Digital Forensics Digital Evidence In Criminal Investigations

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 XVII 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 seventeenth 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 thirteen edited papers from the Seventeenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held virtually in the winter of 2021. Advances in Digital Forensics XVII 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. Essay from the year 2015 in the subject Computer Science - Miscellaneous, UNITEC New Zealand, language: English, abstract: Nowadays the use of computers is increasing more and more. This has allowed the development of the internet. In turn, the Internet has brought many benefits, but the internet has also contributed to the rise of cyber-crime. So, with the rise of cybercrime, it has become critical to increase and develop computer systems security. Each time, the techniques used by cybercriminals are more sophisticated, making it more difficult to protect corporate networks. Because of this, the computer security of these companies has been violated, and it is here at this point when digital analysis forensic is needed to discover cybercriminals. So, with the rise of cybercrime, digital forensics is increasingly gaining importance in the area of information technology. For this reason, when a crime is done, the crime information is stored digitally. Therefore, it must use appropriate mechanisms for the collection, preservation, protection, analysis and presentation of digital evidence stored in electronic devices. It is here that the need arises for digital Page 1/17

forensics. In this report, I am going to explain what digital forensics is. Also, I will describe some forensic software and hardware and the importance of suitable forensic labs. So, let's start.

Handbook of Digital Forensics and Investigation builds on the success of the Handbook of Computer Crime Investigation, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is also designed as an accompanying text to Digital Evidence and Computer Crime. This unique collection details how to conduct digital investigations in both criminal and civil contexts, and how to locate and utilize digital evidence on computers, networks, and embedded systems. Specifically, the Investigative Methodology section of the Handbook provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery, and Intrusion Investigation. The Technology section is extended and updated to reflect the state of the art in each area of specialization. The main areas of focus in the Technology section are forensic analysis of Windows, Unix, Macintosh, and embedded systems (including cellular telephones and other mobile devices), and investigations involving networks (including enterprise environments and mobile telecommunications technology). This handbook is an essential technical reference and on-the-job guide that IT professionals, forensic practitioners, law enforcement, and attorneys will rely on when confronted with computer related crime and digital evidence of any kind. *Provides methodologies proven in practice for conducting digital investigations of all kinds *Demonstrates how to locate and interpret a wide variety of digital evidence, and how it can be useful in investigations *Presents tools in the context of the investigative process, including EnCase, FTK, ProDiscover, foremost, XACT, Network Miner, Splunk, flow-tools, and many other specialized utilities and analysis platforms *Case examples in every chapter give readers a practical understanding of the technical, logistical, and legal challenges that arise in real investigations

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.

Get up and running with collecting evidence using forensics best practices to present your findings in judicial or administrative proceedings Key Features Learn the core techniques of computer forensics to acquire and secure digital evidence skillfully Conduct a digital forensic examination and document the digital evidence collected Analyze security systems and overcome complex challenges with a variety of forensic investigations Book Description A computer forensics investigator must possess a variety of skills, including the ability to answer legal questions, gather and document evidence, and prepare for an investigation. This book will help you get up and running with using digital forensic tools and techniques to investigate cybercrimes successfully. Starting with an overview of forensics and all the open source and commercial tools needed to get the job done, you'll learn core forensic practices for searching databases and analyzing data over networks, personal devices, and web applications. You'll then learn how to acquire valuable information from different places, such as filesystems, e-mails, browser histories, and search queries, and capture data remotely. As you advance, this book will guide you through implementing forensic techniques on multiple platforms, such as Windows, Linux, and macOS, to demonstrate how to recover valuable information as evidence. Finally, you'll get to grips with presenting your findings efficiently in judicial or administrative proceedings. By the end of this book, you'll have developed a clear understanding of how to acquire, analyze, and present digital evidence like a proficient computer forensics investigator. What you will learn Understand investigative processes, the rules of evidence, and ethical guidelines Recognize and document different types of computer hardware Understand the boot process covering BIOS, UEFI, and the boot sequence Validate forensic hardware and software Discover the locations of common Windows artifacts Document your findings using technically correct terminology Who this book is for If you're an IT beginner, student, or an investigator in the public or private sector this book is for you. This book will also help professionals and investigators who are new to incident response and digital forensics and interested in making a career in the cybersecurity domain.

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.

The Basics of Digital Forensics provides a foundation for people new to the digital forensics field. This book teaches you how to conduct examinations by discussing what digital forensics is, the methodologies used, key tactical concepts, and the tools needed to perform examinations. Details on digital forensics for computers, networks, cell phones, GPS, the cloud and the Internet are discussed. Also, learn how to collect evidence, document the scene, and how deleted data can be recovered. The new Second Edition of this book provides you with completely up-to-date real-world examples and all the key technologies used in digital forensics, as well as new coverage of network intrusion response, how hard drives are organized, and electronic discovery. You'll also learn how to incorporate quality assurance into an investigation, how to prioritize evidence items to examine (triage), case processing, and what goes into making an expert witness. The Second Edition also features expanded resources and references, including online resources that keep you current, sample legal documents, and suggested further reading. Learn what Digital Forensics entails Build a toolkit and prepare an investigative plan Understand the common artifacts to look for in an exam Second Edition features all-new coverage of hard drives, triage, network intrusion response, and electronic discovery; as well as updated case studies, expert interviews, and expanded resources and references

"This book is a must for anyone attempting to examine the iPhone. The level of forensic detail is excellent. If only all guides to forensics were written with this clarity!"-Andrew Sheldon, Director of Evidence Talks, computer forensics experts With iPhone use increasing in business networks, IT and security professionals face a serious challenge: these devices store an enormous amount of information. If your staff conducts business with an iPhone, you need to know how to recover, analyze, and securely destroy sensitive data. iPhone Forensics supplies the knowledge necessary to conduct complete and highly specialized forensic analysis of the iPhone, iPhone 3G, and iPod Touch. This book helps you: Determine what type of data is stored on the device Break v1.x and v2.x passcode-protected iPhones to gain access to the device Build a custom recovery toolkit for the iPhone Interrupt iPhone 3G's "secure wipe" process Conduct data recovery of a v1.x and v2.x iPhone user disk partition, and preserve and recover the entire raw user disk partition Recover deleted voicemail, images, email, and other personal data, using data carving techniques Recover geotagged metadata from camera photos Discover Google map

lookups, typing cache, and other data stored on the live file system Extract contact information from the iPhone's database Use different recovery strategies based on case needs And more. iPhone Forensics includes techniques used by more than 200 law enforcement agencies worldwide, and is a must-have for any corporate compliance and disaster recovery plan.

The emergence of the World Wide Web, smartphones, and Computer-Mediated Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives, computer hacking and digital piracy, economic crime and online fraud, pornography and online sex crime, cyber-bulling and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation and the sociology of technology. "Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills. 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

Learn the skills you need to take advantage of Kali Linux for digital forensics investigations using this comprehensive guide Key Features Master powerful Kali Linux tools for digital investigation and analysis Perform evidence acquisition, preservation, and analysis using various tools within Kali Linux Implement the concept of cryptographic hashing and imaging using Kali Linux Perform memory forensics with Volatility and internet forensics with Xplico. Discover the capabilities of professional forensic tools such as Autopsy and DFF (Digital Forensic Framework) used by law enforcement and military personnel alike Book Description Kali Linux is a Linux-based distribution used mainly for penetration testing and digital forensics. It has a wide range of tools to help in forensics investigations and incident response mechanisms. You will start by understanding the fundamentals of digital forensics and setting up your Kali Linux environment to perform different investigation practices. The book will delve into the realm of operating systems and the various formats for file storage, including secret hiding places unseen by the end user or even the operating system. The book will also teach you to create forensic images of data and maintain integrity using hashing tools. Next, you will also master some advanced topics such as autopsies and acquiring investigation data from the network, operating system memory, and so on. The book introduces you to powerful tools that will take your forensic abilities and investigations to a professional level, catering for all aspects of full digital forensic investigations from hashing to reporting. By the end of this book, you will have had hands-on experience in implementing all the pillars of digital forensics—acquisition, extraction, analysis, and presentation using Kali Linux tools. What you will learn Get to grips with the fundamentals of digital forensics and explore best practices Understand the workings of file systems, storage, and data fundamentals Discover incident response procedures and best practices Use DC3DD and Guymager for acquisition and preservation techniques Recover deleted data with Foremost and Scalpel Find evidence of accessed programs and malicious programs using Volatility. Perform network and internet capture analysis with Xplico Carry out professional digital forensics investigations using the DFF and Autopsy automated forensic suites Who this book is for This book is targeted at forensics and digital investigators, security analysts, or any stakeholder interested in learning digital forensics using Kali Linux. Basic knowledge of Kali Linux will be an advantage.

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 Uncover a digital trail of e-evidence by using the helpful, easy-to-understand information in Computer Forensics For Dummies! Professional and armchair investigators alike can learn the basics of computer forensics, from digging out electronic evidence to solving the case. You won't need a computer science degree to master e-discovery. Find and filter data in mobile devices, e-mail, and other Web-based technologies. You'll learn all about e-mail and Webbased forensics, mobile forensics, passwords and encryption, and other e-evidence found through VoIP, voicemail, legacy mainframes, and databases. You'll discover how to use the latest forensic software, tools, and equipment to find the answers that you're looking for in record time. When you understand how data is stored, encrypted, and recovered, you'll be able to protect your personal privacy as well. By the time you finish reading this book, you'll know how to: Prepare for and conduct computer forensics investigations Find and filter data Protect personal privacy Transfer evidence without contaminating it Anticipate legal loopholes and opponents' methods Handle passwords and encrypted data Work with the courts and win the case Plus, Computer Forensics for Dummies includes lists of things that everyone interested in computer forensics should know, do, and build. Discover how to get qualified for a career in computer forensics, what to do to be a great investigator and expert witness, and how to build a forensics lab or toolkit. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Practically every crime now involves some digital

evidence; digital forensics provides the techniques and tools to articulate this evidence. This book 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.

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

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.

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 Digital Evidence and Computer CrimeForensic Science, Computers and the InternetAcademic Press

Security Smarts for the Self-Guided IT Professional Find out how to excel in the field of computer forensics investigations. Learn what it takes to transition from an IT professional to a computer forensic examiner in the private sector. Written by a Certified Information Systems Security Professional, Computer Forensics: InfoSec Pro Guide is filled with real-world case studies that demonstrate the concepts covered in the book. You'll learn how to set up a forensics lab, select hardware and software, choose forensic imaging procedures, test your tools, capture evidence from different sources, follow a sound investigative process, safely store evidence, and verify your findings. Best practices for documenting your results, preparing reports, and presenting evidence in court are also covered in this detailed resource. Computer Forensics: InfoSec Pro Guide features: Lingo—Common security terms defined so that you're in the know on the job IMHO—Frank and relevant opinions based on the author's years of industry experience Budget Note—Tips for getting security technologies and processes into your organization's budget In Actual Practice—Exceptions to the rules of security explained in real-world contexts Your Plan—Customizable checklists you can use on the job now Into Action—Tips on how, why, and when to apply new skills and techniques at work

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. Practical Forensic Imaging takes a detailed look at how to secure and manage

digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: -Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies -Protect attached evidence media from accidental modification -Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal -Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping –Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt –Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OSencrypted drives using BitLocker, FileVault, and TrueCrypt; and others –Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, Practical Forensic Imaging is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab. Python Forensics provides many never-before-published proven forensic modules, libraries, and solutions that can be used right out of the box. In addition, detailed instruction and documentation provided with the code samples will allow even novice Python programmers to add their own unique twists or use the models presented to build new solutions. Rapid development of new cybercrime investigation tools is an essential ingredient in virtually every case and environment. Whether you are performing post-mortem investigation, executing live triage, extracting evidence from mobile devices or cloud services, or you are collecting and processing evidence from a network, Python forensic implementations can fill in the gaps. Drawing upon years of practical experience and using numerous examples and illustrative code samples, author Chet Hosmer discusses how to: Develop new forensic solutions independent of large vendor software release schedules Participate in an open-source workbench that facilitates direct involvement in the design and implementation of new methods that augment or replace existing tools Advance your career by creating new solutions along with the construction of cutting-edge automation solutions to solve old problems Provides hands-on tools, code samples, and detailed instruction and documentation that can be put to use immediately Discusses how to create a Python forensics workbench Covers effective forensic searching and indexing using Python Shows how to use Python to examine mobile device operating systems: iOS, Android, and Windows 8 Presents complete coverage of how to use Python scripts for network investigation Given our increasing dependency on computing technology in daily business

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

This hands-on textbook provides an accessible introduction to the fundamentals of digital forensics. The text contains thorough coverage of the theoretical foundations, explaining what computer forensics is, what it can do, and also what it can't. A particular focus is presented on establishing sound forensic thinking and methodology, supported by practical guidance on performing typical tasks and using common forensic tools. Emphasis is also placed on universal principles, as opposed to content unique to specific legislation in individual countries. Topics and features: introduces the fundamental concepts in digital forensics, and the steps involved in a forensic examination in a digital environment; discusses the nature of what cybercrime is, and how digital evidence can be of use during criminal investigations into such crimes; offers a practical overview of common practices for cracking encrypted data; reviews key artifacts that have proven to be important in several cases, highlighting where to find these and how to correctly interpret them; presents a survey of various different search techniques, and several forensic tools that are available for free; examines the functions of AccessData Forensic Toolkit and Registry Viewer; proposes methods for analyzing applications, timelining, determining the identity of the computer user, and deducing if the computer was remote controlled; describes the central concepts relating to computer memory management, and how to perform different types of memory analysis using the open source tool Volatility; provides review questions and practice tasks at the end of most chapters, and supporting video lectures on YouTube. This easy-to-follow primer is an essential resource for students of computer forensics, and will also serve as a valuable reference for practitioners seeking instruction on performing forensic examinations in law enforcement or in the private sector.

An explanation of the basic principles of data This book explains the basic principles of data as buildingblocks of electronic evidential matter, which are used in a cyberforensics investigations. The entire text is written with noreference to a particular operation system or environment, thus it applicable to all work environments, cyber investigationscenarios, and technologies. The text is written in astep-by-step manner, beginning with the elementary buildingblocks of data progressing upwards to the representation andstorage of information. It inlcudes practical examples and illustrations throughout to guide the reader.

Digital forensics and multimedia forensics are rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended to by contributions from researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic triage, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features: Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of multimedia data and devices Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice guides, test datasets and more case studies Strategic Leadership in Digital Evidence: What Executives Need to Know provides leaders with broad knowledge and understanding of practical concepts in digital evidence, along with its impact on investigations. The book's chapters cover the differentiation of related fields, new market technologies, operating systems, social networking, and much more. This guide is written at the layperson level, although the audience is expected to have reached a level of achievement and seniority in their profession, principally law enforcement, security and intelligence. Additionally, this book will appeal to legal professionals and others in the broader justice system. Covers a broad range of challenges confronting investigators in the digital environment Addresses gaps in currently available resources and the future focus of a fast-moving field Written by a manager who has been a leader in the field of digital forensics for decades Digital forensics has been a discipline of Information Security for decades now. Its principles, methodologies, and techniques have remained consistent despite the evolution of technology, and, ultimately, it and can be applied to any form of digital data. However, within a corporate environment, digital forensic professionals are particularly challenged. They must maintain the legal admissibility and forensic viability of digital evidence in support of a broad range of different business functions that include incident response, electronic discovery (ediscovery), and ensuring the controls and accountability of such information across networks. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise provides the methodologies and strategies necessary for these key business functions to seamlessly integrate digital forensic capabilities to guarantee the admissibility and integrity of digital evidence. In many books, the focus on digital evidence is primarily in the

technical, software, and investigative elements, of which there are numerous publications. What tends to get overlooked are the people and process elements within the organization. Taking a step back, the book outlines the importance of integrating and accounting for the people, process, and technology components of digital forensics. In essence, to establish a holistic paradigm—and best-practice procedure and policy approach—to defending the enterprise. This book serves as a roadmap for professionals to successfully integrate an organization's people, process, and technology with other key business functions in an enterprise's digital forensic capabilities.

Get started with the art and science of digital forensics with this practical, handson guide! About This Book Champion the skills of digital forensics by understanding the nature of recovering and preserving digital information which is essential for legal or disciplinary proceedings Explore new and promising forensic processes and tools based on 'disruptive technology' to regain control of caseloads. Richard Boddington, with 10+ years of digital forensics, demonstrates real life scenarios with a pragmatic approach Who This Book Is For This book is for anyone who wants to get into the field of digital forensics. Prior knowledge of programming languages (any) will be of great help, but not a compulsory prerequisite. What You Will Learn Gain familiarity with a range of different digital devices and operating and application systems that store digital evidence. Appreciate and understand the function and capability of forensic processes and tools to locate and recover digital evidence. Develop an understanding of the critical importance of recovering digital evidence in pristine condition and ensuring its safe handling from seizure to tendering it in evidence in court. Recognise the attributes of digital evidence and where it may be hidden and is often located on a range of digital devices. Understand the importance and challenge of digital evidence analysis and how it can assist investigations and court cases. Explore emerging technologies and processes that empower forensic practitioners and other stakeholders to harness digital evidence more effectively. In Detail Digital Forensics is a methodology which includes using various tools, techniques, and programming language. This book will get you started with digital forensics and then follow on to preparing investigation plan and preparing toolkit for investigation. In this book you will explore new and promising forensic processes and tools based on 'disruptive technology' that offer experienced and budding practitioners the means to regain control of their caseloads. During the course of the book, you will get to know about the technical side of digital forensics and various tools that are needed to perform digital forensics. This book will begin with giving a quick insight into the nature of digital evidence, where it is located and how it can be recovered and forensically examined to assist investigators. This book will take you through a series of chapters that look at the nature and circumstances of digital forensic examinations and explains the processes of evidence recovery and preservation from a range of digital devices, including mobile phones, and other media. This

book has a range of case studies and simulations will allow you to apply the knowledge of the theory gained to real-life situations. By the end of this book you will have gained a sound insight into digital forensics and its key components. Style and approach The book takes the reader through a series of chapters that look at the nature and circumstances of digital forensic examinations and explains the processes of evidence recovery and preservation from a range of digital devices, including mobile phones, and other media. The mystery of digital forensics is swept aside and the reader will gain a quick insight into the nature of digital evidence, where it is located and how it can be recovered and forensically examined to assist investigators.

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 in 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 investigators use 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 Recovering and examining e-mail, Web, and networking activity Investigating users' behavior on mobile devices Overcoming anti-forensics measures that seek to prevent data capture and analysis Performing comprehensive electronic discovery in connection with lawsuits Effectively managing cases and documenting the evidence you find Planning and building your career in digital forensics Digital Archaeology is a key resource for anyone preparing for a career as a professional investigator; for IT professionals who are sometimes called upon to assist in investigations; and for those seeking an explanation of the processes involved in preparing an effective defense, including how to avoid the legally indefensible destruction of digital evidence. 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

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology - and new ways of exploiting information technology - is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters Based on the latest research, it provides novel

insights for students, including an informed look at the future of digital forensics Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals, illustrations and case example images Features real-word examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

Digital Forensics for Legal Professionals provides you with a guide to digital technology forensics in plain English. In the authors' years of experience in working with attorneys as digital forensics experts, common questions arise again and again: "What do I ask for?? "Is the evidence relevant?? "What does this item in the forensic report mean?? "What should I ask the other expert?? "What should I ask you?? "Can you explain that to a jury?? This book answers many of those questions in clear language that is understandable by non-technical people. With many illustrations and diagrams that will be usable in court, they explain technical concepts such as unallocated space, forensic copies, timeline artifacts and metadata in simple terms that make these concepts accessible to both attorneys and juries. The authors also explain how to determine what evidence to ask for, evidence might be that could be discoverable, and the methods for getting to it including relevant subpoena and motion language. Additionally, this book provides an overview of the current state of digital forensics, the right way to select a qualified expert, what to expect from a qualified expert and how to properly use experts before and during trial. Includes a companion Web site with: courtroom illustrations, and examples of discovery motions Provides examples of direct and cross examination questions for digital evidence Contains a reference of definitions of digital forensic terms, relevant case law, and resources for the attorney

The vast majority of modern criminal investigations involve some element of digital evidence, from mobile phones, computers, CCTV and other devices. Digital Forensics: Digital Evidence in Criminal Investigations provides the reader with a better understanding of how digital evidence complements "traditional" scientific evidence and examines how it can be used more effectively and efficiently in a range of investigations. Taking a new approach to the topic, this book presents digital evidence as an adjunct to other types of evidence and discusses how it can be deployed effectively in support of investigations. The book provides investigators/SSMs/other managers with sufficient contextual and technical information to be able to make more effective use of digital evidence sources in support of a range of investigations. In particular, it considers the roles played by digital devices in society and hence in criminal activities. From this, it examines the role and nature of evidential data which may be recoverable from a range of devices, considering issues relating to reliability and usefulness of those data. Includes worked case examples, test questions and review guizzes to enhance student understanding Solutions provided in an accompanying website Includes numerous case studies throughout to highlight how digital evidence is handled at the crime scene and what can happen when procedures are carried out incorrectly Considers digital evidence in a broader context alongside other scientific evidence Discusses the role of digital devices in criminal activities and provides methods for the evaluation and prioritizing of evidence sources Includes discussion of the issues surrounding modern digital evidence examinations, for example; volume of material and its complexity Clear overview of all types of digital evidence Digital Forensics: Digital Evidence in Criminal Investigations is an invaluable

Read Free Digital Forensics Digital Evidence In Criminal Investigations

text for undergraduate students taking either general forensic science courses where digital forensics may be a module or a dedicated computer/digital forensics degree course. The book is also a useful overview of the subject for postgraduate students and forensic practitioners. In a unique and systematic way, this book discusses the security and privacy aspects of the cloud, and the relevant cloud forensics. Cloud computing is an emerging yet revolutionary technology that has been changing the way people live and work. However, with the continuous growth of cloud computing and related services, security and privacy has become a critical issue. Written by some of the top experts in the field, this book specifically discusses security and privacy of the cloud, as well as the digital forensics of cloud data, applications, and services. The first half of the book enables readers to have a comprehensive understanding and background of cloud security, which will help them through the digital investigation guidance and recommendations found in the second half of the book. Part One of Security, Privacy and Digital Forensics in the Cloud covers cloud infrastructure security; confidentiality of data; access control in cloud IaaS; cloud security and privacy management; hacking and countermeasures; risk management and disaster recovery; auditing and compliance; and security as a service (SaaS). Part Two addresses cloud forensics - model, challenges, and approaches; cyberterrorism in the cloud; digital forensic process and model in the cloud; data acquisition; digital evidence management, presentation, and court preparation; analysis of digital evidence; and forensics as a service (FaaS). Thoroughly covers both security and privacy of cloud and digital forensics Contributions by top researchers from the U.S., the European and other countries, and professionals active in the field of information and network security, digital and computer forensics, and cloud and big data Of interest to those focused upon security and implementation, and incident management Logical, well-structured, and organized to facilitate comprehension Security, Privacy and Digital Forensics in the Cloud is an ideal book for advanced undergraduate and master's-level students in information systems, information technology, computer and network forensics, as well as computer science. It can also serve as a good reference book for security professionals, digital forensics practitioners and cloud service providers.

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 tools and techniques of 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. Implementing Digital Forensic Readiness: From Reactive to Proactive Process, Second Edition presents the optimal way for digital forensic and IT security professionals to implement a proactive approach to digital forensics. The book details how digital forensic processes can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and redusing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stances, a company's preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and

credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

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.

Copyright: b77a15f8f24f024860b69b925e4027ce