

## Indice

### CAPITOLO PRIMO

#### Acquisizione forensica di documentazione informatica

di *Paolo Carretta*

1.1. Questioni preliminari .....	p.	9
1.2. La documentazione informatica .....	»	23
1.3. L'acquisizione della documentazione informatica: profili operativi e regole di base .....	»	28

### CAPITOLO SECONDO

#### L'acquisizione delle prove digitali nel processo civile, penale, amministrativo e tributario

di *Antonino Iacoviello*

2.1. Le c.d. "prove digitali": regole per la corretta ricerca ed acquisizione agli atti del processo penale .....	»	41
2.1.1. La <i>digital forensics</i> : metodi, tecniche e campo di applicazione della c.d. <i>computer forensics</i> .....	»	41
2.1.2. Mezzi di ricerca della prova digitale nel procedimento penale: perquisizione, ispezione e sequestro .....	»	46
2.1.3. Acquisizione, conservazione ed analisi della prova digitale .....	»	51
2.2. Le prove digitali nel processo civile, amministrativo e tributario .....	»	54
2.2.1. Valore giuridico ed efficacia probatoria del documento informatico alla luce delle recenti innovazioni normative .....	»	54
2.2.2. L'ingresso delle prove informatiche nel processo civile e nel processo tributario .....	»	61
2.2.3. L'ingresso delle prove informatiche nel processo amministrativo ....	»	64

### CAPITOLO TERZO

#### Computer forensics e procedure standardizzate

di *Francesco Trocchi*

3.1. Introduzione - Computer Forensics e procedure standardizzate .....	»	69
3.2. Pragma operativo .....	»	70
3.3. L'identificazione .....	»	71
3.4. La preservazione .....	»	73
3.5. L'acquisizione .....	»	74
3.6. I vantaggi dell' <i>Open Source</i> .....	»	77
3.7. Efficacia dei <i>block-writer</i> .....	»	78
3.8. Analisi, a basso livello, degli effetti del " <i>mount</i> " sui <i>file system</i> sottoposti a investigazione .....	»	79
3.9. Caso pratico di acquisizione .....	»	93

## CAPITOLO QUARTO

### Indagini digitali mediante strumenti Open Source e Freeware

di *Alessio Grillo*

4.1. Premessa	p.	107
4.2. Recupero dati referenziati: <i>The Sleuth Kit</i>	»	108
4.3. Recupero dati non referenziati: <i>data carving</i>	»	114
4.3.1. <i>Data carving</i> da shell: <i>foremost</i>	»	116
4.3.2. <i>Data carving</i> da interfaccia grafica: <i>Photorec</i>	»	130
4.4. <i>Autopsy Browser</i>	»	132
4.5. <i>Timeline</i>	»	143
4.6. Ricerca file	»	152
4.6.1. <i>Find</i>	»	153
4.6.2. <i>Locate</i>	»	163
4.7. Ricerca nei contenuti: <i>grep</i>	»	165
4.8. <i>Digital Evidence &amp; Forensics Toolkit (DEFT)</i>	»	169
4.9. eMule forensics	»	174
4.10. <i>D.A.R.T.</i>	»	177
4.11. <i>Browser forensic</i>	»	180
4.12. Registro di sistema	»	182
4.13. Cronologia accensioni e spegnimenti	»	196
4.14. <i>Antiforensics (data hiding)</i>	»	198
4.15. Conclusioni	»	201
Ringraziamenti	»	202
Bibliografia	»	202

## CAPITOLO QUINTO

### Indagini digitali e crime mapping

di *Antonio Cilli*

Premessa	»	203
5.1. Dispositivo di navigazione satellitare - TOM TOM	»	204
5.2. <i>Crime Mapping</i>	»	213
5.3. Le tecniche di “ <i>Crime Mapping</i> ” e gli strumenti G.I.S.	»	214
5.4. Presentazione dello strumento <i>CMAF C.A.S.E. (Crime Analysis Spatial Extension)</i>	»	221
5.5. Compiti di base nell’analisi delittuosa spaziale	»	223
5.6. La “ <i>Frame Reference</i> ”	»	223
5.7. Le distribuzioni di punti	»	225
5.8. Tendenza centrale	»	231
5.9. <i>Spider diagram</i>	»	232
5.10. Analisi sequenziale	»	234
5.11. I dati sotto esame: <i>Gotham City</i>	»	236
5.12. Simulazione: come determinare uno spazio di attività criminale nel caso di un evento criminoso seriale	»	238
5.13. Conclusione	»	247
Bibliografia	»	249