Learning iOS Forensics

A practical hands-on guide to acquire and analyze iOS devices with the latest forensic techniques and tools

Mattia Epifani
Pasquale Stirparo
Credits

Authors
Mattia Epifani
Pasquale Stirparo

Copy Editors
Brinda S. Madhu
Vikrant Phadke

Reviewers
John B. Baird
Florian Pradines
Lavneet Sharma
Michael Yasumoto

Project Coordinator
Leena Purkait

Proofreaders
Simran Bhogal
Maria Gould
Paul Hindle
Clyde Jenkins

Commissioning Editor
Ashwin Nair

Indexer
Monica Ajmera Mehta

Acquisition Editor
Sonali Vernekar

Production Coordinator
Nilesh R. Mohite

Content Development Editor
Pooja Nair

Cover Work
Nilesh R. Mohite

Technical Editors
Rosmy George
Novina Kewalramani
Edwin Moses
Mattia Epifani (@mattiaep) is the CEO at Reality Net–System Solutions, an Italian consulting company involved in InfoSec and digital forensics. He works as a digital forensics analyst for judges, prosecutors, lawyers, and private companies. He is a court witness and digital forensics expert.

He obtained a university degree in computer science in Genoa, Italy, and a master's degree in computer forensics and digital investigations in Milan. Over the last few years, he obtained several certifications in digital forensics and ethical hacking (GCFA, GREM, GMOB, CIFI, CEH, CHFI, ACE, AME, ECCE, CCE, and MPSC) and attended several SANS classes (computer forensics and incident response, Windows memory forensics, mobile device security and ethical hacking, reverse engineering malware, and network forensics analysis).

He speaks regularly on digital forensics in different Italian and European universities (Genova, Milano, Roma, Bolzano, Pescara, Salerno, Campobasso, Camerino, Pavia, Savona, Catania, Lugano, Como, and Modena e Reggio Emilia) and events (Security Summit, IISFA Forum, SANS European Digital Forensics Summit, Cybercrime Conference Sibiu, Athens Cybercrime Conference, and DFA Open Day). He is a member of CLUSIT, DFA, IISFA, ONIF, and Tech and Law Center and the author of various articles on scientific publications about digital forensics. More information is available on his LinkedIn profile (http://www.linkedin.com/in/mattiaepifani).
Acknowledgments

My first thank you goes to Pasquale Stirparo. We met in 2009 during a course on digital investigations at the University of Milan. Since then, we became great friends, both with a common passion for digital forensics and the mobile world. This book is the outcome of our continuous discussions on the subject and the exchange of knowledge and opinions. Thank you, Pas! It's always nice working with you!

We, the authors, would like to thank Marco Carlo Spada and Paolo Dal Checco, for their valuable help in revising the entire book and their useful suggestions to improve the final result.

I also want to thank Marco Scarito and Francesco Picasso, my colleagues and friends. Without their daily efforts and our continuous exchange of knowledge, this book would not have been written. I also want to thank my parents, Roberta and Mario, and their (and also mine!) dogs, Nina and Sissi, for supporting me every day!

Then, I would like to thank all the mentors I've had over the years: Giovanni Ziccardi, Gerardo Costabile, Rob Lee, Raul Siles, Jess Garcia, Alessandro Borra, and Alberto Diaspro. Also, a big thank you to my friends and colleagues: Giuseppe Vaciago, Litiano Piccin, Davide Gabrini, Davide D'Agostino, Stefano Fratepietro, Paolo Dal Checco, Andrea Ghirardini, Francesca Bosco, Daniela Quetti, Valerio Vertua, Andrey Belenko, and Vladimir Katalov. Without learning from these teachers and exchanging information with my colleagues, there is not a chance I would be doing what I do today. It is because of them and others who I may not have listed here that I feel proud to pass my knowledge on to those willing to learn.
Pasquale Stirparo (@pstirparo) is currently working as a Senior Information Security and Incident Response Engineer at a Fortune 500 company. Prior to this, he founded SefirTech, an Italian company focusing on mobile security, digital forensics, and incident response. Pasquale has also worked at the Joint Research Centre (JRC) of European Commission as a digital forensics and mobile security researcher, focusing mainly on security and privacy issues related to mobile devices communication protocols, mobile applications, mobile malware, and cybercrime. He was also involved in the standardization of digital forensics as a contributor (the first from Italy) to the development of the standard ISO/IEC 27037: Guidelines for identification, collection and/or acquisition and preservation of digital evidence, for which he led the WG ISO27037 for the Italian National Body in 2010.

The author of many scientific publications, Pasquale has also been a speaker at several national and international conferences and seminars on digital forensics and a lecturer on the same subject for Polytechnic of Milano and United Nations (UNICRI). Pasquale is a Ph.D candidate at Royal Institute of Technology (KTH), Stockholm. He holds an MSc in computer engineering from Polytechnic of Torino, and he has GCFA, GREM, OPST, OWSE, and ECCE certifications and is a member of DFA, Tech and Law Center, and ONIF. You can find his details on LinkedIn at https://www.linkedin.com/in/pasqualestirparo.
Acknowledgments

This book would have hardly been possible without my great friend Mattia Epifani, who agreed to join me in this incredible journey. Our teamwork and brainstorming sessions, along with his knowledge and advice, have been invaluable. Thank you!

We, the authors, would like to thank Marco Carlo Spada and Paolo Dal Checco, for their valuable help in revising the entire book and their useful suggestions to improve the final result.

I would like to thank my girlfriend, Silvia, for her patience during my many sleepless nights spent on writing and researching. Her continuous encouragement and love have been a source of strength and motivation for me. I am also very grateful to my friends and colleagues, Marco Scarito and Francesco Picasso, for all the years we have spent growing together in this amazing field and for the continual exchange of thoughts and ideas. Finally, a big thank you to my parents, Francesco and Silvia, my sisters, Stella and Carmen, and my brother, Rocco, for their endless support throughout my life.

I also owe a thank you to Maurizio Agazzini, Marco Ivaldi, and Andrea Ghirardini, the very first people who taught me everything when I was just a "kid out of university." They made me fall in love with this field of work. Another thank you goes to Francesca Bosco and Giuseppe Vaciago for putting their trust in me since the very beginning and for their guidance throughout these years. Thanks to my friends and colleagues Paolo Dal Checco, Stefano Fratepietro, Daniela Quetti, and Valerio Vertua as well. Last but not least, a huge thank you goes to Heather Mahalik, Lenny Zeltser, and Raul Siles for being great instructors and sources of inspiration and the whole SANS family and the DFIR community, where the knowledge and passion of great-minded and extraordinary people come together. Thank you!
About the Reviewers

John B. Baird was born on January 2, 1981, and grew up on Anna Maria Island, Florida, United States. He learned about computers and technology himself at the age of 13. In 2004, he started his own technology consulting business. In that role, he provided services and training for residential and business clients in the Tampa Bay Area. Some of his most prominent clients and contractual assignments included AOL, Wells Fargo, and Comcast.

John soon decided to amplify his skill set and take on a more challenging endeavor. Working with computer forensic suites, such as EnCase and FTK, and practicing skills ranging from evidence preservation to interim report writing, he graduated from ITT Technical Institute online as an associate of applied science in computer forensics in December, 2012. He graduated with a summa cum laude honor, scoring 3.8 out of 4.0 GPA, and was awarded sponsorship for National Technical Honor Society in 2012.

John is trying to make a difference in cyber security and is seeking to work hard for an organization, local or across America, to help him meet his goals. He always looks for interesting, new topics to help others, work or to volunteer. His computer forensics portfolio is available at [www.johnBbaird.com](http://www.johnBbaird.com).

Florian Pradines is a French student in an engineering school, with experience in the information security field. He began programming some websites at the age of 14 and was soon interested in IT security.

Since 2012, he has been working as an IT security consultant for a French company called Phonesec. At the time of writing this book, he has started carrying out professional security audits for some companies on various platforms such as iOS, Android, and websites.

Since 2013, he has been an active member of Open Web Application Security Project (OWASP) where he writes and maintains some tools to help penetration testers conduct their security audits more quickly.
Lavneet Sharma (cipherux) is an entrepreneur working as a CEO in his own data mining start-up known as Corouter Solutions. He has worked as a digital forensics analyst in one of the leading cybercrime investigation companies in India. He is particularly interested in taking advantage of emerging technologies, such as cloud computing and big data analysis, and basic programming technologies, such as Java and Python, to explore and generate new opportunities in the field of information technology. Other than data mining, his fields of interest include cryptography and digital forensics.

He has recently worked on a few commercial (freeware) cryptography tools, both symmetric and asymmetric, to securely sync data across the cloud. He has also developed a high-speed, scalable, and extensible web crawler to run over the cloud in Java.

I would like to sincerely thank the author of this book for giving me a chance to work with a lot of interesting and useful information. I would also like to thank my parents for trusting me and helping me achieve my targets. I would also like to thank my friends for encouraging me to review such a great book and explore such awesome technology.

Michael Yasumoto is a senior forensic examiner with Deadbolt Forensics, a leading provider of computer and mobile forensic services. He is based in Portland, Oregon. In this role, Michael has conducted examinations on a wide variety of computers and mobile devices running on many types of operating systems.

Michael holds a bachelor's degree in chemistry from the University of Washington and a master's degree in computer science from George Washington University. Some of his forensic credentials include Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE), AccessData Certified Examiner (ACE), Cellebrite Certified Mobile Examiner (CCME), and AccessData Mobile Examiner (AME).
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>1</td>
</tr>
<tr>
<td><strong>Chapter 1: Digital and Mobile Forensics</strong></td>
<td>7</td>
</tr>
<tr>
<td>Digital forensics</td>
<td>7</td>
</tr>
<tr>
<td>Mobile forensics</td>
<td>8</td>
</tr>
<tr>
<td>Digital evidence</td>
<td>9</td>
</tr>
<tr>
<td>Identification, collection, and preservation of evidence</td>
<td>11</td>
</tr>
<tr>
<td>Chain of custody</td>
<td>14</td>
</tr>
<tr>
<td><strong>Going operational – from acquisition to reporting</strong></td>
<td>16</td>
</tr>
<tr>
<td>Evidence integrity</td>
<td>17</td>
</tr>
<tr>
<td><strong>SIM cards</strong></td>
<td>18</td>
</tr>
<tr>
<td>SIM security</td>
<td>21</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>21</td>
</tr>
<tr>
<td><strong>Self-test questions</strong></td>
<td>22</td>
</tr>
<tr>
<td><strong>Chapter 2: Introduction to iOS Devices</strong></td>
<td>23</td>
</tr>
<tr>
<td><strong>iOS devices</strong></td>
<td></td>
</tr>
<tr>
<td>iPhone</td>
<td>23</td>
</tr>
<tr>
<td>iPhone (first model)</td>
<td>24</td>
</tr>
<tr>
<td>iPhone 3G</td>
<td>24</td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>24</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>25</td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>25</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>25</td>
</tr>
<tr>
<td>iPhone 5c</td>
<td>26</td>
</tr>
<tr>
<td>iPhone 5s</td>
<td>26</td>
</tr>
<tr>
<td>iPhone 6</td>
<td>26</td>
</tr>
<tr>
<td>iPhone 6 Plus</td>
<td>26</td>
</tr>
<tr>
<td><strong>iPad</strong></td>
<td>27</td>
</tr>
<tr>
<td>iPad (first model)</td>
<td>27</td>
</tr>
<tr>
<td>iPad 2</td>
<td>27</td>
</tr>
<tr>
<td>iPad 3 (the new iPad)</td>
<td>28</td>
</tr>
</tbody>
</table>
# Table of Contents

- iPad 4 (with Retina display) 28
- iPad Air 28
- iPad mini 28
- iPad mini second generation 29
- iPad mini third generation 29
- iPod touch 29
  - iPod touch (first model) 29
  - iPod touch (second generation) 30
  - iPod touch (third generation) 30
  - iPod touch (fourth generation) 30
  - iPod touch (fifth generation) 30

- **iOS devices matrix** 30
- **iOS operating system** 31
- **iDevice identification** 32
- **iOS file system** 34
  - The HFS+ file system 35
  - Device partitions 40
  - System partition 41
  - Data partition 42
  - The property list file 44
  - SQLite database 45
- **Summary** 46
- **Self-test questions** 46

## Chapter 3: Evidence Acquisition from iDevices 49

- **iOS boot process and operating modes** 49
- **iOS data security** 50
  - Hardware security features 50
  - File data protection 51
- **Unique device identifier** 52
  - Case study – UDID calculation on iPhone 4s 52
- **Lockdown certificate** 55
- **Search and seizure** 56
- **iOS device acquisition** 57
  - Direct acquisition 58
  - Backup or logical acquisition 59
    - Acquisition with iTunes backup 59
    - Logical acquisition with forensic tools 60
    - Case study – logical acquisition with Oxygen Forensic® Suite 61
  - Advanced logical acquisition 66
    - Case study – advanced logical acquisition with UFED Physical Analyzer 66
  - Physical acquisition with forensic tools 69
    - Case study – physical acquisition with UFED Physical Analyzer 70
## Table of Contents

The iOS device jailbreaking ........................................... 75
   Case study – jailbreaking and physical acquisition with
   Elcomsoft iOS Forensic Toolkit .................................. 76

Apple support for law enforcement ................................ 78
Search and seizure flowchart ....................................... 79
Extraction flowchart ................................................... 80
Summary ........................................................................ 82
Self-test questions ......................................................... 83

Chapter 4: Analyzing iOS Devices ................................. 85

How data are stored ..................................................... 85
   Timestamps ................................................................ 88
   Databases .................................................................. 89
   The property list files .............................................. 89

The iOS configuration files ............................................ 89
Native iOS apps ............................................................ 91
   Address book .......................................................... 91
   Audio recordings ....................................................... 91
   Calendar ................................................................... 92
   Call history ............................................................. 93
   E-mail ...................................................................... 94
   Images ..................................................................... 95
   Maps ....................................................................... 96
   Notes ....................................................................... 96
   Safari ....................................................................... 97
   SMS/iMessage .......................................................... 98
   Voicemail .................................................................. 98

Other iOS forensics traces .............................................. 99
   Clipboard ................................................................... 99
   Keyboard ................................................................... 99
   Location .................................................................... 100
   Snapshots .................................................................. 101
   Spotlight .................................................................... 102
   Wallpaper ................................................................... 102

Third-party application analysis .................................... 102
   Skype ....................................................................... 102
   WhatsApp ................................................................... 105
   Facebook .................................................................... 107
   Cloud storage applications ........................................ 108

Deleted data recovery .................................................... 111
   File carving – is it feasible? ...................................... 111
   Carving SQLite deleted records ................................. 112
# Table of Contents

- Case study – iOS analysis with Oxygen Forensics Suite 2014 112
- Summary 117
- Self-test questions 117

## Chapter 5: Evidence Acquisition and Analysis from iTunes Backup 119

- **iTunes backup** 119
  - iTunes backup folders 120
  - iTunes backup content 120
- **iTunes backup structure** 122
  - Standard backup files 123
- **iTunes backup data extraction** 127
  - Case study – iTunes backup analysis with iPBA 127
- **Encrypted iTunes backup cracking** 130
  - Case study – iTunes encrypted backup cracking with EPPB 131
- Summary 136
- Self-test questions 136

## Chapter 6: Evidence Acquisition and Analysis from iCloud 139

- **iCloud** 139
- **iDevice backup on iCloud** 140
- **iDevice backup acquisition** 141
  - Case study – iDevice backup acquisition and EPPB with usernames and passwords 141
  - Case study – iDevice backup acquisition and EPPB with authentication token 145
  - Case study – iDevice backup acquisition with iLoot 148
- **iCloud Control Panel artifacts on the computer** 149
- Summary 150
- Self-test questions 151

## Chapter 7: Applications and Malware Analysis 153

- **Setting up the environment** 153
  - The class-dump-z tool 155
  - Keychain Dumper 156
  - dumpDecrypted 158
- **Application analysis** 158
  - Data at rest 159
  - Data in use 159
  - Data in transit 159
- **Automating the analysis** 162
  - The iOS Reverse Engineering Toolkit 162
  - idb 165
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>169</td>
</tr>
<tr>
<td>Self-test questions</td>
<td>170</td>
</tr>
<tr>
<td><strong>Appendix A: References</strong></td>
<td>171</td>
</tr>
<tr>
<td>Publications freely available</td>
<td>171</td>
</tr>
<tr>
<td>Tools, manuals, and reports</td>
<td>172</td>
</tr>
<tr>
<td>Apple's official documentation</td>
<td>173</td>
</tr>
<tr>
<td>Device security and data protection</td>
<td>174</td>
</tr>
<tr>
<td>Device hardening</td>
<td>175</td>
</tr>
<tr>
<td>iTunes backup</td>
<td>175</td>
</tr>
<tr>
<td>iCloud Backup</td>
<td>176</td>
</tr>
<tr>
<td>Application data analysis</td>
<td>176</td>
</tr>
<tr>
<td>Related books</td>
<td>178</td>
</tr>
<tr>
<td><strong>Appendix B: Tools for iOS Forensics</strong></td>
<td>181</td>
</tr>
<tr>
<td>Acquisition tools</td>
<td>181</td>
</tr>
<tr>
<td>iDevice browsing tools and other nonforensic tools</td>
<td>182</td>
</tr>
<tr>
<td>iDevice backup analyzer</td>
<td>182</td>
</tr>
<tr>
<td>iDevice encrypted backup</td>
<td>183</td>
</tr>
<tr>
<td>iCloud Backup</td>
<td>184</td>
</tr>
<tr>
<td>Jailbreaking tools</td>
<td>184</td>
</tr>
<tr>
<td>iOS 8</td>
<td>184</td>
</tr>
<tr>
<td>iOS 7</td>
<td>184</td>
</tr>
<tr>
<td>iOS 6</td>
<td>184</td>
</tr>
<tr>
<td><strong>Data analysis</strong></td>
<td>185</td>
</tr>
<tr>
<td>Forensic toolkit</td>
<td>185</td>
</tr>
<tr>
<td>SQLite viewer</td>
<td>185</td>
</tr>
<tr>
<td>SQLite record carver</td>
<td>185</td>
</tr>
<tr>
<td>Plist viewer</td>
<td>186</td>
</tr>
<tr>
<td>iOS analysis suite</td>
<td>186</td>
</tr>
<tr>
<td>App analysis tools</td>
<td>186</td>
</tr>
<tr>
<td>Consolidated.db</td>
<td>187</td>
</tr>
<tr>
<td>App reverse engineering tools</td>
<td>187</td>
</tr>
<tr>
<td><strong>Appendix C: Self-test Answers</strong></td>
<td>189</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>191</td>
</tr>
</tbody>
</table>
Preface

This book is a complete discussion of state-of-the-art technology used in identification, acquisition, and forensic analysis of mobile devices with the iOS operating system. It is a practical guide that will help investigators understand how to manage scenarios efficiently during their daily work on this type of mobile devices.

The need for a practical guide in this area arises from the growing popularity of iOS devices and the different scenarios that an investigator may face, according to the type of device, the version of the operating system, and the presence or absence of security systems (code lock, backup password, and so on).

The book is divided (conceptually) into four areas. The first part deals with the basic concepts related to methods and guidelines to be followed in the treatment of digital evidence and information specific to an iOS device. The second part covers the basic techniques and tools for acquisition and analysis of an iOS device. The third part goes deep into the methods of extracting data when you do not have the physical device available, which means you need to depend on backup and iCloud. Finally, the fourth part provides an overview of issues related to the analysis of iOS applications and malware.

For those who are new to this field, we recommend a sequential reading of the book, since the arguments are processed in the order of the main phases of a forensic investigation (identification, acquisition, and analysis). For the more experienced readers, and for those who routinely deal with this type of devices, the book can be considered as a useful tool to evaluate different techniques, depending on the type of case that you have to handle.
What this book covers

Chapter 1, Digital and Mobile Forensics, is an introduction to the most important concepts and definitions in the field of digital and mobile forensics, and the life cycle of the digital evidence, which includes identification, acquisition, analysis, and reporting.

Chapter 2, Introduction to iOS Devices, contains useful information and references that will help you learn how to identify the various types of devices (such as iPhone, iPad, and iPod Touch) with respect to their model and iOS version. It also contains basic information about the filesystem used on a specific kind of device.

Chapter 3, Evidence Acquisition from iDevices, explains how to acquire data from iOS devices with respect to their model and iOS version, which was introduced in the previous chapter. Physical, logical, and advanced logical acquisitions are discussed, along with the most useful techniques on how to crack or bypass the passcode set by the user. This chapter presents examples of acquisitions realized with various tools, and provides a useful flow chart before dealing with the acquisition stage.

Chapter 4, Analyzing iOS Devices, provides a complete set of information on how to analyze data stored in the acquired device. Both preinstalled (such as address book, call history, SMS, MMS, and Safari) and third-party applications (such as chat, social network, and cloud storage) are explained, with particular attention to the core artifacts and how to search and recover them.

Chapter 5, Evidence Acquisition and Analysis from iTunes Backup, gives an overview on how to deal with the analysis of an iTunes backup taken from a PC or a Mac, focusing on how to read its content and how to try to attack a protected password set by the user. This chapter also explains how to recover passwords stored in the device when the backup is not protected by a password of its own or when the analyst is able to crack it.

Chapter 6, Evidence Acquisition and Analysis from iCloud, deals with the case in which the owner is using iCloud to store the device backup. You will learn how to recover the credentials or the authorization token useful to retrieve the information stored in Apple servers.

Chapter 7, Applications and Malware Analysis, is an introduction to the core concepts and tools used to perform an application assessment from a security point of view. You will also learn how to deal with mobile malware that may be present on jailbroken devices.

Appendix A, References, is a complete set of references that will help you understand some core concepts explained in the book so that you can go deeper into specific topics.
Appendix B, Tools for iOS Forensics, is a comprehensive collection of open source, freeware, and commercial tools used to acquire and analyze the content of iOS devices.

Appendix C, Self-test Answers, contains the answers to the questions asked in the chapters of the book.

Appendix D, iOS 8 – What It Changes for Forensic Investigators, is an add-on covering the recent news and challenges introduced by the latest version of iOS available at the time of writing this book. This is not present in the book but is available as an online chapter at https://www.packtpub.com/sites/default/files/downloads/3815OS_Appendix.pdf.

What you need for this book
This book is designed to allow you to use different operating platforms (Windows, Mac, and Linux) through freeware, open source software, and commercial software. Many of the examples shown can be replicated using either the software tested by the authors or equivalent solutions that have been mentioned in Appendix B, Tools for iOS Forensics. Some specific cases require the use of commercial platforms, and among those, we preferred the platforms that we use in our daily work as forensic analysts (such as Cellebrite UFED, Oxygen Forensics, Elcomsoft iOS Forensic Toolkit, and Elcomsoft Phone Breaker). In any case, we were inspired by the principles of ease of use, completeness of information extracted, and the correctness of the presentation of the results by the software. This book is not meant to be a form of advertising for the aforementioned software in any way, and we encourage you to repeat the tests carried out on one operating platform on other platforms and software applications as well.

Who this book is for
This book is intended mainly for a technical audience, and more specifically for forensic analysts (or digital investigators) who need to acquire and analyze information from mobile devices running iOS. This book is also useful for computer security experts and penetration testers because it addresses some issues that must be definitely taken into consideration before the deployment of this type of mobile devices in business environments or situations where data security is a necessary condition. Finally, this book can be also of interest to developers of mobile applications, and they can learn what data is stored in these devices where the application is used. Thus, they will be able to improve security.
Preface

Conventions
In this book, you will find a number of styles of text that distinguish among different kinds of information. Here are some examples of these styles, and explanations of their meanings.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows:
"Compile the source file by simply typing the make command."

A URL is written as follows:
http://www.sqlite.org/

A pathname is written as follows:
/private/var/root/Library/Lockdown/data_ark.plist

Any command-line input or output is written as follows:
$ iproxy 2222 22
$ ssh usb

New terms and important words are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "The first popup appears on the computer in iTunes and it requests the user to click on Continue."

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback
Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to feedback@packtpub.com, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on www.packtpub.com/authors.
Customer support
Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Downloading the color images of this book
We also provide you with a PDF file that has color images of the screenshots/diagrams used in this book. The color images will help you better understand the changes in the output. You can download this file from https://www.packtpub.com/sites/default/files/downloads/38150S_ColorImages.pdf.

Errata
Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting http://www.packtpub.com/submit-errata, selecting your book, clicking on the errata submission form link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from http://www.packtpub.com/support.

Piracy
Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at copyright@packtpub.com with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions
You can contact us at questions@packtpub.com if you are having a problem with any aspect of the book, and we will do our best to address it.