Index

Access controls, 43, 73–79, 211
Accounting, forensic, 104–107, 129–130
Actuators, 22–23
Air travel, 77, 85
Anonymous identities, revealing, 151–152
Application data, 32–35
Apps, 49
Attorneys, 107–111, 118
Audio files, 51–54

Backup systems, 145–147, 173
BIOS (basic input output system), 34
Bots and botnets, 61–62, 184
Boundary scans, 50
Broadband routers, 31

Cars, transporting evidence by, 77, 85
Case management, 128–129
Cellular phones, 50–51, 92
Central processing unit (CPU), 29
Certification, 98, 114
Chain of custody, 76–79, 83–85
Chat, online, 40
China, 180, 197
Clients, 99–100
Cloud computing, 16–164, 47, 63–66, 211–212
Cognitive computing, 212
Collection phase, 5, 191, 192–194, 197–198
Colocation facilities (colos), 57
Computer abuse, 12
Computer-assisted review, 111–112, 142, 195, 203
Computer crime analysis and reconstruction, 147–149
Computer forensic examiners, 85–86, 98, 100–101, 165
Computer forensic laboratories
  establishment, 69–73
  evidence and access controls, 73–79
  staffing, 85–86
  teamwork and workflow, 94–98
  tools, 86–94
  workstations, 79–82
Computer forensics, defined, 4–6
Computer monitoring software, 62–63
Computers, types of, 17
Concept searching (machine-assisted review), 111–112, 142, 195, 203
Connectors, 22
Contracts, 154–155
Cyber investigators, 102–103
Cyberprofiling, 154

Data acquisition forms, 78–79
Data- and traffic-gathering applications, 60–63
Database management system (DBMS), 38
Databases, 37–41, 178
Data breaches, 169, 170–172, 185–186
Data centers, 56–57
Data classification, 140–143
Data collection, 5, 191, 192–194, 197–198
Data concealment, 33
Data hosting and review, 195
Data identification, 189–190, 191
Data maps, 190
Data preservation, 5–6
Data privacy experts, 113–114
Data processing, analysis, and analytics, 6, 191, 194–195
Data reviewers, 115–116

COPYRIGHTED MATERIAL
http://www.pbookshop.com

Data storage, 33–34
DDoS (distributed denial-of-service) attacks, 61
Defense attorneys, 110–111
Deleted data, 143–145
Demilitarized zone (DMZ), 60
Detail, attention to, 124–126
Digital evidence
  characteristics of, 9–11
  control over, 73–79, 83–85
  seizure and examination, 140
  storage and transportation, 83–85
Document usage data, 33
Domain name, 44–45
Drills, 170
Dynamic data capture, 63–65

Early case assessment, 142, 159–160
Electronic discovery (e-discovery), 189–207
  courtroom presentation, 207
  data identification, 189–190
  emerging issues, 202–205
  experts, 111–113
  history of, 3
  international issues, 196–199, 205–206
  model for, 189, 190–192
  stages, 192–196
  tools, 199–202
Electronic discovery reference model (EDRM), 189–192
E-mail, 33, 41–43
Employees, investigations of, 134–136, 173–175
EnCase, 86–87
Encryption, 153–154, 198
Ethical issues, 12, 155–156
Evidence, forms of, 9–10. *See also* Digital evidence
Exhibits, 207
Experts, 111–114
Extra-national investigative networks, 214

Field, handling evidence in, 77
File backup systems, 145–147
File creation time stamps, 45
File sharing, 33
Findings, 11–12, 124–125, 136–137, 165–166
Firewalls, 59–60
Forensic accountants, 104–107, 129–130
Fraud, 129–130, 172
FTK (Forensic Tool Kit), 87–88

Global citizenship, 212–213
Global information networks. *See* Networks

Hacking, 123, 124, 147–148, 151–152, 171, 178–187
Hard drives, 18, 19–24, 27, 29–30, 83–84, 124, 125, 126, 141, 162
Hardware, 27
Heads, 21, 22
High-Tech Crime Investigators Association, 120
Honeypots and honeynets, 63, 176–177
Human resources, 134–136

IaaS (infrastructure as a service), 65–66
IBM, 22
IDE hard drives, 84, 125, 162
Identity theft, 179, 180, 182–183
Imaging hardware, 90–93
Incident response, 167–170
Information management, 191
Intellectual property theft, 133–134, 180, 183–184
Interactive communications data, 33
Internal investigations, 134–136, 173–175
International issues
  cybercrime, 180–181
  data collection, 122–123
  e-discovery, 196–199, 205–206
  global citizenship, 212–214
  investigations, 161–162
  networking, 175–176
  security, 67–68
Internet bots, 61
Internet data, 39–41
Internet servers, 40
Internet Service Provider (ISP) records, 164–165
Interviews and interviewers, 118, 133, 153
Investigations
  case management, 128–129
  challenges, 157–166
  of employees, 134–136
  findings, 11–12, 124–125, 136–137, 165–166
  interviews, 118, 133, 153
  mind-set of investigator, 127–128

http://www.pbookshop.com

  objectives, 11, 157–166
  process, 11–12
  techniques, 130–132
  types of, 11
Investigators, 2–4, 102–104, 127–128, 139–140
iPad, 48–50
IP (Internet Protocol) address, 31, 42, 43–45, 151, 164
Iranian nuclear facilities, STUXNET attack, 181

Judges, 121
Juries, 121–122

Keyloggers, 63–64

Labs. *See* Computer forensic laboratories
LAN (local area network), 31, 58
Law-enforcement officers, 119–120
Legacy devices, 101
LEXIS-NEXIS, 201
Load files, 195, 201
Logicube, 83, 90–93, 200

Machine-assisted review, 111–112, 142, 195, 203
Magistrate judges, 120–121
Magnetic hard drives, 19–24
Malware, 61–63, 103, 147–148, 181, 184–185
Maps and mapping, 58–59, 149–151, 190
Meaning-based computing (machine-assisted review), 111–112, 142, 195, 203
Metadata, 35–37
Mobile devices, 48–51
Motors, hard drive, 23

Nanotechnology, 212
NetAnalyis, 93–94
Network attached storage (NAS), 24, 72, 193
Network engineers, 102
Networks
  data on, 54–58
  fundamentals of, 58–59
  history, 18–19
  routers, 30–32
  types of, 17
Neutrals, 113, 204
Nonvolatile data, 33–34
NoSQL (not only structured query language), 47–48
Nuix, 199–201
Numbering scheme, for evidence, 75

Operating system (OS), 49
Optical drives, 25–27
Organized crime, 178–179

PaaS (platform as a service), 65
Pace, of investigation, 160–161
Packet analysis, 41
Packet filters, 59
Peer-to-peer networks, 58
Phishing, 185
Pickup head (PUH), 25
Plaintiff's attorney, 107–109
Platters, 21, 22
Police officers, 119–120
Policy-based routers, 32
Pornography, 135–136
Predictive coding, 111–112, 142, 195, 203
Presentation, 6, 191–192, 196
Preservation phase, 5–6
Privacy, 14–15, 67–68, 113–114, 209–211
Production of documents, 207
Project managers, 117–118
Prosecutors, 120–121
Proxy servers, 60
The public, 122–123

RAID (redundant array of independent disks), 23–24
RAM (random access memory), 5, 29, 34, 148
Real-time challenges, 175, 214–215
Recorder identification code (RID), 26
Records and recordkeeping, 128–129, 130, 140–143
Relational database management system (RDBMS), 47
Relativity, 201–202
Reporting, investigation results, 136–137, 165–166
Researchers, 118–119
Results, of investigations, 11–12, 124–125, 136–137, 165–166

http://www.pbookshop.com

Routers, 30–32
RPM, 29–30

SaaS (software as a service), 65
Safe zone, 69, 71
SATA hard drives, 84, 126
Search engines, 140–142
Security
  applications, 33
  computer forensic labs, 72–75
  e-mail restrictions, 43
  firewalls, 59–60
  international issues, 67–68
  preparation for attacks, 158–159
  social media, 46
  wireless routers, 31
Sedona Conference, 204–205
Servers, 23, 27–30, 40, 60, 168
Service vendors, 175–176
SilentRunner, 64
Smartphones, 50–51, 92
SMTP (simple mail transfer protocol), 42–43
Sniffers, 62, 63
Social engineering, 152–153
Social media, 45–48, 162–164
Software. *See* Tools
SoloMaster, 90–93
Source identification code (SID), 26
Special masters, 203–204
Spindles, 22
Spoilation, 112, 206
Spyware, 62
SQL (structured query language), 47
SQL injection attacks, 149, 171
Staffing, 85–86
Stateful filters, 59
State-sponsored cybercrime, 181–182
Storage
  application data, 33–34
  databases, 39
  digital evidence, 83–85
  global capacity, 56
  social media, 46–47
Structured data, 178
Surveillance, 132–133
Systems failures, 172–173

Tablets, 48–50
Teamwork, 94–96, 161–162
Technicians, 85–86
Technological changes, 1–2
Technology-assisted review, 111–112, 142, 195, 203
Testimony, 137
Theft, 133–134, 172, 179, 180, 182–184
Third parties, 154–155
Time management, 96–98, 156, 160–161
Time stamps, 45
"Toaster" box, 70
Tools
  computer monitoring software, 62–63
  early case assessment, 159–160
  e-discovery, 199–202
  forensic software, 81–82, 86–94
  investigations, 130–132
Tracks, 21–22
Trade secret theft, 133–134
Transmission control protocol (TCP), 42, 43, 58
Transportation, of digital evidence, 83–85
Trojans, 185
Trust, 9, 13–14, 211
Truth, relevancy of, 8–9

Unstructured data, 178

Victims, 99–100
Video files, 51–54
Volatile data, 33–34

WAN (wide area network), 31, 58
Web 2.0, 45, 46
Web bots, 61
Web browsers, 33, 93–94
Web spiders or crawlers, 61
Web usage data, 33
Whistleblowers, 122
Wireless activity, 41
Wireless routers, 31
WLAN (wireless local area network), 58
Working copy, 75
Workstations, 79–82
Write blockers, 88–90

X1 Discovery, 93, 163

Zero day forensics, 214–215

http://www.pbookshop.com