BOOK REVIEWS

Jigang Liu
Editor
Metropolitan State University
St. Paul, MN 55106
Jigang.Liu@metrostate.edu

If you have any suggestions on books for review, or you would like to write a book review for us, or you have any comments and concerns on the book reviews published on this column, please feel free to send an email to Jigang Liu at Jigang.Liu@metrostate.edu.

BOOK REVIEW

Morrissey, S. (2010). *iOS Forensic Analysis: For iPhone, iPad and iPod Touch*. New York: Apress. 372 pages, ISBN: 978-1-4302-3342-8, US$59.99.

Reviewed by Christopher Schulte, EnCE & ACE, LuciData Inc., Minneapolis, Minnesota (cschulte@lucidatainc.com)

As Digital Forensics practitioners, we know that our discipline is constantly evolving. Keeping abreast means we need to continually refine and broaden our knowledge pools through experience, education, research, peer exchange, and more. Mobile device forensics can be especially dynamic and challenging. With multiple standards in place at the hardware, operating system, and user interface levels, it can be daunting to preserve, analyze, search and report on these tiny yet ubiquitous hand-held computers. Apple Computer's line of mobile products (iOS devices - iPhone, iPad, iPod Touch) is no exception to this rule.

Apple is an established leader in the mobile market. With over 200 millions units sold worldwide, Apple's footprint can be seen everywhere. Whenever I board a commercial airplane, I see row after row of travelers listening to music, playing games, or reading a book using an Apple mobile device. Whether it is a business traveler catching up on corporate email or a youngster playing Angry Birds, I find myself thinking about the forensic artifacts being generated and how critical they might end up being in an investigation. The scope and volume of data stored on iOS devices can be staggering and is continually expanding with the 'App Store' feature that extends the usefulness of the device (both to the user and investigator).

If you have not already seen iOS devices come into your lab, you will, and with increasing frequency. I have been a party to many conversations with corporate clients struggling to define iOS device policies. My clients have end users clamoring for the ability to touch corporate resources with their iPhones, while security and legal are busy evaluating what if any regulatory compliance issues

might arise with their use.

Eventually, of course, an iOS device will become part of your investigation. You will be asked to provide some answers on how it was used or what information it contained. Helping answer those and other questions is Sean Morrissey's "iOS Forensic Analysis: for iPhone, iPad, and iPod touch" published by Apress in December 2010.

This book is full of information any investigator dealing with iOS devices will find extremely useful. It largely takes a tool agnostic approach, providing numerous examples with many tools for both Windows and OS X environments. While Morrissey has a clear preference to working on the Apple side of the house, he understands and explains that it may be necessary to use multiple tools on a number of operating systems to get the job done. No single tool does everything perfectly or can properly interpret every artifact. It is important to know when it might be time to leave the friendly GUI of one tool and break open a hex editor, plist viewer, or sqlite browser. Don't worry if you're not sure what these are or why they are important; the fundamentals are broken out logically and in great detail. The book is designed to bring you up to speed quickly.

Morrissey opens the book with a brief history of Apple's mobile device products, diving right into the meat of how they operate both at the user and operating system levels. He discusses the evolution of the hardware from its origins back in 2007 with the original iPhone, up through the iPhone 4, iPod Touch, and iPad. He introduces iOS (Apple's mobile operating system) and takes us through the software enhancements that have been added over the years and what impact they might have on an investigation. Great care is taken to provide concrete examples to compliment the theory, with tables and screenshots generously sprinkled throughout.

The book covers basic incident response procedures for iOS devices and lists helpful Mac and PC artifacts to be aware of (such as the all-important lockdown certificates). An in-depth analysis of what geolocation data can be found on iOS devices is included and may be especially helpful with law enforcement cases. A concluding chapter describes basic networking concepts and how iOS devices communicate with the outside world.

One of the book's primary focuses is on the acquisition and analysis of iOS devices on a logical level. With logical acquisitions, the iOS device is coaxed into sending a copy of certain logical files, as if an iTunes 'backup' operation is being requested. After those logical files are gathered and preserved, it is possible to perform an analysis on them. Morrissey goes into great detail on the type of information that can be obtained from a logical acquisition, where that information may be stored, and what should be done to convert it into something useful.

One limitation of using logical acquisition methods is that we are restricted to

reviewing only a subset of the total files from the iOS device. We also have no access to unallocated space. Morrissey addresses this by discussing raw image acquisition of the entire iOS device. Morrissey refers to this as 'media exploitation' because the primary method of obtaining raw images of iOS devices has been with so called 'jailbraking' tools. Morrissey's attitude toward raw acquisition methods is that they may not be prudent due to evidentiary concerns and that oftentimes a logical acquisition contains enough useful information. Readers may find that with advances made in raw iOS acquisition methods since the book was published, it may be possible to acquire a full and unencrypted copy of an iOS device without leaving 'residual' data on it. This may partially address Morrissey's concern about best evidence preservation, at the same time giving investigators a complete view of the iOS device. The debate over logical versus raw acquisition may become more pertinent over time, as Apple can arbitrarily limit what data is made available to logical acquisitions. One example is the consolidated.db file, which contains certain historical geolocation data. After privacy concerns were raised about this file in April of 2011, Apple responded by updating iOS. One change Apple made was to limit the usefulness of data returned for consolidated.db from logical iOS acquisitions. Where previously a logical acquisition may have been sufficient to locate certain geolocation data, it may now become necessary to acquire a raw image of the iOS device to properly collect the needed bits.

The book is not without problems. While many screenshots were included, some were of poor quality, including pixilation or sizing issues. There were minor content errors, such as incorrect dates, or software version numbers. There were inconsistencies between chapters when referring to the same fact. There were also grammar and spelling errors. These and other problems were annoying to encounter, and indicate the book may have been rushed too quickly to press. Perhaps it was not reviewed rigorously enough. Even so, the overall message of the book is sound. I consider Sean Morrissey and his team at Katana Forensics leaders in the iOS forensics space. I have spoken to Mr. Morrissey at conferences and seen him lecture in front of groups. He knows this subject matter very well. As a Digital Forensics practitioner, I am most concerned with how well I can take the information presented and put it into a meaningful result that is useful to my clients. As such, I can overlook these minor problems. They can all be corrected with the second edition, which I hope Morrissey will publish.

After reading this book, you will have a solid foundation when working with iOS devices. You will know how to properly acquire them, documenting the correct information as you work. You will know what kinds of information they may contain. You will know what tools are available to analyze them, what their strengths and limitations are, and how to best leverage them to find what you need. You will know where many useful artifacts can be found, along with a basic framework for isolating and analyzing new artifacts. Most importantly, of course, you will be able to bring some order to the chaos and provide helpful

information to your client, supervisor, prosecutor, or whoever is asking the questions.

This book is highly recommended.