Cybercrime Investigative Case Management An Excerpt From Placing The Suspect Behind The Keyboard 1st Edition By Shavers Brett 2012 Paperback

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: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybecrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandates 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 which 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 Editions provides a roadmap that those on both sides of the table can use to navigate the legal and technical landscape to 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.
Cybercrime Investigative Case ManagementAn Excerpt from Placing the Suspect Behind the KeyboardNewnes Cybercrime Investigation Case Studies is a "first look" excerpt from Brett Shavers' new Syngress book, Placing the Suspect Behind the Keyboard. Case studies are an effective method of learning the methods and processes that were both successful and unsuccessful in real cases. Using a variety of case types, including civil and criminal cases, with different cybercrimes, a broad base of knowledge can be gained by comparing the cases against each other. The primary goal of reviewing successful cases involving suspects using technology to facilitate crimes is to be able to find and use the same methods in future cases. This "first look" teaches you how to place the suspect behind the keyboard using case studies.

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 frauds, homeland security, and information warfare.

This book constitutes the refereed proceedings of the 12th Pacific Asia Workshop on Intelligence and Security Informatics, PAISI 2017, held in Jeju Island, South Korea, in May 2017 in conjunction with PAKDD 2017, the 21st Pacific-Asia Conference on Knowledge Discovery and Data Mining. The 8 revised full papers and one short paper were carefully reviewed and selected from 13 submissions. The papers cover topics such as information access and security, cybersecurity and infrastructure protection, data and text mining, and network based data analytics.

Placing the Suspect Behind the Keyboard is the definitive book on conducting a complete investigation of a cybercrime using digital forensics techniques as well as physical investigative procedures. This book merges a digital analysis examiner's work with the work of a case investigator in order to build a solid case to identify and prosecute cybercriminals. Brett Shavers links traditional investigative techniques with high tech crime analysis in a manner that not only determines elements of crimes, but also places the suspect at the keyboard. This book is a first in combining investigative strategies of digital forensics analysis processes alongside physical investigative techniques in which the reader will gain a holistic approach to their current and future cybercrime investigations. Learn the tools and investigative principles of both physical and digital cybercrime investigations—and how they fit together to build a solid and complete case Master the techniques of conducting a holistic investigation that combines both digital and physical evidence to track down the "suspect behind the

keyboard" The only book to combine physical and digital investigative techniques

This book presents 94 papers from the 2nd International Conference of Reliable Information and Communication Technology 2017 (IRICT 2017), held in Johor, Malaysia, on April 23–24, 2017. Focusing on the latest ICT innovations for data engineering, the book presents several hot research topics, including advances in big data analysis techniques and applications; mobile networks; applications and usability; reliable communication systems; advances in computer vision, artificial intelligence and soft computing; reliable health informatics and cloud computing environments, e-learning acceptance models, recent trends in knowledge management and software engineering; security issues in the cyber world; as well as society and information technology.

Presents a collection of articles on human-computer interaction, covering such topics as applications, methods, hardware, and computers and society.

"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 purpose of this project was to develop and evaluate a computer crime investigative distance-learning program for the National Cybercrime Training Partnership. It had been alleged that the current training system did not meet the specific needs of individual law enforcement agencies resulting in a lack of computer crime investigators. A

computer crime investigative distance-learning prototype and evaluative instrument were developed to answer each of the five research questions. Conclusions and recommendations were also included in the study.

The growth of technology allows us to imagine entirely new ways of committing, combating and thinking about criminality, criminals, police, courts, victims and citizens. Technology offers not only new tools for committing and fighting crime, but new ways to look for, unveil, label crimes and new ways to know, watch, prosecute and punish criminals. This book attempts to disentangle the realities, the myths, the politics, the theories and the practices of our new, technology-assisted, era of crime and policing. Technocrime, policing and surveillance explores new areas of technocrime and technopolicing, such as credit card fraud, the use of DNA and fingerprint databases, the work of media in creating new crimes and new criminals, as well as the "proper" way of doing policing, and the everyday work of police investigators and intelligence officers, as seen through their own eyes. These chapters offer new avenues for studying technology, crime and control, through innovative social science methodologies. This book builds on the work of Leman-Langlois' last book Technocrime, and brings together fresh perspectives from eminent scholars to consider how our relationship with technology and institutions of social control are being reframed, with particular emphasis on policing and surveillance. Technocrime, policing and surveillance will be of interest to those studying criminal justice, policing and the sociology of surveillance as well as practitioners involved with the legal aspects of law enforcement technologies, , domestic security government departments and consumer advocacy groups.

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 peripherals 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.

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.

This book constitutes the refereed proceedings of the Pacific Asia Workshop on Intelligence and Security Informatics, PAISI 2014, held in Tainan, Taiwan, in May 2014 in conjunction with PAKDD 2014, the 18th Pacific-Asia Conference on Knowledge Discovery and Data Mining. The 7 revised full papers presented together with one short paper were carefully reviewed and selected from 10 submissions. The papers are organized in topical sections on regional data sets and case studies, cybercrime, information security engineering and text mining.

Contemporary society resides in an age of ubiquitous technology. With the consistent creation and wide availability of multimedia content, it has become imperative to remain updated on the latest trends and applications in this field. Digital Multimedia: Concepts, Methodologies, Tools, and Applications is an innovative source of scholarly content on the latest trends, perspectives, techniques, and implementations of multimedia technologies. Including a comprehensive range of topics such as interactive media, mobile technology, and data management, this multi-volume book is an ideal reference source for engineers, professionals, students, academics, and researchers seeking emerging information on digital multimedia.

The emergence of the World Wide Web, smartphones, and computers has transformed the world and enabled individuals to engage in crimes in a multitude of new ways. Criminological scholarship on these issues has increased dramatically over the

last decade, as have studies on ways to prevent and police these offenses. This book is one of the first texts to provide a comprehensive review of research regarding cybercrime, policing and enforcing these offenses, and the prevention of various offenses as global change and technology adoption increases the risk of victimization around the world. Drawing on a wide range of literature, Holt and Bossler offer an extensive synthesis of numerous contemporary topics such as theories used to account for cybercrime, policing in domestic and transnational contexts, cybercrime victimization and issues in cybercrime prevention. The findings provide a roadmap for future research in cybercrime, policing, and technology, and discuss key controversies in the existing research literature in a way that is otherwise absent from textbooks and general cybercrime readers. This book is an invaluable resource for academics, practitioners, and students interested in understanding the state of the art in social science research. It will be of particular interest to scholars and students interested in cybercrime, cyber-deviance, victimization, policing, criminological theory, and technology in general.

The Digital Age offers many far-reaching opportunities - opportunities that allow for fast global communications, efficient business transactions and stealthily executed cyber crimes. Featuring contributions from digital forensic experts, the editor

of Forensic Computer Crime Investigation presents a vital resource that outlines the latest strategi

With the continued progression of technologies such as mobile computing and the internet of things (IoT), cybersecurity has swiftly risen to a prominent field of global interest. This has led to cyberattacks and cybercrime becoming much more sophisticated to a point where cybersecurity can no longer be the exclusive responsibility of an organization's information technology (IT) unit. Cyber warfare is becoming a national issue and causing various governments to reevaluate the current defense strategies they have in place.

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM provides emerging research exploring the practical aspects of reassessing current cybersecurity measures within organizations and international governments and improving upon them using audit and awareness training models, specifically the Cybersecurity Audit Model (CSAM) and the Cybersecurity Awareness Training Model (CATRAM). The book presents multi-case studies on the development and validation of these models and frameworks and analyzes their implementation and ability to sustain and audit national cybersecurity

strategies. Featuring coverage on a broad range of topics such as forensic analysis, digital evidence, and incident management, this book is ideally designed for researchers, developers, policymakers, government officials, strategists, security professionals, educators, security analysts, auditors, and students seeking current research on developing training models within cybersecurity management and awareness.

This book contains a selection of thoroughly refereed and revised papers from the Fourth International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2012, held in October 2012 in Lafayette, Indiana, USA. The 20 papers in this volume are grouped in the following topical sections: cloud investigation; malware; behavioral; law; mobile device forensics; and cybercrime investigations. Investigative Case Management is a "first look" excerpted from Brett Shavers' new Syngress book, Placing the Suspect Behind the Keyboard. Investigative case management is more than just organizing your case files. It includes the analysis of all evidence collected through digital examinations, interviews, surveillance, and other data sources. In order to place a suspect behind any keyboard, supporting evidence needs to be collected and attributed to a person. This first look provides you with traditional and innovative methods of data

analysis to identify and eliminate suspects through a combination of supporting methods of analysis.
The internet is established in most households worldwide and used for entertainment purposes, shopping, social networking, business activities, banking, telemedicine, and more. As more individuals and businesses use this essential tool to connect with each other and consumers, more private data is exposed to criminals ready to exploit it for their gain. Thus, it is essential to continue discussions involving policies that regulate and monitor these activities, and anticipate new laws that should be implemented in order to protect users. Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications examines current internet and data protection laws and their impact on user experience and cybercrime, and explores the need for further policies that protect user identities, data, and privacy. It also offers the latest methodologies and applications in the areas of digital security and threats. Highlighting a range of topics such as online privacy and security, hacking, and online threat protection, this multi-volume book is ideally designed for IT specialists, administrators, policymakers, researchers, academicians, and upper-level students.
The investigator's practical guide for cybercrime evidence identification and collection Cyber attacks perpetrated against businesses, governments,

organizations, and individuals have been occurring for decades. Many attacks are discovered only after the data has been exploited or sold on the criminal markets. Cyber attacks damage both the finances and reputations of businesses and cause damage to the ultimate victims of the crime. From the perspective of the criminal, the current state of inconsistent security policies and lax investigative procedures is a profitable and low-risk opportunity for cyber attacks. They can cause immense harm to individuals or businesses online and make large sums of money—safe in the knowledge that the victim will rarely report the matter to the police. For those tasked with probing such crimes in the field, information on investigative methodology is scarce. The Cybercrime Investigators Handbook is an innovative guide that approaches cybercrime investigation from the field-practitioner's perspective. While there are high-quality manuals for conducting digital examinations on a device or network that has been hacked, the Cybercrime Investigators Handbook is the first guide on how to commence an investigation from the location the offence occurred—the scene of the cybercrime—and collect the evidence necessary to locate and prosecute the offender. This valuable contribution to the field teaches readers to locate, lawfully seize, preserve, examine, interpret, and manage the technical evidence that is vital for effective cybercrime investigation. Fills the need for a field manual for front-line cybercrime investigators Provides practical guidance with clear, easy-to-understand language Approaches cybercrime form the perspective of the field practitioner Helps companies

comply with new GDPR guidelines Offers expert advice from a law enforcement professional who specializes in cybercrime investigation and IT security Cybercrime Investigators Handbook is much-needed resource for law enforcement and cybercrime investigators, CFOs, IT auditors, fraud investigators, and other practitioners in related areas.

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.

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 be 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 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

Criminal Investigations Today: The Essentials examines the processes, practices, and people involved in the investigation of crime in a brief and accessible format that hones in on the key topics students actually need to know. Drawing from his vast experience in the field, author Richard M. Hough distills the essentials of criminal investigations and takes students through the in-depth processes of criminal investigations while maintaining a streamlined approach that allows for optimal student learning. The text's focus on people within the investigative system is reinforced with running case studies and hands-on application. Included with this title: The password-protected Instructor Resource Site (formally known as SAGE Edge) offers access to all text-specific resources, including a test bank and editable, chapter-specific PowerPoint® slides. Learn more.

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.

Cyber Crime and Cyber Terrorism Investigator's Handbook is a vital tool in the arsenal of today's computer programmers, students, and investigators. As computer networks become ubiquitous throughout the world, cyber crime, cyber terrorism, and cyber war have become some of the most concerning topics in today's security landscape. News stories about Stuxnet and PRISM have brought these activities into the public eye, and serve to show just how effective, controversial, and worrying these tactics can become. Cyber Crime and

Cyber Terrorism Investigator's Handbook describes and analyzes many of the motivations, tools, and tactics behind cyber attacks and the defenses against them. With this book, you will learn about the technological and logistic framework of cyber crime, as well as the social and legal backgrounds of its prosecution and investigation. Whether you are a law enforcement professional, an IT specialist, a researcher, or a student, you will find valuable insight into the world of cyber crime and cyber warfare. Edited by experts in computer security, cyber investigations, and counter-terrorism, and with contributions from computer researchers, legal experts, and law enforcement professionals, Cyber Crime and Cyber Terrorism Investigator's Handbook will serve as your best reference to the modern world of cyber crime. Written by experts in cyber crime, digital investigations, and counter-terrorism Learn the motivations, tools, and tactics used by cyber-attackers, computer security professionals, and investigators Keep up to date on current national and international law regarding cyber crime and cyber terrorism See just how significant cyber crime has become, and how important cyber law enforcement is in the modern world
Introduce students to the challenges, excitement, and rewards of law enforcement today with Dempsey and Forst's AN INTRODUCTION TO POLICING, 8th Edition. Written by law enforcement veterans with extensive first-hand experience in all areas of policing, this engaging, comprehensive book blends practical information with pertinent theory. The authors examine today's most current issues and topics, including homeland security,

recent terrorism incidents, the controversial Secure Communities Program by DHS, Specialized Policing Responses to individuals with mental illness, advances in policing technology, and more. Readers find the latest in academic and practitioner research as well as the most current applications, statistics, court cases, and information on law enforcement careers, all introduced through memorable learning features. The book also discusses small and rural departments while maintaining critical foundational coverage students need to fully understand who police are, what they do, and how they do it. Extensive examples from police departments throughout the nation and world as well as essays from respected law enforcement veterans offer insights into crucial law enforcement issues and challenges. AN INTRODUCTION TO POLICING is an essential read for anyone considering a career in law enforcement today. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This volume presents recent research in cyber security and reports how organizations can gain competitive advantages by applying the different security techniques in real-world scenarios. The volume provides reviews of cutting–edge technologies, algorithms, applications and insights for bio-inspiring cyber security-based systems. The book will be a valuable companion and comprehensive reference for both postgraduate and senior undergraduate students who are taking a course in cyber security. The volume is organized in self-contained chapters to provide greatest reading flexibility.

Cybercrime continues to skyrocket but we are not combatting it effectively yet. We need more cybercrime investigators from all backgrounds and working in every sector to conduct effective investigations. This book is a comprehensive resource for everyone who encounters and investigates cybercrime, no matter their title, including those working on behalf of law enforcement, private organizations, regulatory agencies, or individual victims. It provides helpful background material about cybercrime's technological and legal underpinnings, plus in-depth detail about the legal and practical aspects of conducting cybercrime investigations. Key features of this book include: Understanding cybercrime, computers, forensics, and cybersecurity Law for the cybercrime investigator, including cybercrime offenses; cyber evidence-gathering; criminal, private and regulatory law, and nation-state implications Cybercrime investigation from three key perspectives: law enforcement, private sector, and regulatory Financial investigation Identification (attribution) of cyber-conduct Apprehension Litigation in the criminal and civil arenas. This far-reaching book is an essential reference for prosecutors and law enforcement officers, agents and analysts; as well as for private sector lawyers, consultants, information security professionals, digital forensic examiners, and more. It also functions as an excellent course book for educators and trainers. We need more investigators who know how to fight cybercrime, and this book was written to achieve that goal. Authored by two former cybercrime prosecutors with a diverse array of expertise in criminal justice and the private sector, this

book is informative, practical, and readable, with innovative methods and fascinating anecdotes throughout.

This book contains a selection of thoroughly refereed and revised papers from the Third International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 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.

"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.