C5 Mobile Device Data Population for Tool Testing

Jenise Reyes-Rodriguez, BS, NIST, 100 Bureau Drive, Gaithersburg, MD 20899; and Richard Ayers, MS, 100 Bureau Drive, MS 8970, Gaithersburg, MD 20899-8970*

After attending this presentation, attendees will be aware of the importance of populating and documenting the internal memory of mobile devices in preparation for tool testing and will better understand the mobile device data elements and various data population techniques.

This presentation will impact the forensic science community by increasing awareness of the impact the tool testing process has on informing the forensic community of tool capabilities and limitations. Test reports provide a foundation for toolmakers to improve tools, help users make informed choices, and provide interested parties with an overview of any anomalies found. This presentation will provide an overview of techniques for populating and documenting the internal memory contents of mobile devices used for testing mobile forensic tools.

The Computer Forensics Tool Testing (CFTT) project has been researching and testing forensic tools capable of acquiring and analyzing mobile device forensic tools. This presentation discusses all aspects in preparation for testing tools critical for producing a test report.

Techniques for documenting and populating the internal memory for the following data elements will be discussed: (1) subscriber/equipment data — International Mobile Station Equipment Identity (IMEI), Electronic Serial Numbers/Mobile Equipment Identifiers (ESN/MEID), Integrated Circuit ID (ICCID), and Mobile Station International Subscriber Directory Number (MSISDN); (2) address book/contacts — contact name, number, and contact metadata; (3) Personal Information Management (PIM) data — databook, calendar, memo entries; (4) call logs — incoming, outgoing, missed calls, and call log metadata; (5) Short Message Service (SMS) messages — incoming, outgoing, drafts, and SMS message metadata; (6) Multimedia Messaging Service (MMS) messages — incoming, outgoing, drafts, picture, audio, and video MMS messages; (7) stand-alone files — graphic, audio, and video; (8) application-related data — native mobile device applications; (9) social media-related data — Facebook®, Twitter®, and LinkedIn®; and, (10) Global Positioning System (GPS) -related data — longitude/latitude coordinates for routes, checking-in, geo-tagged photos, and videos.

When testing mobile device forensic tools, it is advantageous to possess knowledge of the internal memory contents of the mobile device(s) used. Documentation of the internal memory contents provides the tester with the ability to determine if the forensic application is acquiring and reporting data completely and accurately. Techniques covered in the document are as follows: (1) email account data syncing: — populating the internal memory of a mobile device by pairing and syncing data contents (e.g., contacts, calendar entries, stand-alone files, etc.); (2) Wi-Fi data transfer — populating the internal memory of a mobile device with Wi-Fi capabilities over an internet-connected router; (3) Personal Computer (PC) synchronization — PC sync software provides the user with the ability to transfer data elements from a PC to the mobile device; and, (4) Bluetooth® data transfer — data transfer between two mobile devices that provide Bluetooth® data transfer facilities.

This presentation provides an overview of populating the internal memory of mobile devices in preparation for the CFTT testing process.

The mobile device data population setup guide is available from the CFTT web site: https//www.cftt.nist.gov/mobile_devices.htm.

Mobile Forensics, Digital, Tool Testing

*Presenting Author