

Computer Forensics And Investigations 4th Edition

Praise for the Fourth Edition of Fraud Auditing and Forensic Accounting "Tommie and Aaron Singleton have made important updates to a book I personally rely very heavily upon: Fraud Auditing and Forensic Accounting (FAFA). In the newest edition, they take difficult topics and explain them in straightforward actionable language. All my students benefitted from reading the third edition of the FAFA to better understand the issues and area of fraud and forensic accounting. With their singular focus on understandability and practicality, this Fourth Edition of the book makes a very important contribution for academics, researchers, practitioners, and students. Bravo!"—Dr. Timothy A. Pearson, Director, Division of Accounting, West Virginia University, Executive Director, Institute for Fraud Prevention "Finally someone has written a book that combines fraud examination and forensic accounting. The authors have clearly explained both in their earlier edition and now they have enhanced the first with additional materials. The order in which the material is presented is easy to grasp and logically follows the 'typical' fraud examination from the awareness that something is wrong to the court case. The explanatory materials presented aid this effort by being both well placed within the book and relevant to the narrative." —Dr. Douglas E. Ziegenfuss, Chair and Professor, Department of Accounting, Old Dominion University "Fraud Auditing and Forensic Accounting is a masterful compilation of the concepts found in this field. The organization of the text with the incorporation of actual cases, facts, and figures provides a logical and comprehensive basis for learning the intricacies of fraud examination and forensic accounting. The authors successfully blend the necessary basics with advanced principles in a manner that makes the book an outstanding resource for students and professionals alike."—Ralph Q. Summerford, President of Forensic/Strategic Solutions, PC

The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

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

FRAUD AUDITING AND FORENSIC ACCOUNTING With the responsibility of detecting and preventing fraud falling heavily on the accounting profession, every accountant needs to recognize fraud and learn the tools and strategies necessary to catch it in time. Providing valuable information to those responsible for dealing with prevention and discovery of financial deception, Fraud Auditing and Forensic Accounting, Fourth Edition helps accountants develop an investigative eye toward both internal and external fraud and provides tips for coping with fraud when it is found to have occurred. Completely updated and revised, the new edition presents: Brand-new chapters devoted to fraud response as well as to the physiological aspects of the fraudster A closer look at how forensic accountants get their job done More about Computer-Assisted Audit Tools (CAATs) and digital forensics Technological aspects of fraud auditing and forensic accounting Extended discussion on fraud schemes Case studies demonstrating industry-tested methods for dealing with fraud, all drawn from a wide variety of actual incidents Inside this book, you will find step-by-step keys to fraud investigation and the most current methods for dealing with financial fraud within your organization. Written by recognized experts in the field of white-collar crime, this Fourth Edition provides you, whether you are a beginning forensic accountant or an experienced investigator, with industry-tested methods for detecting, investigating, and preventing financial schemes.

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.

This book contains a selection of thoroughly refereed and revised papers from the Fourth International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2012, held in October 2012 in Lafayette, Indiana, USA. The 20 papers in this volume are grouped in the following topical sections: cloud investigation; malware; behavioral; law; mobile device forensics; and cybercrime investigations. 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 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,

All you need to know to succeed in digital forensics: technical and investigative skills, in one book Complete, practical, and up-to-date Thoroughly covers digital forensics for Windows, Mac, mobile, hardware, and networks Addresses online and lab investigations, documentation, admissibility, and more By Dr. Darren Hayes, founder of Pace University's Code Detectives forensics lab—one of America's "Top 10 Computer Forensics Professors" Perfect for anyone pursuing a digital forensics career or working with examiners Criminals go where the money is. Today, trillions of dollars of assets are digital, and digital crime is growing fast. In response, demand for digital forensics experts is soaring. To succeed in this exciting field, you need strong technical and investigative skills. In this guide, one of the world's leading computer forensics experts teaches you all the skills you'll need. Writing for students and professionals at all levels, Dr. Darren Hayes presents complete best practices for capturing and analyzing evidence, protecting the chain of custody, documenting investigations, and scrupulously adhering to the law, so your evidence can always be used. Hayes introduces today's latest technologies and technical challenges, offering detailed coverage of crucial topics such as mobile forensics, Mac forensics, cyberbullying, and child endangerment. This guide's practical activities and case studies give you hands-on mastery of modern digital forensics tools and techniques. Its many realistic examples reflect the author's extensive and pioneering work as a forensics examiner in both criminal and civil investigations. Understand what computer forensics examiners do, and the types of digital evidence they work with Explore Windows and Mac computers, understand how their features affect evidence gathering, and use free tools to investigate their contents Extract data from diverse storage devices Establish a certified forensics lab and implement good practices for managing and processing evidence Gather data and perform investigations online Capture Internet communications, video, images, and other content Write comprehensive reports that withstand defense objections and enable successful prosecution Follow strict search and surveillance rules to make your evidence admissible Investigate network breaches, including dangerous Advanced Persistent Threats (APTs) Retrieve immense amounts of evidence from smartphones, even without seizing them Successfully investigate financial fraud performed with digital devices Use digital photographic evidence, including metadata and social media images "Digital forensics is the science of collecting the evidence that can be used in a court of law to prosecute the individuals who engage in electronic crime"--Provided by publisher.

This book constitutes the proceedings of the International Conference on Information Security and Assurance, held in Brno, Czech Republic in August 2011.

Mobile forensics has grown from a relatively obscure tradecraft to a crucial part of many criminal investigations, and is now used daily by examiners and analysts within local, state, and federal law enforcement as well as within the military, US government organizations, and the private "e-Discovery" industry. Developments in forensic research, tools, and processes over the past decade have been very successful and continue to change at a rapid pace. Forensic Investigations and Risk Management in Mobile and Wireless Communications is a collection of innovative research on the methods and applications of analyzing mobile devices and data for collection of information pertaining to the legal evidence related to various security breaches and intrusion detection. While highlighting topics including cybercrime, neural networks, and smartphone security, this book is ideally designed for security analysts, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

Would your company be prepared in the event of: * Computer-driven espionage * A devastating virus attack * A hacker's unauthorized access * A breach of data security? As the sophistication of computer technology has grown, so has the rate of computer-related criminal activity. Subsequently, American corporations now lose billions of dollars a year to hacking, identity theft, and other computer attacks. More than ever, businesses and professionals responsible for the critical data of countless customers and employees need to anticipate and safeguard against computer intruders and attacks. The first book to successfully speak to the nontechnical professional in the fields of business and law on the topic of computer crime, Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers provides valuable advice on the hidden difficulties that can blindside companies and result in damaging costs. Written by industry expert Michael Sheetz, this important book provides readers with an honest look at the computer crimes that can annoy, interrupt--and devastate--a business. Readers are equipped not only with a solid understanding of how computers facilitate fraud and financial crime, but also how computers can be used to investigate, prosecute, and prevent these crimes. If you want to know how to protect your company from computer crimes but have a limited technical background, this book is for you. Get Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers and get prepared.

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

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.

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.

"This book provides academia and organizations insights into practical and applied solutions, frameworks, technologies, and implementations for situational awareness in computer networks"--Provided by publisher.

WEB-BASED LABS FOR GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, FOURTH EDITION provides step-by-step labs taken directly from GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, FOURTH EDITION. Using a real lab environment over the Internet, learners can log on anywhere, anytime via a Web browser to gain essential hands-on experience in computer forensics.

FORENSIC SCIENCE: ADVANCED INVESTIGATIONS is part of a comprehensive course offering as a second-level high school course in forensic science, a course area in which students have the opportunity to expand their knowledge of chemistry, biology, physics, earth science, math, and psychology, as well as associate this knowledge with real-life applications. This text builds on concepts introduced in FORENSIC SCIENCE: FUNDAMENTALS & INVESTIGATIONS, as well as introduces additional topics, such as arson and explosions. Following the same solid instructional design as the FUNDAMENTALS & INVESTIGATIONS text, the book balances extensive scientific concepts with hands-on classroom and lab activities, readings, intriguing case studies, and chapter-opening scenarios. The book's exclusive Gale Forensic Science eCollection database provides instant access to hundreds of articles and Internet resources that spark student interest and extend learning beyond the book. Comprehensive, time-saving teacher support and lab activities deliver exactly what you need to ensure that students receive a solid, complete science education that keeps readers at all learning levels enthused about science. This two-book series provides a solution that is engaging, contemporary, and specifically designed for high school students. Instructors can be confident that the program has been written by high school forensic science instructors with their unique needs in mind, including content tied to the national and state science standards they are accountable to teaching. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Master the skills you need to conduct a successful digital investigation with Nelson/Phillips/Steuart's GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, Sixth Edition--the most comprehensive forensics resource available. While other books offer just an overview of the field, this hands-on learning text provides clear instruction on the tools and techniques of the trade, walking you through every step of the computer forensics investigation--from lab setup to testifying in court. It also explains how to use current forensics software and provides free demo downloads. It includes the most up-to-date coverage available of Linux and Macintosh, virtual machine software such as VMware and Virtual Box, Android, mobile devices, handheld devices, cloud forensics, email, social media and the Internet of Anything. With its practical applications, you can immediately put what you learn into practice.

* Incident response and forensic investigation are the processes of detecting attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks * This much-needed reference covers the methodologies for incident response and computer forensics, Federal Computer Crime law information and evidence requirements, legal issues, and working with law enforcement * Details how to detect, collect, and eradicate breaches in e-mail and malicious code * CD-ROM is packed with useful tools that help capture and protect forensic data; search volumes, drives, and servers for evidence; and rebuild systems quickly after evidence has been obtained

The official, Guidance Software-approved book on the newest EnCE exam! The EnCE exam tests that computer forensic analysts and examiners have thoroughly mastered computer investigation methodologies, as well as the use of Guidance Software's EnCase Forensic 7. The only official Guidance-endorsed study guide on the topic, this book prepares you for the exam with extensive coverage of all exam topics, real-world scenarios, hands-on exercises, up-to-date legal information, and sample evidence files, flashcards, and more. Guides readers through preparation for the newest EnCase Certified Examiner (EnCE) exam Prepares candidates for both Phase 1 and Phase 2 of the exam, as well as for practical use of the certification Covers identifying and searching hardware and files systems, handling evidence on the scene, and acquiring digital evidence using EnCase Forensic 7 Includes hands-on exercises, practice questions, and up-to-date legal information Sample evidence files, Sybex Test Engine, electronic flashcards, and more If you're preparing for the new EnCE exam, this is the study guide you need.

Guide to Computer Forensics and InvestigationsCengage Learning

For introductory and intermediate courses in computer forensics, digital investigations, or computer crime investigation By applying information systems, computer security, and criminal justice principles and practices to crime investigations and other legal actions, this text teaches students how to use forensically-sound methodologies and software to acquire admissible electronic evidence (e-evidence) with coverage of computer and email forensics, cell phone and IM forensics, and PDA and Blackberry forensics.

An introduction to the growing field of computer forensics provides a hands-on guide that explains how to conduct an investigation involving digital media, discussing how computer operating systems work, a wide variety of forensic tools, how to be an expert witness during a trial, and key concepts including chain of custody and evidence documentation procedures. Original. (Intermediate)

Learners will master the skills necessary to launch and complete a successful computer investigation with the updated fourth edition of this popular book, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS. This resource guides readers through conducting a high-tech investigation, from acquiring digital evidence to reporting its findings. Updated coverage includes new software and technologies as well as up-to-date reference sections. Learn how to set up a forensics lab, how to acquire the proper and necessary tools, and how to conduct the investigation and subsequent digital analysis. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

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

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.

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.

As the Web grows and expands into ever more remote parts of the world, the availability of resources over the Internet increases exponentially. Making use of this widely prevalent tool, organizations and individuals can share and store knowledge like never before. Cloud Technology: Concepts, Methodologies, Tools, and Applications investigates the latest research in the ubiquitous Web, exploring the use of applications and software that make use of the Internet's anytime, anywhere availability. By bringing together research and ideas from across the globe, this publication will be of use to computer engineers, software developers, and end users in business, education, medicine, and more. Covering up-to-date mobile platforms, this book focuses on teaching you the most recent tools and techniques for investigating mobile devices. Readers will delve into a variety of mobile forensics techniques for iOS 11-13, Android 8-10 devices, and Windows 10.

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

The Hands-On Information Security Lab Manual allows users to apply the basics of their introductory security knowledge in a hands-on environment with detailed exercises using Windows 2000, XP and Linux. This non-certification based lab manual includes coverage of scanning, OS vulnerability analysis and resolution firewalls, security maintenance, forensics, and more. A full version of the software needed to complete these projects is included on a CD with every text, so instructors can effortlessly set up and run labs to correspond with their classes. The Hands-On Information Security Lab Manual is a suitable resource for introductory, technical and managerial courses, and is a perfect

supplement to the Principles of Information Security and Management of Information Security texts. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Digital Age offers many far-reaching opportunities - opportunities that allow for fast global communications, efficient business transactions and stealthily executed cyber crimes. Featuring contributions from digital forensic experts, the editor of Forensic Computer Crime Investigation presents a vital resource that outlines the latest strategies. Forensic Science: The Basics, Fourth Edition is fully updated, building on the popularity of the prior editions. The book provides a fundamental background in forensic science, criminal investigation and court testimony. It describes how various forms of evidence are collected, preserved and analyzed scientifically, and then presented in court based on the analysis of the forensic expert. The book addresses knowledge of the natural and physical sciences, including biology and chemistry, while introducing readers to the application of science to the justice system. New topics added to this edition include coverage of the formation and work of the NIST Organization of Scientific Area Committees (OSACs), new sections on forensic palynology (pollen), forensic taphonomy, the opioid crisis, forensic genetics and genealogy, recent COVID-19 fraud schemes perpetrated by cybercriminals, and a wholly new chapter on forensic psychology. Each chapter presents a set of learning objectives, a mini glossary, and acronyms. While chapter topics and coverage flow logically, each chapter can stand on its own, allowing for continuous or selected classroom reading and study. Forensic Science, Fourth Edition is an ideal introductory textbook to present forensic science principles and practices to students, including those with a basic science background without requiring prior forensic science coursework.

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Completely revised and rewritten to keep pace with the fast-paced field of Computer Forensics! Computer crimes call for forensics specialists, people who know how to find and follow the evidence. System Forensics, Investigation, and Response, Second Edition begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. New and Key Features of the Second Edition: Examines the fundamentals of system forensics Discusses computer crimes and forensic methods Written in an accessible and engaging style Incorporates real-world examples and engaging cases Instructor Materials for System Forensics, Investigation, and Response include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts Instructor's Manual

[Copyright: e462a4da0d0eaf474d458e76f47fb355](https://www.jonesandbartlett.com/9781285428321/forensic-science-the-basics-fourth-edition)