C13 Unlocking Apple® Mobile Devices: A Forensic Practitioner's Perspective and Lessons Learned

Christina A. Malone, MSFS, Defense Forensic Science Center, Forest Park, GA 30305; Joseph Levi White, MS*, Defense Forensic Science Center, Forest Park, GA 30297*

Learning Overview: After attending this presentation, attendees will have an understanding of the current capabilities of GrayKey as it applies to specific case examples at the Defense Forensic Science Center (DFSC).

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating the benefits and limitations of GrayKey as it pertains to the unlocking and extraction of data from mobile devices in a digital forensics laboratory.

Smart phones are becoming increasingly important in digital evidence investigations. Obtaining data from a smart phone may assist in cases dealing with any number of criminal activities, including theft, sexual assault, and homicide. Evidence extracted from mobile devices may include pictures, call logs, text messages, e-mails, videos, and documents. While this evidence may be critical to a case, accessing the information may prove difficult, especially if the device is locked with enhanced security methods (Personal Identification Number [PIN]/passcode lock, pattern lock, fingerprint, facial recognition, etc.) or utilizes data encryption.

The Apple® iPhone® is one of the most popular smart phones within the United States. Bypassing the security features of Apple® mobile devices to gain access to any maintained data is of great importance to law enforcement and digital forensic examiners. One primary tool used for gaining access to locked Apple® mobile devices is the topic of this presentation.

The tool is a device that allows users to attempt to access locked Apple® iOS® devices within their own facilities. Apple® mobile devices are connected one at a time to the unit, which uses proprietary software to gain access to the device. Once access is gained, the tool performs two actions. First, software designed to determine the unknown passcode is introduced to the mobile device. Second, data is extracted from the device, with accessibility to certain types of data dependent on the security status of the device. When an iOS® device is first powered on, it is in Before First Unlock (BFU) mode. Once the passcode has been entered on the device, it switches into After First Unlock (AFU) mode. Prior to determining the passcode of the mobile device, the tool can perform both BFU and AFU partial file system extractions. After the unknown passcode is determined, the full contents of the file system may be obtained.

The tool has been used in numerous cases at the DFSC since the fall of 2018. In addition to completing routine data extractions from mobile devices, many lessons and unique scenarios have been encountered since the introduction of this capability at the DFSC. During this presentation, insight will be given into the types of scenarios that have been encountered, as well how obstacles have been addressed. Several unique case examples will be highlighted by both an experienced digital forensic examiner and an examiner new to mobile forensics. The experiences and lessons learned will demonstrate how the tool has been implemented in a forensic laboratory setting.

The opinions or assertions contained herein are the private views of the authors and are not to be construed as official or as reflecting the views of the Department of the Army (DA) or the Department of Defense (DoD). Names of commercial manufacturers or products included are incidental only, and inclusion does not imply endorsement by the authors, DFSC, United States Army Criminal Investigation Command, Office of the Provost Marshal General, DA, or DoD.

Mobile Device Forensics, Cell Phone Forensics, Digital Extraction

*Presenting Author