

Real Digital Forensics Computer Security And Incident Response

The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

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-word 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.

CYBER SECURITY AND DIGITAL FORENSICS Cyber security is an incredibly important issue that is constantly changing, with new methods, processes, and technologies coming online all the time. Books like this are invaluable to professionals working in this area, to stay abreast of all of these changes. Current cyber threats are getting more complicated and advanced with the rapid evolution of adversarial techniques. Networked computing and portable electronic devices have broadened the role of digital forensics beyond traditional investigations into computer crime. The overall increase in the use of computers as a way of storing and retrieving high-security information requires appropriate security measures to protect the entire computing and communication scenario worldwide. Further, with the introduction of the internet and its underlying technology, facets of information security are becoming a primary concern to protect networks and cyber infrastructures from various threats. This groundbreaking new volume, written and edited by a wide range of professionals in this area, covers broad technical and socio-economic perspectives for the utilization of information and communication technologies and the development of practical solutions in cyber security and digital forensics. Not just for the professional working in the field, but also for the student or academic on the university level, this is a must-have for any library. Audience: Practitioners, consultants, engineers, academics, and other professionals working in the areas of cyber analysis, cyber security, homeland security, national defense, the protection of national critical infrastructures, cyber-crime, cyber vulnerabilities, cyber-attacks related to network systems, cyber threat reduction planning, and those who provide leadership in cyber security management both in public and private sectors

Explains both cloud security and privacy, and digital forensics in a unique, systematical 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

Practical Linux Forensics

Incident Response Essentials

A beginner's guide to searching, analyzing, and securing digital evidence

Digital Forensics and Incident Response

Proceedings of ICCSDF 2021

Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition

From getting started to in-depth discovery, a complete library for anyone dealing with forensics.

This book features high-quality research papers presented at the International Conference on Applications and Techniques in Cyber Security and Digital Forensics (ICCSDF 2021), held at The NorthCap University, Gurugram, Haryana, India, during April 3–4, 2021. This book discusses the topics ranging from information security to cryptography, mobile application attacks to digital forensics, and from cyber security to blockchain. The goal of the book is to provide 360-degree view of cybersecurity to the readers which include cyber security issues, threats, vulnerabilities, novel idea, latest technique and technology, and mitigation of threats and attacks along with demonstration of practical applications. This book also highlights the latest development, challenges, methodologies as well as other emerging areas in this field. It brings current understanding of common Web vulnerabilities while maintaining awareness and knowledge of contemporary standards, practices, procedures, and methods of Open Web Application Security Project. It also expounds how to recover information after a cybercrime.

"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.

This is an analysis of the major security weaknesses and loopholes of the Internet and of some solutions to those problems. The book informs readers of problems that are currently unsolvable and cautions them to the tricks which hackers use, offering solutions to such problems.

Digital Forensics, Investigation, and Response

An Introduction

Digital Forensics Processing and Procedures

Incident Response & Computer Forensics, Third Edition

Cyber Security and Digital Forensics

A Practical Guide Using Windows OS

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

Updated with the latest advances from the field, **GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS**, Fifth Edition combines all-encompassing topic coverage and authoritative information from seasoned experts to deliver the most comprehensive forensics resource available. This proven author team's wide ranging areas of expertise mirror the breadth of coverage provided in the book, which focuses on techniques and practices for gathering and analyzing evidence used to solve crimes involving computers. Providing clear instruction on the tools and techniques of the trade, it introduces readers to every step of the computer forensics investigation-from lab set-up to testifying in court. It also details step-by-step guidance on how to use current forensics software. Appropriate for learners new to the field, it is also an excellent refresher and technology update for professionals in law enforcement, investigations, or computer security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

A resource to help forensic investigators locate, analyze, and understand digital evidence found on modern Linux systems after a crime, security incident or cyber attack. Practical Linux Forensics dives into the technical details of analyzing postmortem forensic images of Linux systems which have been misused, abused, or the target of malicious attacks. It helps forensic investigators locate and analyze digital evidence found on Linux desktops, servers, and IoT devices. Throughout the book, you learn how to identify digital artifacts which may be of interest to an investigation, draw logical conclusions, and reconstruct past activity from incidents. You'll learn how Linux works from a digital forensics and investigation perspective, and how to interpret evidence from Linux environments. The techniques shown are intended to be independent of the forensic analysis platforms and tools used. Learn how to:
• Extract evidence from storage devices and analyze partition tables, volume managers, popular Linux filesystems (Ext4, Btrfs, and Xfs), and encryption
• Investigate evidence from Linux logs, including traditional syslog, the systemd journal, kernel and audit logs, and logs from daemons and applications
• Reconstruct the Linux startup process, from boot loaders (UEFI and Grub) and kernel initialization, to systemd unit files and targets leading up to a graphical login
• Perform analysis of power, temperature, and the physical environment of a Linux machine, and find evidence of sleep, hibernation, shutdowns, reboots, and crashes
• Examine installed software, including distro installers, package formats, and package management systems from Debian, Fedora, SUSE, Arch, and other distros
• Perform analysis of time and Locale settings, internationalization including language and keyboard settings, and geolocation on a Linux system
• Reconstruct user login sessions (shell, X11 and Wayland), desktops (Gnome, KDE, and others) and analyze keyrings, wallets, trash cans, clipboards, thumbnails, recent files and other desktop artifacts
• Analyze network configuration, including interfaces, addresses, network managers, DNS, wireless artifacts (Wi-Fi, Bluetooth, WWAN), VPNs (including WireGuard), firewalls, and proxy settings
• Identify traces of attached peripheral devices (PCI, USB, Thunderbolt, Bluetooth) including external storage, cameras, and mobiles, and reconstruct printing and scanning activity

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

Digital Forensics and Investigations

Computer Forensics Library

Cyber and Digital Forensic Investigations

A Law Enforcement Practitioner's Perspective

Learn Computer Forensics

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

Understanding the latest capabilities in the cyber threat landscape as well as the cyber forensic challenges and approaches is the best way users and organizations can prepare for potential negative events. Adopting an experiential learning approach, this book describes how cyber forensics researchers, educators and practitioners can keep pace with technological advances, and acquire the essential knowledge and skills, ranging from IoT forensics, malware analysis, and CCTV and cloud forensics to network forensics and financial investigations. Given the growing importance of incident response and cyber forensics in our digitalized society, this book will be of interest and relevance to researchers, educators and practitioners in the field, as well as students wanting to learn about cyber forensics.

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

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.

Forensic Discovery

Applications and Perspectives

Big Data Analytics and Computing for Digital Forensic Investigations

Digital Forensics Basics

Digital Forensics Explained

Handbook of Digital Forensics and Investigation

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. 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 En

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 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 Na 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.

Exploring Careers in Cybersecurity and Digital Forensics serves as a career guide, providing information about education, certifications, and tools to help those making career decisions within the cybersecurity field.

An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is a must for all organizations. This book offers concrete and detailed guidance on how to conduct the full spectrum of incident response and digital forensic activities.

The Definitive, Up-to-Date Guide to Digital Forensics The rapid proliferation of cyber crime is increasing the demand for digital forensics experts in both law enforcement and in the private sector. In Digital Archaeology, expert practitioner Michael Graves has written the most thorough, realistic, and up-to-date guide to the principles and techniques of modern digital forensics. Graves begins by providing the underpinnings of and critical laws affecting computer forensics, including key principles of evidence and case law. Next, he explains how to systematically and thoroughly investigate computer systems to unearth crimes or other misbehavior, and back it up with evidence that will stand up in court. Drawing on the analogy of archaeological research, Graves explains each key tool and method involved in digital systems. His detailed demonstrations often include the actual syntax of command-line utilities. Along the way, he presents exclusive coverage of facilities management, a full chapter on the crucial topic of first response to a digital crime scene, and up-to-the-minute coverage of investigating evidence in the cloud. Graves concludes by presenting coverage of important professional and legal digital forensics, including current licensing and certification requirements. Topics Covered Include Acquiring and analyzing data in ways consistent with forensic procedure Recovering and examining e-mail, Web, and networking activity Investigating users' behavior on mobile devices Overcoming anti-forensics measures that seek to prevent data capture and analysis Performing comprehensive electronic discovery Effectively managing cases and documenting the evidence you find Planning and building your career in digital forensics Digital Archaeology is a key resource for anyone preparing for a career as a professional investigator; for IT professionals who are sometimes called upon to assist in investigations; and for those seeking an explanation of the processes involved in preparing an effective defense.

destruction of digital evidence.

File System Forensic Analysis

Computer Forensics

Digital Forensics

Advances in Digital Forensics II

Digital Evidence and Computer Crime

Cybercrime 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

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

Recent developments in cyber security, crime, and forensics have attracted researcher and practitioner interests from technological, organizational and policy-making perspectives. Technological advances address challenges in information sharing, surveillance and analysis, but organizational advances are needed to foster collaboration between federal, state and local agencies as well as the private sector. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives provides broad coverage of technical and socio-economic perspectives for utilizing information and communication technologies and developing practical solutions in cyber security, cyber crime and cyber forensics.

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.

What Every Engineer Should Know About Cyber Security and Digital Forensics

The Primer for Getting Started in Digital Forensics

People, Process, and Technologies to Defend the Enterprise

computer security and incident response

Guide to Computer Forensics and Investigations

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-bulling 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.

The widespread use of information and communications technology (ICT) has created a global platform for the exchange of ideas, goods and services, the benefits of which are enormous. However, it has also created boundless opportunities for fraud and deception. Cybercrime is one of the biggest growth industries around the globe, whether it is in the form of violation of company policies, fraud, hate crime, extremism, or terrorism. It is therefore paramount that the security industry raises its game to combat these threats. Today's top priority is to use computer technology to fight computer crime, as our commonwealth is protected by firewalls rather than firepower. This is an issue of global importance as new technologies have provided a world of opportunity for criminals. This book is a compilation of the collaboration between the researchers and practitioners in the security field; and provides a comprehensive literature on current and future e-security needs across applications, implementation, testing or investigative techniques, judicial processes and criminal intelligence. The intended audience includes members in academia, the public and private sectors, students and those who are interested in and will benefit from this handbook.

Get up and running with collecting evidence using forensics best practices to present your findings in judicial or administrative proceedings Key Features Learn the core techniques of computer forensics to acquire and secure digital evidence skillfully Conduct a digital forensic examination and document the digital evidence collected Analyze security systems and overcome complex challenges with a variety of forensic investigations Book Description A computer forensics investigator must possess a variety of skills, including the ability to answer legal questions, gather and document evidence, and prepare for an investigation. This book will help you get up and running with using digital forensic tools and techniques to investigate cybercrimes successfully. Starting with an overview of forensics and all the open source and commercial tools needed to get the job done, you'll learn core forensic practices for searching databases and analyzing data over networks, personal devices, and web applications. You'll then learn how to acquire valuable information from different places, such as filesystems, e-mails, browser histories, and search queries, and capture data remotely. As you advance, this book will guide you through implementing forensic techniques on multiple platforms, such as Windows, Linux, and macOS, to demonstrate how to recover valuable information as evidence. Finally, you'll get to grips with presenting your findings efficiently in judicial or administrative proceedings. By the end of this book, you'll have developed a clear understanding of how to acquire, analyze, and present digital evidence like a proficient computer forensics investigator. What you will learn Understand investigative processes, the rules of evidence, and ethical guidelines Recognize and document different types of computer hardware Understand the boot process covering BIOS, UEFI, and the boot sequence Validate forensic hardware and software Discover the locations of common Windows artifacts Document your findings using technically correct terminology Who this book is for If you're an IT beginner, student, or an investigator in the public or private sector this book is for you.This book will also help professionals and investigators who are new to incident response and digital forensics and interested in making a career in the cybersecurity domain.

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.

The Art and Science of Digital Forensics

The Best Damn Cybercrime and Digital Forensics Book Period

A Guide for Digital Investigators

The Basics of Digital Forensics

Theory, Methods, and Real-Life Applications

Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives

Real digital forensicscomputer security and incident responseReal digital forensicscomputer security and incident responseReal Digital ForensicsAddison-Wesley Professional

This book provides a valuable reference for digital forensics practitioners and cyber security experts operating in various fields of law enforcement, incident response and commerce. It is also aimed at researchers seeking to obtain a more profound knowledge of Digital Forensics and Cybercrime. Furthermore, the book is an exceptional advanced text for PhD and Master degree programmes in Digital Forensics and Cyber Security. Each chapter of this book is written by an internationally-renowned expert who has extensive experience in law enforcement, industry and academia. The increasing popularity in the use of IoT devices for criminal activities means that there is a maturing discipline and industry around IoT forensics. As technology becomes cheaper and easier to deploy in an increased number of discrete, everyday objects, scope for the automated creation of personalised digital footprints becomes greater. Devices which are presently included within the Internet of Things (IoT) umbrella have a massive potential to enable and shape the way that humans interact and achieve objectives. These also forge a trail of data that can be used to triangulate and identify individuals and their actions. As such, interest and developments in autonomous vehicles, unmanned drones and 'smart' home appliances are creating unprecedented opportunities for the research communities to investigate the production and evaluation of evidence through the discipline of digital 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*

Every computer crime leaves tracks—you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity. Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, Computer Forensics provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process—from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data. Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

Digital Archaeology

Digital Forensics for Handheld Devices

Digital Forensic Investigation of Internet of Things (IoT) Devices

Real Digital Forensics

Handbook of Electronic Security and Digital Forensics

Exploring Careers in Cybersecurity and Digital Forensics

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.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Practically every crime now involves some digital evidence; digital forensics provides the techniques and tools to articulate this evidence. This book describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Most digital evidence is stored within the computer's file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed. Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today's most valuable open source file system analysis tools—including tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk's Host Protected Area (HPA) Reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more Analyzing DOS, Apple, and GPT partitions; BSD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques Analyzing the contents of multiple disk volumes, such as RAID and disk spanning Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools When it comes to file system analysis, no other book offers this much detail or expertise. Whether you're a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist, or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use.

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)

Fundamentals of Digital Forensics

Real digital forensics

Forensic Science, Computers and the Internet

Security, Privacy, and Digital Forensics in the Cloud

Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements

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, 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,