C18 Federated Testing: Shared Test Materials From the Computer Forensics Tool Testing (CFTT) Program at NIST for Digital Forensics Tool Validation and Shared Test Reports

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

After attending this presentation, attendees will be familiar with the Federated Testing materials being developed by Computer Forensics Tool Testing (CFTT), understand how they can be used in their labs to timely and effectively validate tools, and learn how the Federated Testing initiative encourages shared tool validation results. Federated Testing at the National Institute of Standards and Technology (NIST) is an expansion of the CFTT Program that provides digital forensics labs and practitioners with test materials for tool validation.

This presentation will impact the forensic science community by providing information as to how the NIST Federated Testing materials can be used in digital forensics labs for tool validation at a savings of time and expense and how the Federated Testing materials support shared tool validation results.

Forensic tools need to be validated before being used in the forensic process. These tools need to be validated: (1) to ensure that digital evidence is being correctly processed; and, (2) to support the admissibility of digital evidence in court and legal proceedings. Tool validation is difficult, expensive, and time consuming.

The various federal, state, and local digital forensics laboratories use the same tools or the same types of tools. It follows that a lot of work is duplicated in tool validation. The CFTT program currently creates tool specifications, test methods, and test reports. The goal and purpose of Federated Testing is to simplify, package, and export the CFTT test methodologies and the expertise used to produce the NIST test reports to laboratories and individual examiners for use in tool validation.

The Federated Testing initiative offers several anticipated benefits to laboratories and examiners. A primary benefit is one of time and cost savings. If laboratories can use the NIST methodology and materials for tool validation, they save the time otherwise spent to develop their own. Federated Testing can also improve the quality of testing. CFTT's shared test materials additionally present a new opportunity for shared tool validation reports. A current barrier for laboratories for sharing tool validation results is that each laboratory will test a tool differently. A further barrier is dissimilar formats between laboratories for documenting and presenting tool validation results. This makes it difficult for a laboratory to understand how an externally validated tool was tested and to determine if the tests and validation results are acceptable for use in their own laboratory.

When tools are validated using the CFTT shared test materials, a common methodology is used and the results are reported in a common format. This makes it easy for a laboratory receiving a shared validation report to quickly understand how a tool was tested and to determine whether the validation results are acceptable and applicable for use in their own laboratory. Tool validation results from CFTT's Federated Testing shared test materials can be shared informally between laboratories, could be submitted to and shared via public websites such as the Department of Homeland Security Science and Technology (DHS S&T) -sponsored cyberfetch.org or CFTT's Computer Forensics Tool Catalog, or be kept private within the tester's organization.

Federated Testing is a work in progress. CFTT currently has test methodologies for disk imaging, forensic media preparation, hardware write blocking, deleted file recovery, mobile device acquisition and analysis, and file carving. CFTT is first implementing Federated Testing for disk imaging; test materials for the other functionalities will follow.

The test materials are being packaged on a live Linux® Digital Video Disc (DVD). The materials consist of the DVD, which contains video tutorials on how to use the materials, a website, and command line test support tools. Using the website, users select the type of tool they wish to test (e.g., disk imaging tool), then select the specific features they wish to validate. This results in a list of the tests to run in order to test these features, along with the steps and instructions for each test. The test instructions reference CFTT's test support tools. Run from the command line on the DVD, the support tools are used to set up each test and to analyze the results. When all the tests have been run, the website generates the tool validation results in the CFTT Federated Testing common report format.

Digital Forensics, Tool Validation, Federated Testing

Copyright 2015 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.