

Encase Computer Forensics The Official Ence Encase Certified Examiner Study Guide 3rd Third Edition By Bunting Steve Published By Sybex 2012

Windows Forensics Computer Forensics CCFP Certified Cyber Forensics Professional All-in-One Exam Guide EnCase Computer Forensics Mastering Windows Network Forensics and Investigation EnCase Computer Forensics -- The Official EnCE Handbook of Electronic Security and Digital Forensics Learning Malware Analysis The Basics of Digital Forensics Computer Forensics with FTK Integrating Python with Leading Computer Forensics Platforms Digital Forensics for Legal Professionals Digital Forensics with Kali Linux Digital Archaeology Advances in Digital Forensics II Cyber Forensics Computer Forensics JumpStart Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book Implementing Digital Forensic Readiness Computer Forensics For Dummies Learn Computer Forensics File System Forensic Analysis EnCase Computer Forensics, includes DVD Windows Forensics Cookbook EnCE EnCase Computer Forensics Computer Forensics: Investigating Data and Image Files (CHFI) Guide to Computer Forensics and Investigations Computer Forensics Computer Forensics and Digital Investigation with EnCase Forensic Advances in Digital Forensics IX Handbook of Digital Forensics and Investigation Digital Evidence and Computer Crime Hands-On Ethical Hacking and Network Defense A Practical Guide to Computer Forensics Investigations Digital Forensics and Investigations Computer Forensics InfoSec Pro Guide EnCase Computer Forensics -- The Official EnCE Digital Forensics Basics Introductory Computer Forensics The Official CHFI Study Guide (Exam 312-49)

Windows 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.

Computer Forensics

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

CCFP Certified Cyber Forensics Professional All-in-One Exam Guide

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

EnCase Computer Forensics

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

Mastering Windows Network Forensics and Investigation

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 a solid understanding of the legal 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 investigators use to reliably uncover hidden information 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 business issues associated with building a career in 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 in connection with lawsuits 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, including how to avoid the legally indefensible destruction of digital evidence.

EnCase Computer Forensics -- The Official EnCE

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.

Handbook of Electronic Security and Digital Forensics

Launch Your Career in Computer Forensics—Quickly and Effectively Written by a team of computer forensics experts, Computer Forensics JumpStart provides all the core information you need to launch your career in this fast-growing field:

- Conducting a computer forensics investigation
- Examining the layout of a network
- Finding hidden data
- Capturing images
- Identifying, collecting, and preserving computer evidence
- Understanding encryption and examining encrypted files
- Documenting your case
- Evaluating common computer forensic tools
- Presenting computer evidence in court as an expert witness

Learning Malware Analysis

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.

The Basics of Digital Forensics

Hands-On Ethical Hacking and Network Defense, Second Edition provides an in-depth understanding of how to effectively protect computer networks. This book describes the tools and penetration testing methodologies used by ethical hackers and provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Readers are provided with updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also included is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking. With cyber-terrorism and corporate espionage threatening the fiber of our world, the need for trained network security professionals continues to grow. Hands-On Ethical Hacking and Network Defense, Second Edition provides a structured knowledge base to prepare readers to be security professionals who understand how to protect a network by using the skills and tools of an ethical hacker. Important Notice: Media content

referenced within the product description or the product text may not be available in the ebook version.

Computer Forensics with FTK

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

Integrating Python with Leading Computer Forensics Platforms

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.

Digital Forensics for Legal Professionals

Digital forensics and multimedia forensics are rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended to by contributions from researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic triage, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features:

- Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of multimedia data and devices
- Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices
- Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work
- Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice guides, test datasets and more case studies

Digital Forensics with Kali Linux

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

Digital Archaeology

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.

Advances in Digital Forensics II

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.

Cyber Forensics

Digital Forensics for Legal Professionals provides you with a guide to digital technology forensics in plain English. In the authors' years of experience in working with attorneys as digital forensics experts, common questions arise again and again: "What do I ask for?? "Is the evidence relevant?? "What does this item in the forensic report mean?? "What should I ask the other expert?? "What should I ask you?? "Can you explain that to a jury?? This book answers many of those questions

in clear language that is understandable by non-technical people. With many illustrations and diagrams that will be usable in court, they explain technical concepts such as unallocated space, forensic copies, timeline artifacts and metadata in simple terms that make these concepts accessible to both attorneys and juries. The authors also explain how to determine what evidence to ask for, evidence might be that could be discoverable, and the methods for getting to it including relevant subpoena and motion language. Additionally, this book provides an overview of the current state of digital forensics, the right way to select a qualified expert, what to expect from a qualified expert and how to properly use experts before and during trial. Includes a companion Web site with: courtroom illustrations, and examples of discovery motions Provides examples of direct and cross examination questions for digital evidence Contains a reference of definitions of digital forensic terms, relevant case law, and resources for the attorney

Computer Forensics JumpStart

EnCE certification tells the world that you've not only mastered the use of EnCase Forensic Software, but also that you have acquired the in-depth forensics knowledge and techniques you need to conduct complex computer examinations. This official study guide, written by a law enforcement professional who is an expert in EnCE and computer forensics, provides the complete instruction, advanced testing software, and solid techniques you need to prepare for the exam. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book

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.

Implementing Digital Forensic Readiness

This tutorial contains detailed instructions with useful integrated examples that help you understand the main features of FTK and how you can use it to analyze evidence. This book has clear and concise guidance in an easily accessible format. This tutorial-based guide is great for you if you want to conduct digital

investigations with an integrated platform. Whether you are new to Computer Forensics or have some experience, this book will help you get started with FTK so you can analyze evidence effectively and efficiently. If you are a law enforcement official, corporate security, or IT professional who needs to evaluate the evidentiary value of digital evidence, then this book is ideal for you.

Computer Forensics For Dummies

Learn Computer Forensics

"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.

File System Forensic Analysis

Integrating Python with Leading Computer Forensic Platforms takes a definitive look at how and why the integration of Python advances the field of digital forensics. In addition, the book includes practical, never seen Python examples that can be immediately put to use. Noted author Chet Hosmer demonstrates how to extend four key Forensic Platforms using Python, including EnCase by Guidance Software, MPE+ by AccessData, The Open Source Autopsy/SleuthKit by Brian Carrier and WetStone Technologies, and Live Acquisition and Triage Tool US-LATT. This book is for practitioners, forensic investigators, educators, students, private investigators, or anyone advancing digital forensics for investigating cybercrime. Additionally, the open source availability of the examples allows for sharing and growth within the industry. This book is the first to provide details on how to directly integrate Python into key forensic platforms. Provides hands-on tools, code samples, detailed instruction, and documentation that can be immediately put to use Shows how to integrate Python with popular digital forensic platforms, including EnCase, MPE+, The Open Source Autopsy/SleuthKit, and US-LATT Presents complete coverage of how to use Open Source Python scripts to extend and modify popular digital forensic Platforms

EnCase Computer Forensics, includes DVD

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book's 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students' understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and

preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book.

Windows Forensics Cookbook

Master the techniques for gathering electronic evidence and explore the new frontier of crime investigation. The demand for computer forensics experts greatly exceeds the supply. With the rapid growth of technology in all parts of our lives, criminal activity must be tracked down and investigated using electronic methods that require up-to-date techniques and knowledge of the latest software tools. Authors Linda Volonino, Jana Godwin, and Reynaldo Anzaldua share their expertise to give you the legal, technical, and investigative skills you need to launch your career in computer forensics. You can also use Computer Forensics: Principles and Practices to help you advance in careers such as criminal justice, accounting, law enforcement, and federal investigation. Computer Forensics Principles and Practices gives you in-depth understanding of: Using the correct investigative tools and procedures to maximize effectiveness of evidence gathering. Keeping evidence in pristine condition so it will be admissible in a legal action. . Investigating large-scale attacks such as identity theft, fraud, phishing, extortion, and malware infections. The legal foundations for proper handling of traditional and electronic evidence such as the Federal Rules of Evidence and Procedure as well as the Fourth Amendment and other laws regarding search warrants and civil rights. Practical tools such as FTK, EnCase, Passware, Ethereal, LADS, WinHex, GIMP, Camouflage, and Snort. This book is filled with tools to help you move beyond simply learning concepts and help you apply them. These tools include: . In Practice tutorials: Apply concepts and learn by doing. . Exercises and Projects: Assignments show you how to employ your new skills. Case Studies: Apply what you learn in real-world scenarios. The companion Web site (www.prenhall.com/security) includes: . Additional testing materials and projects to reinforce book lessons. . Downloadable checklists and templates used in the book. . Links to additional topics and resources to assist you in your professional development. "

EnCE EnCase Computer Forensics

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

Computer Forensics: Investigating Data and Image Files (CHFI)

Get complete coverage of all six CCFP exam domains developed by the International Information Systems Security Certification Consortium (ISC)2. Written by a leading computer security expert, this authoritative guide fully addresses cyber forensics techniques, standards, technologies, and legal and ethical principles. You'll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. **COVERS ALL SIX EXAM DOMAINS:** Legal and ethical principles Investigations Forensic science Digital forensics Application forensics Hybrid and emerging technologies **ELECTRONIC CONTENT INCLUDES:** 250 practice exam questions Test engine that provides full-length practice exams and customized quizzes by chapter or by exam domain

Guide to Computer Forensics and Investigations

Maximize the power of Windows Forensics to perform highly effective forensic investigations About This Book Prepare and perform investigations using powerful tools for Windows, Collect and validate evidence from suspects and computers and uncover clues that are otherwise difficult Packed with powerful recipes to perform highly effective field investigations Who This Book Is For If you are a forensic analyst or incident response professional who wants to perform computer forensics investigations for the Windows platform and expand your tool kit, then this book is for you. What You Will Learn Understand the challenges of acquiring evidence from Windows systems and overcome them Acquire and analyze Windows memory and drive data with modern forensic tools. Extract and analyze data from Windows file systems, shadow copies and the registry Understand the main Windows system artifacts and learn how to parse data from them using forensic tools See a forensic analysis of common web browsers, mailboxes, and instant messenger services Discover how Windows 10 differs from previous versions and how to overcome the specific challenges it presents Create a graphical timeline and visualize data, which can then be incorporated into the final report Troubleshoot issues that arise while performing Windows forensics In Detail Windows Forensics Cookbook provides recipes to overcome forensic challenges and helps you carry out effective investigations easily on a Windows platform. You will begin with a refresher on digital forensics and evidence acquisition, which will help you to understand the challenges faced while acquiring evidence from Windows systems. Next you will learn to acquire Windows memory data and analyze Windows systems with modern forensic tools. We also cover some more in-depth elements of forensic

analysis, such as how to analyze data from Windows system artifacts, parse data from the most commonly-used web browsers and email services, and effectively report on digital forensic investigations. You will see how Windows 10 is different from previous versions and how you can overcome the specific challenges it brings. Finally, you will learn to troubleshoot issues that arise while performing digital forensic investigations. By the end of the book, you will be able to carry out forensics investigations efficiently. Style and approach This practical guide filled with hands-on, actionable recipes to detect, capture, and recover digital artifacts and deliver impeccable forensic outcomes.

Computer Forensics

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance - investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics IX describe original research results and innovative applications in the 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 areas of coverage include: Themes and Issues, Forensic Models, Forensic Techniques, File system Forensics, Network Forensics, Cloud Forensics, Forensic Tools, and Advanced Forensic Techniques. This book is the ninth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-five edited papers from the Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA in the winter of 2013. Advances in Digital Forensics IX is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoj is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Computer Forensics and Digital Investigation with EnCase Forensic

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.

Advances in Digital Forensics IX

Learn the skills you need to take advantage of Kali Linux for digital forensics investigations using this comprehensive guide Key Features Master powerful Kali Linux tools for digital investigation and analysis Perform evidence acquisition, preservation, and analysis using various tools within Kali Linux Implement the concept of cryptographic hashing and imaging using Kali Linux Perform memory forensics with Volatility and internet forensics with Xplico. Discover the capabilities of professional forensic tools such as Autopsy and DFF (Digital Forensic Framework) used by law enforcement and military personnel alike Book Description Kali Linux is a Linux-based distribution used mainly for penetration testing and digital forensics. It has a wide range of tools to help in forensics investigations and incident response mechanisms. You will start by understanding the fundamentals of digital forensics and setting up your Kali Linux environment to perform different investigation practices. The book will delve into the realm of operating systems and the various formats for file storage, including secret hiding places unseen by the end user or even the operating system. The book will also teach you to create forensic images of data and maintain integrity using hashing tools. Next, you will also master some advanced topics such as autopsies and acquiring investigation data from the network, operating system memory, and so on. The book introduces you to powerful tools that will take your forensic abilities and investigations to a professional level, catering for all aspects of full digital forensic investigations from hashing to reporting. By the end of this book, you will have had hands-on experience in implementing all the pillars of digital

forensics—acquisition, extraction, analysis, and presentation using Kali Linux tools. What you will learn Get to grips with the fundamentals of digital forensics and explore best practices Understand the workings of file systems, storage, and data fundamentals Discover incident response procedures and best practices Use DC3DD and Guymager for acquisition and preservation techniques Recover deleted data with Foremost and Scalpel Find evidence of accessed programs and malicious programs using Volatility. Perform network and internet capture analysis with Xplico Carry out professional digital forensics investigations using the DFF and Autopsy automated forensic suites Who this book is for This book is targeted at forensics and digital investigators, security analysts, or any stakeholder interested in learning digital forensics using Kali Linux. Basic knowledge of Kali Linux will be an advantage.

Handbook of Digital Forensics and Investigation

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

Digital Evidence and Computer Crime

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

Hands-On Ethical Hacking and Network Defense

The Computer Forensic Series by EC-Council provides the knowledge and skills to identify, track, and prosecute the cyber-criminal. The series is comprised of four books covering a broad base of topics in Computer Hacking Forensic Investigation, designed to expose the reader to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Learners are introduced to advanced techniques in computer investigation and analysis with interest in generating potential legal evidence. In full, this and the other three books provide preparation to identify evidence in computer related crime and abuse cases as well as track the intrusive hacker's path through a client system. The series and accompanying labs help prepare the security student or professional to profile an intruder's footprint and gather all necessary information and evidence to support prosecution in a court of law. Investigating Data and Image Files provides a basic understanding of steganography, data acquisition and duplication, encase, how to recover deleted files and partitions and image file forensics. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

A Practical Guide to Computer Forensics Investigations

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.

Digital Forensics and Investigations

An authoritative guide to investigating high-technology crimes Internet crime is seemingly ever on the rise, making the need for a comprehensive resource on how to investigate these crimes even more dire. This professional-level book--aimed at law enforcement personnel, prosecutors, and corporate investigators--provides you with the training you need in order to acquire the sophisticated skills and software solutions to stay one step ahead of computer criminals. Specifies the techniques needed to investigate, analyze, and document a criminal act on a Windows computer or network Places a special emphasis on how to thoroughly investigate criminal activity and now just perform the initial response Walks you through ways to present technically complicated material in simple terms that will hold up in court Features content fully updated for Windows Server 2008 R2 and Windows 7 Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academic adoption, Mastering Windows Network Forensics and Investigation, 2nd Edition offers help for investigating high-technology crimes.

Computer Forensics InfoSec Pro Guide

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.

EnCase Computer Forensics -- The Official EnCE

Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually

progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

Digital Forensics Basics

Hands-on labs to reinforce critical skills --

Introductory Computer Forensics

This is the official CHFI (Computer Hacking Forensics Investigator) study guide for professionals studying for the forensics exams and for professionals needing the skills to identify an intruder's footprints and properly gather the necessary evidence to prosecute. The EC-Council offers certification for ethical hacking and computer forensics. Their ethical hacker exam has become very popular as an industry gauge and we expect the forensics exam to follow suit. Material is presented in a logical learning sequence: a section builds upon previous sections and a chapter on previous chapters. All concepts, simple and complex, are defined and explained when they appear for the first time. This book includes: Exam objectives covered in a chapter are clearly explained in the beginning of the chapter, Notes and Alerts highlight crucial points, Exam's Eye View emphasizes the important points from the exam's perspective, Key Terms present definitions of key terms used in the chapter, Review Questions contains the questions modeled after real exam questions based on the material covered in the chapter. Answers to the questions are presented with explanations. Also included is a full practice exam modeled after the real exam. The only study guide for CHFI, provides 100% coverage of all exam objectives. CHFI Training runs hundreds of dollars for self tests to thousands of dollars for classroom training.

The Official CHFI Study Guide (Exam 312-49)

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

Download File PDF Encase Computer Forensics The Official Ence Encase
Certified Examiner Study Guide 3rd Third Edition By Bunting Steve
Published By Sybex 2012

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