

The Basics Of Digital Forensics Second Edition The Primer For Getting Started In Digital Forensics

[Digital Forensics and Cyber Crime](#) [Advances in Digital Forensics II](#) [The Basics of Digital Forensics](#) **Digital Forensics Explained** [Digital Forensics with Open Source Tools](#) [The Best Damn Cybercrime and Digital Forensics Book Period](#) [Digital Forensics and Incident Response](#) **Implementing Digital Forensic Readiness** [Cybercrime and Digital Forensics](#) **Guide to Computer Forensics and Investigations** [Cyber Forensics](#) [Cybercrime and Digital Forensics Security, Privacy, and Digital Forensics in the Cloud](#) [The Basics of Digital Forensics](#) **Hacking Exposed** [Computer Forensics, Second Edition](#) [Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice](#) [Digital Evidence and Computer Crime](#) [Fundamentals of Digital Forensics](#) **Windows Registry Forensics** [Mastering Windows Network Forensics and Investigation](#) **Handbook of Digital Forensics and Investigation** [Digital Forensics and Incident Response](#) [Digital Forensics, Investigation, and Response](#) [Placing the Suspect Behind the Keyboard](#) **Cyber Forensics** [Computer Forensics](#) [Digital Forensics and Cyber Crime](#) **Digital Forensics for Legal Professionals** **Computer Forensics** [Learn Computer Forensics](#) [Learning IOS Forensics - Second Edition](#) **Digital Evidence and Computer Crime** **Windows Forensics Cookbook** [Computer Forensics](#) [InfoSec Pro Guide](#) **Digital Forensics** [Practical Mobile Forensics](#) **Digital Forensics and Incident Response - Second Edition** [Scene of the Cybercrime](#) **Cyber Crime and Forensic Computing** **Digital Forensics Basics**

When people should go to the ebook stores, search foundation by shop, shelf by shelf, it is in reality problematic. This is why we provide the books compilations in this website. It will very ease you to look guide **The Basics Of Digital Forensics Second Edition The Primer For Getting Started In Digital Forensics** as you such as.

By searching the title, publisher, or authors of guide you truly want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be all best area within net connections. If you take aim to download and install the The Basics Of Digital Forensics Second Edition The Primer For Getting Started In Digital Forensics, it is enormously easy then, past currently we extend the belong to to purchase and create bargains to download and install The Basics Of Digital Forensics Second Edition The Primer For Getting Started In Digital Forensics in view of that simple!

Fundamentals of Digital Forensics May 19 2021 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.

Handbook of Digital Forensics and Investigation Feb 13 2021 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

Digital Forensics, Investigation, and Response Dec 14 2020 Digital Forensics, Investigation, and Response, Fourth Edition examines the fundamentals of system forensics, addresses the tools, techniques, and methods used to perform computer forensics and investigation, and explores incident and intrusion response,

Guide to Computer Forensics and Investigations Jan 27 2022 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.

The Best Damn Cybercrime and Digital Forensics Book Period May 31 2022 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

Windows Forensics Cookbook Feb 02 2020 Maximize the power of Windows Forensics to perform highly effective forensic investigations About This Book Prepare and perform investigations using powerful tools for Windows, Collect and validate evidence from suspects and computers and uncover clues that are otherwise difficult Packed with powerful recipes to perform highly effective field investigations Who This Book Is For If you are a forensic analyst or incident response professional who wants to perform computer forensics investigations for the Windows platform and expand your tool kit, then this book is for you. What You Will Learn Understand the challenges of acquiring evidence from Windows systems and overcome them Acquire and analyze Windows memory and drive data with modern forensic tools. Extract and analyze data from Windows file systems, shadow copies and the registry Understand the main Windows system artifacts and learn how to parse data from them using forensic tools See a forensic analysis of common web browsers, mailboxes, and instant messenger services Discover how Windows 10 differs from previous versions and how to overcome the specific challenges it presents Create a graphical timeline and visualize data, which can then be incorporated into the final

report Troubleshoot issues that arise while performing Windows forensics In Detail Windows Forensics Cookbook provides recipes to overcome forensic challenges and helps you carry out effective investigations easily on a Windows platform. You will begin with a refresher on digital forensics and evidence acquisition, which will help you to understand the challenges faced while acquiring evidence from Windows systems. Next you will learn to acquire Windows memory data and analyze Windows systems with modern forensic tools. We also cover some more in-depth elements of forensic analysis, such as how to analyze data from Windows system artifacts, parse data from the most commonly-used web browsers and email services, and effectively report on digital forensic investigations. You will see how Windows 10 is different from previous versions and how you can overcome the specific challenges it brings. Finally, you will learn to troubleshoot issues that arise while performing digital forensic investigations. By the end of the book, you will be able to carry out forensics investigations efficiently. Style and approach This practical guide filled with hands-on, actionable recipes to detect, capture, and recover digital artifacts and deliver impeccable forensic outcomes.

The Basics of Digital Forensics Sep 22 2021 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

Cyber Forensics Oct 12 2020 Designed as an introduction and overview to the field, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition integrates theory and practice to present the policies, procedures, methodologies, and legal ramifications and implications of a cyber forensic investigation. The authors guide you step-by-step through the basics of investigation and introduce the tools and procedures required to legally seize and forensically evaluate a suspect machine. Updating and expanding information on concealment techniques, new technologies, hardware, software, and relevant new legislation, this second edition delineates the scope and goals of cyber forensics to reveal and track legal and illegal activity. Beginning with an introduction and definition of cyber forensics, chapters explain the rules of evidence and chain of custody in maintaining legally valid electronic evidence. They describe how to begin an investigation and employ investigative methodology, as well as establish standard operating procedures for the field and cyber forensic laboratory. The authors provide an in depth examination of the manipulation of technology to conceal illegal activities and the use of cyber forensics to uncover them. They discuss topics and issues such as conducting a cyber forensic investigation within both the local and federal legal framework, and evaluating the current data security and integrity exposure of multifunctional devices. Cyber Forensics includes details and tips on taking control of a suspect computer or PDA and its "operating" environment, mitigating potential exposures and risks to chain of custody, and establishing and following a flowchart for the seizure of electronic evidence. An extensive list of appendices include websites, organizations, pertinent legislation, further readings, best practice recommendations, more information on hardware and software, and a recap of the federal rules of civil procedure.

Cybercrime and Digital Forensics Nov 24 2021 "Types of hardware, peripherals, and electronic evidence" -- "Evidence integrity" -- "Summary" -- "13 ACQUISITION AND EXAMINATION OF FORENSIC EVIDENCE" -- "Introduction" -- "Data preservation" -- "Digital forensic imaging tools" -- "Uncovering digital evidence" -- "Data analysis" -- "Data reduction and filtering" -- "Reporting of findings" -- "Summary" -- "14 LEGAL CHALLENGES IN DIGITAL FORENSIC INVESTIGATIONS" -- "Introduction" -- "Constitutional issues in digital investigations" -- "Federal Rules of Evidence 702" -- "Summary" -- "15 THE FUTURE OF CYBERCRIME, TERROR, AND POLICY" -- "Introduction" -- "Considering the future of cybercrime" -- "How technicways will shift with new technologies" -- "Social movements, technology, and social change" -- "Need for new cyber criminological theories?" -- "Shifting enforcement strategies in the age of the Internet" -- "Considering the future of forensics" -- "The challenge to policy makers globally" -- "Summary" -- "Glossary"

Digital Forensics Dec 02 2019 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-world 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.

The Basics of Digital Forensics Sep 03 2022 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

Digital Forensics Basics Jun 27 2019 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

Mastering Windows Network Forensics and Investigation Mar 17 2021 An authoritative guide to investigating high-technology crimes Internet crime is seemingly ever on the rise, making the need for a comprehensive resource on how to investigate these crimes even more dire. This professional-level book--aimed at law enforcement personnel, prosecutors, and corporate investigators--provides you with the training you need in order to acquire the sophisticated skills and software solutions to stay one step ahead of computer criminals. Specifies the techniques needed to investigate, analyze, and document a criminal act on a Windows computer or network Places

a special emphasis on how to thoroughly investigate criminal activity and now just perform the initial response Walks you through ways to present technically complicated material in simple terms that will hold up in court Features content fully updated for Windows Server 2008 R2 and Windows 7 Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academic adoption, Mastering Windows Network Forensics and Investigation, 2nd Edition offers help for investigating high-technology crimes.

Learn Computer Forensics May 07 2020 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.

Digital Forensics and Incident Response Apr 29 2022 Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book Description An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

Digital Evidence and Computer Crime Mar 05 2020 Digital evidence--evidence that is stored on or transmitted by computers--can play a major role in a wide range of crimes, including homicide, rape, abduction, child abuse, solicitation of minors, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, espionage, and terrorism. Though an increasing number of criminals are using computers and computer networks, few investigators are well-versed in the evidentiary, technical, and legal issues related to digital evidence. As a result, digital evidence is often overlooked, collected incorrectly, and analyzed ineffectively. The

aim of this hands-on resource is to educate students and professionals in the law enforcement, forensic science, computer security, and legal communities about digital evidence and computer crime. This work explains how computers and networks function, how they can be involved in crimes, and how they can be used as a source of evidence. As well as gaining a practical understanding of how computers and networks function and how they can be used as evidence of a crime, readers will learn about relevant legal issues and will be introduced to deductive criminal profiling, a systematic approach to focusing an investigation and understanding criminal motivations.

Computer Forensics Jun 07 2020 Every computer crime leaves tracks—you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity. Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, *Computer Forensics* provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process—from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data. *Computer Forensics* is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

Cybercrime and Digital Forensics Feb 25 2022 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-bullying and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further 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 Forensics and Cyber Crime Nov 05 2022 This book contains a selection of thoroughly refereed and revised papers from the Second International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2010, held October 4-6, 2010 in Abu Dhabi, United Arab Emirates. The field of digital forensics is becoming increasingly important for law enforcement, network security, and information assurance. It is a multidisciplinary area that encompasses a number of fields, including law, computer science, finance, networking, data mining, and criminal justice. The 14 papers in this volume describe the various applications of this technology and cover a wide range of topics including law enforcement, disaster recovery, accounting frauds, homeland security, and information warfare.

Digital Forensics and Incident Response Jan 15 2021 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 Explained Aug 02 2022 This book covers the full life cycle of conducting a mobile and computer digital forensic examination, including planning and performing an investigation as well as report writing and testifying. Case reviews in corporate, civil, and criminal situations are also described from both prosecution and defense perspectives. Digital Forensics Explained, Second Edition draws from years of experience in local, state, federal, and international environments and highlights the challenges inherent in deficient cyber security practices. Topics include the importance of following the scientific method and verification, legal and ethical issues, planning an investigation (including tools and techniques), incident response, case project management and authorization, social media and internet, cloud, anti-forensics, link and visual analysis, and psychological considerations. The book is a valuable resource for the academic environment, law enforcement, those in the legal profession, and those working in the cyber security field. Case reviews include cyber security breaches, anti-forensic challenges, child exploitation, and social media investigations. Greg Gogolin, PhD, CISSP, is a Professor of Information Security and Intelligence at Ferris State University and a licensed Professional Investigator. He has worked more than 100 cases in criminal, civil, and corporate environments.

Digital Forensics with Open Source Tools Jul 01 2022 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

Implementing Digital Forensic Readiness Mar 29 2022 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 reducing 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.

Advances in Digital Forensics II Oct 04 2022 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.

Scene of the Cybercrime Aug 29 2019 When it comes to computer crimes, the criminals got a big head start. But the law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cybercrime cases. When the first edition of "Scene of the Cybercrime" published in 2002, it was one of the first books that educated IT security professionals and law enforcement how to fight Cybercrime. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cybercrime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cybercrime report: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybercrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandated by federal compliance regulations such as Sarbanes-Oxley, HIPAA, or the Payment Card Industry (PCI) Data Security Standard. *Scene of the Cybercrime, Second Edition* is a completely revised and updated book which covers all of the technological, legal, and regulatory changes, which have occurred since the first edition. The book is written for dual audience; IT security professionals and members of law enforcement. It gives the technical experts a little peek into the law enforcement world, a highly structured environment where the "letter of the law" is paramount and procedures must be followed closely lest an investigation be contaminated and all the evidence collected rendered useless. It also provides law enforcement officers with an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. *Scene of the Cybercrime, Second Edition* provides a roadmap that those on both sides of the table can use to navigate the legal and technical landscape to understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live. Also included is an all new chapter on Worldwide Forensics Acts and Laws. * Companion Web site provides custom tools and scripts, which readers can download for conducting digital, forensic investigations. * Special chapters outline how Cybercrime investigations must be reported and investigated by corporate IT staff to meet federal mandates from Sarbanes Oxley, and the Payment Card Industry (PCI) Data Security Standard * Details forensic investigative techniques for the most common operating systems (Windows, Linux and UNIX) as well as cutting edge devices including iPods, Blackberries, and cell phones.

Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice Jul 21 2021 As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice* addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

Learning iOS Forensics - Second Edition Apr 05 2020 A practical guide to analyzing iOS devices with the latest forensics tools and techniques
About This Book- This book is a comprehensive update to *Learning iOS Forensics*- This practical book will not only cover the critical aspects of digital forensics, but also mobile forensics- Whether you're a forensic analyst or an iOS developer, there's something in this book for you- The authors, Mattia Epifani and Pasquale Stirparo, are respected members of the community, they go into extensive detail to cover critical topics
Who This Book Is For The book is for digital forensics analysts, incident response analysts, IT security experts, and malware analysts. It would be beneficial if you have basic knowledge of forensics
What You Will Learn- Identify an iOS device between various models (iPhone, iPad, iPod Touch) and verify the iOS version installed- Crack or bypass the protection passcode chosen by the user- Acquire, at the most detailed level, the content of an iOS Device (physical, advanced logical, or logical)- Recover information from a local backup and eventually crack the backup password- Download back-up information stored on iCloud- Analyze system, user, and third-party information from a device, a backup, or iCloud- Examine malicious

apps to identify data and credential thefts
In Detail
Mobile forensics is used within many different domains, but is chiefly employed in the field of information security. By understanding common attack vectors and vulnerability points, security professionals can develop measures and examine system architectures to harden security on iOS devices. This book is a complete manual on the identification, acquisition, and analysis of iOS devices, updated to iOS 8 and 9. You will learn by doing, with various case studies. The book covers different devices, operating system, and apps. There is a completely renewed section on third-party apps with a detailed analysis of the most interesting artifacts. By investigating compromised devices, you can work out the identity of the attacker, as well as what was taken, when, why, where, and how the attack was conducted. Also you will learn in detail about data security and application security that can assist forensics investigators and application developers. It will take hands-on approach to solve complex problems of digital forensics as well as mobile forensics.
Style and approach
This book provides a step-by-step approach that will guide you through one topic at a time. This intuitive guide focuses on one key topic at a time. Building upon the acquired knowledge in each chapter, we will connect the fundamental theory and practical tips by illustrative visualizations and hands-on code examples.

Placing the Suspect Behind the Keyboard Nov 12 2020
Placing the Suspect Behind the Keyboard is the definitive book on conducting a complete investigation of a cybercrime using digital forensics techniques as well as physical investigative procedures. This book merges a digital analysis examiner's work with the work of a case investigator in order to build a solid case to identify and prosecute cybercriminals. Brett Shavers links traditional investigative techniques with high tech crime analysis in a manner that not only determines elements of crimes, but also places the suspect at the keyboard. This book is a first in combining investigative strategies of digital forensics analysis processes alongside physical investigative techniques in which the reader will gain a holistic approach to their current and future cybercrime investigations. Learn the tools and investigative principles of both physical and digital cybercrime investigations—and how they fit together to build a solid and complete case
Master the techniques of conducting a holistic investigation that combines both digital and physical evidence to track down the "suspect behind the keyboard"
The only book to combine physical and digital investigative techniques

Windows Registry Forensics Apr 17 2021
Windows Registry Forensics provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques are presented that take the student and analyst beyond the current use of viewers and into real analysis of data contained in the Registry, demonstrating the forensic value of the Registry. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this book is packed with real-world examples using freely available open source tools. It also includes case studies and a CD containing code and author-created tools discussed in the book. This book will appeal to computer forensic and incident response professionals, including federal government and commercial/private sector contractors, consultants, etc. Named a 2011 Best Digital Forensics Book by InfoSec Reviews
Packed with real-world examples using freely available open source tools
Deep explanation and understanding of the Windows Registry – the most difficult part of Windows to analyze forensically
Includes a CD containing code and author-created tools discussed in the book

Practical Mobile Forensics Oct 31 2019
The book is an easy-to-follow guide with clear instructions on various mobile forensic techniques. The chapters and the topics within are structured for a smooth learning curve, which will swiftly empower you to master mobile forensics. If you are a budding forensic analyst, consultant, engineer, or a forensic professional wanting to expand your skillset, this is the book for you. The book will also be beneficial to those with an interest in mobile forensics or wanting to find data lost on mobile devices. It will be helpful to be familiar with forensics in general but no prior experience is required to follow this book.

Computer Forensics Sep 10 2020
Updated to include the most current events and information on cyberterrorism, the second edition of Computer Forensics: Cybercriminals, Laws, and Evidence continues to balance technicality and legal analysis as it enters into the world of cybercrime by exploring what it is, how it is investigated, and the regulatory laws around the collection and use of electronic evidence. Students are introduced to the technology involved in computer forensic investigations and the technical and legal difficulties involved in searching, extracting, maintaining, and storing electronic evidence, while simultaneously looking at the legal implications of such investigations and the rules of legal procedure relevant to electronic evidence. Significant and current computer forensic developments are examined, as well as the implications for a variety of fields including computer science, security, criminology, law, public policy, and administration.

Digital Forensics for Legal Professionals Jul 09 2020
Section 1: What is Digital Forensics? Chapter 1. Digital Evidence is Everywhere Chapter 2. Overview of Digital Forensics Chapter 3. Digital Forensics -- The Sub-Disciplines Chapter 4. The Foundations of Digital Forensics -- Best Practices Chapter 5. Overview of Digital Forensics Tools Chapter 6. Digital Forensics at Work in the Legal System
Section 2: Experts Chapter 7. Why Do I Need an Expert? Chapter 8. The Difference between Computer Experts and Digital Forensic Experts Chapter 9. Selecting a Digital Forensics Expert Chapter 10. What to Expect from an Expert Chapter 11.

Approaches by Different Types of Examiners Chapter 12. Spotting a Problem Expert Chapter 13. Qualifying an Expert in Court Sections 3: Motions and Discovery Chapter 14. Overview of Digital Evidence Discovery Chapter 15. Discovery of Digital Evidence in Criminal Cases Chapter 16. Discovery of Digital Evidence in Civil Cases Chapter 17. Discovery of Computers and Storage Media Chapter 18. Discovery of Video Evidence Ch ...

Digital Evidence and Computer Crime Jun 19 2021 Though an increasing number of criminals are using computers and computer networks, few investigators are well versed in the issues related to digital evidence. This work explains how computer networks function and how they can be used in a crime.

Hacking Exposed Computer Forensics, Second Edition Aug 22 2021 "Provides the right mix of practical how-to knowledge in a straightforward, informative fashion that ties it all the complex pieces together with real-world case studies. ...Delivers the most valuable insight on the market. The authors cut to the chase of what people must understand to effectively perform computer forensic investigations." --Brian H. Karney, COO, AccessData Corporation The latest strategies for investigating cyber-crime Identify and investigate computer criminals of all stripes with help from this fully updated. real-world resource. Hacking Exposed Computer Forensics, Second Edition explains how to construct a high-tech forensic lab, collect prosecutable evidence, discover e-mail and system file clues, track wireless activity, and recover obscured documents. Learn how to re-create an attacker's footsteps, communicate with counsel, prepare court-ready reports, and work through legal and organizational challenges. Case studies straight from today's headlines cover IP theft, mortgage fraud, employee misconduct, securities fraud, embezzlement, organized crime, and consumer fraud cases. Effectively uncover, capture, and prepare evidence for investigation Store and process collected data in a highly secure digital forensic lab Restore deleted documents, partitions, user activities, and file systems Analyze evidence gathered from Windows, Linux, and Macintosh systems Use the latest Web and client-based e-mail tools to extract relevant artifacts Overcome the hacker's anti-forensic, encryption, and obscurity techniques Unlock clues stored in cell phones, PDAs, and Windows Mobile devices Prepare legal documents that will hold up to judicial and defense scrutiny

Computer Forensics InfoSec Pro Guide Jan 03 2020 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

Digital Forensics and Incident Response - Second Edition Sep 30 2019 Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book Description An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident

response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

Cyber Forensics Dec 26 2021 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

Security, Privacy, and Digital Forensics in the Cloud Oct 24 2021 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.

Digital Forensics and Cyber Crime Aug 10 2020 The First International Conference on Digital Forensics and Cyber Crime (ICDF2C) was held in Albany from September 30 to October 2, 2009. The field of digital forensics is growing rapidly with implications for several fields including law enforcement, network security, disaster recovery and accounting. This is a multidisciplinary area that requires expertise in several areas including, law, computer science, finance, networking, data mining, and criminal justice. This conference brought together practitioners and researchers from diverse fields providing opportunities for business and intellectual engagement among attendees. All the conference sessions were very well attended with vigorous discussions and strong audience interest. The conference featured an excellent program comprising high-quality presentations and invited speakers from all around the world. The first day featured a plenary session including George Philip, President of University at Albany, Harry Corbit, Superintendent of New York State Police, and William Pelgrin, Director of New York State Office of Cyber Security and Critical Infrastructure Coordination. An outstanding keynote was provided by Miklos Vasarhelyi on continuous auditing. This was followed by two parallel sessions on accounting fraud /financial crime, and multimedia and handheld forensics. The second day of the conference featured a mesmerizing keynote talk by Nitesh Dhanjani from Ernst and Young that focused on psychological profiling based on open source intelligence from social network analysis. The third day of the conference featured both basic and advanced tutorials on open source forensics.

Cyber Crime and Forensic Computing Jul 29 2019 This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication

streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.