Mobile Phone Security And Forensics A Practical Approach Springerbriefs In Electrical And Computer Engineering

JAMARI GREYSON

Mobile Network Forensics: Emerging Research and Opportunities Springer
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.
Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, Second Edition IGI Global
Seeking the Truth from Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations will assist those who have never collected mobile evidence and augment the work of professionals who are not currently performing advanced destructive techniques. This book is intended for any professional that is interested in pursuing work that involves mobile forensics, and is designed around the outcomes of criminal investigations that involve mobile digital evidence. Author John Bair brings to life the techniques and concepts that can assist those in the private or corporate sector. Mobile devices have always been very dynamic in nature. They have also become an integral part of our lives, and often times, a digital representation of where we are, who we communicate with and what we document around us. Because they constantly change features, allow user enabled security, and or encryption, those employed with extracting user data are often overwhelmed with the process. This book presents a complete guide to mobile device forensics, written in an easy to understand format. Provides readers with basic, intermediate, and advanced mobile forensic concepts and methodology Thirty overall chapters which include such topics as, preventing evidence contamination,

triaging devices, troubleshooting, report writing, physical memory and encoding, date and time stamps, decoding Multi-Media-Messages, decoding unsupported application data, advanced validation, water damaged phones, Joint Test Action Group (JTAG), Thermal and Non-Thermal chip removal, BGA cleaning and imaging, In-System-Programming (ISP), and more Popular JTAG boxes – Z3X and RIFF/RIFF2 are expanded on in detail Readers have access to the companion guide which includes additional image examples, and other useful materials

Mobile Malware Attacks and Defense Penerbit Andi

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.

Mastering Mobile Forensics Packt Publishing Ltd

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.

Practical Mobile Forensics Packt Publishing Ltd

Mobile technologies have become a staple in society for their accessibility and diverse range of applications that are continually growing and advancing. Users are increasingly using these devices for activities beyond simple communication including gaming and e-commerce and to access confidential information including banking accounts and medical records. While mobile devices are being so widely used and accepted in daily life, and subsequently housing more and more personal data, it is evident that the security of these devices is paramount. As mobile applications now create easy access to personal information, they can incorporate location tracking services, and data collection can happen discreetly behind the scenes. Hence, there needs to be more security and privacy measures enacted to ensure that mobile technologies can be used safely. Advancements in trust and privacy, defensive strategies, and steps for securing the device are important foci as mobile technologies are highly popular and rapidly developing. The Research Anthology on Securing Mobile Technologies and Applications discusses the strategies, methods, and technologies being employed for security amongst mobile devices and applications. This comprehensive book explores the security support that needs to be required on mobile devices to avoid application damage, hacking, security breaches and attacks, or unauthorized accesses to personal data. The chapters cover the latest technologies that are being used such as cryptography, verification systems, security policies and contracts, and general network security procedures along with a look into cybercrime and forensics. This book is essential for software engineers, app developers, computer scientists, security and IT professionals, practitioners, stakeholders, researchers, academicians, and students interested in how mobile technologies and applications are implementing security protocols and tactics amongst devices.

Handbook of Research on Cyber Crime and Information Privacy IGI Global

Telepon seluler atau mobile phone sudah menjadi bagian dari kehidupan sehari-hari manusia modern saat ini. Penggunaan telepon seluler untuk memenuhi kebutuhan individu dan organisasi menjadikan data yang terkait telepon seluluer sangat beragam, dengan jumlah yang semakin hari semakin banyak dan bersifat pribadi.Kebutuhan akan penyajian data digital dari telepon seluler baik untuk keperluan litigasi dan non-litigasi membuat para penegak hukum dan fraud examiner membutuhkan teknik, prosedur, dan peralatan yang dapat mendukung kegiatan perolehan, analisis, penyimpanan, dan penyajian data digital terkait telepon seluler yang memenuhi aspek legal yang berlaku. Oleh karena itu, mobile phone forensics sebagai bagian dari ilmu digital forensics dikembangkan untuk memenuhi kebutuhan spesifik tersebut.

Guidelines on Cell Phone Forensics IGI Global

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications comprehensively discusses the implications of cloud (storage) services and mobile applications on digital forensic investigations. The book provides both digital forensic practitioners and researchers with an up-to-date and advanced knowledge of collecting and preserving electronic evidence from different types of cloud services, such as digital remnants of cloud applications accessed through mobile devices. This is the first book that covers the investigation of a wide range of cloud services. Dr. Kim-Kwang Raymond Choo and Dr. Ali Dehghantanha are leading researchers in cloud and mobile security and forensics, having organized research, led research, and been published widely in the field. Users will gain a deep overview of seminal research in the field while also identifying prospective future research topics and open challenges. Presents the most current, leading edge research on cloud and mobile application forensics, featuring a panel of top experts in the field Introduces the first book to provide an in-depth overview of the issues surrounding digital forensic investigations in cloud and associated mobile apps Covers key technical topics and provides readers with a complete understanding of the most current research findings Includes discussions on future research directions and challenges

Advanced Research in Applied Artificial Intelligence CRC Press

Mobile Phone Security and ForensicsSpringer

Cyber Security and Digital Forensics

Mobile Phone Security and Forensics

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

Mastering Mobile Forensics Packt Publishing Ltd

This book constitutes the refereed proceedings of the 27th IFIP TC 11 International Information Security Conference, SEC 2012, held in Heraklion, Crete, Greece, in June 2012. The 42 revised full papers presented together with 11 short papers were carefully reviewed and selected from 167 submissions. The papers are organized in topical sections on attacks and malicious code, security architectures, system security, access control, database security, privacy attitudes and properties, social networks and social engineering, applied cryptography, anonymity and trust, usable security, security and trust models, security economics, and authentication and delegation.

Security and Privacy Protection in Information Processing Systems IGI Global

A comprehensive guide to Android forensics, from setting up the workstation to analyzing key artifacts Key FeaturesGet up and running with modern mobile forensic strategies and techniquesAnalyze the most popular Android applications using free and open source forensic toolsLearn malware detection and analysis techniques to investigate mobile cybersecurity incidentsBook 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 learnUnderstand Android OS and architectureSet up a forensics environment for Android analysisPerform logical and physical data extractionsLearn to recover deleted dataExplore how to analyze application dataIdentify malware on Android devicesAnalyze Android malwareWho 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.

Digital Forensics for Handheld Devices Springer

Master powerful strategies to acquire and analyze evidence from real-life scenarios About This Book A straightforward guide to address the roadblocks face when doing mobile forensics Simplify mobile forensics using the right mix of methods, techniques, and tools Get valuable advice to put you in the mindset of a forensic professional, regardless of your career level or experience Who This Book Is For This book is for forensic analysts and law enforcement and IT security officers who have to deal with digital evidence as part of their daily job. Some basic familiarity with digital forensics is assumed, but no experience with mobile forensics is required. What You Will Learn Understand the challenges of mobile forensics Grasp how to properly deal with digital evidence Explore the types of evidence available on iOS, Android, Windows, and BlackBerry mobile devices Know what forensic outcome to expect under given circumstances Deduce when and how to apply physical, logical, over-the-air, or low-level (advanced) acquisition methods Get in-depth knowledge of the different acquisition methods for all major mobile platforms Discover important mobile acquisition tools and techniques for all of the major platforms In Detail Investigating digital media is impossible without forensic tools. Dealing with complex forensic problems requires the use of dedicated tools, and even more importantly, the right strategies. In this book, you'll learn strategies and methods to deal with information stored on smartphones and tablets and see how to put the right tools to work. We begin by helping you understand the concept of mobile devices as a source of valuable evidence. Throughout this book, you will explore strategies and "plays" and decide when to use each technique. We cover important techniques such as seizing techniques to shield the device, and acquisition techniques including physical acquisition (via a USB connection), logical acquisition via data backups, over-the-air acquisition. We also explore cloud analysis, evidence discovery and data analysis, tools for mobile forensics, and tools to help you discover and analyze evidence. By the end of the book, you will have a better understanding of the tools and methods used to deal with the challenges of acquiring, preserving, and extracting evidence stored on smartphones, tablets, and the cloud. Style and approach This book takes a unique strategy-based approach, executing them on real-world scenarios. You will be introduced to thinking in terms of "game plans," which are essential to succeeding in analyzing evidence and conducting investigations.

Forensic Investigations and Risk Management in Mobile and Wireless Communications Packt Publishing

Modern communications are now more than ever heavily dependent on mobile networks, creating the potential for higher incidents of sophisticated crimes, terrorism acts, and high impact cyber security breaches. Disrupting these unlawful actions requires a number of digital forensic principles and a comprehensive investigation process. Mobile Network Forensics: Emerging Research and Opportunities is an essential reference source that discusses investigative trends in mobile devices and the internet of things, examining malicious mobile network traffic and traffic irregularities, as well as software-defined

mobile network backbones. Featuring research on topics such as lawful interception, system architecture, and networking environments, this book is ideally designed for forensic practitioners, government officials, IT consultants, cybersecurity analysts, researchers, professionals, academicians, and students seeking coverage on the technical and legal aspects of conducting investigations in the mobile networking environment.

Practical Mobile Forensics Packt Publishing Ltd

This volume constitutes the thoroughly refereed conference proceedings of the 25th International Conference on Industrial Engineering and Other Applications of Applied Intelligend Systems, IEA/AIE 2012, held in Dalian, China, in June 2012. The total of 82 papers selected for the proceedings were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on machine learning methods; cyber-physical system for intelligent transportation applications; AI applications; evolutionary algorithms, combinatorial optimization; modeling and support of cognitive and affective human processes; natural language processing and its applications; social network and its applications; mission-critical applications and case studies of intelligent systems; AI methods; sentiment analysis for asian languages; aspects on cognitive computing and intelligent interaction; spatio-temporal datamining, structured learning and their applications; decision making and knowledge based systems; pattern recognition; agent based systems; decision making techniques and innovative knowledge management; machine learning applications.

Security of Mobile Communications Springer Science & Business Media

Advancing technologies, especially computer technologies, have necessitated the creation of a comprehensive investigation and collection methodology for digital and online evidence. The goal of cyber forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device or on a network and who was responsible for it. Critical Concepts, Standards, and Techniques in Cyber Forensics is a critical research book that focuses on providing in-depth knowledge about online forensic practices and methods. Highlighting a range of topics such as data mining, digital evidence, and fraud investigation, this book is ideal for security analysts, IT specialists, software engineers, researchers, security professionals, criminal science professionals, policymakers, academicians, and students.

Seeking the Truth from Mobile Evidence McGraw Hill Professional

Become well-versed with forensics for the Android, iOS, and Windows 10 mobile platforms by learning essential techniques and exploring real-life scenarios Key FeaturesApply advanced forensic techniques to recover deleted data from mobile devicesRetrieve and analyze data stored not only on mobile devices but also on the cloud and other connected mediumsUse the power of mobile forensics on popular mobile platforms by exploring different tips, tricks, and techniquesBook Description Mobile phone forensics is the science of retrieving data from a mobile phone under forensically sound conditions. This updated fourth edition of Practical Mobile Forensics delves into the concepts of mobile forensics and its importance in today's world. The book focuses on teaching you the latest forensic techniques to investigate mobile devices across various mobile platforms. You will learn forensic techniques for multiple OS versions, including iOS 11 to iOS 13, Android 8 to Android 10, and Windows 10. The book then takes you through the latest open source and commercial mobile forensic tools, enabling you to analyze and retrieve data effectively. From inspecting the device and retrieving data from the cloud, through to successfully documenting reports of your investigations, you'll explore new techniques while building on your practical knowledge. Toward the end, you will understand the reverse engineering of applications and ways to identify malware. Finally, the book guides you through parsing popular third-party applications, including Facebook and WhatsApp. By the end of this book, you will be proficient in various mobile forensic techniques to analyze and extract data from mobile devices with the help of open source solutions. What you will learnDiscover new data extraction, data recovery, and reverse engineering techniques in mobile forensicsUnderstand iOS, Windows, and Android security mechanismsIdentify sensitive files on every mobile platformExtract data from iOS, Android, and Windows platformsUnderstand malware analysis, reverse engineering, and data analysis of mobile devicesExplore various data recovery techniques on all three mobile platformsWho this book is for This book is for forensic examiners with basic experience in mobile forensics or open source solutions for mobile forensics. Computer security professionals, researchers or anyone looking to gain a deeper understanding of mobile internals will also find this book useful. Some understanding of digital forensic practices will be helpful to grasp the concepts covered in the book more effectively.

Practical Mobile Forensics, Academic Press

Discover the tools and techniques of mobile forensic investigations and make sure your mobile autopsy doesn't miss a thing, all through powerful practical recipes About This Book Acquire in-depth knowledge of mobile device acquisition using modern forensic tools Understand the importance of clouds for mobile forensics and learn how to extract data from them Discover advanced data extraction techniques that will help you to solve forensic tasks and challenges Who This Book Is For This book is aimed at practicing digital forensics analysts and information security professionals familiar with performing basic forensic investigations on mobile device operating systems namely Android, iOS, Windows, and Blackberry. It's also for those who need to broaden their skillset by adding more data extraction and recovery techniques. What You Will Learn Retrieve mobile data using modern forensic tools Work with Oxygen Forensics for Android devices acquisition Perform a deep dive analysis of iOS, Android, Windows, and BlackBerry Phone file systems Understand the importance of cloud in mobile forensics and extract data from the cloud using different tools Learn the application of SQLite and Plists Forensics and parse data with digital forensics tools Perform forensic investigation on iOS, Android, Windows, and BlackBerry mobile devices Extract data both from working and damaged mobile devices using JTAG and Chip-off Techniques In Detail Considering the emerging use of mobile phones, there is a growing need for mobile forensics. Mobile forensics focuses specifically on performing forensic examinations of mobile devices, which involves extracting, recovering and analyzing data for the purposes of information security, criminal and civil investigations, and internal investigations. Mobile Forensics Cookbook starts by explaining SIM cards acquisition and analysis using modern forensics tools. You will discover the different software solutions that enable digital forensic examiners to quickly and easily acquire forensic images. You will also learn about forensics analysis and acquisition on Android, iOS, Windows Mobile, and BlackBerry devices. Next, you will understand the importance of cloud

computing in the world of mobile forensics and understand different techniques available to extract data from the cloud. Going through the fundamentals of SQLite and Plists Forensics, you will learn how to extract forensic artifacts from these sources with appropriate tools. By the end of this book, you will be well versed with the advanced mobile forensics techniques that will help you perform the complete forensic acquisition and analysis of user data stored in different devices. Style and approach This book delivers a series of extra techniques and methods for extracting and analyzing data from your Android, iOS, Windows, and Blackberry devices. Using practical recipes, you will be introduced to a lot of modern forensics tools for performing effective mobile forensics.

Learning Android Forensics Packt Publishing Ltd

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics. This guide attempts to bridge that gap by providing an in-depth look into mobile phones and explaining the technologies involved and their relationship to forensic procedures. It covers phones with features beyond simple voice communication and text messaging and their technical and operating characteristics. This guide also discusses procedures for the preservation, acquisition, examination, analysis, and reporting of digital information present on cell phones, as well as available forensic software tools that support those activities.

Data Hiding Packt Publishing Ltd

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, What Every Engineer Should Know About Cyber Security and Digital Forensics is an overview of the field of cyber security. Exploring the cyber security topics that every engineer should understand, the book discusses: Network security Personal data security Cloud computing Mobile computing Preparing for an incident Incident response Evidence handling Internet usage Law and compliance Security and forensic certifications Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of cyber security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding profession.

Handbook of Digital Forensics and Investigation IGI Global

Develop the capacity to dig deeper into mobile device data acquisitionAbout This Book*A mastering guide to help you overcome the roadblocks you face when dealing with mobile forensics*Excel at the art of extracting data, recovering deleted data, bypassing screen locks, and much more*Get best practices to how to collect and analyze mobile device data and accurately document your investigationsWho This Book Is ForThe book is for mobile forensics professionals who have experience in handling forensic tools and methods. This book is designed for skilled digital forensic examiners, mobile forensic investigators, and law enforcement officers.What You Will Learn*Understand the mobile forensics process model and get guidelines on mobile device forensics*Acquire in-depth knowledge about smartphone acquisition and acquisition methods*Gain a solid understanding of the architecture of operating systems, file formats, and mobile phone internal memory*Explore the topics of of mobile security, data leak, and evidence recovery*Dive into advanced topics such as GPS analysis, file carving, encryption, encoding, unpacking, and decompiling mobile application processesIn DetailMobile forensics presents a real challenge to the forensic community due to the fast and unstoppable changes in technology. This book aims to provide the forensic community an in-depth insight into mobile forensic techniques when it comes to deal with recent smartphones operating systemsStarting with a brief overview of forensic strategies and investigation procedures, you will understand the concepts of file carving, GPS analysis, and string analyzing. You will also see the difference between encryption, encoding, and hashing methods and get to grips with the fundamentals of reverse code engineering. Next, the book will walk you through the iOS, Android and Windows Phone architectures and filesystem, followed by showing you various forensic approaches and data gathering techniques.You will also explore advanced forensic techniques and find out how to deal with third-applications using case studies. The book will help you master data acquisition on Windows Phone 8. By the end of this book, you will be acquainted with best practices and the different models used in mobile forensics.