

Page numbers in *italics* indicate figures and tables

A

AAFS, *see* American Academy of Forensic Sciences
 AccessData's, 37, 38
 FTK, 37
 MPE+, 156
 Accreditation, 40–43
 Active data, 20
 Administrative review process, 32
 Allocated space, 22–23
 American Academy of Forensic Sciences (AAFS), 8–9
 American Society for Testing and Materials (ASTM), 9–10, 42
 American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (ASCLD/LAB), 9, 40–42
 Analysis, 138
 Android, 150
 Anonymous remailing, 127
 Antiforensics techniques, 82
 Anti-Forensics.com, 81
 Antistatic material bags, 52
 Apple FileVault, 88
 Apple OSX, 97
 Application logs, 139
 Archival data, 21
 ASCII, 14–15
 ASCLD/LAB, *see* American Society of Crime Laboratory Directors/Laboratory Accreditation Board
 ASTM, *see* American Society for Testing and Materials
 Asymmetrical encryption, 85
 Attribution, 69
 AuC, *see* Authentication Center
 Authentication Center (AuC), 147
 Authentication log, 139

B

Base station, 147
 Base station controller (BSC), 147

Binary, 13
 Bind, Torture, Kill (BTK), 3–4
 Bit, 13–15
 BitLocker, 86–88
 BitPim, 156
 Blackberrys, 150
 Blind test, 33
 Blocks, 168
 Botnet, 135
 Browsers, 117–118
 Brute force attacks, 88–90
 BSC, *see* Base station controller
 BTK, *see* Bind, Torture, Kill
 Byte, 13–15

C

Caesar Cipher, 84
 Call detail records (CDR), 151–152
 Campus Area Networks (CANs), 133
 CANs, *see* Campus Area Networks
 Carrier files, 92
 Casey Anthony trial, 129
 CDMA, *see* Code Division Multiple Access
 CDR, *see* Call detail records
 Cell phone, 47–49
 acquisition, 155
 CDR, 151–152
 evidence, 150
 collecting and handling, 152–154, 153
 faraday bag and, 48, 48
 forensic tools, 155–157
 network signals, 48
 SIMs, 154–155
 Cell site, 147
 Celebrite UFED device, 156–157, 156
 Cellular networks
 cell site, 147
 components, 147–148
 layout of, 146, 146
 types of, 148–149
 Central processing unit (CPU), 19, 27
 Certification, 42–43
 CFTT, *see* Computer Forensic Tool Testing
 Chain of custody, 52, 53
 Chat clients, 124–125
 Chronological order method, 51
 Cipher text, 83
 Client/server network, 132
 Cloning, 52–56
 eDiscovery, 56
 forensic image formats, 55
 forensically clean media, 55
 process of, 54–55
 purpose of, 54
 risks and challenges, 55
 Cloud
 benefits of, 166
 computing, 19–20, 165–166
 forensics, 165–167
 private and public, 165
 Cloud Service Provider (CSP), 165
 Code Division Multiple Access (CDMA), 148–149
 Complex encryption schemes, 86
 Computer Forensic Tool Testing (CFTT), 9, 36
 Computer Security Incident Handling Guide, 137
 Computer storage devices, 109–110
 Computing environments, 19–20
 Consent, 105–106
 forms, 106
 Containment, 138
 Cookies, 120–121
 CPU, *see* Central processing unit
 CRC, *see* Cyclical redundancy check
 Crime scenes, 46–49
 Criminal law
 duty to preserve, 111–113
 ECPA, 105
 eDiscovery, 111–113
 e-mail, 105

Criminal law (*Cont.*)
 off-site analysis, 109–110
 private searches, 105
 in workplace, 112–113
 reasonable expectation of privacy,
 104–105
 SCA, 110–111
 search warrant requirement,
 exceptions, 105–108
 warrant, 108–111
 Cryptographic algorithm, 83
 CSI effect, 10
 CSP, *see* Cloud Service Provider
 Cybernap process, 66
 Cyclical redundancy check (CRC), 134

D

Data
 destruction, 94
 hiding, 94
 persistence, 22–23
 safe, 31
 sampling, 112
Daubert, 164
v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), 114
 DCC, *see* Direct Client Connection
 DCO, *see* Device Configuration Overlays
 DDoS, *see* Distributed Denial of Service
 Dead system, 56–59
 Decimal, 13
 Deep sleep modes, 66
 Deleted data, 66
 Detection, 138
 Device Configuration Overlays (DCO), 22
 Device logs, 139
 Dictionary attack, 88, 90–92
 Digital evidence, 111
 Digital forensics, 2–3, 69
 tools
 hardware, 36–39
 selection, 36
 uses of
 AAFS, 8–9
 administrative matters, 6–7
 ASTM, 9–10
 civil litigation, 4–5
 criminal investigations, 3–4
 intelligence, 5–6
 Locard's exchange principle, 7
 NIST, 9

scientific method, 7
 SWGDE, 8
 Digital solutions, 30
 Direct Client Connection (DCC), 125
 Directional antenna, 152
 Distributed Denial of Service (DDoS), 135
 DNS, *see* Domain Name Server
 Document and Media Exploitation (DOMEX), 5
 Documentation process, 49
 Domain Name Server (DNS), 118
 DOMEX, *see* Document and Media Exploitation
 Drive wiping, 94–99
 Dutch National High Tech Crime Unit (NHTCU), 136
 Dutch NHTCU, *see* Dutch National High Tech Crime Unit
 Duty to preserve, 111–112
 Dynamic page, 118

E

ECPA, *see* Electronic Communications Privacy Act
 ECS, *see* Electronic communication service
 eDiscovery, *see* Electronic Discovery
 EFS, *see* Encrypting File System
 Electronic communication service (ECS), 110
 Electronic Communications Privacy Act (ECPA), 105
 Electronic Discovery (eDiscovery), 4, 56, 111–113
 Electronic Serial Number (ESN), 149
 Electronically stored information (ESI), 111
 E-mail, 105
 accessing, 126
 as evidence, 126–127
 headers, 128–129
 protocols, 126
 tracing, 127–128
 URL, 117
 EMF, *see* Enhanced Meta File
 Encoding schemes, 14
 Encrypting File System (EFS), 87
 Encryption, 94
 algorithms, 85–86
 breaking passwords, 88–89
 definition, 83–84
 key space, 86
 types of, 86–88

Enhanced Meta File (EMF), 70
 Eradication, 138
 ESI, *see* Electronically stored information
 ESN, *see* Electronic Serial Number
 Evidence Eliminator, 78
 Examiner's final report, 35
 Exigent circumstances, 107
 External drives, 70
 External test, 33

F

Faraday bag, 48, 48
 FAT, *see* File Allocation Table
 FDE, *see* Full disk encryption
 FDLE, *see* Florida Department of Law Enforcement
 Federal Rules of Civil Procedure, 4
 FEPAC, *see* Forensic Science Education Programs Accreditation Commission
 Fidelity National Information Services Inc. (FIS), 131
 File Allocation Table (FAT), 21
 File carving, 15, 66
 File extensions, 15–16, 16
 File header, 26
 File signature analysis, 15–16, 16
 File system, 21–22
 File Translation Layer, 168
 FileVault, 86
 Firewall, 135
 FIS, *see* Fidelity National Information Services Inc.
 Flash based hard drives, 18
 Flash memory, 18
 Florida Department of Law Enforcement (FDLE), 164
 Footer, 26
 Footprinting/fingerprinting, 136
 Forensic cloning, 56
 Forensic examiner in judicial system, role of, 10
 Forensic image formats, 55
 Forensic laboratories
 evidence storage, 31–32
 lab security, 30–31
 virtual labs, 30
 Forensic science, 2
 committee, 9
 gold standard of, 7
 Forensic Science Education Programs Accreditation Commission (FEPAC), 8
 Forensic Toolkit (FTK), 37, 39

Forensic tools, 40, 41, 70
 Forensically clean media, 55
 Fourth Amendment, 104
 Frye Test, 113
 FTK, *see* Forensic Toolkit
 Full disk encryption (FDE), 86

G

GANs, *see* Global area networks
 Garbage Collection, 168
 Gateway, 135
 GB, *see* Gigabytes
 Gigabytes (GB), 46
 Global area networks (GANs), 133
 Global Positioning System (GPS), 157–160
 Global System for Mobile Communication (GSM), 148–149
 Gnutella, 119
 GPS, *see* Global Positioning System
 GSM, *see* Global System for Mobile Communication

H

Hackers, 132
 Handoff, 148
 Hard drives, 54
 Hardware write blocking (HWB) device, 36
 Hash functions, 59
 Hashing
 algorithms, types of, 59
 example of, 59–60
 uses of, 60
 Header, 26, 127
 Hexadecimal, 14
 numbers, 96
 HFS+, *see* Hierarchical File System Plus
 Hiberfile.sys, 66–67
 Hibernation, 67
 Hierarchical File System Plus (HFS+), 22
 HLR, *see* Home Location Register
 Home Location Register (HLR), 147
 Host Protected Area (HPA), 22
 HPA, *see* Host Protected Area
 HTML, *see* Hypertext Markup Language
 HTTP, *see* Hypertext Transfer Protocol
 HWB device, *see* Hardware write blocking device
 Hybrid sleep, 67

Hypertext Markup Language (HTML), 118
 Hypertext Transfer Protocol (HTTP), 117

I

IaaS, *see* Infrastructure as a Service
 ICC-ID, *see* Integrated Circuit Card Identifier
 ICQ, 125–126
 iDEN, *see* Integrated Digitally Enhanced Network
 Identity Spoofing (IP Spoofing), 136
 IDS, *see* Intrusion Detection System
 IMAP, *see* Internet Message Access Protocol
 IMEI, *see* International Mobile Equipment Identifier
 IMSI, *see* International Mobile Subscriber Identity
 Index.dat file, 120
 Infrastructure as a Service (IaaS), 19–20
 Insider threat, 130–131
 Integrated Circuit Card Identifier (ICC-ID), 154
 Integrated Digitally Enhanced Network (iDEN), 149
 Internal test, 33
 International electronic discovery, 113
 International Mobile Equipment Identifier (IMEI), 149
 International Mobile Subscriber Identity (IMSI), 154
 Internet
 history, 122–123
 HTML, 118
 HTTP, 117
 index.dat file, 120
 IP, 118
 P2P, 119–120
 TLD, 117
 whois, 119
 Internet Message Access Protocol (IMAP), 126
 Internet Protocol (IP), 118
 address, 133
 Internet Relay Chat (IRC), 125
 Internet Service Providers (ISPs), 110, 134, 140
 Interworking functions, 147
 Intranets, 133
 Intrusion Detection System (IDS), 135

iOS, 150
 IP, *see* Internet Protocol
 IRC, *see* Internet Relay Chat
 ISPs, *see* Internet Service Providers

J

JavaScript, 118

K

Key space, 86

L

LAN, *see* Local Area Network
 Lands, 18
 Latent data, 21
 Legacy data, 21
 Link files, 78–79
 Live system
 live acquisition concerns, 56–57
 live collection
 advantage of, 57–58
 conducting and documenting, 58–59
 principles of, 58
 Local Area Network (LAN), 133
 Locard's exchange principle, 7
 Log files, 139–140

M

Magnetic disks, 17, 17–18
 Mainframe system, 19
 Malware, 31
 Man-In-The-Middle-Attack, 136
 MANs, *see* Metropolitan Area Networks
 Marshall University Digital Forensics, 14
 MEID, 153
 Memory, 16–19
 cards, 46–47
 Message ID, 127
 Metadata, 72–75
 removing, 74–75
 Metropolitan Area Networks (MANs), 133
 Microsoft's TechNet, 67
 Mini-computers, 145
 MMS, *see* Multimedia Messaging Services
 Mobile Switching Center (MSC), 147–148
 Most Recently Used (MRU), 76, 76
 Moussaoui, Zacarias, 5–6
 MRU, *see* Most Recently Used
 MSC, *see* Mobile Switching Center

Multimedia Messaging Services (MMS), 148
Multiple tools, 35

N

NAS, *see* National Academy of Sciences
National Academy of Sciences (NAS), 8
National Initiative Cyber Security Education (NICE), 9
National Institute of Standards and Technology (NIST), 8, 36, 137, 165
National Software References Library, 9
Network intrusion detection system (NIDS), 135
Network security tools
 evidence and investigations
 log files, 139–140
 tools, 140–141
 firewall, 135
 hacks and attacks, 135–137
 incident response, 137–139
Network signals, protecting cell phones from, 48
Networked computer, 19
New Technology File System (NTFS), 21, 87
NICE, *see* National Initiative Cyber Security Education
NIDS, *see* Network intrusion detection system
NIST, *see* National Institute of Standards and Technology
Nonvolatile memory, 18–19
NTFS, *see* New Technology File System
NTUSER.DAT file, 123
NukeOnDelete, 71
Numbering schemes, 13–15

O

Obfuscation, 84
Office of the Inspector General (OIG), 6
Off-site analysis, 109–110
OIG, *see* Office of the Inspector General
Open Handset Alliance, 150
Open test, 32
Operating system (OS), 149–150
 logs, 139
Optical media, 18

Optical storage, 18
Order of volatility, 49
OS, *see* Operating system
Oxygen Forensic Suite, 156

P

PaaS, *see* Platform as a Service
Packet switching, 134
Pages, 168
 file, 25–26
PANs, *see* Personal Area Networks
Paraben Corporation, 156
Password Recovery Toolkit (PRTK), 89
Password reset, 90
Patch, 132
Patriot Act, 105
Payload files, 92
Peer-to-peer (P2P), 119–120, 133
Personal Area Networks (PANs), 133
Personal Identification Number (PIN), 151, 155
Personal Unlock Key (PUK), 151
Photography, 50–51
PIN, *see* Personal Identification Number
Plain text, 83
Plain view doctrine, 107
Platform as a Service (PaaS), 19–20
POI, *see* Points of Interest
Points of Interest (POI), 158
POP, *see* Post Office Protocol
Post Office Protocol (POP), 126
Postincident activity, 138
P2P, *see* Peer-to-Peer
Predictive text, 151
Prefetch, 78
Prepaid cell phones, 149
Preparation phase, 138
Preprinted forms, 34
Print spooling, 70
Private clouds, 165
Private searches, 105
 in workplace, 112–113
Probable cause, 104
Proficiency testing, 32
PRTK, *see* Password Recovery Toolkit
PSTN, *see* Public Switched Telephone Network
Public clouds, 165
Public Switched Telephone Network (PSTN), 148
PUK, *see* Personal Unlock Key

Push to Talk, 149
Push-button tools, 40

Q

QA, *see* Quality assurance
Quality assurance (QA)
 documentation, 34–35
 tool validation, 33–34

R

RAM, *see* Random Access Memory
Random Access Memory (RAM), 19, 26
 preserving evidence in, 57
RCFL program, *see* Regional Computer Forensic Laboratory program
RCS, *see* Remote computing service
Reasonable expectation of privacy, 104–105
Recovery, 138
Recycle bin, 70–72, 72
Regional Computer Forensic Laboratory (RCFL) program, 30
Registry, 67–70
 internet explorer artifacts, 123–124
Remote computing service (RCS), 110
Removable storage media, 47
Resetting passwords, 88
Restore points (RP), 76–77
Routers, 139
 direct data, 135
 logs, 140
RP, *see* Restore points
Rules of Civil Procedure, 111

S

SaaS, *see* Software as a Service
SARC, *see* Steganography Analysis and Research Center
SCA, *see* Stored Communications Act
Scientific method, 7
Scientific Working Group for DNA Analysis Methods (SWGDM), 8
Scientific Working Group on Digital Evidence (SWGDE), 8, 43, 164–165
Scientific Working Groups (SWGs), 8
SEC, *see* Securities and Exchange Commission
Sectors, 23, 23–24

Secure Erase options, 97
 Securities and Exchange Commission (SEC), 6–7
 Security identifier (SID), 69
 Sedona Conference, 111
 Service Level Agreements (SLAs), 167
 Shadow copies, 77–78
 Short Message Service (SMS), 148
 Short Message Service Center (SMSC), 147
 SID, *see* Security identifier
 SIFT, 39
 SIM, *see* Subscriber Identity Module
 Simple Mail Transfer Protocol (SMTP), 126
 Slack space, 23, 25, 25
 SLAs, *see* Service Level Agreements
 Sleep mode, 67
 Small-scale devices, 38
 Smartphone, 159
 SMS, *see* Short Message Service
 SMSC, *see* Short Message Service Center
 SMTP, *see* Simple Mail Transfer Protocol
 Sniffer, 135, 140
 Social engineering, 132, 136
 Social media evidence, 129
 Social networking sites, 129
 Software, 39–40
 Software as a Service (SaaS), 19–20
 Solid state drive (SSD), 18, 167–168
 SOPs, *see* Standard Operating Procedures
 Spindle, 17
 Spoliation, 111
 Spoofing, 127
 Spooling, 70
 SSD, *see* Solid state drive
 Stand-alone computer, 19
 Standard Operating Procedures (SOPs), 32
 Standards & controls, 164–165
 Static Web page, 118
 Steganography, 92–94
 Steganography Analysis and Research Center (SARC), 93

Stored Communications Act (SCA), 110–111
 Subscriber Identity Module (SIM), 154–155
 Swap space, 25–26
 SWGDAM, *see* Scientific Working Group for DNA Analysis Methods
 SWGDE, *see* Scientific Working Group on Digital Evidence
 SWGs, *see* Scientific Working Groups
 Symmetrical encryption, 85
 System encryption, 57

T

Tapes, 21
 TCP/IP, *see* Transmission Control Protocol/Internet Protocol
 TDMA, *see* Time Division Multiple Access
 Technical review process, 32
 Technical Working Groups (TWGs), 8
 Temporary Internet Files (TIF), 121–122
 Third parties, 107
 Thumb drives, 70
 Thumbnail cache, 75–76
 TIF, *see* Temporary Internet Files
 Time Division Multiple Access (TDMA), 149
 TLD, *see* Top Level Domain
 Top Level Domain (TLD), 117
 TPM, *see* Trusted Platform Module
 Track log, 157–158
 Trackpoints, 157–158
 Transistors, 18
 Transmission Control Protocol/Internet Protocol (TCP/IP), 132
 Triangulation, 152
 Trilateration, 157
 TrueCrypt, 88
 Trusted Platform Module (TPM), 87
 TWGs, *see* Technical Working Groups
 Twitter, 169–170

U

Unallocated space, 22–23
 Unicode, 14–15
 Uniform Resource Locator (URL), 117, 123
 United States Secret Service (USSS), 136
United States v. Frye, 113
 URL, *see* Uniform Resource Locator
 USSS, *see* United States Secret Service

V

Vance, Christopher, 159–160
 Virtual memory, 26
 Virtualization, 165
 Visitor Location Register (VLR), 147
 VLR, *see* Visitor Location Register
 Voice-mail, 154
 Volatile memory, 18–19

W

WAN, *see* Wide Area Network
 Warp speed, 135
 Warrant, 108–111
 Waypoints, 158
 Wear leveling process, 168
 Web browsers
 chat clients, 124–125
 cookies, 120–121
 ICQ, 125–126
 internet history, 122–123
 IRC, 125
 registry, internet explorer artifacts, 123–124
 TIF, 121–122
 Whois, 119
 Wide Area Network (WAN), 133
 Windows Registry, 67
 Wiretap Act, 105
 Write block, 36

Z

Zombies, 135
Zubalake v. USB Warburg, 111