

## Practical Forensic Imaging Securing Digital Evidence With Linux Tools

Memory forensics provides cutting edge technology to help investigate digital attacks. Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller *Malware Analyst's Cookbook*, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac* is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. *The Art of Memory Forensics* explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

Network security is not simply about building impenetrable walls—determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In *The Practice of Network Security Monitoring*, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: –Determine where to deploy NSM platforms, and size them for the monitored networks –Deploy stand-alone or distributed NSM installations –Use command line and graphical packet analysis tools, and NSM consoles –Interpret network evidence from server-side and client-side intrusions –Integrate threat intelligence into NSM software to identify sophisticated adversaries There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. *The Practice of Network Security Monitoring* will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

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.

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.

*Understanding Incident Detection and Response*

*Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice*

*Practical Windows Forensics*

*The Practice of Network Security Monitoring*

*Digital and Document Examination*

**Linux Forensics** is the most comprehensive and up-to-date resource for those wishing to quickly and efficiently perform forensics on Linux systems. It is also a great asset for anyone that would like to better understand Linux internals. Linux Forensics will guide you step by step through the process of investigating a computer running Linux. Everything you need to know from the moment you receive the call from someone who thinks they have been attacked until the final report is written is covered in this book. All of the tools discussed in this book are free and most are also open source. Dr. Philip Polstra shows how to leverage numerous tools such as Python, shell scripting, and MySQL to quickly, easily, and accurately analyze Linux systems. While readers will have a strong grasp of Python and shell scripting by the time they complete this book, no prior knowledge of either of these scripting languages is assumed. Linux Forensics begins by showing you how to determine if there was an incident with minimally invasive techniques. Once it appears likely that an incident has occurred, Dr. Polstra shows you how to collect data from a live system before shutting it down for the creation of filesystem images. Linux Forensics contains extensive coverage of Linux ext2, ext3, and ext4 filesystems. A large collection of Python and shell scripts for creating, mounting, and analyzing filesystem images are presented in this book. Dr. Polstra introduces readers to the exciting new field of memory analysis using the Volatility framework. Discussions of advanced attacks and malware analysis round out the book. **Book Highlights** 370 pages in large, easy-to-read 8.5 x 11 inch format Over 9000 lines of Python scripts with explanations Over 800 lines of shell scripts with explanations A 102 page chapter containing up-to-date information on the ext4 filesystem Two scenarios described in detail with images available from the book website All scripts and other support files are available from the book website **Chapter Contents** First Steps General Principles Phases of Investigation High-level Process Building a Toolkit Determining If There Was an Incident Opening a Case Talking to Users Documentation Mounting Known-good Binaries Minimizing Disturbance to the Subject Automation With Scripting Live Analysis Getting Metadata Using Spreadsheets Getting Command Histories Getting Logs Using Hashes Dumping RAM Creating Images Shutting Down the System Image Formats DD DCFLDD Write Blocking Imaging Virtual Machines Imaging Physical Drives Mounting Images Master Boot Record Based Partitions GUID Partition Tables Mounting Partitions In Linux Automating With Python Analyzing Mounted Images Getting Timestamps Using LibreOffice Using MySQL Creating Timelines Extended Filesystems Basics Superblocks Features Using Python Finding Things That Are Out Of Place Inodes Journaling Memory Analysis Volatility Creating Profiles Linux Commands Dealing With More Advanced Attackers Malware Is It Malware? Malware Analysis Tools Static Analysis Dynamic Analysis Obfuscation The Road Ahead Learning More Communities Conferences Certifications

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. **Practical Forensic Imaging** takes a detailed look at how to secure and manage digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: –Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies –Protect attached evidence media from accidental modification –Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal –Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping –Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt –Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OS-encrypted drives using BitLocker, FileVault, and TrueCrypt; and others –Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, **Practical Forensic Imaging** is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab.

**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,

You don't need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and **Game Hacking** will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to: –Scan and modify memory with Cheat Engine –Explore program structure and execution flow with OllyDbg –Log processes and pinpoint useful data files with Process Monitor –Manipulate control flow through NOPing, hooking, and more –Locate and dissect common game memory structures You'll even discover the secrets behind common game bots, including: –Extrasensory perception hacks, such as wallhacks and heads-up displays –Responsive hacks, such as autohealers and combo bots –Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn't have to be. Once you understand how bots are made, you'll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with **Game Hacking**, and leave with a deeper understanding of both game design and computer security.

**A Practical Guide to Digital Forensics Investigations**

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

**Forensic Digital Image Processing**

A Practical Approach

**Harriet and the Piper (EasyRead Comfort Edition)**

**Understanding Digital Evidence from the Warrant to the Courtroom**

Become well-versed with forensics for the Android, iOS, and Windows 10 mobile platforms by learning essential techniques and exploring real-life scenarios **Key Features**Apply advanced forensic techniques to recover deleted data from mobile devicesRetrieve and analyze data stored not only on mobile devices but also on the cloud and other connected mediumsUse the power of mobile forensics on popular mobile platforms by exploring different tips, tricks, and techniques**Book Description** Mobile phone forensics is the science of retrieving data from a mobile phone under forensically sound conditions. This updated fourth edition of **Practical Mobile Forensics** delves into the concepts of mobile forensics and its importance in today's world. The book focuses on teaching you the latest forensic techniques to investigate mobile devices across various mobile platforms. You will learn forensic techniques for multiple OS versions, including iOS 11 to iOS 13, Android 8 to Android 10, and Windows 10. The book then takes you through the latest open source and commercial mobile forensic tools, enabling you to analyze and retrieve data effectively. From inspecting the device and retrieving data from the cloud, through to successfully documenting reports of your investigations, you'll explore new techniques while building on your practical knowledge. Toward the end, you will understand the reverse engineering of applications and ways to identify malware. Finally, the book guides you through parsing popular third-party applications, including Facebook and WhatsApp. By the end of this book, you will be proficient in various mobile forensic techniques to analyze and extract data from mobile devices with the help of open source solutions. What you will learnDiscover new data extraction, data recovery, and reverse engineering techniques in mobile forensicsUnderstand iOS, Windows, and Android security mechanismsIdentify sensitive files on every mobile platformExtract data from iOS, Android, and Windows platformsUnderstand malware analysis, reverse engineering, and data analysis of mobile devicesExplore various data recovery techniques on all three mobile platformsWho this book is for This book is for forensic examiners with basic experience in mobile forensics or open source solutions for mobile forensics. Computer security professionals, researchers or anyone looking to gain a deeper understanding of mobile internals will also find this book useful. Some understanding of digital forensic practices will be helpful to grasp the concepts covered in the book more effectively.

Get started with the art and science of digital forensics with this practical, hands-on guide! About This Book Champion the skills of digital forensics by understanding the nature of recovering and preserving digital information which is essential for legal or disciplinary proceedings Explore new and promising forensic processes and tools based on 'disruptive technology' to regain control of caseloads. Richard Boddington, with 10+ years of digital forensics, demonstrates real life scenarios with a pragmatic approach Who This Book Is For This book is for anyone who wants to get into the field of digital forensics. Prior knowledge of programming languages (any) will be of great help, but not a compulsory prerequisite. What You Will Learn Gain familiarity with a range of different digital devices and operating and application systems that store digital evidence. Appreciate and understand the function and capability of forensic processes and tools to locate and recover digital evidence. Develop an understanding of the critical importance of recovering digital evidence in pristine condition and ensuring its safe handling from seizure to tendering it in evidence in court. Recognise the attributes of digital evidence and where it may be hidden and is often located on a range of digital devices. Understand the importance and challenge of digital evidence analysis and how it can assist investigations and court cases. Explore emerging technologies and processes that empower forensic practitioners and other stakeholders to harness digital evidence more effectively. In Detail Digital Forensics is a methodology which includes using various tools, techniques, and programming language. This book will get you started with digital forensics and then follow on to preparing investigation plan and preparing toolkit for investigation. In this book you will explore new and promising forensic processes and tools based on 'disruptive technology' that offer experienced and budding practitioners the means to regain control of their caseloads. During the course of the book, you will get to know about the technical side of digital forensics and various tools that are needed to perform digital forensics. This book will begin with giving a quick insight into the nature of digital evidence, where it is located and how it can be recovered and forensically examined to assist investigators. This book will take you through a series of chapters that look at the nature and circumstances of digital forensic examinations and explains the processes of evidence recovery and preservation from a range of digital devices, including mobile phones, and other media. This book has a range of case studies and simulations will allow you to apply the knowledge of the theory gained to real-life situations. By the end of this book you will have gained a sound insight into digital forensics and its key components. Style and approach The book takes the reader through a series of chapters that look at the nature and circumstances of digital forensic examinations and explains the processes of evidence recovery and preservation from a range of digital devices, including mobile phones, and other media. The mystery of digital forensics is swept aside and the reader will gain a quick insight into the nature of digital evidence, where it is located and how it can be recovered and forensically examined to assist investigators.

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

Provides an overview and case studies of computer crimes and discusses topics including data recovery, evidence collection, preservation of digital evidence, information warfare, and the cyber underground.

Incident Response Essentials

Practical Cyber Forensics

File System Forensic Analysis

Digital Forensics Explained

The Basics of Digital Forensics

Computer Crime Scene Investigation

Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book Description An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and

techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems Leverage the power of digital forensics for Windows systems About This Book Build your own lab environment to analyze forensic data and practice techniques. This book offers meticulous coverage with an example-driven approach and helps you build the key skills of performing forensics on Windows-based systems using digital artifacts. It uses specific open source and Linux-based tools so you can become proficient at analyzing forensic data and upgrade your existing knowledge. Who This Book Is For This book targets forensic analysts and professionals who would like to develop skills in digital forensic analysis for the Windows platform. You will acquire proficiency, knowledge, and core skills to undertake forensic analysis of digital data. Prior experience of information security and forensic analysis would be helpful. You will gain knowledge and an understanding of performing forensic analysis with tools especially built for the Windows platform. What You Will Learn Perform live analysis on victim or suspect Windows systems locally or remotely Understand the different natures and acquisition techniques of volatile and non-volatile data. Create a timeline of all the system actions to restore the history of an incident. Recover and analyze data from FAT and NTFS file systems. Make use of various tools to perform registry analysis. Track a system user's browser and e-mail activities to prove or refute some hypotheses. Get to know how to dump and analyze computer memory. In Detail Over the last few years, the wave of the cybercrime has risen rapidly. We have witnessed many major attacks on the governmental, military, financial, and media sectors. Tracking all these attacks and crimes requires a deep understanding of operating system operations, how to extract evident data from digital evidence, and the best usage of the digital forensic tools and techniques. Regardless of your level of experience in the field of information security in general, this book will fully introduce you to digital forensics. It will provide you with the knowledge needed to assemble different types of evidence effectively, and walk you through the various stages of the analysis process. We start by discussing the principles of the digital forensics process and move on to show you the approaches that are used to conduct analysis. We will then study various tools to perform live analysis, and go through different techniques to analyze volatile and non-volatile data. Style and approach This is a step-by-step guide that delivers knowledge about different Windows artifacts. Each topic is explained sequentially, including artifact analysis using different tools and techniques. These techniques make use of the evidence extracted from infected machines, and are accompanied by real-life examples.

As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations:

Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

Mobile Phone Security and Forensics

Optimization of Impression Evidence

Securing Digital Evidence with Linux Tools

A Guide for Digital Investigators

The Primer for Getting Started in Digital Forensics

An Incident-Based Approach to Forensic Investigations

***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.***

***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 plays a crucial role in identifying, analysing, and presenting cyber threats as evidence in a court of law. Artificial intelligence, particularly machine learning and deep learning, enables automation of the digital investigation process. This book provides an in-depth look at the fundamental and advanced methods in digital forensics. It also discusses how machine learning and deep learning algorithms can be used to detect and***

*investigate cybercrimes. This book demonstrates digital forensics and cyber-investigating techniques with real-world applications. It examines hard disk analytics and style architectures, including Master Boot Record and GUID Partition Table as part of the investigative process. It also covers cyberattack analysis in Windows, Linux, and network systems using virtual machines in real-world scenarios. Digital Forensics in the Era of Artificial Intelligence will be helpful for those interested in digital forensics and using machine learning techniques in the investigation of cyberattacks and the detection of evidence in cybercrimes.*

*Updated to include the most current events and information on cyberterrorism, the second edition of Computer Forensics: Cybercriminals, Laws, and Evidence continues to balance technicality and legal analysis as it enters into the world of cybercrime by exploring what it is, how it is investigated, and the regulatory laws around the collection and use of electronic evidence. Students are introduced to the technology involved in computer forensic investigations and the technical and legal difficulties involved in searching, extracting, maintaining, and storing electronic evidence, while simultaneously looking at the legal implications of such investigations and the rules of legal procedure relevant to electronic evidence. Significant and current computer forensic developments are examined, as well as the implications for a variety of fields including computer science, security, criminology, law, public policy, and administration.*

*Incident response techniques and procedures to respond to modern cyber threats*

*Game Hacking*

*Breakthroughs in Research and Practice*

*Linux Forensics*

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

*Real digital forensics*

*The book is an easy-to-follow guide with clear instructions on various mobile forensic techniques. The chapters and the topics within are structured for a smooth learning curve, which will swiftly empower you to master mobile forensics. If you are a budding forensic analyst, consultant, engineer, or a forensic professional wanting to expand your skillset, this is the book for you. The book will also be beneficial to those with an interest in mobile forensics or wanting to find data lost on mobile devices. It will be helpful to be familiar with forensics in general but no prior experience is required to follow this book.*

*Jerry Thigpen's study on the history of the Combat Talon is the first effort to tell the story of this wonderfully capable machine. This weapons system has performed virtually every imaginable tactical event in the spectrum of conflict and by any measure is the most versatile C-130 derivative ever produced. First modified and sent to Southeast Asia (SEA) in 1966 to replace theater unconventional warfare (UW) assets that were limited in both lift capability and speed the Talon I quickly adapted to theater UW tasking including infiltration and resupply and psychological warfare operations into North Vietnam. After spending four years in SEA and maturing into a highly respected UW weapons system the Joint Chief of Staff (JCS) chose the Combat Talon to lead the night low-level raid on the North Vietnamese prison camp at Son Tay. Despite the outcome of the operation the Talon I cemented its reputation as the weapons system of choice for long-range clandestine operations. In the period following the Vietnam War United States Air Force (USAF) special operations gradually lost its political and financial support which was graphically demonstrated in the failed Desert One mission into Iran. Thanks to congressional supporters like Earl Hutto of Florida and Dan Daniel of Virginia funds for aircraft upgrades and military construction projects materialized to meet the ever-increasing threat to our nation. Under the leadership of such committed hard-driven officers as Brenci Uttaro Ferkes Meller and Thigpen the crew force became the most disciplined in our Air Force. It was capable of penetrating hostile airspace at night in a low-level mountainous environment covertly to execute any number of unconventional warfare missions.*

*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.*

*A resource to help forensic investigators locate, analyze, and understand digital evidence found on modern Linux systems after a crime, security incident or cyber attack. Practical Linux Forensics dives into the technical details of analyzing postmortem forensic images of Linux systems which have been misused, abused, or the target of malicious attacks. It helps forensic investigators locate and analyze digital evidence found on Linux desktops, servers, and IoT devices. Throughout the book, you learn how to identify digital artifacts which may be of interest to an investigation, draw logical conclusions, and reconstruct past activity from incidents. You'll learn how Linux works from a digital forensics and investigation perspective, and how to interpret evidence from Linux environments. The techniques shown are intended to be independent of the forensic analysis platforms and tools used. Learn how to:*

- Extract evidence from storage devices and analyze partition tables, volume managers, popular Linux filesystems (Ext4, Btrfs, and Xfs), and encryption*
- Investigate evidence from Linux logs, including traditional syslog, the systemd journal, kernel and audit logs, and logs from daemons and applications*
- Reconstruct the Linux startup process, from boot loaders (UEFI and Grub) and kernel initialization, to systemd unit files and targets leading up to a graphical login*
- Perform analysis of power, temperature, and the physical environment of a Linux machine, and find evidence of sleep, hibernation, shutdowns, reboots, and crashes*
- Examine installed software, including distro installers, package formats, and package management systems from Debian, Fedora, SUSE, Arch, and other distros*
- Perform analysis of time and Locale settings, internationalization including language and keyboard settings, and geolocation on a Linux system*
- Reconstruct user login sessions (shell, X11 and Wayland), desktops (Gnome, KDE, and others) and analyze keyrings, wallets, trash cans, clipboards, thumbnails, recent files and other desktop artifacts*
- Analyze network configuration, including interfaces, addresses, network managers, DNS, wireless artifacts (Wi-Fi, Bluetooth, WWAN), VPNs (including WireGuard), firewalls, and proxy settings*
- Identify traces of attached peripheral devices (PCI, USB, Thunderbolt, Bluetooth) including external storage, cameras, and mobiles, and reconstruct printing and scanning activity*

*Photoshop CS3 for Forensics Professionals*

*Forensically investigate and analyze iOS, Android, and Windows 10 devices, 4th Edition*

*Practical Digital Forensics*

*Digital Forensics with Open Source Tools*

*Detecting Malware and Threats in Windows, Linux, and Mac Memory*

*Digital Forensics, Investigation, and Response*

This new edition provides both theoretical and practical background of security and forensics for mobile phones. The author discusses confidentiality, integrity, and availability threats in mobile telephones to provide background for the rest of the book. Security and secrets of mobile phones are discussed including software and hardware interception, fraud and other malicious techniques used "against" users. The purpose of this book is to raise user awareness in regards to security and privacy threats present in the use of mobile phones while readers will also learn where forensics data reside in the mobile phone and the network and how to conduct a relevant analysis. The information on denial of service attacks has been thoroughly updated for the new edition. Also, a major addition to this edition is a section discussing software defined radio and open source tools for mobile phones.

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

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

Practical Forensic Imaging Securing Digital Evidence with Linux Tools No Starch Press

Practical Mobile Forensics

The Art of Memory Forensics

Applications and Techniques

Windows Forensics Cookbook

The Praetorian STARShip : the untold story of the Combat Talon

computer security and incident response

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

Well-documented scenes can prove to be invaluable pieces of evidence at trial, and the ability to take compelling photographs is a critical skill for forensic scientists and investigators. Practical Forensic Digital Imaging: Applications and Techniques is an up-to-date and thorough treatment of digital imaging in the forensic sciences. Balancing pr

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

A Complete Digital Imaging Course for Investigators

Practical Forensic Imaging

Computer Forensics For Dummies

Digital Forensics in the Era of Artificial Intelligence

Practical Forensic Digital Imaging

Learn Computer Forensics

Handbook of Digital Forensics and Investigation builds on the success of the Handbook of Computer Crime Investigation, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is 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

The digital revolution over the past several decades has advanced every facet of evidence detection, photography, optimization, and interpretation. Forensic scientists and practitioners have benefited tremendously from the move from film to digital. With proper procedure in place, digital images and casework capabilities have increased tremendously in both complexity and range due to a vast array of tools to enhance evidence and photography. Forensic Digital Image Processing: Optimization of Impression Evidence provides the forensic investigator with the tools and understanding to extract, optimize, and interpret the maximum evidence possible from crime scenes to increase identifications. The book begins by examining the emergence of forensic digital image processing, and the gradual improvement and acceptance of the science over the past four decades. Coverage includes looking at the issues of image integrity and authentication including forensic image optimization and the manipulation of images. Chapters explore techniques exploiting color theory, modes, and channels to optimize signal-to-noise ratio in images. One of the greatest assets of digital image technology is the ability to combine multiple images of the same subject to create a final, blended image: one that displays the desired evidence and is especially useful for fingerprint or footwear impression. Later chapters demonstrate image subtraction, focus stacking, and high dynamic range, utilizing images in optimum focus and with substrate interference diminished or removed entirely. The authors look at fast Fourier transform as an optimal tool for noise removal, addressing basic theory and diagnosis of the noise signatures. The book discusses the history of digital imaging techniques and their treatment within the court system. Forensic Digital Image Processing: Optimization of Impression Evidence serves as an invaluable resource and tool for practicing professionals—as well as those new to the field—to look at best practices, the latest technology, and advances in the increasing array of tools of the trade.

Digital Forensics for Legal Professionals

Digital Forensics Processing and Procedures

Handbook of Digital Forensics and Investigation

Practical Linux Forensics

Developing Autonomous Bots for Online Games

Digital Forensics and Incident Response