BOOK REVIEWS

Gary C. Kessler
Editor
Champlain College
Burlington, VT 05401
gary.kessler@champlain.edu

BOOK REVIEW

Varsalone, J. (Tech. Ed.), Kubasiak, R.R., Morrissey, S., et al. (2009). *Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit.* Burlington, MA: Syngress. 551 + xix pages, ISBN: 978-1-59749-297-3, US$59.95..

Reviewed by Gary C. Kessler (gary.kessler@champlain.edu)

At last! A quality book about computer forensics for Apple products! Alas, I get ahead of myself.

Apple's hold on the personal computer marketplace started dwindling on August 12, 1981, the day that the IBM PC was introduced. As an Apple][+ bigot myself, I refused to touch a PC for some years. But I was also a command line bigot, so when the first Macintosh was introduced in 1983 and hermetically sealed the operating system from users, I did not go out and buy one. In fact, like many of my era, I did eventually end up on the PC side which, ironically, let me do many of the things that my trusty Apple][+ had in earlier times -- write code, play with the hardware, and, indeed, get to a command line. And, of course, tons of application developers flocked to the PC because of its open architecture.

So, has Apple been offering better products for the last 25 years? Maybe, maybe not -- but that's not the topic of this book review. The real point of the walk down memory lane is that the PC and Microsoft operating systems have dominated the desktop marketplace since the mid-1980s. For that reason, most computer forensics tools since the 1990s have been written for DOS or Windows platforms with the intent of examining DOS or Windows PC systems. Windows PCs so dominate the computer forensics field as forensics platforms and the target of forensics examinations that some labs will not even take in a Mac systems due to lack of staff expertise.

But the market is changing. Mac sales, at least in North America, have surged in the last few years, largely since Apple embraced Intel hardware and a Unix-based operating system kernel. Portable music players have become nearly ubiquitous in the last few years, with Apple iPods being the gold standard. And mobile phones are ubiquitous -- and the iPhone is setting a new standard for mobile phone functionality.

Jesse Varsalone, Ryan Kubasiak, Sean Morrissey, and five contributing authors (Walter Barr, James "Kelly" Brown, Mac Caceres, Mike Chasman, and James Cornell) have provided a welcome new entry in the computer forensics practitioner's literature. Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit provides background information about these popular Apple platforms that are increasingly being found to contain probative information in criminal investigations and civil litigations.

The book comprises 16 chapters and two appendices. All of the chapters tell the reader right up front about the major topics covered in the chapter, and include a detailed summary ("Solution Fast Track") and FAQ at the end.

The first 12 chapters are about Mac systems, covering the current operating systems, hardware, and primary applications. Chapter 1 provides a high-level overview of the Mac OS X Tiger (10.4) and Leopard (10.5) operating systems. This chapter is a great introduction to the history and terminology of Macs, the Mac desktop and basic operating system tools, and an overview of the disk structure and file system. This chapter presents information that would be useful to a first responder having to acquire a Mac in the field.

Chapter 2 provides an introduction to MacBook, Mac desktop, iPod, and iPhone hardware. The chapter provides a nice catalog of the MacBook, MacBook Air, MacBook Pro, PowerMac, iMac, and other computer systems so that the first responder can distinguish between these models in the field and have an idea about available features. Similarly, the chapter covers the various incarnations of the iPod (Classic, Nano, Shuffle, and Touch) followed by a section on the iPhone. The chapter closes out by covering some other pertinent Apple hardware such as the AirPort, Apple TV, and Time Capsule.

Chapter 3 covers disks and partitioning, including the tools available to monitor disks, manage partitions, control startup, forensically wipe or format a drive, build RAID sets, and more. Chapter 4 then goes into great detail about HFS+, the native file system for the Mac (although the Mac can deal with DOS/Windows file systems such as FAT and NTFS). This chapter is essential for the understanding of HFS volumes, file system logical structures, the concept of forks, B*-trees, and commands that allow one to look at these structures and contents.

The next two chapters address two important system applications. Chapter 5 discusses FileVault, the native Mac OS X application to encrypt files on the system. This chapter describes how FileVault works, procedures to acquire an unlocked FileVault, and methods to decrypt a locked FileVault. Chapter 6 covers Time Machine, the Mac OS X backup application. Here, you will read about how Time Machine works, how files can be restored from Time Machine, and the implications for forensics exams.

Chapter 7 focuses on the process of acquiring Mac forensic images. This

chapter starts with a guide about setting up a Mac as a forensic analysis system and moving into the step-by-step process of imaging one Mac from another. Finally, the chapter describes using a live CD to image a Mac.

The next five chapters describe features of important Mac applications and issues related to forensic analysis, including important file locations, file formats, and tools. Chapters 8-12 include coverage of the Safari Web browser, e-mail and iChat artifacts, iPhoto and image library applications, iMovie and video artifacts, and recovery of PDF and Microsoft Office documents, respectively.

The next two chapters cover the iPod. Chapter 13 describes some open source and proprietary tools with which to acquire an iPod with a Mac and Chapter 14 demonstrates ways in which to analyze iPod image files and system artifacts. Chapter 14 also describes the iPod file structure, as well as calendar, contact, iTune, and other application files.

The final two chapters cover the iPhone. Chapter 15 describes specific forensic concerns and logical acquisitions of the iPhone (and iPod Touch), and physically imaging and analyzing the iPhone. Chapter 16 goes into some deeper detail on the iPhone, describing the device's functions, file carving, and alternative methods of iPhone analysis. This chapter is filled with outstanding information about the iPhone file system, application file formats, and a variety of applications with which to analyze the iPhone image.

Appendix A describes a variety of tools with which to run Windows or other operating systems on a Mac using Boot Camp, Parallels, VMware Fusion, and VirtualBox. This appendix also provides detailed instructions on installing Windows XP or Vista, Ubuntu Linux, and OS X Leopard Server in a virtual machine environment. Appendix B discusses methods with which to acquire volatile data from a Mac.

True to the book's title, the reader will also find a DVD containing five tools and two image files that nicely supplement the book. The tools include a converter from system absolute time to a human readable form, an e-mail file conversion program (particularly useful for iPhone analysis), and an iPod photo reader. Mactracker is a very cool open source application that contains a history of every Mac model back to 1983 and hinfo is a supplement to the book's chapter on the HFS+ file system. More impressive are the two images that can be used for analysis, one of a user profile from a Mac and one of an iPod Nano. Both can used with exercises from the book to find the kinds of artifacts that would be useful in a forensic examination.

This book was well worth waiting for, as I ordered it prepublication (Amazon One-Click strikes again!). The book is very well written and filled with screen shots and command line examples, taking up what I estimate to be about 40% of the book. It is also extraordinarily practical, clearly written by authors that

not only understand the Mac issues but also the practice of digital forensics.

I do have a small quibble and that is with the index. While writing this review, I searched the index for various terms; nine out of ten of my lookups were unsuccessful. Heck, chapter 1 is about Tiger and Leopard and neither term has an index entry.

Although I believe that this book has the potential to become an important part of the practitioner's bookshelf, it is only the beginning. The acceleration of change in our business is incredible; this book came out in December 2008 and there are already new Mac, iPod, and iPhone hardware platforms. The book contains a good number of references and the reader will want to build up a list of favorite sites and listserves to monitor to stay abreast of these products and forensic solutions.

Bottom-line -- I highly recommend this book for students, teachers, and practitioners.

(Full disclosure requires that I acknowledge my recent return to the Apple family. I purchased a Mac a year ago because it runs on an Intel platform and I observe that I not only have access to a command line, but it is a Unix command line! And my virtual machine software runs Windows XP better than any of my PCs.)