C32 Reevaluating the Mobile Forensic Acquisition Levels

Troy Lawrence, BBA, Fort Worth Police Department, Fort Worth, TX 76107; Umit Karabiyik, PhD*, Purdue University, West Lafayette, IN 47907*

Learning Overview: After attending this presentation, attendees will be able to clarify the confusion in mobile device acquisition methods as well as understand the current acquisition methods and their impact on the devices with respect to rapidly changing technology.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing an updated common framework for mobile device acquisition in digital forensics investigations.

Mobile Device Forensics (also known as Mobile Phone Forensics) is a subdiscipline of Digital Forensics, much like Computer Forensics, Audio Forensics, and Forensic Video. This subdiscipline is relatively new and did not begin to gain popularity until just prior to the invention of the iPhone® in 2007. Forensic examiners used manufacturer-developed tools designed to backup user data or were forced to photograph data as it was displayed on the screen prior to the development of mobile device forensic tools. It was during this time frame that a schema was developed to categorize the types of forensic tool capabilities. In 2008, Sam Brothers, a mobile forensic examiner working for the United States Customs and Border Protection, first articulated the current classifications of mobile device forensic tools.[1] The five levels of classification for forensic tools include: (1) manual extraction, (2) logical extraction, (3) hex dump/JTAG, (4) chip-off, and (5) micro read.

The pyramid diagram was later incorporated into the National Institute of Standards and Technology's (NIST's) SP800-101r1 and is referenced in many books, documents, and articles describing not only the forensic tool classifications but also the elevated levels of data acquisition.[2] For years, Mobile Device Forensic examiners have been well-served using Brothers' popular pyramid listing five levels of data acquisition from mobile devices. However, processing methods have evolved over the ten years since the diagram was introduced. There is confusion regarding which level of extraction applies to a process as new techniques are continually being developed. A re-evaluation of the Mobile Forensic acquisition levels and the associated tool capability pyramid graphic is needed to reflect the current methods of mobile device acquisition and their impact on the devices. Some of the more advanced levels of acquisition may require extensive training and years of practice to become proficient in their use. Others may require no specific skills other than operating a camera to photograph a screen. Regardless, the levels of acquisition need to be properly identified based upon the type of data collected, how it is collected, and whether it may damage the device.

The presenters will provide clarity to the extraction process and propose an update to Sam Brothers' forensic tool categories of acquisition as well as adequately describe each option currently available. Although it may be necessary in the future to update these processes as new acquisition techniques become available, it is believed that the updated framework will serve the digital forensics community for better understanding of the acquisition methods with respect to the state-of-the-art mobile device investigations.

Reference(s):

1. Samuel Brothers. *Cell Phone Forensic Tool Classification Pyramid.* Presented at Mobile Forensics World 2008, Breakout Presentation, Chicago, IL, May 2008.
2. Wayne Jansen, Rick Ayers, Sam Brothers. Guidelines on Mobile Device Forensics. *NIST Special Publication* (2014): 800-101.

Digital Forensics, Mobile Devices, Acquisition Levels