## C36 A Constantly Moving Target: Best Practices for Apple® iOS® Device Seizure, Access, and Extraction

*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 best practices for seizing Apple® iOS® devices to ensure a higher probability of obtaining access to any valuable maintained data.

**Impact on the Forensic Science Community:** This presentation will impact the forensic science community by demonstrating the current best practices for seizing and processing various Apple® iOS® mobile devices. This presentation will demonstrate how the methods used during seizure and submission to a laboratory may dictate the potential unlocking capabilities, extraction capabilities, and types of data that can be obtained.

Evidence maintained on mobile devices, such as the Apple® iPhone®, may be critical to a case, but the advanced security measures (encryption, Personal Identification Number (PIN)/passcode lock, pattern lock, fingerprint, facial recognition, etc.) enabled on the majority of newer mobile devices to protect the owner from unauthorized access to their personal device also stands in the way of the digital forensic examiner. The actions taken by the first responder, the initial person to seize and/or interact with the mobile device, the evidence custodian, any triage personnel, etc., all may have a drastic impact on what can be done to obtain data from that device later in a laboratory setting.

Many, if not most/all, law enforcement/crime scene agencies and forensic science laboratories adhere to strict methods and/or policies and procedures for seizing evidence, conducting an inventory, photographing the evidence, processing the evidence through the laboratory, and issuing reports. These policies and procedures are required for obtaining and maintaining agency/laboratory accreditation. The problem lies within the fact that many of these policies and procedures, if adhered to, will result in either the loss of digital data or the loss of access to digital data maintained on locked iOS® devices.

This presentation will highlight multiple current typical mobile device seizure/processing methodologies and their potential impact on casework. As specific actions are taken with an iOS® device, access and security features utilized by laboratory personnel to gain access to the device may be altered. Something as simple as removing the Subscriber Identity Module (SIM) card from the device for evidence inventory can disable future biometric (facial identification or fingerprint) access to the device. Powering off mobile devices at seizure is a typical practice for evidence storage and transfer, but this action changes the lock state on iOS® devices from After First Unlock (AFU) to Before First Unlock (BFU) mode. This change from one of the device's least secure states (AFU) to one of the most protected states (BFU) causes an iOS® device to block access to various types of data maintained on the device. The timeline from device seizure to obtaining access to maintained data has become very critical. With each passing second, there is a greater potential for evidentiary data to be deleted from the device or blocked from future access.

Due to seemingly constant security and feature updates to the Apple® iOS® operating system, best practices for iOS® device seizure and processing are constantly evolving. With each new software release, digital forensic examiners must be willing to adjust and implement changes to methods and/or policies and procedures quickly to remain steady on the moving target of defeating advanced mobile device security.

*The opinions or assertions contained herein are the private views of the author 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, the Defense Forensic Science Center (DFSC), the United States Army Criminal Investigation Command, the Office of the Provost Marshal General (OPMG), the DA, or the DoD.*

**Apple® iPhone®, Mobile Forensics, Cell Phone Forensics**