C20 An Analysis of Apple® Mobile Devices to Support or Refute Claims of Spoliation of Data

Andrew N. Crouse, BA, Epiq Systems, Inc, 1300 Pennsylvania Avenue, NW, Ste 851, Washington, DC 20004; and Samuel I. Brothers, BBA*, 6643 Patent Parish Lane, Alexandria, VA 22315*

The goal of this presentation is to present forensic analysis and case studies of Apple® iOS® mobile device data in connection with claims of data spoliation.

This presentation will impact the forensic science community by discussing various key forensic artifacts analysts can use to confirm or refute claims of data spoliation from Apple® mobile devices that may arise during civil proceedings.

In both criminal and civil court proceedings, the hiding or destruction of digital evidence can be an obstruction investigators and attorneys encounter. These same acts can also provide key evidence in both criminal and civil cases. Specifically, in civil cases, the intentional or negligent act of destroying evidence that is relevant to a legal matter can lead to spoliation sanctions against one party, including financial penalties and dismissal of a case with prejudice. Spoliation claims involving digital evidence have been routinely investigated on computer hard drives using standard digital forensic methods and tools. With the ever-rising popularity of mobile devices in the business world, especially Apple® iPhones® and iPads®, more and more relevant digital evidence is being stored on these devices, requiring digital forensic examiners to confirm or refute claims of spoliation in civil proceedings.

The examination of deleted data is generally performed on physical images of storage media. Ever since the release of the iPhone® 4s and the iPad® 2, Apple® iOS® technology has enabled security features that do not permit the capture of full physical images of Apple® mobile devices without first circumventing the native iOS® security layers, otherwise called "jail breaking." E-Discovery collections for civil matters do not generally involve the bypassing of iOS® security layers or jail breaking custodian devices in order to obtain a physical image. As a result, digital forensic practitioners performing data collections and forensic analysis in civil matters have had to rely on available evidence from logical file systems (as opposed to physical images) obtained through items such as Apple® iTunes® and iCloud® backups, as well as Apple® File Connection (AFC) data.

This presentation will focus on key data areas within an iOS® mobile device that can help digital forensic examiners confirm or refute spoliation claims. Analysis of various areas of mobile devices will include artifacts relating to Mobile Device Management (MDM) policies, various device reset actions, and text message retention/forwarding policies. An analysis of artifacts present on erased iPhones® will be discussed, along with a comparison of extracted data from erased iPhones® that have been restored with previously backed up data using both Apple® iCloud® and Apple® iTunes®. Case studies involving the forensic analysis of spoliation claims from Apple® mobile devices will also be presented with the analysis to demonstrate real-world practical scenarios.

Apple® iOS®, Data Spoliation, Mobile Devices

*Presenting Author