Learning Android Forensics
Second Edition

Analyze Android devices with the latest forensic tools and techniques

Oleg Skulkin
Donnie Tindall
Rohit Tamma

Packt

BIRMINGHAM - MUMBAI

Learning Android Forensics
Second Edition

Commissioning Editor: Gebin George
Acquisition Editor: Rohit Rajkumar
Content Development Editor: Ronn Kurien
Technical Editor: Prachi Sawant
Copy Editor: Safis Editing
Project Coordinator: Jagdish Prabhu
Proofreader: Safis Editing
Indexer: Pratik Shirodkar
Graphics: Tom Scaria
Production Coordinator: Jyoti Chauhan

First published: April 2015
Second edition: December 2018

Production reference: 1211218

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78913-101-7

www.packtpub.com

mapt.io

Mapt is an online digital library that gives you full access to over 5,000 books and videos, as well as industry leading tools, to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Mapt is fully searchable
- Copy and paste, print, and bookmark content

Packt.com

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Contributors

About the authors

Oleg Skulkin is senior digital forensic analyst at Group-IB, one of the global leaders in preventing and investigating high-tech crimes and online fraud. He holds a number of certifications, including GCFA, MCFE, and ACE. Oleg is the co-author of Windows Forensics Cookbook and Practical Mobile Forensics, as well as the author of many blog posts and articles you can find online. Finally, he is one of the people behind Cyber Forensicator.

I would like to thank my mom and wife for their support and caring, the Packt team who worked on this book with me, my co-authors, Donnie Tindal and Rohit Tamma, Igor Mikhaylov for being technical reviewer, and the whole Group-IB Digital Forensics and Incident Response Team, especially Vitaliy Trifonov and Roman Rezvukhin.

Donnie Tindall is a principal incident response consultant with the Crypsis Group, where he handles incident response engagements encompassing the full lifecycle of cyber security events. His corporate and consulting background is primarily in conducting sensitive forensics examinations for federal government clients, particularly the U.S. military and the Intelligence Community. Before moving into Incident Response, Donnie had an extensive background in mobile forensics, application security research, and exploitation. He is also an IACIS Certified Forensic Computer Examiner and former Community Instructor of FOR585, the SANS Institute's smartphone forensics course.

First, I need to thank my wife, Amber, for putting up with me locking up myself in the office for hours at a time while writing this book. Also, thank you to my son, Dominic, for allowing me to use the computer long enough to get things done (without complaining — most of the time). And of course, thanks to my parents for helping me get where I am today.

Rohit Tamma is a security program manager currently working for Microsoft. With over 9 years of experience in the field of security, his background spans management and technical consulting roles in the areas of application and cloud security, mobile security, penetration testing, and security training. Rohit has also co-authored a couple of books, *Practical Mobile Forensics* and *Learning Android Forensics*, which explain a number of ways of performing forensics on mobile platforms. You can contact him on Twitter at `@RohitTamma`.

> *Writing this book has been a great experience because it has taught me several things that would not have been possible otherwise. I would like to dedicate this book to my parents for helping me in every possible way throughout my life.*

About the reviewers

Igor Mikhaylov has been working as a forensic examiner for 21 years. During this time, he has attended a lot of seminars and training classes organized by leading digital forensic companies (such as Guidance Software, AccessData, and Cellebrite) and forensic departments of government organizations of the Russian Federation. He has experience and skills in computer forensics, incident response, cell phone forensics, chip-off forensics, malware forensics, data recovery, digital image analysis, video forensics, and big data. He has written three tutorials on cell phone forensics and incident response for Russian forensic examiners.

Gautam Kumawat is world's youngest cyber crime investigator and self-trained cyber security expert who hails from India. He is currently helping various prestigious institutions, such as the State Police, the Central Bureau of Investigation, the Department of Defense, the Indian Army, and the Central Detective Training School, in the sphere of training officials and solving complex cyber crime cases. He has also provided training for the New York City Police Department and Interpol. His expertise in the cyber security industry far outweighs the standard number of security assessments, audits, compliance, governance, incident response, and forensic projects that he carries out in day-to-day operations involving big fortune companies.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface 1

Chapter 1: Introducing Android Forensics 5
- **Mobile forensics** 6
- **The mobile forensics approach** 8
  - Investigation preparation 8
  - Seizure and isolation 9
  - The acquisition phase 13
  - Examination and analysis 15
  - Reporting 15
- **Challenges in mobile forensics** 16
- **Android architecture** 17
  - The Linux kernel 19
  - Hardware abstraction level 19
  - Android Runtime 20
  - Native C/C++ Libraries 20
  - Java API Framework 20
  - The application layer 20
- **Android security** 21
  - Security at OS level through the Linux kernel 22
  - Permission model 22
    - Sample permission model in Android 23
  - Application sandboxing 24
  - SELinux in Android 26
  - Application signing 26
  - Secure inter-process communication 27
  - Binder communication model 28
- **Android hardware components** 29
  - Core components 29
    - Central Processing Unit (CPU) 29
    - Baseband processor 30
    - Memory 30
    - SD Card 31
    - Display 31
    - Battery 32
- **Android boot process** 33
  - Boot ROM code execution 33
  - The bootloader 34
  - The Linux kernel 35
  - The init process 36
    - Zygote and Dalvik 37

System server 38
Summary 40
Chapter 2: Setting up the Android Forensic Environment 41
Android forensic setup 41
Android SDK 42
Installing the Android SDK 42
Android Virtual Device 44
Connecting and accessing Android devices from the workstation 46
Identifying the correct device cable 46
Installing device drivers 47
Accessing the device 47
Android Debug Bridge 51
Using ADB to access the device 52
Detecting a connected device 52
Directing commands to a specific device 53
Issuing shell commands 53
Basic Linux commands 54
Installing an application 57
Pulling data from the device 58
Pushing data to the device 58
Restarting the ADB server 58
Viewing log data 59
Rooting Android 60
What is rooting? 61
Why root? 62
Recovery and fastboot 63
Recovery mode 63
Accessing recovery mode 63
Custom recovery 64
Fastboot mode 65
Locked and unlocked boot loaders 66
How to root 67
Rooting an unlocked boot loader 67
Rooting a locked boot loader 69
ADB on a rooted device 70
Summary 71
Chapter 3: Understanding Data Storage on Android Devices 73
Android partition layout 73
Common partitions in Android 74
Identifying partition layout 74
Android file hierarchy 76
Overview of directories 77
The acct directory 77
The cache directory 77
The config directory 78
The data directory 78

The dev directory 79
The mnt directory 79
The proc directory 80
The sbin directory 80
The storage directory 81
The system directory 82
Application data storage on the device 82
Shared preferences 84
Internal storage 84
External storage 87
SQLite database 87
Network 87
Android filesystem overview 88
Viewing filesystems on an Android device 89
Common Android filesystems 90
Flash memory filesystems 90
Media-based filesystems 91
Pseudo filesystems 92
Summary 95

Chapter 4: Extracting Data Logically from Android Devices 97
Logical extraction overview 97
What data can be recovered logically? 98
Root access 98
Manual ADB data extraction 99
USB Debugging 99
Using adb shell to determine if a device is rooted 101
adb pull 101
Recovery Mode 103
Fastboot mode 107
Determining bootloader status 107
Booting to a custom recovery image 110
ADB backup extractions 111
Extracting a backup over ADB 111
Parsing ADB backups 113
Data locations within ADB backups 115
ADB dumpsys 118
Dumpsys batterystats 119
Dumpsys procstats 120
Dumpsys user 120
Dumpsys App Ops 121
Dumpsys Wi-Fi 122
Dumpsys notification 122
Dumpsys conclusions 123
Helium backup extractions 124
Bypassing Android lock screens 128
Lock screen types 128

None/Slide lock screens 129
Pattern lock screens 129
Password/PIN lock screens 129
Smart Locks 129
Trusted Face 129
Trusted Voice 130
Trusted Location 130
Trusted Device 130
On-body Detection 130
General bypass information 130
Removing Android lock screens 131
Removing PIN/password with ADB 132
Removing PIN/Password with ADB and SQL 132
Android SIM card extractions 132
Acquiring SIM card data 133
SIM Security 136
SIM cloning 136
Summary 137

Chapter 5: Extracting Data Physically from Android Devices 139
Physical extraction overview 139
What data can be acquired physically? 140
Root access 140
Extracting data physically with dd 141
Determining what to image 142
Writing to an SD card 143
Writing directly to an examiner's computer with netcat 144
Installing netcat on the device 145
Using netcat 145
Extracting data physically with nanddump 146
Extracting data physically with Magnet ACQUIRE 147
Verifying a full physical image 151
Analyzing a full physical image 151
Autopsy 152
Issues with analyzing physical dumps 155
Imaging and analyzing Android RAM 157
What can be found in RAM? 157
Imaging RAM with LiME 158
Acquiring Android SD cards 159
What can be found on an SD card? 159
SD card security 160
Advanced forensic methods 161
JTAG 161
Chip-off 163
Summary 164

Chapter 6: Recovering Deleted Data from an Android Device 165