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

NIST United States Department of Commerce
National Institute of Standards and Technology

Computer Forensics Tool Testing Program Overview

- 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

CFTT Federated Testing DVD - Home Page - Mozilla Firefox

CFTT Federated Testing DVD - ...

localhost/Federated_Testing_Home_Page.php

Federated Testing

NIST National Institute of Standards and Technology U.S. Department of Commerce

Home FAQs About Contacts

Select the type of tool you want to test

- Test a *disk imaging* tool
- Test a *forensic media preparation* tool- **coming soon!**
- Test a *hardware write block* tool- **coming soon!**
- Test a *mobile device* tool- **coming soon!**

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.

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Commerce Department.

Privacy policy / security notice / accessibility statement / Disclaimer

localhost/diskimaging/

Disk Imaging Home

CFTT Federated Testing CD - test a disk imaging tool - Mozilla Firefox

CFTT Federated Testing CD - te...

localhost/diskimaging/

Google

Federated Testing

NIST National Institute of Standards and Technology U.S. Department of Commerce

Home | About | Glossary of Terms | FAQs | Contacts

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

Home > Disk Imaging Home

Disk Imaging Home

How to Use This Website | What You Will Need | Overview of a Sample Test & Test Case List

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.cftt.nist.gov/federated-testing.html or ft_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.
4. Generate a test report for your tool using the *'Generate Test Report' page.*
5. Submit the test report and your testing log files to CFTT (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 - Test a Disk Imaging Tool - Generate Test Cases - Mozilla Firefox

Federated Testing - Test a Disk...

localhost/diskimaging/customizetest.php

Federated Testing

NIST National Institute of Standards and Technology U.S. Department of Commerce

Home | About | Glossary of Terms | FAQs | Contacts

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

Home > Disk Imaging Home > Generate Test Cases

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

Federated Testing - Test a Disk Imaging Tool - Test Dashboard - Mozilla Firefox

Federated Testing - Test a Disk...

localhost/diskimaging/runtests.php

Google

Federated Testing

NIST National Institute of Standards and Technology U.S. Department of Commerce

Home | FAQs | About | Contacts

Disk imaging selections

- Disk Imaging
- Video Tutorials
- Format Your Thumb Drive 'FT-LOGS'
- Generate Test Cases & Start Testing
- Go to Test Dashboard
- Generate Test Report
- View Test Case Instructions
- View Common Procedures
- View Media Setup

Home > Test a Disk Imaging tool > Test Dashboard

'test-configuration.txt' written to '/media/FT-LOGS'

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-01-ATA48
FT-DI-02-ATA28	FT-DI-02-ATA48

Partially completed:

None

Tests completed:

None

Test Case Instructions

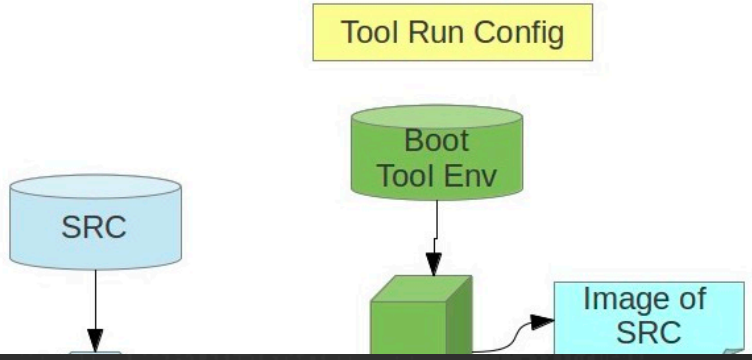
Federated Testing - Test a Disk Imaging Tool - Run Tests - Test Instructions - Mozilla Firefox

Federated Testing - Test a Disk...

localhost/diskimaging/testinstructions.php?runtests=true&testcase=FT-DI-01-ATA28

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 comming 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.



Command Line Tool

Terminal

root@ubuntu: /home/ubuntu

```
Source Drives Setup so Far:
00      drive is wiped, drive is not hashed, No hashed partitions

Each test drive needs to be assigned a unique drive id.
SOURCE drives should be assigned A1, A2, A3 and so forth.
DESTINATION drives should be assigned D1, D2, D3 and so forth.

Type the drive id assigned to this drive: A1

Select the device to operate on (type the code to the left of the device name):
a /dev/sda 41,943,040 (21.47 GB, 20.00 GiB)
b /dev/sdb 128,000 (65.54 MB, 62.50 MiB)
Enter code to the left of device name: b

/tmp/setup/a1 does not exist. Type 'yes' to create the log directory: yes

Wipe device /dev/sdb with a1
Go ahead (yes): yes

Starting wipe

Start time: Mon Feb 16 21:11:12 2015

Feedback every 1280/12800 sectors (10%) of 128000
at 1280 of 128000   1.0%    0:00:00 remains on Mon Feb 16 21:11:12 2015
at 2560 of 128000   2.0%    0:00:49 remains on Mon Feb 16 21:11:13 2015
at 3840 of 128000   3.0%    0:00:32 remains on Mon Feb 16 21:11:13 2015
at 5120 of 128000   4.0%    0:00:24 remains on Mon Feb 16 21:11:13 2015
at 6400 of 128000   5.0%    0:00:19 remains on Mon Feb 16 21:11:13 2015
at 7680 of 128000   6.0%    0:00:15 remains on Mon Feb 16 21:11:13 2015
at 8960 of 128000   7.0%    0:00:13 remains on Mon Feb 16 21:11:13 2015
at 10240 of 128000   8.0%    0:00:11 remains on Mon Feb 16 21:11:13 2015
at 11520 of 128000   9.0%    0:00:10 remains on Mon Feb 16 21:11:13 2015
at 12800 of 128000  10.0%    0:00:09 remains on Mon Feb 16 21:11:13 2015
at 25600 of 128000  20.0%    0:00:04 remains on Mon Feb 16 21:11:13 2015
at 38400 of 128000  30.0%    0:00:02 remains on Mon Feb 16 21:11:13 2015
at 51200 of 128000  40.0%    0:00:03 remains on Mon Feb 16 21:11:14 2015
at 64000 of 128000  50.0%    0:00:02 remains on Mon Feb 16 21:11:14 2015
at 76800 of 128000  60.0%    0:00:02 remains on Mon Feb 16 21:11:15 2015
at 89600 of 128000  70.0%    0:00:03 remains on Mon Feb 16 21:11:19 2015
at 102400 of 128000  80.0%    0:00:02 remains on Mon Feb 16 21:11:22 2015
at 115200 of 128000  90.0%    0:00:01 remains on Mon Feb 16 21:11:26 2015
at 128000 of 128000 100.0%    0:00:00 remains on Mon Feb 16 21:11:30 2015
```

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 Evalution 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

Case	Src	Ref MD5	Tool MD5
FT-DI-01-ATA28	01-ide-96	F458F	F458F
FT-DI-01-ATA48	4c	D10F7	D10F7
FT-DI-01-SATA28	4b-sata	746B4	746B4
FT-DI-01-SATA48	16-sata	7BB1D	7BB1D
FT-DI-01-USB	63-fu2	EE217	EE217
FT-DI-01-FW	63-fu2	EE217	EE217

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?