

BRIEF CONTENTS

Foreword by Eoghan Casey	xvii
Introduction	xix
Chapter 0: Digital Forensics Overview	1
Chapter 1: Storage Media Overview	11
Chapter 2: Linux as a Forensic Acquisition Platform	47
Chapter 3: Forensic Image Formats	59
Chapter 4: Planning and Preparation	69
Chapter 5: Attaching Subject Media to an Acquisition Host	101
Chapter 6: Forensic Image Acquisition	141
Chapter 7: Forensic Image Management	187
Chapter 8: Special Image Access Topics	229
Chapter 9: Extracting Subsets of Forensic Images	259
Closing Remarks	275
Index	277

CONTENTS IN DETAIL

FOREWORD BY EOGHAN CASEY

xvii

INTRODUCTION

xix

Why I Wrote This Book	xix
How This Book Is Different	xx
Why Use the Command Line?	xx
Target Audience and Prerequisites	xxii
Who Should Read This Book?	xxii
Prerequisite Knowledge	xxii
Preinstalled Platform and Software	xxii
How the Book Is Organized	xxii
The Scope of This Book	xxv
Conventions and Format	xxv

0

DIGITAL FORENSICS OVERVIEW

1

Digital Forensics History	1
Pre-Y2K	1
2000–2010	2
2010–Present	3
Forensic Acquisition Trends and Challenges	4
Shift in Size, Location, and Complexity of Evidence	4
Multijurisdictional Aspects	5
Industry, Academia, and Law Enforcement Collaboration	5
Principles of Postmortem Computer Forensics	5
Digital Forensic Standards	6
Peer-Reviewed Research	7
Industry Regulations and Best Practice	8
Principles Used in This Book	9

1

STORAGE MEDIA OVERVIEW

11

Magnetic Storage Media	12
Hard Disks	12
Magnetic Tapes	13
Legacy Magnetic Storage	15

Non-Volatile Memory	15
Solid State Drives	16
USB Flash Drives	17
Removable Memory Cards	17
Legacy Non-Volatile Memory	19
Optical Storage Media	19
Compact Discs	20
Digital Versatile Discs	21
Blu-ray Discs	21
Legacy Optical Storage	22
Interfaces and Physical Connectors	22
Serial ATA	22
Serial Attached SCSI and Fibre Channel	25
Non-Volatile Memory Express	27
Universal Serial Bus	29
Thunderbolt	30
Legacy Interfaces	32
Commands, Protocols, and Bridges	34
ATA Commands	34
SCSI Commands	36
NVME Commands	37
Bridging, Tunneling, and Pass-Through	38
Special Topics	39
DCO and HPA Drive Areas	39
Drive Service and Maintenance Areas	40
USB Attached SCSI Protocol	40
Advanced Format 4Kn	41
NVME Namespaces	44
Solid State Hybrid Disks	45
Closing Thoughts	46

2

LINUX AS A FORENSIC ACQUISITION PLATFORM

47

Linux and OSS in a Forensic Context	48
Advantages of Linux and OSS in Forensics Labs	48
Disadvantages of Linux and OSS in Forensics Labs	49
Linux Kernel and Storage Devices	50
Kernel Device Detection	50
Storage Devices in /dev	51
Other Special Devices	52
Linux Kernel and Filesystems	52
Kernel Filesystem Support	52
Mounting Filesystems in Linux	53
Accessing Filesystems with Forensic Tools	54
Linux Distributions and Shells	55
Linux Distributions	55
The Shell	56

Command Execution	56
Piping and Redirection	56
Closing Thoughts	57

3 FORENSIC IMAGE FORMATS 59

Raw Images	60
Traditional dd	60
Forensic dd Variants	61
Data Recovery Tools	61
Forensic Formats	62
EnCase EWF	62
FTK SMART	62
AFF	62
SquashFS as a Forensic Evidence Container	63
SquashFS Background	63
SquashFS Forensic Evidence Containers	64
Closing Thoughts	67

4 PLANNING AND PREPARATION 69

Maintain an Audit Trail	70
Task Management	70
Shell History	73
Terminal Recorders	75
Linux Auditing	76
Organize Collected Evidence and Command Output	76
Naming Conventions for Files and Directories	76
Scalable Examination Directory Structure	79
Save Command Output with Redirection	81
Assess Acquisition Infrastructure Logistics	83
Image Sizes and Disk Space Requirements	83
File Compression	85
Sparse Files	85
Reported File and Image Sizes	86
Moving and Copying Forensic Images	87
Estimate Task Completion Times	87
Performance and Bottlenecks	88
Heat and Environmental Factors	91
Establish Forensic Write-Blocking Protection	93
Hardware Write Blockers	94
Software Write Blockers	97
Linux Forensic Boot CDs	99
Media with Physical Read-Only Modes	100
Closing Thoughts	100

5 ATTACHING SUBJECT MEDIA TO AN ACQUISITION HOST 101

Examine Subject PC Hardware	101
Physical PC Examination and Disk Removal.....	102
Subject PC Hardware Review	102
Attach Subject Disk to an Acquisition Host	102
View Acquisition Host Hardware	103
Identify the Subject Drive	105
Query the Subject Disk for Information.....	107
Document Device Identification Details	107
Query Disk Capabilities and Features with hdparm.....	108
Extract SMART Data with smartctl.....	112
Enable Access to Hidden Sectors	118
Remove a DCO.....	118
Remove an HPA	121
Drive Service Area Access	122
ATA Password Security and Self-Encrypting Drives	125
Identify and Unlock ATA Password-Protected Disks	126
Identify and Unlock Opal Self-Encrypting Drives.....	128
Encrypted Flash Thumb Drives	131
Attach Removable Media	132
Optical Media Drives	132
Magnetic Tape Drives	133
Memory Cards	136
Attach Other Storage	136
Apple Target Disk Mode.....	137
NVME SSDs.....	138
Other Devices with Block or Character Access	140
Closing Thoughts	140

6 FORENSIC IMAGE ACQUISITION 141

Acquire an Image with dd Tools	142
Standard Unix dd and GNU dd	142
The dcfldd and dc3dd Tools	144
Acquire an Image with Forensic Formats	145
The ewfacquire Tool.....	145
AccessData ftkimager	147
SquashFS Forensic Evidence Container.....	149
Acquire an Image to Multiple Destinations	150
Preserve Digital Evidence with Cryptography.....	150
Basic Cryptographic Hashing	151
Hash Windows	152
Sign an Image with PGP or S/MIME.....	154
RFC-3161 Timestamping.....	157

Manage Drive Failure and Errors	159
Forensic Tool Error Handling	160
Data Recovery Tools	162
SMART and Kernel Errors	163
Other Options for Failed Drives	164
Damaged Optical Discs	165
Image Acquisition over a Network	166
Remote Forensic Imaging with rdd	166
Secure Remote Imaging with ssh	168
Remote Acquisition to a SquashFS Evidence Container	169
Acquire a Remote Disk to EnCase or FTK Format	171
Live Imaging with Copy-On-Write Snapshots	172
Acquire Removable Media	172
Memory Cards	173
Optical Discs	174
Magnetic Tapes	176
RAID and Multidisk Systems	178
Proprietary RAID Acquisition	178
JBOD and RAID-0 Striped Disks	179
Microsoft Dynamic Disks	181
RAID-1 Mirrored Disks	182
Linux RAID-5	183
Closing Thoughts	185

7

FORENSIC IMAGE MANAGEMENT

187

Manage Image Compression	187
Standard Linux Compression Tools	188
EnCase EWF Compressed Format	189
FTK SMART Compressed Format	190
AFFlib Built-In Compression	190
SquashFS Compressed Evidence Containers	191
Manage Split Images	191
The GNU split Command	192
Split Images During Acquisition	192
Access a Set of Split Image Files	194
Reassemble a Split Image	195
Verify the Integrity of a Forensic Image	197
Verify the Hash Taken During Acquisition	197
Recalculate the Hash of a Forensic Image	198
Cryptographic Hashes of Split Raw Images	199
Identify Mismatched Hash Windows	199
Verify Signature and Timestamp	200
Convert Between Image Formats	202
Convert from Raw Images	202
Convert from EnCase/E01 Format	205

Convert from FTK Format	208
Convert from AFF Format	209
Secure an Image with Encryption	211
GPG Encryption	211
OpenSSL Encryption	213
Forensic Format Built-In Encryption	214
General Purpose Disk Encryption	216
Disk Cloning and Duplication	219
Prepare a Clone Disk	219
Use HPA to Replicate Sector Size	219
Write an Image File to a Clone Disk	220
Image Transfer and Storage	221
Write to Removable Media	221
Inexpensive Disks for Storage and Transfer	223
Perform Large Network Transfers	223
Secure Wiping and Data Disposal	224
Dispose of Individual Files	224
Secure Wipe a Storage Device	225
Issue ATA Security Erase Unit Commands	226
Destroy Encrypted Disk Keys	227
Closing Thoughts	228

8 SPECIAL IMAGE ACCESS TOPICS 229

Forensically Acquired Image Files	230
Raw Image Files with Loop Devices	230
Forensic Format Image Files	233
Prepare Boot Images with xmount	235
VM Images	237
QEMU QCOW2	237
VirtualBox VDI	239
VMWare VMDK	240
Microsoft VHD	241
OS-Encrypted Filesystems	243
Microsoft BitLocker	243
Apple FileVault	248
Linux LUKS	251
TrueCrypt and VeraCrypt	254
Closing Thoughts	258

9 EXTRACTING SUBSETS OF FORENSIC IMAGES 259

Assess Partition Layout and Filesystems	259
Partition Scheme	260

Partition Tables	261
Filesystem Identification	263
Partition Extraction	264
Extract Individual Partitions	264
Find and Extract Deleted Partitions	266
Identify and Extract Inter-Partition Gaps	269
Extract HPA and DCO Sector Ranges	269
Other Piecewise Data Extraction	271
Extract Filesystem Slack Space	271
Extract Filesystem Unallocated Blocks	272
Manual Extraction Using Offsets	272
Closing Thoughts	274

CLOSING REMARKS **275**

INDEX **277**