B20 Macintosh® Forensics: A Crash Course

Gavin W. Manes, PhD, Avansic: E-Discovery and Digital Forensics, 401 South Boston Avenue, Suite 1701, Tulsa, OK 74103*

The goals of this presentation are to discuss: (1) data preservation and forensic collection from a Macintosh® system; (2) forensics investigation of a Macintosh® system; (3) differences between Windows™ and Macintosh® systems related to forensic collection and investigation; and, (4) additional challenges of the Macintosh® based on file system structure, file formats, and caches.

This presentation will impact the forensic science community by providing the basic tools and techniques to forensically acquire Macintosh® computers. Participants will also be aware of the complexities and difficulties of Mac computers vs. Windows™.

Most investigators spend their time an energy learning and keeping up with the latest tools and techniques for Windows™ investigators. However, the steadily increasing market share of Mac OSX means that most investigators will find themselves in a position to examine these systems. This presentation will give forensic investigator with little knowledge of the Mac OSX platform the basic knowledge necessary to acquire and analyze one of these systems.

The first step in any digital forensics investigation is to imaging evidence drives. However, Apple® has made it very difficult to work with hardware components, meaning that this seemingly simple task can become a complicated operation. A brief overview will be given of how to “crack the cases” for some of these machines and retrieve hard drives for imaging. Alternative means of acquiring images will be discussed, particularly when hardware, time, or other circumstances require that clever techniques be employed. Solutions presented will include the well-known “Firewire Target Mode” workaround, as well as instructions in using common Live CDs for imaging Apple® computers.

Once the basics of acquisition have been covered, A basic overview of the of the Mac OSX file system will be provided. The basic challenges to investigators will be described, the tools used to address those challenges, and the differences in the ways that each of those tools approaches the problems. Interpretation of HFS+ MAC times and unusual file types that have significant evidentiary value will be discussed. Other important evidence caches include information related to such user activity as web browsing, file usage, iPod and iPhone usage.

Working with Macintosh® computers is an increasingly necessary tool in the forensic investigator’s arsenal. But the Macinstosh operating system has proved a very unique beast with its own set of challenges, requiring a body of specialized knowledge to tackle it effectively. The

goal of this presentation is to familiarize the investigator with many of these basic problems and arm them with the some of the tools needed to level the playing field.

Digital Forensics, Data Preservation, Investigation

* *Presenting Author*