Virtualization And Forensics A Digital Forensic Investigators Guide To Virtual Environments

Cloud Storage Forensics
Advances in Digital Forensics
Vintroductory Computer Forensics
Advances in Digital Forensics
VAdvances
in Digital Forensics
XVI
Digital Forensics
Explained
Building a Digital Forensic Laboratory
Mastering Python Forensics
Forensics in Telecommunications, Information and Multimedia
Computer Forensics
Cybercrime and Cloud Forensics:
Applications for Investigating Processes
Digital Forensics and Cyber Crime
Research Anthology on Privatizing and Securing Data
Securing the Virtual Environment, Included DVD
Digital Forensics and Born-digital Content in Cultural Heritage Collections
Mac OS X, iPod, and iPhone Forensic Analysis DVD
Toolkit
Guide to Computer Forensics and Digital Evidence
Collection
or
An Introduction to the Art and Science of Digital Forensics
and Investigation
Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions
Digital Archaeology of Digital Forensics for Handheld Devices
Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics
Digital Forensics
Basics
Virtualization
for Security Advances in Digital Forensics
VII
Information Security and Digital Forensics
Windows Registry Forensics
Operating System Forensics
Augmented Reality
The Art of Memory Forensics
Advances in Digital Forensics
IX
TechnoSecurity's Guide to E-Discovery and Digital Forensics
The Best Damn Cybercrime and Digital Forensics Book
Period
Virtualization and Forensics
Cuckoo Malware Analysis
Computational Intelligence and Information Technology

One of the biggest buzzwords in the IT industry for the past few years, virtualization has matured into a practical requirement for many best-practice business scenarios, becoming an invaluable tool for security professionals at companies of every size. In addition to saving time and other resources, virtualization affords unprecedented means for intrusion and malware detection, prevention, recovery, and analysis.

Taking a practical approach in a growing market underserved by books, this book is the first comprehensive guide to virtualization for enhanced security, including sandboxing, disaster recovery and high availability, forensic analysis, and honeypotting. Already gaining buzz and traction in actual use at an impressive rate, Gartner research indicates that virtualization will be the most significant trend in IT infrastructure over the next four years. A recent report by IT research firm IDC predicts the virtualization services market will grow from $5.5 billion in 2006 to $11.7 billion in 2011. With this growth in adoption, becoming increasingly common even for small and midsize businesses, security is becoming a much more serious concern, both in terms of how to secure virtualization and how virtualization can serve critical security objectives.

Tilts exist and are on the way to fill the need for securing virtualization, but security professionals do not yet have a book outlining the many security applications of virtualization that will become increasingly important in their job requirements. This book is the first to fill that need, covering tactics such as isolating a virtual environment on the desktop for application testing, creating virtualized storage solutions for immediate disaster recovery and high availability across a network, migrating physical systems to virtual systems for analysis, and creating complete virtual systems to entice hackers and expose potential threats to actual production systems. About the Technologies A sandbox is an isolated environment created to run and test applications that might be a security risk. Recovering a compromised system is as easy as restarting the virtual machine to revert to the point before failure. Employing virtualization on actual production systems, rather than just test environments, yields similar benefits for disaster recovery and high availability. While traditional disaster recovery methods require time-consuming reinstallation of the operating system and applications before restoring data, backing up to a virtual machine makes the recovery process much easier, faster, and efficient. The virtual machine can be restored to same physical machine or an entirely different machine if the original machine has experienced irreversible hardware failure. Decreased downtime translates into higher availability of the system and increased productivity in the enterprise.

Virtualization has been used for years in the field of forensic analysis, but new tools, techniques, and automation capabilities are making it an increasingly important tool. By means of virtualization, an investigator can create an exact working copy of a physical machine on another machine, including hidden or encrypted partitions, without altering any data, allowing complete access for analysis. The investigator can also take a live "snapshot" to review or freeze the target computer at any point in time, before an attacker has a chance to cover his tracks or inflict further damage.

Master the art of digital forensics and analysis with Python About This Book Learn to perform forensic analysis and investigations with the help of Python, and gain an advanced understanding of the various Python libraries and frameworks Analyze Python scripts to extract metadata and investigate forensic artifacts The writers, Dr. Michael Spritelzenbarth and Dr. Johann Uhrmann, have used their experience to craft this hands-on guide to using Python for forensic analysis and investigations. Who This book is for If you are a network security professional or forensics analyst who wants to gain a deeper understanding of performing forensic analysis with Python, then this book is for you. Some Python experience would be helpful. What You Will Learn Explore the forensic analysis of different platforms such as Windows, Android, and vSphere Semi-automatically reconstruct major parts of the system activity and time-line Leverage Python cytopes for protocol decoding Examine artifacts from mobile, Skype, and browsers Discover how to utilize Python to improve the focus of your analysis Investigate in volatile memory with the help of volatility on the Android and Linux platforms In Detail Digital forensic analysis is the process of examining and extracting data digitally and examining it. Python has the combination of power, expressiveness, and ease of use that makes it an essential complementary tool to the traditional, off-the-shelf digital forensic tools. This book will teach you how to perform forensic analysis and investigations by exploring the capabilities of various Python libraries. The book starts by explaining the building blocks of the Python programming language, especially cytopes in-depth, along with how to automate typical tasks in file system analysis, common correlation tasks to discover anomalies, as well as templates for investigations. Next, we'll show you cryptographic algorithms that can be used during forensic investigations to check for known files or to compare suspicious files with online services such as VirusTotal or Mobile-Sandbox. Moving on, you'll learn how to sniff on the network, generate and analyze network flows, and perform log correlation with the help of Python scripts and tools. You'll get to know about the concepts of virtualization and how virtualization influences IT forensics, and you'll discover how to perform forensic analysis of a jailbroken/vrooted mobile device that is based on iOS or Android. Finally, the book teaches you how to analyze volatile memory and search for known malware samples based on YARA rules. Style and approach This easy-to-follow guide will demonstrate forensic analysis techniques by showing you how to solve real-world-scenarios step by step.

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to answer questions such as the following: How can you use the tools and techniques in this book to analyze and investigate computer crime? What tools are available to you, and how do you use them? How do you follow the proper procedures and legal guidelines for conducting an investigation? How do you present your findings to a court of law?
to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to describe the inner workings of each technique and to help users with varying IT skills. What is also included for users with varying IT skills is an explanation of the importance of each technique in their investigation process.

In establishing dedicated examinations free of viruses, spyware, and connections to other devices that could taint evidence Supplies guidance on determining protocols for complicated crime scenes with further connectivity and tampering of evidence. Emphasizing the policies required in the work environment, the author provides readers with a clear understanding of the differences between a corporate computer security professional and a personal computer security professional.

Every year, in response to new laws and new laws in different countries and regions, there are changes to the fundamental knowledge, skills, techniques, and tools required by all IT security professionals. In step with the lightning-quick, increasingly fast pace of change in the technology field, the Information Security Management Handbook, updated yearly, has become the standard on which all IT security programs and certifications are based. It reflects new updates to the Common Body of Knowledge (CBK) that IT security professionals all over the globe need to know. Captures the crucial elements of the CBK. The book explores access control, telecommunications and network security, information security and risk management, application security, and cryptography. In addition, the book offers best practices for establishing an incident response policy and seizing data from company or privately owned digital devices.

While the purview of digital forensics was once specialized to fields of law enforcement, computer security, and national defense, the increasing ubiquity of computers and electronic devices means that digital forensics tools and practices have found their way into the hands of anyone with access to a computer and an Internet connection. Digital forensics is the newest branch of computer security, focusing on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, Compact and Concise provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensic process—from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A’s of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data. Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

ISDF 2009, the First International Conference on Information Security and Digital Forensics, was held at City University London during September 7-8, 2009. The conference was organized as a meeting point for leading national and international - perts of information security and digital forensics. The conference was rewarding in many ways; ISDF 2009 was an exciting and vibrant event, with 4 keynote talks, 25 invited talks, 30 well-paper presentations and those attending had the opportunity to meet and talk with many distinguished people who are responsible for shaping the area of information security. This conference was organized as part of two major research projects funded by the UK Engineering and Physical Sciences Research Council in the areas of Security and Digital Forensics. I would like to thank all the people who contributed to the technical program. The most apparent of these are the Indian delegates who all accepted our invite to give presentations at this conference. Less apparent perhaps is the terrific work of the members of the Technical Program Committee, especially in reviewing the papers, which is a critical and time-consuming task. I would like to thank Raj Rajaran (City University London) for making the idea of the ISDF 2009 conference a reality with his hard work. Last but not least, I would like to thank all the authors who submitted papers, making the conference possible, and the authors of accepted papers for their cooperation. Dasun Weerasinghe

Approximately 80 percent of the world’s population now owns a cell phone, which can hold evidence or contain logs about communications concerning a crime. Cameras, PDAs, and GPS devices can also contain information related to corporate policy infractions and crimes. Aimed to prepare investigators in the public and private sectors, Digital Forensics for Handheld Devices examines both the theoretical and practical aspects of investigating handheld digital devices. This book focuses on all areas of mobile device forensics, including topics from the legal, technical, academic, and social aspects of the discipline. It provides guidance on how to seize data, examine it, and prepare it as evidence for court. This includes the use of chain of custody forms for seized evidence and Faraday Bags for digital devices to prevent further connectivity and tampering of evidence. Emphasizing the policies required in the work environment, the book provides a clear understanding of the differences between a corporate investigation and a criminal investigation. The book also: Offers best practices for establishing an incident response policy and seizing data from company or privately owned digital devices Provides guidance in establishing dedicated examinations free of viruses, spyware, and connections to other devices that could taint evidence Supplies guidance on determining protocols for complicated crime scenes with external media and devices that may have connected with the handheld device Considering important privacy issues and the Fourth Amendment, this book facilitates an understanding of how to use digital forensic tools to investigate the complete range of available digital devices, including flash drives, cell phones, PDAs, digital cameras, and netbooks. It includes examples of commercially available digital forensic tools and ends with a discussion of the education and certifications required for various careers in mobile device forensics.

*While the purview of digital forensics was once specialized to fields of law enforcement, computer security, and national defense, the increasing ubiquity of computers and electronic devices means that digital
forensics is now used in a wide variety of cases and circumstances. Most records today are born digital, and libraries and other collecting institutions increasingly receive computer storage media as part of their acquisition of "papers" from writers, scholars, scientists, musicians, and public figures. This poses new challenges to librarians, archivists, and curators—challenges related to accessing and preserving legacy formats, recovering data, ensuring authenticity, and maintaining trust. The methods and tools developed by forensics experts represent a novel approach to these demands. For example, the same forensics software that indexes a criminal suspect's hard drive allows the archivist to prepare a comprehensive manifest of the electronic files a donor has turned over for accession. This report introduces the field of digital forensics in the cultural heritage sector and explores some points of convergence between the interests of those charged with collecting and maintaining born-digital cultural heritage materials and those charged with collecting and maintaining legal evidence."

A step-by-step guide to identifying and defending against attacks on the virtual environment As more and more data is moved into virtual environments the need to secure them becomes increasingly important. Useful for service providers as well as enterprise and small business IT professionals the book offers a broad look across virtualization used in various industries as well as a narrow view of vulnerabilities unique to virtual environments. A companion DVD is included with recipes and testing scripts. Examines the difference in a virtual model versus traditional computing models and the appropriate technology and procedures to defend it from attack. The book offers a deep look at the virtual environment and the steps necessary for defense. Covers information security in virtual environments: building a virtual attack lab, finding leaks, getting a side-channel, denying or compromising services, using the hypervisor, forcing an interception, and spreading infections. Accompanying DVD includes hands-on examples and code. This how-to guide arms IT managers, vendors, and architects of virtual environments with the tools they need to protect against common threats. Windows Registry Forensics provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques are presented that take the student and analyst beyond the current use of viewers and into real analysis of data contained in the Registry, demonstrating the forensic value of the Registry. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this book is packed with real-world examples using freely available open source tools. It also includes case studies and a CD containing code and author-created tools discussed in the book. This book will appeal to computer forensic and incident response professionals, including federal government and commercial/private sector contractors, consultants, etc. Named a 2011 Best Digital Forensics Book by InfoSec Reviews Packed with real-world examples using freely available open source tools Deep explanation and understanding of the Windows Registry—the most difficult part of Windows to analyze forensically Includes a CD containing code and author-created tools discussed in the book.

Updated with the latest advances from the field, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, Fifth Edition combines all-encompassing topic coverage and authoritative information from seasoned experts to deliver the most comprehensive forensics resource available. This proven author team's wide ranging areas of expertise mirror the breadth of coverage provided in the book, which focuses on techniques and practices for gathering and analyzing evidence used to solve crimes involving computers. Providing clear instruction on the topics and techniques involved in the trade, it introduces readers to every step of the computer forensics investigation—from lab set-up to testifying in court. It also details step-by-step guidance on how to use current forensics software. Appropriate for learners new to the field, it is also an excellent refresher and technology update for professionals in law enforcement, investigations, or computer security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XV describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: forensic models, mobile and embedded device forensics, filesystem forensics, image forensics, and forensic techniques. This book is the fifteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of fourteen edited papers from the Fifteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA in the winter of 2019. Advances in Digital Forensics XV is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

Preparing for and Identifying Attacks in Virtual Environments A step-by-step guide to identifying and defending against attacks on the virtual environment As more and more data is moved into virtual environments the need to secure them becomes increasingly important. The methods and tools developed by forensics experts represent a novel approach to these demands. For example, the same forensics software that indexes a criminal suspect's hard drive allows the archivist to prepare a comprehensive manifest of the electronic files a donor has turned over for accession. This report introduces the field of digital forensics in the cultural heritage sector and explores some points of convergence between the interests of those charged with collecting and maintaining born-digital cultural heritage materials and those charged with collecting and maintaining legal evidence."

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercriminals have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is stored and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing...
Electronic discovery refers to a process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case. Computer forensics is the application of computer investigation and analysis techniques to perform an investigation to find out exactly what happened on a computer and who was responsible. IDC estimates that the U.S. market for computer forensics will grow from $252 million in 2004 to $630 million by 2009. Business is strong outside the United States, as well. By 2011, the estimated international market will be $1.8 billion dollars. The Techno Forensics Conference has increased in size by almost 50% in its second year; another example of the rapid growth in the market. This book is the first to combine cybercrime and digital forensic topics to provide law enforcement and IT security professionals with the information needed to manage a digital investigation. Everything needed for analyzing forensic data and recovering digital evidence can be found in one place, including instructions for building a digital forensics lab. *Digital investigation and forensics is a growing industry * Corporate IT, 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

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance - investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics V describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, integrity and privacy, network forensics, forensic computing, investigative techniques, legal issues and evidence management. This book is the fifth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-three edited papers from the Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, USA in the spring of 2009. Advances in Digital Forensics V is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

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.

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

Operating System Forensics is the first book to cover all three critical operating systems for digital forensic investigations in one comprehensive reference. Users will learn how to conduct successful digital forensic examinations in Windows, Linux, and Mac OS, the methodologies used, key technical concepts, and the tools needed to perform examinations. Mobile operating systems such as Android, iOS, Windows, and Blackberry are also covered, providing everything practitioners need to conduct a forensic investigation of the most commonly used operating systems, including technical details of how each operating system works and how to find artifacts. This book walks you through the critical components of investigation and operating system functionality, including file systems, data recovery, memory forensics, system configuration, Internet access, cloud computing, tracking artifacts, executing malware, and log files. You'll find coverage of key technical topics like Windows Registry, etc directory, Web browsers caches, Mbox, PST files, GPS data, ELF, and more. Hands-on exercises in each chapter drive home the concepts covered in the book. You'll get everything you need for a successful forensic
examination, including incident response tactics and legal requirements. Operating System Forensics is the only place you’ll find all this covered in one book. Covers digital forensic investigations of the three major operating systems, including Windows, Linux, and Mac OS. Presents the technical details of each operating system, allowing users to find artifacts that might be missed using automated tools. Hands-on exercises drive home key concepts covered in the book. Includes discussions of cloud, Internet, and major mobile operating systems such as Android and iOS.

This book is a step-by-step, practical tutorial for analyzing and detecting malware and performing digital investigations. This feature offers clear and concise guidance in an easily accessible format. Cuckoo Malware Analysis is great for anyone who wants to analyze malware through programming, networking, disassembling, forensics, and virtualization. Whether you are new to malware analysis or have some experience, this book will help you get started with Cuckoo Sandbox so you can start analyzing malware effectively and efficiently.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance - investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics V describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, integrity and privacy, network forensics, forensic computing, investigative techniques, legal issues and evidence management. This book is the fifth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-three edited papers from the Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, USA in the spring of 2009. Advances in Digital Forensics V is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

Cyber-attacks are rapidly becoming one of the most prevalent issues globally, and as they continue to escalate, it is imperative to explore new approaches and technologies that help ensure the security of the online community. Beyond cyber-attacks, personal information is now routinely and exclusively housed in cloud-based systems. The rising use of information technologies requires stronger information security and system procedures to reduce the risk of information breaches. Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics presents emerging research and methods on preventing information breaches and further securing system networks. While highlighting the rising concerns in information privacy and system security, this book explores the cutting-edge methods combatting digital risks and cyber threats. This book is an important resource for information technology professionals, cybercrime researchers, network analysts, government agencies, business professionals, academics, and practitioners seeking the most up-to-date information and methodologies on cybercrime, digital terrorism, network security, and information technology ethics.

The Definitive, Up-to-Date Guide to Digital Forensics The rapid proliferation of cyber crime is increasing the demand for digital forensics experts in both law enforcement and the private sector. In Digital Archaeology, expert practitioner Michael Graves has written the most thorough, realistic, and up-to-date guide to the principles and techniques of modern digital forensics. Graves begins by providing a solid understanding of the legal underpinnings of and critical laws affecting computer forensics, including key principles of evidence and case law. Next, he explains how to systematically and thoroughly investigate computer systems to unearth crimes or other misbehavior, and back it up with evidence that will stand up in court. Drawing on the analogy of archaeological research, Graves explains each key tool and method investigato uses to reliably uncover hidden information in digital systems. His detailed demonstrations often include the actual syntax of command-line utilities. Along the way, he presents exclusive coverage of facilities management, a full chapter on the crucial topic of first response to a digital crime scene, and up-to-the-minute coverage of investigating evidence in the cloud. Graves concludes by presenting coverage of important professional and business issues associated with building a career in digital forensics, including current licensing and certification requirements. Topics Covered Include: Acquiring and analyzing data in ways consistent with forensic procedure Requirements for computer forensics and evidence recovery, including incident response and legal issues, data forensics, and computer forensics. The book contains a selection of twenty-three edited papers from the Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, USA in the spring of 2009. Advances in Digital Forensics V is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

"This book provides a media for advancing research and the development of theory and practice of digital crime prevention and forensics, embracing a broad range of digital crime and forensics disciplines"--Provided by publisher.

With the explosive growth in mobile phone usage and rapid rise in search engine technologies over the last decade, augmented reality (AR) is poised to be one of this decade’s most disruptive technologies, as the information that is constantly flowing around us is brought into view, in real-time, through augmented reality. In this cutting-edge book, the authors outline and discuss never-before-published information about augmented reality and its capabilities. With coverage of mobile, desktop, developers, security, challenges, and gaming, this book gives you a comprehensive understanding of what augmented reality is, what it can do, what is in store for the future and most importantly: how to benefit from using AR in our lives and careers. Educates readers how best to use augmented reality regardless of industry Provides an in-depth understanding of AR and ideas ranging from new business applications to new crime fighting methods Includes actual examples and case studies from both private and government application

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 specific forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students’ understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital
The need to professionally and successfully conduct computer forensic investigations of incidents and crimes has never been greater. This has caused an increased requirement for information about the creation and management of computer forensic laboratories and the investigations themselves. This includes a great need for information on how to cost-effectively establish and manage a computer forensic laboratory. This book meets that need: a clearly written, non-technical book on the topic of computer forensics with emphasis on the establishment and management of a computer forensic laboratory and its subsequent support to successfully conducting computer-related crime investigations. Provides guidance on creating and managing a computer forensic lab Covers the regulatory and legislative environment in the US and Europe Meets the needs of IT professionals and law enforcement as well as consultants.

TechnoSecurity's Guide to E-Discovery and Digital Forensics provides IT security professionals with the information, tools, and procedural requirements needed to create, manage and sustain a digital forensics lab and investigative team that can accurately and effectively analyze forensic data and recover digital evidence, while preserving the integrity of the electronic evidence for discovery and trial. Internationally known experts in computer forensics share their years of experience at the forefront of digital forensics. Bonus chapters on how to build your own Forensics Lab 50% discount to the upcoming Techno Forensics conference for everyone who purchases a book.

An authoritative guide to investigating high-technology crimes Internet crime is seemingly ever on the rise, making the need for a comprehensive resource on how to investigate these crimes even more dire. This professional-level book--aimed at law enforcement personnel, prosecutors, and corporate investigators--provides you with the training you need in order to acquire the sophisticated skills and software solutions to stay one step ahead of computer criminals. Specifies the techniques needed to investigate, analyze, and document a criminal act on a Windows computer or network Places a special emphasis on how to thoroughly investigate a criminal activity and now just perform the initial response Walks you through ways to present technically complicated material in simple terms that will hold up in court Features content fully updated for Windows Server 2008 R2 and Windows 7 Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academic adoption, Mastering Windows Network Forensics and Investigation, 2nd Edition offers help for investigating high-technology crimes.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advanced Digital Forensics XVI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, file system forensics, cloud forensics, social media forensics, multimedia forensics, and novel applications. This book is the sixteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of sixteen edited papers from the Sixteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India, in the winter of 2020. Advances in Digital Forensics XVI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

This book provides digital forensic investigators, security professionals, and law enforcement with all of the information, tools, and utilities required to conduct forensic investigations of computers running any variant of the Macintosh OS X operating system, as well as the iPod and iPhone. Digital forensic investigators and security professionals can use data gathered from these devices to aid in the prosecution of criminal cases, litigate civil cases, audit adherence to federal regulatory compliance issues, and identify breech of corporate and government usage policies on networks. MAC Disks, Partitioning, and HFS+ File System Manage multiple partitions on a hard disk, and understand how the operating system stores data. FileVault and Time Machine Decrypt locked FileVault files and restore files backed up with Leopard's Time Machine. Recovering Browser History Recover traces of Web surfing activity in Safari with Web cache and .plist files Recovering Email Artifacts, iChat, and Other Chat Logs Expose communications data in iChat, Address Book, Apple's Mail, MobileMe, and Web-based email. Locating and Recovering Photos Use iPhoto, Spotlight, and shadow files to find artifacts of photos (e.g., thumbnails) when the original photos no longer exist. Finding and Recovering QuickTime Movies and Other Video Understand video file formats—created with iSight, iMovie, or another application—and how to find them. PDF, Word, and Other Document Recovery Recover text documents and metadata with Microsoft Office, OpenOffice, Entourage, Adobe PDF, or other formats. Forensic Acquisition and Analysis of an iPod Document seize an iPod model and analyze the iPod image file and artifacts on a Mac. Forensic Acquisition and Analysis of an iPhone Acquire a physical image of an iPhone or iPod Touch and safely analyze without jailbreaking. Includes unique information about Mac OS X, iPod, iMac, and iPhone Forensics Analysis Unavailable Anywhere Else Authors Are Pioneering Researchers in the Field of Macintosh Forensics, with Combined Experience in Law Enforcement, Military, and Corporate Forensics.

This book constitutes the thoroughly refereed post-conference proceedings of the 7th International ICST Conference on Digital Forensics and Cyber Crime, ICFDC2C 2013, held in September 2013 in Moscow, Russia. The 16 revised full papers presented at this conference were carefully reviewed and selected from 38 submissions. The papers cover diverse topics in the field of digital forensics and cybercrime, ranging from regulation of social networks to file carving, as well as technical issues, information warfare, cyber terrorism, critical infrastructure protection, standards, certification, accreditation, automation and digital forensics in the cloud.

Memory forensics provides cutting edge technology to help investigate digital attacks. Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a free day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly.
Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

To reduce the risk of digital forensic evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and set of procedures for conducting digital forensic investigations and examinations. Digital forensic investigation in the cloud computing environment, however, is in infancy due to the comparatively recent prevalence of cloud computing. Cloud Storage Forensics presents the first evidence-based cloud forensic framework. Using three popular cloud storage services and one private cloud storage service as case studies, the authors show you how their framework can be used to undertake research into the data remnants on both cloud storage servers and client devices when a user undertakes a variety of methods to store, upload, and access data in the cloud. By determining the data remnants on client devices, you gain a better understanding of the types of terrestrial artifacts that are likely to remain at the Identification stage of an investigation. Once it is determined that a cloud storage service account has potential evidence of relevance to an investigation, you can communicate this to legal liaison points within service providers to enable them to respond and secure evidence in a timely manner. Learn to use the methodology and tools from the first evidenced-based cloud forensic framework. Case studies provide detailed tools for analysis of cloud storage devices using popular cloud storage services. Includes coverage of the legal implications of cloud storage forensic investigations. Discussion of the future evolution of cloud storage and its impact on digital forensics.

Digital forensics deals with the acquisition, preservation, examination, analysis, and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics VII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Forensic Techniques, Fraud and Malware Investigations, Network Forensics, and Advanced Forensic Techniques. This book is the 7th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers, and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of 96 papers from the 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA in the spring of 2011.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics VI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, filesystem forensics, cloud forensics, social media forensics, multimedia forensics, and novel applications. This book is the sixteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of 199 edited papers from the Sixteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India, in the winter of 2020. Advances in Digital Forensics XVI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeeet Shenoi is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma, USA.

This book constitutes the proceedings of the First International Conference on Computational Intelligence and Information Technology, CIIT 2011, held in Pune, India, in November 2011. The 58 revised full papers, 67 revised short papers, and 32 poster papers presented were carefully reviewed and selected from 483 initial submissions. The papers are contributed by innovative academics and industrial experts in the field of computer science, information technology, computational engineering, mobile communication and security and offer a stage to a common forum, where a constructive dialog on theoretical concepts, practical ideas and results of the state of the art can be developed.

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