



Advances in Digital Forensics XVI

Gilbert Peterson, Sujeet Shenoï

► To cite this version:

Gilbert Peterson, Sujeet Shenoï. Advances in Digital Forensics XVI: 16th IFIP WG 11.9 International Conference New Delhi, India, January 6–8, 2020. Springer International Publishing, AICT-589, 2020, IFIP Advances in Information and Communication Technology, 978-3-030-56223-6. hal-03657590

HAL Id: hal-03657590

<https://inria.hal.science/hal-03657590>

Submitted on 3 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.




Distributed under a Creative Commons Attribution 4.0 International License

Editor-in-Chief

Kai Rannenber, Goethe University Frankfurt, Germany

Editorial Board Members

TC 1 – Foundations of Computer Science

Luís Soares Barbosa , University of Minho, Braga, Portugal

TC 2 – Software: Theory and Practice

Michael Goedicke, University of Duisburg-Essen, Germany

TC 3 – Education

Arthur Tatnall , Victoria University, Melbourne, Australia

TC 5 – Information Technology Applications

Erich J. Neuhold, University of Vienna, Austria

TC 6 – Communication Systems

Burkhard Stiller, University of Zurich, Zürich, Switzerland

TC 7 – System Modeling and Optimization

Fredi Tröltzsch, TU Berlin, Germany

TC 8 – Information Systems

Jan Pries-Heje, Roskilde University, Denmark


TC 9 – ICT and Society

David Kreps , University of Salford, Greater Manchester, UK

TC 10 – Computer Systems Technology

Ricardo Reis , Federal University of Rio Grande do Sul, Porto Alegre, Brazil


TC 11 – Security and Privacy Protection in Information Processing Systems

Steven Furnell , Plymouth University, UK

TC 12 – Artificial Intelligence

Eunika Mercier-Laurent , University of Reims Champagne-Ardenne, Reims, France

TC 13 – Human-Computer Interaction

Marco Winckler , University of Nice Sophia Antipolis, France

TC 14 – Entertainment Computing

Rainer Malaka, University of Bremen, Germany

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. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

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 generally smaller and occasionally 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.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at <http://www.springer.com/series/6102>

Gilbert Peterson · Sujeet Shenoj (Eds.)

Advances in Digital Forensics XVI

16th IFIP WG 11.9 International Conference
New Delhi, India, January 6–8, 2020
Revised Selected Papers

Editors

Gilbert Peterson
Department of Electrical
and Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, OH, USA

Sujeet Sheno
Tandy School of Computer Science
University of Tulsa
Tulsa, OK, USA

ISSN 1868-4238

ISSN 1868-422X (electronic)

IFIP Advances in Information and Communication Technology

ISBN 978-3-030-56222-9

ISBN 978-3-030-56223-6 (eBook)

<https://doi.org/10.1007/978-3-030-56223-6>

© IFIP International Federation for Information Processing 2020

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Contributing Authors	ix
Preface	xvii
PART I THEMES AND ISSUES	
1	
Digital Forensics and the Big Data Deluge – Some Concerns Based on Ramsey Theory	3
<i>Martin Olivier</i>	
2	
Identity and Sufficiency of Digital Evidence	25
<i>Michael Losavio</i>	
PART II FORENSIC TECHNIQUES	
3	
Interactive Temporal Digital Forensic Event Analysis	39
<i>Nikolai Adderley and Gilbert Peterson</i>	
4	
Enhancing the Feature Profiles of Web Shells by Analyzing the Performance of Multiple Detectors	57
<i>Weiqing Huang, Chenggang Jia, Min Yu, Kam-Pui Chow, Jiuming Chen, Chao Liu and Jianguo Jiang</i>	
5	
A Novel Approach for Generating Synthetic Datasets for Digital Forensics	73
<i>Thomas Göbel, Thomas Schäfer, Julien Hachenberger, Jan Türr and Harald Baier</i>	
6	
Detecting Attacks on a Water Treatment System Using One-Class Support Vector Machines	95
<i>Ken Yau, Kam-Pui Chow and Siu-Ming Yiu</i>	

PART III FILESYSTEM FORENSICS

7

- A Digital Media Similarity Measure for Triage of Digital Forensic Evidence 111

Myeong Lim and James Jones

8

- Resident Data Pattern Analysis Using Sector Clustering for Storage Drive Forensics 137

Nitesh Bharadwaj, Upasna Singh and Gaurav Gupta

PART IV CLOUD FORENSICS

9

- Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments 161

Changwei Liu, Anoop Singhal and Duminda Wijesekera

10

- A Taxonomy of Hypervisor Forensic Tools 181

Anand Kumar Mishra, Mahesh Govil and Emmanuel Pilli

PART V SOCIAL MEDIA FORENSICS

11

- Public Opinion Monitoring for Proactive Crime Detection Using Named Entity Recognition 203

Wencan Wu, Kam-Pui Chow, Yonghao Mai and Jun Zhang

12

- Retrieving E-Dating Application Artifacts from iPhone Backups 215

Ranul Thantilage and Nhien-An Le-Khac

PART VI MULTIMEDIA FORENSICS

13

- Target Identity Attacks on Facial Recognition Systems 233

Saheb Chhabra, Naman Banati, Gaurav Gupta and Garima Gupta

14

- Electric Network Frequency Based Audio Forensics Using Convolutional Neural Networks 253

Maoyu Mao, Zhongcheng Xiao, Xiangui Kang, Xiang Li and Liang Xiao

PART VII NOVEL APPLICATIONS

15	
Insider Threat Detection Using Multi-Autoencoder Filtering and Unsupervised Learning	273
<i>Yichen Wei, Kam-Pui Chow and Siu-Ming Yiu</i>	
16	
Detecting Local Machine Data Leakage in Real Time	291
<i>Jingcheng Liu, Yaping Zhang, Yuze Li, Yongheng Jia, Yao Chen and Jin Cao</i>	

Contributing Authors

Nikolai Adderley recently received his M.S. degree in Cyber Operations from the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensic analysis and investigation, digital forensic visualization and computer forensic time analysis.

Harald Baier is a Professor of Internet Security at Darmstadt University of Applied Sciences, Darmstadt, Germany; and a Principal Investigator at the National Research Center for Applied Cybersecurity, Darmstadt, Germany. His research interests include digital forensics, network anomaly detection and security protocols.

Naman Banati received a B.Tech. degree in Computer Science and Engineering from Netaji Subhas University of Technology, New Delhi, India. His research interests include security in machine learning applications, image processing and computer vision.

Nitesh Bharadwaj is a Ph.D. student in Computer Science and Engineering at the Defence Institute of Advanced Technology, Pune, India. His research interests include digital forensics and machine learning.

Jin Cao is a Computer Science Researcher at Tianjin University, Tianjin, China. His research interests are in the area of digital forensics.

Jiuming Chen is a Ph.D. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include digital forensics, data mining and machine learning.

Yao Chen is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests are in the area of data privacy.

Saheb Chhabra is a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include image processing and computer vision, and their applications to document fraud detection.

Kam-Pui Chow, Chair, IFIP WG 11.9 on Digital Forensics, 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.

Thomas Göbel is a Ph.D. student in Computer Science at Darmstadt University of Applied Sciences, Darmstadt, Germany; and a Researcher at the National Research Center for Applied Cybersecurity, Darmstadt, Germany. His research interests include network security, network forensics and anti-forensics.

Mahesh Govil is a Professor of Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India; and the Director of National Institute of Technology Sikkim, Ravangla, India. His research interests include real-time systems, parallel and distributed systems, fault-tolerant systems and cloud computing.

Garima Gupta is a Postdoctoral Researcher in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. Her research interests include image processing and computer vision, and their applications to document fraud detection.

Gaurav Gupta, Vice Chair, IFIP WG 11.9 on Digital Forensics, is a Scientist E in the Ministry of Electronics and Information Technology, New Delhi, India. His research interests include mobile device security, digital forensics, web application security, Internet of Things security and security in emerging technologies.

Julien Hachenberger is a Researcher at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research focuses on security in the manufacturing industry, especially in the context of Industrie 4.0.

Weiqing Huang is a Professor of Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include signal processing theory and technology, electromagnetic acoustic-optic detection and protection, and information security.

Chenggang Jia is a Ph.D. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include digital forensics and information security.

Yongheng Jia is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests include malware detection and classification.

Jianguo Jiang is a Professor of Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include network security, threat intelligence and data security.

James Jones is an Associate Professor of Digital Forensics at George Mason University, Fairfax, Virginia. His research interests include digital artifact persistence, extraction, analysis and manipulation.

Xiangui Kang is a Professor of Computer Science and Cyber Security in the School of Data and Computer Science at Sun Yat-Sen University, Guangzhou, China. His research interests include information forensics, watermarking, and multimedia communications and security.

Nhien-An Le-Khac is a Lecturer of Computer Science and the Director of the Forensic Computing and Cybercrime Investigation Program at University College Dublin, Dublin, Ireland. His research interests include digital forensics, cyber security and artificial intelligence.

Xiang Li is an M.E. student in Information and Communications Engineering at Hainan University, Haikou, China. His research interests include machine learning, computer vision and image processing.

Yuze Li is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests include digital forensics and deep learning.

Myeong Lim is a Ph.D. student in Information Technology at George Mason University, Fairfax, Virginia. His research interests include digital forensics, big data analysis and drive similarity.

Changwei Liu is a Principal Technology R&D Associate with Accenture in Arlington, Virginia. Her research interests include trustworthy artificial intelligence, cloud security and digital forensics.

Chao Liu is a Professor of Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include mobile Internet security and network security evaluation.

Jingcheng Liu is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests include data privacy and intrusion detection.

Michael Losavio is an Assistant Professor of Criminal Justice at the University of Louisville, Louisville, Kentucky. His research interests include legal and social issues related to computing and digital crime.

Yonghao Mai is a Professor of Information Technology at Hubei Police University, Wuhan, China. His research interests include digital forensics, cyber security, data warehousing and data mining.

Maoyu Mao is an M.E. student in Cyber Security at Sun Yat-sen University, Guangzhou, China. Her research interests include audio forensics and machine learning.

Anand Kumar Mishra is a Ph.D. student in Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India. His research interests include digital forensics and cyber security, especially related to cloud computing and container technology.

Martin Olivier is a Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research focuses on digital forensics – in particular, the science of digital forensics and database forensics.

Gilbert Peterson is a Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensics, artificial intelligence and statistical machine learning.

Emmanuel Pilli is an Associate Professor and Head of the Department of Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India. His research interests include cyber security, digital forensics, cloud computing, big data, blockchains and the Internet of Things.

Thomas Schäfer is a Researcher at the National Research Center for Applied Cybersecurity, Darmstadt, Germany. His research interests include network forensics and automobile forensics.

Upasna Singh is an Assistant Professor of Computer Science and Engineering at the Defence Institute of Advanced Technology, Pune, India. Her research interests include digital forensics, machine learning and social network analysis.

Anoop Singhal is a Senior Computer Scientist and Program Manager in the Computer Security Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include network security, network forensics, cloud security and data mining.

Ranul Thantilage is a Ph.D. student in Computer Science at University College Dublin, Dublin, Ireland. His research interests include digital forensics, cyber security and big data analytics.

Jan Türr is an M.Sc. student in Computer Science at Technical University Darmstadt, Darmstadt, Germany. His research interests include digital forensics, network forensics and anti-forensics.

Yichen Wei is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include information security, digital forensics and artificial intelligence.

Duminda Wijesekera is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research interests include systems security, digital forensics and transportation systems.

Wencan Wu is an M.S. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics and cyber security.

Liang Xiao is a Professor of Communications Engineering and Cyber Security in the School of Communications Engineering at Xiamen University, Fujian, China. Her research interests include wireless security, privacy protection and wireless communications.

Zhongcheng Xiao is an M.E. student in Software Engineering at Sun Yat-sen University, Guangzhou, China. His research interests include audio forensics and reinforcement learning.

Ken Yau is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests are in the area of digital forensics, with an emphasis on industrial control system forensics.

Siu-Ming Yiu is a Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include security, cryptography, digital forensics and bioinformatics.

Min Yu is an Assistant Professor of Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include malicious document detection, document content security and document security design and evaluation.

Jun Zhang is a Professor of Information Technology at Hubei Police University, Wuhan, China. His research interests include digital forensics, cryptography and cyber security.

Yaping Zhang is an Assistant Professor of Computer Science at Tianjin University, Tianjin, China. His research interests include network security, data mining and digital forensics.

Preface

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every 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 cyber security – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems.

This book, *Advances in Digital Forensics XVI*, is the sixteenth 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 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 sixteen revised and edited chapters based on papers presented at the Sixteenth IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India on January 6-8, 2020. The papers were refereed by members of IFIP Working Group 11.9 and other internationally-recognized experts in digital forensics. The post-conference manuscripts submitted by the authors were rewritten to accommodate the suggestions provided by the conference attendees. They were subsequently revised by the editors to produce the final chapters published in this volume.

The chapters are organized into seven sections: Themes and Issues, Forensic Techniques, Filesystem Forensics, Cloud Forensics, Social Media Forensics, Multimedia Forensics and Novel Applications. 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 Gaurav Gupta for his tireless work on behalf of IFIP Working Group 11.9 on Digital Forensics. We also acknowledge the conference sponsors, Cellebrite, Magnet Forensics and Lab Systems, as well as the support provided by the Ministry of Electronics and Information Technology of the Government of India, U.S. National Science Foundation, U.S. National Security Agency and U.S. Secret Service.

GILBERT PETERSON AND SUJEET SHENOI