Federated Testing: Shared Test Materials from the CFTT Program at NIST for Digital Forensics Tool Validation and Shared Test Reports

DFRWS – August 11, 2015

Ben Livelsberger
NIST
Information Technology Laboratory,
CFTT Program
The Computer Forensics Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.

CFTT develops test methodologies and tests selected tools.

Directed by a steering committee composed of representatives of the law enforcement community.

CFTT is a joint project of: DHS, NIST/SPO, FBI, DoD, Secret Service, NIJ and other agencies.
What is Federated Testing?

- Federated Testing is an expansion of CFTT to provide the digital forensics community with:
  - test materials for validating digital forensics tools and
  - to support shared test reports.
Tool Validation – Why?

Why do Labs Perform Tool Validation?
- Demonstrates reliability of results
- Identifies tool limitations
- May support admissibility of results
- May be required for lab accreditation
State of Tool Testing

- Test Reports
  - CFTT, published through DHS S&T
  - Department of Defense Cyber Crime Center, U.S. Law Enforcement
  - Other agencies and labs, in-house

- Tool testing is expensive

- Duplicated work
Barriers to sharing test results

Idea: share test results

Barriers:
- Labs test differently
- Dissimilar report formats
Federated Testing Proposes

- Shared test materials from CFTT:
  - Use a common test methodology
  - Common test data sets with known ground truth
  - Use a common test report format

- Sharing Test Reports
  - Via public websites, e.g., DHS S&T
  - Informally between labs
  - Kept private
Target Areas

- CFTT has methodologies for:
  - Disk Imaging
  - Hardware Write Block
  - Mobile Devices
  - Forensic Media Preparation
  - Deleted File Recovery
  - File Carving

- Implementing:
  - Disk Imaging
What do the test materials look like?

- Download live Linux® CD .iso file

- Components:
  - User Interface
    - Select tool features to test
    - Instructions for creating test data and for running test cases
    - Generate test report
  - Command line test support tool
    - Setup test cases and analyze the results
User Interface - Home

Welcome to the CFTT Federated Testing DVD

Welcome to the Federated Testing DVD produced by the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST). The purpose of this DVD is to allow forensic labs to test their forensic tools with the same rigor as CFTT (see www.cftt.nist.gov) and to generate sharable test reports with the test results.

To get started, select the type of tool you want to test from the menu on the left.

If you need help, have questions call (301) 975-4411 or email cftt@nist.gov
Disk Imaging Home

Federated Testing

Home > Disk Imaging Home

Disk Imaging Home

We understand that you might normally test a disk imaging tool differently than we do. It is critical to understand how this website functions and how the steps fit together to test your tool. See the videos at www.cfft.nist.gov/federated-testing.html or fl_disk-imaging-tutorial.pdf.

Use the sidebar menu on the left to navigate the Disk Imaging test materials.

Follow these key steps to test your Disk Imaging tool:

1. Prepare a dedicated removable flash drive to store your test log files and test information using the ‘Format Your Log Drive FT-LOGS’ page. **IMPORTANT!!! DO NOT SKIP!!!**
2. Generate the list of tests to run for your tool using the ‘Generate Test Cases & Start Testing’ pages.
3. Run each test to test your tool. If you have to reboot your computer, use ‘Go to Test Dashboard’ to return to the Test Dashboard.
5. Submit the test report and your testing log files to CFFT (if approved by your management) to share with the forensics community! See ‘Share Your Results’ for instructions on how to share your test results.

The other sidebar selections are navigational aids:
- Use the ‘Disk Imaging’ link to return to this page.
- Use the ‘Video Tutorials’ link to access short video tutorials on how to use this website and test your tool.
Selecting Tool Features

Federated Testing

Disk imaging selections
- Disk Imaging
- Video Tutorials
- Format Your Log Drive
- 'FT LOGS'
- Generate Test Cases & Start Testing
- Go to Test Dashboard
- Generate Test Report
- Share Your Results
- View Test Case instructions
- View Visual Guides
- View Common Procedures
- View Media Setup

Select the Features of Your Disk Imaging Tool to Test

Use this page to select the features of your tool (either a hardware device or software running on a computer) you want to test. IMPORTANT: SELECT ONLY THE FEATURES YOU WANT TO TEST YOUR TOOL FOR.

You need to specify the following:
1. The name and version of your tool
2. At least one hash algorithm
3. The features you want to test your tool for

1 Tool Name and Version
Enter the tool name: Tool A
Enter the tool version: 1.3

2 Hash Algorithms
Select the hash algorithms that you want to test for your tool. Note: selecting multiple algorithms will not slow down testing significantly.
- MD5
- SHA1
- SHA256
- SHA512

3 Tool Features to Test
Select the tool features you want to test. SELECT ONLY THE FEATURES YOU WANT TO TEST YOUR TOOL FOR.

- Operations on DRIVE Interfaces (e.g., USB, SATA, SCSI)

What operations on physical devices (e.g., SATA or ATA hard drive) do you want to test?
Tests To Run

Test Dashboard

Based on the features you selected, these test cases need to be run. If you have 2 PCs available for testing your tool (1 PC dedicated to running this DVD and 1 PC for running your forensic tool), use this page as your testing home. Click on each test case for instructions to run it. Use the browser's back button to return to this page.

Press the 'F5' button with your FT-LOGS thumb drive mounted to see your updated progress.

If you only have one PC available for testing your tool, click HERE to see all the test case instructions on one page. You need to save them to your thumb drive so that you can access them after you've shut this DVD down (optionally print them).

Tests to run:
- FT-DI-01-ATA28
- FT-DI-02-ATA28
- FT-DI-01-ATA48
- FT-DI-02-ATA48

Partially completed:
None

Tests completed:
None
Test Case Instructions

Running Test Case FT-DI-01-ATA28

1. When you attach the write blocker to the test PC, you **MUST** use the ATA cable to force the computer to use the ATA interface for access to the drive (through the write blocker). As for connecting the blocker to the source drive, it is OK to use any interface to connect the write blocker with the source drive. If there is no write blocker and the drive is connected directly to the PC motherboard then the cable coming out of the PC and connecting with the source drive must be ATA.

2. While the test PC is powered off, attach any fixed drives (ATA, SCSI, etc.) to the test PC.

3. Boot the test PC into the test environment.

4. If the system clock time is not correct, reset to current date and time.

5. Attach the FT-LOGS log drive and mount. The exact method depends on your forensic tool's run environment, i.e., Windows, Linux, etc.

6. Attach source drive via write blocker if not already attached

7. Attach and mount removable device for storing image files.

8. **Configure** the tool you are testing.
   - Select: "compute hash of acquired data"
   - Select: "acquire to an image file"
   - Name the image file image-01-ATA28 plus image file type extension.

Tool Run Config
Command Line Tool
Sample Test Report

**FT-DI-01**

**Test Case Description**

Acquire a drive to an image file. Repeat variations for each interface that might be acquired.

Note that in addition to testing the ability of the tool to access data over the interface between the PC and the write blocker, the ability to access the type of drive attached to the write blocker is also tested.

For example, if a SATA drive is attached to a write blocker that is attached to the test PC with a USB interface, two things are tested:

1. test ability of the tool to access the USB interface, and
2. test ability of the tool to acquire a SATA drive through a USB write blocker.

**Test Evaluation Criteria**

The hash values computed by the tool should match the reference hash values computed for the source drive.

The hash values computed by the tool are in the tool log file saved in the test case directory on the FT-LOGS log drive. The reference hashes are located in the 'setup' subdirectory for the source drive on the FT-LOGS log drive.

**Test Case Results**

<table>
<thead>
<tr>
<th>Case</th>
<th>Src</th>
<th>Ref MD5</th>
<th>Tool MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>FT-DI-01-ATA28</td>
<td>01-ide-96</td>
<td>F458F</td>
<td>F458F</td>
</tr>
<tr>
<td>FT-DI-01-ATA48</td>
<td>4c</td>
<td>D10F7</td>
<td>D10F7</td>
</tr>
<tr>
<td>FT-DI-01-SATA28</td>
<td>4b-sata</td>
<td>746B4</td>
<td>746B4</td>
</tr>
<tr>
<td>FT-DI-01-SATA48</td>
<td>16-sata</td>
<td>7BB1D</td>
<td>7BB1D</td>
</tr>
<tr>
<td>FT-DI-01-USB</td>
<td>63-fu2</td>
<td>EE217</td>
<td>EE217</td>
</tr>
<tr>
<td>FT-DI-01-FW</td>
<td>63-fu2</td>
<td>EE217</td>
<td>EE217</td>
</tr>
</tbody>
</table>
Framework for Sharing Test Reports

- Lab/individual tests tool using Federated Testing materials
- Tester submits test report and logs to CFTT
- CFTT reviews test report and logs
- Vendor comment period
- Post test report to website (alternately post contact information)
Anticipated Benefits

- More tools validated
- Shared test reports
- Cost savings
- Allows vendors to improve their tools
- Helps users to make informed choices on what tools/tool versions they use
- Allows labs to mitigate known errors
- Faster testing
Federated Testing for Disk Imaging Release Plan

- Release plan:
  - Receiving feedback from beta testers
  - Improve materials based on beta testing
  - Record companion video tutorials
  - Prerelease version available at www.cftt.nist.gov/federated-testing.html
  - Release version 1.0
Project Sponsors

- Department of Homeland Security, Science and Technology Directorate (Major funding)
- NIST Special Programs Office / Forensics
Contacts

Ben Livelsberger

benjamin.livelsberger@nist.gov

www.cftt.nist.gov/federated_testing.cfm

cftt@nist.gov

Sue Ballou, Special Program Office at NIST

susan.ballou@nist.gov
Questions?