C7 Validating Mobile Forensics Tools in Your Lab With the National Institute of Standards and Technology's (NIST) Federated Testing

Barbara Guttman, BA, National Institute of Standards & Technology, Mail Stop 8970, Gaithersburg, MD 20899-8970; James R. Lyle, PhD, National Institute of Standards & Technology, 100 Bureau Drive, MS 8970, Gaithersburg, MD 20899; Benjamin R. Livelsberger, MS, National Institute of Standards & Technology, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899-8970; Richard Ayers, MS, National Institute of Standards & Technology, 100 Bureau Drive, MS 8970, Gaithersburg, MD 20899-8970; and Jenise Reyes-Rodriguez, BS, National Institute of Standards & Technology, 100 Bureau Drive, Gaithersburg, MD 20899*

After attending this presentation, attendees will be aware of a tool that can help test mobile forensics tools in a lab using the Computer Forensic Tool Testing (CFTT) Federated Testing Forensic Tool Testing Environment developed by the NIST.

This presentation will impact the forensic science community by increasing awareness of the capabilities of Federated Testing when applied to tools capable of extracting data from mobile devices and associated media (e.g., Universal Integrated Circuit Cards (UICCs)/Subscriber Identity Modules (SIMs)). This presentation will provide examples of using the Federated Testing Mobile Devices Test Suite to test mobile forensic tools in the same fashion as a digital forensics laboratory would conduct validation testing. In addition, by documenting the resource commitment required to perform the tool testing, forensic practitioners will be able to estimate the cost in time and effort to test mobile forensic tools in their laboratory. This presentation will aid the forensic practitioner choosing to use Federated Testing by providing examples of using the Federated Testing Mobile Test Suite to test actual mobile forensic tools, much as a digital forensics laboratory would conduct validation testing.

The CFTT project at NIST develops methodologies for testing digital forensic tools. Currently, there are CFTT methodologies for testing the following: disk imaging, write blocking, deleted file recovery, file carving, forensic media preparation, and mobile devices.

A variety of tools in each of these categories have been tested and observed flaws in the tools have been reported by the National Institute of Justice (NIJ) and the Department of Homeland Security (DHS). These results can be used as a basis for identifying the types of likely failures that occur in forensic tools. Currently, CFTT has implemented testing disk imaging, hardware write blocking and mobile forensics tools into Federated Testing.

Using Federated Testing has several advantages: (1) it relieves a forensic laboratory of the task of developing a test plan for tool testing because Federated Testing generates a test plan based on selections made by the user describing how the laboratory uses the tested tool (a list of test runs; detailed procedures for documenting and populating mobile devices with known active and deleted content; detailed procedures for performing essential and optional test runs; and tools to generate a skeleton test report that can then can be prepared in the style favored by the laboratory); (2) the test reports can be shared with other laboratories; and, (3) completed test reports can be submitted to CFTT for administrative review and, if no issues are found, the report is passed on to the vendor for comment. The final report is published by the DHS, Science & Technology Directorate, Cyber Security Division.

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the authors or the authors' employers, nor does it imply that the products are necessarily the best available for the purpose.

Digital Forensics, Tool Testing, Mobile Forensics

*Presenting Author