Guide To Computer Forensics And Investigations Cd

The primary purpose of computer forensics is to enable organisations to pinpoint where the malware has infected their computer systems and which files have been infected, so that they can close the vulnerability. More and more organisations have realised that they need to acquire a forensic capability to ensure they are ready to cope with an information security incident. This pocket guide illustrates the technical complexities involved in computer forensics, and shows managers what makes the discipline relevant to their organisation. For technical staff, the book offers an invaluable insight into the key processes and procedures that are required.

Annotation A comprehensive and broad introduction to computer and intrusion forensics, covering the areas of law enforcement, national security and corporate fraud, this practical book helps professionals understand case studies from around the world, and treats key emerging areas such as stegoforensics, image identification, authorship categorization, and machine learning.

Essential for anyone who works with technology in the field, E-DISCOVERY is a hands-on, how-to training guide that provides students with comprehensive coverage of the

technology used in e-discovery in civil and criminal cases. From discovery identification to collection, processing, review, production, and trial presentation, this practical text covers everything your students need to know about e-discovery, including the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and Federal Rules of Evidence. Throughout the text, students will have the opportunity to work with e-discovery tools such as Discovery Attender, computer forensics tools such as AccessData's Forensics ToolKit, as well as popular processing and review platforms such as iConect, Concordance, and iPro. An interactive courtroom tutorial and use of Trial Director are included to complete the litigation cycle. Multiple tools are discussed for each phase, giving your students a good selection of potential resources for each task. Finally , real-life examples are woven throughout the text, revealing little talked-about potential pitfalls, as well as best practice and cost management suggestions. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

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

A Practical Guide to Digital Forensics Investigations
Computer Forensics For Dummies
Investigative Computer Forensics
Computer Forensics
TechnoSecurity's Guide to E-Discovery and Digital Forensics

Mobile devices are ubiquitous; therefore, mobile device forensics is absolutely critical. Whether for civil or criminal investigations, being able to extract evidence from a mobile device is essential. This book covers the technical details of mobile devices and transmissions, as well as forensic methods for extracting evidence. There are books on specific issues like Android forensics or iOS forensics, but there is not currently a book that covers all the topics covered in this book. Furthermore, it is such a critical skill that mobile device forensics is the most common topic the Author is asked to teach to law enforcement. This is a niche that is not being adequately filled with current titles. An In-Depth Guide to Mobile Device Forensics is aimed towards undergraduates and graduate students studying cybersecurity or digital forensics. It covers both technical and legal issues, and includes exercises, tests/quizzes, case studies, and slides to aid comprehension.

How would your organization cope with a cyber attack? Pinpoint and close vulnerabilities using effective computer forensics! The primary purpose of computer forensics is to enable organizations to pinpoint where the malware has infected their computer systems and which files have been infected, so that they can close the vulnerability. More and more organizations have realised that they need to acquire a forensic capability to ensure they are ready to cope with an information security incident. This pocket guide illustrates the technical complexities involved in computer forensics, and shows managers what makes the discipline relevant to their organization. For technical staff, the book offers an invaluable insight into the key processes and procedures that are required. Benefits to business include: Defend your company effectively against attacks - By developing a computer forensic capability, your organisation will

Would your company be prepared in the event of: * Computer-driven espionage * A devastating virus attack * A hacker's unauthorized access * A breach of data security? As the sophistication of computer technology has grown, so has therate of computer-related criminal activity. Subsequently, Americancorporations now lose billions of dollars a year to

hacking,identity theft, and other computer attacks. More than ever,businesses and professionals responsible for the critical data ofcountless customers and employees need to anticipate and safeguardagainst computer intruders and attacks. The first book to successfully speak to the nontechnicalprofessional in the fields of business and law on the topic ofcomputer crime, Computer Forensics: An Essential Guide forAccountants, Lawyers, and Managers provides valuable advice on thehidden difficulties that can blindside companies and result indamaging costs. Written by industry expert Michael Sheetz, this important bookprovides readers with an honest look at the computer crimes thatcan annoy, interrupt--and devastate--a business. Readers areequipped not only with a solid understanding of how computersfacilitate fraud and financial crime, but also how computers can beused to investigate, prosecute, and prevent these crimes. If you want to know how to protect your company from computercrimes but have a limited technical background, this book is foryou. Get Computer Forensics: An Essential Guide for Accountants,Lawyers, and Managers and get prepared.

An introduction to the growing field of computer forensics provides a

hands-on guide that explains how to conduct an investigation involving digital media, discussing how computer operating systems work, a wide variety of forensic tools, how to be an expert witness during a trial, and key concepts including chain of custody and evidence documentation procedures. Original. (Intermediate)

A Practical Guide Using Windows OS

Computer Forensics InfoSec Pro Guide

Guide to Computer Forensics and Investigations, Loose-leaf Version, 6th + Mindtap Computing, 2 Terms 12 Months Printed Access Card

Learning Guide

Windows Forensics

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

Malware Forensics Field Guide for Windows Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Windows-based systems, the largest running OS in the world. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Windows system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Windows systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Windows system; and analysis of a suspect program. This field guide is intended for computer forensic investigators, analysts, and specialists. A condensed hand-held guide complete with on-the-job tasks and checklists Specific for Windows-based systems, the largest running OS in the world Authors are world-renowned leaders in investigating and analyzing malicious code

Investigating Corporate Fraud Accounting Irregularities E-discovery Challenges Trade Secret Theft Social Networks Data Breaches The Cloud Hackers "Having worked with Erik on some of the most challenging

computer forensic investigations during the early years of this industry's formation as well as having competed with him earnestly in the marketplace...I can truly say that Erik is one of the unique pioneers of computer forensic investigations. He not only can distill complex technical information into easily understandable concepts, but he always retained a long-term global perspective on the relevancy of our work and on the impact of the information revolution on the social and business structures of tomorrow." From the Foreword by James Gordon, Managing Director, Navigant Consulting, Inc. Get the knowledge you need to make informed decisions throughout the computer forensic investigation process Investigative Computer Forensics zeroes in on a real need felt by lawyers, jurists, accountants, administrators, senior managers, and business executives around the globe: to understand the forensic investigation landscape before having an immediate and dire need for the services of a forensic investigator. Author Erik Laykin leader and pioneer of computer forensic investigations presents complex technical information in easily understandable concepts, covering: A primer on computers and networks Computer forensic fundamentals Investigative fundamentals Objectives and challenges in investigative computer forensics E-discovery responsibilities The future of computer forensic investigations Get the knowledge you need to make tough decisions during an internal investigation or while engaging the capabilities of a computer forensic professional with the proven guidance found in Investigative Computer Forensics.

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.

The Field Guide for Corporate Computer Investigations

Computer Forensics and Investigations

Computer and Intrusion Forensics

A Concise and Practical Introduction

Guide to Computer Forensics and Investigations, Loose-Leaf Version

Open Source Software for Digital Forensics is the first book dedicated to the use of FLOSS (Free Libre Open Source Software) in computer forensics. It presents the motivations for using FLOSS applications as tools for collection, preservation and analysis of digital evidence in computer and network forensics. It also covers extensively several forensic FLOSS tools, their origins and evolution. Open Source Software for Digital Forensics is based on the OSSCoNF workshop, which was held in Milan, Italy, September 2008 at the World Computing Congress, co-located with OSS 2008. This edited volume is a collection of contributions from researchers and practitioners world wide. Open Source Software for Digital Forensics is designed for advanced level

students and researchers in computer science as a secondary text and reference book. Computer programmers, software developers, and digital forensics professionals will also find this book to be a valuable asset. Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treaterous condition for any forensic investigator or analyst. Written by information security experts with real-world investigative experience, Malware Forensics Field Guide for Windows Systems is a "tool" with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. *A condensed hand-held guide complete with on-the-job tasks and checklists *Specific for Windows-based systems, the largest running OS in the world *Authors are world-renowned leaders in investigating and analyzing malicious code Conduct repeatable, defensible investigations with EnCase Forensic v7 Maximize the powerful tools and features of the industry-leading digital investigation software. Computer Forensics and Digital Investigation with EnCase Forensic v7 reveals, step by step, how to detect illicit activity, capture and verify evidence, recover deleted and encrypted artifacts, prepare court-ready documents, and ensure legal and regulatory compliance. The book illustrates each concept using downloadable evidence from the National

Institute of Standards and Technology CFReDS. Customizable sample procedures are included throughout this practical guide. Install EnCase Forensic v7 and customize the user interface Prepare your investigation and set up a new case Collect and verify evidence from suspect computers and networks Use the EnCase Evidence Processor and Case Analyzer Uncover clues using keyword searches and filter results through GREP Work with bookmarks, timelines, hash sets, and libraries Handle case closure, final disposition, and evidence destruction Carry out field investigations using EnCase Portable Learn to program in EnCase EnScript

The evidence is in--to solve Windows crime, you need Windows tools An arcane pursuit a decade ago, forensic science today is a household term. And while the computer forensic analyst may not lead as exciting a life as TV's CSIs do, he or she relies just as heavily on scientific principles and just as surely solves crime. Whether you are contemplating a career in this growing field or are already an analyst in a Unix/Linux environment, this book prepares you to combat computer crime in the Windows world. Here are the tools to help you recover sabotaged files, track down the source of threatening e-mails, investigate industrial espionage, and expose computer criminals. * Identify evidence of fraud, electronic theft, and employee Internet

abuse * Investigate crime related to instant messaging, Lotus Notes(r), and increasingly popular browsers such as Firefox(r) * Learn what it takes to become a computer forensics analyst * Take advantage of sample forms and layouts as well as case studies * Protect the integrity of evidence * Compile a forensic response toolkit * Assess and analyze damage from computer crime and process the crime scene * Develop a structure for effectively conducting investigations * Discover how to locate evidence in the Windows Registry

Open Source Software for Digital Forensics

An Essential Guide for Accountants, Lawyers, and Managers

E-Discovery: An Introduction to Digital Evidence

The Best Damn Cybercrime and Digital Forensics Book Period

EnCase Computer Forensics -- The Official EnCE

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,

The Laboratory Manual is a valuable tool designed to enhance your lab experience. Lab activities, objectives, materials lists, step-by-step procedures, illustrations, and review questions are commonly found in a Lab Manual.

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. TechnoSecurity's Guide to E-Discovery and Digital Forensics provides IT security professionals with the information (hardware, software, and procedural requirements) needed to create, manage and sustain a digital forensics lab and

investigative team that can accurately and effectively analyze forensic data and recover digital evidence, while preserving the integrity of the electronic evidence for discovery and trial. Internationally known experts in computer forensics share their years of experience at the forefront of digital forensics Bonus chapters on how to build your own Forensics Lab 50% discount to the upcoming Techno Forensics conference for everyone who purchases a book

Digital Forensics Basics

An Introduction

EnCase Certified Examiner Study Guide

An In-Depth Guide to Mobile Device Forensics

Guide to Computer Forensics and Investigatn

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.

The leading introduction to computer crime and forensicsis now fully updated to reflect today's newest attacks, laws, and investigatory best practices. Packed with new case studies, examples, and statistics, Computer Forensics and Cyber Crime, Third Edition adds up-to-the-minute coverage of smartphones, cloud computing, GPS, Mac OS X, Linux, Stuxnet, cyberbullying, cyberterrorism, search and seizure, online gambling, and much more. Covers all forms of modern and traditional computer crime, defines all relevant terms, and explains all technical and legal concepts in plain English, so students can succeed even if they have no technical, legal, or investigatory background.

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

Security Smarts for the Self-Guided IT Professional Find out how to excel in the field of computer forensics investigations. Learn what it takes to transition from an IT professional to a computer forensic examiner in the private sector. Written by a Certified Information Systems Security Professional, Computer Forensics: InfoSec Pro Guide is filled with real-world case studies that demonstrate the concepts covered in the book. You'll learn how to set up a forensics lab, select hardware and software, choose forensic imaging procedures, test your tools, capture evidence from different sources, follow a sound investigative process, safely store evidence, and verify your findings. Best practices for documenting your results, preparing reports, and presenting evidence in court are also covered in this detailed resource. Computer Forensics: InfoSec Pro Guide features:

Lingo—Common security terms defined so that you're in the know on the job IMHO—Frank and relevant opinions based on the author's years of industry experience Budget Note—Tips for getting security technologies and processes into your organization's budget In Actual Practice—Exceptions to the rules of security explained in real-world contexts Your Plan—Customizable checklists you can use on the job now Into Action—Tips on how, why, and when to apply new skills and techniques at work

A Comprehensive Handbook

Guide to Computer Forensics and Investigations + MindTap Security Lab, 1 Term 6 Months Access Card for Guide to Computer Forensics and Investigations Via Live Virtual Machines, 5th Ed.

Learn Computer Forensics

Processing Digital Evidence

Computer Forensics and Digital Investigation with EnCase Forensic

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.

This work introduces the reader to the world of digital forensics in a practical and accessible manner. The text was

written to fulfill a need for a book that introduces forensic methodology and sound forensic thinking, combined with hands-on examples for common tasks in a computer forensic examination. The author has several years of experience as a computer forensics examiner and is now working as a university-level lecturer. Guide to Digital Forensics: A Concise and Practical Introduction is intended for students that are looking for an introduction to computer forensics and can also be used as a collection of instructions for practitioners. The aim is to describe and explain the steps taken during a forensic examination, with the intent of making the reader aware of the constraints and considerations that apply during a fo rensic examination in law enforcement and in the private sector. Upon reading this book, the reader should have a proper overview of the field of digital forensics, starting them on the journey of becoming a computer forensics expert.

A Practical Guide to Computer Forensics Investigations introduces the newest technologies along with detailed

information on how the evidence contained on these devices should be analyzed. Packed with practical, hands-on activities, students will learn unique subjects from chapters including Mac Forensics, Mobile Forensics, Cyberbullying, and Child Endangerment. This well-developed book will prepare students for the rapidly-growing field of computer forensics for a career with law enforcement, accounting firms, banks and credit card companies, private investigation companies, or government agencies.

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 investigationsGather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10-specific feature forensicsUtilize 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

The Basics of Digital Forensics

Handbook of Digital Forensics and Investigation

The Primer for Getting Started in Digital Forensics

Guide to Computer Forensics and Investigations with Access Code

Guide to Computer Forensics and Investigations + Mindtap Security Lab, 1 Term 6 Months Access Card for Nelson/Phillips/steuart's Guide to Computer Forensics and Investigations Via Live Virtual Machines

Guide to Computer Forensics and InvestigationsCengage Learning

Now extensively updated, this authoritative, intensely practical guide to digital forensics draws upon the author's wide-ranging experience in law enforcement,

including his pioneering work as a forensics examiner in both criminal and civil investigations. Writing for students and other readers at all levels of experience, Dr. Darren Hayes presents comprehensive, modern best practices for capturing and analyzing evidence, protecting the chain of custody, documenting investigations, and more -- all designed for application in actual crime scenes. In this edition, Hayes tightly aligns his coverage with widely-respected government curricula, including NSA Knowledge Units; and with key professional certifications such as AccessData Certified Examiner (ACE). A Practical Guide to Digital Forensics Investigations, Second Edition presents more hands-on activities and case studies than any book of its kind, including short questions, essay questions, and discussion questions in every chapter. It addresses issues ranging from device hardware and software to law, privacy and ethics; scientific and government protocols to techniques for investigation and reporting. Reflecting his deep specialized knowledge, this edition offers unsurpassed coverage of mobile forensics, including a full chapter on mobile apps. It also adds new discussions of capturing investigatory data from today's ubiquitous Internet of Things (IoT) devices; as well as digital forensics techniques for incident response and related cybersecurity tasks. Throughout, Hayes presents detailed chapters on crucial topics that competitive books gloss over, including Mac forensics and investigating child endangerment.

The official, Guidance Software-approved book on the newest EnCE exam! The EnCE exam tests that computer forensic analysts and examiners have thoroughly mastered computer investigation methodologies, as well as the use of Guidance Software's EnCase Forensic 7. The only official Guidance-endorsed study guide on the topic, this book prepares you for the exam with extensive coverage of all exam topics, real-world scenarios, hands-on exercises, up-to-date legal information, and sample evidence files, flashcards, and more. Guides readers through preparation for the newest EnCase Certified Examiner (EnCE) exam Prepares candidates for both Phase 1 and Phase 2 of the exam, as well as for practical use of the certification Covers identifying and searching hardware and files systems, handling evidence on the scene, and acquiring digital evidence using EnCase Forensic 7 Includes hands-on exercises, practice questions, and up-to-date legal information Sample evidence files, Sybex Test Engine, electronic flashcards, and more If you're preparing for the new EnCE exam, this is the study guide you need.

Master the skills you need to conduct a successful digital investigation with Nelson/Phillips/Steuart's GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, Sixth Edition--the most comprehensive forensics resource available. While other books offer just an overview of the field, this hands-on learning text provides clear instruction on the tools and techniques of the trade,

walking you through every step of the computer forensics investigation--from lab setup to testifying in court. It also explains how to use current forensics software and provides free demo downloads. It includes the most up-to-date coverage available of Linux and Macintosh, virtual machine software such as VMware and Virtual Box, Android, mobile devices, handheld devices, cloud forensics, email, social media and the Internet of Anything. With its practical applications, you can immediately put what you learn into practice.

Digital Forensics, Investigation, and Response

Malware Forensics Field Guide for Windows Systems

Guide to Computer Forensics and Investigations

Guide to Computer Forensics and Investigations + Mindtap Computing, 1 Term 6 Months Printed Access Card