C19 Experience Validating Disk-Imaging Tools With Computer Forensic Tool Testing (CFTT) Federated Testing

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

After attending this presentation, attendees will be aware of the CFTT Federated Testing forensic tool-testing environment utility that is used for validating disk-imaging tools.

This presentation will impact the forensic science community by increasing awareness of the capabilities of Federated Testing when applied to real imaging tools. This presentation will provide examples of Federated Testing on actual disk-imaging tools, in the same manor 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 disk-imaging tools in their laboratory. This presentation will aid the forensic practitioner choosing to use Federated Testing by providing examples of using Federated Testing to test actual disk-imaging tools, much as a digital forensics laboratory would conduct validation testing.

The CFTT project at the National Institute of Standards and Technology (NIST) develops methodologies for testing computer 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 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) a list of test cases (based on user input); (b) tools and detailed procedures for creating test drives (adding known content); (c) detailed procedures for running each test case; (d) tools to evaluate test results; (e) tools to generate a skeleton test report that can then can be finished in the style favored by the laboratory; (2) the test reports can be shared with other laboritories; 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.

In this round of testing, the following tools were tested, making slight variations in feature selection:

Tool	Version
FTK	3.4.2.6
Guymager	0.8.1
Logicube Falcon	2.4U1
Logicube Falcon	3.0U1
Paladin/ewfacquire	6.09/20160403
Paladin/dc3dd	6.08/7.1.614
X-Ways	18.8
dc3dd	7.2.641
Ditto FieldStation	2016 Mar01
Tableau TD2u	1.1.2.3948-4270f9c

Temporal and physical resources to measure the level of commitment that was required to test each tool were tracked. It was found that with two PCs, a single practitioner could set up test drives in just a few hours. The drives can be set up faster if more Personal Computers (PCs) were devoted to the task. After the test drives are set up, running the tests takes less than two days. The most time expended is actually taking the generated skeleton test report and adding laboratory-specific information.

If a laboratory uses (or just wants to test) more than one imaging tool, the drive set up only needs to be executed once and can be reused for additional tool testing.

Digital Forensics, Tool Testing, Disk Imaging