1. Record Nr. UNINA9910299205603321

Titolo	Advances in Digital Forensics XI : 11th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 26-28, 2015, Revised Selected Papers / / edited by Gilbert Peterson, Sujeet Shenoi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-24123-0
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVIII, 357 p. 74 illus. in color.)
Collana	IFIP Advances in Information and Communication Technology, , 1868-422X ; ; 462
Disciplina	363.25968
Soggetti	Data protection Computers and civilization Electronic commerce Information technology - Management Cryptography Data encryption (Computer science) Data and Information Security Computers and Society e-Commerce and e-Business Computer Application in Administrative Data Processing Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Contents -- Contributing Authors -- Preface -- THEMES AND ISSUES -- A TALE OF TWO TRACES - DIPLOMATICS AND FORENSICS -- 1. Introduction -- 1.1 Causality as a Foundation of Science -- 1.2 Diplomatics -- 1.3 Archival Science and Public Records -- 1.4 Digital Records -- 1.5 Digital Diplomatics -- 1.6 Forensic Science -- 1.7 Digital Forensics -- 2. Digital Diplomatics and Forensics -- 2.1 Case 1 Background -- 2.2 Case 2 Background -- 2.3 Admitting the Documents -- 2.4 Related Information on Records -- 3. Case Resolution -- 3.1 Case 1 -- 3.2 Case 2 -- 4. Implications and the Path Forward -- 4.1 Implications -- 4.2 The Path Forward -- 5. Conclusions -- References

-- NOTIONS OF HYPOTHESIS IN DIGITAL FORENSICS -- 1. Motivation -- 2. Related Work -- 3. Carrier's Work -- 3.1 History Duration -- 3.2 Primitive Storage System Configuration -- 3.3 Primitive Event System Configuration -- 3.4 Primitive State and Event Definition -- 3.5 Complex Storage System Configuration -- 3.6 Complex Event System Configuration -- 3.7 Complex State and Event Definition -- 4. Bunge's Classification -- 5. Limitations of the Study -- 6. Conclusions -- References -- USING YIN'S APPROACH TO CASE STUDIES AS A PARADIGM FOR CONDUCTING EXAMINATIONS -- 1. Introduction -- 2. Understanding a Case -- 2.1 What is a Case? -- 2.2 Case Study Design -- 2.3 Case Study Design -- 3. Digital Forensic Case Studies -- 3.1 Case Study 1 -- 3.2 Case Study 2 -- 3.3 Case Study 3 -- 4. Analytic Generalizations -- 5. Assessing Case Study Quality -- 6. Conclusions -- References -- AN INFORMATION EXTRACTION FRAMEWORK FOR DIGITAL FORENSIC INVESTIGATIONS -- 1. Introduction -- 2. Related Work -- 3. Information Extraction Framework -- 3.1 Named Entity Recognition -- 3.2 Relation Extraction -- 4. Experiments and Analysis -- 4.1 Dataset Description -- 4.2 Data Pre-Processing -- 4.3 Experimental Results.
5. Conclusions -- References -- INTERNET CRIME INVESTIGATIONS -- A GRAPH-BASED INVESTIGATION OF BITCOIN TRANSACTIONS -- 1. Introduction -- 2. Bitcoin System Overview -- 3. Transaction Data Collection -- 4. Graph-Based Bitcoin Transaction Analysis -- 4.1 Address Clustering -- 4.2 Address Graph Observations -- 4.3 Currency Flow Analysis -- 4.4 Mt. Gox Case Study -- 5. Discussion -- 6. Conclusions -- References -- PROFILING AND TRACKING ACYBERLOCKER LINK SHARERIN A PUBLIC WEB FORUM -- 1. Introduction -- 2. Related Work -- 3. Methodology -- 3.1 Data Collection -- 3.2 User Profile Construction -- 3.3 Multidimensional Scaling Analysis -- 3.4 Cluster Analysis -- 4. Experiments -- 4.1 Datasets -- 4.2 Evaluation Metric -- 4.3 Analysis of Sharers -- 4.4 Analysis of Sharers and Followers -- 5. Conclusions -- References -- A PRIVACY-PRESERVING ENCRYPTIONSCHEME FOR AN INTERNET REALNAMEREGISTRATION SYSTEM -- 1. Introduction -- 2. Background -- 2.1 Privacy -- 2.2 Real-Name Registration in South Korea -- 2.3 Real-Name Registration in China -- 3. Real-Name Registration Requirements -- 4. Real-Name Registration Overview -- 5. Privacy-Preserving Real-Name Registration -- 5.1 User Real-Name Registration Process -- 5.2 User Web-Name Registration Process -- 5.3 Privacy-Preserving Properties -- 6. Conclusions -- References -- A LOGIC-BASED NETWORK FORENSICMODEL FOR EVIDENCE ANALYSIS -- 1. Introduction -- 2. Background and Related Work -- 2.1 MulVAL and Logical Attack Graphs -- 2.2 Evidence Graphs -- 2.3 Related Work -- 3. Network Example -- 4. Attack Scenario Reconstruction -- 4.1 Rules and Facts -- 4.2 Evidence Graph Generation -- 5. Extending MulVAL -- 5.1 Using an Anti-Forensic Database -- 5.2 Integrating Evidence Standards -- 6. Experimental Results -- 7. Conclusions -- References -- FORENSIC TECHNIQUES -- CHARACTERISTICS OF MALICIOUSDLLS IN WINDOWS MEMORY.
1. Introduction -- 2. Motivation -- 3. Related Work -- 4. Test Data Generation -- 5. Data Classification -- 6. Injected DLL Characteristics -- 7. Threats to Validity -- 8. Conclusions -- References -- DETERMINING TRIGGERINVOLVEMENT DURING FORENSICATTRIBUTION IN DATABASES -- 1. Introduction -- 2. Background -- 2.1 Forensic Attribution -- 2.2 Triggers -- 3. Trigger Identification -- 4. Algorithm Implementation -- 5. Implementation Challenges -- 5.1 Scope and Visibility -- 5.2 Encryption -- 5.3 Case Sensitivity -- 5.4 False Positive Errors -- 5.5 Data Types -- 5.6 Recursion -- 5.7 Performance -- 6.

Conclusions -- References -- USING INTERNAL MySQL/InnoDBB-TREE INDEX NAVIGATION FORDATA HIDING -- 1. Introduction -- 2. Background and Related Work -- 3. InnoDB Index -- 4. Data Removal -- 4.1 Physical Deletion of Data Records -- 4.2 Forensic Impact -- 5. Data Hiding -- 5.1 Manipulating Search Results -- 5.2 Reorganizing the Index -- 5.3 Hiding Data in Index Page Garbage Space -- 5.4 Hiding Data in Index Page Free Space -- 5.5 Removing a Page from the Index -- 6. Conclusions -- References -- IDENTIFYING PASSWORDSSTORED ON DISK -- 1. Introduction -- 2. Related Work -- 3. Background -- 3.1 Probabilistic Context-Free Grammars -- 4. Examining a Disk -- 4.1 Recovering Files from a Disk -- 4.2 Retrieving Tokens from Files -- 4.3 Initial Filtering -- 4.4 Specialized Alpha String Filtering -- 5. Identifying Passwords -- 5.1 Calculating Token Probabilities -- 5.2 Ranking Algorithms -- 6. Experimental Evaluation -- 6.1 Experimental Setup -- 6.2 Initial Filtering -- 6.3 Ranking Algorithms -- 6.4 Specialized Filtering -- 7. Conclusions -- References -- FRAGMENTED JPEG FILE RECOVERYUSING PSEUDO HEADERS -- 1. Introduction -- 2. Related Work -- 3. JPEG Background -- 3.1 Essential Configurations in JPEG Headers -- 3.2 Synchronization Point. 4. JPEG File Recovery Methodology -- 4.1 Huffman Table and Sub-Sampling Factor -- 4.2 Image Resolution -- 4.3 Quantization Table -- 5. Experimental Results -- 6. Conclusions -- References -- MOBILE DEVICEFORENSICS -- FORENSIC-READY SECURE iOS APPSFOR JAILBROKEN iPHONES -- 1. Introduction -- 2. Related Work -- 3. Implementation Methodology -- 3.1 Securing Apps -- 3.2 Preserving Dates and Timestamps -- 3.3 Static Library -- 3.4 Dynamic Library -- 4. Preventing Attacks and Anti-Forensics -- 4.1 Using the Static Library -- 4.2 Using the Dynamic Library -- 5. Experimental Results -- 6. Case Study -- 7. Conclusions -- References -- A FRAMEWORK FOR DESCRIBINGMULTIMEDIA CIRCULATION INA SMARTPHONE ECOSYSTEM -- 1. Introduction -- 2. Related Work -- 3. Using Graph Databases -- 4. Use Case Experiments -- 5. Results -- 6. System Design -- 7. Conclusions -- References -- CLOUD FORENSICS -- A TRUSTWORTHY CLOUDFORENSICS ENVIRONMENT -- 1. Introduction -- 2. Related Work -- 3. Desired Properties -- 4. Challenges -- 5. FECloud Architecture -- 5.1 Logger (Themis) -- 5.2 Data Possession Manager (Metis) -- 5.3 Timestamp Manager (Chronos) -- 5.4 Provenance Manager (Clio) -- 5.5 Proof Publisher (Brizo) -- 5.6 Evidence Access Interface (Horizon) -- 5.7 Forensics-Enabled Image -- 5.8 Preliminary Results -- 6. Conclusions -- References -- LOCATING AND TRACKING DIGITALOBJECTS IN THE CLOUD -- 1. Introduction -- 2. Background -- 2.1 Cloud Computing -- 2.2 Digital Forensics -- 2.3 Data Provenance -- 3. Related Work -- 3.1 Storing Provenance Data -- 3.2 Data Provenance Requirements -- 4. Cloud-Based Provenance Model -- 5. Using a Central Logging Server -- 5.1 File Wrapper -- 5.2 Tracking Wrapper Locations -- 6. Discussion -- 7. Conclusions -- References -- FORENSIC TOOLS -- A TOOL FOR EXTRACTING STATIC ANDVOLATILE FORENSIC ARTIFACTS OFWINDOWS 8.x APPS -- 1. Introduction. 2. Related Work -- 2.1 Windows 8 Forensics -- 2.2 Forensic Analysis of Apps -- 3. Background -- 3.1 Hibernation File -- 3.2 Swap File -- 3.3 Static vs. Volatile Artifacts -- 4. Experimental Methodology -- 5. Experimental Results -- 5.1 Facebook -- 5.2 Other Apps -- 5.3 Performance -- 6. Conclusions -- References -- CRITERIA FOR VALIDATINGSECURE WIPING TOOLS -- 1. Introduction -- 2. Deletion Effects and Deletion Types -- 2.1 Deletion Effects -- 2.2 Deletion Types -- 3. File Deletion Artifacts -- 3.1 MFT Records (Recycle Bin Deletion) -- 3.2 LogFile (Recycle Bin Deletion) -- 3.3 Hard Disk (Recycle Bin Deletion) -- 3.4 MFT Records (Permanent File Deletion) -- 3.5

LogFile (Permanent File Deletion) -- 3.6 Hard Disk (Permanent File Deletion) -- 4. Validation Criteria -- 4.1 Specifications -- 4.2 Test Assertions -- 4.3 Test Cases (SW-TC) -- 4.4 Relational Summary Table -- 5. Validation Testing of Eraser -- 6. Conclusions -- References -- DO DATA LOSS PREVENTIONSYSTEMS REALLY WORK? -- 1. Introduction -- 2. Related Work -- 3. Evaluated Systems -- 3.1 Agent-Based Solution -- 3.2 Agentless Solution -- 3.3 Hybrid Solution -- 3.4 File System Scanning Tool -- 4. Experimental Setup -- 5. Experimental Results -- 6. Discussion -- 7. Conclusions -- References.

Sommario/riassunto

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 XI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues re lated to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues Internet Crime Investigations Forensic Techniques Mobile Device Forensics Cloud Forensics Forensic Tools This book is the eleventh 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 th e art of research and practice in digital forensics. The book contains a selection of twenty edited papers from the Eleventh Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida in the winter of 2015. Advances in Digital Forensics XI 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. .