CONTENTS IN DETAIL

INTRODUCTION 1

Why I Wrote This Book 2
How This Book Is Unique 2
Linux Forensic Analysis Scenarios 3
Target Audience and Prerequisites 5
Who Should Read This Book? 5
Prerequisite Knowledge 6
Forensic Tools and Platforms Needed 6
Scope and Organization 7
Content Scope 7
Book Organization and Structure 8
Overview of Chapters 10
Conventions and Format 12
Formatting and Presentation 13
Data Flow Diagrams 14

1
DIGITAL FORENSICS OVERVIEW 17

Digital Forensics History 17
Pre-Y2K 18
2000–2010 18
2010–2020 19
2020 and Beyond 20
Forensic Analysis Trends and Challenges 21
Shift in Size, Location, and Complexity of Evidence 21
Multi-Jurisdictional Aspects 22
Industry, Academia, and Law Enforcement Collaboration 22
Principles of Postmortem Computer Forensic Analysis 23
Digital Forensic Standards 23
Peer-Reviewed Research 23
Industry Regulation and Best Practice 24
Special Topics in Forensics 25
Forensic Readiness 25
Anti-Forensics 25

2
LINUX OVERVIEW 27

History of Linux 28

Unix Roots 28
Early Linux Systems 30
Early Desktop Environments 31
Modern Linux Systems 32
Hardware 33
The Kernel 34
Devices 35
Systemd 36
The Command Line 37
Modern Desktop Environments 38
Linux Distributions 39
The Evolution of Linux Distributions 40
Debian-Based Distributions 41
SUSE-Based Distributions 42
Red Hat–Based Distributions 43
Arch-Based Distributions 43
Other Distributions 44
Forensic Analysis of Linux Systems 44

3
EVIDENCE FROM STORAGE DEVICES AND FILESYSTEMS 47

Analysis of Storage Layout and Volume Management 49
Analysis of Partition Tables 49
Logical Volume Manager 53
Linux Software RAID 57
Filesystem Forensic Analysis 60
Linux Filesystem Concepts 60
Forensic Artifacts in Linux Filesystems 62
List and Extract Data 64
An Analysis of ext4 67
Filesystem Metadata: Superblock 67
File Metadata: Inodes 69
List and Extract Files 71
An Analysis of btrfs 72
Filesystem Metadata: Superblock 73
File Metadata: Inodes 75
Multiple Devices and Subvolumes 77
List and Extract Files 80
An Analysis of xfs 81
Filesystem Metadata: Superblock 81
File Metadata: Inodes 83
List and Extract Files 84
Linux Swap Analysis 85
Identifying and Analyzing Swap 85
Hibernation 87
Analyzing Filesystem Encryption 89

LUKS Full-Disk Encryption 90
eCryptfs Encrypted Directories 93
Fscrypt and Ext4 Directory Encryption 96
Summary 98

4
DIRECTORY LAYOUT AND FORENSIC ANALYSIS OF LINUX FILES 99

Linux Directory Layout 99
Filesystem Hierarchy 100
User Home Directory 104
Hashsets and NSRL for Linux 109
Linux File Types and Identification 111
POSIX File Types 111
Magic Strings and File Extensions 113
Hidden Files 114
Linux File Analysis 115
Application Metadata 115
Content Analysis 116
Executable Files 117
Crash and Core Dumps 120
Process Core Dumps 120
Application and Distro-Specific Crash Data 123
Kernel Crashes 125
Summary 130

5
INVESTIGATING EVIDENCE FROM LINUX LOGS 131

Traditional Syslog 132
Syslog Facility, Severity, and Priority 132
Syslog Configuration 134
Analyzing Syslog Messages 135
Systemd Journal 137
Systemd Journal Features and Components 137
Systemd Journal Configuration 138
Analysis of Journal File Contents 141
Other Application and Daemon Logs 145
Custom Logging to Syslog or Systemd Journal 145
Independent Server Application Logs 147
Independent User Application Logs 149
Plymouth Splash Startup Logs 150
Kernel and Audit Logs 151
The Kernel Ring Buffer 152
The Linux Auditing System 155
Summary 159

6
RECONSTRUCTING SYSTEM BOOT AND INITIALIZATION 161

Analysis of Bootloaders 161
- BIOS/MBR GRUB Booting 163
- UEFI GRUB Booting 164
- GRUB Configuration 166
- Other Bootloaders 168

Analysis of Kernel Initialization 169
- Kernel Command Line and Runtime Parameters 170
- Kernel Modules 171
- Kernel Parameters 173
- Analyzing initrd and initramfs 174

Analysis of Systemd 177
- Systemd Unit Files 178
- Systemd Initialization Process 180
- Systemd Services and Daemons 182
- Activation and On-Demand Services 184
- Scheduled Commands and Timers 188

Power and Physical Environment Analysis 191
- Power and Physical Environment Analysis 191
- Sleep, Shutdown, and Reboot Evidence 192
- Human Proximity Indicators 194

Summary 198

7
EXAMINATION OF INSTALLED SOFTWARE PACKAGES 199

System Identification 200
- Distro Release Information 201
- Unique Machine ID 202
- System Hostname 202

Distro Installer Analysis 203
- Debian Installer 204
- Raspberry Pi Raspian 205
- Fedora Anaconda 206
- SUSE YaST 207
- Arch Linux 208

Package File Format Analysis 209
- Debian Binary Package Format 210
- Red Hat Package Manager 214
- Arch Pacman Packages 216

Package Management System Analysis 218
- Debian apt 219
- Fedora dnf 222
- SUSE zypper 224
- Arch pacman 226

Universal Software Package Analysis 228

AppImage 229
Flatpak 231
Snap 234
Software Centers and GUI Frontends 235
Other Software Installation Analysis 237
Manually Compiled and Installed Software 237
Programming Language Packages 238
Application Plug-Ins 239
Summary 239

8
IDENTIFYING NETWORK CONFIGURATION ARTIFACTS 241

Network Configuration Analysis 242
Linux Interfaces and Addressing 242
Network Managers and Distro-Specific Configuration 245
DNS Resolution 247
Network Services 250
Wireless Network Analysis 253
Wi-Fi Artifacts 253
Bluetooth Artifacts 258
WWAN Artifacts 260
Network Security Artifacts 262
WireGuard, IPsec, and OpenVPN 262
Linux Firewalls and IP Access Control 265
Proxy Settings 267
Summary 269

9
FORENSIC ANALYSIS OF TIME AND LOCATION 271

Linux Time Configuration Analysis 271
Time Formats 271
Time Zones 273
Daylight Saving and Leap Time 275
Time Synchronization 276
Timestamps and Forensic Timelines 278
Internationalization 280
Locale and Language Settings 280
Physical Keyboard Layout 282
Linux and Geographic Location 284
Geographic Location History 285
GeoClue Geolocation Service 287
Summary 288

10
RECONSTRUCTING USER DESKTOPS AND LOGIN ACTIVITY 289

- Linux Login and Session Analysis 289
  - Seats and Sessions 291
  - Shell Login 294
  - X11 and Wayland 298
  - Desktop Login 300
- Authentication and Authorization 304
  - User, Group, and Password Files 304
  - Elevated Privileges 309
  - GNOME Keyring 312
  - KDE Wallet Manager 314
  - Biometric Fingerprint Authentication 316
  - GnuPG 317
- Linux Desktop Artifacts 319
  - Desktop Settings and Configuration 319
  - Desktop Clipboard Data 323
  - Desktop Trash Cans 324
  - Desktop Bookmarks and Recent Files 326
  - Desktop Thumbnail Images 328
  - Well-Integrated Desktop Applications 330
  - Other Desktop Forensic Artifacts 331
- User Network Access 333
  - Secure Shell Access 334
  - Remote Desktop Access 336
  - Network Shares and Cloud Services 338
  - Summary 341

11
FORENSIC TRACES OF ATTACHED PERIPHERAL DEVICES 343

- Linux Peripheral Devices 344
  - Linux Device Management 344
  - Identify Attached USB Devices 345
  - Identify PCI and Thunderbolt Devices 347
- Printers and Scanners 348
  - Analysis of Printers and Printing History 349
  - Analysis of Scanning Devices and History 351
- External Attached Storage 352
  - Storage Hardware Identification 353
  - Evidence of Mounted Storage 354
- Summary 355

AFTERWORD 357

APPENDIX A: FILE AND DIRECTORY LIST FOR DIGITAL INVESTIGATORS 361

/ 362
/boot/ 363
- /boot/grub/ 363
- /boot/loader/ 364
- EFI/ 364

/etc/ 364
/home/*/ 369
- XDG and freedesktop directories 369
- .cache/ 370
- .config/ 370
- .local/ 371
- Other Dot Files and Directories 371

/usr/ 372
- /usr/lib/ 372
- /usr/lib/systemd/ 373
- /usr/local/, /usr/opt/ 373
- /usr/share/ 373

/var/ 374
- /var/cache/ 374
- /var/log/ 375
- /var/lib/ 376
- /var/spool/ 377