B21 Macintosh® PList Files: Hidden Information for Digital Forensics Investigators

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

The goals of this presentation are to: (1) educate the audience about forensically relevant information contained within Macintosh® Plist files; (2) discuss the basic structure, functions, and location of Plist files; and (3) provide the audience with tools and information to appropriately interpret Plist files (particularly those who have digital forensics experience).

This presentation will impact the forensic science community by arming attendees with techniques and information in order to retrieve forensically relevant information from Macintosh® Plist files.

Although extremely common in system running Mac OSX and devices such as the Apple® iPhone and iPad, the structures of Apple® plist files remain mysterious to many forensic investigators. This creates an obstacle for many investigators tackling OSX systems, since plist files contain valuable information relevant to forensic investigations. Further complicating the issue, graphical interfaces for handling with these files are confusing and primitive at best.

An in-depth overview of the Apple® plist format in all of its incarnations, including the “binary,” “XML,” and “ASCII,” or “old- fashioned” formats will be given. Furthermore, information will be provided to help decode other formats an investigator may consider “unusual” that are sometimes seen stored in plist files relevant to forensic investigations. These include formats such as the “alias records,” which can be found storing potentially useful information about files that may exist in different locations across a system.

Finally, tips to efficiently process and analyze these files when encountered in the field using several readily available tools will be provided. The structure of commonly examined plist files will be discussed, along with important practical examples for handling some of the more complex structures.

This will give investigators inexperienced with this aspect of Mac OSX investigations a deep and informative look at what challenges might be normally encounter in the field.

Digital Forensics, Investigation, Computers

** Presenting Author*