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.

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

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

Typeset by: diacriTech, Chennai, India

Contents

PART IV COMMERCIAL NETWORK FORENSICS APPLICATIONS

PART VI THE FUTURE OF NETWORK FORENSICS

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*.