



HAL
open science

Advances in Digital Forensics XVII

Gilbert Peterson, Sujeet Shenoï

► **To cite this version:**

Gilbert Peterson, Sujeet Shenoï. Advances in Digital Forensics XVII. Springer International Publishing, AICT-612, 2021, IFIP Advances in Information and Communication Technology, 978-3-030-88380-5. 10.1007/978-3-030-88381-2 . hal-03764367

HAL Id: hal-03764367

<https://inria.hal.science/hal-03764367v1>

Submitted on 31 Aug 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

Luis 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 , National University of Ireland, Galway, Ireland

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 XVII

17th IFIP WG 11.9 International Conference
Virtual Event, February 1–2, 2021
Revised Selected Papers

Editors

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

Sujeet Shenoj
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 978-3-030-88380-5

ISBN 978-3-030-88381-2 (eBook)

<https://doi.org/10.1007/978-3-030-88381-2>

© IFIP International Federation for Information Processing 2021

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	vii
Preface	xiii
PART I THEMES AND ISSUES	
1	
Digital Forensic Acquisition Kill Chain – Analysis and Demonstration <i>Gunnar Alendal, Geir Olav Dyrkolbotn and Stefan Axelsson</i>	3
2	
Enhancing Industrial Control System Forensics Using Replication- Based Digital Twins <i>Marietheres Dietz, Ludwig Englbrecht and Günther Pernul</i>	21
3	
Comparison of Cyber Attacks on Services in the Clearnet and Darknet <i>York Yannikos, Quang Anh Dang and Martin Steinebach</i>	39
PART II APPROXIMATE MATCHING TECHNIQUES	
4	
Using Parallel Distributed Processing to Reduce the Computational Time of Digital Media Similarity Measures <i>Myeong Lim and James Jones</i>	65
5	
Evaluation of Network Traffic Analysis Using Approximate Matching Algorithms <i>Thomas Göbel, Frieder Uhlig and Harald Baier</i>	89

PART III ADVANCED FORENSIC TECHNIQUES

6		
Leveraging USB Power Delivery Implementations for Digital Forensic Acquisition		111
<i>Gunnar Alendal, Stefan Axelsson and Geir Olav Dyrkolbotn</i>		
7		
Detecting Malicious PDF Documents Using Semi-Supervised Machine Learning		135
<i>Jianguo Jiang, Nan Song, Min Yu, Kam-Pui Chow, Gang Li, Chao Liu and Weiqing Huang</i>		
8		
Malicious Login Detection Using Long Short-Term Memory with an Attention Mechanism		157
<i>Yanna Wu, Fucheng Liu and Yu Wen</i>		

PART IV NOVEL APPLICATIONS

9		
Predicting the Locations of Unrest Using Social Media		177
<i>Shengzhi Qin, Qiaokun Wen and Kam-Pui Chow</i>		
10		
Extracting Threat Intelligence Relations Using Distant Supervision and Neural Networks		193
<i>Yali Luo, Shengqin Ao, Ning Luo, Changxin Su, Peian Yang and Zhengwei Jiang</i>		
11		
Security Auditing of Internet of Things Devices in a Smart Home		213
<i>Suryadipta Majumdar, Daniel Bastos and Anoop Singhal</i>		

PART V IMAGE FORENSICS

12		
Indian Currency Database for Forensic Research		237
<i>Saheb Chhabra, Gaurav Gupta, Garima Gupta and Monika Gupta</i>		
13		
Security and Privacy Issues Related to Quick Response Codes		255
<i>Pulkit Garg, Saheb Chhabra, Gaurav Gupta, Garima Gupta and Monika Gupta</i>		

Contributing Authors

Gunnar Alendal is a Special Investigator with Kripos/NCIS Norway, Oslo, Norway; and a Ph.D. student in Computer Security at the Norwegian University of Science and Technology, Gjøvik, Norway. His research interests include digital forensics, reverse engineering, security vulnerabilities, information security and cryptography.

Shengqin Ao is an M.S. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. Her research interests include threat intelligence information processing and information extraction.

Stefan Axelsson is an Associate Professor of Digital Forensics at the Norwegian University of Science and Technology, Gjøvik, Norway; and a Professor of Digital Forensics and Cyber Security at Stockholm University, Stockholm, Sweden. His research interests include digital forensics, data analysis and digital investigations.

Harald Baier is a Professor of Digital Forensics at Bundeswehr University, Munich, Germany. His research interests include bulk data handling in digital forensics, data synthesis and RAM forensics.

Daniel Bastos is a Senior Cyber Security Engineer at Bosch Security and Safety Systems, Ovar, Portugal. His research interests include Internet of Things security, cloud security and information security and 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 in 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.

Quang Anh Dang is an M.S. student in Information Technology Security at the Technical University of Darmstadt, Darmstadt, Germany. His research interests include penetration testing, the darknet and automobile security.

Marietheres Dietz is a Ph.D. student in Business Information Systems at the University of Regensburg, Regensburg, Germany. Her research focuses on the digital twin paradigm with an emphasis on security.

Geir Olav Dyrkolbotn is a Major in the Norwegian Armed Forces, Lillehammer, Norway; and an Associate Professor of Cyber Defense at the Norwegian University of Science and Technology, Gjøvik, Norway. His research interests include cyber defense, reverse engineering, malware analysis, side-channel attacks and machine learning.

Ludwig Englbrecht is a Ph.D. student in Business Information Systems at the University of Regensburg, Regensburg, Germany. His research interests include new approaches in digital forensics and digital forensic readiness.

Pulkit Garg is a Ph.D. student in Computer Science and Engineering at the Indian Institute of Technology Jodhpur, Karwar, India. His research interests include image processing and computer vision, and their applications in document fraud detection.

Thomas Göbel is a Ph.D. student in Computer Science and a Researcher in the Research Institute of Cyber Defense at Bundeswehr University, Munich, Germany. His research interests include digital forensics, data synthesis and machine learning.

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 in 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.

Monika Gupta received her Ph.D. degree in Physics from the National Institute of Technology, Kurukshetra, India. Her research interests include image processing and computer vision and their applications in document fraud detection.

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.

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.

Zhengwei Jiang is a Senior Engineer at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include threat intelligence, malicious code analysis and suspicious network traffic analysis.

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

Gang Li is an Associate Professor of Information Technology at Deakin University, Burwood, Australia. His research interests include data science and business intelligence.

Myeong Lim received his Ph.D. degree in Information Technology from George Mason University, Fairfax, Virginia. His research interests include digital forensics, data mining and artificial intelligence.

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.

Fucheng Liu is a Ph.D. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include insider threat detection and malicious entity detection.

Ning Luo is an M.S. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. Her research interests include cyber security event extraction and threat intelligence analysis.

Yali Luo is an M.S. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. Her research interests include threat intelligence analysis and threat intelligence assessment.

Suryadipta Majumdar is an Assistant Professor of Information Systems Engineering at Concordia University, Montreal, Canada. His research interests include cloud security, Internet of Things security, Internet of Things forensics and security auditing.

Günther Pernul is a Professor and Chair of Information Systems at the University of Regensburg, Regensburg, Germany. His research interests include information systems security, individual privacy and data protection.

Shengzhi Qin is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include public opinion analysis, knowledge graphs and information security.

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.

Nan Song is an M.S. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include malicious document detection, threat intelligence and data security.

Martin Steinebach is the Head of Media Security and Information Technology Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany; and an Honorary Professor of Computer Science at the Technical University of Darmstadt, Darmstadt, Germany. His research interests include digital watermarking, robust hashing, steganalysis and multimedia forensics.

Changxin Su is an M.S. student in Computer Science at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include threat intelligence information processing and information extraction.

Frieder Uhlig is an M.S. student in Information Technology Security at the Technical University of Darmstadt, Darmstadt, Germany. His research interests include network forensics and applications of approximate matching.

Qiaokun Wen is an M.S. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include deep learning and information security.

Yu Wen is a Senior Engineer at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include data mining, big data security and privacy, and insider threat detection.

Yanna Wu is an M.S. student in Cyber Security at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. Her research interests include threat perception detection and intelligent attack tracing.

Peian Yang is a Ph.D. student in Cyber Security at the Institute of High Energy Physics, Chinese Academy of Sciences, Beijing, China. His research interests include attack recognition and threat intelligence analysis.

York Yannikos is a Research Associate at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include digital forensic tool testing, darknet marketplaces and open-source intelligence.

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.

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 XVII*, is the seventeenth 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 thirteen revised and edited chapters based on papers presented at the Seventeenth IFIP WG 11.9 International Conference on Digital Forensics, a fully-remote event held on February 1-2, 2021. 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 five sections: Themes and Issues, Approximate Matching Techniques, Advanced Forensic Techniques, Novel Applications and Image Forensics. 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 Kam-Pui Chow and Gaurav Gupta for their tireless work on behalf of IFIP Working Group 11.9 on Digital Forensics. We also acknowledge the support provided by the U.S. National Science Foundation, U.S. National Security Agency and U.S. Secret Service.

GILBERT PETERSON AND SUJEET SHENOI