Digital Forensics Elsevier

Malware Forensics Field Guide for Windows Systems
Handbook of Digital Forensics and Investigation
Environmental Forensics
Digital Evidence and Computer Crime
Digital Forensics
Investigating Computer-Related Crime, Second Edition
Preserving Electronic Evidence for Trial
Linux Malware Incident Response: A Practitioner's Guide to Forensic Collection and Examination of Volatile Data
Digital Forensics, Investigation, and Response
Encyclopedia of Forensic Sciences
Strategic Leadership in Digital Evidence
Forensic Textile Science
Windows Registry Forensics
Contemporary Digital Forensic Investigations of Cloud and Mobile Applications
Cyber Forensics
The Basics of Digital Forensics
Ethics in Forensic Science
The Best Damn Cybercrime and Digital Forensics Book Period
Introductory Computer Forensics
Digital and Document Examination
Malware Forensics Field Guide for Linux Systems

Digital Forensics Explained
Placing the Suspect Behind the Keyboard
Strategic Leadership in Digital Evidence
Digital Forensics for Legal Professionals
Digital Evidence and Computer Crime
Cloud Storage Forensics
Digital Forensics with Open Source Tools
Handbook of Computer Crime Investigation
Digital Forensics Trial Graphics
Digital Forensics for Network, Internet, and Cloud Computing
Fundamentals of Forensic Science
Implementing Digital Forensic Readiness
Investigating Windows Systems
Introduction to Environmental Forensics
Digital Forensics Processing and Procedures
Seeking the Truth from Mobile Evidence
Alternate Data Storage Forensics
Malware Forensics
Forensic Engineering

ZAYDEN NIXON

Malware Forensics Field Guide for Windows Systems
Elsevier
This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable

forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody--from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab A comprehensive guide for all roles in a digital forensics laboratory Based on international standards and certifications Handbook of Digital Forensics and Investigation Syngress 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 *Environmental Forensics* CRC Press This book covers the full life cycle of conducting a mobile and computer digital forensic examination, including planning and performing an investigation as well as

report writing and testifying. Case reviews in corporate, civil, and criminal situations are also described from both prosecution and defense perspectives. Digital Forensics Explained, Second Edition draws from years of experience in local, state, federal, and international environments and highlights the challenges inherent in deficient cyber security practices. Topics include the importance of following the scientific method and verification, legal and ethical issues, planning an investigation (including tools and techniques), incident response, case project management and authorization, social media and internet, cloud, anti-forensics, link and visual analysis, and psychological considerations. The book is a valuable resource for the academic environment, law enforcement, those in the legal profession, and those working in the cyber security field. Case reviews include cyber security breaches, anti-forensic challenges, child exploitation, and social media investigations. Greg Gogolin, PhD, CISSP, is a Professor of Information Security and Intelligence at Ferris State University and a licensed Professional Investigator. He has worked more than 100 cases in criminal, civil, and corporate environments.

Digital Evidence and Computer Crime

Elsevier

Digital Forensics,

Investigation, and Response, Fourth Edition examines the fundamentals of system forensics, addresses the tools, techniques, and methods used to perform computer forensics and investigation, and explores incident and intrusion response,

Digital Forensics

Syngress

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

Investigating Computer-Related Crime, Second Edition Elsevier

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book’s 21 chapters focuses on a

particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students' understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or

researchers working in these related fields as a reference book.

Preserving Electronic Evidence for Trial Springer

The Basics of Digital Forensics provides a foundation for people new to the digital forensics field. This book offers guidance on how to conduct examinations by discussing what digital forensics is, the methodologies used, key tactical concepts, and the tools needed to perform examinations. Details on digital forensics for computers, networks, cell phones, GPS, the cloud and the Internet are discussed. Also, learn how to collect evidence, document the scene, and how deleted data can be recovered. The new Second Edition of this book provides the reader with real-world examples and all the key technologies used in digital forensics, as well as new coverage of network intrusion response, how hard drives are organized, and electronic discovery. This valuable resource also covers how to incorporate quality assurance into an investigation, how to prioritize evidence items to examine (triage), case processing, and what goes into making an expert witness. Learn what Digital Forensics entails Build a toolkit and prepare an investigative plan Understand the common artifacts to look for in an exam Second Edition features all-new coverage of hard

drives, triage, network intrusion response, and electronic discovery; as well as updated case studies and expert interviews

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

Placing the Suspect Behind the Keyboard is the definitive book on conducting a complete investigation of a cybercrime using digital forensics techniques as well as physical investigative procedures. This book merges a digital analysis examiner's work with the work of a case investigator in order to build a solid case to identify and prosecute cybercriminals. Brett Shavers links traditional investigative techniques with high tech crime analysis in a manner that not only determines elements of crimes, but also places the suspect at the keyboard. This book is a first in combining investigative strategies of digital forensics analysis processes alongside physical investigative techniques in which the reader will gain a holistic approach to their current and future cybercrime investigations. Learn the tools and investigative principles of both physical and digital cybercrime investigations—and how they fit together to build a solid and complete case Master the techniques of conducting a holistic investigation that combines both digital

and physical evidence to track down the "suspect behind the keyboard" The only book to combine physical and digital investigative techniques
Digital Forensics, Investigation, and Response CRC Press
The third edition of Introduction to Environmental Forensics is a state-of-the-art reference for the practicing environmental forensics consultant, regulator, student, academic, and scientist, with topics including compound-specific isotope analysis (CSIA), advanced multivariate statistical techniques, surrogate approaches for contaminant source identification and age dating, dendroecology, hydrofracking, releases from underground storage tanks and piping, and contaminant-transport modeling for forensic applications. Recognized international forensic scientists were selected to author chapters in their specific areas of expertise and case studies are included to illustrate the application of these methods in actual environmental forensic investigations. This edition provides updates on advances in various techniques and introduces several new topics. Provides a comprehensive review of all aspects of environmental forensics Coverage ranges from emerging statistical methods to state-of-the-art analytical techniques,

such as gas chromatography-combustion-isotope ratio mass spectrometry and polytopic vector analysis Numerous examples and case studies are provided to illustrate the application of these forensic techniques in environmental investigations

Encyclopedia of Forensic Sciences

Academic Press

Malware Forensics: Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system. It is the first book detailing how to perform live forensic techniques on malicious code. The book gives deep coverage on the tools and techniques of conducting runtime

behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more. It explores over 150 different tools for malware incident response and analysis, including forensic tools for preserving and analyzing computer memory. Readers from all educational and technical backgrounds will benefit from the clear and concise explanations of the applicable legal case law and statutes covered in every chapter. In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter. This book is intended for system administrators, information security professionals, network personnel, forensic examiners, attorneys, and law enforcement working with the inner-workings of computer memory and malicious code. Winner of Best Book Bejtlich read in 2008! http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader First book to detail how to perform "live forensic"

techniques on malicous code In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

Strategic Leadership in Digital Evidence CRC Press

Unlike other books, courses and training that expect an analyst to piece together individual instructions into a cohesive investigation, Investigating Windows Systems provides a walk-through of the analysis process, with descriptions of the thought process and analysis decisions along the way. Investigating Windows Systems will not address topics which have been covered in other books, but will expect the reader to have some ability to discover the detailed usage of tools and to perform their own research. The focus of this volume is to provide a walk-through of the analysis process, with descriptions of the thought process and the analysis decisions made along the way. A must-have guide for those in the field of digital forensic analysis and incident response. Provides the reader with a detailed walk-through of the analysis process, with decision points along the way, assisting the user in understanding the resulting data Coverage will include malware detection, user activity, and how to set up a testing environment Written at

a beginner to intermediate level for anyone engaging in the field of digital forensic analysis and incident response

Forensic Textile Science Academic Press

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 *Windows Registry Forensics* Syngress The word "ethical" can be defined as proper conduct. A failure of forensic scientists to act ethically can result in serious adverse outcomes. However, while seemingly simple to define, the application of being "ethical" is somewhat more obscure. That is, when is ethical, ethical, and when is it not? Because we have an adversarial legal system, differences of opinion exist in forensic science. However, there are instances when differences are so divergent that an individual's ethics are called into question. In light of not only the O.J. Simpson trial - the first national trial to question the ethical behavior of forensic scientists - and the National Academy of Science critique of forensic science, ethical issues have come to the forefront of concern within the forensic community. Ethics in Forensic Science draws upon the expertise of the editors and numerous contributors in order to present several different perspectives with the goal of better understanding when ethical lines are crossed. In order to achieve this goal, comparisons of various canons of ethics from medicine, law, science, religion, and politics will be examined and applied. Lastly, case studies will be

presented to illustrate ethical dilemmas and provide a real-world context for readers. Edited by a well known forensic attorney/consultant and a leading medical examiner, Ethics in Forensic Science addresses the concerns of the entire forensic community - the laboratory, medical examiner, and crime scene investigator. It will be an invaluable reference for practitioners in forensic and/or criminal justice programs, crime scene investigators/photographers, law enforcement training centers, police academies and local agencies, as well as forensic consultants and forensic scientists.

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications Elsevier Strategic Leadership in Digital Evidence: What Executives Need to Know provides leaders with broad knowledge and understanding of practical concepts in digital evidence, along with its impact on investigations. The book's chapters cover the differentiation of related fields, new market technologies, operating systems, social networking, and much more. This guide is written at the layperson level, although the audience is expected to have reached a level of achievement and seniority in their profession, principally law enforcement, security and intelligence. Additionally, this book will appeal to legal professionals and

others in the broader justice system. Covers a broad range of challenges confronting investigators in the digital environment Addresses gaps in currently available resources and the future focus of a fast-moving field Written by a manager who has been a leader in the field of digital forensics for decades

Cyber Forensics
Syngress
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

The Basics of Digital Forensics Elsevier Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators;

forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems Ethics in Forensic Science Elsevier 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

The Best Damn Cybercrime and Digital Forensics Book Period

Academic Press Electronic discovery refers to a process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case. Computer forensics is the application of computer investigation and analysis techniques to perform an investigation to find out exactly what happened on a computer and who was responsible. IDC estimates that the U.S. market for computer forensics will be grow from $252 million in 2004 to $630 million by 2009. Business is strong outside the United States, as well. By 2011, the estimated international market will be $1.8 billion dollars. The Techno Forensics Conference has increased in size by almost 50% in its second year; another example of the rapid growth in the market. This book is the first to combine cybercrime and digital forensic topics to provides law enforcement and IT security professionals with the information needed to manage a digital investigation. Everything needed for analyzing forensic data and recovering digital evidence can be found in one place, including

instructions for building a digital forensics lab. * Digital investigation and forensics is a growing industry * Corporate I.T. departments investigating corporate espionage and criminal activities are learning as they go and need a comprehensive guide to e-discovery * Appeals to law enforcement agencies with limited budgets *Introductory Computer Forensics* Elsevier Contemporary Digital Forensic Investigations of Cloud and Mobile Applications comprehensively discusses the implications of cloud (storage) services and mobile applications on digital forensic investigations. The book provides both digital forensic practitioners and researchers with an up-to-date and advanced knowledge of collecting and preserving electronic evidence from different types of cloud services, such as digital remnants of cloud applications accessed through mobile devices. This is the first book that covers the investigation of a wide range of cloud services. Dr. Kim-Kwang Raymond Choo and Dr. Ali Dehghantanha are leading researchers in cloud and mobile security and forensics, having organized research, led research, and been published widely in the field. Users will gain a deep overview of seminal research in the field while also identifying prospective future research topics and

open challenges. Presents the most current, leading edge research on cloud and mobile application forensics, featuring a panel of top experts in the field Introduces the first book to provide an in-depth overview of the issues surrounding digital forensic investigations in cloud and associated mobile apps Covers key technical topics and provides readers with a complete understanding of the most current research findings Includes discussions on future research directions and challenges

Digital and Document Examination

Academic Press

Learn to pull “digital fingerprints from alternate data storage (ADS) devices including: iPod, Xbox, digital cameras and more from the cyber sleuths who train the Secret Service, FBI, and Department of Defense in bleeding edge digital forensics techniques. This book sets a new forensic methodology standard for investigators to use. This book begins by describing how alternate data storage devices are used to both move and hide data. From here a series of case studies using bleeding edge forensic analysis tools demonstrate to readers how to perform forensic investigations on a variety of ADS devices including: Apple iPods, Digital Video Recorders, Cameras, Gaming Consoles (Xbox, PS2, and PSP), Bluetooth devices, and more

using state of the art tools. Finally, the book takes a look into the future at “not yet every day devices which will soon be common repositories for hiding and moving data for both legitimate and illegitimate purposes. Authors are undisputed leaders who train the Secret Service, FBI, and Department of Defense Book presents "one of a kind" bleeding edge information that absolutely can not be found anywhere else Today the industry has exploded and cyber investigators can be found in almost every field