C8 New in Computer Forensics Tool Testing's (CFTT's) Mobile Forensics—SQLite, SQLite Recovery, and a New Federated Testing Tool

Jenise Reyes-Rodriguez, BS, National Institute of Standards and Technology, Gaithersburg, MD 20899; Barbara Guttman, BA*, National Institute of Standards and Technology, Gaithersburg, MD 20899-8970; Richard Ayers, MS*, Gaithersburg, MD 20899-8970*

Learning Overview: After attending this presentation, attendees will be familiar with the three major updates CFTT is working on to enhance its testing methodology.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing an overview of the current updates happening within CFTT's Mobile Forensic project and how the updates will be beneficial to forensic tool users in general.

The SQLite extension to the mobile forensic tool testing and the new specification for SQLite data recovery will provide a more thorough set of results to the forensic community. There are forensic tools designed or focused on SQLite data recovery, thus the creation of a new and separate specification tailored to SQLite data recovery only. This will inform the users about the handling of SQLite database files by the tools used during an investigation.

In addition, CFTT is working on a new Federated Testing tool. There are multiple forensic tools on the market with different versions, as it is expected. The Federated Testing project is an expansion of the CFTT program that provides test suites, using National Institute of Standards and Technology (NIST) methodology, for tool testing within the labs. The test suites allow users to test their own tool version, especially if it has not been tested by the CFTT project. The new version of Federated Testing will be portable, allowing users to run it on Windows® 10 without the need for installing any software.

The goal of the new project, within CFTT, and expansions of existing specifications is to establish and enhance the testing methodology to then apply it to newer forensic tool versions. This will provide tool makers with necessary information to improve their tools, users with would gather more information that will help them select the appropriate tool(s), and, last, help interested parties to understand the tool's capabilities.

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 author or the author's employer, nor does it imply that the products are necessarily the best available for the purpose.

Mobile Forensics, SQLite Data Recovery, Federated Testing