotto copertura” effettuate in assenza dei presupposti normativi	510
4.	Il regime di utilizzabilità dei risultati legittimamente acquisiti “sotto copertura”	511
4.1.	<i>Segue</i> : la natura giuridica: strumenti di ricerca della <i>notitia criminis</i> o atti d’indagine preliminare	514

## Capitolo 14

**LA POSTA ELETTRONICA**

*Gerardo Costabile e Francesco Cajani*

PARTE I – ASPETTI TECNICI DI BASE

1.	Nozioni di base	519
2.	L’invio di e-mail anonime	522
3.	L’header dei protocolli	522

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.)	523
2.	La nozione di “corrispondenza” oggetto di tutela costituzionale	525
3.	Il messaggio di posta elettronica (e-mail): comunicazione “aperta” o “chiusa”?	526
3.1.	<i>Segue</i> : con quale istituto giuridico può essere “appresa” la posta elettronica?	531
3.2.	<i>Segue</i> : i tre “luoghi” ove di regola può essere acquisita una e-mail: A) il client del mittente, B) il client del destinatario, C) il server del gestore di posta elettronica	532
4.	L’acquisizione degli SMS e dei dati segnalati sul display di un cellulare (comprensivi dei messaggi WhatsApp)	536
5.	La nuova disciplina prevista dalla legge n. 48/2008 e i suoi riflessi sulla acquisizione delle e-mail	538

## Capitolo 15

LE “NUOVE FRONTIERE” DELL’INVESTIGAZIONE DIGITALE  
 ALLA LUCE DELLA LEGGE N. 48/2008, OVVERO:  
 QUELLO CHE LE NORME (ANCORA) NON DICONO

*Francesco Cajani*

- |    |                                                                                                                                                                                                           |     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. | L’ispezione di un client ubicato in Italia (ma interconnesso ad un server allocato all’estero) e la relativa acquisizione degli elementi di prova digitale <i>ivi</i> complessivamente presenti           | 541 |
| 2. | L’accesso “da remoto” ad una casella di posta elettronica e la relativa acquisizione degli elementi di prova digitale <i>ivi</i> complessivamente presenti                                                | 548 |
|    | 2.1. <i>Segue</i> : la c.d. perquisizione on line, questa sconosciuta                                                                                                                                     | 549 |
|    | 2.2. <i>Segue</i> : la consapevole rivelazione delle credenziali di accesso di una casella di posta elettronica                                                                                           | 551 |
|    | 2.3. <i>Segue</i> : la conoscenza delle credenziali di accesso in capo alla polizia giudiziaria senza che l’utente ne abbia consapevolezza                                                                | 552 |
| 3. | L’accesso “da remoto” ai messaggi in bozze di una casella di posta elettronica utilizzata come “bacheca” e la relativa acquisizione degli elementi di prova digitale <i>ivi</i> complessivamente presenti | 555 |
|    | 3.1. <i>Segue</i> : la diversa impostazione recentemente adottata dalla Suprema Corte                                                                                                                     | 556 |

## Capitolo 16

IL CONSULENTE TECNICO, IL PERITO E LO SVOLGIMENTO  
 DELLE ATTIVITÀ PREVISTE DAL CODICE DI PROCEDURA PENALE.  
 RESPONSABILITÀ

*Stefano Aterno*

- |    |                                                                                     |     |
|----|-------------------------------------------------------------------------------------|-----|
| 1. | Le fonti normative                                                                  | 563 |
| 2. | La consulenza tecnica                                                               | 564 |
|    | 2.1. <i>Segue</i> : la nomina del consulente tecnico; il conferimento dell’incarico | 567 |
|    | 2.2. <i>Segue</i> : la consulenza tecnica fuori dai casi di perizia                 | 572 |
|    | 2.3. <i>Segue</i> : incompatibilità e astensione del consulente                     | 574 |
|    | 2.4. <i>Segue</i> : il quesito “tipo”                                               | 575 |
| 3. | La perizia: natura e ambito di operatività                                          | 578 |
| 4. | Ammissibilità e discrezionalità del giudice                                         | 581 |
|    | 4.1. <i>Segue</i> : la valutazione dei risultati da parte dell’organo giudicante    | 588 |
| 5. | La nomina del perito                                                                | 594 |

	<i>pag.</i>
5.1. <i>Segue</i> : incapacità e incompatibilità	598
5.2. <i>Segue</i> : astensione e ricusazione	600
5.3. <i>Segue</i> : obblighi	602
5.4. <i>Segue</i> : la liquidazione del compenso al perito (art. 232 c.p.p.)	602
6. I provvedimenti del giudice che dispone la perizia	604
6.1. <i>Segue</i> : ordinanza (contenuto)	607
6.2. <i>Segue</i> : conferimento dell'incarico e formulazione dei quesiti	608
7. L'attività del perito	609
7.1. <i>Segue</i> : la relazione peritale	613
7.2. <i>Segue</i> : le comunicazioni alle altre parti	617
8. L'incidente probatorio	619

## Capitolo 17

### LE INVESTIGAZIONI DIGITALI DIFENSIVE E L'ALIBI INFORMATICO

*Stefano Aterno*

1. L'indagine difensiva in generale e il ruolo del difensore	623
2. Le diverse sottospecie di indagini difensive	628
2.1. <i>Segue</i> : le indagini preventive	628
2.2. <i>Segue</i> : le indagini suppletive	629
2.3. <i>Segue</i> : le indagini integrative	630
3. I poteri e limiti del difensore e del suo consulente tecnico	631
3.1. <i>Segue</i> : l'accesso ai luoghi	633
3.2. <i>Segue</i> : l'accertamento tecnico ripetibile e irripetibile	634
3.3. <i>Segue</i> : l'esame delle cose sequestrate	635
4. La richiesta di documenti alla pubblica amministrazione e ai privati; il diniego dei documenti. La particolare richiesta ai gestori telefonici dei tabulati di traffico telefonico e telematico	636
5. L'alibi informatico	640

## Capitolo 18

### LA CONFISCA DEI BENI INFORMATICI E LA LORO DESTINAZIONE D'USO

*Francesco Cajani*

1. La modifica normativa originariamente introdotta con legge n. 12/2012	645
2. Le innovazioni del 2016 al testo dell'art. 240, comma 2, n. 1- <i>bis</i>	652

INDICE DEI CASI PRATICI (*On Line*  )a cura di *Francesco Cajani***Capitolo 4 – LA RICEZIONE DELLA *NOTITIA CRIMINIS* E I PRIMI ATTI DI INDAGINE**

1. Presenza/assenza della condizione di procedibilità – il cd. processo Fineco
2. L'ambito operativo degli accertamenti di polizia giudiziaria relativi alla falsificazione delle carte di credito
3. Un arresto in flagranza in caso di phishing
4. Truffa tradizionale *vs.* truffa on line
5. Attacco informatico al Pio Albergo Trivulzio di Milano
6. La pericolosità del truffatore seriale

**Capitolo 5 – GIURISDIZIONE E COMPETENZA NELLE INDAGINI INFORMATICHE**

7. Coolstreaming.it – un sistema di *peer to peer TV*
8. La struttura di una associazione dedita alla commissione di reati di phishing e i problemi di competenza territoriale connessi ad ipotesi di cyber-riciclaggio

**Capitolo 7 – L'ACQUISIZIONE DEI DATI DEL TRAFFICO**

## PARTE II: TABULATI TELEFONICI E LOG FILES

9. Tabulati telefonici – l'indagine sul rapimento di Abu Omar
10. Una telefonata poco prima dell'accesso ad una 'wifi bucata'
11. Il 'blog anti-premier' e il paradosso della privacy
12. Una ipotesi concreta di acquisizione di log files presso gli ISP italiani

**Capitolo 9 – LE RICHIESTE PER FINALITÀ DI GIUSTIZIA RIVOLTE AGLI *INTERNET PROVIDERS* ESTERI**

13. Quale regime giuridico per le chiamate VOIP?
14. Le indagini relative alla scomparsa dell'imprenditore Roveraro

**Capitolo 12 – I “NUOVI” STRUMENTI DI INDAGINE**

15. Le e-mail traccianti e il processo Svanityfair

**Capitolo 15 – LE “NUOVE FRONTIERE” DELL’INVESTIGAZIONE DIGITALE ALLA LUCE DELLA LEGGE N. 48/2008, OVVERO: QUELLO CHE LE NORME (ANCORA) NON DICONO**

16. Analisi forense di computer portatili con cifratura dell’intero hard disk
17. Accesso alla casella di posta elettronica @yahoo.com in uso all’indagato, durante l’interrogatorio del PM