

Table of Contents

Preface	1
Chapter 1: Incident Response	7
The incident response process	8
The role of digital forensics	11
The incident response framework	12
The incident response charter	12
CSIRT	13
CSIRT core team	14
Technical support personnel	16
Organizational support personnel	17
External resources	19
The incident response plan	20
Incident classification	21
The incident response playbook	23
Escalation procedures	25
Maintaining the incident response capability	26
Summary	28
Chapter 2: Forensic Fundamentals	29
Legal aspects	29
Laws and regulations	30
Rules of evidence	31
Digital forensic fundamentals	32
A brief history	32
The digital forensic process	34
Identification	35
Preservation	35
Collection	36
Proper evidence handling	36
Chain of custody	37
Examination	40
Analysis	41
Presentation	41
Digital forensic lab	42
Physical security	42
Tools	43
Hardware	43

Software	46
Jump kit	52
Summary	54
Chapter 3: Network Evidence Collection	55
<hr/>	
Preparation	55
Network diagram	56
Configuration	57
Logs and log management	57
Network device evidence	59
Security information and event management system	61
Security onion	63
Packet capture	64
tcpdump	65
WinPcap and RawCap	68
Wireshark	70
Evidence collection	73
Summary	75
Chapter 4: Acquiring Host-Based Evidence	77
<hr/>	
Preparation	77
Evidence volatility	78
Evidence acquisition	78
Evidence collection procedures	80
Memory acquisition	81
Local acquisition	82
FTK Imager	82
Winpmem	85
Remote acquisition	88
Winpmem	88
F-Response	89
Virtual machines	98
Non-volatile data	99
Summary	100
Chapter 5: Understanding Forensic Imaging	101
<hr/>	
Overview of forensic imaging	101
Preparing a stage drive	104
Imaging	109
Dead imaging	109
Live imaging	120
Imaging with Linux	122

Summary	128
Chapter 6: Network Evidence Analysis	129
<hr/>	
Analyzing packet captures	129
Command-line tools	130
Wireshark	131
Xplico and CapAnalysis	138
Xplico	138
CapAnalysis	142
Analyzing network log files	148
DNS blacklists	150
SIEM	152
ELK Stack	152
Summary	155
Chapter 7: Analyzing System Memory	157
<hr/>	
Memory evidence overview	157
Memory analysis	158
Memory analysis methodology	158
SANS six-part methodology	159
Network connections methodology	160
Tools	160
Redline	160
Volatility	169
Installing Volatility	169
Identifying the image	170
pslist	171
psscan	172
pstree	173
DLLlist	174
Handles	174
svcsan	175
netscan and sockets	176
LDR modules	177
psxview	178
DllDump	179
memdump	181
procdump	183
Rekall	184
imageinfo	185
pslist	186
Event logs	186
Sockets	187
Malfind	187

Summary	189
Chapter 8: Analyzing System Storage	191
<hr/>	
Forensic platforms	191
Autopsy	194
Installing Autopsy	194
Opening a case	194
Navigating Autopsy	201
Examining a Case	204
Web Artifacts	206
Email	209
Attached Devices	210
Deleted Files	212
Keyword Searches	213
Timeline Analysis	215
Registry analysis	219
Summary	224
Chapter 9: Forensic Reporting	225
<hr/>	
Documentation overview	226
What to document	226
Types of documentation	227
Sources	229
Audience	229
Incident tracking	230
Fast incident response	231
Written reports	239
Executive summary	239
Incident report	239
Forensic report	242
Summary	246
Chapter 10: Malware Analysis	247
<hr/>	
Malware overview	248
Malware analysis overview	250
Static analysis	250
Dynamic analysis	252
Analyzing malware	253
Static analysis	254
Pestudio	254
Remnux	258
Dynamic analysis	261
Process Explorer	262

Cuckoo sandbox	263
Summary	270
Chapter 11: Threat Intelligence	271
<hr/>	
Threat intelligence overview	271
Threat intelligence types	274
Threat intelligence methodology	275
Threat intelligence direction	277
Cyber kill chain	278
Diamond model	279
Threat intelligence sources	281
Internally developed sources	281
Commercial sourcing	282
Open source	282
Threat intelligence platforms	283
MISP threat sharing	284
Using threat intelligence	288
Proactive threat intelligence	289
Reactive threat intelligence	291
Autopsy	291
Redline	292
Yara and Loki	294
Summary	299
Index	301
<hr/>	