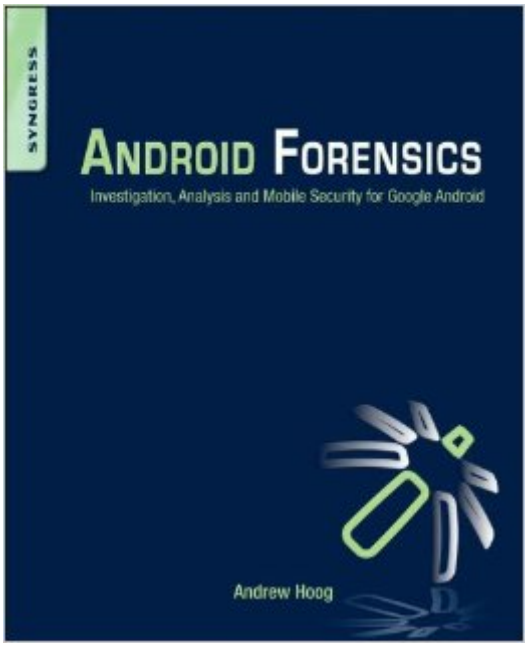
Android Forensics: Investigation, Analysis And Mobile Security For Google Android



Synopsis

Android Forensics: Investigation, Analysis, and Mobile Security for Google Android examines the Android mobile platform and shares techniques for the forensic acquisition and subsequent analysis of Android devices. Organized into seven chapters, the book looks at the history of the Android platform and its internationalization; it discusses the Android Open Source Project (AOSP) and the Android Market; it offers a brief tutorial on Linux and Android forensics; and it explains how to create an Ubuntu-based virtual machine (VM). The book also considers a wide array of Android-supported hardware and device types, the various Android releases, the Android software development kit (SDK), the Davlik VM, key components of Android security, and other fundamental concepts related to Android forensics, such as the Android debug bridge and the USB debugging setting. In addition, it analyzes how data are stored on an Android device and describes strategies and specific utilities that a forensic analyst or security engineer can use to analyze an acquired Android device. Core Android developers and manufacturers, app developers, corporate security officers, and anyone with limited forensic experience will find this book extremely useful.Named a 2011 Best Digital Forensics Book by InfoSec ReviewsAbility to forensically acquire Android devices using the techniques outlined in the bookDetailed information about Android applications needed for forensics investigationsImportant information about SQLite, a file based structured data storage relevant for both Android and many other platforms.

Book Information

File Size: 12344 KB

Print Length: 432 pages

Publisher: Syngress; 1 edition (July 21, 2011)

Publication Date: July 21, 2011

Sold by:Â Digital Services LLC

Language: English

ASIN: B005PLWT0S

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Enabled

Best Sellers Rank: #855,638 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #105

inÂ Books > Computers & Technology > Mobile Phones, Tablets & E-Readers > Android #461 inÂ Kindle Store > Kindle eBooks > Computers & Technology > Microsoft > Windows - General #610 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Storage & Retrieval

Customer Reviews

As Brian Carrier is to file system forensics and Harlan Carvey is to Windows registry analysis, Andrew Hoog is to the Android operating system. The level of detail in this book demonstrates a deep understanding of this complex and unique operating system. Chapter 1 begins with an overview of both Android and Linux in general. Instructions are provided for creating a virtual machine environment so the reader can follow along with the examples in the book. Throughout, the reader is encouraged to follow along, and ample opportunities are provided. This is highly appreciated as most technical books overwhelm the reader with information rather than guide them along the way. Chapter 2 presents an overview of the hardware that is supported by the Android OS. Chapter 3 begins the discussion of the Android OS proper. Included in this chapter are instructions on augmenting the previously created VM with the Android SDK providing additional tools for use in analysis. Chapter 4 is devoted to discussing the file systems likely to be encountered in the Android environment. Special attention is paid to YAFFS and YAFFS2. Chapter 5 discusses securing the data within the device. Also presented are recommendations for securely using Android devices in an enterprise environment. Additional advice is given for both users and developers to limit the exposure of sensitive data. Chapter 6 covers the most significant portion of the book with instructions on acquiring the data from device. Logical and physical acquisitions from the handset as well as the removable storage are discussed. The issue of passcode circumvention is discussed along with potential solutions. Chapter 7 finishes with timeline analysis techniques for the YAFFS file system and the FAT file system. Additional locations of interest to both security researchers and forensic analysts are also presented. Overall the book is enjoyable to read and will be a valuable asset for both forensic analysts and researchers.

One reviewer commented that code samples are unreadable for the Kindle version. That seems to be true for standard, small screen, non-color devices (i.e. classic Kindles). However, on my iPad Kindle app the code samples are fine. In fact you can unpinch them to zoom in, and rotate your device to portrait mode if needed. Also, the online Kindle Cloud Reader shows the code samples clearly. Hopefully future conversions of technical texts such as this one will be done with more care

to allow resizing of special text. For now you will need your PC with the free Cloud Reader, or some large screen tablet device to take advantage of this ebook.

Andrew Hoog has done an outstanding job presenting a complex topic that should interest not only advanced forensic practitioners but the typical Android Smartphone user as well. Highly recommended, whether its for work, or you want to know what "rooting" your Android phone actually does to the device.

A very well written book that contains Android essentials and advanced topics. Andrew Hoog does a great job explaining concepts and making even the most complex topics understandable. Highly recommended!

Android Forensics: Investigation, Analysis and Mobile Security for Google Android Google Classroom: The 2016 Google Classroom Guide (Google Classroom, Google Guide, Google Classrooms, Google Drive) Android: Android Programming And Android App Development For Beginners (Learn How To Program Android Apps, How To Develop Android Applications Through Java Programming, Android For Dummies) Mobile Apps Made Simple: The Ultimate Guide to Quickly Creating, Designing and Utilizing Mobile Apps for Your Business - 2nd Edition (mobile application, ... programming, android apps, ios apps) Android: Programming in a Day! The Power Guide for Beginners In Android App Programming (Android, Android Programming, App Development, Android App Development, ... App Programming, Rails, Ruby Programming) Programming #8:C Programming Success in a Day & Android Programming In a Day! (C Programming, C++programming, C++ programming language, Android , Android Programming, Android Games) Android Security Internals: An In-Depth Guide to Android's Security Architecture Mobile App Marketing And Monetization: How To Promote Mobile Apps Like A Pro: Learn to promote and monetize your Android or iPhone app. Get hundreds of thousands of downloads & grow your app business Evidence in Traffic Crash Investigation And Reconstruction: Identification, Interpretation And Analysis of Evidence, And the Traffic Crash Investigation And Reconstruction Process Apps: Make Your First Mobile App Today- App Design, App Programming and Development for Beginners (ios, android, smartphone, tablet, apple, samsung, App ... Programming, Mobile App, Tablet App Book 1) Home Security: Top 10 Home Security Strategies to Protect Your House and Family Against Criminals and Break-ins (home security monitor, home security system diy, secure home network) The Basics of Digital Forensics: The Primer for Getting

Started in Digital Forensics Android XBMC Kodi 5 In 1 User Guide (Updated September 2016): Android Tablet, Phone & Google TV User Guide, XBMC Kodi & TV Streaming User Guide 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)) Android Tips and Tricks: Covers Android 5 and Android 6 devices (2nd Edition) Android Tips and Tricks: Covers Android 5 and Android 6 devices Android at Work: 150-Plus Must Have Apps for Android Phones and Tablets: The complete guide to the best free phone and tablet Android apps Android Programming BOX SET: ANDROID PROGRAMMING and ANDROID GAME PROGRAMMING - 2 Books in 1 (Second Edition) Accelerated Linux Core Dump Analysis: Training Course Transcript with GDB Practice Exercises (Pattern-Oriented Software Diagnostics, Forensics, Prognostics, Root Cause Analysis, Debugging Courses) Embedded Programming with Android: Bringing Up an Android System from Scratch (Android Deep Dive)