
Practical Forensic Imaging Securing Digital Evidence With Linux Tools

If you ally infatuation such a referred **Practical Forensic Imaging Securing Digital Evidence With Linux Tools** book that will find the money for you worth, get the certainly best seller from us currently from several preferred authors. If you desire to humorous books, lots of novels, tale, jokes, and more fictions collections are along with launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every book collections Practical Forensic Imaging Securing Digital Evidence With Linux Tools that we will definitely offer. It is not roughly the costs. Its nearly what you infatuation currently. This Practical Forensic Imaging Securing Digital Evidence With Linux Tools, as one of the most committed sellers here will agreed be accompanied by the best options to review.

*Practical Forensic
Imaging Securing
Digital Evidence With
Linux Tools*

2022-11-02

RAMOS FRENCH

Digital Forensics with

Open Source Tools Packt
Publishing Ltd
Digital forensics deals

with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has

myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics X describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The

areas of coverage include:

- Internet Crime Investigations;
- Forensic Techniques;
- Mobile Device Forensics;
- Forensic Tools and Training.

This book is the 10th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book

contains a selection of twenty-two edited papers from the 10th Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Vienna, Austria in the winter of 2014. *Advances in Digital Forensics X* is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

File System Forensic

Analysis Springer
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

Handbook of Digital Forensics and Investigation Academic Press

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. *Advances in Digital Forensics IV* Addison-Wesley Professional 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 Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book Apress This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book's 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on

experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students' understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of

digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research.

It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book. *Practical Forensic Imaging* 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.

Computer Forensics InfoSec Pro Guide Elsevier 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.

Practical Mobile Forensics
BPB Publications
Practically every crime now involves some aspect of digital evidence. This is the most recent volume in the Advances in Digital Forensics series. It

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. This book contains a selection of twenty-eight edited papers from the Fourth Annual IFIP WG 11.9 Conference on Digital Forensics, held at Kyoto University, Kyoto, Japan in the spring of 2008.

Advances in Digital

Forensics XV CRC 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**
Practical Forensic Digital Imaging John Wiley & Sons
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** **Perform a variety of Windows forensic investigations to analyze and overcome complex challenges** **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

sequenceValidate forensic hardware and softwareDiscover the locations of common Windows artifactsDocument your findings using technically correct terminologyWho 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. Individuals planning to pass the Certified Forensic Computer Examiner (CFCE) certification will also find this book useful. [Windows Forensics Cookbook](#) Springer 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.

Digital Forensics Basics

John Wiley & Sons

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically

sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. *Digital Forensics Basics* is written

as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. *What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and*

more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigations Gather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10-specific feature forensics Utilize anti-forensic techniques, including steganography, data destruction

techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals
Imaging for Forensics

and Security Packt Publishing Ltd 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 in the Era of Artificial Intelligence Springer Science & Business Media Imaging for Forensics and Security: From Theory to Practice provides a detailed analysis of new imaging and pattern recognition techniques for the understanding and deployment of biometrics and forensic techniques as practical solutions to

increase security. It contains a collection of the recent advances in the technology ranging from theory, design, and implementation to performance evaluation of biometric and forensic systems. This book also contains new methods such as the multiscale approach, directional filter bank, and wavelet maxima for the development of practical solutions to biometric problems. The book introduces a new forensic system based on shoeprint imagery with

advanced techniques for use in forensics applications. It also presents the concept of protecting the originality of biometric images stored in databases against intentional and unintentional attacks and fraud detection data in order to further increase the security.

Handbook of Digital Forensics of Multimedia Data and Devices

Springer

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.

iPhone and iOS Forensics Newnes

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.

Digital Forensics

Processing and

Procedures Pearson IT Certification

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.

A Practical Guide to Digital Forensics Investigations Springer
Digital forensics and multimedia forensics are

rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital

forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended to by contributions from researchers and forensic

practitioners specializing in diverse topics such as forensic authentication, forensic triage, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features: Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of

multimedia data and devices Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice

guides, test datasets and more case studies [Practical Windows Forensics](#) Springer 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 OS Forensics

Pearson Education
Security Smarts for the Self-Guided IT Professional Find out how to excel in the field of computer forensics investigations. Learn what it takes to transition from an IT professional to a computer forensic examiner in the private sector. Written by a

Certified Information Systems Security Professional, Computer Forensics: InfoSec Pro Guide is filled with real-world case studies that demonstrate the concepts covered in the book. You'll learn how to set up a forensics lab, select hardware and software, choose forensic imaging procedures, test your tools, capture evidence from different sources, follow a sound investigative process, safely store evidence, and verify your findings. Best practices for documenting

your results, preparing reports, and presenting evidence in court are also covered in this detailed resource. Computer Forensics: InfoSec Pro Guide features:
Lingo—Common security terms defined so that you're in the know on the job IMHO—Frank and relevant opinions based on the author's years of industry experience
Budget Note—Tips for getting security technologies and processes into your organization's budget In Actual

Practice—Exceptions to the rules of security explained in real-world contexts Your

Plan—Customizable checklists you can use on the job now Into

Action—Tips on how, why, and when to apply new skills and techniques at work