Guide To Computer Forensics And Investigations

This Computer Forensic Guide is meant for IT professional who wants to enter into Computer Forensic domain.

Guidance Software?s EnCase product is the premier computer forensics tool on the market, used in law enforcement labs for digital evidence collection; in commercial settings for incident response and information assurance; and by the FBI and Department of Defense to detect domestic and international threats This guide prepares readers for both the CBT and practical phases of the exam that validates mastery of EnCase Written by two law enforcement professionals who are computer forensics specialists and EnCase trainers Includes the EnCase Legal Journal, essential for forensics investigators who need to be sure they are operating within the law and able to give expert testimony The CD includes tools to help readers prepare for Phase II of the certification, which requires candidates to examine computer evidence, as well as a searchable PDF of the text

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. 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 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.

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 the rate of computer-related criminal activity. Subsequently, American corporations 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 of countless customers and employees need to anticipate and safeguard against computer intruders and attacks. The first book to successfully speak to the nontechnical professional in the fields of business and law on the topic of computer crime, Computer Forensics: An Essential Guide for Accountants,

Lawyers, and Managers provides valuable advice on the hidden difficulties that can blindside companies and result in damaging costs. Written by industry expert Michael Sheetz, this important book provides readers with an honest look at the computer crimes that can annoy, interrupt--and devastate--a business. Readers are equipped not only with a solid understanding of how computers facilitate fraud and financial crime, but also how computers can be used to investigate, prosecute, and prevent these crimes. If you want to know how to protect your company from computer crimes but have a limited technical background, this book is for you. Get Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers and get prepared.

In recent years, there have been a record number of computer security related crimes and breeches than ever before. The more the technology advances, the more chances computer criminals will learn more ways of breaching computer security. Computer Forensics now aid in solving crimes We now live in a digital age where the computer permeates almost every aspect of our lives. Almost all transactions and records of our activities are now recorded electronically. Computers are digital devices are everywhere. Those who pursue a career in the field will be gainfully employed for a long time. There is more so in the computer forensics field and this book is here to help you AMONG THE OBJECTIVES OF

WRITING THIS BOOK: - What is Computer Forensic Experts? - In general, we know that the jobs of a computer forensics expert are to extract and examine data to look for evidence or supportive evidence. In fact, their job scope is very wide. Let's have a better understanding on what digital forensics experts can do. You will be eager to join this line after knowing how wonderful they are. Computer Forensics Software - Computer forensics software programs are used to detect computer frauds, crimes, etc., automatically, without retaining the services of a computer forensic specialist. Software solution processes detect operations done on a computer illegally or without authorization. How to Find the Best Software to Compare Recovered Data - Recovering data is not impossible to do anymore at the present time. Learn how you can spot the best application that will allow you to compare recovered data through this book. Cell Phone Forensics - Using Technology to Catch a Cheater - Learn from a private investigator that's an expert in infidelity investigations how you can use cell phone forensics to catch a cheater. These days, many cheaters, and otherwise unfaithfully married spouses, take advantage of technology to help them hide their extramarital activity. What Are the Skills Needed by a Computer Forensics Accountant? - The field of computer forensics has emerged as the best solution to investigate the types of crimes that are committed with computers. The job of a

computer forensic accountant is to identify, preserve, extract, maintain and documenting all the related date involved in online criminal activity. In order to perform the tasks successfully, ones must equip themselves with necessary knowledge and practical skills. Internet and mobile technology are great. But with along with the excitement comes cybercrime. And computer forensic professionals are needed to catch cyber criminals. Find out some of your options in this book. Get Your Copy Now

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.

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 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.

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

Never HIGHLIGHT a Book Again Includes all testable terms, concepts, persons, places, and events. Cram101 Just the FACTS101 studyguides gives all of the outlines, highlights, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanies: 9780872893795. This item is printed on demand.

To ensure a successful experience for instructors and students alike, this book includes the following sections for each lab: Lab Objectives - Every lab has a brief description and list of learning objectives Materials Required - Every lab includes information on the hardware, software, and other materials you need to complete the lab. Estimated Completion Time - Every lab has an estimated completion time, so that you can plan your activities accurately. Activity - The actual lab activity is presented in this section. Logical and precise step-by-step instructions guide you through the lab. Review Questions - Each lab includes follow-up questions to help reinforce concepts presented in the lab. WEB-BASED LABS FOR GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, FOURTH EDITION provides step-by-step labs taken directly from GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, FOURTH EDITION. Using a real lab environment over the Internet, learners can log on anywhere, anytime via a Web browser to gain essential hands-on experience in

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.

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

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.

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.

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.

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 ???????????????????????????????,?????????,?????????????????????
Never HIGHLIGHT a Book Again! Virtually all of the testable terms, concepts,

persons, places, and events from the textbook are included. Cram101 Just the FACTS101 studyguides give all of the outlines, highlights, notes, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanys: 9780073378152 .

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.

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 Computer forensics touches on a lot of skills - from answering legal or investigative questions to preparing for an investigation, evidence acquisition, and more. The goal of this book is to acquaint you with some of the forensic tools and techniques to successfully investigate cybercrimes, and become a proficient computer forensics investigator.

Copyright: 2dbb262afb7a8df59f3770f300a7c46b