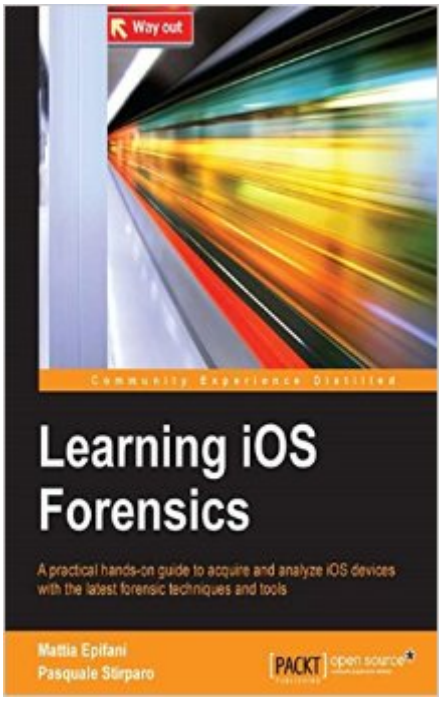
Learning IOS Forensics



Synopsis

A practical hands-on guide to acquire and analyze iOS devices with the latest forensic techniques and toolsAbout This BookPerform logical, physical, and file system acquisition along with jailbreaking the deviceGet acquainted with various case studies on different forensic toolkits that can be usedA step-by-step approach with plenty of examples to get you familiarized with digital forensics in iOSWho This Book Is ForIf you are a digital forensics examiner daily involved in the acquisition and analysis of mobile devices and want to have a complete overview of how to perform your work on iOS devices, this book is definitely for you.What You Will LearnIdentify an iOS device among various models (iPhone, iPad, and iPod Touch) and verify the iOS version installedCrack or bypass the passcode protection chosen by the userAcquire detailed physical or logical info of an iOS deviceRetrieve extra information from side channel data leaksRecover information from a local backup and eventually crack the backup passwordDownload backup information stored on iCloudAnalyze the system, user, and third-party information from a device, backup, or iCloudExamine malicious apps to identify the stolen data and credentialsIn DetailMobile device forensics relates to the recovery of data from a mobile device. It has an impact on many different situations including criminal investigations and intelligence gathering. iOS devices, with their wide range of functionality and usability, have become one of the mobile market leaders. Millions of people often depend on iOS devices for storing sensitive information, leading to a rise in cybercrime. This has increased the need to successfully retrieve this information from these devices if stolen or lost.Learning iOS Forensics will give you an insight into the forensics activities you can perform on iOS devices. You will begin with simple concepts such as identifying the specific iOS device and the operating system version and then move on to complex topics such as analyzing the different recognized techniques to acquire the content of the device. Throughout the journey, you will gain knowledge of the best way to extract most of the information by eventually bypassing the protection passcode. After that, you, the examiner, will be taken through steps to analyze the data. The book will give you an overview of how to analyze malicious applications created to steal user credentials and data.

Book Information

File Size: 15264 KB
Print Length: 220 pages
Publisher: Packt Publishing (March 10, 2015)
Publication Date: March 10, 2015

Sold by:Â Digital Services LLC

Language: English

ASIN: B00UJRFGVW

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Enabled

Best Sellers Rank: #415,607 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #93 inÂ Books > Computers & Technology > Web Development & Design > User Generated Content #388 inÂ Books > Computers & Technology > Mobile Phones, Tablets & E-Readers > Programming & App Development #1558 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

If you’re a digital forensics investigator (which I’m not), or a developer of Apple mobile applications who wants to know how to deal with security issues in Apple devices, I highly recommend reading this book.Although it is aimed at a highly technical audience, any lay person who owns an Apple device should also read it, or try to. It doesn’t just discuss security issues, but also describes how data inside Apple devices can be analyzed, and extracted from them.The book is organized, in the authors’ own words, "in the order of the main phases of a forensic investigation (identification, acquisition, and analysis)."The first chapter discusses digital and mobile forensics, including the difference between the two. The second chapter introduces Apple devices (iPhones, iPads, iPad minis, and iPod touches), and describes how to identify them. The next two chapters tell how to acquire data from Apple devices, and analyzing data in these devices. Then there are chapters on how to acquire and analyze iTunes backups, and do the same with backups stored in iCloud. Finally, there is chapter on how to assess applications, whether they’re malware or not.I really liked how detailed this book was when it described the different types of tools (these include open source, freeware, and commercial software) you can use to do all of the above. At the end of the book, it gives a list of these tools. There is also a section on publications about mobile device forensics.

I found this to be a highly readable technical handbook of iOS forensics. The authors emphasize a hands-on approach, showing not just what information can be extracted but how. The authors go into great detail on the use of many forensic tools both commercial and free. Of special interest are

the numerous mini-discussions on the difficulties encountered in attempting forensic extraction and analysis, for instance the impact of Appleâ ™s adoption of encryption in iOS 8 and later.This book can serve as a reference for iOS forensics activities. In addition to direct extraction from devices, there is coverage of the many other potential sources of forensic data including iTunes backups, iCloud and even Google Drive.For those interested in the nitty gritty of iOS forensics or actually in the business, this book provides a comprehensive look at how iOS forensics can be carried out and of the issues that will be encountered along the way.I found it to be enjoyable and thorough. I'd buy it again.

Outstanding Book! The author does a very good job taking the reader through the inner workings of the iOS operating system and its strengths and weaknesses. Whether you are a forensic pro or a novice you can rest assured once you finished reading this book you will have a solid foundation to build on.

A very detailed look into evidence gathering from iOS devices. Merely the descriptions and examples of the tools that exist for this task, and the amount of information that can be retrieved is well worth the price of the book. At each step of the discussion the authors never lose sight of the rules of forensic evidence gathering - it's not enough to get data out, but it must be done in a manner that maintains the information as useful evidence for use in a court of law. The tools and techniques described cover everything from the first iPhone, on up to iOS 8.0. Case studies and examples help to show how to get the information you need, and which tools to best retrieve and interpret it.

Learn to Code in Swift: The new language of iOS Apps (iOS App Development for Non-Programmers Book 2) Beginning iOS 7 Development: Exploring the iOS SDK iOS 8 Swift Programming Cookbook: Solutions & Examples for iOS Apps SWIFT: PROGRAMMING ESSENTIALS (Bonus Content Included): Learn iOS development! Code and design apps with Apple's New programming language TODAY (iOS development, swift programming) Apps: Mobile App Trends in 2015 (iOS, Xcode Programming, App Development, iOS App Development, App Programming, Swift, Without Coding) ((Android, Android ... App Programming, Rails, Ruby Programming)) Learning OpenGL ES for iOS: A Hands-on Guide to Modern 3D Graphics Programming Learning Swift: Building Apps for OS X and iOS Learning Core Data for iOS with Swift: A Hands-On Guide to Building Core Data Applications Scene of the Cybercrime: Computer Forensics Handbook Computer Forensics JumpStart Computer Forensics: Cybercriminals, Laws, And Evidence