

Forensic Data Recovery From Flash Memory

This timely text/reference presents a detailed introduction to the essential aspects of computer network forensics. The book considers not only how to uncover information hidden in email messages, web pages and web servers, but also what this reveals about the functioning of the Internet and its core protocols. This, in turn, enables the identification of shortcomings and highlights where improvements can be made for a more secure network. Topics and features: provides learning objectives in every chapter, and review questions throughout the book to test understanding; introduces the basic concepts of network process models, network forensics frameworks and network forensics tools; discusses various techniques for the acquisition of packets in a network forensics system, network forensics analysis, and attribution in network forensics; examines a range of advanced topics, including botnet, smartphone, and cloud forensics; reviews a number of freely available tools for performing forensic activities.

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.

Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical Deluxe Study Guide Covers 100% of exam objectives including threats, attacks, and vulnerabilities; technologies and tools; architecture and design; identity and access management; risk management; cryptography and PKI, and much more... Includes interactive online learning environment and study tools with: 4 custom practice exams 100 Electronic Flashcards Searchable key term glossary Plus 33 Online Security+ Practice Lab Modules Expert Security+ SY0-601 exam preparation--Now with 33 Online Lab Modules The Fifth edition of CompTIA Security+ Deluxe Study Guide offers invaluable preparation for Exam SY0-601. Written by expert authors, Mike Chapple and David Seidl, the book covers 100% of the exam objectives with clear and concise explanations. Discover how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while gaining and understanding the role of architecture and design. Spanning topics from everyday tasks like identity and access management to complex subjects such as risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Illustrative examples show how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-the-job application. Coverage of 100% of all exam objectives in this Study Guide means you'll be ready for: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance Interactive learning environment Take your exam prep to the next level with Sybex's superior interactive online study tools. To access our learning environment, simply visit www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and instantly gain one year of FREE access after activation to: Interactive test bank with 4 bonus exams. Practice questions help you identify areas where further review is needed. 100 Electronic Flashcards to reinforce learning and last-minute prep before the exam. Comprehensive glossary in PDF format gives you instant access to the key terms so you are fully prepared. ABOUT THE PRACTICE LABS SECURITY+ LABS So you can practice with hands-on learning in a real environment, Sybex has bundled Practice Labs virtual labs that

run from your browser. The registration code is included with the book and gives you 6 months unlimited access to Practice Labs CompTIA Security+ Exam SY0-601 Labs with 33 unique lab modules to practice your skills.

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

PBX Security and Forensics presents readers with theoretical and practical background for Private Branch Exchanges (PBXs). PBX is privately owned equipment that serve the communication needs of a private or public entity making connections among internal telephones and linking them to other users in the Public Switched Telephone Network (PSTN). Targeted damages and attacks in PBXs can cause significant instability and problems. The author provides examples of these threats and how to prevent against such attacks in the future. Readers will also be shown where to find forensics data and how to conduct relevant analysis.

This book presents recent applications and approaches as well as challenges in digital forensic science. One of the evolving challenges that is covered in the book is the cloud forensic analysis which applies the digital forensic science over the cloud computing paradigm for conducting either live or static investigations within the cloud environment. The book also covers the theme of multimedia forensics and watermarking in the area of information security. That includes highlights on intelligence techniques designed for detecting significant changes in image and video sequences. Moreover, the theme proposes recent robust and computationally efficient digital watermarking techniques. The last part of the book provides several digital forensics related applications, including areas such as evidence acquisition enhancement, evidence evaluation, cryptography, and finally, live investigation through the importance of reconstructing the botnet attack scenario to show the malicious activities and files as evidences to be presented in a court.

Mobile Phone Security and Forensics provides both theoretical and practical background of security and forensics for mobile phones. The author discusses confidentiality, integrity, and availability threats in mobile telephones to provide background for the rest of the book. Security and secrets of mobile phones are discussed including software and hardware interception, fraud and other malicious techniques used “against” users. The purpose of this book is to raise user awareness in regards to security and privacy threats present in the use of mobile phones while readers will also learn where forensics data reside in the mobile phone and the network and how to conduct a relevant analysis.

In this book, the editors explain how students enrolled in two digital forensic courses at their institution are exposed to experiential learning opportunities, where the students acquire the knowledge and skills of the subject-matter while also learning how to adapt to the ever-changing digital forensic landscape. Their findings (e.g., forensic examination of different IoT devices) are also presented in the book. Digital forensics is a topic of increasing importance as our society becomes “smarter” with more of the “things” around us being internet- and inter-connected (e.g., Internet of Things (IoT) and smart home devices); thus, the increasing likelihood that we will need to acquire data from these things in a forensically sound manner. This book is of interest to both digital forensic educators and digital forensic practitioners, as well as students seeking to learn about digital forensics.

Kali - Computer Forensics Data Recovery 101 - TrainingJeremy Martin

Forensic Accounting provides comprehensive coverage of fraud detection and deterrence and includes the broader educational material of the forensic accounting field with all the necessary accompaniments. The text follows the model curriculum for education in fraud and forensic funded by the U.S. national Institute of Justice and developed by a Technical Working Group of experts in the field. The text serves as a comprehensive and authoritative resource for teaching forensic accounting concepts and procedures that is also and appropriate and pedagogically ready for class room use. This easy to read, comprehensive textbook includes case study examples to clearly explain technical concepts and bring the material to life. 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.

This book constitutes the refereed proceedings of the 18th International Conference on Information Security, ISC 2015, held in Trondheim, Norway, in September 2015. The 30 revised full papers presented were carefully reviewed and selected from 103 submissions. The papers cover a wide range of topics in the area of cryptography and cryptanalysis and are organized in the following topical sections: signatures; system and software security; block ciphers; protocols; network and cloud security; encryption and fundamentals; PUFs and implementation security; and key generation, biometrics and image security.

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.

Welcome to the proceedings of the 10th Pacific Rim Conference on Multimedia (PCM 2009)

held in Bangkok, Thailand, December 15-18, 2009. Since its inception in 2000, PCM has rapidly grown into a major conference on multimedia in the Asia-Pacific Rim region and has built up its reputation around the world. Following the success of the preceding conferences, PCM 2008 in Taiwan, PCM 2007 in Hong Kong, PCM 2006 in China, PCM 2005 in Korea, PCM 2004 in Japan, PCM 2003 in Singapore, PCM 2002 in Taiwan, PCM 2001 in China, and PCM 2000 in Australia, the tenth PCM brought researchers, developers, practitioners, and educators together to disseminate their new discoveries in the field of multimedia. Theoretical breakthroughs and practical systems were presented at this conference, thanks to the support of Naresuan University, Mahanakorn University of Technology, and the IEEE Thailand Section. PCM 2009 featured a comprehensive program including keynote talks, regular presentations, posters, and special sessions. We received 171 papers from 16 countries including Australia, Sweden, Germany, Italy, Iran, France, Canada, China, Japan, Korea, Malaysia, Singapore, Taiwan, Hong Kong, the UK, and the USA. After a rigorous review process, we accepted only 67 oral presentations and 45 poster presentations. Four special sessions were also organized by world-leading researchers.

Computer Forensics: Evidence Collection and Management examines cyber-crime, E-commerce, and Internet activities that could be used to exploit the Internet, computers, and electronic devices. The book focuses on the numerous vulnerabilities and threats that are inherent on the Internet and networking environments and presents techniques and suggestions for corporate security personnel, investigators, and forensic examiners to successfully identify, retrieve, and protect valuable forensic evidence for litigation and prosecution. The book is divided into two major parts for easy reference. The first part explores various crimes, laws, policies, forensic tools, and the information needed to understand the underlying concepts of computer forensic investigations. The second part presents information relating to crime scene investigations and management, disk and file structure, laboratory construction and functions, and legal testimony. Separate chapters focus on investigations involving computer systems, e-mail, and wireless devices. Presenting information patterned after technical, legal, and managerial classes held by computer forensic professionals from Cyber Crime Summits held at Kennesaw State University in 2005 and 2006, this book is an invaluable resource for those who want to be both efficient and effective when conducting an investigation.

This is the official CHFI (Computer Hacking Forensics Investigator) study guide for professionals studying for the forensics exams and for professionals needing the skills to identify an intruder's footprints and properly gather the necessary evidence to prosecute. The EC-Council offers certification for ethical hacking and computer forensics. Their ethical hacker exam has become very popular as an industry gauge and we expect the forensics exam to follow suit. Material is presented in a logical learning sequence: a section builds upon previous sections and a chapter on previous chapters. All concepts, simple and complex, are defined and explained when they appear for the first time. This book includes: Exam objectives covered in a chapter are clearly explained in the beginning of the chapter, Notes and Alerts highlight crucial points, Exam's Eye View emphasizes the important points from the exam's perspective, Key Terms present definitions of key terms used in the chapter, Review Questions contains the questions modeled after real exam questions based on the material covered in the chapter. Answers to the questions are presented with explanations. Also included is a full practice exam modeled after the real exam. The only study guide for CHFI, provides 100% coverage of all exam objectives. CHFI Training runs hundreds of dollars for self tests to thousands of dollars for classroom training.

This thesis explores the forensic opportunities afforded by flash memory. It starts with a discussion of flash storage starting with the physics of flash devices, the development of flash translation layers (which allow flash devices to be used with unmodified legacy

operating systems), and flash file systems (which provide for better utilization of flash storage at a somewhat higher cost). Then this thesis provides a comprehension survey of the relevant academic literature and evaluates the work that others have done in the field of flash data recovery. It provides a theory of circumstances when residual data may exist on flash memory through the intentional deletion and overwrite of previously saved data, based upon a thorough patent review and freely available documentation. It clearly documents the steps of configuring a Linux kernel to use the YAFFS2 (Yet Another Flash File System used in Android) and the JFFS2 (the Journaling Flash File System used on the One Laptop per Child Program) flash file systems. It then conducts experiments to confirm or deny these theories, with a focus on the recovery of data and other evidence that overwritten and deleted data once existed. Finally, this thesis makes recommendations for further research.

Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical study guide The Eighth Edition of the CompTIA Security+ Study Guide Exam SY0-601 efficiently and comprehensively prepares you for the SY0-601 Exam. Accomplished authors and security experts Mike Chapple and David Seidl walk you through the fundamentals of crucial security topics, including the five domains covered by the SY0-601 Exam: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance The study guide comes with the Sybex online, interactive learning environment that includes a pre-assessment test, hundreds of review questions, practice exams, flashcards, and a glossary of key terms. The book is written in a practical and straightforward manner, ensuring you can easily learn and retain the material. Perfect for everyone planning to take the SY0-601 Exam—as well as those who hope to secure a high-level certification like the CASP+, CISSP, or CISA—the study guide also belongs on the bookshelves of everyone who has ever wondered if the field of IT security is right for them. It's a must-have reference!

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics VIII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, mobile phone forensics, cloud forensics, network forensics, and advanced forensic techniques. This book is the eighth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-two edited papers from the Eighth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the University of

Pretoria, Pretoria, South Africa in the spring of 2012. *Advances in Digital Forensics VIII* is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoj is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

The Computer Forensic Series by EC-Council provides the knowledge and skills to identify, track, and prosecute the cyber-criminal. The series is comprised of four books covering a broad base of topics in Computer Hacking Forensic Investigation, designed to expose the reader to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Learners are introduced to advanced techniques in computer investigation and analysis with interest in generating potential legal evidence. In full, this and the other three books provide preparation to identify evidence in computer related crime and abuse cases as well as track the intrusive hacker's path through a client system. The series and accompanying labs help prepare the security student or professional to profile an intruder's footprint and gather all necessary information and evidence to support prosecution in a court of law. *File and Operating Systems, Wireless Networks, and Storage* provides a basic understanding of file systems, storage and digital media devices. *Boot processes, Windows and Linux Forensics* and application of password crackers are all discussed. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. 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 paper 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.

Become an effective cyber forensics investigator and gain a collection of practical, efficient techniques to get the job done. Diving straight into a discussion of anti-forensic

techniques, this book shows you the many ways to effectively detect them. Now that you know what you are looking for, you'll shift your focus to network forensics, where you cover the various tools available to make your network forensics process less complicated. Following this, you will work with cloud and mobile forensic techniques by considering the concept of forensics as a service (FaSS), giving you cutting-edge skills that will future-proof your career. Building on this, you will learn the process of breaking down malware attacks, web attacks, and email scams with case studies to give you a clearer view of the techniques to be followed. Another tricky technique is SSD forensics, so the author covers this in detail to give you the alternative analysis techniques you'll need. To keep you up to speed on contemporary forensics, Practical Cyber Forensics includes a chapter on Bitcoin forensics, where key crypto-currency forensic techniques will be shared. Finally, you will see how to prepare accurate investigative reports. What You Will Learn Carry out forensic investigation on Windows, Linux, and macOS systems Detect and counter anti-forensic techniques Deploy network, cloud, and mobile forensics Investigate web and malware attacks Write efficient investigative reports Who This Book Is For Intermediate infosec professionals looking for a practical approach to investigative cyber forensics techniques.

This 2-volume set constitutes the thoroughly refereed post-conference proceedings of the 10th International Conference on Security and Privacy in Communication Networks, SecureComm 2014, held in Beijing, China, in September 2014. The 27 regular and 17 short papers presented were carefully reviewed. It also presents 22 papers accepted for four workshops (ATCS, SSS, SLSS, DAPRO) in conjunction with the conference, 6 doctoral symposium papers and 8 poster papers. The papers are grouped in the following topics: security and privacy in wired, wireless, mobile, hybrid, sensor, ad hoc networks; network intrusion detection and prevention, firewalls, packet filters; malware, and distributed denial of service; communication privacy and anonymity; network and internet forensics techniques; public key infrastructures, key management, credential management; secure routing, naming/addressing, network management; security and privacy in pervasive and ubiquitous computing; security & privacy for emerging technologies: VoIP, peer-to-peer and overlay network systems; security & isolation in data center networks; security & isolation in software defined networking.

Learn to pull "digital fingerprints from alternate data storage (ADS) devices including: iPod, Xbox, digital cameras and more from the cyber sleuths who train the Secret Service, FBI, and Department of Defense in bleeding edge digital forensics techniques. This book sets a new forensic methodology standard for investigators to use. This book begins by describing how alternate data storage devices are used to both move and hide data. From here a series of case studies using bleeding edge forensic analysis tools demonstrate to readers how to perform forensic investigations on a variety of ADS devices including: Apple iPods, Digital Video Recorders, Cameras, Gaming Consoles (Xbox, PS2, and PSP), Bluetooth devices, and more using state of the art tools. Finally, the book takes a look into the future at "not yet every day devices which will soon be common repositories for hiding and moving data for both legitimate and illegitimate purposes. Authors are undisputed leaders who train the Secret Service, FBI, and Department of Defense Book presents "one of a kind" bleeding edge information that absolutely can not be found anywhere else Today the industry has exploded and cyber investigators can be found in almost every field

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. *Advances in Digital Forensics VII* describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Forensic Techniques, Fraud and Malware Investigations, Network Forensics, and Advanced Forensic Techniques. This book is the 7th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of 21 edited papers from the 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, USA in the spring of 2011. *Advances in Digital Forensics VII* is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma, USA.

The widespread use of information and communications technology (ICT) has created a global platform for the exchange of ideas, goods and services, the benefits of which are enormous. However, it has also created boundless opportunities for fraud and deception. Cybercrime is one of the biggest growth industries around the globe, whether it is in the form of violation of company policies, fraud, hate crime, extremism, or terrorism. It is therefore paramount that the security industry raises its game to combat these threats. Today's top priority is to use computer technology to fight computer crime, as our commonwealth is protected by firewalls rather than firepower. This is an issue of global importance as new technologies have provided a world of opportunity for criminals. This book is a compilation of the collaboration between the researchers and practitioners in the security field; and provides a comprehensive literature on current and future e-security needs across applications, implementation, testing or investigative techniques, judicial processes and criminal intelligence. The intended audience includes members in academia, the public and private sectors, students and those who are interested in and will benefit from this handbook.

Flash memories and memory systems are key resources for the development of electronic products implementing converging technologies or exploiting solid-state memory disks. This book illustrates state-of-the-art technologies and research studies on Flash memories. Topics in modeling, design, programming, and materials for memories are covered along with real application examples.

This is a training lab covering forensic data recovery using Kali linux

If you are a forensic analyst or an information security professional wanting to develop your knowledge of Android forensics, then this is the book for you. Some basic knowledge of the Android mobile platform is expected.

Cell phones and Personal Digital Assistants (PDAs) have become indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used not only for voice calls, simple text messages, and Personal Information Management (PIM),

but also for many functions done at a desktop computer. While these devices provide productivity benefits, they also pose new risks. This document is intended to assist organizations in securing cell phones and PDAs. More specifically, this document describes in detail the threats faced by organizations that employ handheld devices and the measures that can be taken to counter those threats.

The need to professionally and successfully conduct computer forensic investigations of incidents and crimes has never been greater. This has caused an increased requirement for information about the creation and management of computer forensic laboratories and the investigations themselves. This includes a great need for information on how to cost-effectively establish and manage a computer forensics laboratory. This book meets that need: a clearly written, non-technical book on the topic of computer forensics with emphasis on the establishment and management of a computer forensics laboratory and its subsequent support to successfully conducting computer-related crime investigations. Provides guidance on creating and managing a computer forensics lab Covers the regulatory and legislative environment in the US and Europe Meets the needs of IT professionals and law enforcement as well as consultants

This book constitutes the refereed proceedings of the 8th International Conference on Wireless Algorithms, Systems, and Applications, WASA 2013, held in Zhangjiajie, China, in August 2013. The 25 revised full papers presented together with 18 invited papers were carefully reviewed and selected from 80 submissions. The papers cover the following topics: effective and efficient state-of-the-art algorithm design and analysis, reliable and secure system development and implementations, experimental study and testbed validation, and new application exploration in wireless networks.

This book begins with an introduction to PBXs (Private Branch Exchanges) and the scene, statistics and involved actors. It discusses confidentiality, integrity and availability threats in PBXs. The author examines the threats and the technical background as well as security and forensics involving PBXs. The purpose of this book is to raise user awareness in regards to security and privacy threats present in PBXs, helping both users and administrators safeguard their systems. The new edition includes a major update and extension to the VoIP sections in addition to updates to forensics.

Approximately 80 percent of the worlds population now owns a cell phone, which can hold evidence or contain logs about communications concerning a crime. Cameras, PDAs, and GPS devices can also contain information related to corporate policy infractions and crimes. Aimed to prepare investigators in the public and private sectors, Digital Forensics

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

The Second International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2009) took place in Adelaide, South Australia during January 19-21, 2009, at the Australian National Wine Centre, University of Adelaide. In addition to the peer-reviewed academic papers presented in this volume, the conference featured a significant number of plenary contributions from recognized national and international leaders in digital forensic investigation. Keynote speaker Andy Jones, head of security research at British Telecom, outlined the emerging challenges of investigation as new devices enter the market. These include the impact of solid-state memory, ultra-portable devices, and distributed storage – also known as cloud computing. The plenary session on Digital Forensics Practice included Troy O'Malley, Queensland Police Service, who outlined the paperless case file system now in use in Queensland, noting that efficiency and efficacy gains in using the system have now meant that police can arrive at a suspect's home before the suspect! Joseph Razik, representing Patrick Perrot of the Institut de Recherche Criminelle de la Gendarmerie Nationale, France, summarized research activities in speech, image, video and multimedia at the IRCGN. The plenary session on The Interaction Between Technology and Law brought a legal perspective to the technological challenges of digital forensic investigation.

This new edition provides both theoretical and practical background of security and forensics for mobile phones. The author discusses confidentiality, integrity, and availability threats in mobile telephones to provide background for the rest of the book. Security and secrets of mobile phones are discussed including software and hardware interception, fraud and other malicious techniques used “against” users. The purpose of this book is to raise user awareness in regards to security and privacy threats present in the use of mobile phones while readers will also learn where forensics data reside in the mobile phone and the network and how to conduct a relevant analysis. The information on denial of service attacks has been thoroughly updated for the new edition. Also, a major addition

to this edition is a section discussing software defined radio and open source tools for mobile phones.

A comprehensive guide to Android forensics, from setting up the workstation to analyzing key artifacts
Key Features
Get up and running with modern mobile forensic strategies and techniques
Analyze the most popular Android applications using free and open source forensic tools
Learn malware detection and analysis techniques to investigate mobile cybersecurity incidents
Book Description
Many forensic examiners rely on commercial, push-button tools to retrieve and analyze data, even though there is no tool that does either of these jobs perfectly.

Learning Android Forensics will introduce you to the most up-to-date Android platform and its architecture, and provide a high-level overview of what Android forensics entails. You will understand how data is stored on Android devices and how to set up a digital forensic examination environment. As you make your way through the chapters, you will work through various physical and logical techniques to extract data from devices in order to obtain forensic evidence. You will also learn how to recover deleted data and forensically analyze application data with the help of various open source and commercial tools. In the concluding chapters, you will explore malware analysis so that you'll be able to investigate cybersecurity incidents involving Android malware. By the end of this book, you will have a complete understanding of the Android forensic process, you will have explored open source and commercial forensic tools, and will have basic skills of Android malware identification and analysis. What you will learn
Understand Android OS and architecture
Set up a forensics environment for Android analysis
Perform logical and physical data extractions
Learn to recover deleted data
Explore how to analyze application data
Identify malware on Android devices
Analyze Android malware
Who this book is for
If you are a forensic analyst or an information security professional wanting to develop your knowledge of Android forensics, then this is the book for you. Some basic knowledge of the Android mobile platform is expected.

As future generation information technology (FGIT) becomes specialized and fragmented, it is easy to lose sight that many topics in FGIT have common threads and, because of this, advances in one discipline may be transmitted to others. Presentation of recent results obtained in different disciplines encourages this interchange for the advancement of FGIT as a whole. Of particular interest are hybrid solutions that combine ideas taken from multiple disciplines in order to achieve something more significant than the sum of the individual parts. Through such hybrid philosophy, a new principle can be discovered, which has the propensity to propagate throughout multifaceted disciplines. FGIT 2009 was the first mega-conference that attempted to follow the above idea of hybridization in FGIT in a form of multiple events related to particular disciplines of IT, conducted by separate scientific committees, but coordinated in order to expose the most important contributions. It included the following international conferences:
Advanced Software Engineering and Its Applications (ASEA), Bio-Science and

Bio- Technology (BSBT), Control and Automation (CA), Database Theory and Appli- tion (DTA), Disaster Recovery and Business Continuity (DRBC; published indepe- ently), Future Generation Communication and Networking (FGCN) that was c- bined with Advanced Communication and Networking (ACN), Grid and Distributed Computing (GDC), Multimedia, Computer Graphics and Broadcasting (MulGraB), Security Technology (SecTech), Signal Processing, Image Processing and Pattern Recognition (SIP), and u- and e-Service, Science and Technology (UNESST).

This book contains extended and revised versions of the best papers presented at the 27th IFIP WG 10.5/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2019, held in Cusco, Peru, in October 2019. The 15 full papers included in this volume were carefully reviewed and selected from the 28 papers (out of 82 submissions) presented at the conference. The papers discuss the latest academic and industrial results and developments as well as future trends in the field of System-on-Chip (SoC) design, considering the challenges of nano-scale, state-of-the-art and emerging manufacturing technologies. In particular they address cutting-edge research fields like heterogeneous, neuromorphic and brain-inspired, biologically-inspired, approximate computing systems.

[Copyright: 6a99623889645c73f4e36ea93f707ac8](https://doi.org/10.1007/978-1-4939-9888-8)