As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.
covers the dormant and contentious issues of the subject in most scientific and objective manner. Various case studies addressing contemporary network forensics issues are also included in this book to provide practical know – how of the subject. Network Forensics: A privacy & Security provides a significant knowledge of network forensics in different functions and spheres of the security. The book gives the complete knowledge of network security, all kind of network attacks, intention of an attacker, identification of attack, detection, its analysis, incident response, ethical issues, botnet and botnet forensics. This book also refer the recent trends that comes under network forensics. It provides in-depth insight to the dormant and latent issues of the acquisition and system live investigation too. Features: Follows an outcome-based learning approach. A systematic overview of the state-of-the-art in network security, tools, Digital forensics. Differentiation among network security, computer forensics, network forensics and botnet forensics. Discussion on various cybercrimes, attacks and cyber terminologies. Discussion on network forensics process model. Network forensics tools and different techniques Network Forensics analysis through case studies. Discussion on evidence handling and incident response. System Investigations and the ethical issues on network forensics. This book serves as a reference book for post graduate and research investigators who need to study in cyber forensics. It can also be used as a textbook for a graduate level course in Electronics & Communication, Computer Science and Computer Engineering.

Security, Privacy, and Digital Forensics in the Cloud

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.

Computer Forensics Practical Guide
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 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 provide 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*

**Cybercrime and Digital Forensics**

This book covers the full life cycle of conducting a mobile and computer digital forensic examination, including planning and performing an investigation as well as report writing and testifying. Case reviews in corporate, civil, and criminal situations are also described from both prosecution and defense perspectives. Digital Forensics Explained, Second Edition draws from years of experience in local, state, federal, and international environments and highlights the challenges inherent in deficient cyber security practices. Topics include the importance of following the scientific method and verification, legal and ethical issues, planning an investigation (including tools and techniques), incident response, case project management and authorization, social media and internet, cloud, anti-forensics, link and visual analysis, and psychological considerations. The book is a valuable resource for the academic environment, law enforcement, those in the legal profession, and those working in the cyber security field. Case reviews include cyber security breaches, anti-forensic challenges, child exploitation, and social media investigations. Greg Gogolin, PhD, CISSP, is a Professor of Information Security and Intelligence at Ferris State University and a licensed Professional Investigator. He has worked more than 100 cases in criminal, civil, and corporate environments.

**Cybercrime and Digital Forensics**

The vast majority of modern criminal investigations involve some element of digital evidence, from mobile phones, computers, CCTV and other devices. Digital Forensics: Digital Evidence in Criminal Investigations provides the reader with a better understanding of how digital evidence complements “traditional” scientific evidence and examines how it can be used more effectively and efficiently in a range of investigations. Taking a new approach to the topic, this book presents digital evidence as an adjunct to other types of evidence and discusses how it can be deployed effectively in support of investigations. The book provides investigators/SSMs/other managers with sufficient contextual and technical information to be able to make more effective use of digital evidence sources in support of a range of investigations. In particular, it considers the roles played by digital devices in society and hence in criminal activities. From this, it examines the role and nature of evidential data which may be recoverable from a range of devices, considering issues relating to reliability and usefulness of those data. Includes worked case examples, test questions and review quizzes to enhance student understanding Solutions provided in an accompanying website Includes numerous case studies throughout to highlight
how digital evidence is handled at the crime scene and what can happen when procedures are carried out incorrectly Considers digital evidence in a broader context alongside other scientific evidence Discusses the role of digital devices in criminal activities and provides methods for the evaluation and prioritizing of evidence sources Includes discussion of the issues surrounding modern digital evidence examinations, for example; volume of material and its complexity Clear overview of all types of digital evidence Digital Forensics: Digital Evidence in Criminal Investigations is an invaluable text for undergraduate students taking either general forensic science courses where digital forensics may be a module or a dedicated computer/digital forensics degree course. The book is also a useful overview of the subject for postgraduate students and forensic practitioners.

**Computer Forensics JumpStart**

The need for computer investigations began with the passing of the Computer Crime Act of 1984. In the beginning, digital forensic applications were limited since few criminal cases required digital media to be analyzed and evidence was located without the need of recovery tools. Presently, computer/digital forensics have evolved into a scientific discipline encompassing many different types of analysis including but not limited to intrusion detection, triage, static, live, mobile, or network. The first generation computer forensic tools were based on convenient access and review of data in a safe manner (Ayers, 2009). Traditional two step method of creating a forensic image of a storage medium and analyzing the contents of the copy became the accepted standard for computer forensic evidence since it could maintain admissibility in court. Technological advancements such as encryption, virtual machines, virtualization, and cloud computing have hindered computer forensics since acquisition and validation of data cannot always be completed. There are challenges facing computer forensics along with many research and tool developments attempting to reduce the growing gap between the advancements in technology and forensic tools necessary for investigation. A proactive approach of forensic readiness and changes in the scientific and corporate environments are necessary for admissible digital evidence in criminal or civil proceedings. Keywords: Economic Crime Management, Suzanne Lynch M.S., non-queticent, anti-forensics, semantic gap, introspection, and integrity.

**A Practical Guide to Computer Forensics Investigations**

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
corporate security professionals, incident response team members, IT military and intelligence
services officers, system administrators, e-business security professionals, and banking and
insurance professionals

Hacking Exposed Computer Forensics, Second Edition

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,

Digital Forensics and Cyber Crime

This book constitutes the refereed proceedings of the 7th International Conference on Digital
Forensics and Cyber Crime, ICDF2C 2015, held in Seoul, South Korea, in October 2015. The
14 papers and 3 abstracts were selected from 40 submissions and cover diverse topics ranging
from tactics of cyber crime investigations to digital forensic education, network forensics, and
international cooperation in digital investigations.

The Official CHFI Study Guide (Exam 312-49)

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving
crime. 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.

Digital Forensics, Investigation, and Response

Computer Forensics: Evidence Collection and Management examines cyber-crime, E-
commerce, and Internet activities that could be used to exploit the Internet, computers, and
electronic devices. The book focuses on the numerous vulnerabilities and threats that are
inherent on the Internet and networking environments and presents techniques and suggestions
for corporate security personnel, investigators, and forensic examiners to successfully identify,
retrieve, and protect valuable forensic evidence for litigation and prosecution. The book is
divided into two major parts for easy reference. The first part explores various crimes, laws, policies, forensic tools, and the information needed to understand the underlying concepts of computer forensic investigations. The second part presents information relating to crime scene investigations and management, disk and file structure, laboratory construction and functions, and legal testimony. Separate chapters focus on investigations involving computer systems, e-mail, and wireless devices. Presenting information patterned after technical, legal, and managerial classes held by computer forensic professionals from Cyber Crime Summits held at Kennesaw State University in 2005 and 2006, this book is an invaluable resource for those who want to be both efficient and effective when conducting an investigation.

**Computer Forensics: Investigation Procedures and Response (CHFI)**

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field. Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters. Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics. Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals, illustrations and case example images. Features real-world examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media. Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

**Technology Assessment of Computer Forensic Investigations**

Due to the continuing rise of criminal conduct with technology, computer forensics is a rapidly growing discipline and one of the fastest growing segments of IT. If you are considering a career in this hot field, Computer Forensics JumpStart is for you. The second edition of an in-depth introduction to computer forensics, this major update covers the latest tools and practices as well as available certifications that can help you to launch a new career. Written by a team of computer forensics experts, coverage includes: Conducting a computer forensics investigation, Examining the layout of a network, Finding hidden data, Capturing images, Identifying, collecting, and preserving computer evidence, Understanding encryption and examining encrypted files, Documenting your case, Evaluating common computer forensic tools, Presenting computer evidence in court as an expert witness.
The Electronic Evidence, Discovery and Forensic Laws

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives; computer hacking and malicious software; digital piracy and intellectual theft; economic crime and online fraud; pornography and online sex crime; cyber-bullying and cyber-stalking; cyber-terrorism and extremism; digital forensic investigation and its legal context around the world; the law enforcement response to cybercrime transnationally; cybercrime policy and legislation across the globe. The new edition features two new chapters, the first looking at the law enforcement response to cybercrime and the second offering an extended discussion of online child pornography and sexual exploitation. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. This new edition includes QR codes throughout to connect directly with relevant websites. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

Cyber Crime and Forensic Computing

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.

Cyber Crime

The emergence of the World Wide Web, smartphones, and Computer-Mediated
Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives, computer hacking and digital piracy, economic crime and online fraud, pornography and online sex crime, cyber-bullying and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation and the sociology of technology.

Network Forensics

Under the prevailing laws in the Pakistan this is the first book which delivers an introduction to the topic of Digital Forensics, covering theoretical, practical and legal aspects. The first part of the book focuses on the history of digital forensics as a discipline and discusses the mannerisms and requirements needed to become a forensic analyst. The middle portion of the book constitutes a general guide to a digital forensic investigation, mostly focusing on computers. It finishes with a discussion of the legal aspects of digital forensics as well as some other observations for managers or other interested parties. This book provides 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 discovery section of the book provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery and Interception Investigation. Digital evidence is type of evidence that is stored on or transmitted by computers which can play a major role in a wide range of crimes, including homicide, rape, abduction, child abuse, solicitation of minors, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, espionage, and terrorism. Nevertheless an aggregate number of criminals are using computers and computer networks, few investigators are familiar in the evidentiary, technical, and legal issues related to digital evidence. As a result, digital evidence is often overlooked, collected incorrectly, and analyzed ineffectively. The aim of this book is to educate students and professionals and personnel of investigation agencies in the law enforcement, forensic science, computer security, and legal communities about digital evidence and computer crime. This book offers a comprehensive and integrative introduction of e-discovery evidence of digital forensics. It is the first to connect the different literature on the various types of digital forensics, the investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals.

Digital Forensics

Launch Your Career in Computer Forensics—Quickly and Effectively Written by a team of computer forensics experts, Computer Forensics JumpStart provides all the core information you need to launch your career in this fast-growing field: Conducting a computer forensics
investigation Examining the layout of a network Finding hidden data Capturing images
Identifying, collecting, and preserving computer evidence Understanding encryption and
examining encrypted files Documenting your case Evaluating common computer forensic tools
Presenting computer evidence in court as an expert witness

**Computer Forensics: Investigating Network Intrusions and Cybercrime (CHFI)**

The Computer Forensic Series by EC-Council provides the knowledge and skills to identify,
track, and prosecute the cyber-criminal. The series is comprised of four books covering a broad
base of topics in Computer Hacking Forensic Investigation, designed to expose the reader to
the process of detecting attacks and collecting evidence in a forensically sound manner with the
intent to report crime and prevent future attacks. Learners are introduced to advanced
techniques in computer investigation and analysis with interest in generating potential legal
evidence. In full, this and the other three books provide preparation to identify evidence in
computer related crime and abuse cases as well as track the intrusive hacker’s path through a
client system. The series and accompanying labs help prepare the security student or
professional to profile an intruder’s footprint and gather all necessary information and evidence
to support prosecution in a court of law. Network Intrusions and Cybercrime includes a
discussion of tools used in investigations as well as information on investigating network traffic,
Web attacks, DoS attacks, corporate espionage and much more! Important Notice: Media
content referenced within the product description or the product text may not be available in the
ebook version.

**Cybercrime and Cloud Forensics: Applications for Investigation Processes**

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

**Computer Forensics JumpStart**

While cloud computing continues to transform developments in information technology services,
these advancements have contributed to a rise in cyber attacks; producing an urgent need to
extend the applications of investigation processes. Cybercrime and Cloud Forensics: Applications
for Investigation Processes presents a collection of research and case studies of
applications for investigation processes in cloud computing environments. This reference
source brings together the perspectives of cloud customers, security architects, and law enforcement agencies in the developing area of cloud forensics.

**Scene of the Cybercrime: Computer Forensics Handbook**

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

**Information Systems: Modeling, Development, and Integration**

Computer crimes call for forensics specialists---people who know to find and follow the evidence. System Forensics, Investigation, and Response examines the fundamentals of system forensics what forensics is, an overview of computer crime, the challenges of system forensics, and forensics methods. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation, including evidence collection, investigating information-hiding, recovering data, and more. The book closes with an exploration of incident and intrusion response, emerging technologies and future directions of the field, and additional system forensics resources. The Jones & Bartlett Learning Information Systems Security & Assurance Series delivers fundamental IT security principles packed with real world applications and examples for IT Security, Cybersecurity, Information Assurance, and Information Systems, Security programs. Authored by Certified Information Systems Security professionals (CISSPs), and reviewed by leading technical experts in the field, these books are current, forward-thinking resources that enable readers to solve the cybersecurity challenges of
Investigative Computer Forensics

Designed as an introduction and overview to the field, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition integrates theory and practice to present the policies, procedures, methodologies, and legal ramifications and implications of a cyber forensic investigation. The authors guide you step-by-step through the basics of investigation and introduce the tools and procedures required to legally seize and forensically evaluate a suspect machine. Updating and expanding information on concealment techniques, new technologies, hardware, software, and relevant new legislation, this second edition delineates the scope and goals of cyber forensics to reveal and track legal and illegal activity. Beginning with an introduction and definition of cyber forensics, chapters explain the rules of evidence and chain of custody in maintaining legally valid electronic evidence. They describe how to begin an investigation and employ investigative methodology, as well as establish standard operating procedures for the field and cyber forensic laboratory. The authors provide an in depth examination of the manipulation of technology to conceal illegal activities and the use of cyber forensics to uncover them. They discuss topics and issues such as conducting a cyber forensic investigation within both the local and federal legal framework, and evaluating the current data security and integrity exposure of multifunctional devices. Cyber Forensics includes details and tips on taking control of a suspect computer or PDA and its "operating" environment, mitigating potential exposures and risks to chain of custody, and establishing and following a flowchart for the seizure of electronic evidence. An extensive list of appendices include websites, organizations, pertinent legislation, further readings, best practice recommendations, more information on hardware and software, and a recap of the federal rules of civil procedure.

The Best Damn Cybercrime and Digital Forensics Book Period

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 and Forensic Investigations: Breakthroughs in Research and Practice

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a
key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years.

Encompasses all aspects of the field, including methodological, scientific, technical and legal matters Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals, illustrations and case example images Features real-word examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

Virtualization and Forensics

The Computer Forensic Series by EC-Council provides the knowledge and skills to identify, track, and prosecute the cyber-criminal. The series is comprised of four books covering a broad base of topics in Computer Hacking Forensic Investigation, designed to expose the reader to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Learners are introduced to advanced techniques in computer investigation and analysis with interest in generating potential legal evidence. In full, this and the other three books provide preparation to identify evidence in computer related crime and abuse cases as well as track the intrusive hacker’s path through a client system. The series and accompanying labs help prepare the security student or professional to profile an intruder’s footprint and gather all necessary information and evidence to support prosecution in a court of law. The first book in the Computer Forensics series is Investigation Procedures and Response. Coverage includes a basic understanding of the importance of computer forensics, how to set up a secure lab, the process for forensic investigation including first responder responsibilities, how to handle various incidents and information on the various reports used by computer forensic investigators. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Computer Incident Response and Forensics Team Management

This Computer Forensic Guide is meant for IT professional who wants to enter into Computer Forensic domain.

Guide to Computer Forensics and Investigations

Computer Incident Response and Forensics Team Management provides security professionals with a complete handbook of computer incident response from the perspective of forensics team management. This unique approach teaches readers the concepts and principles they need to conduct a successful incident response investigation, ensuring that proven policies and
procedures are established and followed by all team members. Leighton R. Johnson III describes the processes within an incident response event and shows the crucial importance of skillful forensics team management, including when and where the transition to forensics investigation should occur during an incident response event. The book also provides discussions of key incident response components. Provides readers with a complete handbook on computer incident response from the perspective of forensics team management. Identify the key steps to completing a successful computer incident response investigation. Defines the qualities necessary to become a successful forensics investigation team member, as well as the interpersonal relationship skills necessary for successful incident response and forensics investigation teams.

Computer Forensics

Investigating Corporate Fraud Accounting Irregularities E-discovery Challenges Trade Secret Theft Social Networks Data Breaches The Cloud Hackers "Having worked with Erik on some of the most challenging computer forensic investigations during the early years of this industry’s formation as well as having competed with him earnestly in the marketplace I can truly say that Erik is one of the unique pioneers of computer forensic investigations. He not only can distill complex technical information into easily understandable concepts, but he always retained a long-term global perspective on the relevancy of our work and on the impact of the information revolution on the social and business structures of tomorrow." From the Foreword by James Gordon, Managing Director, Navigant Consulting, Inc. Get the knowledge you need to make informed decisions throughout the computer forensic investigation process. Investigative Computer Forensics zeroes in on a real need felt by lawyers, jurists, accountants, administrators, senior managers, and business executives around the globe: to understand the forensic investigation landscape before having an immediate and dire need for the services of a forensic investigator. Author Erik Laykin, leader and pioneer of computer forensic investigations, presents complex technical information in easily understandable concepts, covering: A primer on computers and networks Computer forensic fundamentals Investigative fundamentals Objectives and challenges in investigative computer forensics E-discovery responsibilities The future of computer forensic investigations Get the knowledge you need to make tough decisions during an internal investigation or while engaging the capabilities of a computer forensic professional with the proven guidance found in Investigative Computer Forensics.

Digital Forensics

Virtualization and Forensics: A Digital Forensic Investigators Guide to Virtual Environments offers an in-depth view into the world of virtualized environments and the implications they have on forensic investigations. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this guide gives you the end-to-end knowledge needed to identify server, desktop, and portable virtual environments, including: VMware, Parallels, Microsoft, and Sun. It covers technological advances in virtualization tools, methods, and issues in digital forensic investigations, and explores trends and emerging technologies surrounding virtualization technology. This book consists of three parts. Part I explains the process of virtualization and the different types of virtualized environments. Part II details how virtualization interacts with the basic forensic process, describing the methods used to find virtualization artifacts in dead and live environments as well as identifying the virtual activities that affect the examination process. Part III addresses advanced virtualization issues, such as the challenges of virtualized environments, cloud computing, and the future of virtualization. This book will be a valuable resource for forensic investigators (corporate and law enforcement) and incident response professionals.
Named a 2011 Best Digital Forensics Book by InfoSec Reviews Gives you the end-to-end knowledge needed to identify server, desktop, and portable virtual environments, including: VMware, Parallels, Microsoft, and Sun Covers technological advances in virtualization tools, methods, and issues in digital forensic investigations Explores trends and emerging technologies surrounding virtualization technology

Digital Forensics

This book provides a valuable reference for digital forensics practitioners and cyber security experts operating in various fields of law enforcement, incident response and commerce. It is also aimed at researchers seeking to obtain a more profound knowledge of Digital Forensics and Cybercrime. Furthermore, the book is an exceptional advanced text for PhD and Master degree programmes in Digital Forensics and Cyber Security. Each chapter of this book is written by an internationally-renowned expert who has extensive experience in law enforcement, industry and academia. The increasing popularity in the use of IoT devices for criminal activities means that there is a maturing discipline and industry around IoT forensics. As technology becomes cheaper and easier to deploy in an increased number of discrete, everyday objects, scope for the automated creation of personalised digital footprints becomes greater. Devices which are presently included within the Internet of Things (IoT) umbrella have a massive potential to enable and shape the way that humans interact and achieve objectives. These also forge a trail of data that can be used to triangulate and identify individuals and their actions. As such, interest and developments in autonomous vehicles, unmanned drones and 'smart' home appliances are creating unprecedented opportunities for the research communities to investigate the production and evaluation of evidence through the discipline of digital forensics.

Learn Computer Forensics

Security Smarts for the Self-Guided IT Professional Find out how to excel in the field of computer forensics investigations. Learn what it takes to transition from an IT professional to a computer forensic examiner in the private sector. Written by a Certified Information Systems Security Professional, Computer Forensics: InfoSec Pro Guide is filled with real-world case studies that demonstrate the concepts covered in the book. You'll learn how to set up a forensics lab, select hardware and software, choose forensic imaging procedures, test your tools, capture evidence from different sources, follow a sound investigative process, safely store evidence, and verify your findings. Best practices for documenting your results, preparing reports, and presenting evidence in court are also covered in this detailed resource. Computer Forensics: InfoSec Pro Guide features: Lingo—Common security terms defined so that you're in the know on the job IMHO—Frank and relevant opinions based on the author's years of industry experience Budget Note—Tips for getting security technologies and processes into your organization's budget In Actual Practice—Exceptions to the rules of security explained in real-world contexts Your Plan—Customizable checklists you can use on the job now Into Action—Tips on how, why, and when to apply new skills and techniques at work

Introductory Computer Forensics

"Cybercrime and cyber-terrorism represent a serious challenge to society as a whole." - Hans Christian Krüger, Deputy Secretary General of the Council of Europe Crime has been with us as long as laws have existed, and modern technology has given us a new type of criminal activity: cybercrime. Computer and network related crime is a problem that spans the globe, and unites
those in two disparate fields: law enforcement and information technology. This book will help both IT pros and law enforcement specialists understand both their own roles and those of the other, and show why that understanding and an organized, cooperative effort is necessary to win the fight against this new type of crime. 62% of US companies reported computer-related security breaches resulting in damages of $124 million dollars. This data is an indication of the massive need for Cybercrime training within the IT and law enforcement communities. The only book that covers Cybercrime from forensic investigation through prosecution. Cybercrime is one of the battlefields in the war against terror.

Cyber Forensics

Cyber Crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, Cyber Crime has assumed rather sinister implications. Cyber Crime poses great challenges for law enforcement and for society in general. To understand why this is true, it is necessary to understand why, and how, cybercrime differs from traditional, terrestrial crime. Net-crime refers to criminal use of the Internet. Cyber-crimes are essentially a combination of these two elements and can be best defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the Internet (Chat rooms, e-mails, notice boards and groups) and mobile phones (SMS/MMS)". Since Cyber Crime is a newly specialized field, growing in cyber laws, there is absolutely no comprehensive law on Cyber Crime anywhere in the world. This is precisely the reason why investigating agencies are finding cyberspace to be an extremely difficult terrain to handle. This book explores technical, legal, and social issues related to Cyber Crime. Cyber Crime is a broad term that includes offences where a computer may be the target, crimes where a computer may be a tool used in the commission of an existing offence, and crimes where a computer may play a subsidiary role such as offering evidence for the commission of an offence.

System Forensics, Investigation, and Response

UNISCON 2009 (United Information Systems Conference) was the third conference in the series that is based on the idea to pool smaller but highly interesting scientific events on information systems into one large conference. Here, people from different scientific backgrounds can present their research results, share their ideas and discuss future trends in these various areas. UNISCON 2009 was held in Sydney, Australia in the University of Western Sydney, Campbelltown Campus. In 2009 the following scientific events were held under the umbrella of UNISCON 2009: 8th International Conference on Information Systems Technology and Its Applications (ISTA 2009) 8th International Workshop on Conceptual Modelling Approaches for e-Business (eCOMO 2009) – Second Workshop on Model-Based Software and Data Integration (MBSDI 2009) We received 115 papers for the three events. Papers were submitted from over 25 countries. After a rigorous review process, 39 papers were accepted as full papers and 14 papers as short papers for presentation at the conference and published in these proceedings. In addition to the above three events, we also organized a Doctoral Consortium to provide a forum for doctoral students to get feedback from experts in the area about their research projects.

Computer Forensics InfoSec Pro Guide
In a unique and systematic way, this book discusses the security and privacy aspects of the cloud, and the relevant cloud forensics. Cloud computing is an emerging yet revolutionary technology that has been changing the way people live and work. However, with the continuous growth of cloud computing and related services, security and privacy has become a critical issue. Written by some of the top experts in the field, this book specifically discusses security and privacy of the cloud, as well as the digital forensics of cloud data, applications, and services. The first half of the book enables readers to have a comprehensive understanding and background of cloud security, which will help them through the digital investigation guidance and recommendations found in the second half of the book. Part One of Security, Privacy and Digital Forensics in the Cloud covers cloud infrastructure security; confidentiality of data; access control in cloud IaaS; cloud security and privacy management; hacking and countermeasures; risk management and disaster recovery; auditing and compliance; and security as a service (SaaS). Part Two addresses cloud forensics – model, challenges, and approaches; cyberterrorism in the cloud; digital forensic process and model in the cloud; data acquisition; digital evidence management, presentation, and court preparation; analysis of digital evidence; and forensics as a service (FaaS). Thoroughly covers both security and privacy of cloud and digital forensics Contributions by top researchers from the U.S., the European and other countries, and professionals active in the field of information and network security, digital and computer forensics, and cloud and big data Of interest to those focused upon security and implementation, and incident management Logical, well-structured, and organized to facilitate comprehension Security, Privacy and Digital Forensics in the Cloud is an ideal book for advanced undergraduate and master's-level students in information systems, information technology, computer and network forensics, as well as computer science. It can also serve as a good reference book for security professionals, digital forensics practitioners and cloud service providers.

Big Data Analytics and Computing for Digital Forensic Investigations

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic,
firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

Digital Forensics Explained

"Provides the right mix of practical how-to knowledge in a straightforward, informative fashion that ties it all the complex pieces together with real-world case studies. Delivers the most valuable insight on the market. The authors cut to the chase of what people must understand to effectively perform computer forensic investigations." --Brian H. Karney, COO, AccessData Corporation The latest strategies for investigating cyber-crime Identify and investigate computer criminals of all stripes with help from this fully updated, real-world resource. Hacking Exposed Computer Forensics, Second Edition explains how to construct a high-tech forensic lab, collect prosecutable evidence, discover e-mail and system file clues, track wireless activity, and recover obscured documents. Learn how to re-create an attacker's footsteps, communicate with counsel, prepare court-ready reports, and work through legal and organizational challenges. Case studies straight from today's headlines cover IP theft, mortgage fraud, employee misconduct, securities fraud, embezzlement, organized crime, and consumer fraud cases. Effectively uncover, capture, and prepare evidence for investigation Store and process collected data in a highly secure digital forensic lab Restore deleted documents, partitions, user activities, and file systems Analyze evidence gathered from Windows, Linux, and Macintosh systems Use the latest Web and client-based e-mail tools to extract relevant artifacts Overcome the hacker's anti-forensic, encryption, and obscurity techniques Unlock clues stored in cell phones, PDAs, and Windows Mobile devices Prepare legal documents that will hold up to judicial and defense scrutiny

Copyright code : f4add99c7f0c6b451cdea5ccdc69a520