2013

Book Review: iPhone and iOS Forensic: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices

Garfinkel, Simson

Garfinkel, Simson. "Book Review: iPhone and iOS Forensic: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices." Journal of Digital

BOOK REVIEWS

Diane Barrett
Book Review Editor
University of Advancing Technology
2625 W. Baseline Rd
Tempe, AZ 85283

If you have any suggestions on books for review, would like to write a book review for us, or have any comments or concerns on the book reviews published in this column, please feel free to send an email to Diane Barrett, the editor for this column, at dm_barrett@msn.com.

BOOK REVIEW

Hoog, A., and Strzempka, K. (2011). *iPhone and iOS Forensic: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*. Syngress, Elsevier, xv + 310 pages; ISBN-10: 1597496596; ISBN-13: 978-1597496599, $69.95

Reviewed by ***Simson Garfinkel, Naval Postgraduate School***

In April 2011 news outlets around the world revealed shocking news about Apple's iPhone: for reasons that were not apparently clear, every iPhone contained a small SQLite database that logged where and when the user had been whenever the phone was turned on, and those records went back for pretty much as long as the user had owned their phone. Apple eventually declared that the data cache was the result of a bug and issued a software update to prune the database (it had previously grown without limit). Privacy activists rejoiced that their beloved iPhones were once again trustworthy. But forensics examiners just shook their heads: many had known about the iPhone's tracking capabilities for more than a year and had kept quiet. They had made good use of that data. Apple's pro-privacy patch was actually a setback for law enforcement.

At least, that's how the story played out in the media. But after reading Hoog and Strzempka's *iPhone and iOS Forensics*, you may come to a different conclusion. Even without the detailed repository of positional information, there is still a wealth of sensitive, personal information that's available for the taking on most the vast majority of iPhones walking the streets. In fact, there is so much revelatory information on the typical iPhone that the real problem faced by investigators isn't a paucity of data–it's how to deal with the information torrent.

iPhone and iOS Forensics contains a wealth of information about the design of Apple’s iPhone, iPad, iPod Touch and Apple TV computers. Not surprisingly, the book focuses on the aspects of the computers that are relevant to a forensic examination–the phone’s physical specifications, its modes of operation, and the layout of data within the device. There have been significant changes in the iPhone since the release of the original iPhone 2G in June 2007, and the authors track the majority of changes that are relevant to the forensic examiner. Chapters include hardware, file system layout, iOS security, data acquisition, data analysis, and commercial tool testing reports.

The book’s strongpoint is its aggregation of forensic minutia. There is in-depth discussion of the iPhone’s use of Apple property lists and SQLite databases, application wrapper, partitions, imaging techniques, and various kinds of sensitive data left on the phone by popular downloadable applications. There are also roughly 80 pages of reports detailing test results of iPhone forensic tools by viaForensics, the company where both of the authors work. These test reports are also available on the company’s website, and in some cases the results are updated making the printed reports of limited use.

The Computer Forensic Tool Testing Program at the National Institute of Standards and Technology also engages in the testing of cell phone exploitation tools, so it’s interesting the compare the approach taken by the two organizations. Whereas NIST tests with phones that have been specially procured for the purpose and filled with data by experimenters using scripts, viaForensics appears to populate its cell phones with real data from real users. Although this may be more realistic, the result is that the book contains many black boxes over screen shots in an attempt to obscure personal information. A related problem is that the electronic results of the tools cannot be made available, as it is not clear how they would be redacted. On the other hand, viaForensics appears to have tested many more tools than NIST.

In addition to the specific information about iOS, this book also contains general information on how to use the popular open source forensic tools, and a short tutorial on the Unix command line. Although such information is surely redundant with other volumes, it will be nice for those unfamiliar with the tools to have. What’s missing is a clear explanation of when the author would want to use SleuthKit, Scalpel or Strings in the course of an investigation, how that decision would be made, and what information might be found.

Indeed, while the book is comprehensive, the organization is challenging, the presentation is at times confusing, and the editing is sloppy. For example, on page 10 the authors present a taxonomy of data extraction techniques under the headline *iPhone leveling*. The phrase *leveling* presumably comes from the fact that the taxonomy refers to different *levels* of acquisition. The centerpiece of the section is a graphic titled *iPhone Classification Tool* that’s reprinted from a blog posting. However, the actual blog posting was titled *iPhone Tool*

Classification; transposing the second and third words gives the impression that it's the taxonomy itself that's the tool, which was certainly not the intent of the original author.

Another problem with the book is its index. For example, encryption and PIN locks represent barrier to performing a physical acquisition of an iPhone 4 running on some versions of iOS but not others. Yet the phrases *Encryption*, *PIN Lock*, and *physical acquisition* do not appear in the Index, not even when prefixed by the word *iPhone*. Overall, the poor organization of the Index makes it read like an afterthought. That's too bad, because physical indexes are vitally important for books that are sold in paper form. (You can purchase the book for Kindle or Nook, but the price is the same.)

While there are at least two other books on iPhone forensics, both are at least three years out of date. For this reason alone iPhone and iOS Forensics is a must-have book for those who are professionally engaged in the practice of digital forensics. The book has a wealth of information, and one would not want to be cross-examined as an expert witness without having read this book first. The book is also useful for students, as it brings together in one place information that is now scattered on many websites.