OMB No. 5903652047881

Practical Forensic Imaging Securing Digital Evidence With Linux Tools

What is Forensics Imaging? #opentext | Digital Forensic | Tableau Write Blocker TX1 Review | Create a Forensic Image EX01 Digital Forensics with Kali Linux : Introduction to Forensic Imaging | packtpub.com Forensic imaging | How To Calculate Hash Value | Imaging Using Write Blocker Tool | Forensic Imaging with FTK Imager | Free Digital Forensics Tutorial Autopsy - Forensic Acquisition Tool | Digital Forensics Investigation | Autopsy Tutorial Best digital forensics | computer forensics| cyber forensic free tools Starting a New Digital Forensic Investigation Case in Autopsy 4.19+ TX1 Forensic Imager #TX1ForensicImager #DigitalForensicTX1 Linear Bookscanner | Studio Mango Digital Forensics Case Study Intro to DIY film scanning Archival Grade Flatbed Book Scanner - Avision FB6080E Performing Digital Forensic Scan an entire book in literally MINUTES!! M1 MacBook and Forensics How to Identify Digital Evidence | Introduction to Digital Forensics What's in the box? Digital Intelligence UltraBlock Kit! Creating a Forensic Image using FTK Imager/Encase Imager | Cyber Forensic practical 1 How to set up a digital forensics lab | Cyber Work Hacks Forensic Imaging Creating a forensic image of any drive with Kali Linux [English] Elon Musk Laughs at the Idea of Getting a PhD and Explains How to Actually Be Useful! Acquiring Digital Forensics Evidence - CompTIA Security+ Lab 30 What's in the box? Tableau Forensic Imager TX1! Intro to Computer Forensics: Module 4: Forensic imaging □□ Learn about Digital Forensics! □AMA and Digital Forensic Hardware□ DFIRScience 20k Live Stream

Practical Mobile Forensics
Learn Computer Forensics
Introductory Computer Forensics
Windows Forensics Cookbook
Game Hacking
Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice
Computer and Intrusion Forensics
The Best Damn Cybercrime and Digital Forensics Book Period
Digital Forensics and Incident Response
Digital Forensics, Investigation, and Response
Digital Evidence and Computer Crime
File System Forensic Analysis
Big Data Analytics and Computing for Digital Forensic Investigations
Advances in Digital Forensics II
Digital Image Forensics
Practical Digital Forensics

Practical Forensic Imaging Securing Digital Evidence With Linux Tools *OMB No. 5903652047881 edited by*

BROOKLYN STRICKLAND

Practical Mobile Forensics Packt Publishing Ltd
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.
Learn Computer Forensics Packt Publishing Ltd
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.

Introductory Computer Forensics

Packt Publishing Ltd
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.
Windows Forensics Cookbook Springer Science & Business Media
Electronic discovery refers to a process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case. Computer forensics is the application of computer investigation and analysis techniques to perform an investigation to find out exactly what happened on a computer and who was responsible. IDC estimates that the U.S. market for computer forensics will be grow from $252 million in 2004 to $630 million by 2009. Business is strong outside the United States, as well. By 2011, the estimated international market will be $1.8 billion dollars. The Techno Forensics Conference has increased in size by almost 50% in its second year; another example of the rapid growth in the market. This book is the first to combine cybercrime and digital forensic topics to provides law enforcement and IT security professionals with the information needed to manage a digital investigation. Everything needed for analyzing forensic data and recovering digital evidence can be found in one place, including instructions for building a digital forensics lab. * Digital investigation and forensics is a growing industry * Corporate I.T. departments investigating corporate espionage and criminal activities are learning as they go and need a comprehensive guide to e-discovery * Appeals to law enforcement agencies with limited budgets
Game Hacking Academic Press
This hands-on textbook provides an accessible introduction to the fundamentals of digital forensics. The text contains thorough coverage of the theoretical foundations, explaining what computer forensics is, what it can do, and also what it can’t. A particular focus is presented on establishing sound forensic thinking and methodology, supported by practical guidance on performing typical tasks and using common forensic tools. Emphasis is also placed on universal principles, as opposed to content unique to specific legislation in individual countries. Topics and features: introduces the fundamental concepts in digital forensics, and the steps involved in a forensic examination in a digital environment; discusses the nature of what cybercrime is, and how digital evidence can be of use during criminal investigations into such crimes; offers a practical overview of common practices for cracking encrypted data; reviews key artifacts that have proven to be important in several cases, highlighting where to find these and how to

correctly interpret them; presents a survey of various different search techniques, and several forensic tools that are available for free; examines the functions of AccessData Forensic Toolkit and Registry Viewer; proposes methods for analyzing applications, timelining, determining the identity of the computer user, and deducing if the computer was remote controlled; describes the central concepts relating to computer memory management, and how to perform different types of memory analysis using the open source tool Volatility; provides review questions and practice tasks at the end of most chapters, and supporting video lectures on YouTube. This easy-to-follow primer is an essential resource for students of computer forensics, and will also serve as a valuable reference for practitioners seeking instruction on performing forensic examinations in law enforcement or in the private sector.

Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice No Starch Press

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

Computer and Intrusion Forensics CRC Press

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.

The Best Damn Cybercrime and Digital Forensics Book Period Academic Press

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

Digital Forensics and Incident Response

Springer

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

Digital Forensics, Investigation, and Response

Packt Publishing Ltd

Understanding Forensic Digital Imaging offers the principles of forensic digital imaging and photography in a manner that is straightforward and easy to digest for the professional and student. It provides information on how to photograph any setting that may have forensic value, details how to follow practices that are acceptable in court, and recommends what variety of hardware and software are most valuable to a practitioner. In addition to chapters on basic topics such as light and lenses, resolution, and file formats, the book contains forensic-science-specific information on SWGIT and the use of photography in investigations and in court. Of particular note is Chapter 17, Establishing Quality Requirements, which offers information on how to create a good digital image, and is more comprehensive than any other source currently available. Covers topics that are of vital importance to the practicing professional Serves as an up-to-date reference in the rapidly evolving world of digital imaging Uses clear and concise language so that any reader can understand the technology and science behind digital imaging

Digital Evidence and Computer Crime Cengage Learning

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

File System Forensic Analysis Packt Publishing Ltd

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.

Big Data Analytics and Computing for Digital Forensic Investigations

Springer
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.
Advances in Digital Forensics II Jones & Bartlett Learning
Updated with the latest advances from the field, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, Fifth Edition combines all-encompassing topic coverage and authoritative information from seasoned experts to deliver the most comprehensive forensics resource available. This proven author team's wide ranging areas of expertise mirror the breadth of coverage provided in the book, which focuses on techniques and practices for gathering and analyzing evidence used to solve crimes involving computers. Providing clear instruction on the tools and techniques of the trade, it introduces readers to every step of the computer forensics investigation-from lab set-up to testifying in court. It also details step-by-step guidance on how to use current forensics software. Appropriate for learners new to the field, it is also an excellent refresher and technology update for professionals in law enforcement, investigations, or computer security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Digital Image Forensics Packt Publishing Ltd
Digital forensics has recently gained a notable development and become the most demanding area in today’s information security requirement. This book investigates the areas of digital forensics, digital investigation and data analysis procedures as they apply to computer fraud and cybercrime, with the main objective of describing a variety of digital crimes and retrieving potential digital evidence. Big Data Analytics and Computing for Digital Forensic Investigations gives a contemporary view on the problems of information security. It presents the idea that protective mechanisms and software must be integrated along with forensic capabilities into existing forensic software using big data computing tools and techniques. Features Describes trends of digital forensics served for big data and the challenges of evidence acquisition Enables digital forensic investigators and law enforcement agencies to enhance their digital investigation capabilities with the application of data science analytics, algorithms and fusion technique This book is focused on helping professionals as well as researchers to get ready with next-generation security systems to mount the rising challenges of computer fraud and cybercrimes as well as with digital forensic investigations. Dr Suneeta Satpathy has more than ten years of teaching experience in different subjects of the Computer Science and Engineering discipline. She is currently working as an associate professor in the Department of Computer Science and Engineering, College of Bhubaneswar, affiliated with Biju Patnaik University and Technology, Odisha. Her research interests include computer forensics, cybersecurity, data fusion, data mining, big data analysis and decision mining. Dr Sachi Nandan Mohanty is an associate professor in the Department of Computer Science and Engineering at ICFAI Tech, ICFAI Foundation for Higher Education, Hyderabad, India. His research interests include data mining, big data analysis, cognitive science, fuzzy decision-making, brain–computer interface, cognition and computational intelligence.
Practical Digital Forensics Artech House
A Guide to Enter the Journey of a Digital Forensic Investigator KEY FEATURES ● Provides hands-on training in a forensics lab, allowing learners to conduct their investigations and analysis. ● Covers a wide range of forensics topics such as web, email, RAM, and mobile devices. ● Establishes a solid groundwork in digital forensics basics including evidence-gathering tools and methods. DESCRIPTION Forensics offers every IT and computer professional a wide opportunity of exciting and lucrative career. This book is a treasure trove of practical knowledge for anyone interested in forensics, including where to seek evidence and how to extract it from buried digital spaces. The book begins with the exploration of Digital Forensics with a brief overview of the field's most basic definitions, terms, and concepts about scientific investigations. The book lays down the groundwork for how digital forensics works and explains its primary objectives, including collecting, acquiring, and analyzing digital evidence. This book focuses on starting from the essentials of forensics and then practicing the primary tasks and activities that forensic analysts and investigators execute for every security incident. This book will provide you with the technical abilities necessary for Digital Forensics, from the ground up, in the form of stories, hints, notes, and links to further reading. Towards the end, you'll also have the opportunity to build up your lab, complete with detailed instructions and a wide range of forensics tools, in which you may put your newly acquired knowledge to the test. WHAT YOU WILL LEARN ● Get familiar with the processes and procedures involved in establishing your own in-house digital forensics lab. ● Become confident in acquiring and analyzing data from RAM, HDD, and SSD. ● In-detail windows forensics and analyzing deleted files, USB, and IoT firmware. ● Get acquainted with email investigation, browser forensics, and different tools to collect the evidence. ● Develop proficiency with anti-forensic methods, including metadata manipulation, password cracking, and steganography. WHO THIS BOOK IS FOR Anyone working as a forensic analyst, forensic investigator, forensic specialist, network administrator, security engineer, cybersecurity analyst, or application engineer will benefit from reading this book. You only need a foundational knowledge of networking and hardware to get started with this book. TABLE OF CONTENTS 1. Introduction to Digital Forensics 2. Essential Technical Concepts 3. Hard Disks and File Systems 4. Requirements for a Computer Forensics Lab 5. Acquiring Digital Evidence 6. Analysis of Digital Evidence 7. Windows Forensic Analysis 8. Web Browser and E-mail Forensics 9. E-mail Forensics 10. Anti-Forensics Techniques and Report Writing 11. Hands-on Lab Practical

Strengthening Forensic Science in the United States

No Starch Press
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
Fundamentals of Digital Forensics BPB Publications
The Advanced Forensic Science Series grew out of the recommendations from the 2009 NAS Report: Strengthening Forensic Science: A Path Forward. This volume, Digital and Document Examination, will serve as a graduate level text for those studying and teaching digital forensics and forensic document examination, as well as an excellent reference for forensic scientist’s libraries or use in their casework. Coverage includes digital devices, transportation, types of documents, forensic accounting and professional issues. Edited by a world-renowned leading forensic expert, the Advanced Forensic Science Series is a long overdue solution for the forensic science community. Provides basic principles of forensic science and an overview of digital forensics and document examination Contains sections on digital devices, transportation, types of documents and forensic accounting Includes sections on professional issues, such as from crime scene to court, forensic laboratory reports and health and safety Incorporates effective pedagogy, key terms, review questions, discussion questions and additional reading suggestions

Digital Forensics Basics

Packt Publishing Ltd
Practical Forensic ImagingNo Starch Press

Computer Forensics InfoSec Pro Guide

Packt Publishing Ltd
Scores of talented and dedicated people serve the forensic science community, performing vitally important work. However, they are often constrained by lack of adequate resources, sound policies, and national support. It is clear that change and advancements, both systematic and scientific, are needed in a number of forensic science disciplines to ensure the reliability of work, establish enforceable standards, and promote best practices with consistent application. Strengthening Forensic Science in the United States: A Path Forward provides a detailed plan for addressing these needs and suggests the creation of a new government entity, the National Institute of Forensic Science, to establish and enforce standards within the forensic science community. The benefits of improving and regulating the forensic science disciplines are clear: assisting law enforcement officials, enhancing homeland security, and reducing the risk of wrongful conviction and exoneration. Strengthening Forensic Science in the United States gives a full account of what is needed to advance the forensic science disciplines, including upgrading of systems and organizational structures, better training, widespread adoption of uniform and enforceable best practices, and mandatory certification and accreditation programs. While this book provides an essential call-to-action for congress and policy makers, it also serves as a vital tool for law enforcement agencies, criminal prosecutors and attorneys, and forensic science educators.

Related with Practical Forensic Imaging Securing Digital Evidence With Linux Tools:
© Practical Forensic Imaging Securing Digital Evidence With Linux Tools What Happened In Sign Language
© Practical Forensic Imaging Securing Digital Evidence With Linux Tools What Grade Is Level E In Iready Math
© Practical Forensic Imaging Securing Digital Evidence With Linux Tools What Goes Putt Putt Putt Putt Answer Key