

Il Manuale, unico nel suo genere in Italia, ha lo scopo di guidare gli investigatori (Magistrati e Forze dell'ordine), gli Avvocati, i consulenti e gli studiosi della materia nelle varie fasi delle indagini digitali, soffermandosi sull'analisi degli aspetti giuridici e accompagnandoli passo passo nell'approfondimento delle fasi più tecniche della *computer forensics* e degli accertamenti informatici.

Gli aggiornamenti saranno disponibili sul sito [www.telematici.com](http://www.telematici.com).

### Profilo degli autori

**STEFANO ATERNO** - [www.studioaterno.it](http://www.studioaterno.it) - Avvocato penalista, docente di informatica e diritto all'Università La Sapienza di Roma, responsabile del Corso di diritto penale dell'informatica presso l'Università LUMSA di Roma. Ha pubblicato diversi libri, articoli e commenti sul diritto delle nuove tecnologie. È Vice Presidente del capitolo italiano di IISFA (*International Information Systems Forensics Association* - [www.iisfa.net](http://www.iisfa.net)).

**FRANCESCO CAJANI** - Sostituto Procuratore della Repubblica presso il Tribunale di Milano, *pool* reati informatici. Sui temi attinenti alle indagini in materia di *cybercrime* sono stati pubblicati suoi interventi in occasioni istituzionali (Eurojust e Consiglio d'Europa) e in convegni di studio anche internazionali, nonché note a sentenze e commenti su riviste giuridiche. È membro del comitato tecnico & scientifico di IISFA - *Italian Chapter*.

**GERARDO COSTABILE** - [www.costabile.net](http://www.costabile.net) - Responsabile della Sicurezza delle informazioni - Tutela Aziendale del Gruppo Poste Italiane, fino al 2006 è stato investigatore nel Gruppo Repressione Frodi della Guardia di Finanza di Milano. Al suo attivo ha numerose indagini ed attività di *computer forensics* nel settore degli abusi tecnologici e del contrasto al terrorismo nazionale e internazionale. Esperto nella formazione e cristallizzazione della c.d. prova informatica, è Presidente dell'*Italian Chapter* e Vicepresidente dell'*International Chapter* di IISFA.

**MARCO MATTIUCCI** - [www.marcomattiucci.it](http://www.marcomattiucci.it) - Ingegnere Elettronico e Maggiore dell'Arma dei Carabinieri, è Comandante della Sezione Telematica del Reparto Tecnologie Informatiche dell'Arma con sede nel RaCIS di Roma. Investigatore, ha coordinato numerose indagini complesse. Ricercatore scientifico e docente, insegna presso i maggiori reparti addestrativi dell'Arma quale referente unico ed esternamente presso Corsi di laurea, di specializzazione e master nelle maggiori università italiane.

**GIUSEPPE MAZZARACO** - Responsabile del *Corporate Investigation e Fraud Prevention* del Gruppo Poste Italiane, fino al 2006 è stato investigatore nel Gruppo Repressione Frodi della Guardia di Finanza di Milano. Ha cooperato con Autorità Governative, militari e di *intelligence* americane ed europee, quali ad esempio la NASA, l'US Army, l'US Navy, l'United States Secret Service e l'OLAF (Ufficio europeo per la lotta antifrode presso la Commissione Europea a Bruxelles). È *Director of Certification dell'International Chapter* di IISFA e docente in numerose Università Italiane.

S. ATERNO, F. CAJANI, G. COSTABILE,  
M. MATTIUCCI, G. MAZZARACO

# COMPUTER FORENSICS E INDAGINI DIGITALI

Manuale tecnico-giuridico e casi pratici

prefazione di Pietro Grasso e Domenico Vulpiani



cofanetto con 3 volumi indivisibili

## PIANO GENERALE DELL'OPERA

### VOLUME I

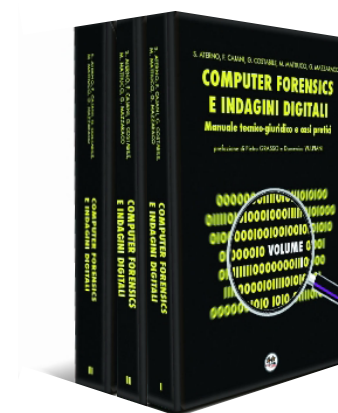
- nozioni ed elementi tecnici di principio
- la ricezione della *notitia criminis*: i primi passi verso una corretta individuazione ed acquisizione degli elementi di prova di natura informatica
- i file di *log* e la conservazione dei dati aziendali: aspetti investigativi e tecnici di base
- aspetti giuridici comuni delle indagini informatiche: giurisdizione e competenza, le modifiche apportate dalle legge n. 48 del 2008 al codice di procedura penale, la disciplina della *data retention* (conservazione dei dati del traffico), acquisizioni ripetibili e irripetibili della *digital evidence*, perquisizioni ed ispezioni informatiche, sequestri, attività del consulente tecnico e del perito, indagini difensive informatiche, limiti di utilizzabilità in dibattimento degli elementi di prova informatica raccolti nelle indagini, confisca dei beni.

### VOLUME II

- identificazione, acquisizione ed analisi delle *digital evidence*: approfondimenti tecnici
- la rete internet e "dintorni" (aspetti tecnici ed investigativi di base, P2P e digital forensics: il caso Emule, motori di ricerca e social network, sequestro probatorio e preventivo di pagine e siti web, Internet 3.0)
- la posta elettronica
- acquisizione dati del traffico ed intercettazioni telematiche
- le operazioni digitali sotto copertura: l'agente provocatore e l'attività di contrasto nelle indagini informatiche
- i "nuovi" mezzi di ricerca della prova: videoriprese investigative, agente segreto attrezzato per il suono, pedinamento elettronico ed appostamenti informatici, installazione di captatori informatici (cd. Trojan ad uso investigativo)

### VOLUME III

- *quality management* e *digital forensics* industriale
- *windows forensics*
- *macintosh forensics*
- *windows memory forensics*
- *malware* e *crimeware forensics*
- tecniche di attacchi informatici a siti web: analisi delle casistiche e *log analysis*
- *mobile forensics*
- crittografia, steganografia e tecniche di analisi forense
- *electronic forensics*
- *media forensics*
- *cloud forensics*
- *printer and scanner forensics*
- *case study* ed esercizi tecnici
- bibliografia e sitografia
- glossario
- appendice delle immagini



**Editore:** Experta srl  
**ISBN:** 978-88-6021-258-0  
**Pagine:** 2232 + 32  
(Appendice a colori)  
**Formato:** 17x24  
**Anno:** 2011  
**Prezzo di copertina:** 135 Euro

Disponibile su [WWW.EXPERTA.IT](http://WWW.EXPERTA.IT) e [WWW.TELEMATICI.COM](http://WWW.TELEMATICI.COM)  
senza spese di spedizione