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

Hoog, A., & Strzempka, K. (2011). *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices.* Waltham, MA: Syngress. 336 pages, ISBN: 978-1-59749-659-9, US$69.95.

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

These are exciting times for Digital Forensics practitioners. While our examinations of mobile devices (including cell phones and tablet computers) continue to bring new and sometimes hair-pulling challenges into our labs and on-site engagements, research and understanding of these tiny computers is increasing at what seems an exponential rate. This is especially true in the iOS (Apple Computer's mobile operating system that powers the iPhone, iPad, iPod Touch and Apple TV) space. The diligent work of talented computer scientists in this field allows examiners everywhere to reap the benefits of easier, faster and more effective examinations that yield more accurate and defendable results.

The popularity of Apple's mobile devices is growing at a rapid pace and it's no surprise that more and more of these mini-computers are finding their way into forensic labs. Additionally, their capability of storing potentially responsive data increases with every new hardware release, software update and new 'app' that is developed for the platform. Of course, each update also brings the possibility that an existing forensic method is no longer reliable or an expected artifact is no longer present. External resources are needed by examiners to stay on top of the game and ensure that our results are valid.

One such resource that gives some insight into iOS devices and their digital forensics ramifications is "iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices" from Andrew Hoog and Katie Strzempka. Both are from the digital forensics and security firm viaForensics.

The book opens with a brief introduction to mobile devices, Apple's mobile device strategy and a description of the iPhone itself. It then moves to describe different forensic examination approaches, touching on some of the challenges that are specific to working with mobile devices versus traditional computer systems. It's especially pleasing that the authors discuss the different acquisition types examiners may encounter with iOS devices – working with existing backups, performing logical acquisitions, obtaining a full physical dump, and even using jailbreaking techniques. Throughout the book, they skillfully differentiate between these acquisition types, both in terms of the types of data that can be unlocked at each level, along with the complexity of performing the acquisition and working with the resulting data set (evidentiary concerns associated with the acquisition type are also addressed). Finally, the first chapter closes with a primer on the Linux operating system. Because the book's working examples make liberal use of Linux-based open-source tools, this overview is helpful for those unfamiliar with command-line interfaces. It also gives examiners exposure to a set of powerful tools that otherwise may go unused.

As the book progresses, the authors provide more pertinent information about iOS devices. This includes their various operating modes, an overview of firmware versions, how the iTunes program is used to interface with them, the physical nature of iOS flash-based storage devices, how logical data is laid out using a file system, where important files (such as system preferences and app data) are stored on that file system and more. We're also introduced to the all-important sqlite and plist data files, which are used by many applications on iOS devices to store information that is often critical in an investigation. All this information builds gradually; the book's flow and pace work well in laying out fundamental concepts. Familiarity with these concepts becomes useful as more advanced material is presented later in the book.

With the first third of the book intended to bring the reader up to speed with basic concepts, the real fun starts around chapter five and continues through the remained of the book. Here we start off with detailed information about acquisition methodologies, including how to properly secure a seized device and how to manage passcodes and various forms of encryption that may be encountered depending on the acquisition type and the specific hardware/OS version that's in use.

After the iOS device has been acquired, of course, some type of analysis typically needs to be performed on that acquired data before a report can be generated with relevant and key findings. This is where the book heavily utilizes Linux tools. The examples make use of Linux programs such as: basic Linux commands like \`mount\`, \`tree\`, \`grep\`, and \`strings\` for image triage and searching, Scalpel for file carving, various TSK (The Sleuth Kit) commands for generating a timeline of activity, \`sqlite\` and \`plutil\` for iOS data file analysis and conversion, and more. The authors are quite intent on showing how free and open-source applications can be utilized effectively with iOS devices and data.

Building on what's been presented thus far, a detailed forensic breakdown is provided for several of the default applications that ship on iOS devices, such as the text messaging app, calendar app, mail app, map app (including information on parsing historical geo-location data), phone app (which manages the call log and voicemail features), safari app, and so on. For each application, the specific files that contain relevant data are listed along with how to parse them and what to look for. In addition to these default apps, several third-party apps are also deconstructed for our benefit, including the Facebook and Dropbox apps.

At this point in the book the reader should have a solid grasp of the fundamentals of iOS devices including: what iOS devices are, how they operate, the types of data that they store, how that data is encoded and where it's stored on the device's file system, how best to acquire the data from the device, and then how to go about extracting and reporting on relevant information from the acquisition. The learning thus far has been almost exclusively using command-line programs. This 'down and dirty' approach is spectacular for coercing readers into a deeper understanding and appreciation for the internals of how these devices truly operate. I agree with this approach over opening the book with a simple GUI program and a 'process evidence and generate report' button. Our GUI tools allow us to perform quick and efficient analysis, but without a deep technical understanding of exactly what they're doing, these tools can lull the examiner into complacency where results are blindly accepted and external validation never happens.

It's at this point that the book appropriately closes with a detailed report on thirteen commercial tools that are available for acquiring and/or analyzing iOS devices. This closing chapter is more or less a reprint of a white paper that the authors published to the viaforensics.com website back in November of 2010, so many examiners are already familiar with it. Even so, this is a helpful piece and provides a stepping-stone for further tool research and evaluation.

This book truly provides a wealth of information that every iOS examiner should be familiar with. As is the nature of all printed books, some of the material provided can become somewhat stale by the time it reaches the hands of the reader. For example, recent research has spawned advances in our physical acquisition capabilities, providing the ability to fully remove the encryption on both allocated and unallocated data on iPhone 4 devices running iOS 4.x. The omission of this new development is understandable. The authors' blog provided a timely report on this and other related developments as they were announced to the community. This provides a good reminder that examiners must rely on multiple sources of information such as published books, peer reviewed journals, blogs, forums, email lists, conferences, user groups, social networking sites and more as they go about their work.

Digital Forensics professionals are always looking to the future. What does the future hold with regard to iOS investigations, and mobile investigations in general? One guarantee is that as technology and social norms evolve, so will the forensics. Now that iOS version 5 has been released (along with a newer generation of the iPhone 4), a whole new set of questions will need to be answered. Will our existing acquisition methods continue to work? Will the file formats and locations of key data points on iOS devices remain the same? Now that a computer is no longer required to activate, update or use iOS devices on a daily basis, how will data usage and storage patterns evolve? Will data continue to be backed up primarily to a PC, or will it move to Apple's new iCloud service? How will investigative procedures need to be updated to account for this and other new changes? Additionally, what new artifacts will we encounter as new iOS features (such as the Siri voice activated assistant) are activated and used en masse?

For answers to these and other questions… stay tuned…