B31 Mobile Device Tool Testing

Richard Ayers, MS, 100 Bureau Dr, Mailstop 8970, Gaithersburg, MD 20899-8970*

After attending the presentation, attendees will be aware of the importance of tool testing and gain an understanding of the mobile device tool testing process conducted within the Computer Forensics Tool Testing (CFTT) project.

The presentation will impact the forensic science community by increasing awareness of the role of tool testing in informing the forensic community of tool capabilities and limitations. Test reports provide a foundation for toolmakers to improve tools, help users to make informed choices, and provide interested parties with an overview of any anomalies found. The presentation will provide an overview of the motivation behind testing mobile device forensic tools and the challenges faced by toolmakers and forensic examiners.

The CFTT project has spent several years researching and testing forensic tools capable of acquiring data from the internal memory of mobile devices and Subscriber Identity Modules (SIMs). This presentation discusses all aspects of the testing process that are critical for producing a test report.

The development of mobile device forensic tools and acquisition techniques continues to grow within the field of digital forensics. Mobile subscribers far outnumber personal computer owners and studies have shown an increase of mobile device personal data storage compared to personal computers. Higher-end mobile devices present users with advanced features and capabilities similar to those of a personal computer. Mobile devices provide users with the ability to maintain contact information, upcoming appointments, day-to-day activities, important news events, and provide the ability to correspond with friends and family via telephony, text message, email, chat, and social networking sites. Over time, mobile devices can accumulate a sizeable amount of information about their owners. Data acquired from these devices may be useful in criminal cases or civil disputes.

As mobile device usage and sophistication continue to grow, so does the need for tool validation. For acquired information to be admissible in a court of law, verification of a tool's behavior and strict forensic acquisition methods are paramount. Potentially, one piece of data acquired from a mobile device may play a critical role in shedding light on an incident or, possibly, criminal activity. The need for rigorous testing conducted on a combination of forensic tools and specific families of mobile devices is critical for providing law enforcement and forensic examiners informative test results yielding known expectations of a tool's behavior, capabilities, and limitations. Over the past three years, the CFTT project at the National Institute of Standards and Technology (NIST) has tested numerous mobile device forensic tools capable of acquiring data from mobile devices operating over Global System for Mobile (GSM) communications and Code Division Multiple Access (CDMA) networks.

The presentation covers information on the motivation behind testing mobile device forensic tools, specification and test plan development, creation of a known data set, mobile device data population, and tool testing.

Mobile Forensics, Digital, Testing

 ** Presenting Author*