

INDEX

The letter t following a page number denotes a table; the letter f following a page number denotes a figure.

Numbers

4Kn disks, 12, 41–44, 42*f*
512e sector emulation, 41, 42, 43

A

abstraction layers, disk interfaces, 34, 35*f*
AccessData. *See* ftkimager tool; FTK
SMART format
Ace Laboratory PC-3000 tool, 122
ACPO (Association of Chief Police
Officers), UK, 2, 6–7
acquisition host
attaching subject disk to
Apple Target Disk Mode, 137–138
devices with block or character
access, 140
enabling access to hidden sectors,
118–125
examining subject PC hardware,
101–102
identifying subject drive, 105–107
NVME SSDs, 138–139
querying subject disk, 107–118
removable storage media, 132–136
viewing examiner workstation
hardware, 103–104
performance, optimizing, 88–90
acquisition process. *See* forensic
acquisition
ACS (ATA Command Set). *See* ATA
commands
Advanced Forensic Format. *See* AFF
Advanced Format 4Kn disks, 12,
41–44, 42*f*
Advanced Format 512e disks, 41, 42, 43
Advanced Host Controller Interface
(AHCI) mode, SATA, 23–24
Advanced Technology Attachment
commands. *See* ATA
commands

AFF (Advanced Forensic Format)
aff4imager tool, 190
affcat tool, 209–210
affconvert tool, 204–205, 209
affcrypto tool, 215
affinfo tool, 198, 210, 211
AFFlib software package
affuse tool, 196–197, 235
built-in compression, 190
built-in encryption, 215
overview, 62
piping, 209
signing and validating
signatures, 202
built-in compression, 190
built-in encryption, 215
converting raw images to, 204–205
converting to another format,
209–211
overview, 62–63
piping, 209
recalculating hash of forensic image,
198–199
AHCI (Advanced Host Controller
Interface), mode, SATA,
23–24
aimage tool, 190
Appelbaum, Jacob, 251
Apple
FileVault, 248–251
Target Disk Mode, 31, 137–138
Thunderbolt interface, 30–32, 31*f*, 137
array-info tool, 178
Association of Chief Police Officers
(ACPO), UK, 2, 6–7
ATA (Advanced Technology Attachment)
commands
common, 35*t*
DCO and HPA drive areas, 39–40
overview, 34–36
password-protected disks, 126–128
and SCSI, 39
security erase command, 226–227
SSD devices, 16–17
ATA Command Set (ACS). *See* ATA
commands

- ATAPI (ATA Packet Interface)
 - DCO and HPA drive areas, 39–40
 - overview, 35–36
 - password-protected disks, 126–128
 - SCSI commands, 39
- Atola Insight Forensic, 122
- auditd package, 76
- audit trail
 - overview, 70
 - shell history, 73–75
 - task management, 70–73
 - terminal monitors and Linux
 - auditing, 76
 - terminal recorders, 75–76
- aureport command, 76

B

- Bash (Bourne Again shell), 56, 73, 74, 82.
 - See also* command line
- Bash math expansion, 183, 248, 249, 252, 265, 274
- bdeinfo command, 248
- bdemount command, 248
- BDs. *See* Blu-ray discs; optical storage media
- Beginning of Media (BOM) marker,
 - on tapes, 176
- Beginning of Tape (BOT) marker,
 - on tapes, 176
- BitLocker, Microsoft, 243–248
- blkcat command, 274
- blkls command, 271–272
- blktp-utis tool, 241
- blockdev command, 43, 98, 99, 108
- block devices
 - acquiring, 172–173
 - attaching to acquisition host, 140
 - creating from raw image, 230
 - Linux, 50–55
 - making QCOW2 image available as, 237–239
- block-level encryption systems. *See*
 - encrypted filesystems,
 - accessing
- Blu-ray discs (BDs), 19*f*, 21–22. *See also*
 - optical storage media
 - acquiring, 174, 175
 - transferring forensic image to, 222, 223
- BOM (Beginning of Media) marker,
 - on tapes, 176
- bootable Linux CDs, 98, 99

- boot images, preparing with xmount, 235–237
- BOT (Beginning of Tape) marker,
 - on tapes, 176
- BOT (Bulk-Only Transport) USB
 - interface, 29, 40–41
- bottlenecks, performance, 88–90, 91*t*
- Bourne Again shell (Bash), 56, 73, 74, 82.
 - See also* command line
- Bulk-Only Transport (BOT) USB
 - interface, 29, 40–41
- burning forensic image to optical disc, 221–222
- bus speeds, 90, 91*t*. *See also* interfaces
- bzip tool, 188, 189

C

- CA (certificate authority) certificates, 156, 157, 201–202
- C.A.I.N.E. boot CD, 99
- card readers, 18
- Carrier, Brian, 48
- carving tools, 165
- cat command, 196, 199
- cciss-vol-status package, 178
- CDB (command descriptor block), 36
- cd-drive command, 132–133
- cd-info command, 133
- cdparanoia tool, 175
- CDs (compact discs). *See also* optical storage media
 - acquiring, 174, 175
 - Linux forensic boot, 98, 99
 - as storage media, 19*f*, 20–21
 - transferring forensic image to, 221–222
- certificate authority (CA) certificates, 156, 157, 201–202
- CF (CompactFlash) card, 18
- CFTT (Computer Forensic Tool Testing) project
 - dd utility tests, 60
 - forensic-imaging requirements, 9
 - HWB Device Specification, 94
 - overview, 3, 6
 - software write blockers, 99
- chip-off, 15, 125
- Choudary, Omar, 248
- CipherShed, 217
- client mode, rdd tool, 166, 167–168
- cloned disks, 219–221
- Coltel, Romain, 243
- command descriptor block (CDB), 36

- command line. *See also* Linux; *specific commands/tools*
 - audit trail, 70–76
 - command privileges, xxv, 212, 233
 - organizing output, 76–83
 - output
 - organizing, 76–83
 - redirecting, 81–83
 - scalable examination directory structure, 79–81
 - reasons to use, xx–xxi
 - saving output with redirection, 81–83
 - shell history, 73–75
 - task management, 70–73
 - terminal monitors and Linux auditing, 76
 - terminal recorders, 75–76
 - viewing examiner workstation hardware, 103–104
 - command sets
 - ATA, 34–36, 35*t*
 - NVME, 37–38, 37*t*
 - SCSI, 36–37, 37*t*, 39
 - compact discs. *See* CDs; optical storage media
 - CompactFlash (CF) card, 18
 - completeness, forensic, 10
 - completion times, estimating, 87–88
 - compression
 - AFFlib built-in, 190
 - combining with splitting, 192
 - EnCase EWF compressed format, 189
 - FTK SMART compressed format, 190
 - SquashFS, 66–67, 191
 - Computer Forensic Tool Testing project. *See* CFTT project
 - computer-related forensics. *See* digital forensics; forensic acquisition
 - converting between image formats, 202–211
 - conv=noerror parameter, dd utility, 143
 - copying forensic images, 87
 - Copy-on-Write (CoW) snapshots, live imaging with, 172
 - Coroner’s Toolkit, The, 2
 - Corsair Padlock2 thumb drive, 228
 - CoW (Copy-on-Write) snapshots, live imaging with, 172
 - cpqarrayd tool, 178
 - cryptology. *See also* encrypted filesystems, accessing; encryption
 - basic hashing, 151–152, 151*t*
 - hash windows, 143, 152–154, 199–200
 - key-wiping procedures, 227–228
 - RFC-3161 timestamping, 157–159
 - signing forensic images, 154–157
 - verifying forensic image integrity, 197–202
 - cryptsetup tool, 251–254, 257
 - CTRL-Z shortcut, 92–93, 123
 - curl command, 158
- ## D
- dares carver tool, 165
 - data CDs, 20. *See also* CDs; optical storage media
 - data disposal, 224–228
 - data extraction
 - manual, using offsets, 272–274
 - partition extraction, 264–271
 - partition scheme analysis, 259–264
 - slack space, 271–272
 - unallocated blocks, 272
 - data flow, optimizing, 90
 - data recovery tools, 61–62, 162–163
 - dc3dd tool
 - acquiring image to multiple destinations, 150
 - cryptographic hashing algorithms, 151–152, 151*t*
 - error handling, 160–161
 - forensic acquisition with, 142, 144–145
 - optical discs, imaging, 174–175
 - overview, 61
 - piecewise hashing, 153–154
 - splitting functionality, 193
 - SquashFS forensic evidence containers, 65, 149
 - wiping functionality, 225–226
 - writing image file to clone disk, 220–221
 - dcfldd tool
 - acquiring image to multiple destinations, 150
 - compressing images, 189
 - cryptographic hashing algorithms, 151, 151*t*
 - encryption during acquisition, 212
 - error handling, 160
 - forensic acquisition with, 142, 144–145
 - hash windows, 153
 - overview, 61
 - partition extraction, 266
 - splitting functionality, 192–193
 - tapes, extracting data from, 177

- DCO (Device Configuration Overlay)
 - extracting sector ranges belonging to, 269–271
 - overview, 39–40, 118
 - removing, 118–121
- dd_rescue tool, 61, 62, 142, 163, 215–216
- ddrescue tool, 61, 142, 162–163, 165
- dd utility
 - combining compressing and splitting, 192
 - cryptographic hashing algorithms, 152
 - forensic acquisition with, 142–144
 - forensic variants, 61, 144–145
 - manual extraction using offsets, 273–274
 - partition extraction, 266
 - raw images, 60
 - secure remote imaging, 168, 169–170
 - sparse files, 85
 - validating acquisition hash, 197–198
 - wiping functionality, 226
- debug ports, accessing storage media using, 122–125
- decryption. *See also* cryptography; encrypted filesystems, accessing; encryption
 - of GPG-encrypted image, 212, 213
 - of OpenSSL-encrypted file, 213–214
- DEFT (Digital Evidence & Forensics Toolkit), 98–99
- deleted partitions, extracting, 266–268
- deleting forensic image data, 224–228
- desktop environments, Linux, 56
- /dev directory, Linux, 50, 51–52
- Device Configuration Overlay. *See* DCO
- device mapper, 179–182, 231–232, 253, 255–256
- device tree, Linux, 50–51
- DFRWS (Digital Forensic Research Workshop), 2, 8, 59
- diagnostic ports, accessing storage media using, 122–125
- Diaz Diaz, Antonio, 61, 162
- diff tool, 200
- Digital Evidence & Forensics Toolkit (DEFT), 98–99
- digital evidence bags. *See* forensic file formats
- Digital Forensic Research Workshop (DFRWS), 2, 8, 59
- digital forensics. *See also* forensic acquisition
 - defined, 2
 - history of, 1–4
 - Linux and OSS in context of, 48–50
 - peer-reviewed research, 7–8
 - principles of, 6–10
 - standards for, 6–7
 - trends and challenges, 4–5
- Digital Investigation: The International Journal of Digital Forensics & Incident Response*, 7
- digital signatures, 154–157
- digital versatile discs. *See* DVDs; optical storage media
- directories
 - naming conventions for, 76–79
 - scalable examination structure, 79–81
- disk block recovery tools, 162–163
- disk cloning and duplication, 219–221
- disk coolers, 93
- disk imaging. *See* forensic acquisition
- disk partition scheme, analyzing, 259–264
- disks. *See* forensic acquisition; storage media; subject disk
- disktype tool, 260–261, 263
- dislocker package, 243–247
- dismounting VeraCrypt volume, 218. *See also* unmounting
- disposal, data, 224–228
- distributions, Linux, 55–56
- dm-crypt encryption, 251, 254
- dmesg tool, 206
- dmraid tool, 178–179
- dmsetup tool, 159–160, 179–180, 182, 183
- documenting device identification
 - details, 107–108
- DOS partition scheme, 262
- dpt-i2o-raidutils package, 178
- drive maintenance sectors, 40, 122–125
- drives. *See* forensic acquisition; *specific media*; storage media; subject disk
- Dulaunoy, Alexandre, 61
- duplication, disk, 219–221
- DVDs (digital versatile discs), 19f, 21. *See also* optical storage media
 - acquiring, 174, 175
 - overview, 21
 - reassembling split forensic images, 196
 - transferring forensic image to, 222
- dynamic disks, Microsoft, 181–182

E

EIDE (Enhanced Integrated Drive Electronics), 32

eject shell command, 133

Electronic Crime Scene Investigation: A Guide for First Responders (US DOJ), 3, 7

EnCase EWF

- built-in encryption, 215
- compressed format, 189
- converting AFF images to, 209–210
- converting FTK files to, 208
- converting raw images to, 202–203
- converting to another format, 205–208
- forensic acquisition, 145–146
- hash windows, 153
- image access tasks, 233–234
- overview, 62
- recalculating hash of forensic image, 198
- remote forensic acquisition, 171–172
- splitting images during acquisition, 193

encrypted filesystems, accessing

- Apple FileVault, 248–251
- Linux LUKS, 251–254
- Microsoft BitLocker, 243–248
- overview, 243
- TrueCrypt, 254–257
- VeraCrypt, 254–257

EncryptedRoot.plist.wipekey file, 249–250

encryption. *See also* cryptography;

- encrypted filesystems, accessing
- flash drives, 17, 131, 131*f*, 228
- key-wiping procedures, 227–228
- Opal, 128–131
- securing disk image with, 211–218

Enhanced Integrated Drive Electronics (EIDE), 32

environmental factors, 91–93

EO1. *See* EnCase EWF

EOD (End of Data) marker, on tapes, 14, 176

EOF (End of File) marker, on tapes, 176

EOM (End of Media) marker, on tapes, 176

EOT (End of Tape) marker, on tapes, 176

erasing forensic image data, 224–228

errors, drive, 159–165

estimated completion time, 87–88

evidence

- containers. *See* forensic file formats
- disk. *See* subject disk
- integrity of, 197–202. *See also* cryptography
- organizing, 76–83

EWf. *See* EnCase EWF

ewf_acquirestream tool, 172, 210

ewf_acquire tool

- compressing images, 189
- converting raw images to EWF, 202–203
- cryptographic hashing algorithms, 151, 151*t*
- error handling, 161
- forensic acquisition, 141, 145–147
- splitting images during acquisition, 193

ewf_export tool, 205, 206, 207

ewf_info tool, 206, 207

ewf_mount tool, 233, 234

ewf_verify tool, 198

examination directory structure, 79–81

examination host. *See* acquisition host

Expert Witness Format. *See* EnCase EWF

EXTENDED SECURITY ERASE command, 227

Extensible Host Controller Interface (xHCI), 29–30

external drives, encrypting, 216, 217–218

extracted files, naming conventions for, 77–78

extracting subsets of data. *See* data extraction

F

failure, drive, 159–165

FC (Fibre Channel) interface, 25–26, 26*f*

FDE (full-disk encryption), 128–131, 216–218

fg command, 93

Fibre Channel (FC) interface, 25–26, 26*f*

file compression, 85

file formats. *See* forensic file formats

files, naming conventions for, 76–79

file shredder, 224–225

file sizes, reporting, 86–87

file slack, 43

filesystems. *See also* encrypted filesystems,

- accessing
- accessing forensic file format as, 233–235
- data CD, 20

- filesystems, *continued*
 - general purpose disk encryption, 216–217, 218
 - identifying, 263–264
 - Linux kernel and, 52–55
 - slack space, extracting, 271–272
 - unallocated blocks, extracting, 272
- file transfer protocols, 224
- FileVault, Apple, 248–251
- FileVault Cracking software, 251
- FireWire (IEEE1394) interface, 33, 33*f*, 137
- first responder triage of live PCs, 102
- flash drives, 17, 131, 131*f*, 173, 228
- flash memory. *See* non-volatile memory
- Flash Translation Layer (FTL), 15
- fls command, 180, 238, 242, 249–250, 265–266
- forensic acquisition. *See also* data extraction; digital forensics; forensic image management; image access tasks
 - completeness of, 10
 - dd-based tools, 142–145
 - encryption during, 212, 213, 214
 - with forensic formats, 145–150
 - Linux as platform for, 47–57
 - managing drive failure and errors, 159–165
 - to multiple destinations, 150
 - over network, 166–172
 - overview, 141, 275–276
 - peer-reviewed research, 7–8
 - performance, 88–90, 91*t*
 - prerequisites, 9
 - RAID and multidisk systems, 178–184
 - removable media, 172–178
 - signing forensic images, 154–157
 - splitting image during, 192–194
 - standards for, 6–7
 - suspending process, 92–93
 - tools for, choosing between, 141–142
 - trends and challenges, 4–5
 - verifying hash during, 197–198
 - writing image file to clone disk, 220–221
- forensic boot CDs, 98, 99
- forensic file formats. *See also specific formats*
 - acquiring image with, 145–150
 - built-in encryption, 214–216
 - converting between, 202–211
 - image access tasks, 233–235
 - image compression support, 188
 - naming conventions for, 77
 - overview, , 59–60
 - raw images, 60–62
 - SquashFS, 63–67
- forensic filesystem analysis, 271, 274
- forensic image management
 - compression, 187–191
 - converting between image formats, 202–211
 - disk cloning and duplication, 219–221
 - overview, 187
 - secure wiping and data disposal, 224–228
 - securing image with encryption, 211–218
 - split images, 191–197
 - transfer and storage, 221–224
 - verifying image integrity, 197–202
- forensic imaging. *See* forensic acquisition
- forensic readiness, 69–70
- forensic write blockers. *See* write blockers
- forks, in open source software, 49
- formats, file. *See* forensic file formats
- FreeTSA, 158, 159, 201
- freeze commands, ATA password-protected disks, 127
- frozen DCO configuration, 119–120
- fsstat command, 263–264
- ftkimager tool
 - built-in encryption, 214–215
 - compressing images, 190
 - converting files from EnCase to FTK, 207–208
 - converting from FTK format, 208–209
 - converting raw image to FTK SMART, 203
 - cryptographic hashing algorithms, 151, 151*t*
 - error handling, 161–162
 - forensic acquisition, 141, 147–149
 - overview, 62
 - splitting images during acquisition, 193–194
- FTK SMART format
 - compressed format, 190
 - converting AFF images to, 209–210
 - converting EnCase EWF files to, 207–208
 - converting raw images to, 203

- converting to another format, 208–209
- overview, 62
- remote forensic acquisition, 171–172
- FTL (Flash Translation Layer), 15
- full-disk encryption (FDE), 128–131, 216–218
- FUSE filesystem, 196, 233, 241–243, 245, 246, 250–251
- fusermount command, 234
- fvdeinfo tool, 249
- fvdmount tool, 250–251

G

- Garfinkel, Simson, 62
- Garloff, Kurt, 62, 163
- Globally Unique Identifier (GUID), LDM disk group, 181
- GNU dd. *See* dd utility
- GNU dd_rescue tool, 61, 62, 142, 163 215–216
- GNU ddrescue tool, 61, 142, 162–163, 165
- GNU Privacy Guard (GnuPG or GPG), 155–156, 200–201, 211–213
- GNU screen terminal multiplexer, 75–76
- GNU split command, 192
- gpart tool, 267
- GPG (GNU Privacy Guard), 155–156, 200–201, 211–213
- gpgsm tool, 156–157
- gptparser.pl tool, 263
- GPT partition scheme, 262
- Grenier, Christophe, 267
- growisofs command, 222
- GUID (Globally Unique Identifier), LDM disk group, 181
- Guidance Software. *See* EnCase EWF
- GUI interface
 - versus command line, xxi
 - Linux, 55–56
- gunzip tool, 188, 213
- gzip tool, 188–189, 192, 204, 214

H

- Harbour, Nicholas, 61
- hard disks. *See also* forensic acquisition; storage media; subject disk
 - magnetic, 12–13, 13f
 - service areas, 40
 - transferring forensic image to, 223

- hardware
 - examiner workstation, viewing, 103–104
 - managing drive failure and errors, 159–165
 - subject PC, examining, 101–102
 - write blockers, 39, 94–97, 94f, 95f, 97f, 107–108
- Hardware Write Block (HWB)
 - Device Specification, Version 2.0, 94
- hashing
 - basic, 151–152, 151t
 - GPG encryption, 213
 - OpenSSL encryption, 214
 - overview, 197
 - recalculating hash, 198–199
 - split raw images, 199
 - verifying hash during acquisition, 197–198
- hash windows, 143, 152–154, 199–200
- HBA (host bus adapter), 36
- hd (hexdump) tool, 226
- HDDGURU, 125
- HDD Oracle, 125
- hddtemp tool, 91
- hdparm tool
 - ATA password-protected disks, 126, 127
 - ATA security erase unit commands, 227
 - DCO, removing, 118–120
 - HPA
 - removing, 121–122
 - replicating sector size with, 220
 - sector ranges, extracting, 270
 - querying disk capabilities and features with, 108–112
 - read-only property, 98
 - SSDs, 16–17
- heat, monitoring, 91–93
- heat sinks, 93
- hexdump (hd) tool, 226
- hidden sectors, enabling access to
 - DCO removal, 118–121
 - HPA removal, 121–122
 - overview, 118
 - system areas, 122–125
- hidden volume, VeraCrypt, 256–257
- history, shell, 73–75
- host bus adapter (HBA), 36

HPA (Host Protected Area)
 extracting sector ranges belonging
 to, 269–271
 overview, 39–40, 118
 removing, 121–122
 replicating sector size with, 219–220
Hulton, David, 251
HWB (Hardware Write Block) Device
 Specification, Version 2.0, 94
hxxp, 79

I

IAAC (Information Assurance Advisory
 Council), 8
icat tool, 249–250
IDE (Integrated Drive Electronics), 18,
 32, 32*f*
IEEE1394 (FireWire) interface, 33,
 33*f*, 137
image access tasks. *See also* encrypted
 filesystems, accessing
 boot images, preparing with xmount,
 235–237
 forensic format image files, 233–235
 overview, 229–230
 raw images, 230–233
 VM images, 237–243
image acquisition/imaging. *See* forensic
 acquisition
img_stat command, 59–60, 194, 195,
 197–198
industry
 collaboration within, 5
 regulations and best practice, 8–9
Information Assurance Advisory Council
 (IAAC), 8
information security, 211–218
initiator, SCSI commands, 36
Integrated Drive Electronics (IDE), 18,
 32, 32*f*
integrity. *See* cryptography; verifying
 forensic image integrity
interfaces. *See also specific interfaces*
 bus speeds, 90, 91*t*
 legacy, 32–34, 32*f*, 33*f*, 34*f*
 NVME, 27–29, 27*f*, 28*f*
 overview, 22
 SAS and Fibre Channel, 25–26,
 25*f*, 26*f*
 SATA, 22–25, 23*f*, 24*f*, 25*f*
 Thunderbolt, 30–32, 31*f*
 USB, 29–30, 29*f*, 30*f*
International Organization for
 Standardization (ISO), 6

International Organization of Computer
 Evidence (IOCE), 2, 3
Internet of Things, 4
inter-partition gaps, extracting, 269
IOCE (International Organization of
 Computer Evidence), 2, 3
ISO (International Organization for
 Standardization), 6
iStorage datashur drives, 228

J

jail-broken devices, 5
JBOD (Just a Bunch Of Disks), 179–180
JTAG interface, 125
jumper setting, Advanced Format 512e
 disks, 43
Just a Bunch Of Disks (JBOD), 179–180

K

Kali Linux, 99
kernel, Linux
 defined, 55
 determining partition details, 264
 and filesystems, 52–55
 and storage devices, 50–52
kernel patch, write-blocking, 98–99
kernel ring buffer, 106
Kessler, Gary, 262–263
key-wiping procedures, 227–228
Kornblum, Jesse, 61
kpartx tool, 231, 233, 234, 241, 242

L

law enforcement, and digital forensics
 collaboration, 5
 history of, 1–2
LDM (Logical Disk Manager), 181
ldmtool tool, 181
legacy technologies
 magnetic, 15
 optical storage media, 22
 storage media interfaces, 32–34, 32*f*,
 33*f*, 34*f*
Lenovo ThinkPad Secure Hard Drives,
 216, 216*f*
libata library, 39
libbde package, 247–248
libewf library, 62, 215
libfve software package, 248–251
libqcow-utils package, 237
libvhdi tools, 241
libvmdk-utils software package, 240

- link layer, disk interfaces, 34, 35*f*, 38
 - Linux. *See also* command line; *specific commands*
 - Advanced Format 4Kn disks, 42–43
 - Apple Target Disk Mode, 137–138
 - audit trail, 76
 - command execution, 56
 - compression tools, 188–189
 - distributions, 55–56
 - forensic boot CDs, 98, 99
 - in forensic context, 48–50
 - kernel and filesystems, 52–55
 - kernel and storage devices, 50–52
 - loop devices, 230–233
 - LUKS, 251–254
 - overview, xx–xxi, 47, 57
 - pipng and redirection, 56–57
 - RAID-5 acquisition, 183–184
 - SCSI commands, 36–37
 - shell history, 73, 74
 - shells, 56
 - software RAID, 178
 - Thunderbolt interface, 31–32
 - Linux Storage Stack Diagram, 52, 53*f*
 - live imaging with CoW snapshots, 172
 - live PCs, triage of, 102
 - locked DCO configuration, 119–120
 - Logical Disk Manager (LDM), 181
 - Logical Volume Manager (LVM)
 - layers, 254
 - logistical issues
 - environmental factors, 91–93
 - estimating task completion times, 87–88
 - file compression, 85
 - image sizes and disk space
 - requirements, 83–84
 - moving and copying forensic images, 87
 - overview, 83
 - performance and bottlenecks, 88–90, 91*t*
 - reported file and image sizes, 86–87
 - sparse files, 85–86
 - logs, SMART, 115
 - long-term storage of forensic images, 221–224
 - loop devices, 183–184, 230–233, 252–253, 265–266
 - loop option, `mount` command, 245, 247
 - `losetup` command, 183, 230, 231, 252, 265
 - Lougher, Phillip, 63
 - `lsblk` command, 106–107, 108
 - `ls` command, 86–87, 196
 - `lshw` tool, 103, 104, 133–134
 - `lspci` tool, 103–104
 - `lsscsi` command, 105, 108
 - `lsusb` tool, 104, 105, 108
 - `luksDump` command, 252–253
 - LUKS encryption system, 251–254
 - LVM (Logical Volume Manager)
 - layers, 254
- ## M
- M.2 interface
 - NVME, 27, 27*f*
 - SATA, 24, 24*f*
 - magnetic storage media. *See also* hard disks; magnetic tapes
 - legacy, 15
 - overview, 12
 - magnetic tapes, 14*f*
 - acquiring, 176–178
 - attaching to acquisition host, 133–135
 - overview, 13–14
 - with physical read-only modes, 100
 - maintenance sectors, 40, 122–125
 - managing image files. *See* forensic image management
 - manual extraction using offsets, 272–274
 - mapper devices, 179–182, 231–232, 253, 255–256
 - mass storage technologies. *See* storage media
 - master boot record (MBR), 129
 - master password, ATA password-protected disks, 126–127, 128
 - maximum visible sectors, on clone drive, 220
 - MBR (master boot record), 129
 - `md5sum` tool, 152, 154, 207
 - `mdadm` tool, 183, 184
 - media. *See* storage media
 - memory. *See specific types of memory;* storage media
 - memory cards, 18*f*
 - acquiring, 173–174
 - attaching to acquisition host, 136
 - overview, 17–18
 - memory slack, 43
 - metadata, forensic file formats, 62
 - Metz, Joachim, 62, 237, 247, 248
 - micro IDE ZIF interface, 33, 33*f*
 - micro SATA interface, 24, 24*f*
 - Micro SD cards, 173–174
 - Microsoft BitLocker, 243–248
 - Microsoft dynamic disks, 181–182

- Microsoft VHD format, 241–243
- mini IDE interface, 33, 33*f*
- Mini-SAS HD interface, 26*f*
- mini-SATA (mSATA) interface, 23, 23*f*
- mirrored disks, RAID-1, 182–183
- mismatched hash windows, 199–200
- mkisofs command, 221–222
- mksquashfs tool, 63, 170, 206–207
- mmcat tool, 266, 268, 269, 270
- mm1s command, 262
- mmstat command, 260, 261
- mount command, 184, 241, 245, 247
- mounting
 - decrypted filesystem image, 245, 246, 247, 250, 253, 256
 - filesystems in Linux, 53–54
 - forensic format image files, 233–235
 - image files as regular filesystems, 229
 - loop partitions, 232–233
 - SquashFS container, 66
 - VeraCrypt volume, 218
 - VM images, 236, 238–239, 240–243
- moving forensic images, 87
- mpt-status tool, 178
- mSATA (mini-SATA) interface, 23, 23*f*
- msed tool, 129
- mt tool, 134–135
- multidisk systems, acquiring
 - JBOD and RAID-0 striped disks, 179–180
 - Linux RAID-5, 183–184
 - Microsoft dynamic disks, 181–182
 - overview, 178
 - proprietary systems, 178–179
 - RAID-0 striped disks, 179–180
 - RAID-1 mirrored disks, 182–183
- multifunction drivebay write blocker, 94, 95*f*
- multiple destinations, forensic acquisition to, 150
- music CDs, 20, 175. *See also* CDs; optical storage media
- myrescue tool, 163

N

- namespaces, NVME, 44–45, 138, 139, 226
- naming conventions for files and directories, 76–79
- NAND flash technology, 15
- National Institute of Standards and Technology. *See* CFTT project
- nbd kernel module, 237–238, 239
- negative sectors, 40, 122–125

- Netherlands Forensic Institute (NFI), 166
- network
 - image acquisition over
 - to EnCase or FTK format, 171–172
 - live imaging with CoW snapshots, 172
 - overview, 166
 - with rdd, 166–168
 - to SquashFS evidence container, 169–171
 - with ssh, 168–169
 - transferring acquired images, 223–224, 223*t*
 - performance tuning, 90
 - Next Generation Form Factor (NGFF), 27
 - NFI (Netherlands Forensic Institute), 166
 - NIST. *See* CFTT project
 - nonprivileged user, 241–243, 246, 251, 254
 - non-volatile memory
 - legacy, 19
 - overview, 15–16
 - removable memory cards, 17–18, 18*f*
 - solid state drives, 16–17, 16*f*
 - USB flash drives, 17, 17*f*
 - Non-Volatile Memory Express (NVME)
 - command set, 37–38, 37*t*
 - interface, 27–29, 27*f*, 28*f*
 - namespaces, 44–45, 138, 139, 226
 - nvme-cli software package, 44–45
 - nvme tool, 138, 139
 - SSDs, 138–139
 - wiping drives, 226
 - nwipe tool, 226

O

- of= flags, dc3dd tool, 150
- offset flag, losetup command, 231
- offsets, manual extraction using, 272–274
- Opal self-encrypting drives, 128–131, 228
- opengates tool, 236
- openjobs tool, 236
- open source software (OSS), 48–50, 276
- OpenSSH software package, 224
- OpenSSL command line tool, 157–159, 201–202, 213–214
- optical storage media
 - acquiring, 174–175
 - attaching to acquisition host, 132–133
 - Blu-ray discs, 19*f*, 21–22
 - acquiring, 174, 175
 - transferring forensic image to, 222, 223

- CDs, 19*f*, 20–21
 - acquiring, 174, 175
 - Linux forensic boot, 98, 99
 - transferring forensic image to, 221–222
- damaged, 165
- DVDs, 19*f*, 21
 - acquiring, 174, 175
 - reassembling split forensic images, 196
 - transferring forensic image to, 222
- legacy, 22
- overview, 19–20
- transferring forensic image to, 221–223

OS-encrypted filesystems. *See* encrypted filesystems, accessing

OS image, booting in VM, 235–237

OSS (open source software), 48–50, 276

OS X, booting image in VM, 236

over-provisioning, 15–16

P

Parallel ATA (PATA), 18

parallel interfaces, 22

parsing tools, 262–263

partition devices, 51–52, 231–233, 238, 239–240

partition extraction

- deleted, 266–268
- HPA and DCO sector ranges, 269–271
- individual, 264–266
- inter-partition gaps, 269
- overview, 264

partition scheme, analyzing, 259–264

partition tables, 261–263

password-protected disks, 126–128

password recovery techniques, 125

PATA (Parallel ATA), 18

PC-3000 tool, Ace Laboratory, 122

PCI bus, listing devices attached to, 103–104

PCI Express write blockers, 96, 97*f*

PEM signature file, 157, 201

Pentoo forensic CD, 99

PEOT (Physical End of Tape) marker, 176

performance, forensic acquisition, 88–90, 91*t*

PGP (Pretty Good Privacy), 155–156

PHY devices, 38

Physical End of Tape (PEOT) marker, 176

physical errors, SMART data on, 117–118

physical layer, disk interfaces, 34, 35*f*, 38–39

physical PC examination, 102

physical read-only modes, media with, 100, 100*f*

Physical Security ID (PSID), 128, 129*f*, 228

piecewise data extraction. *See* data extraction

piecewise hashing, 152–154, 199–200

pipng

- acquiring image to multiple destinations, 150
- with AFF files, 209
- combining compressing and splitting, 192
- compressing images with, 189
- cryptographic hashes of split raw images, 199
- cryptographic hashing algorithms, 152
- in Linux, 56–57
 - to validate acquisition hash, 197–198

PKI (public key infrastructure), 156, 216

plain dm-crypt encryption, 251, 254

planning for forensic acquisition. *See* preparatory forensic tasks

post-acquisition tasks. *See* data extraction; forensic image management; image access tasks

postmortem computer forensics. *See* digital forensics; forensic acquisition

power management, 93

preparatory forensic tasks. *See also* logistical issues

- audit trail, 70–76
- organizing collected evidence and command output, 76–83
- overview, 69–70
- write-blocking protection, 93–100

Pretty Good Privacy (PGP), 155–156

private sector forensic readiness, 70

privileges, command, xxv, 212, 233. *See also* nonprivileged user

proc filesystem, Linux, 107

proprietary RAID acquisition, 178–179

pseudo definition file, mksquashfs, 206

PSID (Physical Security ID), 128, 129*f*, 228

public key infrastructure (PKI), 156, 216

public sector forensic readiness, 70

Q

- QCOW2 format, 237–239
- qcowinfo tool, 237
- qcowmount tool, 237
- QEMU emulator, 237–239
- qemu-img command, 237
- qemu-nbd tool, 237–238, 239
- querying subject disk
 - documenting device identification details, 107–108
 - extracting SMART data, 112–118
 - with hdparm, 108–112
 - overview, 107

R

- RAID (Redundant Array of Independent Disks) systems, acquiring
 - JBOD striped disks, 179–180
 - Linux RAID-5, 183–184
 - Microsoft dynamic disks, 181–182
 - overview, 178
 - proprietary systems, 178–179
 - RAID-0 striped disks, 180
 - RAID-1 mirrored disks, 182–183
- RAM slack, 43
- raw devices, in Linux, 51, 52
- raw images
 - accessing forensic file format as, 233–235
 - converting to and from AFF, 209
 - converting to another format, 202–205
 - cryptographic hashes of split, 199
 - data recovery tools, 61–62
 - dd utility, 60
 - forensic dd variants, 61
 - image access tasks, 230–233
 - naming conventions for, 77
 - overview, 60
 - preparing boot images with
 - xmount tool, 236
 - reassembled, 196–197
 - writing to clone disk, 220–221
- rdd tool, 166–168
- read errors, dd utility, 143–144
- read-only modes, media with, 100, 100*f*
- read-only property, setting with write blockers, 97–98
- reassembling split forensic images, 195–197

- recalculating hash of forensic image, 198–199
- Recorder Identification Code (RID), CDs, 21
- recoverdm tool, 163
- redirection
 - with AFF files, 209
 - compressing images with, 189
 - in Linux, 56–57
 - saving command output with, 81–83
- Redundant Array of Independent Disks.
 - See* RAID systems, acquiring
- regulations, industry-specific, 8–9
- remapped sectors, 40
- remote access to command line, xxi
- remote forensic acquisition
 - to EnCase or FTK format, 171–172
 - live imaging with CoW snapshots, 172
 - overview, 166
 - with rdd, 166–168
 - secure, with ssh, 168–169
 - to SquashFS evidence container, 169–171
 - transferring acquired images, 223–224, 223*t*
- removable storage media. *See also specific media types*; storage media
 - acquiring, 172–178
 - attaching to acquisition host, 132–136
 - encrypting, 216
 - transferring forensic image to, 221–223
- reported file and image sizes, 86–87
- research, peer-reviewed, 3, 7–8
- RFC-3161 timestamping, 157–159, 201
- RID (Recorder Identification Code), CDs, 21
- ring buffer, kernel, 106
- ripping music CDs, 175

S

- S01. *See* FTK SMART format
- SAS (Serial Attached SCSI) interface, 25–26, 25*f*, 26*f*, 37
- SAT (SCSI-ATA Translation), 39
- SATA (Serial ATA) interface, 16, 22–25, 23*f*, 24*f*, 25*f*, 94*f*
- SATA Express disk interface, 25, 25*f*
- scalable examination directory structure, 79–81

- Scientific Working Group on Digital Evidence (SWGDE), 3
- scp (secure copy) tool, 224
- screen terminal multiplexer, 75–76
- script command, 75
- scripting, with command line, xxi
- scriptreplay command, 75
- SCSI-ATA Translation (SAT), 39
- SCSI interface, 34*f*
 - command sets for, 36–37, 37*t*, 39
 - documenting device identification details, 108
 - identifying subject drive, 105
 - overview, 33–34
 - querying drives, 112
 - tape drives, querying, 134
- SD (Secure Digital) standard, 18
- sdparm command, 112
- sector offsets
 - converting into byte offset, 247–248, 249, 252, 265
 - filesystem identification, 263–264
 - manual extraction using, 272–274
- sectors. *See also* hidden sectors, enabling access to; 4Kn disks
 - hard disks, 12, 40
 - replicating with HPA, 219–220
 - user-accessible, wiping, 225–226
- secure copy (scp) tool, 224
- secure_deletion toolkit, 224
- Secure Digital (SD) standard, 18
- Secure/Multipurpose Internet Mail Extensions (S/MIME), 155, 156–157, 201
- secure network data transfer, 223–224
- secure remote imaging, 168–169
- secure wiping and data disposal, 224–228
- security erase command, ATA, 226–227
- security features, subject disk
 - ATA password-protected disks, 126–128
 - encrypted flash thumb drives, 131
 - overview, 125
 - self-encrypting drives, 128–131
- security levels, ATA password-protected disks, 127
- security of forensic image, 211–218
- SEDs (self-encrypting drives), 128–131, 218, 228
- sedutil-cli command, 129–130, 218, 228
- seeking, within compressed files, 188, 204
- self-encrypting drives (SEDs), 128–131, 218, 228
- Self-Monitoring, Analysis and Reporting Technology (SMART)
 - extracting data with smartctl, 112–118
 - managing drive failure and errors, 163–164
 - NVME drives, 139
- self-tests, SMART data on, 115–116
- serial access to disks, 122–125
- Serial ATA (SATA) interface, 16, 22–25, 23*f*, 24*f*, 25*f*, 94*f*
- Serial Attached SCSI (SAS) interface, 25–26, 25*f*, 26*f*, 37
- serial bus controller class, 104
- serial point-to-point connections, 22
- server mode, rdd tool, 166, 167, 168
- service areas, 40, 122–125
- sessions, CD, 20
- sfsimage tool
 - acquiring image with, 149–150
 - converting AFF file to compressed SquashFS, 210
 - converting FTK files to SquashFS, 208–209
 - converting raw image to SquashFS, 203–204
- dcfldd and dc3dd tools, 145
- image access tasks, 235
- overview, 63
- remote forensic acquisition, 169–171
- removable media, acquiring image of, 174
- SquashFS compression, 191
- SquashFS evidence containers, 64–67
- sg3_utils software package, 36–37
- shadow MBR on Opal SEDs, 129–130, 131
- shared buses, 22
- shell alias, 72–73
- shell history, 73–75
- shells. *See* Bash; command line
- shredding files, 224–225
- SID (Source Unique Identifier), CDs, 21
- sigfind tool, 266
- signatures, confirming validity of, 200–202
- signing forensic images, 154–157
- size
 - disk image, 83–84
 - reported file and image, 86–87
- skip parameter, for partition extraction with dd, 266

- slack space, 43, 271–272
- Sleuth Kit
 - blkcat command, 274
 - blkls command, 271–272
 - fls command, 180, 238, 242, 249–250, 265–266
 - fsstat command, 263–264
 - img_stat command, 59–60, 194, 195, 197–198
 - mmcat tool, 266, 268, 269, 270
 - mm1s command, 262
 - mmstat command, 260, 261
 - sigfind tool, 266
- SMART (FTK forensic format). *See* FTK SMART format
- SMART (Self-Monitoring, Analysis and Reporting Technology)
 - extracting data with smartctl, 112–118
 - managing drive failure and errors, 163–164
 - NVME drives, 139
- smartctl command, 91–92, 112–118
- S/MIME (Secure/Multipurpose Internet Mail Extensions), 155, 156–157, 201
- Snoopy command logger, 74–75
- software
 - open source, 48–50
 - proprietary, 49–50
 - write blockers, 97–99, 108
- solid state drives (SSDs), 12, 16–17, 16*f*, 43, 138–139
- Solid State Hybrid Disks (SSHDs), 45
- source-level access, to open source software, 48
- Source Unique Identifier (SID), CDs, 21
- space requirements, 83–84
- sparse files, 85–86
- split command, 192
- split forensic images
 - accessing, 194–195
 - cryptographic hashes of, 199
 - during acquisition, 192–194
 - overview, 191–192
 - reassembling, 195–197
- SquashFS
 - background of, 63
 - burning file to CD, 221–222
 - converting AFF file to compressed, 210–211
 - converting FTK files to, 208–209
 - converting raw images, 202–205
 - forensic evidence containers, 64–67, 149–150, 191
 - image access tasks, 235
 - manual container creation, 205–207
 - overview, 63
 - remote forensic acquisition, 169–171
- squashfs-tools package, 64
- SSDs (solid state drives), 12, 16–17, 16*f*, 43, 138–139
- ssh command, 168–172
- SSHDs (Solid State Hybrid Disks), 45
- standards, digital forensics, 6–7
- stderr, 82
- stdin, 82, 189
- stdout, 81–82, 189
- storage, forensic image, 221–224
- storage media. *See also* forensic acquisition; *specific media types*; subject disk
 - Advanced Format 4Kn disks, 12, 41–44, 42*f*
 - DCO and HPA drive areas, 39–40
 - encrypting, 216–218
 - examiner workstation hardware, 103–104
 - image sizes and disk space requirements, 83–84
 - interfaces and connectors, 22–32
 - Linux kernel and, 50–52, 53*f*
 - magnetic, 12–15
 - naming conventions for, 77, 78
 - non-volatile memory, 15–19
 - NVME namespaces, 44–45
 - optical, 19–22
 - overview, 11–12, 46
 - remapped sectors, 40
 - scalable examination directory structure, 80, 81
 - secure disk wiping, 225–226
 - Solid State Hybrid Disks, 45
 - system areas, 40, 122–125
 - terms used for, xxvii
 - trends and challenges, 4
 - UASP, 29, 40–41
 - write-blocking protection, 93–100
- strace command, 195
- striped disks, 179–180
- subject disk. *See also* forensic acquisition; storage media
 - attaching to acquisition host
 - Apple Target Disk Mode, 137–138
 - devices with block or character access, 140

- enabling access to hidden sectors, 118–125
- examining subject PC hardware, 101–102
- identifying subject drive, 105–107
- NVME SSDs, 138–139
- overview, 101
- querying subject disk, 107–118
- removable storage media, 132–136
- security features, 125–131
- viewing examiner workstation hardware, 103–104
- defined, xxvi
- image sizes and disk space requirements, 83–84
- preparing boot images with xmount tool, 235–237
- removal from PC, 102
- temperature monitoring, 91–93
- subsets of data, extracting. *See* data extraction
- sudo command, 212, 242–243, 246, 251, 254
- support, for open source software, 48, 49
- suspect disk. *See* subject disk
- suspending acquisition process, 92–93
- SWGDE (Scientific Working Group on Digital Evidence), 3
- symmetric encryption, 211–213, 215–216
- sync parameter, dd utility, 143
- /sys pseudo filesystem, 42–43
- system areas, 40, 122–125

T

- tableau-parm tool, 95–96, 121
- Tableau write blocker, 94*f*, 95–96
- tapeinfo tool, 134–135
- tapes, magnetic, 14*f*
 - acquiring, 176–178
 - attaching to acquisition host, 133–135
 - overview, 13–14
 - with physical read-only modes, 100
- target, SCSI commands, 36
- Target Disk Mode (TDM), Apple, 31, 137–138
- task completion times, estimating, 87–88
- task management, 70–73
- Taskwarrior, 71–72
- TCG (Trusted Computing Group), 128
- tc-play, 217
- TDM (Target Disk Mode), Apple, 31, 137–138

- tee command, 152
- temperature data, SMART, 116–117
- temperature monitoring, 91–93
- terminal monitors, 76
- terminal multiplexers, 75–76
- terminal recorders, 75–76
- testdisk tool, 267–268
- text files, naming conventions for, 78, 79
- thumb drives, 17, 131, 131*f*, 173, 228
- Thunderbolt interface, 30–32, 31*f*, 137
- Thunderbolt-to-FireWire adapter, 137–138
- time command, 82
- timestamps, 82–83, 157–159, 201–202
- tmux terminal multiplexer, 75–76
- todo.txt* file format, 72
- transfer, forensic image, 221–224
- transport layer, disk interfaces, 34, 35*f*
- Trapani, Gina, 72
- triage of live PCs, 102
- TRIM command, ATA, 16–17
- TrueCrypt, 216–217, 254–257
- Trusted Computing Group (TCG), 128
- TSA certificates, 201
- ts command, 83, 158–159
- tsget command, 158
- Type C interface, USB, 30, 30*f*

U

- U.2 interface, NVME, 28, 28*f*
- UASP (USB Attached SCSI Protocol), 29, 40–41
- UDF (Universal Disk Format), 21
 - udevadm tool, 50–51
 - udev system, Linux, 50–51
- umount command, 54, 207, 232–233, 234, 241
- unallocated blocks, extracting, 272
- unique identifiers, 77, 105
- Universal Disk Format (UDF), 21
- Universal Serial Bus. *See* USB
- unmounting
 - decrypted filesystem image, 245, 251, 254, 256
 - filesystems in Linux, 54
 - forensic format image files, 234
 - loop partitions, 232–233
 - VeraCrypt volume, 218
 - virtual images, 236
- unsquashfs command, 207
- URLs, naming conventions for, 79

- USB (Universal Serial Bus), 29*f*, 30*f*
 - card readers, 18
 - documenting device identification details, 108
 - flash drives, 17, 17*f*, 131, 131*f*, 173, 228
 - listing devices attached to, 104, 105
 - multifunctional devices, 140
 - overview, 29–30
 - serial access to disks, 122–125
- USB Attached SCSI Protocol (UASP), 29, 40–41
- usb_modeswitch tool, 140
- useless use of cat (UUOC), 199
- user-accessible sectors, wiping, 225–226
- user password, ATA password-protected disks, 126–127
- UUOC (useless use of cat), 199

V

- varmon tool, 178
- VBoxManage tool, 239
- VDI format, 236, 239–240
- VeraCrypt, 217–218, 254–257
- verifying forensic image integrity
 - GPG encryption, 213
 - manual creation of SquashFS container, 207
 - mismatched hash windows, 199–200
 - OpenSSL encryption, 214
 - overview, 197
 - recalculating hash, 198–199
 - signature and timestamp, 200–202
 - split raw images, 199
 - verifying hash during acquisition, 197–198
- VFDecrypt tool, 251
- VFS (Virtual File System) abstraction layer, 52
- VHD format, Microsoft, 241–243
- vhdiinfo command, 241–242
- vhdimount command, 242
- VirtualBox VDI images, 236, 239–240
- Virtual File System (VFS) abstraction layer, 52
- Virtual Machine Disk (VMDK) format, 240–241
- Vital Product Data (VPD), 112
- vmdkinfo command, 240

- VM images, accessing
 - dislocker package, 244–245
 - Microsoft VHD, 241–243
 - overview, 237
 - QEMU QCOW2, 237–239
 - VirtualBox VDI, 239–240
 - VMWare VMDK, 240–241
- VMs, booting subject drive in, 235–237
- VMWare VMDK format, 240–241
- VPD (Vital Product Data), 112

W

- wear leveling, 15
- Weinmann, Ralf-Philipp, 251
- window managers, Linux, 55–56
- Windows, booting image in VM, 236
- wiping forensic image data, 224–228
- World Wide Name (WWN), 111–112
- write blockers
 - documenting evidence for use of, 107–108
 - hardware, 39, 94–97, 94*f*, 95*f*, 97*f*
 - importance of, 93–94
 - for legacy interferences, 34
 - Linux forensic boot CDs, 99
 - media with physical read-only modes, 100, 100*f*
 - NVME, 28–29
 - overview, 21
 - software, 97–99, 108
 - for USB devices, 30
 - when mounting filesystems, 54
- WWN (World Wide Name), 111–112

X

- X11 window system, Linux, 55
- Xen blktap xapi interface, 241
- xHCI (Extensible Host Controller Interface), 29–30
- xmount tool, preparing boot images with, 235–237

Z

- zcat tool, 189, 196, 199
- ZIP archive format, 211
- zuluCrypt, 217