

SYNGRESS

DIGITAL FORENSICS FOR NETWORK, INTERNET, AND CLOUD COMPUTING

A Forensic Evidence Guide for Moving Targets and Data

Terrence V. Lillard, Clint P. Garrison
Craig A. Schiller, James Steele



Contents

About the Authors	xi
-------------------------	----

PART I INTRODUCTION

CHAPTER 1 What Is Network Forensics?	3
Introduction to Cloud Computing	6
Introduction to the Incident Response Process	10
Investigative and Forensics Methodologies	14
Where Network Forensics Fits In	17
Summary	19
References	20

PART II GATHERING EVIDENCE

CHAPTER 2 Capturing Network Traffic	23
The Importance of DHCP Logs	24
Using tcpdump/WinDump	24
Limitations of tcpdump.....	25
tcpdump Command Line	25
Troubleshooting tcpdump	34
Using Wireshark.....	36
Wireshark GUI.....	37
Limitations of Wireshark.....	42
Limitations of Using Libpcap and Derivatives	43
Wireshark Utilities.....	44
TShark.....	44
Rawshark	46
Dumpcap.....	46
Mergecap	47
Editcap	48
Text2pcap.....	48
Using SPAN Ports or TAPS	48
SPAN Port Issues	49
Network Tap	50
Using Fiddler.....	51
Firewalls	56
Placement of Sensors	57
Summary	58

CHAPTER 3 Other Network Evidence	59
Overview of Botnets and Other Network-Aware Malware	62
The Botnet Life Cycle	63
Temporal, Relational, and Functional Analyses and Victimology	65
First Responder Evidence	67
Sources of Network-Related Evidence	69
Dynamic Evidence Capture	85
Malware Analysis: Using Sandbox Technology	90
Summary	92

PART III ANALYZING EVIDENCE WITH OPEN SOURCE SOFTWARE

CHAPTER 4 Deciphering a TCP Header	95
OSI and TCP Reference Models	96
TCP Header	98
Source Port Number	100
Destination Port Number	101
Sequence Number	101
Acknowledgment Number	102
Data Offset	102
Reserved	103
TCP Flags	103
Windows Size	106
TCP Checksum	106
Urgent Pointer	106
TCP Options	106
Padding	107
Decipherment of a TCP Segment	107
TCP Signature Analysis	108
Summary	111
 CHAPTER 5 Using Snort for Network-Based Forensics	 113
IDS Overview	114
Snort Architecture	116
Real-Time Network Traffic Capturing	118
Playback Binary Network Traffic (pcap Format)	118
Snort Preprocessor Component	118
Snort Detection Engine Component	123
Network Forensics Evidence Generated with Snort	129
Summary	132

PART IV COMMERCIAL NETWORK FORENSICS APPLICATIONS

CHAPTER 6 Commercial NetFlow Applications	135
What Is NetFlow?	135
How Does NetFlow Work?	136
The Benefit of NetFlow	137
NetFlow Collection.....	138
NetFlow User Datagram Protocol (UDP) Datagrams.....	139
NetFlow Header.....	139
Enabling NetFlow	140
Enabling NetFlow v9 (Ingress and Egress)	144
What Is an FNF?	146
Key Advantages	146
Enabling FNF.....	147
What Is an sFlow?.....	151
Enabling sFlow	152
Which Is Better: NetFlow or sFlow?.....	153
Scrutinizer	154
Scaling	154
Scrutinizer Forensics Using Flow Analytics.....	155
Using Flow Analytics to Identify Threats within NetFlow	161
Summary	163
 CHAPTER 7 NetWitness Investigator	 165
Introduction.....	165
NetWitness Investigator Architecture	166
Import/Live Capture Network Traffic	167
Collections	168
Parsers, Feeds, and Rules	169
Navigation Views	172
Data Analysis	174
Exporting Captured Data	176
Summary	177
 CHAPTER 8 SilentRunner by AccessData	 179
History of SilentRunner	179
Parts of the SilentRunner System	181
Installing SilentRunner	184
Stand-Alone Installation	184
Distributed Installation	189

SilentRunner Terminology	191
Graphs.....	191
Spec Files.....	191
Customizing the Analyzer	209
Context Management.....	213
Data Investigator Tools	215
Some Final Tricks and Tips	216
Summary	218
References.....	218

PART V MAKING YOUR NETWORK FORENSICS CASE

CHAPTER 9 Incorporating Network Forensics into Incident Response Plans	221
Investigation Method	222
Incident Response	224
Spearphishing	225
DMCA Violations	244
Web Site Compromise: Search Engine Spam and Phishing	261
Summary	274
References.....	274
 CHAPTER 10 Legal Implications and Considerations	 275
Internet Forensics.....	277
Admissibility of Internet Evidence.....	277
Hearsay Exceptions and Internet Evidence	279
Cloud Forensics	282
Evidence Collection in the Cloud.....	282
Admissibility of Cloud Evidence	284
E-Discovery in the Cloud	286
International Complexities of Internet and Cloud Forensics	288
The Hague Convention on Evidence	292
Privacy	293
Summary	296
References.....	297
Case Law	298
Legislation	299
 CHAPTER 11 Putting It All Together	 301
Network Forensics Examiner Skills.....	301
Network Forensics Investigation Life Cycle.....	302
Summary	315

PART VI THE FUTURE OF NETWORK FORENSICS

CHAPTER 12 The Future of Cloud Computing319

History of Cloud Computing	320
What Drives the Cloud	321
A Break from Dependence on IT to Solve a Business Problem.....	322
The Cloud Is Enabled through Virtualization.....	322
Accelerating Development and Delivery of New Applications	323
Private versus Public Cloud Computing.....	324
Which Cloud Vendors Will Rise to the Top?.....	324
Yes, There Are Risks	326
The Risks Are Worthwhile	326
Will Microsoft and Google Be the 1000-Pound Gorillas of the Cloud?.....	326
The Current State of Cloud Computing	328
Cloud Usage Patterns.....	328
Who Will Host the Cloud?	328
Cloud Computing and Collective Intelligence	329
Security and IT from the Cloud.....	330
Other Widely Used Cloud Applications	331
Cloud Market Size	332
Elements of the Cloud	333
The U.S. Federal Government Is Leading the Movement to the Cloud	334
Rapid Rate of Change.....	334
Common Security Risks of the Current Cloud.....	335
Next Phases of Cloud Computing.....	336
New Database Models Will Greatly Change Product Creation.....	336
Integrated Applications Will Accelerate Cloud Product Creation.....	336
Microsoft Azure Will Enable a Cloud Cottage Industry	337
Other Changes in the New Cloud World	337
Security Improvements in the Future Cloud.....	338
Summary.....	339

CHAPTER 13 The Future of Network Forensics341

Today's Challenges with Existing Devices for Network Forensics	342
Network Forensics Quadrants of Focus	342
Network Forensics Analysis Tools.....	345
Summary.....	347