

INDEX

A

- abrt (automated bug reporting tool), 107
- activation and on-demand services
 - concept behind, 168
 - D-Bus activation, 169
 - device activation, 171
 - path-based activation, 170
 - scheduled commands and timers, 172–175
 - socket activation, 168
- addressing, 226–229
- advanced persistent threat (APT)
 - malware, 3
- Anaconda, 190
- analysis hosts, xxix
- Anonymous, 3
- anti-forensics, 9
- AppImage, 213–215
- application crash data, 107–109
- application logs, 129–135
- application metadata, 99
- application plug-ins, 223
- APT. *See* advanced persistent threat (APT) malware
- apt command, 203–206
- Arch Linux, 27, 192
- Arch pacman packages, 210–212
- at program, 172
- attached storage devices, 334–337
- audit logs, 135–143
- authentication and authorization, 288–303
 - biometric fingerprint
 - authentication, 300
 - elevated privileges, 293
 - GNOME Keyrings, 296
 - GNU Privacy Guard (GnuPG), 301
 - KDE wallet manager, 298
 - PAM module, 288
 - user, group, and password files, 288

B

- backdoors, 234–237
- best practices, 8
- biometric fingerprint authentication, 300
- BIOS/MBR GRUB booting, 147
- block device type, 19
- blocks, 44
- Bluetooth artifacts, 242–244
- bookmarks, 310–311
- bootloader analysis, 145–153
 - BIOS/MBR GRUB booting, 147
 - booting overview, 145
 - GRUB configuration, 150
 - other bootloaders, 152
 - UEFI GRUB booting, 148
- brfs analysis, 56–65
- buttons, physical, 181

C

- cache directory, 89
- carving tools, 71
- CentOS Stream, 27
- CERT (Computer Emergency Response Team), 2
- CFTT (Computer Forensics Tool Testing project), 3
- character device type, 19
- chip-off technique, 32
- clipboard data, 307–308
- cloud services, 321–324
- code examples
 - formatting and presentation, xxix
- collaboration, 6
- command line (Linux systems), 21
- commands, scheduled, 172–175
- Comprehensive Perl Archive Network (CPAN), 222
- Computer Emergency Response Team (CERT), 2

- Computer Forensics Tool Testing project (CFTT), 3
 - configuration artifacts. *See also*
 - desktop settings and configurations
 - areas covered, 225
 - network configuration analysis, 226–237
 - network security artifacts, 246–253
 - wireless network analysis, 237–246
 - configuration directory, 89
 - content analysis, 100
 - copy-on-write (CoW) snapshots, 41
 - core dumps, 104–114
 - Coroner’s Toolkit, 2
 - COVID-19 health crisis, 4
 - CPAN (Comprehensive Perl Archive Network), 222
 - crash dumps, 104–114
 - cron system, 173
 - cryptographic hashes, 93
 - cryptsetup tool, 76
 - custom logs, 129–131
 - cyber insurance, 8
- D**
- daemon logs, 129–135
 - daemons, 166–168
 - DARPA (Defense Advanced Research Projects Agency), 2
 - data flow diagrams, xxx
 - daylight saving time, 259
 - D-Bus activation, 169
 - dead disk forensics, xix
 - Debian apt command, 203–206
 - Debian binary package format (DEB), 194–198
 - Debian Installer, 188
 - Debian Linux, 25
 - debugfs tool, 55
 - Defense Advanced Research Projects Agency (DARPA), 2
 - desktop artifacts, 303–317
 - desktop bookmarks and recent files, 310
 - desktop clipboard data, 307
 - desktop search engines, 315
 - desktop settings and configurations, 303
 - desktop thumbnail images, 311
 - desktop trash cans, 308
 - GNOME desktop searches, 315
 - KDE desktop searches, 316
 - other search engines, 317
 - screenshots, 315
 - well-integrated desktop applications, 313
 - desktop environments (Linux systems), 22
 - desktop logins, 284–287
 - desktop search engines, 315
 - desktop settings and configurations, 303–306
 - GNOME configuration, 303
 - KDE configuration, 306
 - other desktop configurations, 306
 - desktop thumbnail images, 311–313
 - desktop trash cans, 308
 - device activation, 171
 - devices (Linux system), 19
 - DFRWS. *See* Digital Forensics Research Workshop (DFRWS)
 - digital forensics
 - analysis trends and challenges, 5–7
 - anti-forensics, 9
 - forensic readiness, 9
 - future concerns, 4
 - history of, 1–4
 - principles of, 7–8
 - Digital Forensics Research Workshop (DFRWS)
 - 2001 conference, 2
 - role of, 8
 - Digital Investigation* journal, 7
 - Digital Millennium Copyright Act, 2
 - directory files, 45
 - directory layout and file analysis
 - crash and core dumps, 104–114
 - Linux directory layout, 83–95
 - Linux file analysis, 99–104
 - Linux file types and identification, 95–99
 - DISCARD command, 32
 - disktype tool, 35, 46
 - distro installer analysis, 187–193
 - Arch Linux, 192
 - basic questions, 187
 - building timelines, 187

- Debian Installer, 188
- Fedora Anaconda, 190
- initial steps, 187
- Raspberry Pi Raspian, 190
- SUSE YaST, 191
- timestamps, 188
- distro release information, 185
- distro-specific configurations, 229–231
- distro-specific crash data, 107–109
- dnf (Dandified Yum), 206–208
- DNS (domain name system), 231
- DNS resolution, 231–234
- domain name system (DNS), 231
- dot files, 88, 98
- dumpe2fs tool, 52
- dumping core, 104

E

- eCryptfs encrypted directories, 77–80
- elevated privileges, 293–295
- ELF (Executable and Linkable Format), 101
- encryption analysis, 72–81
 - eCryptfs encrypted directories, 77–80
 - ext4 directory encryption, 80–81
 - fsencrypt directory encryption, 80–81
 - LUKS full-disk encryption, 74–77
- erasing files, versus trashing files, 308
- Ethernet cables, 180
- evidence collection, trends and challenges in, 5
- evidence drives, xxix
- Ewing, Marc, 27
- examination hosts, xxix
- Executable and Linkable Format (ELF), 101
- executable files, 101–104
- ext4 analysis, 50–56
- ext4 directory encryption, 80–81
- extended filesystem (ext), 50
- external attached storage, 334–337

F

- Farmer, Dan, 2
- fast user switching, 287
- favorites, 310–311
- Fedora, 27

- Fedora Anaconda, 190
- Fedora dnf, 206–208
- file analysis. *See* directory layout and file analysis
- file extensions, 97
- file managers, 308, 314
- filesystems and storage devices, 334–337
 - btrfs analysis, 56–65
 - erasing files versus trashing files, 308
 - ext4 analysis, 50–56
 - extracting evidence from, 31
 - filesystem encryption analysis, 72–81
 - filesystem forensic analysis, 44–50
 - filesystem hierarchy, 84–88
 - Linux swap analysis, 69
 - storage layout and volume management, 33–44
 - xfx analysis, 65–69
- file types, POSIX standard, 95
- financial technologies (FinTech), 5
- firewalls, 249–251
- Flatpak, 215–218
- fls tool, 48
- forensic readiness, 9
- Forensic Science International (FSI), 8
- forensics tools and platforms
 - carving tools, 71
 - cryptsetup tool, 76
 - debugfs tool, 55
 - disktype tool, 35, 46
 - dumpe2fs tool, 52
 - first open source, 2
 - fls tool, 48
 - fstat tool, 46, 52
 - istat tool, 54
 - lvdisplay tool, 39
 - mdadm tool, 42
 - mmls tool, 35
 - pvdisplay tool, 39
 - requirements for, xxii
 - The Sleuth Kit (TSK), 2, 32
 - undelete-btrfs tool, 64
- fsencrypt directory encryption, 80–81
- FSI (Forensic Science International), 8
- fstat tool, 46, 52

G

- GeoClue geolocation service, 271
- geographic location, 268–272
 - location history, 269
 - overview of, 268
- GNOME configuration, 303–305
- GNOME desktop searches, 315
- GNOME Keyrings, 296–297
- GNU Privacy Guard (GnuPG), 301
- GNU software packages, 221
- group files, 288–293
- GRUB configuration, 150
- GRUB MBR booting, 147
- GRUB UEFI booting, 148
- GUI frontends, 219–221

H

- hardware (Linux systems), 17
- hash databases, 93–95
- hashsets, 93–95
- hibernation, 71
- hidden files/directories, 88, 98
- hostname, 186
- human proximity indicators, 179–182

I

- i18n. *See* internationalization
- independent server application logs, 131
- independent user application logs, 133–134
- industry-specific regulations, 8
- initialization. *See* system boot and initialization
- initrd and initramfs files, 158–161
- inodes, 44
- installed software packages. *See* software packages installed
- interfaces, 226–229
- internationalization, 264
 - locale and language settings, 264
 - overview of, 264
 - physical keyboard layout, 266
- International Organization of Computer Evidence (IOCE), 2
- Internet of Things (IoT) devices
 - increase in, 4
 - trends and challenges, 5

- INTERPOL Forensic Science Symposium, 3
- IOCE (International Organization of Computer Evidence), 2
- IoT. *See* Internet of Things (IoT) devices
- IP access control, 249–251
- IP geolocation, 269
- IPsec, 248
- istat tool, 54

K

- KDE configuration, 306
- KDE desktop searches, 316
- KDE wallet manager, 298–300
- kernel architecture (Linux systems), 18
- kernel crashes, 109
- kernel initialization analysis, 153–161
 - analyzing initrd and initramfs, 158
 - initialization overview, 153
 - kernel command line and runtime parameters, 154
 - kernel modules, 155
 - kernel parameters, 157
- kernel logs, 135–143
- kernel ring buffer, 136–139
- keyboard layout, 266–268
- keyrings, 296–297

L

- language settings, 264–266
- laptop lid interactions, 179
- LBA. *See* logical block access (LBA)
- leap time, 259
- Linux. *See also* Linux forensics; Linux logs
 - access points, 241
 - distributions, 23–28
 - filesystem concepts, 44
 - firewalls, 249–251
 - forensic analysis of, 28
 - history of, 12–16
 - interfaces, 226–229
 - system components, 16–23
- Linux Auditing System, 139–143
- Linux forensics. *See also* Linux; Linux logs
 - analysis scenarios, xix–xxi

- book conventions and format, xxviii
- book organization and structure, xxiv
- book overview by chapter, xxvi
- data flow diagrams, xxx
- defined, xvii
- formatting and presentation, xxix
- increased need for, 5
- prerequisites to learning, xxii
- reliable resources, xxviii
- scope of coverage, xxiii
- target audience, xxi
- terminology, xxix
- tools and platforms required, xxii
- Linux From Scratch (LFS), 184
- Linux logs. *See also* Linux; Linux forensics
 - kernel and audit logs, 135–143
 - other application and daemon logs, 129–135
 - systemd journals, 121–129
 - traditional syslogs, 116–121
- Linux time configuration analysis, 264
- live system incident response, xix
- locale settings, 264–266
- location history, 269–271
- lock-down technologies, 5
- logical block access (LBA), 44
- Logical Volume Manager (LVM), 37–41
- login activity. *See* user desktops and login activity reconstruction
- login and session analysis, 273–287
 - desktop logins, 284
 - overview of, 273
 - seats and sessions, 275
 - shell logins, 278
 - X11 and Wayland, 281
- logs. *See* Linux logs
- LUKS full-disk encryption, 74–77
- lvsdisplay tool, 39
- LVM. *See* Logical Volume Manager (LVM)

M

- machine IDs, 186
- magic strings, 46, 97
- man pages, xxviii
- manually compiled software, 221

- Mason, Chris, 56
- MBR GRUB booting, 147
- mdadm tool, 42
- media, removable, 181
- mm1s tool, 35
- mounted storage, 336
- multi-jurisdictional concerns, 6
- Murdock, Ian, 25

N

- National Institute of Standards and Technology (NIST), 3, 94
- National Software Reference Library (NSRL), 94
- network access. *See* user network access; wireless network analysis
- network addressing, 226–229
- network configuration analysis, 226–237
 - DNS resolution, 231
 - Linux interfaces and addressing, 226
 - network managers and distro-specific configuration, 229
 - network services, 234
- network configuration artifacts. *See* configuration artifacts
- network managers, 229–231
- network security artifacts, 246–253
 - IPsec, 248
 - Linux firewalls and IP access control, 249
 - openvpn program, 249
 - proxy settings, 251
 - WireGuard, 246
- network services, 234–237
- network shares, 321–324
- NIST (National Institute of Standards and Technology), 3, 94
- NSRL (National Software Reference Library), 94

O

- on-demand services. *See* activation and on-demand services
- oops conditions, 109
- openvpn program, 249

P

- package file format analysis, 193
 - Arch pacman packages, 200–202
 - Debian binary package format (DEB), 194
 - forensic analysis tasks, 193
 - Red Hat Package Manager (RPM), 198
- PackageKit, 219–221
- package management systems analysis, 202–212
 - Arch pacman packages, 210
 - Debian apt command, 203
 - Fedora dnf, 206
 - SUSE zypper, 208
 - typical components, 202
- pacman tool, 210–212
- PAM module, 288, 301
- panic conditions, 109
- partition tables, 33–37
- password files, 288–293
- path-based activation, 170
- PCI Express devices, 329
- peer-reviewed research, 7
- peripheral devices
 - external attached storage, 334–337
 - human proximity indicator, 181
 - identifying attached USB devices, 327
 - identifying PCI and Thunderbolt devices, 329
 - Linux device management, 326
 - printers and scanners, 330–334
- perpetrators, xix–xxi
- physical buttons, 181
- physical environment analysis. *See* power and physical environment analysis
- physical keyboard layout, 266–268
- plug-ins, 223
- Plymouth splash startup logs, 134
- POSIX file types, 95
- power and physical environment, 182
- power and physical environment analysis, 175
 - human proximity indicators, 179
 - overview of, 175
 - sleep, shutdown, and reboot evidence, 176

- power cables, 179
- prerequisite knowledge, xxii
- printers, 330–334
- privileges, 293–295
- programming language packages, 222
- proxy settings, 251–253
- pvdisplay tool, 39
- Python Package Installer, 222

R

- RAID. *See* redundant array of independent disks (RAID)
- Raspberry Pi clock, 262
- Raspbian, 190
- reboot evidence, 176–178
- recent files, 310–311
- Red Hat Linux, 27
- Red Hat Package Manager (RPM), 198–200
- redundant array of independent disks (RAID), 41, 44
- regulations, industry-specific, 8
- remote desktop access, 320
- removable media, 181
- resources, locating accurate and reliable, xxviii
- rolling-release distributions, 27
- rolling-release model, 184
- root directory, 83
- Ruby Gems, 222

S

- Sarbanes–Oxley Act, 2, 8
- scanners, 330–334
- scheduled commands, 172–175
- Scientific Working Group on Digital Evidence (SWGDE), 3
- scope of coverage, xviii
- screenshots, 315
- seats, 275–278
- secure shell access, 317–320
- September 11, 2001 attack, 2
- sessions, 275–278
- shell logins, 278–281
- shutdown evidence, 176–178
- signatures, 46
- slackspace, 47
- sleep evidence, 176–178

- Sleuth Kit, The (TSK), 2, 32
 - Snap, 218–219
 - Snowden, Edward, 3
 - social engineering attacks, xix, 4, 73
 - socket activation, 168
 - software centers, 219–221
 - software packages installed
 - areas of interest, 183
 - distro installer analysis, 187–193
 - lack of installation standards, 184
 - manual installation process, 183
 - other software installation analysis, 221–223
 - package file format analysis, 193–202
 - package management systems
 - analysis, 202–212
 - software release management, 184
 - system identification, 184–187
 - universal software package analysis, 212–221
 - version numbers, 184
 - standards, lack of, 7
 - storage devices, external attached. *See*
 - filesystems and storage devices
 - storage layout and volume management
 - Linux software RAID, 41
 - storage layout and volume management analysis
 - Linux software RAID, 44
 - Logical Volume Manager (LVM), 37–41
 - partition tables, 33–37
 - Stuxnet worm, 3
 - subject drives, xxix
 - superblocks, 46
 - SUSE YaST, 191
 - SUSE zypper, 208
 - suspect drives, xxix
 - swap analysis, 69–72
 - SWGDE (Scientific Working Group on Digital Evidence), 3
 - switch user option, 287
 - symlinks, 161
 - syslogs, 116–121
 - system boot and initialization
 - reconstruction
 - bootloader analysis, 145–153
 - kernel initialization analysis, 153–161
 - power and physical environment
 - analysis, 175–182
 - systemd analysis, 161–175
 - systemd analysis, 161–175
 - activation and on-demand services, 168
 - overview of, 161
 - systemd initialization process, 164
 - systemd services and daemons, 166
 - systemd unit files, 161
 - systemd journals, 121–129
 - systemd (Linux systems), 20
 - systemd timers, 174
 - system hostname, 186
 - system identification, 184–187
 - distro release information, 185
 - initial steps, 184
 - system hostname, 186
 - unique machine IDs, 186
- ## T
- target audience, xxi
 - thumbnail images, 311–313
 - Thunderbolt devices, 329
 - time and location analysis
 - internationalization, 264
 - Linux and geographic location, 268–272
 - Linux time configuration analysis, 255–264
 - time configuration analysis, 255
 - daylight saving time and leap time, 259
 - time formats, 256
 - timestamps and forensic timelines, 262
 - time synchronization, 260
 - time zones, 257
 - time formats, 256–257
 - timers, 172–175
 - timestamps, 188, 256, 262–264
 - time synchronization, 260–262
 - time zones, 257–259
 - tools. *See* forensics tools and platforms
 - Torvalds, Linus, 12, 14
 - trash cans, 308
 - TRIM command, 32
 - typographical conventions, xxviii

U

- UEFI GRUB booting, 148
- undelete-btrfs tool, 64
- unique machine IDs, 186
- unit configuration files (systemd), 161
- universal package systems, 212
- universal software package analysis,
 - 212–221
 - AppImage, 213
 - Flatpak, 215
 - role of universal packages, 212
 - Snap, 218
 - software centers and GUI frontends, 219
- Unix, 12–14
- user desktops and login activity
 - reconstruction
 - authentication and authorization, 288–303
 - Linux desktop artifacts, 303–317
 - Linux login and session analysis, 273–287
 - user network access, 317–324
- user files, 288–293
- user home directory, 88–93
- user network access, 317–324
 - network shares and cloud services, 321
 - remote desktop access, 320
 - secure shell access, 317

V

- Venema, Wietse, 2
- version numbers, 184

- victims, xix–xxi
- Vinet, Judd, 27
- volume management. *See* storage
 - layout and volume management

W

- wallet managers, 298–300
- Wayland, 281–284
- well-integrated applications, 313–315
- Wi-Fi artifacts, 237–242
- Wikileaks, 3
- WireGuard, 246–248
- wireless network analysis, 237–246
 - areas of interest, 237
 - Bluetooth artifacts, 242
 - Wi-Fi artifacts, 237
 - WWAN artifacts, 244
- WWAN artifacts, 244–246

X

- X11 window system, 281–284
- XDG base directories, 88
- xfstools analysis, 65–69

Y

- YaST (Yet another Setup Tool), 191
- Young, Bob, 27

Z

- zypper tool, 208