

Editor-in-Chief

*A. Joe Turner, Seneca, SC, USA*

Editorial Board

Foundations of Computer Science

*Mike Hinchey, Lero, Limerick, Ireland*

Software: Theory and Practice

*Michael Goedicke, University of Duisburg-Essen, Germany*

Education

*Arthur Tatnall, Victoria University, Melbourne, Australia*

Information Technology Applications

*Ronald Waxman, EDA Standards Consulting, Beachwood, OH, USA*

Communication Systems

*Guy Leduc, Université de Liège, Belgium*

System Modeling and Optimization

*Jacques Henry, Université de Bordeaux, France*

Information Systems

*Jan Pries-Heje, Roskilde University, Denmark*

ICT and Society

*Jackie Phahlamohlaka, CSIR, Pretoria, South Africa*

Computer Systems Technology

*Paolo Prinetto, Politecnico di Torino, Italy*

Security and Privacy Protection in Information Processing Systems

*Kai Rannenber, Goethe University Frankfurt, Germany*

Artificial Intelligence

*Tharam Dillon, Curtin University, Bentley, Australia*

Human-Computer Interaction

*Annelise Mark Pejtersen, Center of Cognitive Systems Engineering, Denmark*

Entertainment Computing

*Ryohei Nakatsu, National University of Singapore*

## **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 also 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 about information processing 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.

Gilbert Peterson Sujeet Shenoj (Eds.)

# Advances in Digital Forensics IX

9th IFIP WG 11.9 International Conference  
on Digital Forensics  
Orlando, FL, USA, January 28-30, 2013  
Revised Selected Papers



Springer

## Volume Editors

Gilbert Peterson

Air Force Institute of Technology

Wright-Patterson Air Force Base, OH 45433-7765, USA

E-mail: gilbert.peterson@afit.edu

Sujeet Sheno

University of Tulsa

Tulsa, OK 74104-3189, USA

E-mail: sujeet@utulsa.edu

ISSN 1868-4238

e-ISSN 1868-422X

ISBN 978-3-642-41147-2

e-ISBN 978-3-642-41148-9

DOI 10.1007/978-3-642-41148-9

Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013948502

CR Subject Classification (1998): K.6.5, K.4, J.1, E.3, H.3, C.2, E.5, H.2.7, F.2

© IFIP International Federation for Information Processing 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Contents

Contributing Authors	ix
Preface	xix
PART I THEMES AND ISSUES	
1	
History, Historiography and the Hermeneutics of the Hard Drive <i>Mark Pollitt</i>	3
2	
Protecting Third Party Privacy in Digital Forensic Investigations <i>Wynand van Staden</i>	19
3	
On the Scientific Maturity of Digital Forensics Research <i>Martin Olivier and Stefan Gruner</i>	33
PART II FORENSIC MODELS	
4	
Cognitive Approaches for Digital Forensic Readiness Planning <i>Antonio Pooe and Les Labuschagne</i>	53
5	
A Harmonized Process Model for Digital Forensic Investigation Readiness <i>Aleksandar Valjarevic and Hein Venter</i>	67
6	
Evaluation of the Semi-Automated Crime-Specific Digital Triage Process Model <i>Gary Cantrell and David Dampier</i>	83

## PART III FORENSIC TECHNIQUES

7

- Reducing the Time Required for Hashing Operations 101  
*Frank Breitinger and Kaloyan Petrov*

8

- Hash-Based File Content Identification Using Distributed Systems 119  
*York Yannikos, Jonathan Schluessler, Martin Steinebach,  
Christian Winter and Kalman Graffi*

9

- Creating Super Timelines in Windows Investigations 135  
*Stephen Esposito and Gilbert Peterson*

10

- Log File Analysis with Context-Free Grammars 145  
*Gregory Bosman and Stefan Gruner*

11

- Using a Goal-Driven Approach in the Investigation of a Questioned  
Contract 153  
*Clive Blackwell, Shareeful Islam and Benjamin Aziz*

## PART IV FILESYSTEM FORENSICS

12

- File Fragment Analysis Using Normalized Compression Distance 171  
*Stefan Axelsson, Kamran Ali Bajwa and Mandhapati Venkata Srikanth*

13

- Quantifying Windows File Slack Size and Stability 183  
*Martin Mulazzani, Sebastian Neuner, Peter Kieseberg, Markus Huber,  
Sebastian Schrittwieser and Edgar Weippl*

14

- Automating Video File Carving and Content Identification 195  
*York Yannikos, Nadeem Ashraf, Martin Steinebach and  
Christian Winter*

15

- Data Recovery from Proprietary-Formatted CCTV Hard Disks 213  
*Aswami Ariffin, Jill Slay and Kim-Kwang Choo*

## PART V NETWORK FORENSICS

- 16  
Creating Integrated Evidence Graphs for Network Forensics 227  
*Changwei Liu, Anoop Singhal and Duminda Wijesekera*
- 17  
A Generic Bayesian Belief Model for Similar Cyber Crimes 243  
*Hayson Tse, Kam-Pui Chow and Michael Kwan*
- 18  
An Empirical Study Profiling Internet Pirates 257  
*Pierre Lai, Kam-Pui Chow, Xiao-Xi Fan and Vivien Chan*
- 19  
Real-Time Covert Timing Channel Detection in Networked Virtual 273  
Environments  
*Anyi Liu, Jim Chen and Harry Wechsler*

## PART VI CLOUD FORENSICS

- 20  
Impact of Cloud Computing on Digital Forensic Investigations 291  
*Stephen O'Shaughnessy and Anthony Keane*
- 21  
Rule-Based Integrity Checking of Interrupt Descriptor Tables in 305  
Cloud Environments  
*Irfan Ahmed, Aleksandar Zoranic, Salman Javaid, Golden Richard III  
and Vassil Roussev*

## PART VII FORENSIC TOOLS

- 22  
Comparison of the Data Recovery Function of Forensic Tools 331  
*Joe Buchanan-Wollaston, Tim Storer and William Glisson*
- 23  
Security Analysis and Decryption of FileVault 2 349  
*Omar Choudary, Felix Grobert and Joachim Metz*

## PART VIII ADVANCED FORENSIC TECHNIQUES

24

Detecting Counterfeit Currency and Identifying its Source 367  
*Ankit Sarkar, Robin Verma and Gaurav Gupta*

25

Towards Active Linguistic Authentication 385  
*Patrick Juola, John Noecker Jr., Ariel Stolerman, Michael Ryan,  
Patrick Brennan and Rachel Greenstadt*



## Contributing Authors

**Irfan Ahmed** is a Postdoctoral Research Associate in the Department of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests include malware detection and analysis, digital forensics and operating systems internals.

**Aswami Ariffin** is a Ph.D. student in Digital Forensics at the University of South Australia, Adelaide, Australia. His research interests include digital forensics and computer security.

**Nadeem Ashraf** is a Security Consultant at ABM Info Tech, Islamabad, Pakistan. His research interests include digital forensics and network security.

**Stefan Axelsson** is a Senior Lecturer of Computer Science at the Blekinge Institute of Technology, Karlskrona, Sweden. His research interests include digital forensics, intrusion and fraud detection, visualization and digital surveillance.

**Benjamin Aziz** is a Senior Lecturer of Computer Security at the University of Portsmouth, Portsmouth, United Kingdom. His research interests include security and trust management, formal methods and requirements engineering, digital forensics and cloud computing.

**Kamran Ali Bajwa** is a Software Developer at Tabaq Software, Lahore, Pakistan. His research interests include digital forensics.

**Clive Blackwell** is a Research Fellow in Digital Forensics at Oxford Brookes University, Oxford, United Kingdom. His research interests include the application of software engineering and formal methods to digital forensics and information security.

**Gregory Bosman** was a graduate student in the Department of Computer Science, University of Pretoria, Pretoria, South Africa. His research interests include formal methods and computer security.

**Frank Breitingner** is a Ph.D. student in Computer Science at the University of Applied Sciences, Darmstadt, Germany; and a Researcher at the Center for Advanced Security Research Darmstadt (CASED), Darmstadt, Germany. His research interests include digital forensics, file analysis and similarity hashing.

**Patrick Brennan** is the President of Juola and Associates, Pittsburgh, Pennsylvania. His research interests include digital forensics and stymometry.

**Joe Buchanan-Wollaston** is a Research Assistant in the School of Computing Science, University of Glasgow, Glasgow, United Kingdom. His research interests include digital forensics and e-discovery.

**Gary Cantrell** is an Associate Professor of Criminal Justice and a Digital Forensics Examiner at the Southwest Regional Cyber Crime Institute, Dixie State University, St. George, Utah. His research interests include digital forensics, computer security and software engineering.

**Vivien Chan** is a Research Project Manager at the University of Hong Kong, Hong Kong, China. Her research interests include cyber criminal profiling and digital forensics.

**Jim Chen** is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research includes graphics, visualization, simulation and networked virtual environments.

**Kim-Kwang Choo** is a Senior Lecturer of Forensic Computing at the University of South Australia, Adelaide, Australia. His research interests include cyber crime and digital forensics.

**Omar Choudary** is a Ph.D. student in Computer Science at the University of Cambridge, Cambridge, United Kingdom. His research interests include authentication, payment protocol security, applied cryptography, hardware security and digital communications.

**Kam-Pui Chow** is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include information security, digital forensics, live system forensics and digital surveillance.

**David Dampier** is a Professor of Computer Science and Engineering, Director of the Center for Computer Security Research, and Director of the National Forensics Training Center at Mississippi State University, Mississippi State, Mississippi. His research interests include digital forensics, information assurance and software engineering.

**Stephen Esposito** received his M.S. degree in Cyber Warfare from the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensics and computer network operations.

**Xiao-Xi Fan** is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include digital forensics, digital profiling and data mining.

**William Glisson** is the Director of the Digital Forensics Laboratory and a Lecturer of Computer Forensics at the University of Glasgow, Glasgow, United Kingdom. His research interests include digital forensics and information security methods and practices in organizations.

**Kalman Graffi** is an Assistant Professor of Computer Science at the University of Dusseldorf, Dusseldorf, Germany. His research interests include distributed systems, social networks and security.

**Rachel Greenstadt** is an Assistant Professor of Computer Science at Drexel University, Philadelphia, Pennsylvania. Her research centers on the privacy and security properties of multi-agent systems and the economics of electronic privacy and information security.

**Felix Grobert** is an Information Security Engineer at Google in Zurich, Switzerland. His research interests include browser security, Mac OS X security and fuzz testing.

**Stefan Gruner** is an Associate Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include software science, formal methods and the philosophy of science.

**Gaurav Gupta** is an Assistant Professor of Computer Science at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include digital forensics, digitized document fraud detection and mobile device forensics.

**Markus Huber** is a Ph.D. student in Computer Science at Vienna University of Technology, Vienna, Austria; and a Computer Security Researcher at SBA Research, Vienna, Austria. His research focuses on security and privacy issues in social networks.

**Shareeful Islam** is a Lecturer of Secure Software Systems at the University of East London, London, United Kingdom. His research interests include risk management, requirements engineering, security, privacy, digital forensics and cloud computing.

**Salman Javaid** is a Ph.D. student in Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests include digital forensics, malware analysis, security and privacy in cloud environments, and network penetration testing.

**Patrick Juola** is a Founder and Chief Executive Officer of Juola and Associates, Pittsburgh, Pennsylvania; and an Associate Professor of Computer Science at Duquesne University, Pittsburgh, Pennsylvania. His research interests include humanities computing, computational psycholinguistics, and digital and linguistic forensics.

**Anthony Keane** is the Head of Research of the Information Security and Digital Forensics Group at the Institute of Technology Blanchardstown, Dublin, Ireland. His research interests include digital forensics, cyber security, and distributed and mobile systems.

**Peter Kieseberg** received an M.Sc. degree in Computer Science from Vienna University of Technology, Vienna, Austria. His research interests include digital forensics, cryptography and mobile security.

**Michael Kwan** is an Honorary Assistant Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics, digital evidence evaluation and the application of probabilistic models in digital forensics.

**Les Labuschagne** is the Executive Director of Research at the University of South Africa, Pretoria, South Africa. His research interests include project management and information security.

**Pierre Lai** is an Instructor of Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include cryptography, peer-to-peer networks and digital forensics.

**Anyi Liu** is an Assistant Professor of Computer Science at Indiana University-Purdue University Fort Wayne, Fort Wayne, Indiana. His research interests include information security and digital forensics.

**Changwei Liu** is a Ph.D. student in Computer Science at George Mason University, Fairfax, Virginia. Her research interests include computer security and network forensics.

**Joachim Metz** is an Information Security Engineer at Google in Zurich, Switzerland. His research interests include incident response and digital forensics.

**Martin Mulazzani** is a Ph.D. student in Computer Science at Vienna University of Technology, Vienna, Austria; and a Computer Security Researcher at SBA Research, Vienna, Austria. His research interests include privacy, digital forensics and applied security.

**Sebastian Neuner** is an M.Sc. student in Software Engineering and Internet Computing at Vienna University of Technology, Vienna, Austria; and a Computer Security Researcher at SBA Research, Vienna, Austria. His research interests include vulnerability discovery, penetration testing and digital forensics.

**John Noecker Jr.** is a Founder and Staff Scientist at Juola and Associates, Pittsburgh, Pennsylvania. His research interests include authorship attribution, author profiling and distractorless authorship verification technology.

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

**Stephen O'Shaughnessy** is a Researcher in the Information Security and Digital Forensics Group at the Institute of Technology Blanchardstown, Dublin, Ireland. His research interests include digital forensics, cyber security, advanced data mining techniques and data analytics.

**Gilbert Peterson**, Vice Chair, IFIP Working Group 11.9 on Digital Forensics, is an Associate Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensics and statistical machine learning.

**Kaloyan Petrov** is a Programmer at the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences, Sofia, Bulgaria. His research interests include parallel programming, multicore architectures and distributed computing.

**Mark Pollitt**, Chair, IFIP Working Group 11.9 on Digital Forensics, is an Associate Professor of Engineering Technology at Daytona State College, Daytona Beach, Florida. His research interests include digital forensics, textual and narrative theory, and knowledge management.

**Antonio Poee** is a Ph.D. student in Information Systems at the University of South Africa, Pretoria, South Africa; and an Information Security Researcher at Exactech Forensics, Provo, Utah. His research interests include digital forensics, forensic readiness and information security.

**Golden Richard III** is a Professor of Computer Science and a University Research Professor at the University of New Orleans, New Orleans, Louisiana. His research interests include digital forensics, reverse engineering, malware analysis and operating systems internals.

**Vassil Roussev** is an Associate Professor of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests are in the area of large-scale digital forensics, particularly performance, scalability, automated sampling and triage, and visual analytics support.

**Michael Ryan** is a Founder and Staff Scientist at Juola and Associates, Pittsburgh, Pennsylvania. His research interests include text analysis, high performance computing and systems architecture.

**Ankit Sarkar** is a B.Tech. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include image processing and its applications to digital forensics.

**Jonathan Schuessler** is a Software Development Engineer at Vector Informatik, Stuttgart, Germany. His research interests include distributed systems and information retrieval.

**Sebastian Schrittwieser** is a Ph.D. candidate in Computer Science at Vienna University of Technology, Vienna, Austria; and a Researcher at SBA Research, Vienna, Austria. His research interests include digital forensics, software protection and code obfuscation.

**Anoop Singhal** is a Senior Computer Scientist in the Computer Security Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include network security, web services security, databases and data mining systems.

**Jill Slay** is the Executive Dean of Information Technology at Namibia University of Science and Technology, Windhoek, Namibia; and a Professor of Forensic Computing at the University of South Australia, Adelaide, Australia. Her research interests include information assurance, digital forensics and critical infrastructure protection.

**Mandhapati Venkata Srikanth** is an M.Sc. student in Computer Science at the Blekinge Institute of Technology, Karlskrona, Sweden. His research interests include digital forensics.

**Martin Steinebach** is the Head of Media Security and IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include digital watermarking and robust hashing.

**Ariel Stoleran** is a Ph.D. student in Computer Science at Drexel University, Philadelphia, Pennsylvania. His research interests include security and privacy, applied machine learning and text analysis.

**Tim Storer** is a Lecturer of Software Engineering at the University of Glasgow, Glasgow, United Kingdom. His research interests include software and software-based system dependability.

**Hayson Tse** is a Computer Science Researcher at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics, artificial intelligence and law.

**Aleksandar Valjarevic** is a Ph.D. student in Computer Science at the University of Pretoria, Pretoria, South Africa; and System Integration Team Leader at Vlatacom Research and Development Center, Belgrade, Serbia. His research interests include information systems security and digital forensics.

**Wynand van Staden** is a Senior Lecturer of Computer Science at the University of South Africa, Florida Park, South Africa. His research interests include digital forensics, anonymity and privacy.

**Hein Venter** is an Associate Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics, with a current focus on the standardization of the digital forensic investigation process.

**Robin Verma** is a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include digitized document fraud detection, mobile device forensics and cloud forensics.



**Harry Wechsler** is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research interests include cyber security, biometrics, machine learning and data mining.

**Edgar Weippl** is the Research Director at SBA Research, Vienna, Austria; and an Associate Professor of Computer Science at Vienna University of Technology, Vienna, Austria. His research focuses on information security and e-learning.

**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.

**Christian Winter** is a Research Associate in IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include statistical forensics and fuzzy hashing.

**York Yannikos** is a Research Associate in IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include digital forensic tool testing, synthetic test data generation and multimedia file carving.

**Aleksandar Zoranic** is a Ph.D. student of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests are in the area of cloud security and live forensics via virtualization introspection, particularly memory analysis through introspection and kernel memory malware detection.

# Preface

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every type of crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in information assurance – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems.

This book, *Advances in Digital Forensics IX*, is the ninth volume in the annual series produced by 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 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-five edited papers from the Ninth IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, January 28–30, 2013. The papers were refereed by members of IFIP Working Group 11.9 and other internationally-recognized experts in digital forensics.

The chapters are organized into eight sections: themes and issues, forensic models, forensic techniques, filesystem forensics, network forensics, cloud forensics, forensic tools and advanced forensic techniques. 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 Mark Pollitt and Jane Pollitt for their tireless work on behalf of IFIP Working Group 11.9. We also acknowledge the support provided by the National Science Foundation, National Secu-

riety Agency, Immigration and Customs Enforcement, Internal Revenue Service and U.S. Secret Service.

GILBERT PETERSON AND SUJEET SHENOI