

Digital Forensics for Network, Internet, and Cloud Computing

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

Technical Editor **Jim Murray**



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

SYNGRESS®

Syngress is an imprint of Elsevier.
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

This book is printed on acid-free paper.

© 2010 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our Web site: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods, they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data/Terrence Lillard ... [et al.].

p. cm.

Includes index.

ISBN 978-1-59749-537-0 (pbk. : alk. paper) 1. Computer crimes—Investigation. 2. Computer security. 3. Computer networks—Security measures. 4. Cloud computing—Security measures. I. Lillard, Terrence.

HV8079.C65D54 2010

363.250285'4678—dc22

2010014493

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-537-0

Printed in the United States of America

10 11 12 13 5 4 3 2 1

Elsevier Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights;
e-mail m.pedersen@elsevier.com

For information on all Syngress publications,
visit our Web site at www.syngress.com

Typeset by: diacriTech, Chennai, India

Working together to grow
libraries in developing countries

www.elsevier.com | www.bookaid.org | www.sabre.org

ELSEVIER

BOOK AID
International

Sabre Foundation

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 Plans221

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 Considerations275

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 Together301

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

INDEX	349
-------------	-----

About the Authors

Lead Author

Terrence V. Lillard (Linux+, CEH, CISSP) is an information technology (IT) security architect and cybercrime and cyberforensics expert. He was a contributing author of the *CompTIA Linux+ Certification Study Guide (Exam XK0-003)* and the *Eleventh Hour Linux+ (Exam XK0-003 Study Guide)*. He is actively involved in computer, intrusion, network, and steganography cybercrime and cyberforensics cases, including investigations, security audits, and assessments – both nationally and internationally. Terrence has testified in U.S. District Court as a computer forensics/security expert witness. He has designed and implemented security architectures for various government, military, and multinational corporations. His background includes positions as principal consultant at Microsoft, the IT Security Operations Manager for the District of Columbia's government IT Security Team, and instructor at the Defense Cyber Crime Center's Computer Investigation Training Academy Program. He has taught IT security and cybercrime/cyberforensics at the undergraduate and graduate level. He holds a BS in electrical engineering and a Master of Business Administration (MBA). In addition, he is currently pursuing a PhD in information security.

Contributors

Clint P. Garrison (MBS/MS, CISSP, CISM) has over 15 years of experience in information security, law enforcement, and digital forensics. He currently manages enterprise security and compliance programs for a Fortune 100 global online retailer and teaches Cyber Crimes and Information Systems Security for the University of Phoenix's graduate degree program. He is a member of several regional working groups dedicated to improving cloud computing security, compliance, and forensics initiatives, and he volunteers as a police officer for a small Texas community.

Clint has a BS in administration of criminal justice from Mountain State University, an MS in IT, and a MBA in information assurance from the University of Dallas. Clint is also a Certified Information System Security Professional (CISSP) and a Certified Information Security Manager (CISM). He also holds an active Master Peace Officer license and Instructor license from the Texas Commission on Law Enforcement Standards and Education.

Craig A. Schiller (CISSP-ISSMP, ISSAP) is the Chief Information Security Officer for Portland State University, an adjunct instructor of security management for Portland State University, an adjunct instructor of digital forensics for Portland Community College, and President of Hawkeye Security Training, LLC. He is the primary author of *Botnets – The Killer Web App* (Syngress, ISBN: 9781597491357) and the first *Generally accepted System Security Principles (GSSP)*. He is a contributing author of several editions of the *Handbook of Information Security Management* and *Data Security Management*. Craig was also a contributor to *Virtualization for Security* (Syngress, ISBN 9781597493055), *Infosecurity*

2008 Threat Analysis (Syngress, ISBN: 9781597492249), *Combating Spyware in the Enterprise* (Syngress, ISBN: 1597490644), and *Winternals Defragmentation, Recovery, and Administration Field Guide* (Syngress, ISBN: 1597490792).

Craig was the senior security engineer and coarchitect of the NASA, Mission Operations AIS Security Engineering Team. He cofounded two ISSA U.S. regional chapters – the Central Plains Chapter and the Texas Gulf Coast Chapter – and is currently the Director of Education for ISSA Portland. He is a Police Reserve Specialist for the Hillsboro Police Department in Oregon.

James “Jim” Steele (CISSP #85790, ACE, DREC, MCSE: Security, Security+) is Manager of Digital Forensics with a large wireless carrier. His responsibilities include performing workstation, server, PDA, cell phone, and network forensics, as well as acting as a liaison to multiple law enforcement agencies, including the United States Secret Service and the FBI. On a daily basis, he investigates cases of fraud, employee integrity, and compromised systems. Jim has a career rich with experience in the security, computer forensics, network development, and management fields. For over 18 years, he has played integral roles regarding project management, systems administration, network administration, and enterprise security management in public safety and mission-critical systems. As a senior technical consultant with iXP assigned to the NYPD E-911 Center, he designed and managed implementation of multiple systems for enterprise security; he also supported operations on-site during September 11, 2001, and the blackout of 2003. Jim has also participated in foreign projects such as the development of the London Metropolitan Police C3i Project, for which he was a member of the Design and Proposal Team. His career as a technical consultant also includes time with the University of Pennsylvania and the FDNY. He is a member of HTCC, NYECTF, InfraGard, and the HTCIA. Jim has contributed to several Syngress books, including *Cyber Crime Investigations: Bridging the Gaps* and *Cisco Router Forensics*.

Technical Editor

Jim Murray is an information security architect for NCCI Holdings, Inc. in Boca Raton, FL. For the past 12 years, he has served in various IT roles at NCCI with a primary focus on network services and information security. Jim currently holds various certifications, including the CISSP, CEH, EnCE, and a number of GIAC certifications from the SANS Institute. He has also served as a local mentor and community instructor for SANS and coauthored the *SANS Securing Linux Step By Step Guide*.