

CY-FI: The Future of Cyber Forensics

As I mentioned in my previous column, this edition will be focused on Macintosh forensics. It is probably a good idea to explain the rather mysterious second-half of the title to this column. In ancient times it was not uncommon for cartographers to indicate unknown areas by placing drawings of dragons on their maps. Some investigators I have talked to indicate that dealing with Macintosh computers or Apple devices is definitely unknown territory. Hopefully we can begin to erase many of these dragons and start to chart the unknown.

As I sit here writing this column, we at Purdue University have just finished teaching a three day introduction to Macintosh forensics training class for law enforcement. Preparing the materials for the class reinforced my belief that Macintosh computers make an excellent platform for investigating digital evidence, and yet at the same time, present unique challenges to investigators tasked with examining these systems or devices.

It is quite easy to get lulled into a false sense that this is strictly a Microsoft/Windows world. But in fact, with the introduction of the Intel chipset in Macintosh computers, Apple is increasing its market share dramatically year-to-year. If we move our focus away from strictly computers and look at devices in general, Apple in fact has the market share in several sectors – digital music devices (iPod), and even smart phones (iPhone). A very recent survey concluded that Macintosh laptops were the biggest sellers on university campuses in the United States, even surpassing Dell.

It should come as no surprise that Macintosh computers are being used in a myriad of different criminal activities. Criminals in general and cyber criminals specifically are gravitating towards the non-Windows based computing platforms. Some have indicated that this might be due to the built-in “counter forensics” of law enforcement not being familiar with anything but Windows-based machines. Criminals assume that law enforcement is incapable of dealing with non-Windows-based operating systems such as Mac OS X. Criminals tend to also believe that the current crop of forensics tools are focused exclusively on Windows/NTFS, and therefore do not work well on other filesystems such as EXT2 or Mac OS X.

Given this criminal cultural belief, and the reality that Apple computers are gaining a significant market share, it behooves investigators to become familiar with Macintosh computers and Mac OS X. Over the last year, we have seen a dramatic increase in the number of investigations we have assisted in that included Macintosh computers, iPods, and iPhones. Once one gets over the initial shock of not being in an NTFS world, the Mac OS X file system is not really that different. In fact, the much maligned Windows Vista shares a lot in common with Mac OS X. While there are several notable books (see reference section) that can assist the investigator in becoming familiar with the structure of Mac OS X, there is no substitute for hands-on experience. The relatively low

price of the entry level Mac books, or iMacs, should allow investigators to be able to purchase at least one system to use in their labs.

Unfortunately, the belief that the current stock of forensics tools is lacking in its ability to deal properly with Mac OS X, is a reality. This has prompted several companies to begin development of forensics tools that not only handle Mac OS X properly, but also run natively on Macintosh systems (see the reference section at the end of this article). However, to date these tools are not as graphically mature as their Windows counterparts, which may increase the learning curve for some investigators.

Even Apple itself has recognized that law enforcement and investigators need assistance in dealing with Macintosh computers and devices. In order to address this demand, Apple has sponsored several seminars, webcasts, and support pages devoted to digital investigations.

The private sector has also recognized the need for training in this area. There are now several companies that offer both introductory and advanced training in Macintosh forensics. As I mentioned previously, colleges are also beginning to offer courses for law-enforcement, private sector, and traditional students in the area of Macintosh forensics and other non-Windows-based file systems (Linux).

Although it is very difficult to keep up with every one of the latest trends, we need to be extremely careful that we do not develop blind spots in our investigative abilities. If at the current time your lab or investigative department lacks the ability to deal with Macintosh computers or devices, you have a glaring blind spot that needs to be addressed. ☒

References

Forensic Software for Macs

<http://www.macforensicslab.com>

<http://www.blackbagtech.com>

Books

Seibold, C. (2008). Big book of Apple hacks – first edition. Sebastopol, CA: O'Reilly

Singh, A. (2006). Mac OS X internals: A systems approach. Indianapolis: Addison-Wesley

URLS

<http://www.cyberforensics.purdue.edu>

http://www.seminars.apple.com/seminaronline/forensics/apple/index.html?s=207&loc=us_en

<http://www.macosxforensics.com>

List Servers

appleforensics@lists.apple.com