

Real Digital Forensics Computer Security And Incident Response Mixed Media Product

Security, Privacy, and Digital Forensics in the Cloud
Computer Security Handbook, Set
Digital Forensics
Real Digital Forensics
Digital Evidence and Computer Crime
Guide to Computer Forensics and Investigations
The Best Damn Cybercrime and Digital Forensics Book Period
Digital Forensics Explained
Real Digital Forensics
Computer Forensics For Dummies
Digital Forensics Trial Graphics
Big Data Analytics and Computing for Digital Forensic Investigations
Digital Forensics for Handheld Devices
Big Digital Forensic Data
Implementing Digital Forensic Readiness
Fundamentals of Digital Forensics
Computer and Information Security Handbook
Digital Forensics
Contemporary Digital Forensic Investigations of Cloud and Mobile Applications
Practical Cyber Forensics
Digital Forensics Basics
Real digital forensics
What Every Engineer Should Know About Cyber Security and Digital Forensics
Introduction to Security and Network Forensics
Internet Forensics
Digital Forensics Processing and Procedures
Digital Forensic Science
Digital Forensics with Open Source Tools
Digital Forensics and Incident Response
Investigating Windows Systems
What Every Engineer Should Know About Cyber Security and Digital Forensics
Real digital forensics
Cybercrime and Digital Forensics
Digital Forensics and Investigations
Handbook of Digital Forensics and Investigation
The Basics of Digital Forensics
Cyber Forensics
Cybersecurity Fundamentals
Digital Forensics and Incident Response
Hands-on Incident Response and Digital Forensics

Security, Privacy, and Digital Forensics in the Cloud

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 behavioral 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 threatscape 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

Computer Security Handbook, Set

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

Digital Forensics

Uncover a digital trail of e-evidence by using the helpful, easy-to-understand information in Computer Forensics For Dummies! Professional and armchair investigators alike can learn the basics of computer forensics, from digging out electronic evidence to solving the case. You won't need a computer science degree to master e-discovery. Find and filter data in mobile devices, e-mail, and other Web-based technologies. You'll learn all about e-mail and Web-based forensics, mobile forensics, passwords and encryption, and other e-evidence found through VoIP, voicemail, legacy mainframes, and databases. You'll discover how to use the latest forensic software, tools, and equipment to find the answers that you're looking for in record time. When you understand how data is stored, encrypted, and recovered, you'll be able to protect your personal privacy as well. By the time you finish reading this book, you'll know how to: Prepare for and conduct computer forensics investigations Find and filter data Protect personal privacy Transfer evidence without contaminating it Anticipate legal loopholes and opponents' methods Handle passwords and encrypted data Work with the courts and win the case Plus, Computer Forensics for Dummies includes lists of things that everyone interested in computer forensics should know, do, and build. Discover how to get qualified for a career in computer forensics, what to do to be a great investigator and expert witness, and how to build a forensics lab or toolkit. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Real Digital Forensics

Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems as well as application standards and technologies required to build secure VPNs, configure client software and server operating systems, IPsec-

enabled routers, firewalls and SSL clients. This comprehensive book will provide essential knowledge and skills needed to select, design and deploy a public key infrastructure (PKI) to secure existing and future applications. * Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical expertise * Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple viewpoints * Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Digital Evidence and Computer Crime

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, What Every Engineer Should Know About Cyber Security and Digital Forensics is an overview of the field of cyber security. Exploring the cyber security topics that every engineer should understand, the book discusses: Network security Personal data security Cloud computing Mobile computing Preparing for an incident Incident response Evidence handling Internet usage Law and compliance Security and forensic certifications Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of cyber security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding profession.

Guide to Computer Forensics and Investigations

The Best Damn Cybercrime and Digital Forensics Book Period

Given our increasing dependency on computing technology in daily business processes, and the growing opportunity to use engineering technologies to engage in illegal, unauthorized, and unethical acts aimed at corporate infrastructure, every organization is at risk. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence o

Digital Forensics Explained

Keeping up with the latest developments in cyber security requires ongoing commitment, but without a firm foundation in the principles of computer security and digital forensics, those tasked with safeguarding private information can get lost in a turbulent and shifting sea. Providing such a foundation, Introduction to Security and Network Forensics covers the basic principles of intrusion detection systems, encryption, and authentication, as well as the key academic principles related to digital forensics. Starting with an overview of general security concepts, it addresses hashing, digital certificates, enhanced software security, and network

security. The text introduces the concepts of risk, threat analysis, and network forensics, and includes online access to an abundance of ancillary materials, including labs, Cisco challenges, test questions, and web-based videos. The author provides readers with access to a complete set of simulators for routers, switches, wireless access points (Cisco Aironet 1200), PIX/ASA firewalls (Version 6.x, 7.x and 8.x), Wireless LAN Controllers (WLC), Wireless ADUs, ASDMs, SDMs, Juniper, and much more, including: More than 3,700 unique Cisco challenges and 48,000 Cisco Configuration Challenge Elements 60,000 test questions, including for Certified Ethical Hacking and CISSP® 350 router labs, 180 switch labs, 160 PIX/ASA labs, and 80 Wireless labs Rounding out coverage with a look into more advanced topics, including data hiding, obfuscation, web infrastructures, and cloud and grid computing, this book provides the fundamental understanding in computer security and digital forensics required to develop and implement effective safeguards against ever-evolving cyber security threats. Along with this, the text includes a range of online lectures and related material, available at: <http://asecuritybook.com>.

Real Digital Forensics

Implementing Digital Forensic Readiness: From Reactive to Proactive Process, Second Edition presents the optimal way for digital forensic and IT security professionals to implement a proactive approach to digital forensics. The book details how digital forensic processes can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and reducing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stances, a company's preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

Computer Forensics For Dummies

The Basics of Digital Forensics provides a foundation for people new to the digital forensics field. This book teaches you 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 you with completely up-to-date 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. You'll also learn 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. The Second Edition also features expanded resources and references, including online resources that keep you current, sample legal documents, and suggested further reading. 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, expert interviews, and expanded resources and references

Digital Forensics Trial Graphics

Incident response is the method by which organisations take steps to identify and recover from an information security incident, with as little impact as possible on business as usual. Digital forensics is what follows - a scientific investigation into the causes of an incident with the aim of bringing the perpetrators to justice. These two disciplines have a close but complex relationship and require a balancing act to get right, but both are essential when an incident occurs. In this practical guide, the relationship between incident response and digital forensics is explored and you will learn how to undertake each and balance them to meet the needs of an organisation in the event of an information security incident. Best practice tips and real-life examples are included throughout.

Big Data Analytics and Computing for Digital Forensic Investigations

Digital forensics has recently gained a notable development and become the most demanding area in today's information security requirement. This book investigates the areas of digital forensics, digital investigation and data analysis procedures as they apply to computer fraud and cybercrime, with the main objective of describing a variety of digital crimes and retrieving potential digital evidence. Big Data Analytics and Computing for Digital Forensic Investigations gives a contemporary view on the problems of information security. It presents the idea that protective mechanisms and software must be integrated along with forensic capabilities into existing forensic software using big data computing tools and techniques. Features Describes trends of digital forensics served for big data and the challenges of evidence acquisition Enables digital forensic investigators and law enforcement agencies to enhance their digital investigation capabilities with the application of data science analytics, algorithms and fusion technique This book is focused on helping professionals as well as researchers to get ready with next-generation security systems to mount the rising challenges of computer fraud and cybercrimes as well as with digital forensic investigations. Dr Suneeta Satpathy has more than ten years of teaching experience in different subjects of the Computer Science and Engineering discipline. She is currently working as an associate professor in the Department of Computer Science and Engineering, College of Bhubaneswar, affiliated with Biju Patnaik University and Technology, Odisha. Her research interests include computer forensics, cybersecurity, data fusion, data mining, big data analysis and decision mining. Dr Sachi Nandan Mohanty is an associate professor in the Department of Computer Science and Engineering at ICFAI Tech, ICFAI Foundation for Higher Education, Hyderabad,

India. His research interests include data mining, big data analysis, cognitive science, fuzzy decision-making, brain-computer interface, cognition and computational intelligence.

Digital Forensics for Handheld Devices

Digital forensic science, or digital forensics, is the application of scientific tools and methods to identify, collect, and analyze digital (data) artifacts in support of legal proceedings. From a more technical perspective, it is the process of reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system or (digital) artifacts. Over the last three decades, the importance of digital evidence has grown in lockstep with the fast societal adoption of information technology, which has resulted in the continuous accumulation of data at an exponential rate. Simultaneously, there has been a rapid growth in network connectivity and the complexity of IT systems, leading to more complex behavior that needs to be investigated. The goal of this book is to provide a systematic technical overview of digital forensic techniques, primarily from the point of view of computer science. This allows us to put the field in the broader perspective of a host of related areas and gain better insight into the computational challenges facing forensics, as well as draw inspiration for addressing them. This is needed as some of the challenges faced by digital forensics, such as cloud computing, require qualitatively different approaches; the sheer volume of data to be examined also requires new means of processing it.

Big Digital Forensic Data

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

Implementing Digital Forensic Readiness

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

Fundamentals of Digital Forensics

Cybersecurity Fundamentals: A Real-World Perspective explains detailed concepts within computer networks and computer security in an easy-to-understand way, making it the perfect introduction to the topic. This book covers fundamental issues using practical examples and real-world applications to give readers a rounded understanding of the subject and how it is applied. The first three chapters provide a deeper perspective on computer networks, cybersecurity, and different types of cyberattacks that hackers choose to unleash on cyber environments. It then goes on to cover the types of major computer malware and cybersecurity attacks that shook the cyber world in the recent years, detailing the attacks and analyzing their impact on the global economy. The details of the malware codes that help the hacker initiate the hacking attacks on networks are fully described. It then covers high-tech cybersecurity programs, devices, and mechanisms that are extensively adopted in modern security systems. Examples of those systems include intrusion detection systems (IDS), intrusion prevention systems (IPS), and security firewalls. It demonstrates how modern technologies can be used to create and manage passwords for secure data. This book also covers aspects of wireless networks and their security mechanisms. The details of the most commonly used Wi-Fi routers are provided with step-by-step procedures to configure and secure them more efficiently. Test questions are included throughout the chapters to ensure comprehension of the material. Along with this book's step-by-step approach, this will allow undergraduate students of cybersecurity, network security, and related disciplines to gain a quick grasp of the fundamental topics in the area. No prior knowledge is needed to get the full benefit of this book.

Computer and Information Security Handbook

The field of computer forensics has experienced significant growth recently and those looking to get into the industry have significant opportunity for upward mobility. Focusing on the concepts investigators need to know to conduct a

thorough investigation, *Digital Forensics Explained* provides an overall description of the forensic practice from a practitioner's perspective. Starting with an overview, the text describes best practices based on the author's decades of experience conducting investigations and working in information technology. It illustrates the forensic process, explains what it takes to be an investigator, and highlights emerging trends. Filled with helpful templates and contributions from seasoned experts in their respective fields, the book includes coverage of: Internet and email investigations Mobile forensics for cell phones, iPads, music players, and other small devices Cloud computing from an architecture perspective and its impact on digital forensics Anti-forensic techniques that may be employed to make a forensic exam more difficult to conduct Recoverability of information from damaged media The progression of a criminal case from start to finish Tools that are often used in an examination, including commercial, free, and open-source tools; computer and mobile tools; and things as simple as extension cords Social media and social engineering forensics Case documentation and presentation, including sample summary reports and a cover sheet for a cell phone investigation The text includes acquisition forms, a sequential process outline to guide your investigation, and a checklist of supplies you'll need when responding to an incident. Providing you with the understanding and the tools to deal with suspects who find ways to make their digital activities hard to trace, the book also considers cultural implications, ethics, and the psychological effects that digital forensics investigations can have on investigators.

Digital Forensics

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>

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications

Practical Cyber Forensics

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

Digital Forensics Basics

Because it's so large and unregulated, the Internet is a fertile breeding ground for all kinds of scams and schemes. Usually it's your credit card number they're after, and they won't stop there. Not just mere annoyances, these scams are real crimes, with real victims. Now, thanks to Internet Forensics from O'Reilly, there's something you can do about it. This practical guide to defending against Internet fraud gives you the skills you need to uncover the origins of the spammers, con artists, and identity thieves that plague the Internet. Targeted primarily at the developer community, Internet Forensics shows you how to extract the information that lies hidden in every email message, web page, and web server on the Internet. It describes the lengths the bad guys will go to cover their tracks, and offers tricks that you can use to see through their disguises. You'll also gain an understanding for how the Internet functions, and how spammers use these protocols to their devious advantage. The book is organized around the core technologies of the Internet-email, web sites, servers, and browsers. Chapters describe how these are used and abused and show you how information hidden in each of them can be revealed. Short examples illustrate all the major techniques that are discussed. The ethical and legal issues that arise in the uncovering of Internet abuse are also addressed. Not surprisingly, the audience for Internet Forensics is boundless. For developers, it's a serious foray into the world of Internet security; for weekend surfers fed up with spam, it's an entertaining and fun guide that lets them play amateur detective from the safe confines of their home or office.

Real digital forensics

Explains both cloud security and privacy, and digital forensics in a unique, systematic way Discusses both security and privacy of cloud and digital forensics in a systematic way Contributions by top U.S., Chinese and international researchers, and professionals active in the field of information / network security, digital / computer forensics, and the cloud and big data Of interest to those focused upon security and implementation, and those focused upon incident management Logical, well-structured and organized

What Every Engineer Should Know About Cyber Security and Digital Forensics

Introduction to Security and Network Forensics

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

Internet Forensics

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigations Gather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of

Windows operating systems covering Windows 10-specific feature forensics Utilize anti-forensic techniques, including steganography, data destruction techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals

Digital Forensics Processing and Procedures

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

Digital Forensic Science

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, What Every Engineer Should Know About Cyber Security and Digital Forensics is an overview of the field of cyber security. Exploring the cyber security topics that every engineer should understand, the book discusses: Network security Personal data security Cloud computing Mobile computing Preparing for an incident Incident response Evidence handling Internet usage Law and compliance Security and forensic certifications Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of cyber security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding profession.

Digital Forensics with Open Source Tools

The emergence of the World Wide Web, smartphones, and Computer-Mediated Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives, computer hacking and digital piracy,

economic crime and online fraud, pornography and online sex crime, cyber-bullying and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation and the sociology of technology.

Digital Forensics and Incident Response

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 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.

Investigating Windows Systems

Learners will master the skills necessary to launch and complete a successful computer investigation with the updated fourth edition of this popular book, *GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS*. This resource guides readers through conducting a high-tech investigation, from acquiring digital evidence to reporting its findings. Updated coverage includes new software and technologies as well as up-to-date reference sections. Learn how to set up a forensics lab, how to acquire the proper and necessary tools, and how to conduct the investigation and subsequent digital analysis. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

What Every Engineer Should Know About Cyber Security and

Digital Forensics

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field. Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters. Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics. Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals, illustrations and case example images. Features real-world examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media. Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

Real digital forensics

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.

Cybercrime and Digital Forensics

Become an effective cyber forensics investigator and gain a collection of practical, efficient techniques to get the job done. Diving straight into a discussion of anti-

forensic techniques, this book shows you the many ways to effectively detect them. Now that you know what you are looking for, you'll shift your focus to network forensics, where you cover the various tools available to make your network forensics process less complicated. Following this, you will work with cloud and mobile forensic techniques by considering the concept of forensics as a service (FaSS), giving you cutting-edge skills that will future-proof your career. Building on this, you will learn the process of breaking down malware attacks, web attacks, and email scams with case studies to give you a clearer view of the techniques to be followed. Another tricky technique is SSD forensics, so the author covers this in detail to give you the alternative analysis techniques you'll need. To keep you up to speed on contemporary forensics, Practical Cyber Forensics includes a chapter on Bitcoin forensics, where key crypto-currency forensic techniques will be shared. Finally, you will see how to prepare accurate investigative reports. What You Will Learn Carry out forensic investigation on Windows, Linux, and macOS systems Detect and counter anti-forensic techniques Deploy network, cloud, and mobile forensics Investigate web and malware attacks Write efficient investigative reports Who This Book Is For Intermediate infosec professionals looking for a practical approach to investigative cyber forensics techniques.

Digital Forensics and Investigations

The classic and authoritative reference in the field of computer security, now completely updated and revised With the continued presence of large-scale computers; the proliferation of desktop, laptop, and handheld computers; and the vast international networks that interconnect them, the nature and extent of threats to computer security have grown enormously. Now in its fifth edition, Computer Security Handbook continues to provide authoritative guidance to identify and to eliminate these threats where possible, as well as to lessen any losses attributable to them. With seventy-seven chapters contributed by a panel of renowned industry professionals, the new edition has increased coverage in both breadth and depth of all ten domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium (ISC). Of the seventy-seven chapters in the fifth edition, twenty-five chapters are completely new, including: 1. Hardware Elements of Security 2. Fundamentals of Cryptography and Steganography 3. Mathematical models of information security 4. Insider threats 5. Social engineering and low-tech attacks 6. Spam, phishing, and Trojans: attacks meant to fool 7. Biometric authentication 8. VPNs and secure remote access 9. Securing Peer2Peer, IM, SMS, and collaboration tools 10. U.S. legal and regulatory security issues, such as GLBA and SOX Whether you are in charge of many computers or just one important one, there are immediate steps you can take to safeguard your computer system and its contents. Computer Security Handbook, Fifth Edition equips you to protect the information and networks that are vital to your organization.

Handbook of Digital Forensics and Investigation

An interactive book-and-DVD package designed to help readers master the tools and techniques of forensic analysis offers a hands-on approach to identifying and solving problems related to computer security issues; introduces the tools, methods, techniques, and applications of computer forensic investigation; and

allows readers to test skills by working with real data with the help of five scenarios. Original. (Intermediate)

The Basics of Digital Forensics

Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques

Key Features

- Create a solid incident response framework and manage cyber incidents effectively
- Perform malware analysis for effective incident response
- Explore real-life scenarios that effectively use threat intelligence and modeling techniques

Book Description

An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn

- Create and deploy an incident response capability within your own organization
- Perform proper evidence acquisition and handling
- Analyze the evidence collected and determine the root cause of a security incident
- Become well-versed with memory and log analysis
- Integrate digital forensic techniques and procedures into the overall incident response process
- Understand the different techniques for threat hunting
- Write effective incident reports that document the key findings of your analysis

Who this book is for

This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

Cyber Forensics

A practical guide to deploying digital forensic techniques in response to cyber security incidents

About This Book

- Learn incident response fundamentals and create an effective incident response framework
- Master forensics investigation utilizing digital investigative techniques
- Contains real-life scenarios that effectively use threat intelligence and modeling techniques

Who This Book Is For

This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the

incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.

Cybersecurity Fundamentals

This hands-on textbook provides an accessible introduction to the fundamentals of digital forensics. The text contains thorough coverage of the theoretical foundations, explaining what computer forensics is, what it can do, and also what it can't. A particular focus is presented on establishing sound forensic thinking and methodology, supported by practical guidance on performing typical tasks and using common forensic tools. Emphasis is also placed on universal principles, as opposed to content unique to specific legislation in individual countries. Topics and features: introduces the fundamental concepts in digital forensics, and the steps involved in a forensic examination in a digital environment; discusses the nature of what cybercrime is, and how digital evidence can be of use during criminal investigations into such crimes; offers a practical overview of common practices for cracking encrypted data; reviews key artifacts that have proven to be important in several cases, highlighting where to find these and how to correctly interpret them; presents a survey of various different search techniques, and several forensic tools that are available for free; examines the functions of AccessData Forensic Toolkit and Registry Viewer; proposes methods for analyzing applications, timelining, determining the identity of the computer user, and deducing if the computer was remote controlled; describes the central concepts relating to computer memory management, and how to perform different types of memory analysis using the open source tool Volatility; provides review questions and practice tasks at the end of most chapters, and supporting video lectures on YouTube. This easy-to-follow primer is an essential resource for students of computer forensics, and will also serve as a valuable reference for practitioners seeking instruction on performing

forensic examinations in law enforcement or in the private sector.

Digital Forensics and Incident Response

Approximately 80 percent of the world's population now owns a cell phone, which can hold evidence or contain logs about communications concerning a crime. Cameras, PDAs, and GPS devices can also contain information related to corporate policy infractions and crimes. Aimed to prepare investigators in the public and private sectors, *Digital Forensics for Handheld Devices* examines both the theoretical and practical aspects of investigating handheld digital devices. This book touches on all areas of mobile device forensics, including topics from the legal, technical, academic, and social aspects of the discipline. It provides guidance on how to seize data, examine it, and prepare it as evidence for court. This includes the use of chain of custody forms for seized evidence and Faraday Bags for digital devices to prevent further connectivity and tampering of evidence. Emphasizing the policies required in the work environment, the author provides readers with a clear understanding of the differences between a corporate investigation and a criminal investigation. The book also: Offers best practices for establishing an incident response policy and seizing data from company or privately owned digital devices Provides guidance in establishing dedicated examinations free of viruses, spyware, and connections to other devices that could taint evidence Supplies guidance on determining protocols for complicated crime scenes with external media and devices that may have connected with the handheld device Considering important privacy issues and the Fourth Amendment, this book facilitates an understanding of how to use digital forensic tools to investigate the complete range of available digital devices, including flash drives, cell phones, PDAs, digital cameras, and netbooks. It includes examples of commercially available digital forensic tools and ends with a discussion of the education and certifications required for various careers in mobile device forensics.

Hands-on Incident Response and Digital Forensics

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

[ROMANCE](#) [ACTION & ADVENTURE](#) [MYSTERY & THRILLER](#) [BIOGRAPHIES &
HISTORY](#) [CHILDREN'S](#) [YOUNG ADULT](#) [FANTASY](#) [HISTORICAL FICTION](#) [HORROR](#)
[LITERARY FICTION](#) [NON-FICTION](#) [SCIENCE FICTION](#)