1. Record Nr. UNINA9910254836703321

Titolo	Advances in Digital Forensics XIII : 13th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 30 - February 1, 2017, Revised Selected Papers / / edited by Gilbert Peterson, Sujeet Shenoi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-67208-8
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XVIII, 303 p. 98 illus.)
Collana	IFIP Advances in Information and Communication Technology, , 1868-422X ; ; 511
Disciplina	004
Soggetti	Data protection Information technology - Management Computers and civilization Cryptography Data encryption (Computer science) Data and Information Security Computer Application in Administrative Data Processing Computers and Society Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Intro -- Contents -- Contributing Authors -- Preface -- I THEMES AND ISSUES -- 1 ESTABLISHING FINDINGS IN DIGITAL FORENSIC EXAMINATIONS: A CASE STUDY METHOD -- 1. Introduction -- 2. Causality and Digital Systems -- 3. Using Yin's Method -- 3.1 Body of Knowledge -- 3.2 Hypotheses Formulation -- 3.3 Hypotheses Testing -- 4. Causal Relationships in Digital Forensics -- 4.1 Understanding Causal Relationships -- 4.2 Establishing Causal Relationships -- 5. Lottery Terminal Hacking Incident -- 5.1 The Case -- 5.2 The Investigation -- 5.3 The Examination -- 5.4 Hypotheses Formulation -- 5.5 Hypothesis Testing -- 6. Conclusions -- References -- 2 A MODEL FOR DIGITAL EVIDENCE ADMISSIBILITY ASSESSMENT -- 1. Introduction -- 2. Background -- 2.1 Digital Forensics and Digital

Evidence -- 2.2 Harmonization and Standardization -- 3. Requirements for Assessing Admissibility -- 3.1 Harmonization of Requirements -- 3.2 Technical Requirements and Assessment -- 3.3 Legal Requirements and Assessment -- 4. Model for Assessing Evidence Admissibility -- 4.1 Phase 1: Evidence Assessment Phase -- 4.2 Phase 2: Evidence Consideration Phase -- 4.3 Phase 3: Evidence Determination Phase -- 5. Application in Legal Proceedings -- 6. Conclusions -- References -- II MOBILE AND EMBEDDED DEVICE FORENSICS -- 3 EVALUATING THE AUTHENTICITY OF SMARTPHONE EVIDENCE -- 1. Introduction -- 2. Related Research -- 3. Reference Architecture -- 3.1 Architectural Designs of Applications -- 3.2 Reference Architecture Components -- 3.3 Modeling Application Behavior -- 3.4 Exploring an Android Application -- 4. Theories of Normality -- 5. Discussion -- 6. Conclusions -- References -- 4 FORENSIC EVALUATION OF AN AMAZON FIRE TV STICK -- 1. Introduction -- 2. Related Work -- 2.1 Chromecast -- 2.2 Measy A2W Miracast -- 2.3 Amazon Kindle Fire HD -- 3. Proposed Forensic Methodology.
3.1 Experimental Methodology -- 3.2 Sample Data -- 4. Forensic Assessment -- 4.1 ADB Extraction Test -- 4.2 UFED Touch Test -- 4.3 Python Script Test -- 4.4 Rooting Test -- 4.5 ADB Extraction Test -- 4.6 Manual Acquisition Test -- 5. Recommended Forensic Analysis Method -- 6. Conclusions -- References -- 5 DETECTING ANOMALOUS PROGRAMMABLE LOGIC CONTROLLER EVENTS USING MACHINE LEARNING -- 1. Introduction -- 2. Programmable Logic Controllers -- 3. Forensic Challenges -- 4. Machine Learning -- 5. Related Work -- 6. Experimental Setup and Methodology -- 6.1 Experimental Setup -- 6.2 Classifying Anomalous Operations -- 7. Experimental Results and Discussion -- 8. Conclusions -- References -- III NETWORK AND CLOUD FORENSICS -- 6 A FORENSIC METHODOLOGY FOR SOFTWARE-DEFINED NETWORK SWITCHES -- 1. Introduction -- 2. Background -- 3. Related Work -- 4. Proposed Forensic Methodology -- 5. Experimental Evaluation -- 5.1 Experimental Setup -- 5.2 Attack Scenario -- 5.3 Memory Analysis -- 5.4 Southbound Traffic Analysis -- 5.5 Service-Level Event Logging -- 5.6 Discussion -- 6. Conclusions -- Acknowledgement -- References -- 7 IDENTIFYING EVIDENCE FOR CLOUD FORENSIC ANALYSIS -- 1. Introduction -- 2. Background and Related Work -- 3. Attack Reconstruction -- 4. Reconstructing Attack Scenarios -- 4.1 Experimental Setup -- 4.2 Experimental Attacks -- 4.3 Collecting Evidence for Reconstruction -- 5. Using System Calls for Evidence Analysis -- 6. Conclusions -- References -- IV THREAT DETECTION AND MITIGATION -- 8 DIGITAL FORENSIC IMPLICATIONS OF COLLUSION ATTACKS ON THE LIGHTNING NETWORK -- 1. Introduction -- 2. Related Work -- 3. Bitcoin Blockchain -- 4. Lightning Network -- 4.1 Payment Routing -- 4.2 Lightning Network Topology -- 5. Collusion Attack on the Lightning Network -- 6. Collusion Attack Implications -- 6.1 Fraud -- 6.2 Money Laundering -- 6.3 Forfeiture.
7. Attack Mitigation -- 8. Conclusions -- References -- 9 INSIDER THREAT DETECTION USING TIME-SERIES-BASED RAW DISK FORENSIC ANALYSIS -- 1. Introduction -- 2. Methodology -- 2.1 Sample Data -- 2.2 Data Driven Algorithm Development -- 2.3 Time-Series-Based Anomaly Detection -- 3. Experimental Results -- 3.1 Unpaired t-Test/Split Window Method -- 3.2 Unpaired t-Test/Sliding Window Method -- 3.3 Autoregressive Method -- 3.4 Ground Truth Analysis -- 4. Conclusions -- Acknowledgement -- References -- 10 ANTI-FORENSIC THREAT MODELING -- 1. Introduction -- 2. Threats to the Digital Forensic Process -- 2.1 Evidence Destruction -- 2.2 Evidence Hiding -- 2.3 Evidence Source Elimination -- 2.4 Evidence Counterfeiting -- 3. Threat Modeling Applied to Digital Forensics --

3.1 Case Understanding -- 3.2 Evidence Source Identification -- 3.3 Threat Identification -- 3.4 Risk Management -- 3.5 Result Reporting and Model Updating -- 4. Applying the Threat Model -- 5. Conclusions -- References -- V MALWARE FORENSICS -- 11 A BEHAVIOR-BASED APPROACH FOR MALWARE DETECTION -- 1. Introduction -- 2. Related Work -- 2.1 Static Analysis -- 2.2 Dynamic Analysis -- 3. Windows Handles and Objects -- 4. Malware Detection Using Handles -- 4.1 Experimental Setup -- 4.2 Vectorizing the Handle Data -- 4.3 Model Training -- 5. Results and Analysis -- 6. Conclusions -- References -- 12 CATEGORIZING MOBILE DEVICE MALWARE BASED ON SYSTEM SIDE-EFFECTS -- 1. Introduction -- 2. Live Memory Analysis of Mobile Devices -- 2.1 Information in Volatile Memory -- 2.2 Memory Capture Techniques -- 3. Android Exploitation Techniques -- 3.1 Heap Exploitation -- 3.2 Defeating ASL Randomization -- 4. Stagefright Exploits -- 4.1 Zimperium zLabs -- 4.2 Google Project Zero -- 4.3 NorthBit -- 5. Categorizing Malware by Behavior -- 5.1 Malware Categories -- 5.2 Benefits of Malware Categorization.
5.3 Detecting Malware Side-Effects -- 6. Conclusions -- References -- VI IMAGE FORENSICS -- 13 SEMANTIC VIDEO CARVING USING PERCEPTUAL HASHING AND OPTICAL FLOW -- 1. Introduction -- 2. Related Work -- 3. Proposed Video Carving Approach -- 3.1 Perceptual Grouping -- 3.2 Precise Stitching -- 4. Experimental Results -- 5. Conclusions -- Acknowledgements -- References -- 14 DETECTING FRAUDULENT BANK CHECKS -- 1. Introduction -- 2. Related Work -- 3. Experimental Setup -- 4. Fraud Detection Methodology Overview -- 5. Details of the Fraud Detection Methodology -- 5.1 Check Pantographs -- 5.2 Check Microlines -- 5.3 Check Alterations -- 5.4 Printed vs. Handwritten Signatures -- 6. Experimental Results -- 6.1 Check Pantograph Results -- 6.2 Check Microline Results -- 6.3 Check Alteration Results -- 6.4 Printed vs. Handwritten Signature Results -- 6.5 Results for Checks from Multiple Banks -- 7. Integrated Check Fraud Detection Tool -- 8. Conclusions -- References -- VII FORENSIC TECHNIQUES -- 15 AUTOMATED COLLECTION AND CORRELATION OF FILE PROVENANCE INFORMATION -- 1. Introduction -- 2. Related Work -- 2.1 File Provenance Maintenance Systems -- 2.2 Sources of Provenance Data -- 2.3 Evidence Correlation -- 3. Provenance Collection -- 3.1 Data Gathering -- 3.2 Data Processing -- 4. Experimental Results -- 5. Conclusions -- References -- 16 USING PERSONAL INFORMATION IN TARGETED GRAMMAR-BASED PROBABILISTIC PASSWORD ATTACKS -- 1. Introduction -- 2. Background and Related Work -- 3. Building a Targeted Attack -- 3.1 Merging Context-Free Grammars -- 3.2 Integrating Personal Information -- 3.3 Using Old Password Information -- 3.4 Predicting New Passwords -- 3.5 Merging Grammars and Generating Guesses -- 4. Experiments -- 4.1 Password Survey -- 4.2 Testing and Cracking Results -- 5. Conclusions -- References.

Sommario/riassunto

Advances in Digital Forensics XIII Edited by: Gilbert Peterson and Sujeet Shenoi 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 crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. 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 systems. Advances in Digital Forensics XIII describes original

research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major techn ical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues; Mobile and Embedded Device Forensics; Network and Cloud Forensics; Threat Detection and Mitigation; Malware Forensics; Image Forensics; and Forensic Techniques. This book is the thirteenth volume in the annual series produced by the International Federation for Information Processing (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 contains a selection of sixteen edited papers from the Thirteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA in the winter of 2017. Advances in Digital Forensics XIII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.