

Index

Symbols and Numerics

802.11 technology, 219, 221, 331

• A •

AccessData, 326

AccessData Certified Examiner (ACE), 313, 326

ACPO (Association of Chief Police Officers), 235

acquisition (process). *See also* images/imaging;

retrieving/extracting (data)

for authenticating data, 113–115

copying different from, 92

defined, 91, 331

documentation process of, 96

of duplicating duplicate, 116

generalized format of, 96

hardware for, 234, 328

importance of, 95

for media types, 97–100

from mobile phones, 225, 232–233, 236–239

non-forensic, 224

physical/logical, 232

software for, 236–239, 326

standard rule for, 96

terms created during, 125

tools for, 95–96, 101–105

for transferring data, 105–113

acquittal, 301

active file, 331

Adam Walsh Child Protection and Safety Act

(AWA), 85, 331

address resolution protocol (ARP), 258

ADFSL (Association of Digital Forensics,

Security and Law), 316

admissible evidence

cross-examination on, 302

defending, 89

defined, 331

e-mail as, 299

encryption blurs, 149

expert testimony as, 83, 84

as goal, 21, 89

from Internet, 17

from mobile devices, 234

pretrial effect of, 282

rules of evidence for, 24–25, 26, 27

seizure and, 279

trial stipulation on, 297

ADS (alternate data streams), 141, 181, 331

affidavit, 43, 45–50, 86, 290, 292–293

agent, 245, 246, 247

Airplane mode, 235, 236

alternate data streams (ADS), 141, 181, 331

America Online (AOL), 12, 18, 153, 164

answering machines, 266

antistatic mat, 195

AOL (America Online), 12, 18, 153, 164

appeal, 302

Apple, 175, 183–184

application specific integrated circuit

(ASIC), 144

ARP (address resolution protocol), 258

ASIC (application specific integrated

circuit), 144

Association of Chief Police Officers (ACPO), 235

Association of Digital Forensics, Security and

Law (ADFSL), 316

AT&T, 16

audio devices, digital, 231, 330

authentication

for admissibility, 90

of contaminated data, 288

defined, 331

demonstrating, 92, 96

documentation for, 56

of e-mails, 299

as forensic process, 90

forensic server for, 328

method of, 113–115

for mobile phones, 222

of network data, 247, 258

reports for, 34

tools for, 92

AWA (Adam Walsh Child Protection and Safety

Act), 85, 331

• B •

backups

- of contaminated evidence, 78
- e-discovery of, 30, 33, 36
- during extraction process, 199
- of fail-safe protected data, 150
- finding documents from, 215–217
- for hidden data, 142
- information preservation via, 12
- on tape, 216–217

Bad Block Inode (BBI), 185

Basic Input Output System (BIOS), 177

BBI (Bad Block Inode), 185

Best Buy, 330

Best Buy v. Developers Diversified Realty, 28

Best Evidence rule, 331

biometrics, 130

BIOS (Basic Input Output System), 177

BIOS setup area, 111

bit defined, 331

bitstream image/copy, 91, 101, 105, 108, 331, 332. *See also* images/imaging

BitTorrent, 258

Blair, Tony, 205

block, 184

blogs, 5, 17, 30, 83, 291, 323–324

Bluetooth, 219, 221, 228, 234, 236, 269, 332

BMW, MVEDR in, 271

Boolean connectors, 126

boot media, 110–111

boot sector, 332

Boot Sequence tab/page, 111

Boucher, Sebastien, 149

Brady v. U.S., 280

Broadcom Corp, 28

browser files, 170–173

brute force, 142–143, 146, 147, 149, 332

Bryant, Kobe, 16

BTK Killer, 206

• C •

cache, 19, 144, 168, 186, 187, 332

Cain & Abel software, 147

calendar, 222

CAM (content addressable memory), 249

CAM (create, access, modify) facts, 203, 207–208, 214–215, 332

cameras, digital, 230–231

card reader, 100, 226, 234

case filings, 76

case folder, 86

case journal, 59, 332

case manager, 41

case theory, 75–76

case-file index, 60

catalog file, 183

catalog node identification (CNID), 183

CCDA (Cisco Certified Design Associate), 314

CCE (Certified Computer Examiner), 314

CCNA (Cisco Certified Network Associate), 314

CDMA (Code Division Multiple Access), 226, 233

CEECS (Certified Electronic Evidence Collection Specialist), 314

cell phones. *See* mobile phones

CellDEK kit, 233

cellular networks, 226–227

certification, investigator, 313–317, 323, 326

Certified Computer Examiner (CCE), 314

Certified Electronic Evidence Collection Specialist (CEECS), 314

Certified Forensic Computer Examiner (CFCE), 314

certified information systems security professional (CISSP), 315

CFCE (Certified Forensic Computer Examiner), 314

CFRDC (Computer Forensics Research and Development Center), 316

chain of custody, 33, 56, 59, 280, 281, 282, 298, 332

Champlain College degree program, 316

chat log, 332

chat room, 297

chatting, 13, 17, 18, 44, 156, 173–174

checksum, 113–115, 332

child custody case, 174

child pornography (CP), 75, 79, 85, 88, 122, 149, 230

chloral hydrate, 120

Cingular, 226

circumstantial evidence, 22, 27, 299, 332

Cisco Certified Design Associate (CCDA), 314

Cisco Certified Network Associate (CCNA), 314

- CISSP (certified information systems security professional), 315
 - civil rights, 149
 - client, accepting, 74–78, 82, 324
 - cluster, 10–11, 178, 180, 182, 333
 - cluster chaining, 180
 - CNID (catalog node identification), 183
 - CNN, 45
 - Cochran, Johnnie, 75
 - Code Division Multiple Access (CDMA), 226, 233
 - command-and-control server, 246–247
 - Compact Flash, 231
 - compression, 137, 181, 244, 333
 - CompTIA, 315
 - Computer Forensics Research and Development Center (CFRDC), 316
 - computer operating system. *See also* Windows, Microsoft
 - Apple HFS, 183–184
 - deleted information and, 10–11
 - file extensions fool, 211
 - Linux, 184–185
 - non-accessible space and, 191–192
 - password for, 147
 - saving files by, 11
 - space allocation by, 101–102
 - understanding, 175
 - Unix, 184–185
 - write blocker and, 103
 - computer, starting, 65
 - ComputerBytesMan.com, 205
 - conflict of interest, 79, 308
 - Constitution, U.S., 39, 48, 149, 280, 297
 - constitutional rights, 278, 279
 - contacts list, 222
 - content addressable memory (CAM), 249
 - contingency, 303
 - contraband, 79, 85, 88, 333
 - contract, 82
 - cookies, 17, 88, 333
 - Coordinated Universal Time (UTC), 253–256
 - copiers, 249, 272–273
 - court cases. *See* rules of evidence; trials
 - Court of Appeals, 299
 - court reporter, 283, 285, 322
 - CourtTV*, 45
 - CP (child pornography), 75, 79, 85, 88, 122, 149, 230
 - CRC (Cyclic Redundancy Check), 333
 - create, access, modify (CAM) facts, 203, 207–208, 214–215, 332
 - crime scene
 - altering evidence at, 64–66
 - camera at, 330
 - documenting, 56–62, 69
 - multiple forensic disciplines at, 57
 - securing, 63, 67–68
 - surveying, 68–69
 - tools needed at, 63–64
 - transporting evidence from, 69
 - crime-supporting tools, 19
 - cross-examination, 21, 298, 300–301, 302, 322
 - Crownhill, 233
 - cryptography, 137, 333
 - Cyclic Redundancy Check (CRC), 333
- D •
- DAS (direct attached storage), 252
 - data cable, 106–107
 - data sampling, 128
 - data sequence, 256–257
 - data storage. *See also* hard drive; retrieving/extracting (data)
 - on answering machines, 266
 - of cached files, 186, 187
 - on copiers, 272–273
 - of deleted files, 185–186
 - for digital cameras, 230–231
 - in external devices, 214
 - in file slack areas, 189–191
 - forensic server for, 328–329
 - in GPS receiver, 269
 - hard disk anatomy and, 176–177
 - on high-capacity devices, 273
 - on mobile phones, 226
 - on network, 247, 248–249
 - from network extraction, 250–252
 - in non-accessible space, 191–192
 - places for, 176
 - in RAM, 192–193
 - search filtering and, 195–196
 - in unallocated space, 186, 188–189
 - in video equipment, 266–267
 - on Windows PC, 178–182
 - in Windows Registry, 194
 - data streams, 258–259
 - data-carved files, 127

- Daubert test, 83, 333
 - Daubert v. Merrell Dow Pharmaceuticals*, 83–84, 280
 - de-duping, 33
 - defendant/defense
 - affidavit response for, 293
 - burden of proof and, 295
 - in child pornography cases, 85
 - cross-examination by, 300–301
 - defined, 333
 - direct examination by, 302
 - dismissal for, 295
 - e-discovery against, 29, 31
 - forensic imaging by, 79
 - in fraud case, 299
 - at pretrial hearings, 281
 - at pretrial motions, 278, 279, 280
 - response report for, 290–291
 - rests, 302
 - rules of evidence for, 27
 - search of, 43
 - stipulation by, 297
 - testifying for, 300–301
 - theory for, 75
 - degree programs, 316–317
 - deleted files, 126, 185–186, 197–199, 333
 - deliverables, 296–297
 - demonstrative evidence, 333
 - Department of Justice (DOJ), 78, 88, 303
 - depositions, 124, 280, 281–286, 333
 - destination address, 154, 157, 158, 160, 161–162, 334
 - Device Seizure, 233, 236, 326–327
 - DFRW (Digital Forensics Research Workshop), 127
 - DHCP (dynamic host configuration protocol), 258
 - dictionary attack, 143, 334
 - digging for information, 88–89
 - Digital Forensics Research Workshop (DFRW), 127
 - Digital Intelligence, 327, 329
 - digital video recorder (DVR), 266–267
 - direct attached storage (DAS), 252
 - direct evidence, 23, 334
 - direct examination, 302
 - directory structure, 334
 - discovery, 26, 334. *See also* e-discovery
 - discovery request, 31–34, 35, 334
 - disk duplicator, 102, 334
 - disk partition, 20–21, 178, 334
 - dismiss, motion to, 279
 - divorce cases, 78, 88, 156–157
 - DIYs (do-it-yourselfers), 78, 288, 334
 - DNA analysis, 57, 64
 - DNS (domain name server), 158, 244, 258, 334
 - document, 334
 - document forensics
 - CAM time stamps in, 207–208
 - finding documents for, 209–214
 - metadata in, 201–206
 - documenting/documentation, 117, 280, 281, 330. *See also* crime scene, documenting
 - do-it-yourselfers (DIYs), 78, 288, 334
 - DOJ (Department of Justice), 78, 88, 303
 - domain name server (DNS), 158, 334
 - domain name system (DNS), 244, 258
 - DOS (Microsoft Disk Operating System), 140, 179, 275
 - driver, 334
 - duplicate files, 144–145
 - DVR (digital video recorder), 266–267
 - dynamic host configuration protocol (DHCP), 258
- E •
- .e01, 331
 - Eades, Simon, 174
 - e-alibi, 1
 - Economic Crime Institute (ECI), 316
 - ECPA (Electronic Communications Privacy Act), 157
 - e-discovery. *See also* search warrant
 - authorization for, 40, 42, 50–54
 - complexity/problems of, 30–31
 - cost of, 26, 31, 35–37
 - deadlines for, 29–30
 - defined, 1, 335
 - in good faith, 34–35
 - in pretrial hearings, 281
 - in pretrial motions, 278
 - request for, 31–34
 - rules of evidence on, 26–27, 28
 - steps of, 29
 - team for, 40–41

- e-evidence. *See also* admissible evidence;
 rules of evidence
 analyzing, 199–200
 assessing strength of, 80
 from automobiles, 268–270
 circumstantial, 22, 27, 299
 defined, 335
 digging for, 88–89
 examining. *See also* querying
 as art, 117
 challenges in, 119–122
 challenging findings from, 128–130
 environments for, 121–122
 no-evidence result of, 130–131
 report for, 131–133
 steps of, 118–119
 time allotment for, 119
 gathering, properly, 21
 hiding. *See* hiding/hidden data
 from home security systems, 267
 from identification transmitters, 270–271
 imperfect, 288
 from instant messages, 173–174
 integrity of, 89–90
 interpreting, 81–82
 invisible, 15. *See also* hiding/hidden data
 manufactured, 14, 128, 129
 from mobile devices. *See* mobile devices
 Occam's razor for, 59
 overview, 2–3, 4
 permission to inspect, 84–85
 permission to obtain, 20
 persuasive presentation of, 304–308
 preservation of. *See* preservation
 in pretrial depositions, 282
 in pretrial hearings, 280–281
 in pretrial motions, 278, 280
 prevalence of, 2, 15
 storage places of, 10
 strategies for searching, 21
 tainted, 13–14, 56, 78, 110, 115, 288
 tampering with, 34, 76
 three-C process for, 56
 trial disputes over, 298
 uncompromised, 21–22
 understanding, 23, 28
 visible, 15
 vulnerability of, 23
 weight of, 23, 288
- EFS (Encrypting File System), 142, 181
- EIDE hard drive, 105–109
- Electronic Communications Privacy Act (ECPA), 157
- electronically stored information (ESI), 26–27, 29–34, 35, 335
- e-mail
 accessing, 153, 160
 admissibility of, 27, 156, 163, 299
 analyzing, 155, 156
 attachments to, 163
 authenticity of, 56
 in caches, 168
 candidness of, 155
 carbon copies of, 78, 163
 characteristics of, 13
 copying, 166–167
 defined, 335
 in divorce cases, 156–157
 e-discovery of, 29, 30
 extracting, from client, 163–167
 extracting, from Web, 168–169
 file extensions of, 164–165
 forwarding, 160, 163
 framing attempts with, 157, 174, 299
 header of, 160–162
 investigator organization of, 86
 on mobile devices, 221, 222
 for MySpace, 89
 network protocols for, 259
 in pre-investigation preparation, 91
 preservation of, 12
 prevalence of, 12, 154
 printing, 167
 privacy delusion about, 162
 protocols of, 158–159
 in querying process, 123
 Registry tracks, 194
 responses to, 163
 route of, 154
 searching/seizing, 51
 systems of, 157
 in tax fraud case, 13
 transfer process of, 159
 unique ID of, 162
 Web-based, 167–173
 weight of, 155
- e-mail virus, 12
- EnCase
 for answering machines, 266
 for Apple operating system, 183

- EnCase (*continued*)
- authentication via, 92
 - defined, 326
 - for deleted files, 197–198
 - for e-mail, 165, 167, 168, 169
 - for finding documents, 209
 - for Internet history, 173
 - for link files, 81–82
 - for networks, 263
 - for operating system bypass, 102
 - for Outlook files, 164
 - search filtering with, 196
 - for video files, 267
- EnCase Certified Examiner (EnCE), 315
- Encrypting File System (EFS), 142, 181
- encryption
- in child porn case, 149
 - compression compared with, 137
 - deciphering, 143, 144, 149–150
 - defined, 335
 - effectiveness of, 192, 197, 199
 - function of, 136, 137
 - methods of, two, 138–139
 - in network forensics, 247
 - on NTFS system, 181
 - software for, 146
- Enron Corporation, 163
- Ericsson, 226
- ESI (electronically stored information), 26–27, 29–34, 35, 335
- Esquire, 206
- Ethernet, 245
- Eudora, 164
- evidence. *See also* admissible evidence;
- e-evidence
 - circumstantial, 22, 27, 299, 332
 - defined, 26
 - destruction of, 35, 342, 343
 - direct, 23, 334
 - exculpatory, 280, 288, 335
 - hearsay, 27, 299, 337
 - preponderance of, 341
 - evidence law, 335. *See also* rules of evidence
- Excel, Microsoft, 76, 212, 308
- exceptions to the rules, 24, 335
- exclusions to the rules, 24, 28, 335
- exculpatory evidence, 280, 288, 335
- exhibits, courtroom, 305–306
- extended partition, 335
- extensions, file, 139–140, 164–165, 210–211
- extortion by e-discovery, 26, 335
- extracting data. *See* retrieving/extracting (data)
- eye contact, 307, 323
- E-ZPass, 18

• F •

- Facciola, John M., 27
- Facebook, 89, 335
- Faraday bag, 234–235, 236
- FAT (File Allocation Table), 10, 11, 179–180, 182, 273, 336
- Federal Bureau of Investigation (FBI), 2, 20, 45
- Federal Rules of Civil Procedure, 26–27, 29, 34, 336
- Federal Rules of Criminal Procedure, 26, 85, 336
- Federal Rules of Evidence, 26, 83, 299, 336
- Fifth Amendment, 149
- File Allocation Table (FAT), 10, 11, 179–180, 182, 273, 336
- file slack, 11, 180, 189–191, 336, 342
- file transfer protocol (FTP), 244, 259
- firewalls, 248–249, 260
- fixed storage device, 97, 336
- flash drives, 97, 103
- floppy disks, 97, 179, 217
- Ford Motor Company, 271
- forensic copy, 91, 336
- Forensic Examination of Digital Evidence: A Guide to Law Enforcement*, 78
- forensic process, 90–93. *See also* acquisition (process); authentication; preservation; reports
- Forensic Recovery of Evidence Device (FRED), 327
- Forensic Talon, 102
- Forensic ToolKit (FTK), 326
- for answering machines, 266
 - for Apple operating system, 183
 - authentication via, 92
 - for deleted files, 197–198
 - for e-mail, 165, 167, 168, 169
 - for finding documents, 209
 - for Internet history, 173
 - for link files, 81–82
 - for operating system bypass, 102
 - for Outlook files, 164
 - vendor for, 313

forensic tools, 336. *See also* tools/toolkit, forensic
 Forensic Ultradock, 102, 344
 Fourth Amendment, 39, 48
 fraud, 13, 74, 124, 163, 169, 299
 FRED (Forensic Recovery of Evidence Device), 327
 friendly environment, 122
Frye v. United States, 83
 FTK. *See* Forensic ToolKit (FTK)
 FTK Imager. *See* Forensic ToolKit (FTK)
 FTP (file transfer protocol), 244, 259
 Fuhrman, Mark, 75

• G •

Gammick, Richard, 156
 Gargoyle, 145
 GB (gigabyte), 101, 219, 273, 336
 GCFAs (GIAC Certified Forensic Analysts), 316
General Electric Co. v. Joiner, 84
 General Motors (GM), 271
 GIAC Certified Forensic Analysts (GCFAs), 316
 GIF (Graphic Image File), 211, 336
 gigabyte (GB), 101, 219, 273, 336
 global positioning systems (GPS), 13, 268–270
 Global System for Mobile Communication (GSM), 226, 233
 GM (General Motors), 271
 Gmail, 18, 154
 GMT (Greenwich Mean Time), 253
 good faith, 34–35
 Google, 17, 18, 87, 120, 153, 167
 GPS (global positioning systems), 13, 268–270
 Graphic Image File (GIF), 211, 336
 graphical user interfaces (GUI), 163, 167, 182, 246
 Greenwich, England, 208
 Greenwich Mean Time (GMT), 253
 GSM (Global System for Mobile Communication), 226, 233
 GUI (graphical user interfaces), 163, 167, 182, 246
 Guidance Software, 263, 315, 326

• H •

hard drive
 acquiring evidence from, 101–102
 anatomy of, 176–177
 e-mail storage on, 160
 as fixed storage device, 97
 imaging, 10, 105–109
 metadata on, 202
 saving files on, 10
 size of, 177
 speed of, 77
 write blocker for, 103
 hash (values)/hashing
 authentication via, 61, 92, 114–115
 for crime scene documentation, 61, 62
 during data transfer, 108, 109
 defined, 336–337
 for duplicating duplicate, 116
 for evidence integrity, 224
 for headers, 212
 libraries for, 212
 Paraben tools for, 233
 of passwords, 143, 146
 of stego software, 144
 header, file, 140, 190, 191, 210–211, 212, 336, 337
 hearings, pretrial, 280–281
 hearsay, 27, 299, 337
 Herndon, Douglas, 156
 hex editor, 102, 140, 148, 191, 192, 193, 337
 HFS (Hierarchical File System), 183–184, 337
 hidden files, 16, 140, 144, 181, 337
 hidden shares, 140, 337
 hiding/hidden data, 135. *See also* encryption; steganography
 in alternate data streams, 331
 in Bad Block Inode, 185
 detecting, 136–137, 144–145
 in non-accessible space, 192
 tactics for, 137–141, 210, 212
 tools for, 142
 Hierarchical File System (HFS), 183–184, 337
 hive, 337
 home security systems, 267–268
 Honda, MVEDR in, 271
 host, 243, 337
 hostile environment, 121
 hot files, 33–34

Hotmail, 167, 169
 HTTP (HyperText Transfer Protocol), 244, 259
 hubs, 243, 259
 human nature, 19, 45, 57, 75, 306, 337
 Hyman, Bruce, 174
 HyperText Transfer Protocol (HTTP), 244, 259

• 1 •

IACIS (International Association of Computer Investigative Specialists), 314
 ICMP (Internet control message protocol), 258
 IDEN (Integrated Digital Enhanced Network), 226
 identification transmitters, 270–271
 IDS (intrusion detection system), 249, 338
 IIC (investigator in charge), 41, 55, 68
 IM (instant messaging), 89, 173–174, 222
 images/imaging
 courtroom terminology of, 305
 defined, 10, 334, 338
 in the field, 105–108
 GPS receiver, 269
 methods for, 92
 from network, 242, 246
 by prosecutor, 79
 searching, 92
 SIM card, 235–236
 time allocation for, 77
 video equipment, 266
 IMAP (Internet Message Access Protocol), 158–159, 164, 168, 259, 338
 index.dat file, 172–173, 338
 indirect evidence, 22, 27, 239, 332
 inferences, 119
 infrared technology, 219, 221, 228, 234, 236, 338
 InsideOut Forensics, 233
 instant messaging (IM), 89, 173–174, 222
 intake form, 59, 78, 338
 Integrated Digital Enhanced Network (IDEN), 226
 intelligence, 87–89
 Internal Revenue Service (IRS), 13
 International Association of Computer Investigative Specialists (IACIS), 314
International Journal of Digital Evidence, 316
 International Society of Forensic Computer Examiners (ISFCE), 314

International Telecommunications Union (ITU), 253
 Internet
 cached files on, 187
 data gathering on, 18
 logs from, 18–19
 for mobile phone information, 227
 on mobile phones, 228
 network devices and, 98
 networks on, 17, 88–89, 214
 in pre-investigation preparation, 91
 Registry tracks, 194
 search engines on, 17–18, 87–88
 security options for, 88
 technological evolution from, 10
 text messages from, 17
 video-sharing sites on, 18, 89, 287
 Internet control message protocol (ICMP), 258
 Internet Explorer, 170, 172, 338
 Internet history, 120, 170, 172–173
 Internet Message Access Protocol (IMAP), 158–159, 164, 168, 259, 338
 Internet Protocol (IP) address
 defined, 66, 338
 devices having, 243
 of e-mail destination, 154, 158
 of e-mail sender, 154, 160, 162
 format of, 17
 from logs, 19
 in murder case, 66
 network protocols and, 258, 259
 router uses, 242
 from search engines, 17
 Internet protocol security (IPSec), 258
 Internet service provider (ISP), 12, 17, 153, 157
 Internet World Stats, 154
 interpretation, 119
 interrogatory question, 338
 interview, 118
 intrusion detection system (IDS), 249, 338
 intrusion prevention system (IPS), 249, 338
 investigative report, 60
 investigator, forensic
 active role by, 80–81
 case potential of, 79–82
 certification of, 313–317, 323, 326
 credentials of, 83–84
 integrity of, 298
 intelligence gathering by, 87–89
 organizing work by, 86–87

payment for, 308, 309, 321
 as reliable witness, 82–84
 responding to opposing experts by, 289–294
 timing work by, 77–78
 investigator in charge (IC), 41, 55, 68
 IP address. *See* Internet Protocol address
 iPods, 13, 97, 231
 IPS (intrusion prevention system), 249, 338
 IPsec (Internet protocol security), 258
 IRS (Internal Revenue Service), 13
 iScrub, 206
 ISFCE (International Society of Forensic
 Computer Examiners), 314
 ISP (Internet service provider), 12, 17, 153, 157
 items, case, 290
 ITU (International Telecommunications
 Union), 253

• J •

John the Ripper, 147
 Joint Photographic Experts Group (JPG), 338
Journal of Digital Forensics, Security and Law, 316
 journaling, 181
 J.P. Morgan Chase & Co., 163
 JPG (Joint Photographic Experts Group), 338
 JPHS for Windows, 144

• K •

Kansas City Regional Computer Forensics
 Lab, 66
 keystroke logger, 143, 148, 150, 157, 338
 Kismet, 262–263
Kumho Tire v. Carmichael, 83

• L •

laboratories, forensic, 328–330
Law and Order, 16
 layers, 141
 Layton, Donald, 163
 least significant bits (LSBs), 144
 legal sufficiency, 338
 Legion V2.1, 140

letter of agreement, 78
 LexisNexis, 88
 licensing bureaus, 42
 link file, 81–82, 213–214, 339
 Linux, 102, 175, 184–185, 193, 339
 Locard's principle, 306
 log files
 in child porn cases, 85
 defined, 339
 e-mail, 164
 for home security systems, 267
 on mobile phones, 222
 on network, 250
 revision, 205, 206
 router, 248
 as visible file, 15
 Web server, 18–19
 logical level search, 339
 logical volume, 178
 Logicube, 162, 233, 328
 log-in verification, 130
 loopholes, legal, 73
 avoiding, 75–76, 84–93, 119
 conflict of interest as, 79
 during cross-examination, 21
 in opposition's report, 81
 overview, 4
 prosecutor detects, 41
 trial disputes over, 297–298
 LSBs (least significant bits), 144
 LSoft Technologies Hard Drive Eraser, 104

• M •

MAC (Media Access Control), 243, 245, 249, 258
 Mac OS X, 183
 Macintosh HFS system, 141
 Mack, Darren, 156
 Macs, 63
 magnetic disk drive, 176, 339
 magnets, 64, 69
 malware, 85, 127, 129
 MAPI (Messaging Application Programming
 Interface), 159, 339
 master boot record (MBR), 178, 339
 Master File Table (MFT), 182
 MB (megabyte), 179, 219, 339
 MBR (master boot record), 178, 339

- McDonald's coffee lawsuit, 75
- MD5 (Message-Digest algorithm 5), 92, 114, 233, 331, 339
- Media Access Control (MAC), 243, 245, 249, 258
- media, network, 243
- media, sterile, 104
- megabyte (MB), 179, 219, 339
- Melissa e-mail virus, 12
- memory card, 100, 339
- memory storage area, 98, 339
- Mercedes-Benz, MVEDR in, 271
- Message-Digest algorithm 5 (MD5), 92, 114, 233, 331, 339
- Messaging Application Programming Interface (MAPI), 159, 339
- metadata
 - cleaning, 203
 - defined, 201, 340
 - in deleted file, 197, 198
 - in document forensics, 202–206
 - e-discovery of, 30
 - for file types, 201
 - information in, 15–16
 - on NTFS system, 181
 - in plagiary case, 205
 - in pre-investigation preparation, 91
 - prevalence of, 15
 - in unallocated space, 188
- Metadata Analyzer, 206
- Metasploit project, 208
- MFT (Master File Table), 182
- Microsoft, 29, 159, 175, 203, 340. *See also specific applications*; Windows, Microsoft
- Microsoft Disk Operating System (DOS), 140, 179, 273
- Microsoft Network (MSN), 120
- Mikus, Nick, 127
- Mills, Dave, 253
- mirror image, 92
- MMC flash cards, 100
- mobile cards, 226
- mobile devices. *See also* mobile phones
 - acquisition types for, 232
 - audio, 13, 97, 231
 - computers compared with, 220
 - defined, 219
 - digital cameras, 230–231
 - evidence integrity for, 224
 - evolution of, 219, 220, 221–222, 224
 - external media for, 223
 - forensic tools for, 232–234, 326–327
 - instant messaging with, 174
 - isolating, 66, 234–235, 236
 - non-forensic software for, 232
 - personal digital assistants (PDAs), 230
 - power of, keeping on, 66
 - standard technology for, 223
 - types of evidence on, 222–223
 - writing to, 224
- mobile phones
 - acquiring evidence from, 98
 - characteristics of, 228–229
 - checksums from, 115
 - components of, 225–226
 - at crime scene, 66
 - data preservation by, 12
 - evidence on, 16, 222, 223
 - forensic procedure for, 236–239
 - forensic tools for, 19, 232–233
 - identification transmitters on, 271
 - identifying type of, 227
 - network systems of, 226–227
 - privacy delusion with, 13
 - SIM card of, 229–230
 - storage space loss in, 103
 - wireless connectivity for, 220–221
- Montgomery, Lisa, 66
- Morgan Stanley, 34
- motion in limine*, 278, 279, 340
- motions, pretrial, 278–280, 340
- Motor Vehicle Event Data Recorder (MVEDR), 271, 340
- Motorola, 226
- mount points, 182
- Mozilla, 173
- MP3 players, 97, 231
- MSN (Microsoft Network), 120
- MVEDR (Motor Vehicle Event Data Recorder), 271, 340
- My Documents folder, 208, 210
- MySpace, 89

• N •

NAS (network attached storage) system, 251–252

National Highway Traffic Safety Administration (NHTSA), 271

National Institute of Justice Journal, 316

National Institute of Standards and Technology (NIST), 105, 235

National Science Foundation (NSF), 299

National Security Agency (NSA), 114

National Software Reference Library (NSRL), 212

negligence cases, 78

NetIntercept, 263

network attached storage (NAS) system, 251–252

network cable, 110

network devices, 98

network interface card (NIC), 243, 261–262, 340

Network Time Protocol (NTP), 253, 259

networks

- client/server system of, 245
- command-and-control server of, 246–247
- components of, 242–243
- data selection from, 248
- data sequence from, 256–257
- data sources on, 248–250
- data streams on, 258–259
- external, 214
- forensic challenge of, 241
- forensic component for, 242
- forensic framework of, 245–247
- forensic tools for, 241, 242, 253–263
- metadata on, 202
- OSI model of, 244–245
- protocols on, 258–259
- static technology for, 242
- storing extracted data from, 250–252
- time stamps on, 253–256

neutral environment, 122

New Technology File System (NTFS), 180–182, 273, 340

NHTSA (National Highway Traffic Safety Administration), 271

NIC (network interface card), 243, 261–262, 340

Niksun, 263

NIST (National Institute of Standards and Technology), 105, 235

Nokia, 226

non-supportive environment, 122

NSA (National Security Agency), 114

NSF (National Science Foundation), 299

NSRL (National Software Reference Library), 212

NTP (Network Time Protocol), 253, 259

• O •

O'Brien, Thomas P., 303

observed evidence, 119

Occam's razor, 59

officers of the court, 54

OnStar, 271

Open Systems Interconnection Model (OSI), 242, 244–245

Opera, 173

operating system (OS). *See also* computer operating system

- defined, 310
- for home security systems, 267
- of mobile devices, 220, 227, 228, 232, 236, 237
- write blockers for, 329

OSI (Open Systems Interconnection Model), 242, 244–245

Outlook Export, 165

Outlook Express, 164

Outlook Extract Pro, 165

Outlook, Microsoft, 159, 164, 194

Oxygen Forensic Suite 2, 233

• P •

packets, 256–257

packet-switched networks, 154

paggers, 66

Paraben

- Device Seizure product, 326–327
- ease of using, 197
- isolation tool by, 329
- for mobile devices, 233, 236–239
- for networks, 263
- for operating systems, 102
- for Registry, 194
- for search filtering, 196
- training by, 315

parallel cable, 110

- partition, 178, 340
 - passphrase, 146, 149
 - Password Recovery Toolkit (PRTK), 313
 - passwords
 - in cache, 144, 147
 - circumventing, 148
 - for compressed file, 137
 - cracking, 19, 91, 142–144, 146–147
 - fail-safe for, 150
 - as non-verification, 130
 - overview, 4
 - in pre-investigation preparation, 91
 - in Registry, 194
 - patent infringement, 28
 - payload, 150, 154, 247, 340
 - PDAs (personal digital assistants), 13, 66, 98, 115, 230, 232
 - performance reports, 75
 - perjury, 302–303, 320, 340
 - personal digital assistants (PDAs), 13, 66, 98, 115, 230, 232
 - petabyte (PT), 273, 340
 - PGP (Pretty Good Privacy), 146, 149, 150, 340
 - Philip Morris, 33
 - phone company, 12
 - physical-level search, 340
 - PIN Unblocking Key (PUK), 230
 - plaintiff/prosecutor
 - burden of proof on, 81, 295
 - case rested by, 301
 - case theory and, 75
 - cost to, 287
 - cross-examination by, 302
 - defined, 341
 - direct examination by, 300
 - evidence provided by, 79–80
 - imaging by, 79
 - lawyer's advice to, 77
 - pretrial motions by, 278
 - redirect examination by, 301
 - in response report, 290, 291
 - search-and-seizure role by, 41, 48
 - during testimony, 300, 301, 302
 - Torkelson's testimony for, 302
 - Pointstone, 141
 - poison, 120
 - POP (Post Office Protocol), 158, 164, 168, 341
 - POP3 (Post Office Protocol version 3), 259
 - port mirroring/spanning, 261
 - portable storage devices, 97, 341
 - Post Office Protocol (POP), 158, 164, 168, 341
 - Post Office Protocol version 3 (POP3), 259
 - Powell, Colin, 205
 - prepays, 163
 - preponderance of the evidence, 341
 - preservation
 - by copying files, 92
 - at crime scene, 67
 - defined, 341
 - of deleted information, 10–12
 - during e-discovery, 33
 - as forensic process, 89
 - imaging methods for, 92
 - for integrity of evidence, 89
 - by search and seizure, 51
 - via backups, 12
 - preservation order, 33
 - pretrial, 277–286, 341
 - Pretty Good Privacy (PGP), 146, 149, 150, 340
 - principles, 77
 - printer, network, 249
 - privacy policies, 51
 - privilege, 27, 30, 31, 33, 341
 - probable cause, 39, 45, 50, 341
 - probative value, 28, 341
 - Properties dialog box, 203–204
 - prosecutor. *See* plaintiff/prosecutor
 - PRTK (Password Recovery Toolkit), 313
 - PT (petabyte), 273, 340
 - PUK (PIN Unblocking Key), 230
 - Purdue University Cyber Forensics Lab, 316
- *Q* •
- Qualcomm, 28, 226
 - querying
 - overview, 122–123
 - search list for, 123–127
 - software for, 124–126, 127
 - via data sampling, 128
- *R* •
- Rader, Dennis, 206
 - radio frequency identification (RFID), 270–271, 342
 - Radio Shack, 330

- rainbow table, 143, 341
- RAM (Random Access Memory), 65, 98, 168, 170, 192–193, 225, 235, 341
- RCFL (regional computer forensic lab), 79, 88, 298, 341
- Read Only Memory (ROM), 225
- reasonable explanation, 283
- recording equipment, 330
- recross, 301, 302
- Recycle Bin, 182, 186
- redirect examination, 301, 302
- referring URL, 19
- refrigerators, 273
- regional computer forensic lab (RCFL), 79, 88, 298, 341
- Registry, 194, 337, 341
- Registry Analyzer, 194
- Registry Editor, 113
- Registry Viewer, 313
- Rehnquist, William H., 84
- remote procedure calls (RPC), 244
- reports
 - on examination findings, 131–133
 - for extraction process, 198
 - guidelines for, 93
 - introduction of, 82
 - for testimony, 289–294, 322
- research journals, 316
- résumé, 79
- retrieving/extracting (data). *See also* acquisition (process); images/imaging
 - cached files, 187
 - from copiers, 272–273
 - deleted files, 186, 197–199
 - ease of, 196–197
 - from file slack areas, 189–191
 - from identification transmitters, 271
 - metadata, 206
 - from networks, 246, 247–250, 259–260
 - from RAM, 193
 - from Registry, 194
 - from SIM card, 235–236
 - from unallocated space, 188–189
 - from video equipment, 267
- revision log, 205, 206
- RFID (radio frequency identification), 270–271, 342
- Rochester Institute of Technology (RIT), 316
- ROM (Read Only Memory), 225
- Rose, Thomas, 157
- routers, 98, 154, 242, 248, 260, 261, 342
- RPC (remote procedure calls), 244
- Rule 16 pretrial conference, 29, 85, 124, 342
- Rule 26, 29, 342
- Rule 34, 342
- Rule 702, 83, 342
- rules of evidence
 - defined, 342
 - on discovery, 26–27, 34–35
 - on exclusions/exceptions, 24, 25, 27–28
 - named, 26–27
 - in pretrial motions, 278
 - on relevancy, 24–25, 26–28
 - for search and seizure, 39, 40–41, 42, 50–54, 281. *See also* search warrant
- S •
- safe harbor rule, 35
- SAN (storage area networks), 250–251
- Sandstorm, 263
- SANS' information Security Reading Room, 316
- Sarbanes-Oxley Act, 250
- Scheindlin, Shira A., 36
- scientific method, 58–59, 118
- scope of work, 78
- SD cards, 223, 226
- search and seizure, 39, 40–41, 42, 50–54, 281. *See also* search warrant
- search engines, 17–18, 87–88. *See also* querying
- search filtering, 195–196
- search options, 125
- search warrant
 - for civil cases, 50, 51
 - drafting affidavit for, 45–48
 - for e-mail access, 153
 - exceptions to, 39, 42, 43
 - judge approves, 39, 42
 - obtaining, 43–45
 - presenting affidavit for, 48–50
 - as required, 20
- searching images. *See* querying
- SEC (Securities and Exchange Commission), 2
- SEC v J.P. Morgan Chase & Co.*, 163
- sector, 92, 177, 178, 342
- Secure Hash Algorithm (SHA), 114, 342
- Secure shell (SSH), 259
- Securities and Exchange Commission (SEC), 2

- self-destruct mechanism, 150
 - sensor, 245, 246
 - serial number, 12, 227
 - service set identifier (SSID), 194
 - SHA (Secure Hash Algorithm), 114, 342
 - shadow copy, 182
 - Show Hidden Files and Folders option, 140
 - Siddiqui, Mohamed, 299
 - SIM (Subscriber Identity Module) card, 222, 226, 229–230, 232–233, 234, 235–236, 342
 - SIMCon, 233
 - SIMIS, 233
 - Simple Mail Transfer Protocol (SMTP), 158, 164, 168, 259, 343
 - Simpson, O. J., 75
 - slack space, 11, 180, 189–191, 336, 342
 - Slashdot.org, 120
 - sleuthing, 143
 - Small Scale Digital Device Forensics Journal*, 316
 - smart phones, 230, 236–239
 - Smith, David L., 12
 - Smith, Richard M., 205
 - SMTP (Simple Mail Transfer Protocol), 158, 164, 168, 259, 343
 - snooper software, 143, 148, 343
 - social networks, 17, 18, 30, 88–89, 91, 335
 - software, forensic. *See also* EnCase; Forensic ToolKit (FTK); Paraben
 - for cached files, 187
 - for compressed files, 137
 - for copiers, 272–273
 - for decryption, 150
 - for deleted files, 126, 186
 - for duplicating duplicate files, 116
 - ease of using, 196–197
 - for e-mail, 160, 164
 - for extension-header match, 211
 - hard drive conversion with, 10
 - hash values and, 115
 - for Info2 files, 182
 - for link files, 213
 - for metadata, 206
 - necessity of using, 13
 - password-cracking, 91, 137, 143, 147
 - purpose of, 224, 232
 - for querying, 122, 124–126, 127
 - for Registry, 194
 - for search filtering, 196
 - for SIM cards, 235–236
 - for slack space, 11
 - for steganography, 145
 - for tape backups, 217
 - for Web-based evidence, 174
 - wiping, 104–105, 330, 344
 - solid-state drive (SSD), 97, 98
 - source address, 154, 343
 - spoilation, 35, 154
 - spoofing e-mail, 160–161
 - Sprint, 226
 - spyware, 288
 - SSD (solid-state drive), 97, 98
 - SSH (Secure shell), 259
 - SSID (service set identifier), 194
 - stealth mode, 121, 247
 - steganography
 - defined, 343
 - detecting, 136–137, 139, 142, 144–145
 - effectiveness of, 199
 - prevalence of, 197
 - technique of, 142
 - Stinnett, Bobbie Jo, 66
 - stipulation, 297
 - storage area networks (SAN), 250–251
 - storage server, 247
 - subpoena, 17, 52–54, 89, 153, 169, 343
 - subpoena ad testificandum*, 53, 343
 - subpoena duces tecum*, 54, 343
 - subscriber identifier, 222, 343
 - Subscriber Identity Module (SIM) card, 222, 226, 229–230, 232–233, 234, 235–236, 342
 - Supreme Court, U.S., 82, 83, 280
 - suspect profile, 17
 - swap file, 168, 171, 343
 - switches, 98, 243, 249, 259, 261, 343
 - system level utilities, 102
- 7 •
- TAPs (test access ports), 259–260
 - tax fraud, 13
 - TB (terabyte), 179, 195, 216, 241, 273, 344
 - temporary files, 14, 168, 170–172, 343
 - terabyte (TB), 179, 195, 216, 241, 273, 344
 - terms, 125
 - test access ports (TAPs), 259–260
 - testimony
 - billing questioned in, 308, 321
 - counsel's tricks during, 320–321

credentials and, 323–324
 cross-examination, 21, 298, 300–301, 302, 322
 direct examination, 300, 302
 dressing for, 323
 eye contact during, 307, 323
 investigator qualifications during, 307–308
 irrefutability of, 321
 jurors instructed on expert, 303
 mistakes during, 21
 nonverbal communication in, 322
 persuasive, 304–308
 preparation for, 22
 redirect examination, 301, 302
 report for, 289–294, 322
 truthfulness of, 302–303, 320
 text messages, 12, 16, 17, 78, 89, 222
 theory, case, 75–76
 Thunderbird, 164
 time stamps, 203, 207–208, 253–256, 257
 T-Mobile, 226
 Token Ring, 245
 Tomlinson, Ray, 154, 158
 tools/toolkit, forensic. *See also* software,
 forensic; write blocker
 choosing, 20–21
 at crime scene, 63–64
 for digital cameras, 231
 for discovery requests, 32, 33
 error rate of, 84
 hardware, 327–328
 for hidden data, 136, 142
 for imaging, 92, 102
 for mobile cards, 226
 for mobile devices, 224, 228, 232–234
 for networks, 241, 242, 245–247, 259–263
 power of, 19
 report function of, 60
 testing, 224, 225, 226
 as time-savers, 325
 for transferring data, 105–112
 verifying, 93
 Torkelsen, John B., 302–303
 Toyota, MVEDR in, 271
 trials. *See also* testimony
 acquittal at, 301
 conclusion of, 302
 deliverables at, 296–297
 disputes at, 297–298
 exhibits at, 305–306
 pretrial phase of, 277–286, 341

scheduling, 297
 testimony at, 298, 300–303
 triers of fact, 344
 Trojan software, 143

• U •

UCF (University of Central Florida), 316
 unallocated space, 180, 186, 188–189, 344
 unique ID, 162
 United Nations, 205
United States v. O'Keefe, 27
United States v. Siddiqui, 299
 University of Central Florida (UCF), 316
 Unix, 184–185, 193, 339
 USB port, 113, 226, 231, 236, 266
 UTC (Coordinated Universal Time), 253–256
 Utica College, 316

• V •

VereSoft, 174
 Verizon, 226
 VicodinES, 12
 video recorders, 230, 266–267, 330
 VideoEgg, 89
 video-sharing sites, 89
 virtual local area network (VLAN), 249
 virtual memory, 171, 344
 virus, e-mail, 12
 Visual Basic, 202
 Visual Basic objects, 206
 VLAN (virtual local area network), 249
 volume, 183, 344
 Volvo, MVEDR in, 271

• W •

Wall Street Journal, The, 75
 WAP (Wireless access point), 98, 249
 weakest link, 150, 344
 WebCase, 174
 Westlaw, 88
 White Canyon's Wipe Drive 5, 104
 WiebeTech, 102, 327–328, 329, 344
 WiFi network, 214, 228, 234

- Windows 95, 179
 - Windows Explorer, 141, 166, 167, 331, 338
 - Windows, Microsoft
 - data organization on, 178
 - file systems of, 179–182
 - hard drive accessibility on, 101
 - Registry of, 194, 341
 - virtual memory settings in, 171
 - Windows NT, 141, 180–182
 - Windows Vista, 113, 140, 181
 - Windows XP, 113, 140
 - WinHex, 65, 148, 193
 - wiping software, 104–105, 330, 344
 - Wireless access point (WAP), 98, 249
 - wireless connectivity
 - device isolation from, 329
 - Faraday bag prevents, 234
 - finding documents having, 214
 - isolating device from, 234, 235
 - for mobile devices, 219, 220–221
 - of mobile phones, 228
 - for network TAPs, 262–263
 - Registry tracks, 194
 - wireless devices, 64
 - Wireless Stronghold Box, 329
 - wiretapping, 288
 - witness, reliable, 82–84
 - Word document, 10, 15–16, 209, 210, 212
 - wrap-around cipher, 136
 - write blocker
 - defined, 344
 - at forensic lab, 329
 - function of, 103
 - physical/logical, 103
 - proper, having, 112
 - purpose of, 329
 - in transfer process, 105–106, 108, 109
 - write protection
 - defined, 344
 - for evidence integrity, 224
 - on tape backups, 216
 - tools for, 102
 - for USB port, 113, 226, 231, 236
 - wrongful termination cases, 14, 75, 76
- **Y** •
- Yahoo!, 17, 18, 87, 167, 169
 - YouTube, 18, 89, 287
- **Z** •
- ZA Technologies v. Microsoft*, 29
 - zeroed out, 11
 - Zubulake v. USB Warburg*, 36–37
 - Zulu time, 208, 253–256