Computer Forensics: Cybercriminals, Laws, and Evidence

The Cybersecurity Body of Knowledge explains the content, purpose, and use of eight knowledge areas that define the boundaries of the discipline of cybersecurity. The discussion focuses on, and is driven by, the essential concepts of each knowledge area that collectively capture the cybersecurity body of knowledge to provide a complete picture of the field. This book is based on a brand-new and up-to this point unique, global initiative, known as CSECO217, which was created and endorsed by ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. This has practical relevance to every educator in the discipline of cybersecurity. Because the specifics of this body of knowledge cannot be imparted in a single text, the authors provide the necessary comprehensive overview. In essence, this is the entry-level survey of the comprehensive field of cybersecurity. It will serve as the roadmap for individuals to later drill down into a specific area of interest. This presentation is also explicitly designed to aid faculty members, administrators, CISOs, policy makers, and stakeholders involved with cybersecurity workforce development initiatives. The book is oriented toward practical application of a computing-based foundation, crosscutting concepts, and essential knowledge and skills of the cybersecurity discipline to meet workforce demands. Dan Shoemaker, PhD, is full professor, senior research scientist, and program director at the University of Detroit Mercy’s Center for Cyber Security and Intelligence Studies. Dan is a former chair of the Cybersecurity & Information Systems Department and has authored numerous books and journal articles focused on cybersecurity. A.5 Kohnke, PhD, is an associate professor of cybersecurity and the principal investigator of the Center for Academic Excellence in Cyber Defence at the University of Detroit Mercy. A.5’s research is focused in cybersecurity, risk management, threat modeling, and mitigating attack vectors. K. E. Sigler, MS, is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills campus of Oakland Community College in Michigan. Ken’s research is in the areas of software management, software assurance, and cybersecurity.

The Cybersecurity Body of Knowledge

The emergence of the World Wide Web, smartphones, and Computer-M ediated 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 student exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation and the sociology of technology.

Transnational Security

Digital Forensics: Threatscape and Best Practices surveys the problems and challenges confronting digital forensic professionals today, including massive data sets and everchanging technology. This book provides a coherent overview of the threatscape in a broad range of topics, providing practitioners and students alike with a comprehensive, coherent overview of the threat landscape and what can be done to manage and prepare for it. Digital Forensics: Threatscape and Best Practices delivers you with incisive analysis and best practices from a panel of expert authors, led by John Sammons, bestselling author of The Basics of Digital Forensics. Learn the basics of cryptocurrencies (like Bitcoin) and the artifacts they generate. Learn why examination planning matters and how to do it effectively. Discover how to incorporate behavioral analysis into your digital forensic examinations. Stay updated with the key artifacts created by the latest Mac OS, Windows 10, and Android. El Capitan discusses the threatscapes and challenges facing mobile device forensics, law enforcement, and legal cases. The power of applying the electronic discovery workflows to digital forensics Discover the value of and impact of social media forensics.

Scene of the Cybercrime

This book contains a selection of thoroughly refereed and revised papers from the Second International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2010, held October 4-6, 2010 in Abu Dhabi, United Arab Emirates. The field of digital forensics is becoming increasingly important for law enforcement, network security, and information assurance. It is a multidisciplinary area that encompasses a number of fields, including law, computer science, finance, networking, data mining, and criminal justice. The 14 papers in this volume describe the various applications of this technology and cover a wide range of topics including law enforcement, disaster recovery, accounting fraud, network security, and information warfare.

Careers in Computer Forensics

The First International Conference on Digital Forensics and Cyber Crime (ICDF2C) was held in Albany from September 30 to October 2, 2009. The field of digital forensics is growing rapidly with implications for several fields including law enforcement, network security, disaster recovery and accounting. This is a multidisciplinary area that requires expertise in several areas including, law, computer science, finance, networking, data mining, and criminal justice. This conference brought together practitioners and researchers from diverse fields providing opportunities for business and intellectual engagement among attendees. All the conference sessions were very well attended with vigorous discussions and strong audience interest. The conference featured an excellent program comprising high-quality paper presentations and invited speakers from all around the world.
Access Free Computer Forensics Cybercriminals Laws And Evidence

auditing. This was followed by two parallel sessions on accounting fraud/financial crime, and multimedia and handheld forensics. The second day of the conference featured a

Digital Forensics and Cyber Crime

The leading introduction to computer crime and forensics now fully updated to reflect today’s newest attacks, laws, and investigatory best practices. Packed with new case

An Introduction to Crime Scene Investigation

The sixth edition of Security and Loss Prevention continues the tradition of providing introductory and advanced coverage of the body of knowledge of the security profession. To

Fighting Cybercrime

This book contains a selection of thoroughly refereed and revised papers from the Third International ICST Conference on Digital Forensics and Cyber Crime, ICFD2C 2011, held October 26-28 in Dublin, Ireland. The field of digital forensics is becoming increasingly important for law enforcement, network security, and information assurance. It is a multidisciplinary area that encompasses a number of fields, including law, computer science, finance, networking, data mining, and criminal justice. The 24 papers in this volume cover a variety of topics ranging from tactics of cyber crime investigations to digital forensic education, network forensics, and the use of formal methods in digital investigations. There is a large section addressing forensics of mobile digital devices.

Computer Forensics

"An Introduction to Crime Scene Investigation" serves to eliminate warped impressions influenced by the media, and clearly identifies and explains the crime scene investigative process, components, methods, and procedures.

Digital Forensics and Cyber Crime

Provides a key textbook on the nature of international and transnational crimes and the delivery of justice for crime control and prevention.

Security and Loss Prevention

Today’s society is highly networked. Internet is ubiquitous and world without it is just in-conceivable. As is rightly said that there are two sides of a coin, this blessing in form of

System Forensics, Investigation, and Response

"This textbook presents the forensic methods used to analyze physical evidence along with the scientific principles that are its underpinnings. It is designed for students without a background in science, however students will learn the core principles behind the forensic method which will lead them to be better forensic professionals"--

Digital Forensics and Cyber Crime

"Cybercrime and cyber-terrorism represent a serious challenge to society as a whole." - Hans Christian K. Krüger, Deputy Secretary General of the Council of Europe Crime has

Digital Forensics and Cyber Crime Triage, digital forensics tools testing and validation, hacking.

Cybercrime and Digital Forensics

This book constitutes the refereed proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICFD2C 2017, held in Prague, Czech Republic, in October 2017. The 18 full papers were selected from 50 submissions and are grouped in topical sections on malware and botnet, deanonimization, digital forensics tools, cybercrime investigation and digital forensics triage, digital forensics tools testing and validation, hacking.
Digital Forensics and Cyber Crime

Criminal Investigations & Forensic Science

Digital Forensics

This book constitutes the refereed proceedings of the 11th International Conference on Digital Forensics and Cyber Crime, ICDFFZC 2020, held in Boston, MA, in October 2020. Due to COVID-19 pandemic the conference was held virtually. The 11 reviewed full papers and 4 short papers were selected from 35 submissions and are grouped in topical sections on digital forensics; cyber-physical system Forensics; event reconstruction in digital forensics; emerging topics in forensics; cybersecurity and digital forensics.

Criminalistics

This book lays out the foundation of a privacy doctrine suitable to the cyber age. It limits the volume, sensitivity, and secondary analysis that can be carried out. In studying these matters, the book examines the privacy issues raised by the NSA, publication of state secrets, and DNA usage.

Digital Forensics and Cyber Crime

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

Handbook on Cyber Crime and Law in India Compiled by Falgun Rathod

Cybercrime has become increasingly prevalent in the new millennium as computer-savvy criminals have developed more sophisticated ways to victimize people online and through other digital means. The Law of Cybercrimes and Their Investigations is a comprehensive text exploring the gamut of issues surrounding this growing phenomenon. After an introduction to the history of computer crime, the book reviews a host of topics including: information warfare and cyberterrorism; obscenity, child pornography, sexual predator conduct, and online gambling; cyberstalking; cyberharassment, cyberbullying, and other types of unlawful expression; auction fraud, Ponzi and pyramid schemes, access device fraud, identity theft and fraud, securities and bank fraud; money laundering, and electronic transfer fraud. Data privacy crimes, economic espionage, and intellectual property crimes. Principles applicable to searches and seizures of computers, other digital devices, and peripheral. Laws governing eavesdropping, wiretaps, and other investigatory devices. The admission of digital evidence in court. Procedures for investigating cybercrime beyond the borders of the prosecuting jurisdiction. Each chapter includes key words or phrases readers should be familiar with before moving on to the next chapter. Review problems are supplied to test assimilation of the material, and the book contains weblinks to encourage further study.

Cybercrime and the Law

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.

Digital Forensics and Cyber Crime

This volume provides new insights into the diverse and complex contexts of legal discourse and activity performed across a variety of socially and culturally informed digital media transformations. It addresses topical issues of legal discourse performed by Web-mediated technologies and (social) media usage in professional and institutional contexts of communication. Its analyses rely on specific perspectives, varied applications, and different methodological procedures, providing a multifaceted overview of ongoing research and knowledge in the field.

Computer Forensics: Investigation Procedures and Response (CHFI)

Updated to include the most current events and information on cyberterrorism, the second edition of Computer Forensics: Cybercriminals, Laws, and Evidence continues to balance technicality and legal analysis as it enters into the world of cybercrime by exploring what it is, how it is investigated, and the regulatory laws surrounding the collection and use of electronic evidence. Students are introduced to the technology involved in computer forensic investigations and the technical and legal difficulties involved in searching, extracting, maintaining, and storing electronic evidence, while simultaneously looking at the legal implications of such investigations, and the rules of legal procedure relevant to electronic evidence. Significant and current computer forensic developments are examined, as well as the implications for a variety of fields including cybercrime, computer science, law, public policy, and administration.

Computer Forensics

The first full-scale overview of cybercrime, law, and policy

Introductory Computer Forensics

Computers can be powerful tools for creating positive change, but in the wrong hands, they can also be destructive weapons. Cybercrime is a growing field of criminal activity, and it is important for readers to know as much as possible about it to avoid becoming a victim. Readers learn valuable information through detailed main text, fact boxes, and helpful sidebars. They also discover what they can do now to prepare for an exciting career investigating cybercriminals. Full-color photographs are included to show readers the technological advances used to combat the many forms of cybercrime—from sextortion to cyberterrorism.

Social Media Investigation for Law Enforcement

There are today no more compelling sets of crime and security threats facing nations, communities, organizations, groups, families and individuals than those encompassed by cybercrime. For over fifty years crime enabled by computing and telecommunications technologies have increasingly threatened societies as they have become reliant on information systems for sustaining modernized living. Cybercrime is not a new phenomenon, rather an evolving one with respect to adoption of information technology (IT) for abusive and criminal purposes. Further, by virtue of the myriad ways in which IT is abused, it represents a technological shift in the nature of crime rather than a new form of criminal behavior. In other words, the nature of crime and its impacts on society are changing to the extent computers and other forms of IT are used for ill-intent purposes. Understanding the subject, then, is imperative to combating it and to addressing it at various levels. This work is the first comprehensive encyclopedia to address cybercrime. Topical articles address all key areas of concern and specifically those having to with: terminology, definitions and social constructs of crime; national infrastructure security vulnerabilities and capabilities; types of attacks to computers and information systems; computer abusers and cybercriminals; criminological, sociological, psychological and technological theoretical underpinnings of cybercrime; social and economic impacts of crime enabled with information technology (IT) inclusive of harms experienced by victims.

Page 3/5
of cybercrimes and computer abuse; emerging and controversial issues such as online pornography, the computer hacking subculture and potential negative effects of electronic gaming and so-called computer addiction; bodies and specific examples of U.S. federal laws and regulations that help to prevent cybercrimes; examples and perspectives of law enforcement, regulatory and professional member associations concerned about cybercrime and its impacts; and computer forensics as well as general investigation/prosecution of high tech crimes and attendant challenges within the United States and internationally.

International and Transnational Crime and Justice

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 provides law enforcement and IT security professionals with the information needed to manage a digital investigation. Everything needed for analyzing forensic data and recovering digital evidence can be found in one place, including instructions for building a digital forensics lab. * Digital investigation and forensics is a growing industry * Corporate IT departments investigating corporate espionage and criminal activity are learning as they go and need a comprehensive guide to e-discovery * Appeals to law enforcement agencies with limited budgets

Guidelines for Computer Forensics Investigations in Developing Country

When it comes to computer crimes, the criminals got a big head start. But the law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cybercrime cases. When the first edition of "Scene of the Cybercrime" published in 2002, it was one of the first books that educated IT security professionals and law enforcement how to fight Cybercrime. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cybercrime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cybercrime report: 50% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybercrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandated by federal compliance regulations such as Sarbanes-Oxley, HIPAA, or the Payment Card Industry (PCI) Data Security Standard. Scene of the Cybercrime, Second Edition is a completely revised and updated book that covers all of the technological, legal, and regulatory changes, which have occurred since the first edition. The book is written for dual audience: IT security professionals and members of law enforcement. It gives the technical experts a little peek into the law enforcement world, a highly structured environment where the "letter of the law" is paramount and procedures must be followed closely lest an investigation be contaminated and all the evidence collected rendered useless. It also provides law enforcement officers with an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. Scene of the Cybercrime, Second Edition provides a roadmap that those on both sides of the table can use to navigate the legal and technical landmines; understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live. Also included is an all new chapter on Worldwide Forensics Acts and Laws. * Companion Web site provides custom tools and scripts, which readers can download for conducting digital forensic investigations. * Special chapters outline how Cybercrime investigations must be reported and investigated by corporate IT staff to meet federal mandates from Sarbanes Oxley, and the Payment Card Industry (PCI) Data Security Standard * Details forensic investigative techniques for the most common operating systems (Windows, Linux and UNIX) as well as cutting edge devices including iPods, Blackberries, and cell phones.

Digital Crime and Forensic Science in Cyberspace

Cybersecurity is significant in light of the fact that cybersecurity chance is expanding. Driven by worldwide network and use of cloud administrations, similar to Amazon Web Services, to store touchy information and individual data. A cross the board, helpless setup of cloud administrations combined with progressively refined cybercriminals implies the hazard that your association experiences a fraud or data breach is on the ascent. Digital dangers can emerge out of any degree of your association. You should teach your staff about basic social building tricks like phishing and more complex cybersecurity assaults likeransomware or other malware intended to take protected innovation or individual information and many more. I hereby present a manual which will not only help you to know your rights as well as how to keep yourself safe on cyberspace. The book has been awarded by many experts as well as it has also been recognised by the University of Mumbiar for their B.com - Banking & Insurance as well as on Investment M management Program.

The Context and Media of Legal Discourse

Social Media is becoming an increasingly important—and controversial—investigative source for law enforcement. This project provides an overview of the current state of digital forensics and information forensics on Facebook and other social media networks and the state of the law, touches on hacktivism, and discusses the implications for privacy and other controversial areas. The authors also point to future trends. A bout Forensic Studies for Criminal Justice: The Forensic Studies for Criminal Justice series consists of short-format content on new developments, unique perspectives, or how-to information on areas in forensic science—all specifically designed to meet the needs of the criminal justice community. Instructors wishing to provide their students with more in-depth coverage on certain forensic areas can add these digestible, inexpensive works to their syllabi without having to completely redesign their course, instead selecting the material that suits their needs. Law enforcement and other criminal justice professionals will find a wealth of valuable information to improve training sessions. Written by experts in the disciplines they are covering and edited by a senior scholar in criminal justice, Forensic Studies for Criminal Justice opens up the world of forensic science to the criminal justice community. Part of a new Anderson series presenting brief works on forensic science, written especially for students and law enforcement. Surveys the current state of the digital forensic investigation tools available for social media, looking at legal concerns and pointing to future trends. Discusses the types of crimes committed using social media, including hatecrim, burglary, malware, cyberbullying, and child exploitation, among others Case studies of domestic and international social media investigations

A n Introduction to Crime Scene Investigation

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book’s 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students’ understanding of the material, 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.

Encyclopedia of Cybercrime


In an age of growing cyber crime, cyber-terrorism, hacker activism, and with the ever more central role of digital technology, it is inevitable that the computer will increasingly find itself at the heart of criminal activity and criminal investigations. Used as a powerful tool by both criminals and crime fighters, computers are now providing the virtual evidence that is needed to prosecute Cybercrime. Forensic studies in this book provide the required academic and professional requirements and expectations. Also covered are careers in the private sector relating to corporate security and anti-hacking efforts. Detailed discussions of educational pathways, job search strategies, interview techniques, and lifelong learning and career development are included. Steeped as it is in digital literacy and career preparedness, this power-packed resource also lends itself perfectly to the relevant Common Core curriculum standards for the reading of instructional
Globalization and the easy movement of people, weapons, and toxins across borders has transformed security into a transnational phenomenon. Preventing transnational security threats has proven to be a very difficult challenge for governments and institutions around the world. Transnational Security addresses these issues, which are at the forefront of every global security professional's agenda. This book analyzes the most pressing current transnational security threats, including weapons of mass destruction, terrorism, organized crime, cybercrime, natural disasters, human-made disasters, infectious diseases, food insecurity, water insecurity, and energy insecurity. It considers the applicable international laws and examines how key international organizations are dealing with these issues. The author uses a combination of theory and real-world examples to illustrate the transnational nature of security risks. By providing a detailed account of the different threats, countermeasures, and their implications for a number of different fields—law, public policy and administration, security, and criminology—this book will be an extremely useful resource for academicians, practitioners, and graduate and upper-level undergraduate students in these areas.

Privacy in a Cyber Age

Increasing number of computer crime happens anywhere anytime affecting both developed and developing countries. Surveys and studies related to computer security found that there have been no single technology able to provide total protection on information resources so far. Therefore, post examinations of computer attacks or computer crimes are important and crucial. Computer forensics is an interdisciplinary field of study to deal with investigation of digital evidence to trace the original source of cyber criminals. Unfortunately as a new field, computer forensics still lacks of standardization and consistency. To fill the gap, this study aims at proposing a comprehensive guidelines of computer forensics investigations in developing countries. The results will benefit policy makers, law enforcements as well as security practitioners from academic and industry especially in developing countries.