Virtualization And Forensics A Digital Forensic Investigators Guide To Virtual Environments Author Diane Barrett Aug 2010

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 Spreitzenbarth 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 ctypes 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 ctypes 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/rooted 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-word-scenarios step by step.

This book constitutes the refereed proceedings of two workshops held at the 13th International Conference on Security and Privacy in Communications Networks, SecureComm 2017, held in Niagara Falls, ON, Canada, in October 2017: the 5th International Workshop on Applications and Techniques in Cyber Security, ATCS 2017, and the First Workshop on Security and Privacy in the Internet Of Things, SePrIoT 2017.The 22 revised regular papers were carefully reviewed and selected from 105 submissions. The topics range from access control; language-based security; malicious software; network security; cloud security; software security; operating system security; privacy protection, database security, security models; and many more.The SePrIoT workshop targets to address novel approaches in security and privacy. The papers focuse, amongst others, on novel models, techniques, protocols, algorithms, or architectures.

The field of computer forensics has experienced significant growth recently and those looking to get into the industry have significant opportunity for upward mobility. Focusing on the concepts investigators need to know to conduct a thorough investigation, Digital Forensics Explained provides an overall description of the forensic practice from a practitioner’s perspective. Starting with an overview, the text describes best practices based on the author’s decades of experience conducting investigations and working in information technology. It illustrates the forensic process, explains what it takes to be an investigator, and highlights emerging trends. Filled with helpful templates and contributions from seasoned experts in their respective fields, the book includes coverage of: Internet and email investigations Mobile forensics for cell phones, iPads, music players, and other small devices Cloud computing from an architecture perspective and its impact on digital forensics Anti-forensic techniques that may be employed to make a forensic exam more difficult to conduct Recoverability of information from damaged media The progression of a criminal case from start to finish Tools that are often used in an examination, including commercial, free, and open-source tools; computer and mobile tools; and things as simple as extension cords Social media and social engineering forensics Case documentation and presentation, including sample summary reports and a cover sheet for a cell phone investigation The text includes acquisition forms, a sequential process outline to guide your investigation, and a checklist of supplies you’ll need when responding to an incident. Providing you with the understanding and the tools to deal with suspects who find ways to make their digital activities hard to trace, the book also considers cultural implications, ethics, and the psychological effects that digital forensics investigations can have on investigators.

This book constitutes the thoroughly refereed post-conference proceedings of the First International Joint Conference on Advances in Signal Processing and Information Technology (SPIT 2011) and Recent Trends in Information Processing and Computing (IPC 2011) held in Amsterdam, The Netherlands, in December 2011. The 50 revised full papers presented were carefully selected from 298 submissions. Conference papers promote research and development activities in computer science, information technology, computational engineering, image and signal processing, and communication.

“This book contains some of the most up-to-date information available anywhere on a wide variety of topics related to Techno Security. As you read the book, you will notice that the authors took the approach of identifying some of the risks, threats, and vulnerabilities and then discussing the countermeasures to address them. Some of the topics and thoughts discussed here are as new as tomorrow’s headlines, whereas others have been around for decades without being properly addressed. I hope you enjoy this book as much as we have enjoyed working with the various authors and friends during its development. —Donald Withers, CEO and Cofounder of TheTrainingCo. • Jack Wiles, on Social Engineering offers up a potpourri of tips, tricks, vulnerabilities, and lessons learned from 30-plus years of experience in the worlds of both physical and technical security. • Russ Rogers on the Basics of Penetration Testing illustrates the standard methodology for penetration testing: information gathering, network enumeration, vulnerability identification, vulnerability exploitation, privilege escalation, expansion of reach, future access, and information compromise. • Johnny Long on No Tech Hacking shows how to hack without touching a computer using tailgating, lock bumping, shoulder surfing, and dumpster diving. • Phil Drake on Personal, Workforce, and Family Preparedness covers the basics of creating a plan for you and your family, identifying and obtaining the supplies you will need in an emergency. • Kevin O’Shea on Seizure of Digital Information discusses collecting hardware and information from the scene. • Amber Schroader on Cell Phone Forensics writes on new methods and guidelines for digital forensics. • Dennis O’Brien on RFID: An Introduction, Security Issues, and Concerns discusses how this well-intended technology has been eroded and used for fringe implementations. • Ron Green on Open Source Intelligence details how a good Open Source Intelligence program can help you create leverage in negotiations, enable smart decisions regarding the selection of goods and services, and help avoid pitfalls and hazards. • Raymond Blackwood on Wireless Awareness: Increasing the Sophistication of Wireless Users maintains it is the technologist’s responsibility to educate, communicate, and support users despite their lack of interest in understanding how it works. • Greg Kipper on What is Steganography? provides a solid understanding of the basics of steganography, what it can and can’t do, and arms you with the information you need to set your career path. • Eric Cole on Insider Threat discusses why the insider threat is worse than the external threat and the effects of insider threats on a company. Internationally known experts in information security share their wisdom Free pass to Techno Security Conference for everyone who purchases a book—$1,200 value

Open Source Software for Digital Forensics is the first book dedicated to the use of FLOSS (Free Libre Open Source Software) in computer forensics. It presents the motivations for using FLOSS applications as tools for collection, preservation and analysis of digital evidence in computer and network forensics. It also covers extensively several forensic FLOSS tools, their origins and evolution. Open Source Software for Digital Forensics is based on the OSSCoNF workshop, which was held in Milan, Italy, September 2008 at the World Computing Congress, co-located with OSS 2008. This edited volume is a collection of contributions from researchers and practitioners world wide. Open Source Software for Digital Forensics is designed for advanced level students and researchers in computer science as a secondary text and reference book. Computer programmers, software developers, and digital forensics professionals will also find this book to be a valuable asset.

ADVANCES IN DIGITAL FORENSICS XIV Edited by: Gilbert Peterson and Sujeet Shenoi 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 information assurance - investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XIV 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; Network Forensics; Cloud Forensics; and Mobile and Embedded Device Forensics. This book is the fourteenth 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 nineteen edited papers from the Fourteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India in the winter of 2018. Advances in Digital Forensics XIV 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, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Explains both cloud security and privacy, and digital forensics in a unique, systematical way Discusses both security and privacy of cloud and digital forensics in a systematic way Contributions by top U.S., Chinese and international researchers, and professionals active in the field of information / network security, digital / computer forensics, and the cloud and big data Of interest to those focused upon security and implementation, and those focused upon incident management Logical, well-structured and organized

This book constitutes the refereed proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICDF2C 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, deanonymization, digital forensics tools, cybercrime investigation and digital forensics triage, digital forensics tools testing and validation, hacking

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 21 edited papers from the 7th 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 2011. Advances in Digital Forensics VII 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. Sujeet Shenoi is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma, USA.

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

This book gathers high-quality papers presented at the 2nd International Conference on Communication, Devices & Computing (ICCDC 2019), held at Haldia Institute of Technology from March 14–15, 2019. The papers are divided into three main areas: communication technologies, electronics circuits & devices and computing. Written by students and researchers from around the world, they accurately reflect the global status quo.

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

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 touches 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 author provides readers with 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.

This book gathers the proceedings of the 13th International Conference on Management Science and Engineering Management (ICMSEM 2019), which was held at Brock University, Ontario, Canada on August 5–8, 2019. Exploring the latest ideas and pioneering research achievements in management science and engineering management, the respective contributions highlight both theoretical and practical studies on management science and computing methodologies, and present advanced management concepts and computing technologies for decision-making problems involving large, uncertain and unstructured data. Accordingly, the proceedings offer researchers and practitioners in related fields an essential update, as well as a source of new research directions.

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems

Practically every crime now involves some aspect of digital evidence. This is the most recent volume in the Advances in Digital Forensics series. It describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. This book contains a selection of twenty-eight edited papers from the Fourth Annual IFIP WG 11.9 Conference on Digital Forensics, held at Kyoto University, Kyoto, Japan in the spring of 2008.

The use of computer virtualization technologies has rapidly grown since the early 2000's. Factors driving this growth include the ever-increasing utilization of cloud computing as well as benefits to consolidating physical hardware within a data center. In addition to the growth of virtualization technologies, computer security incidents are also increasing. However, researchers have drawn attention to the problem that many of the traditional computer forensics tools and investigation techniques cannot be used to gather and analyze digital evidence obtained from virtualization technologies or cloud computing resources.To solve a part of this problem, this thesis proposes a new open source tool called ESXimager that securely acquires digital evidence from VMware ESXi hypervisors. The tool securely images selected virtual machine files running on VMware ESXi and ensures image integrity through the entire imaging process. Written in Perl and utilizing Tk, the tool makes use of an ESXi server's ability to execute shell commands. Bit-stream copies are created using the dd command, image integrity is verified using the MD5 and SHA1 hashing algorithms, and images are securely transferred to an external imaging machine with SFTP. With a secure image created, a forensics investigator can load the image into a separate computer forensics tool for analysis. ESXimagers capabilities are validated in a small yet realistic test environment. The tool connects to an ESXi server, creates images of selected virtual machine files, calculates multiple hashes, and securely transfers images to a local imaging machine. In addition, the tool detects if the integrity of an image file is compromised. With some additional development and testing in a larger environment, this could potentially become the go-to tool used to acquire images from VMware ESXi hypervisors.

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 XI 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 Internet Crime Investigations Forensic Techniques Mobile Device Forensics Cloud Forensics Forensic Tools This book is the eleventh 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 prac tice in digital forensics. The book contains a selection of twenty edited papers from the Eleventh Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida in the winter of 2015. Advances in Digital Forensics XI 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, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Network forensics is an evolution of typical digital forensics, in which evidence is gathered from network traffic in near real time. This book will help security and forensics professionals as well as network administrators build a solid foundation of processes and controls to identify incidents and gather evidence from the network. Forensic scientists and investigators are some of the fastest growing jobs in the United States with over 70,000 individuals employed in 2008. Specifically in the area of cybercrime and digital forensics, the federal government is

conducting a talent search for 10,000 qualified specialists. Almost every technology company has developed or is developing a cloud computing strategy. To cut costs, many companies are moving toward network-based applications like SalesForce.com, PeopleSoft, and HR Direct. Every day, we are moving companies' proprietary data into a cloud, which can be hosted anywhere in the world. These companies need to understand how to identify where their data is going and what they are sending. Key network forensics skills and tools are discussed-for example, capturing network traffic, using Snort for network-based forensics, using NetWitness Investigator for network traffic analysis, and deciphering TCP/IP. The current and future states of network forensics analysis tools are addressed. The admissibility of network-based traffic is covered as well as the typical life cycle of a network forensics investigation.

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

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

This book constitutes the thoroughly refereed post-conference proceedings of the Third International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, E-Forensics 2010, held in Shanghai, China, in November 2010. The 32 revised full papers presented were carefully reviewed and selected from 42 submissions in total. These, along with 5 papers from a collocated workshop of E-Forensics Law, cover a wide range of topics including digital evidence handling, data carving, records tracing, device forensics, data tamper identification, and mobile device locating.

Virtualization and ForensicsA Digital Forensic Investigator's Guide to Virtual EnvironmentsSyngress

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

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

"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.

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 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, 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 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.

ISDF 2009, the First International Conference on Information Security and Digital Forensics, was held at City University London during September 7-8, 2009. The c- ference 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 and 18 full-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 Rajarajan (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

This book constitutes the refereed proceedings of the International Symposium on Security in Computing and Communications, SSCC 2014, held in Delhi, India, in September 2013. The 36 revised full papers presented together with 12 work-in-progress papers were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on security and privacy in networked systems; authentication and access control systems; encryption and cryptography; system and network security; work-in-progress.

TechnoSecurity's Guide to E-Discovery and Digital Forensics provides IT security professionals with the information (hardware, software, 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-technologycrimes Internet crime is seemingly ever on the rise, making the needfor a comprehensive resource on how to investigate these crimeseven more dire. This professional-level book--aimed at lawenforcement personnel, prosecutors, and corporateinvestigators--provides you with the training you need in order toacquire the sophisticated skills and software solutions to stay onestep ahead of computer criminals. Specifies the techniques needed to investigate, analyze, anddocument a criminal act on a Windows computer or network Places a special emphasis on how to thoroughly investigatecriminal activity and now just perform the initial response Walks you through ways to present technically complicatedmaterial in simple terms that will hold up in court Features content fully updated for Windows Server 2008 R2 andWindows 7 Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academicadoption, Mastering Windows Network Forensics and Investigation,2nd Edition offers help for investigating high-technologycrimes.

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigations Gather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10–specific feature forensics Utilize anti-forensic techniques, including steganography, data destruction techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals

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.

Every year, in response to new technologies 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 Exploring the ten domains of the CBK, the book explores access control, telecommunications and network security, information

security and risk management, application security, and cryptography. In addition, the expert contributors address security architecture and design, operations security, business continuity planning and disaster recovery planning. The book also covers legal regulations, compliance, investigation, and physical security. In this anthology of treatises dealing with the management and technical facets of information security, the contributors examine varied topics such as anywhere computing, virtualization, podslurping, quantum computing, mashups, blue snarfing, mobile device theft, social computing, voting machine insecurity, and format string vulnerabilities. Also available on CD-ROM Safeguarding information continues to be a crucial concern of all IT professionals. As new risks threaten the security of our systems, it is imperative that those charged with protecting that information continually update their armor of knowledge to guard against tomorrow's hackers and software vulnerabilities. This comprehensive Handbook, also available in fully searchable CD-ROM format keeps IT professionals abreast of new developments on the security horizon and reinforces timeless concepts, providing them with the best information, guidance, and counsel they can obtain.

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 VIII 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, mobile phone forensics, cloud forensics, network forensics, and advanced forensic techniques. This book is the eighth 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-two edited papers from the Eighth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the University of Pretoria, Pretoria, South Africa in the spring of 2012. Advances in Digital Forensics VIII 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. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

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.

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.

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 materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This

textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book.