B20 A Survey of Data Deletion Applications for OS X Systems

Jonathan P. Fowler, MS, First Advantage Litigation Consulting, 1828 L St NW, Ste 1070, Washington, DC 20036*

After attending the presentation, attendees will have a general understanding of the types of data deletion software currently available for OS X systems, the basic functions of each program, and examples of artifacts left behind by each program upon installation and usage.

This presentation will impact the forensic science community by providing useful information for digital forensics examiners to assist in identification of data destruction activity on suspect computers running the OS X operating system. Although geared primarily toward an audience of digital forensics investigators/analysts/examiners, it is also well suited for attorneys, paralegals, or other legal professionals who often deal with the ramifications of the answers provided to the question posed at the outset.

During the course of an investigation, digital forensics investigators are often presented with this relatively simple question by prosecutors, defense attorneys, or supervisors—"Did the person delete anything from their computer?" The reality is, while the question in and of itself is seemingly simple, depending on the type of operating system in play, attempting to determine the answer to that question can be devilishly difficult.

Over the years, the Digital Forensics (DF) community as a whole has developed multiple tools and techniques to assist in answering that question. Drawing on one of the core tenets of criminological theory, Locard's Exchange Principle, one of those techniques is to identify what artifacts are left behind by the installation and subsequent running of data destruction software. Although considerable resources have been spent by the DF community to identify those artifacts—both from the software itself as well as from the operating system—the vast amount of those resources were spent primarily on computers running some version of the Windows operating system. Th goal is that this presentation helps to change that approach.

With the growing popularity of Apple's Macintosh family of computers, more resources will need to be expended to increase the community's collective knowledge of the same types of artifacts that have already been identified on Windows-based systems. This further affects the DF community because, while computers running Windows operating systems still have a virtual stranglehold on the corporate market, a January 2012 article in the *Wall Street Journal* reported that General Electric has a pilot program that allows its employees to choose Apple desktops or laptops running OS X instead of a PC running Windows. According to a *Wall Street Journal* article, around 1,000 employees are currently using an Apple computer (which represents less than 1% of the overall users at G.E.); however, more employees are taking advantage of the program as it becomes more widely known.[1]

A prime example of the disparity between the emphases placed on research of data deletion artifacts between Windows and OS X platforms can be found in one of the well-respected digital forensics books on the market today, *Handbook of Digital Forensics and Investigation*, edited by Eoghan Casey. In Chapter 5 of that book, titled "Windows Forensic Analysis," six pages are devoted to the topic "Deletion and Destruction of Data."[2] In comparison, Chapter 7 of that book, titled "Macintosh Forensic Analysis," contains no such section; however, references to data deletion can be found scattered throughout the chapter.[3]

References:

1. "Apple Macs Land on More Corporate Desks, *Wall Street Journal*, January 18, 2012
2. *Handbook of Digital Forensics and Investigation,* Casey, Eoghan (ed.), 2010
3. *Handbook of Digital Forensics and Investigation,* Casey, Eoghan (ed.), 2010

OS X, Macintosh, Data Deletion

 ** Presenting Author*