Computer Forensics Principles And Practices

Principles and Practice of Forensic Psychiatry, 2EdDigital Forensics Trial GraphicsDigital Forensics Processing and ProceduresComputer ForensicsIntelligence and Security InformaticsForensic PathologyThe Daughter of TimeDigital Evidence and Computer CrimeTrigonometry Formulae Practice WorkbookA Practical Guide to Forensic NursingLearn Computer ForensicsPrinciples of Bloodstain Pattern AnalysisIntroduction to Security and Network ForensicsCybercrime and Digital ForensicsComputer SecurityThe Basics of Digital ForensicsForensic Accounting and FinanceFundamentals of Digital ForensicsCriminal ProfilingEncyclopedia of Forensic SciencesTen Strategies of a World-Class Cybersecurity Operations CenterComputer Forensics and Cyber CrimePractical Windows ForensicsThe Principles of Our World - CompassionA Practical Guide to Computer Forensics InvestigationsCyber ForensicsPrinciples and Practice of Forensic PsychiatryCCFP Certified Cyber Forensics Professional All-in-One Exam GuideWildlife Forensic InvestigationPrinciples with PromiseDigital Forensic Evidence ExaminationDigital Forensics WorkbookDigital Forensics and InvestigationsInvestigative Computer ForensicsForensic Document ExaminationGuide to Computer Forensics and InvestigationsSituational Awareness in Computer Network Defense: Principles, Methods and ApplicationsDigital ForensicsPrinciples and Practice of CriminalisticsDigital Forensics and Incident Response

Principles and Practice of Forensic Psychiatry, 2Ed

This book constitutes the refereed proceedings of the three international workshops PAISI 2008, PACCF 2008, and SOCO 2008, held as satellite events of the IEEE International Conference on Intelligence and Security Informatics, ISI 2008, in Taipei, Taiwan, in June 2008. The 55 revised full papers presented were carefully reviewed and selected from the presentations at the workshops. The 21 papers of the Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2008) cover topics such as information retrieval and event detection, internet security and cybercrime, currency and data protection, cryptography, image and video analysis, privacy issues, social networks, modeling and visualization, and network intrusion detection. The Pacific Asia Workshop on Cybercrime and Computer Forensics (PACCF 2008) furnishes 10 papers about forensic information management, forensic technologies, and forensic principles and tools. The 24 papers of the Workshop on Social Computing (SOCO 2008) are organized in topical sections on social web and social information management, social networks and agent-based modeling, as well as social opinions, e-commerce, security and privacy considerations.

Digital Forensics Trial Graphics

Wildlife forensics is the application of forensic science to the conservation and protection of non-domesticated animals, both in the wild and in captivity. Providing an in-depth introduction to this rapidly evolving field, Wildlife Forensic Investigation: Principles and Practice also chronicles aspects of the history of management, conservation, and environmental protection, with an emphasis on their global importance in the twenty-first century. The book examines the crucial role of wildlife forensic investigation with regard to live animals, dead animals and samples and covers national, regional, and international legislation. While the text particularly focuses on forensic science as it relates to wild animals, it also includes mention of plants and habitats because of their relevance to conservation. The book discusses animal welfare as well as the damage that can be inflicted on humans and property by wildlife. Offering access to sound evidence based on good science and obtained using the best available practices, the book is enhanced by case studies from experts who describe some of their own work. This resource is essential for those involved in a range of endeavours, including investigating wildlife crime, identifying animal remains, ascertaining the circumstances of death of wild species, and other legal proceedings and activities concerning wildlife. The forensic skills described in this book can be applied to a wide range of activities (not necessarily involving the legal process), including environmental impact assessments, insurance claims, governmental and other enquiries, checking of trading standards and the inspection of (for instance) pet-shops, animal boarding establishments, and zoological collections. The authors point out that one of the most important requirements of those persons involved in wildlife forensic work is to retain an open mind. Such personnel should also be conscious of new developments and evolving techniques and be able to anticipate situations where their investigative and scientific skills might be used to advantage—so-called "horizon scanning". Examples of these are given.

Digital Forensics Processing and Procedures

This hands-on textbook provides an accessible introduction to the fundamentals of digital forensics. The text contains thorough coverage of the theoretical foundations, explaining what computer forensics is, what it can do, and also what it can’t. A particular focus is presented on establishing sound forensic thinking and methodology, supported by practical guidance on performing typical tasks and using common forensic tools. Emphasis is also placed on universal principles, as opposed to content unique to specific legislation in individual countries. Topics and features: introduces the fundamental concepts in digital forensics, and the steps involved in a forensic examination in a digital environment; discusses the nature of what cybercrime is, and how digital evidence can be of use during criminal investigations into such crimes; offers a practical overview of common practices for cracking encrypted data; reviews key artifacts that have proven to be important in several cases, highlighting where to find these and how to correctly interpret them;

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

Computer Forensics

A hospitalized English policeman reconstructs historical evidence concerning Richard III's role in the murder of Edward IV's two sons.

Intelligence and Security Informatics

This book introduces the reader to the basic principles of handwriting and the factors that affect their development. The book discusses the basic concept of the characteristics of writing that are compared when making an identification or elimination of a writer. In addition, readers will be able to recognize the signs of forgery and disguise and to distinguish between simulation and disguise.

Forensic Pathology

Digital forensics has been a discipline of Information Security for decades now. Its principles, methodologies, and techniques have remained consistent despite the evolution of technology, and, ultimately, it and can be applied to any form of digital data. However, within a corporate environment, digital forensic professionals are particularly challenged. They must maintain the legal admissibility and forensic viability of digital evidence in support of a broad range of different business functions that include incident response, electronic discovery (ediscovery), and ensuring the controls and accountability of such information across networks. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise provides the methodologies and strategies necessary for these key business functions to seamlessly integrate digital forensic capabilities to guarantee the admissibility and integrity of digital evidence. In many books, the focus on digital evidence is primarily in the technical, software, and investigative elements, of which there are numerous publications. What tends to get overlooked are the people and process elements within the organization. Taking a step back, the book outlines the importance of integrating and accounting for the people, process, and technology components of digital forensics. In essence, to establish a holistic paradigm—and best-practice procedure and policy approach—to defending the enterprise. This book serves as a roadmap for professionals to successfully integrate an organization's people, process, and technology with other key business functions in an enterprise's digital forensic capabilities.

The Daughter of Time

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-bulling 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.

Digital Evidence and Computer Crime

This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody--from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab A comprehensive guide for all roles in a digital forensics laboratory Based on international standards and certifications

Trigonometry Formulae Practice Workbook

Come learn about The Principles of Our World. In a series of real life stories, readers will be introduced to The Principle of Compassion. The stories are meant to remind all of us about the importance of compassion in our lives. Enjoy the book in one sitting or read just one story at a time. It is never too early in the development of a child to start talking about the importance of principles like honesty, courage, and compassion. This book is part of a series of books about The Principles of Our World that provide parents and teachers with the opportunity to read to young children (ages 4+) and talk about a variety of situations they will experience in life. For young, independent readers (ages 7+), The Principles of Our World book series is a great addition to their book collection. At the end of the book, there is a section called, "Where Do We Go From Here?" This section is designed for children, parents, and educators to discuss situations they will encounter in life and talk about how The Principles of Our World can help them effectively handle these situations. The Principles of Our World are here to help.

A Practical Guide to Forensic Nursing

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.

Learn Computer Forensics

Forensic Pathology is a comprehensive reference that uses a case-oriented format to address, explain and guide the reader through the varied topics encountered by forensic pathologists. Developed in response to a severe void in the literature, the book addresses topics ranging from medicolegal investigation of death to death scene investigation, forensic autopsy, and artifacts of resuscitation as well as complications of medical therapy, forensic osteology, forensic odontology, forensic photography, and death certification. The book includes various types of cases, including sudden natural death, asphyxia, motor vehicle collisions, death in custody, child abuse and elder abuse, acute psychiatric and emotional deaths, and pregnancy. It contains sample descriptions of pathological lesions which serve to aid pathologists in reporting their findings to law enforcement agencies, attorneys, and others involved in investigations of sudden death. The concepts outlined in the text are beautifully illustrated by large, colorful photographs. There are also "Do and Don’t" sections at the end of each chapter that provide guidance for handling the types of cases examined. This work will benefit not only experienced forensic pathologists, but also hospital pathologists who occasionally performs medicolegal autopsies; doctors in training; medical examiners; law enforcement personnel; crime scene investigators; attorneys; and fellows and students of the medical sciences. Large, colorful photographs which beautifully illustrate the concepts outlined in the text. Sample descriptions of pathological lesions which serve to aid pathologists in reporting their findings to law enforcement agencies, attorneys, and others involved in investigations of sudden death. 'Do and Don't' sections at the end of each chapter which provide guidance for handling the types of cases examined within preceding sections.

Principles of Bloodstain Pattern Analysis

A complete guide to Forensic Accounting and Finance, this book is ideal for advanced-level students and new or mid-level forensic accounting professionals looking to boost their specialist knowledge as part of their CPD, for accountants who wish to build more knowledge in this skills area or advanced undergraduates who feel ready to stretch themselves. Demand for expertise in this field is growing, and Forensic Accounting and Finance offers a complete, accessible and affordable guide, combining coverage of principle theory with the real and practical needs of the professional. Written by a strong academic and practitioner author team and in association with the Network for Independent Forensic Accountants, this book covers all forensic accounting topics from forensics as an extension of auditing and the basic principles of forensic accounting, to financial analysis and modelling, financial reporting, financial crime, and IT systems. Forensic Accounting and Finance shares current examples and case studies, highlighting cultural differences for key topics with updated regional legislation information available online for those looking for a truly global approach which is always up to date.

Introduction to Security and Network Forensics

Principles with Promise: Old Testament & New Testament is the second in a succession of principle-based topical guides planned for release within the next two years. This publication of Principles with Promise catalogues the doctrines, values, and teachings found in the Bible and their associated references regardless of how they are interpreted and practiced by the various Christian denominations.

Cybercrime and Digital Forensics

"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 marketplaceI 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.

Computer Security

* Aim of this 'formulae practice workbook: To help the students to remember, recollect and apply the various formulae in the appropriate place while solving the problems. * Already tested in India among average and below average higher secondary students (11th & 12th std) with very good results. * Theory is not discussed here in detail. * More number of solved problems and problems for practice with solutions. * A self evaluation test with answers. * Practice! Practice! This practice helps you - to discard your pre-conceived ideas of Trigonometry. You can be friendly (familiar) with the 'truck load of formulae' which is frightening you so far. - to solve the problems given in the text book and assignment sheets easily and independently. - to understand the theory given in your text book without any fear. You can do it! No doubt!! * The thorough knowledge acquired here will be more useful not only in Differential Calculus but also in Integral Calculus, Differential Equations etc. * This workbook is available at Amazon.com Wish you all the best! Prof. M. Subbiah Doss

The Basics of Digital Forensics

Given our increasing dependency on computing technology in daily business processes, and the growing opportunity to use engineering technologies to engage in illegal, unauthorized, and unethical acts aimed at corporate infrastructure, every organization is at risk. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence o

Forensic Accounting and Finance

Get complete coverage of all six CCFP exam domains developed by the International Information Systems Security Certification Consortium (ISC)2. Written by a leading computer security expert, this authoritative guide fully addresses cyber forensics techniques, standards, technologies, and legal and ethical principles. You'll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. COVERS ALL SIX EXAM DOMAINS: Legal and ethical principles Investigations Forensic science Digital forensics Application forensics Hybrid and emerging technologies ELECTRONIC CONTENT INCLUDES: 250 practice exam questions Test engine that provides full-length practice exams and customized quizzes by chapter or by exam domain

Fundamentals of Digital Forensics

Keeping up with the latest developments in cyber security requires ongoing commitment, but without a firm foundation in the principles of computer security and digital forensics, those tasked with safeguarding private information can get lost in a turbulent and shifting sea. Providing such a foundation, Introduction to

Security and Network Forensics covers the basic principles of intrusion detection systems, encryption, and authentication, as well as the key academic principles related to digital forensics. Starting with an overview of general security concepts, it addresses hashing, digital certificates, enhanced software security, and network security. The text introduces the concepts of risk, threat analysis, and network forensics, and includes online access to an abundance of ancillary materials, including labs, Cisco challenges, test questions, and web-based videos. The author provides readers with access to a complete set of simulators for routers, switches, wireless access points (Cisco Aironet 1200), PIX/ASA firewalls (Version 6.x, 7.x and 8.x), Wireless LAN Controllers (WLC), Wireless ADUs, ASDMs, SDMs, Juniper, and much more, including: More than 3,700 unique Cisco challenges and 48,000 Cisco Configuration Challenge Elements 60,000 test questions, including for Certified Ethical Hacking and CISSP® 350 router labs, 180 switch labs, 160 PIX/ASA labs, and 80 Wireless labs Rounding out coverage with a look into more advanced topics, including data hiding, obfuscation, web infrastructures, and cloud and grid computing, this book provides the fundamental understanding in computer security and digital forensics required to develop and implement effective safeguards against ever-evolving cyber security threats. Along with this, the text includes a range of online lectures and related material, available at: http://asecuritybook.com.

Criminal Profiling

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

Encyclopedia of Forensic Sciences

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.

Ten Strategies of a World-Class Cybersecurity Operations Center

Bloodstain evidence has become a deciding factor in the outcome of many of the world's most notorious criminal cases. As a result, substantiation of this evidence is crucial to those on either side of the courtroom aisle. The challenge is to obtain an authoritative reference that provides the latest information in a comprehensive and effective manner. Principles of Bloodstain Pattern Analysis: Theory and Practice presents an in-depth investigation of this important subject matter. A multidisciplinary approach is presented throughout the book that uses scene and laboratory examinations in conjunction with forensic pathology, forensic serology, and chemical enhancement techniques. Emphasis is on a thought process based on taxonomic classification of bloodstains that takes into account their physical characteristics of size, shape, and distribution, and the specific mechanisms that produce them. Individual chapters analyze case studies, with two chapters specifically discussing the details of legal issues as they pertain to bloodstain pattern analysis. Information highlighted throughout the book includes an examination of bloodstained clothing and footwear and information on bloodstain interpretation for crime scene reconstruction. Dramatic color images of bloodletting injuries, bloodstains, and crime scenes are also presented to compliment the technical content of this resource. Features § Provides 500 full color photographs - the first bloodstain pattern book presenting dramatic full color images of bloodletting injuries, bloodstains, and crime scenes § Contains appendices with scientific data that includes trigonometric tables and metric equivalents, as well as crime scene and laboratory check lists, and biohazard safety precautions § Discloses court decisions relating to bloodstain pattern analysis and presumptive blood testing § Written by authors with many years of experience in the field, and features chapters contributed by qualified and respected forensic scientists and attorneys

Computer Forensics and Cyber Crime

"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.

Practical Windows Forensics

"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 Principles of Our World - Compassion

The second edition of this award-winning textbook has been thoroughly revised and updated throughout. Building on the success of the first edition, the book continues to address the History and Practice of Forensic Psychiatry, Legal Regulation of the Practice of Psychiatry, Psychiatry in relation to Civil Law, Criminal Law, and Family Law. Important sections such as Special Issues in Forensic Psychiatry, Law and the Legal System, and Landmark Cases in Mental Health Law are included. Designed to meet the needs of practitioners of forensic psychiatry, for residents in forensic psychiatry, and those preparing for the specialty examination in Forensic Psychiatry of the American Board of Psychiatry and Neurology, this volume will also answer the many questions faced by mental health professionals, mental health administrators, correctional health professionals and correctional health administrators, attorneys, judges, probation and parole officers and administrators all of whom, at one time or another, require a substantive presentation of the entire field of forensic psychiatry in the USA.

A Practical Guide to Computer Forensics Investigations

Digital Forensic Evidence Examination focuses on the scientific basis for analysis, interpretation, attribution, and reconstruction of digital forensic evidence in a legal context. It defines the bounds of "Information Physics" as it affects digital forensics, describes a model of the overall processes associated with the use of such evidence in legal matters, and provides the detailed basis for the science of digital forensic evidence examination. It reviews and discusses digital forensic evidence analysis, interpretation, attribution, and reconstruction and their scientific bases, discusses tools and methodologies and their limits, and reviews the state of the science and its future outlook.

Cyber Forensics

Forensic science includes all aspects of investigating a crime, including: chemistry, biology and physics, and also incorporates countless other specialties. Today, the service offered under the guise of "forensic science’ includes specialties from virtually all aspects of modern science, medicine, engineering, mathematics and technology. The Encyclopedia of Forensic Sciences, Second Edition is a reference source that will inform both the crime scene worker and the laboratory worker of each other’s protocols, procedures and limitations. Written by leading scientists in each area, every article is peer reviewed to establish clarity, accuracy, and comprehensiveness. As reflected in the specialties of its Editorial Board, the contents covers the core theories, methods and techniques employed by forensic scientists – and applications of these that are used in forensic analysis. This 4-volume set represents a 30% growth in articles from the first edition, with a particular increase in coverage of DNA and digital forensics Includes an international collection of contributors The second edition features a new 21-member editorial board, half of which are internationally based Includes over 300 articles, approximately 10pp on average Each article features a) suggested readings which point readers to additional sources for more information, b) a list of related Web sites, c) a 5-10 word glossary and definition paragraph, and d) cross-references to related articles in the encyclopedia Available online via SciVerse ScienceDirect. Please visit www.info.sciencedirect.com for more information This new edition continues the reputation of the first edition, which was awarded an Honorable Mention in the prestigious Dartmouth Medal competition for 2001. This award honors the creation of reference works of outstanding quality and significance, and is sponsored by the RUSA Committee of the American Library Association

Principles and Practice of Forensic Psychiatry

The third edition of this award-winning textbook has been revised and thoroughly updated. Building on the success of the previous editions, it continues to address the history and practice of forensic psychiatry, legal regulation of the practice of psychiatry, forensic evaluation and treatment, psychiatry in relation to civil law, criminal law and family law, as well as correctional forensic psychiatry. New chapters address changes in the assessment and treatment of aggression and violence as well as psychological and neuroimaging assessments.

CCFP Certified Cyber Forensics Professional All-in-One Exam Guide

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

Wildlife Forensic Investigation

Victims of violence are unfortunately ever-present in healthcare today. Regardless of the setting, nurses are often the first to interact with victims and regularly must step into uncomfortable or difficult situations. To ensure patient and provider safety and enable the best possible outcomes, every nurse should be well-versed in forensic and theoretical issues of violence. A Practical Guide to Forensic Nursing is an evidence-based guide to understanding and applying forensic nursing science. Authors Angela F. Amar and L. Kathleen Sekula introduce practical and theoretical perspectives on violence and provide valuable resources, including injury assessment and violence prevention strategies as well as an overview of relevant legal, ethical, societal, and policy issues. Whether you are a student, new nurse, or experienced clinician, you will find the right tools and strategies to broaden your understanding of violence and help you integrate forensic science into your patient care.

Principles with Promise

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.

Digital Forensic Evidence Examination

Expanding on ideas proposed by leading thinkers throughout the history of forensic science, Principles and Practice of Criminalistics: The Profession of Forensic Science outlines a logical framework for the examination of physical evidence in a criminalistics laboratory. The book reexamines prevailing criminalistics concepts in light of both technical and intellectual advances and provides a way of conceptualizing physical evidence from its origin through its interpretation. Conceptually, the book explains what forensic scientists do and discusses the philosophical and practical considerations that affect the conduct of their work. To be sure, some of the ideas challenge conventional wisdom on the subject, and as such, are bound to provoke discussion among members of the forensic community. Against this background, Principles and Practice of Criminalistics: The Profession of Forensic Science is a tremendously valuable reference for professionals involved in forensic science and other related fields.

Digital Forensics Workbook

Computer Security: Principles and Practice, 2e, is ideal for courses in Computer/Network Security. In recent years, the need for education in computer security and related topics has grown dramatically – and is essential for anyone studying Computer Science or Computer Engineering. This is the only text available to provide integrated, comprehensive, up-to-date coverage of the broad range of topics in this subject. In addition to an extensive pedagogical program, the book provides unparalleled support for both research and modeling projects, giving students a broader perspective. The Text and Academic Authors Association named Computer Security: Principles and Practice, 1e, the winner of the Textbook Excellence Award for the best Computer Science textbook of 2008.

Digital Forensics and Investigations

The Digital Forensics Workbook is a filled with over 60 hands-on activities using over 40 different tools for digital forensic examiners who want to gain practice acquiring and analyzing digital data. Topics include analysis of media, network traffic, memory, and mobile apps. By becoming proficient in these activities, examiners can then focus on the recovered data and conduct in-depth analyses. This workbook was designed to augment existing digital forensics learning, whether it be formalized academic courses, industry training classes, on-the-job learning, or independent studying. The hands-on activities include step-by-step procedures for the reader so they obtain the identical results presented in the workbook. Activities include over 150 questions and answers to reinforce content. Additional exercises with answers are also provided so readers can apply what they have learned.

Investigative Computer Forensics

Digital Forensics Trial Graphics: Teaching the Jury Through Effective Use of Visuals helps digital forensic practitioners explain complex technical material to laypeople (i.e., juries, judges, etc.). The book includes professional quality illustrations of technology that help anyone understand the complex concepts behind the science.

Users will find invaluable information on theory and best practices along with guidance on how to design and deliver successful explanations. Helps users learn skills for the effective presentation of digital forensic evidence via graphics in a trial setting to laypeople such as juries and judges Presents the principles of visual learning and graphic design as a foundation for developing effective visuals Demonstrates the best practices of slide design to develop effective visuals for presentation of evidence Professionally developed graphics, designed specifically for digital forensics, that you can use at trial Downloadable graphics available at: http://booksite.elsevier.com/9780128034835

Forensic Document Examination

Criminal Profiling: Principles and Practice provides a compendium of original scientific research on constructing a criminal profile for crimes that are not readily resolvable by conventional police investigative methods. Leading profiling expert Richard N. Kocsis, PhD, utilizes a distinct approach referred to as Crime Action Profiling (CAP), a technique that has its foundations in the disciplinary knowledge of forensic psychology. The initial four chapters examine the skills, accuracy, components, and processes surrounding the construction of a criminal profile. The next two chapters focus on CAP research, the methods developed for the profiling of violent crimes and describing a systematic method for the interpretation and use of the CAP models. The subsequent three chapters canvass the respective CAP studies undertaken for crimes of serial rape, serial/sexual murder, and serial arson. An explanation for how each of the models is developed is also given. The final chapters of the book are devoted to the geographical analysis of crime patterns and to a discussion of the format conventions and procedural guidelines for developing a criminal profile. Offering a scientifically grounded method for the construction of a criminal profile, Criminal Profiling: Principles and Practice provides law enforcement personnel, forensic psychologists and psychiatrists, criminologists, and forensic investigators with a step-by-step, practical guide for understanding and applying CAP techniques for the construction of a criminal profile in a systematic and replicable manner.

Guide to Computer Forensics and Investigations

Master the techniques for gathering electronic evidence and explore the new frontier of crime investigation. The demand for computer forensics experts greatly exceeds the supply. With the rapid growth of technology in all parts of our lives, criminal activity must be tracked down and investigated using electronic methods that require up-to-date techniques and knowledge of the latest software tools. Authors Linda Volonino, Jana Godwin, and Reynaldo Anzaldua share their expertise to give you the legal, technical, and investigative skills you need to launch your career in computer forensics. You can also use Computer Forensics: Principles and Practices to help you advance in careers such as criminal justice, accounting, law enforcement, and federal investigation. Computer Forensics Principles and Practices gives you in-depth understanding of: Using the correct investigative tools and procedures to maximize effectiveness of evidence gathering. Keeping evidence in pristine condition so it will be admissible in a legal action. . Investigating large-scale attacks such as identity theft, fraud, phishing, extortion, and malware infections. The legal foundations for proper handling of traditional and electronic evidence such as the Federal Rules of Evidence and Procedure as well as the Fourth Amendment and other laws regarding search warrants and civil rights. Practical tools such as FTK, EnCase, Passware, Ethereal, LADS, WinHex, GIMP, Camouflage, and Snort. This book is filled with tools to help you move beyond simply learning concepts and help you apply them. These tools include: . In Practice tutorials: Apply concepts and learn by doing. . Exercises and Projects: Assignments show you how to employ your new skills. Case Studies: Apply what you learn in real-world scenarios. The companion Web site (www.prenhall.com/security) includes: . Additional testing materials and projects to reinforce book lessons. . Downloadable checklists and templates used in the book. . Links to additional topics and resources to assist you in your professional development. "

Situational Awareness in Computer Network Defense: Principles, Methods and Applications

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Digital Forensics

The leading introduction to computer crime and forensicsis now fully updated to reflect today's newest attacks, laws, and investigatory best practices. Packed with new case studies, examples, and statistics, Computer Forensics and Cyber Crime, Third Edition adds up-to-the-minute coverage of smartphones, cloud computing, GPS, Mac OS X, Linux, Stuxnet, cyberbullying, cyberterrorism, search and seizure, online gambling, and much more. Covers all forms of modern and traditional computer crime, defines all relevant terms, and explains all technical and legal concepts in plain English, so students can succeed even if they have no technical, legal, or investigatory background.

Principles and Practice of Criminalistics

A Practical Guide to Computer Forensics Investigations introduces the newest technologies along with detailed information on how the evidence contained on these devices should be analyzed. Packed with practical, hands-on activities, students will learn unique subjects from chapters including Mac Forensics, Mobile Forensics, Cyberbullying, and Child Endangerment. This well-developed book will prepare students for the rapidly-growing field of computer forensics for a career with law enforcement, accounting firms, banks and credit card companies, private investigation companies, or government agencies.

Digital Forensics and Incident Response

A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.