Digital Forensics Elsevier

Digital Forensics Trial Graphics
Intelligence and Security Informatics
Managing Information Security
Investigating Windows Systems
Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1
Malware Forensics Field Guide for Linux Systems
Malware Forensics
Forensic Engineering
Digital-Forensics and Watermarking
Proceedings of the Seventh International Workshop on Digital Forensics and Incident Analysis (WDFIA 2012)
Contemporary Digital Forensic Investigations of Cloud and Mobile Applications
Digital Forensics with Open Source Tools
Preserving Electronic Evidence for Trial
Seeking the Truth from Mobile Evidence
Strategic Leadership in Digital Evidence
Digital Forensics
Intelligent Decision Support Systems for Sustainable Computing
Encyclopedia of Forensic Sciences
Digital Forensics
Deception in the Digital Age
Digital and Document Examination
Big Digital Forensic Data
Augmented Reality
Integrating Python with Leading Computer Forensics Platforms
The Basics of Digital Forensics
Digital Evidence and Computer Crime

The Basics of Cyber Safety
Hiding Behind the Keyboard
Perl Scripting for Windows Security
Handbook of Digital Forensics and Investigation
Digital Forensics for Legal Professionals
Digital Forensics and Investigations
Cloud Storage Forensics
Digital Forensics and Cyber Crime
Investigating Child Exploitation and Pornography
ICCSM2015-3rd International Conference on Cloud Security and Management
Mobile Security and Privacy
Malware Forensics Field Guide for Windows Systems
Digital Forensics in the Era of Artificial Intelligence

LOPEZ ROBINSON

Digital Forensics Trial Graphics Syngress
This book provides an in-depth understanding of big data challenges to digital forensic investigations, also known as big digital forensic data. It also develops the basis of using data mining in big forensic data analysis, including data reduction, knowledge management, intelligence, and data mining principles to achieve faster analysis in digital forensic investigations. By collecting and assembling a corpus of test data from a range of devices in the real world, it outlines a process of big data reduction, and evidence and intelligence extraction methods. Further, it includes the experimental results on vast volumes of real digital forensic data. The book is a valuable resource for digital forensic practitioners, researchers in big data, cyber threat hunting and intelligence, data mining and other related areas.
Intelligence and Security Informatics Syngress
Forensic Engineering, the latest edition in the Advanced Forensic Science series that grew out of recommendations from the 2009 NAS Report: Strengthening Forensic Science: A Path Forward, serves as a graduate level text for those studying and teaching digital forensic engineering, as well as an excellent reference for a forensic scientist’s library or for their use in casework. Coverage includes investigations, transportation investigations, fire investigations, other methods and professional issues. Edited by a world-renowned leading forensic expert, this series is a long overdue solution for the forensic science community. Provides basic principles of forensic science and an overview of forensic

engineering Contains sections on investigations, transportation investigations, fire investigations and other methods Includes a section on professional issues, such as: from crime scene to court, forensic laboratory reports and health and safety Incorporates effective pedagogy, key terms, review questions, discussion questions and additional reading suggestions

Managing Information Security Academic Press

This volume includes 74 papers presented at ICTIS 2017: Second International Conference on Information and Communication Technology for Intelligent Systems. The conference was held on 25th and 26th March 2017, in Ahmedabad, India and organized jointly by the Associated Chambers of Commerce and Industry of India (ASSOCHAM) Gujarat Chapter, the G R Foundation, the Association of Computer Machinery, Ahmedabad Chapter and supported by the Computer Society of India Division IV – Communication and Division V – Education and Research. The papers featured mainly focus on information and communications technology (ICT) for computation, algorithms and data analytics. The fundamentals of various data analytics and algorithms discussed are useful to researchers in the field.

Investigating Windows Systems Linux Malware Incident Response: A Practitioner's Guide to Forensic Collection and Examination of Volatile Data

The Advanced Forensic Science Series grew out of the recommendations from the 2009 NAS Report: Strengthening Forensic Science: A Path Forward. This volume, Digital and Document Examination, will serve as a graduate level text for those studying and teaching digital forensics and forensic document examination, as well as an excellent reference for forensic scientist’s libraries or use in their casework. Coverage includes digital devices, transportation, types of documents, forensic accounting and professional issues. Edited by a world-renowned leading forensic expert, the Advanced Forensic Science Series is a long overdue solution for the forensic science community. Provides basic principles of forensic science and an overview of digital forensics and document examination Contains sections on digital devices, transportation, types of documents and forensic accounting Includes sections on professional issues, such as from crime scene to court, forensic laboratory reports and health and safety Incorporates effective pedagogy, key terms, review questions, discussion questions and additional reading suggestions

Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1 Syngress

Digital Forensics: Threatscape and Best Practices surveys the problems and challenges confronting digital forensic professionals today, including massive data sets and everchanging technology. This book provides a coherent overview of the threatscape in a broad range of topics, providing practitioners and students alike with a comprehensive, coherent overview of the threat landscape and what can be done to manage and prepare for it. Digital Forensics: Threatscape and Best Practices delivers you with incisive analysis and best practices from a panel of expert authors, led by John Sammons, bestselling author of The Basics of Digital Forensics. Learn the basics of cryptocurrencies (like Bitcoin) and the artifacts they generate Learn why examination planning matters and how to do it effectively Discover how to incorporate behaviorial analysis into

your digital forensics examinations Stay updated with the key artifacts created by the latest Mac OS, OS X 10.11, El Capitan Discusses the threatscapes and challenges facing mobile device forensics, law enforcement, and legal cases The power of applying the electronic discovery workflows to digital forensics Discover the value of and impact of social media forensics *Malware Forensics Field Guide for Linux Systems* Syngress is Forensic science includes all aspects of investigating a crime, including: chemistry, biology and physics, and also incorporates countless other specialties. Today, the service offered under the guise of "forensic science' includes specialties from virtually all aspects of modern science, medicine, engineering, mathematics and technology. The Encyclopedia of Forensic Sciences, Second Edition is a reference source that will inform both the crime scene worker and the laboratory worker of each other's protocols, procedures and limitations. Written by leading scientists in each area, every article is peer reviewed to establish clarity, accuracy, and comprehensiveness. As reflected in the specialties of its Editorial Board, the contents covers the core theories, methods and techniques employed by forensic scientists – and applications of these that are used in forensic analysis. This 4-volume set represents a 30% growth in articles from the first edition, with a particular increase in coverage of DNA and digital forensics Includes an international collection of contributors The second edition features a new 21-member editorial board, half of which are internationally based Includes over 300 articles, approximately 10pp on average Each article features a) suggested readings which point readers to additional sources for more information, b) a list of related Web sites, c) a 5-10 word glossary and definition paragraph, and d) cross-references to related articles in the encyclopedia Available online via SciVerse ScienceDirect. Please visit www.info.sciencedirect.com for more information This new edition continues the reputation of the first edition, which was awarded an Honorable Mention in the prestigious Dartmouth Medal competition for 2001. This award honors the creation of reference works of outstanding quality and significance, and is sponsored by the RUSA Committee of the American Library Association

Malware Forensics Newnes

Malware Forensics Field Guide for Linux Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems;

legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program. This book will appeal to computer forensic investigators, analysts, and specialists. A compendium of on-the-job tasks and checklists Specific for Linux-based systems in which new malware is developed every day Authors are world-renowned leaders in investigating and analyzing malicious code
Forensic Engineering Academic Conferences and publishing limited
Malware Forensics Field Guide for Windows Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Windows-based systems, the largest running OS in the world. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Windows system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Windows systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Windows system; and analysis of a suspect program. This field guide is intended for computer forensic investigators, analysts, and specialists. A condensed hand-held guide complete with on-the-job tasks and checklists Specific for Windows-based systems, the largest running OS in the world Authors are world-renowned leaders in investigating and analyzing malicious code
Digital-Forensics and Watermarking Academic Press
Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis exposes the latest electronic covert communication techniques used by cybercriminals, along with the needed investigative methods for identifying them. The book shows how to use the Internet for legitimate covert communication, while giving investigators the information they need for detecting cybercriminals who attempt to hide their true identity. Intended for practitioners and investigators, the book offers concrete examples on how to communicate securely, serving as an ideal reference for those who truly need protection, as well as those who investigate cybercriminals. Covers high-level strategies, what they can achieve, and how to implement them Shows discovery and mitigation methods using examples, court cases, and more Explores how social media sites and gaming technologies can be used for illicit communications activities Explores the currently in-use technologies such as TAILS and TOR that help with keeping anonymous online
Proceedings of the Seventh International Workshop on Digital Forensics and Incident Analysis (WDFIA 2012)
Academic Press
Seeking the Truth from Mobile Evidence: Basic Fundamentals,

Intermediate and Advanced Overview of Current Mobile Forensic Investigations will assist those who have never collected mobile evidence and augment the work of professionals who are not currently performing advanced destructive techniques. This book is intended for any professional that is interested in pursuing work that involves mobile forensics, and is designed around the outcomes of criminal investigations that involve mobile digital evidence. Author John Bair brings to life the techniques and concepts that can assist those in the private or corporate sector. Mobile devices have always been very dynamic in nature. They have also become an integral part of our lives, and often times, a digital representation of where we are, who we communicate with and what we document around us. Because they constantly change features, allow user enabled security, and or encryption, those employed with extracting user data are often overwhelmed with the process. This book presents a complete guide to mobile device forensics, written in an easy to understand format. Provides readers with basic, intermediate, and advanced mobile forensic concepts and methodology Thirty overall chapters which include such topics as, preventing evidence contamination, triaging devices, troubleshooting, report writing, physical memory and encoding, date and time stamps, decoding Multi-Media-Messages, decoding unsupported application data, advanced validation, water damaged phones, Joint Test Action Group (JTAG), Thermal and Non-Thermal chip removal, BGA cleaning and imaging, In-System-Programming (ISP), and more Popular JTAG boxes – Z3X and RIFF/RIFF2 are expanded on in detail Readers have access to the companion guide which includes additional image examples, and other useful materials

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications Syngress

Digital evidence--evidence that is stored on or transmitted by computers--can play a major role in a wide range of crimes, including homicide, rape, abduction, child abuse, solicitation of minors, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, espionage, and terrorism. Though an increasing number of criminals are using computers and computer networks, few investigators are well-versed in the evidentiary, technical, and legal issues related to digital evidence. As a result, digital evidence is often overlooked, collected incorrectly, and analyzed ineffectively. The aim of this hands-on resource is to educate students and professionals in the law enforcement, forensic science, computer security, and legal communities about digital evidence and computer crime. This work explains how computers and networks function, how they can be involved in crimes, and how they can be used as a source of evidence. As well as gaining a practical understanding of how computers and networks function and how they can be used as evidence of a crime, readers will learn about relevant legal issues and will be introduced to deductive criminal profiling, a systematic approach to focusing an investigation and understanding criminal motivations.

Digital Forensics with Open Source Tools Springer

The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy presents modern tactics on how to secure computer and mobile devices, including what behaviors are safe while surfing, searching, and interacting with others in the virtual world. The book's author, Professor John Sammons, who teaches

information security at Marshall University, introduces readers to the basic concepts of protecting their computer, mobile devices, and data during a time that is described as the most connected in history. This timely resource provides useful information for readers who know very little about the basic principles of keeping the devices they are connected to—or themselves—secure while online. In addition, the text discusses, in a non-technical way, the cost of connectedness to your privacy, and what you can do to it, including how to avoid all kinds of viruses, malware, cybercrime, and identity theft. Final sections provide the latest information on safe computing in the workplace and at school, and give parents steps they can take to keep young kids and teens safe online. Provides the most straightforward and up-to-date guide to cyber safety for anyone who ventures online for work, school, or personal use Includes real world examples that demonstrate how cyber criminals commit their crimes, and what users can do to keep their data safe

Preserving Electronic Evidence for Trial Syngress
Based on the use of open source tools, this book lends itself to many organizations as well as students who do not have means to purchase new tools for different investigations. Well known forensic methods are demonstrated using open-source computer forensic tools (Sleuthkit, Foremost, dcdd, pyag, etc.) for examining a wide range of target systems (Windows, Mac, Linux, Unix, etc.). The digital forensics industry is growing a rapid pace and this book is perfect for someone entering the field that does not have access to corporate tools. Written by world-renowned forensic practitioners Covers open source forensics tools for all major systems: Windows, Mac, and Linux Uses the most current examination and analysis techniques in the field.

Seeking the Truth from Mobile Evidence Springer
Digital Forensics Trial Graphics: Teaching the Jury Through Effective Use of Visuals helps digital forensic practitioners explain complex technical material to laypeople (i.e., juries, judges, etc.). The book includes professional quality illustrations of technology that help anyone understand the complex concepts behind the science. Users will find invaluable information on theory and best practices along with guidance on how to design and deliver successful explanations. Helps users learn skills for the effective presentation of digital forensic evidence via graphics in a trial setting to laypeople such as juries and judges Presents the principles of visual learning and graphic design as a foundation for developing effective visuals Demonstrates the best practices of slide design to develop effective visuals for presentation of evidence Professionally developed graphics, designed specifically for digital forensics, that you can use at trial Downloadable graphics available at: http://booksite.elsevier.com/9780128034835

Strategic Leadership in Digital Evidence Elsevier
Linux Malware Incident Response: A Practitioner's Guide to Forensic Collection and Examination of Volatile DataElsevier
Digital Forensics Syngress
Crime scenes associated with child sexual exploitation and trafficking in child pornography were once limited to physical locations such as school playgrounds, church vestibules, trusted neighbors' homes, camping trips and seedy darkly lit back rooms of adult bookstores. The explosion of Internet use has created a virtual hunting ground for sexual predators and has fueled a

brisk, multi-billion dollar trade in the associated illicit material. Approximately half of the caseload in computer crimes units involves the computer assisted sexual exploitation of children. Despite the scale of this problem, or perhaps because of it, there are no published resources that bring together the complex mingling of disciplines and expertise required to put together a computer assisted child exploitation case. This work fills this void, providing police, prosecutors and forensic examiners with the historical, legal, technical, and social background for the laws prohibiting child exploitation, in particular, child pornography. The book will become an indispensable resource for those involved in the investigation, prosecution and study of computer-assisted child sexual exploitation. The book provides a history of child exploitation cases and studies, outlining the roles of technology in this type of crime and the evidence they can contain, and documenting new research performed by the authors. It details how successful undercover Internet operations are conducted, how the associated evidence is collected, and how to use the evidence to locate and apprehend the offender. The heart of this work is a legal section, detailing all of the legal issues that arise in Internet child exploitation cases. A forensic examination section presents evidentiary issues from a technical perspective and describes how to conduct a forensic examination of digital evidence gathered in the investigative and probative stages of a child exploitation case. Citations to related documents are provided for readers who want to learn more about certain issues. Actual case examples from computer assisted child exploitation cases are explored, at all times protecting the privacy of the victims while providing enough detail to educate the reader. In addition to providing guidance on the technical and legal aspects of child exploitation investigations, this work identifies and analyzes trends in this type of crime and helps readers understand the similarities and differences between child predators who take to the Internet and predators who do not. Data from the thirty Internet Crimes Against Children (ICAC) Task Forces are compiled and reported to provide a deeper understanding of the types of cases, types of offenders and the level of danger they pose to themselves, their victims, and investigating officers. Also, sex offender data from the Offices of Attorneys General in the United States and similar offices in foreign countries are gathered to increase the study sample size, establish controls, and expand the scope of the research to outside of the United States. - The first comprehensive title in this subject area - It will use real cases and examples of criminal behavior and the means to detect it. - Provides guidelines for developing a Field Manual and a Checklist to supplement the investigation and legal process - Establishes a reliable system and legal, procedural-backed protocol by which to conduct an online sexual investigation and collect evidence

Intelligent Decision Support Systems for Sustainable Computing
Elsevier

Managing Information Security offers focused coverage of how to protect mission critical systems, and how to deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration testing, vulnerability assessment, and more. It offers in-depth coverage of the current technology and practice as it relates to information security management

solutions. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Chapters contributed by leaders in the field covering foundational and practical aspects of information security management, allowing the reader to develop a new level of technical expertise found nowhere else Comprehensive coverage by leading experts allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Encyclopedia of Forensic Sciences CRC Press

Handbook of Digital Forensics and Investigation builds on the success of the Handbook of Computer Crime Investigation, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is also designed as an accompanying text to Digital Evidence and Computer Crime. This unique collection details how to conduct digital investigations in both criminal and civil contexts, and how to locate and utilize digital evidence on computers, networks, and embedded systems. Specifically, the Investigative Methodology section of the Handbook provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery, and Intrusion Investigation. The Technology section is extended and updated to reflect the state of the art in each area of specialization. The main areas of focus in the Technology section are forensic analysis of Windows, Unix, Macintosh, and embedded systems (including cellular telephones and other mobile devices), and investigations involving networks (including enterprise environments and mobile telecommunications technology). This handbook is an essential technical reference and on-the-job guide that IT professionals, forensic practitioners, law enforcement, and attorneys will rely on when confronted with computer related crime and digital evidence of any kind. *Provides methodologies proven in practice for conducting digital investigations of all kinds *Demonstrates how to locate and interpret a wide variety of digital evidence, and how it can be useful in investigations *Presents tools in the context of the investigative process, including EnCase, FTK, ProDiscover, foremost, XACT, Network Miner, Splunk, flow-tools, and many other specialized utilities and analysis platforms *Case examples in every chapter give readers a practical understanding of the technical, logistical, and legal challenges that arise in real investigations

Digital Forensics Elsevier

Digital forensics has been a discipline of Information Security for decades now. Its principles, methodologies, and techniques have remained consistent despite the evolution of technology, and, ultimately, it and can be applied to any form of digital data. However, within a corporate environment, digital forensic professionals are particularly challenged. They must maintain the legal admissibility and forensic viability of digital evidence in support of a broad range of different business functions that include incident response, electronic discovery (ediscovery), and ensuring the controls and accountability of such information across networks. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise provides the methodologies and strategies necessary for these key business functions to seamlessly integrate digital forensic capabilities to

guarantee the admissibility and integrity of digital evidence. In many books, the focus on digital evidence is primarily in the technical, software, and investigative elements, of which there are numerous publications. What tends to get overlooked are the people and process elements within the organization. Taking a step back, the book outlines the importance of integrating and accounting for the people, process, and technology components of digital forensics. In essence, to establish a holistic paradigm—and best-practice procedure and policy approach—to defending the enterprise. This book serves as a roadmap for professionals to successfully integrate an organization's people, process, and technology with other key business functions in an enterprise's digital forensic capabilities.

Deception in the Digital Age Syngress Press

I decided to write this book for a couple of reasons. One was that I've now written a couple of books that have to do with incident response and forensic analysis on Windows systems, and I used a lot of Perl in both books. Okay...I'll come clean...I used nothing but Perl in both books! What I've seen as a result of this is that many readers want to use the tools, but don't know how...they simply aren't familiar with Perl, with interpreted (or scripting) languages in general, and may not be entirely comfortable with running tools at the command line. This book is intended for anyone who has an interest in useful Perl scripting, in particular on the Windows platform, for the purpose of incident response, and forensic analysis, and application monitoring. While a thorough grounding in scripting languages (or in Perl specifically) is not required, it helpful in fully and more completely understanding the material and code presented in this book. This book contains information that is useful to consultants who perform incident response and computer forensics, specifically as those activities pertain to MS Windows systems (Windows 2000, XP, 2003, and some Vista). My hope is that not only will consultants (such as myself) find this material valuable, but so will system administrators, law enforcement officers, and students in undergraduate and graduate programs focusing on computer forensics. *Perl Scripting for Live Response Using Perl, there's a great deal of information you can retrieve from systems, locally or remotely, as part of troubleshooting or investigating an issue. Perl scripts can be run from a central management point, reaching out to remote systems in order to collect information, or they can be "compiled" into standalone executables using PAR, PerlApp, or Perl2Exe so that they can be run on systems that do not have ActiveState's Perl distribution (or any other Perl distribution) installed. *Perl Scripting for Computer Forensic Analysis Perl is an extremely useful and powerful tool for performing computer forensic analysis. While there are applications available that let an examiner access acquired images and perform some modicum of visualization, there are relatively few tools that meet the specific needs of a specific examiner working on a specific case. This is where the use of Perl really shines through and becomes apparent. *Perl Scripting for Application Monitoring Working with enterprise-level Windows applications requires a great deal of analysis and constant monitoring. Automating the monitoring portion of this effort can save a great deal of time, reduce system downtimes, and improve the reliability of your overall application. By utilizing Perl scripts and integrating them with the application technology, you

can easily build a simple monitoring framework that can alert you to current or future application issues.

Related with Digital Forensics Elsevier:
© Digital Forensics Elsevier Fort Benning Basic Training 2022
© Digital Forensics Elsevier Formal Sanctions Definition Sociology
© Digital Forensics Elsevier Forever In Sign Language