Job #: 108332

Author Name: Craiger

Title of Book: Advances in Digital

ISBN #: 9780387737416

ADVANCES IN DIGITAL FORENSICS III

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly. National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

ADVANCES IN DIGITAL FORENSICS III

*IFIP International Conference on Digital Forensics,
National Center for Forensic Science, Orlando,
Florida, January 28- January 31, 2007*

Edited by

Philip Craiger

University of Central Florida, Orlando, Florida, USA

Sujeet Sheno

University of Tulsa, Tulsa, Oklahoma, USA

Springer

Library of Congress Control Number: 2007931957

Advances in Digital Forensics III

Edited by P. Craiger and S. Sheno

p. cm. (IFIP International Federation for Information Processing, a Springer Series in Computer Science)

ISSN: 1571-5736 / 1861-2288 (Internet)

ISBN: 13: 978-0-387-73741-6

eISBN: 13: 978-0-387-73742-3

Printed on acid-free paper

Copyright © 2007 by International Federation for Information Processing.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6 5 4 3 2 1

springer.com

Contents

Contributing Authors	ix
Preface	xix
PART I LEGAL ISSUES	
1	
Calibration Testing of Network Tap Devices	3
<i>Barbara Endicott-Popovsky, Brian Chee and Deborah Frincke</i>	
2	
On the Legality of Analyzing Telephone Call Records	21
<i>C. Swenson, C. Adams, A. Whitledge and S. Sheno</i>	
3	
Survey of Law Enforcement Perceptions Regarding Digital Evidence	41
<i>M. Rogers, K. Scarborough, K. Frakes and C. San Martin</i>	
PART II INSIDER THREAT DETECTION	
4	
Insider Threat Analysis Using Information-Centric Modeling	55
<i>D. Ha, S. Upadhyaya, H. Ngo, S. Pramanik, R. Chinchani and S. Mathew</i>	
5	
An Integrated System for Insider Threat Detection	75
<i>Daniel Ray and Phillip Bradford</i>	
PART III ROOTKIT DETECTION	
6	
Analysis of Tools for Detecting Rootkits and Hidden Processes	89
<i>A. Todd, J. Benson, G. Peterson, T. Franz, M. Stevens and R. Raines</i>	

7

- A Method for Detecting Linux Kernel Module Rootkits 107
Doug Wampler and James Graham

PART IV AUTHORSHIP ATTRIBUTION

8

- Future Trends in Authorship Attribution 119
Patrick Juola

9

- The Keyboard Dilemma and Authorship Identification 133
Carole Chaski

PART V FORENSIC TECHNIQUES

10

- Factors Affecting One-Way Hashing of CD-R Media 149
Christopher Marberry and Philip Craiger

11

- Disk Drive I/O Commands and Write Blocking 163
James Lyle, Steven Mead and Kelsey Rider

12

- A New Process Model for Text String Searching 179
Nicole Beebe and Glenn Dietrich

13

- Detecting Steganography Using Multi-Class Classification 193
Benjamin Rodriguez and Gilbert Peterson

14

- Redacting Digital Information from Electronic Devices 205
A. Barclay, L. Watson, D. Greer, J. Hale and G. Manes

PART VI FILE SYSTEM FORENSICS

15

- In-Place File Carving 217
Golden Richard III, Vassil Roussev and Lodovico Marziale

16

- File System Journal Forensics 231
Christopher Swenson, Raquel Phillips and Sujeet Sheno

PART VII NETWORK FORENSICS

- 17
Using Search Engines to Acquire Network Forensic Evidence 247
Robert McGrew and Rayford Vaughn
- 18
A Framework for Investigating Railroad Accidents 255
Mark Hartong, Rajni Goel and Duminda Wijesekera

PART VIII PORTABLE ELECTRONIC DEVICE FORENSICS

- 19
Forensic Analysis of Xbox Consoles 269
Paul Burke and Philip Craiger
- 20
Super-Resolution Video Analysis for Forensic Investigations 281
Ashish Gehani and John Reif

PART IX EVIDENCE ANALYSIS AND MANAGEMENT

- 21
Specializing CRISP-DM for Evidence Mining 303
Jacobus Venter, Alta de Waal and Cornelius Willers
- 22
Applying the Biba Integrity Model to Evidence Management 317
Kweku Arthur, Martin Olivier and Hein Venter

PART X FORMAL METHODS

- 23
Investigating Computer Attacks Using Attack Trees 331
Nayot Poolsapassit and Indrajit Ray
- 24
Attack Patterns: A New Forensic and Design Tool 345
Eduardo Fernandez, Juan Pelaez and Maria Larrondo-Petrie

Contributing Authors

Charles Adams is a Professor of Law at the University of Tulsa, Tulsa, Oklahoma. His research interests include intellectual property law and digital forensics.

Kweku Arthur is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include information assurance and digital forensics.

Alexander Barclay is a Ph.D. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His current research focuses on adaptive access control, file system forensics and bioinformatics security.

Nicole Beebe is a Ph.D. candidate in Information Systems and Technology Management at the University of Texas at San Antonio, San Antonio, Texas. Her research interests include digital forensics, information security and assurance, and data mining.

Joshua Benson is a Captain in the U.S. Air Force. His research interests include digital forensics, software security and cyber operations.

Phillip Bradford is an Assistant Professor of Computer Science at the University of Alabama, Tuscaloosa, Alabama. His research interests include computer security, digital forensics and high performance computing.

Paul Burke is a Senior Digital Evidence Research Assistant at the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include network security, digital forensics and open source operating systems.

Carole Chaski is the President of ALIAS Technology, LLC and the Executive Director of the Institute for Linguistic Evidence, Georgetown, Delaware. She is also an Adjunct Professor of Linguistics at the University of Delaware, Newark, Delaware. Her research interests include authorship identification and validation methods in forensic linguistics.

Brian Chee is the Director of the Advanced Network Computing Laboratory at the School of Ocean and Earth Science and Technology, University of Hawaii, Manoa, Hawaii. He is also a Senior Contributing Editor of InfoWorld. His research interests include network performance and testing methodologies.

Ramkumar Chinchani is a Senior Software Engineer with Cisco Systems, San Jose, California. His research interests include information security, programming languages and operating systems.

Philip Craiger is an Assistant Professor of Engineering Technology and Assistant Director for Digital Evidence at the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include digital forensics and information security.

Alta de Waal is a Senior Researcher at the Council for Scientific and Industrial Research, Pretoria, South Africa. Her research interests include text modeling, Bayesian analysis, computational methods for Bayesian inference and nonparametric Bayesian analysis.

Glenn Dietrich is an Associate Professor and Chair of Information Systems and Technology Management at the University of Texas at San Antonio, San Antonio, Texas. His research interests include digital forensics, information assurance, systems theory and innovation.

Barbara Endicott-Popovsky is the Director of the Center for Information Assurance and Cybersecurity at the University of Washington, Seattle, Washington. She has a joint faculty appointment with the Information School at the University of Washington at Seattle, and the Department of Computer Science at the University of Washington, Tacoma, Washington. Her research interests include network forensics, critical infrastructure protection and secure coding practices.

Eduardo Fernandez is a Professor of Computer Science and Engineering at Florida Atlantic University, Boca Raton, Florida. His research interests include data security, object-oriented design, fault-tolerant systems and security patterns.

Kelli Frakes is a Research Project Manager with the Justice and Safety Center at Eastern Kentucky University, Richmond, Kentucky. Her research interests include intelligence-led policing, cyber crime and digital evidence.

Timothy Franz is a Major in the U.S. Air Force and a graduate student at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. His research interests are in the area of cyberspace operations.

Deborah Frincke is the Chief Scientist for Cyber Security Research in the Computational Sciences Directorate at Pacific Northwest National Laboratory, Richland, Washington. Her research interests include very large system defense, forensics, infrastructure protection, security visualization, SCADA security and information assurance education.

Ashish Gehani is an I3P Postdoctoral Fellow at SRI's Computer Science Laboratory in Menlo Park, California. His research interests include multimedia protection, sensor and storage network security, intrusion response and DNA computing.

Rajni Goel is an Assistant Professor of Information Systems and Decision Sciences at Howard University, Washington, DC. Her research interests include information assurance, digital forensics, control systems security and data mining.

James Graham is the Henry Vogt Professor of Computer Science and Engineering at the University of Louisville, Louisville, Kentucky. His research interests include information security, digital forensics, critical infrastructure protection, high performance computing and intelligent systems.

David Greer is a Ph.D. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include digital forensics, cyber law, and information security education and training.

Duc Ha is a Ph.D. student in Computer Science and Engineering at the University at Buffalo, Buffalo, New York. His research interests include information assurance, network security, distributed and source-based routing systems.

John Hale is an Associate Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include enterprise security management, applied formal methods, access control and multi-stage attack analysis.

Mark Hartong is a Senior Electronics Engineer with the Office of Safety, Federal Railroad Administration, U.S. Department of Transportation, Washington, DC, and a Ph.D. student in Information Technology at George Mason University, Fairfax, Virginia. His current research focuses on various aspects of software engineering, software systems safety, information assurance, control systems security and digital forensics.

Patrick Juola is an Associate Professor of Computer Science at Duquesne University, Pittsburgh, Pennsylvania. His research interests include humanities computing, computational psycholinguistics, and digital and linguistic forensics.

Maria Larrondo-Petrie is the Associate Dean of Academic and International Affairs and Professor of Computer Science and Engineering at Florida Atlantic University, Boca Raton, Florida. Her research interests include software engineering, data security, formal methods and parallel processing.

James Lyle is a Computer Scientist at the National Institute of Standards and Technology in Gaithersburg, Maryland. His research interests include digital forensics and forensic tool testing.

Gavin Manes is the President of Oklahoma Digital Forensics Professionals, Inc., Tulsa, Oklahoma. He is also a Research Assistant Professor with the Center for Information Security at the University of Tulsa, Tulsa, Oklahoma. His research interests include digital forensics and critical infrastructure protection.

Christopher Marberry is a Senior Digital Evidence Research Assistant at the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include digital forensics, computer security and virtualization technologies.

Lodovico Marziale is a Ph.D. student in Computer Science at the University of New Orleans, New Orleans, Louisiana. His research area is digital forensics.

Sunu Mathew is a Ph.D. student in Computer Science and Engineering at the University at Buffalo, Buffalo, New York. His current research interests include various aspects of information assurance and network security.

Robert McGrew is a Ph.D. student in Computer Science at Mississippi State University, Mississippi State, Mississippi. His research interests include honeypots and attack profiling.

Steven Mead is a Computer Scientist at the National Institute of Standards and Technology in Gaithersburg, Maryland. His research interests include digital forensics and forensic tool testing.

Hung Ngo is an Assistant Professor of Computer Science and Engineering at the University at Buffalo, Buffalo, New York. His research interests include computer networks, network security, algorithms and combinatorics.

Martin Olivier is a Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include privacy, database security and digital forensics.

Juan Pelaez is a Research Scientist with the U.S. Army Research Laboratory in Adelphi, Maryland. He is also a Ph.D. student in Computer Science and Engineering at Florida Atlantic University, Boca Raton, Florida. His research interests include VoIP networks and network forensics.

Gilbert Peterson is an Assistant Professor of Electrical and Computer Engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. His research interests include digital forensics, steganography, image processing, robotics and machine learning.

Raquel Phillips is an undergraduate student in Computer Science and Mathematics at the University of Tulsa, Tulsa, Oklahoma. Her research interests include various aspects of digital forensics, file systems and parallel processing.

Nayot Poolsapassit is a Ph.D. student in Computer Science at Colorado State University, Fort Collins, Colorado. His research interests include information security, attack modeling and intrusion detection.

Suranjan Pramanik is a Ph.D. student in Computer Science and Engineering at the University at Buffalo, Buffalo, New York. His research interests include fault-tolerant systems, anomaly detection, insider threats and binary translation.

Richard Raines is an Associate Professor of Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. His research interests include computer and communications network security and vulnerability analysis.

Daniel Ray is a Ph.D. student in Computer Science at the University at Alabama, Tuscaloosa, Alabama. His research interests include various aspects of digital forensics and computer security.

Indrajit Ray, Chair, IFIP Working Group 11.9 on Digital Forensics, is an Assistant Professor of Computer Science at Colorado State University, Fort Collins, Colorado. His research interests are in the areas of information security, security protocols, digital forensics and database systems.

John Reif is the A. Hollis Edens Professor of Computer Science at Duke University, Durham, North Carolina. His research interests span biomolecular computation, nanostructure fabrication, parallel and randomized algorithms, data compression and quantum computing.

Golden Richard III is an Associate Professor of Computer Science at the University of New Orleans, New Orleans, Louisiana, and the co-founder of Digital Forensics Solutions, LLC, New Orleans, Louisiana. His research interests include digital forensics, mobile computing and operating systems internals.

Kelsey Rider is currently on leave from the National Institute of Standards and Technology, Gaithersburg, Maryland, pursuing graduate studies in Mathematics at the University of Nice, Nice, France. His research interests include digital forensics and forensic tool testing.

Benjamin Rodriguez is a Ph.D. student in Electrical and Computer Engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. His research interests include digital forensics, digital signal processing, digital image and video processing, steganography and steganalysis.

Marcus Rogers is a Professor of Computer and Information Technology at Purdue University, West Lafayette, Indiana. His research interests include psychological digital crime scene analysis, applied behavioral profiling and digital evidence process models.

Vassil Roussev is an Assistant Professor of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests include digital forensics, high-performance computing, distributed collaboration and software engineering.

Cristina San Martin received her M.S. degree in Computer and Information Technology from Purdue University, West Lafayette, Indiana. Her research interests include computer forensics, network security and wireless networks.

Kathryn Scarborough is a Professor of Safety, Security and Emergency Management and the Coordinator of the Homeland Security Degree Program at Eastern Kentucky University, Richmond, Kentucky. Her research interests include law enforcement technologies, cyber crime and security, intelligence and police administration.

Sujeet Shenoi is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include information assurance, digital forensics, critical infrastructure protection and intelligent control.

Michael Stevens is a graduate student in Cyber Operations at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. His research interests are in the areas of information security and digital forensics.

Christopher Swenson is a Ph.D. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include cryptanalysis, network security and digital forensics.

Adam Todd is an M.S. student at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. His research interests include digital forensics and intrusion detection.

Shambhu Upadhyaya is an Associate Professor of Computer Science and Engineering at the University at Buffalo, Buffalo, New York. His research interests are in the areas of information assurance, computer security, fault diagnosis, fault tolerant computing and VLSI testing.

Rayford Vaughn is the Billy J. Ball Professor of Computer Science and Engineering and a William L. Giles Distinguished Professor at Mississippi State University, Mississippi State, Mississippi. His research interests include information assurance and high performance computing.

Hein Venter is a Senior Lecturer in the Department of Computer Science, University of Pretoria, Pretoria, South Africa. His research interests include network security, digital forensics and intrusion detection systems.

Jacobus Venter is a Senior Researcher at the Council for Scientific and Industrial Research, Pretoria, South Africa. His research interests include digital forensics training, evidence mining and probabilistic methods.

Doug Wampler is a Ph.D. student in Computer Engineering and Computer Science at the University of Louisville, Louisville, Kentucky. His research interests include digital forensics, information assurance and legacy systems.

Lance Watson is the Vice President of Client Relations at Oklahoma Digital Forensics Professionals, Inc., Tulsa, Oklahoma, and a Ph.D. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include digital forensics and network security.

Anthony Whitley is an attorney who is retired from the U.S. Department of Justice and the Internal Revenue Service. His research interests include digital forensics, data mining and the application of technology to civil and criminal litigation.

Duminda Wijesekera is an Associate Professor of Information and Software Engineering at George Mason University, Fairfax, Virginia. His research interests include information, network, telecommunications and control systems security.

Cornelius Willers is a Senior Researcher at the Council for Scientific and Industrial Research, Pretoria, South Africa. His research interests include artificial intelligence and intelligent agents.

Preface

In 2006, the Federal Bureau of Investigation (FBI) processed more than two petabytes of digital evidence; in 2007, the volume of digital evidence processed will exceed four petabytes. Electronic devices are becoming smaller and more diverse; memory capacities are increasing according to Moore's Law; distributed networks are growing massively in size and scale. As society embraces new technologies and applications with gusto, digital information will become even more pervasive.

Digital investigations already involve searching for the proverbial needle in the haystack. In five years, possibly sooner, investigators will have to find the one needle in unimaginably large stacks of needles. How will the FBI approach digital investigations of the future? How will state and local law enforcement agents cope?

Digital forensics – the scientific discipline focused on the acquisition, preservation, examination, analysis and presentation of digital evidence – will have to provide solutions. The digital forensics research community must initiate serious efforts to develop the next generation of algorithms, procedures and tools that will be desperately needed.

This book, *Advances in Digital Forensics III*, is the third volume in the annual series produced by the IFIP Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in the emerging discipline of digital forensics. The book presents original research results and innovative applications in digital forensics. Also, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

This volume contains twenty-four edited papers from the Third Annual IFIP WG 11.9 Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, January 28–31, 2007. The papers were selected from forty-one submissions, which were refereed by members of IFIP Working Group 11.9 and other internationally-recognized experts in digital forensics.

The chapters are organized into ten sections: legal issues, insider threat detection, rootkit detection, authorship attribution, forensic techniques, file system forensics, network forensics, portable electronic device forensics, evidence analysis and management, and formal methods. The coverage of topics highlights the richness and vitality of the discipline, and offers promising avenues for future research in digital forensics.

This book is the result of the combined efforts of several individuals. In particular, we thank Anita Presley and Christopher Swenson for their tireless work on behalf of IFIP Working Group 11.9. We also acknowledge the support provided by the National Center for Forensic Science, Orlando, Florida, the FBI, the National Security Agency and the U.S. Secret Service.

PHILIP CRAIGER AND SUJEET SHENOI