Disclaimer

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 National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose. Neither NIST nor myself has financial interest in any of the real products mentioned as part of this talk.

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

AAFS – February 19, 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
  - 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' cyberfetch.org
  - Informally between labs
  - Kept private

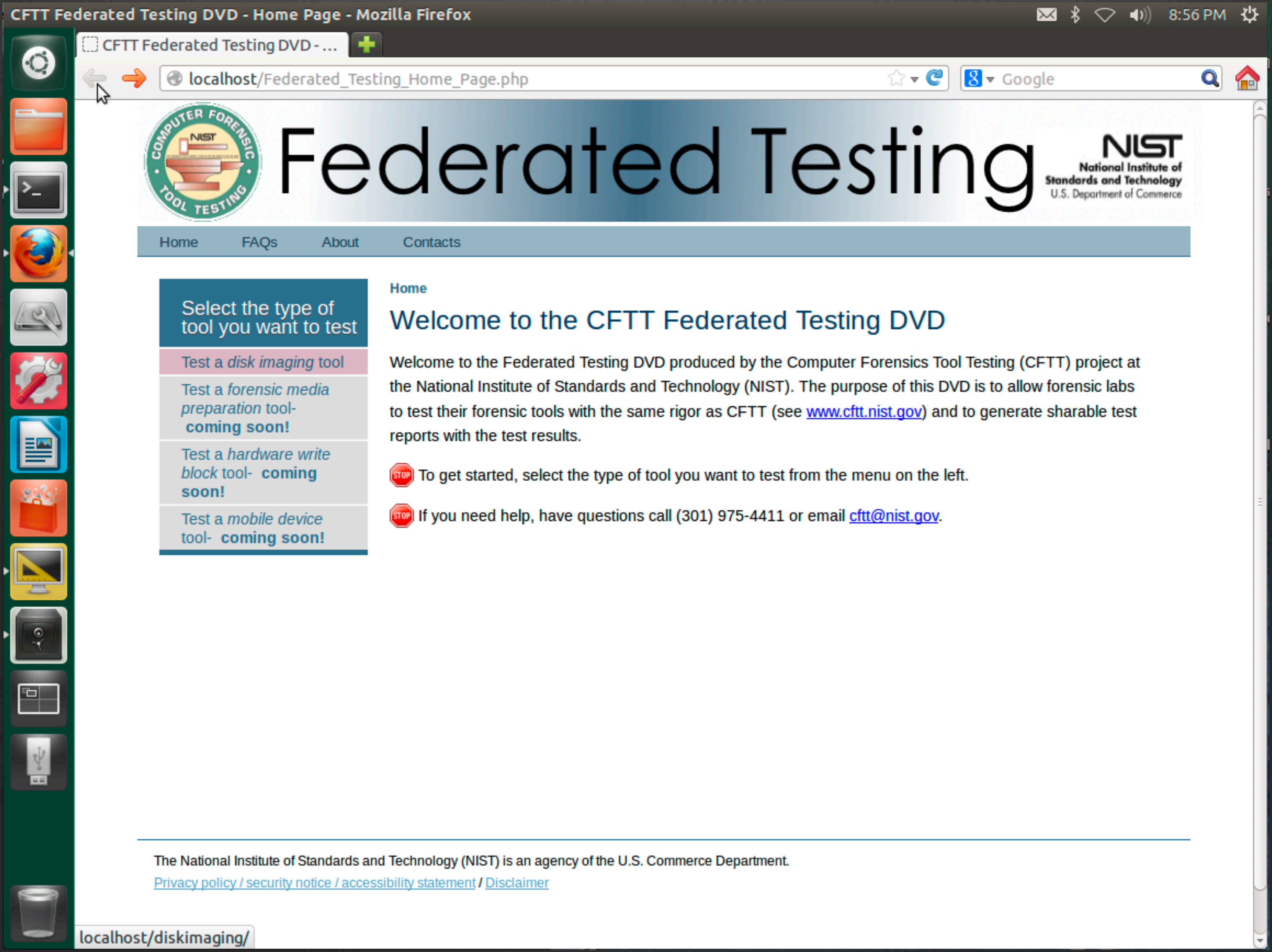
Target Areas

- 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® DVD .iso file
- Components:
  - User Interface
    - Video tutorials
    - Select tool features to test
    - Instructions for creating test data and for running test cases
    - Generate test report
  - Command line test support tools
    - Setup test cases and analyze the results

User Interface - Home



CFTT Federated Testing DVD - Home Page - Mozilla Firefox
8:56 PM
CFTT Federated Testing DVD - ...
localhost/Federated_Testing_Home_Page.php
Google
COMPUTER FORENSIC TOOL TESTING
NIST
Federated Testing
NIST National Institute of Standards and Technology U.S. Department of Commerce
Home
FAQs
About
Contacts
localhost/diskimaging/

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.

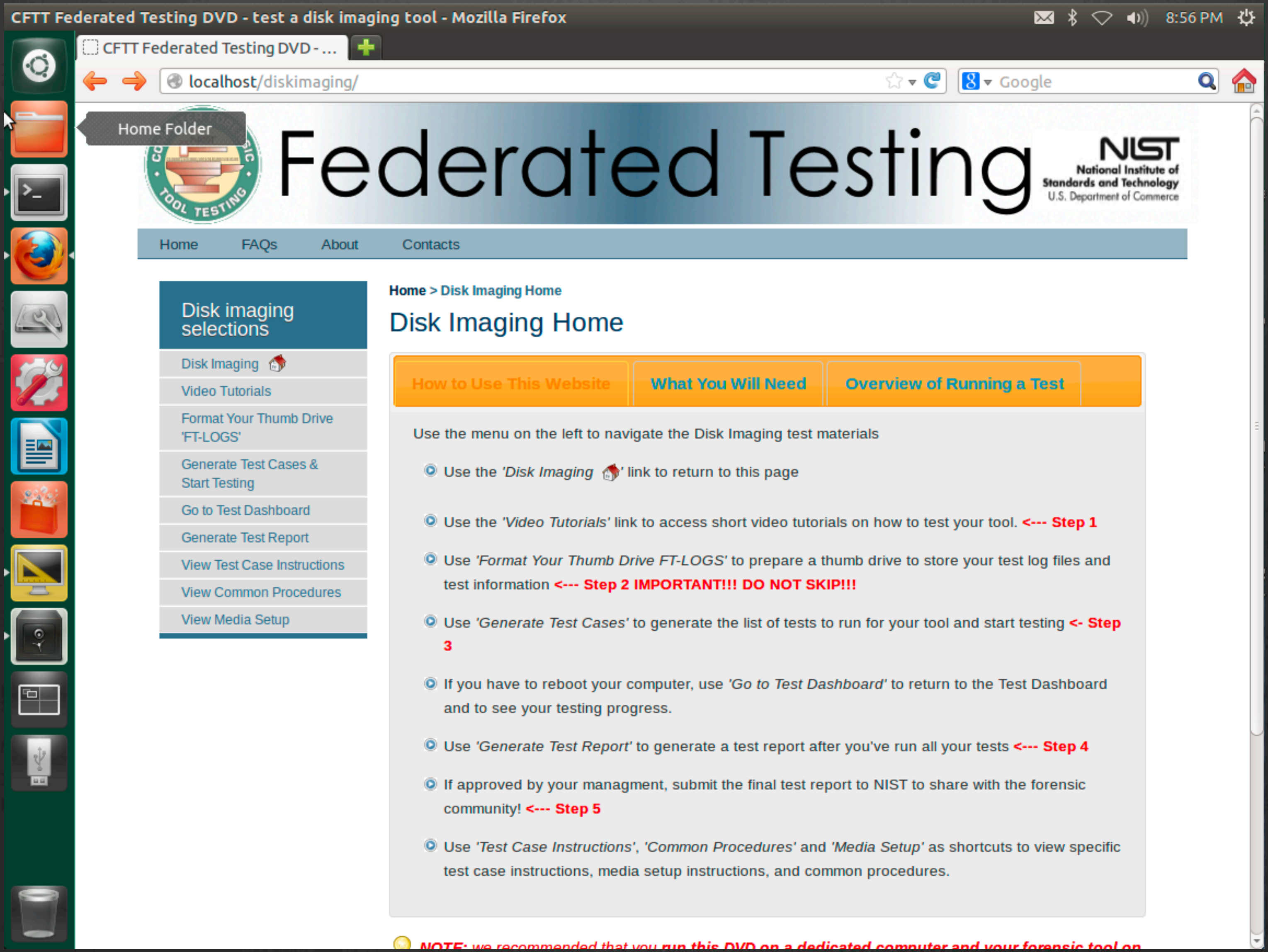
STOP To get started, select the type of tool you want to test from the menu on the left.

STOP 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

Disk Imaging Home


CFTT Federated Testing DVD - test a disk imaging tool - Mozilla Firefox
8:56 PM
CFTT Federated Testing DVD - ...
localhost/diskimaging/
Google
Home Folder
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
How to Use This Website
What You Will Need
Overview of Running a Test

Home > Disk Imaging Home

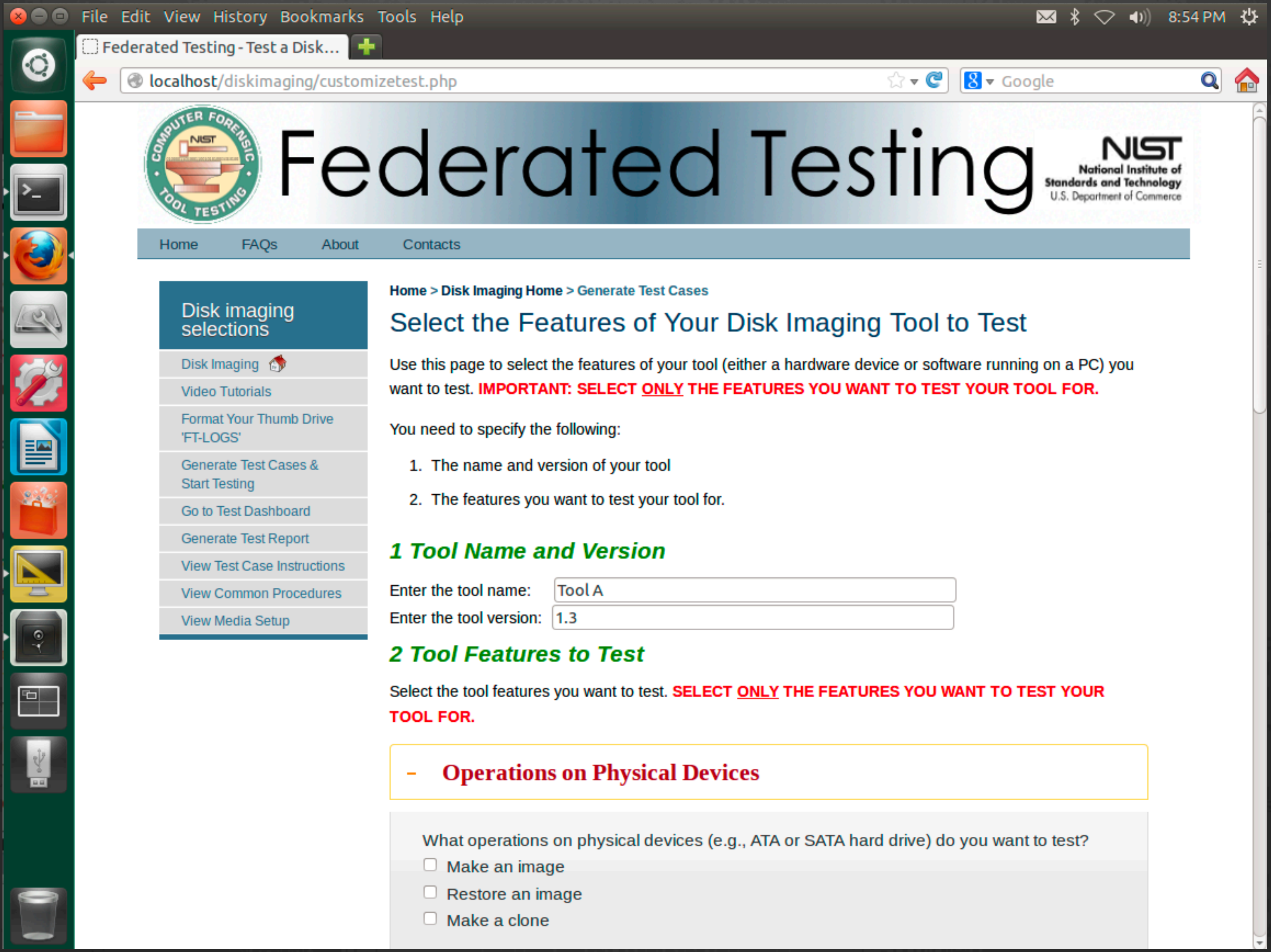
Disk Imaging Home

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

- Use the *'Disk Imaging* ' link to return to this page
- Use the *'Video Tutorials'* link to access short video tutorials on how to test your tool. **<--- Step 1**
- Use *'Format Your Thumb Drive FT-LOGS'* to prepare a thumb drive to store your test log files and test information **<--- Step 2 IMPORTANT!!! DO NOT SKIP!!!**
- Use *'Generate Test Cases'* to generate the list of tests to run for your tool and start testing **<- Step 3**
- If you have to reboot your computer, use *'Go to Test Dashboard'* to return to the Test Dashboard and to see your testing progress.
- Use *'Generate Test Report'* to generate a test report after you've run all your tests **<--- Step 4**
- If approved by your managment, submit the final test report to NIST to share with the forensic community! **<--- Step 5**
- Use *'Test Case Instructions'*, *'Common Procedures'* and *'Media Setup'* as shortcuts to view specific test case instructions, media setup instructions, and common procedures.

*NOTE: we recommended that you **run this DVD on a dedicated computer and your forensic tool on***

Selecting Tool Features


File Edit View History Bookmarks Tools Help
8:54 PM
Federated Testing - Test a Disk...
localhost/diskimaging/customizetest.php
Google
Federated Testing
NIST National Institute of Standards and Technology U.S. Department of Commerce
COMPUTER FORENSIC TOOL TESTING
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 > **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 PC) 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. 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 Tool Features to Test

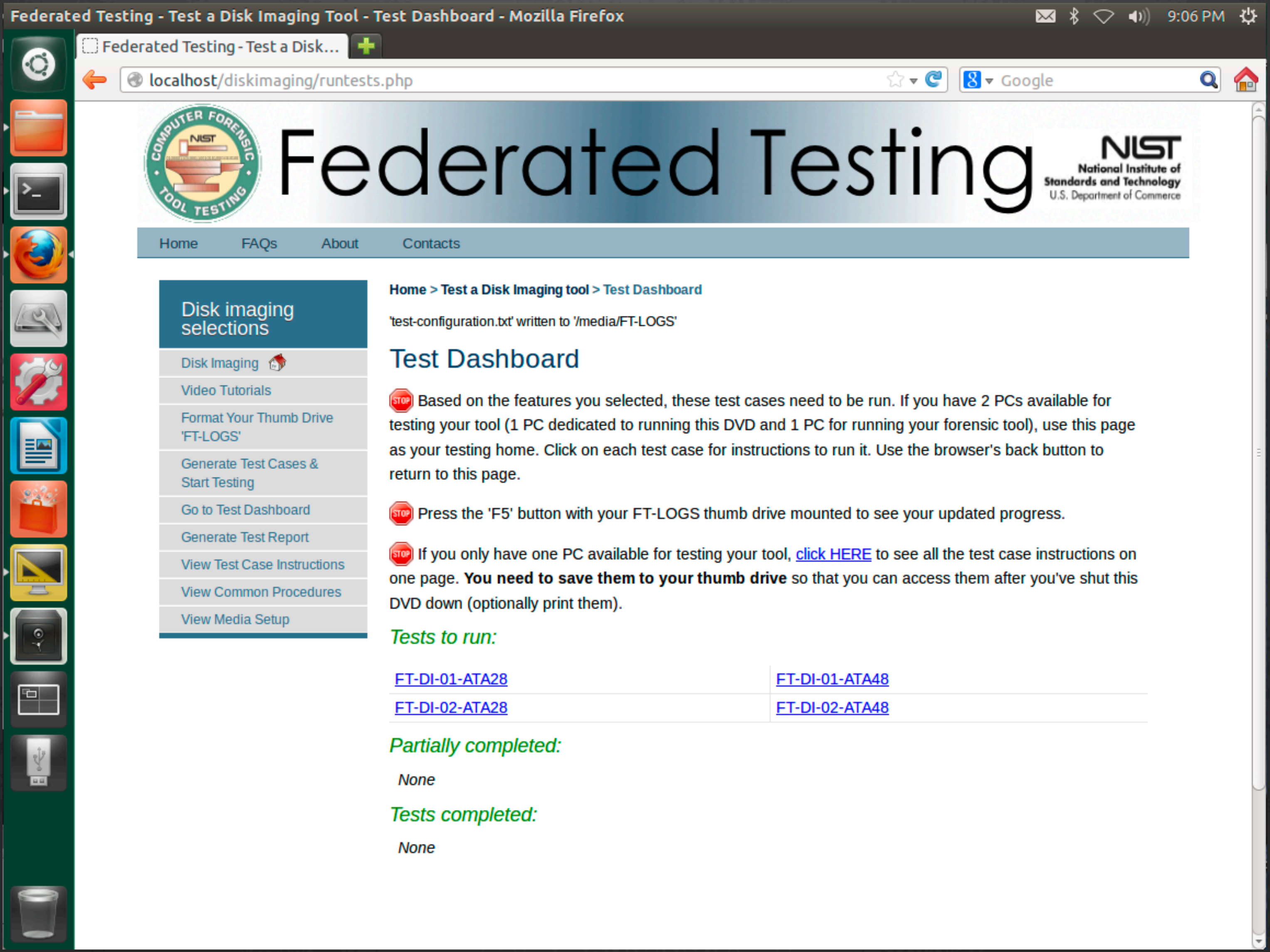
Select the tool features you want to test. **SELECT ONLY THE FEATURES YOU WANT TO TEST YOUR TOOL FOR.**

– **Operations on Physical Devices**

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

- ☐ Make an image
- ☐ Restore an image
- ☐ Make a clone

Tests To Run



Federated Testing - Test a Disk Imaging Tool - Test Dashboard - Mozilla Firefox
9:06 PM
Federated Testing - Test a Disk...
localhost/diskimaging/runtests.php
Google
COMPUTER FORENSIC TOOL TESTING
NIST
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

STOP 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.

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

STOP 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

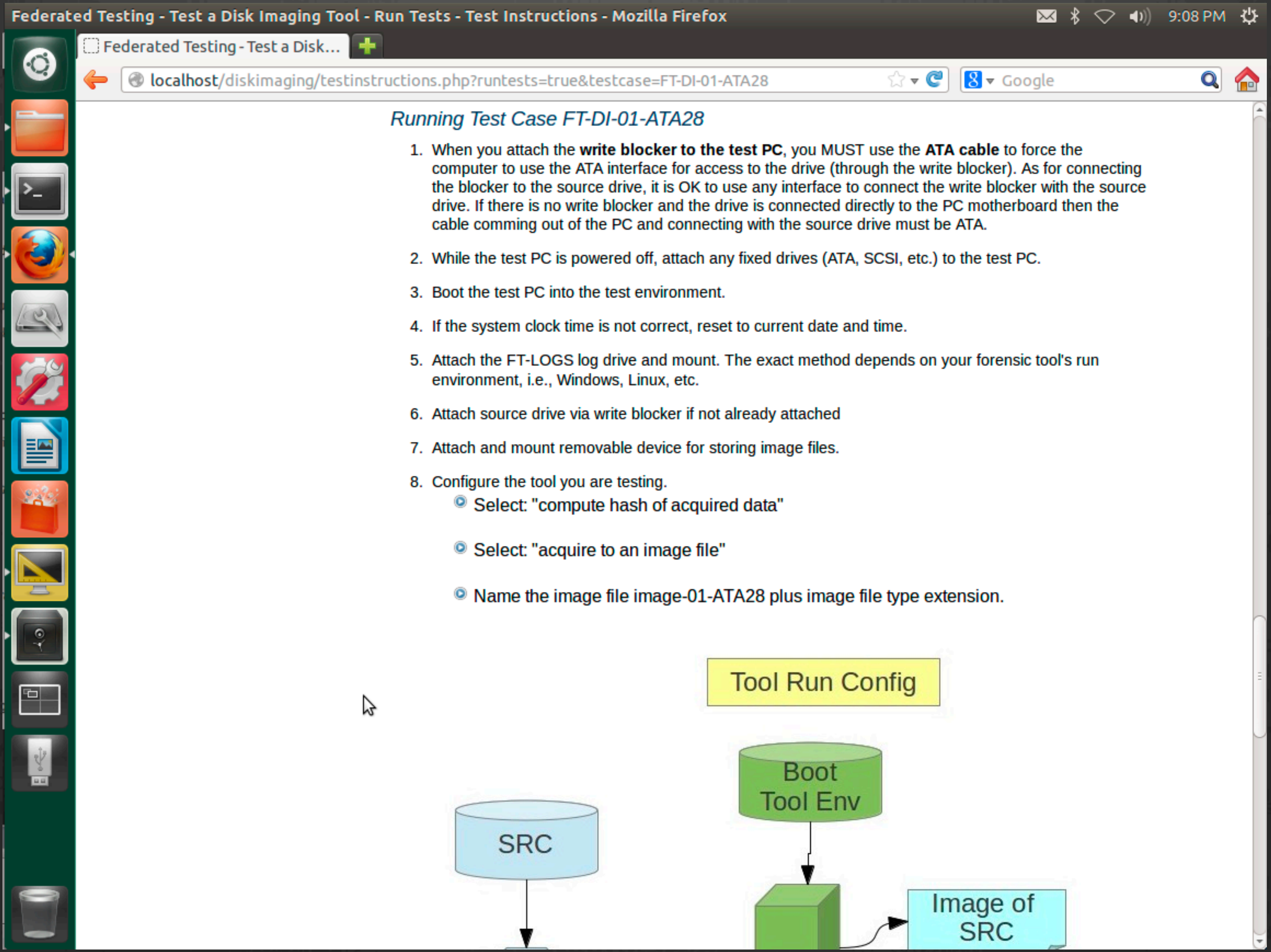
Partially completed:

None

Tests completed:

None

Test Case Instructions

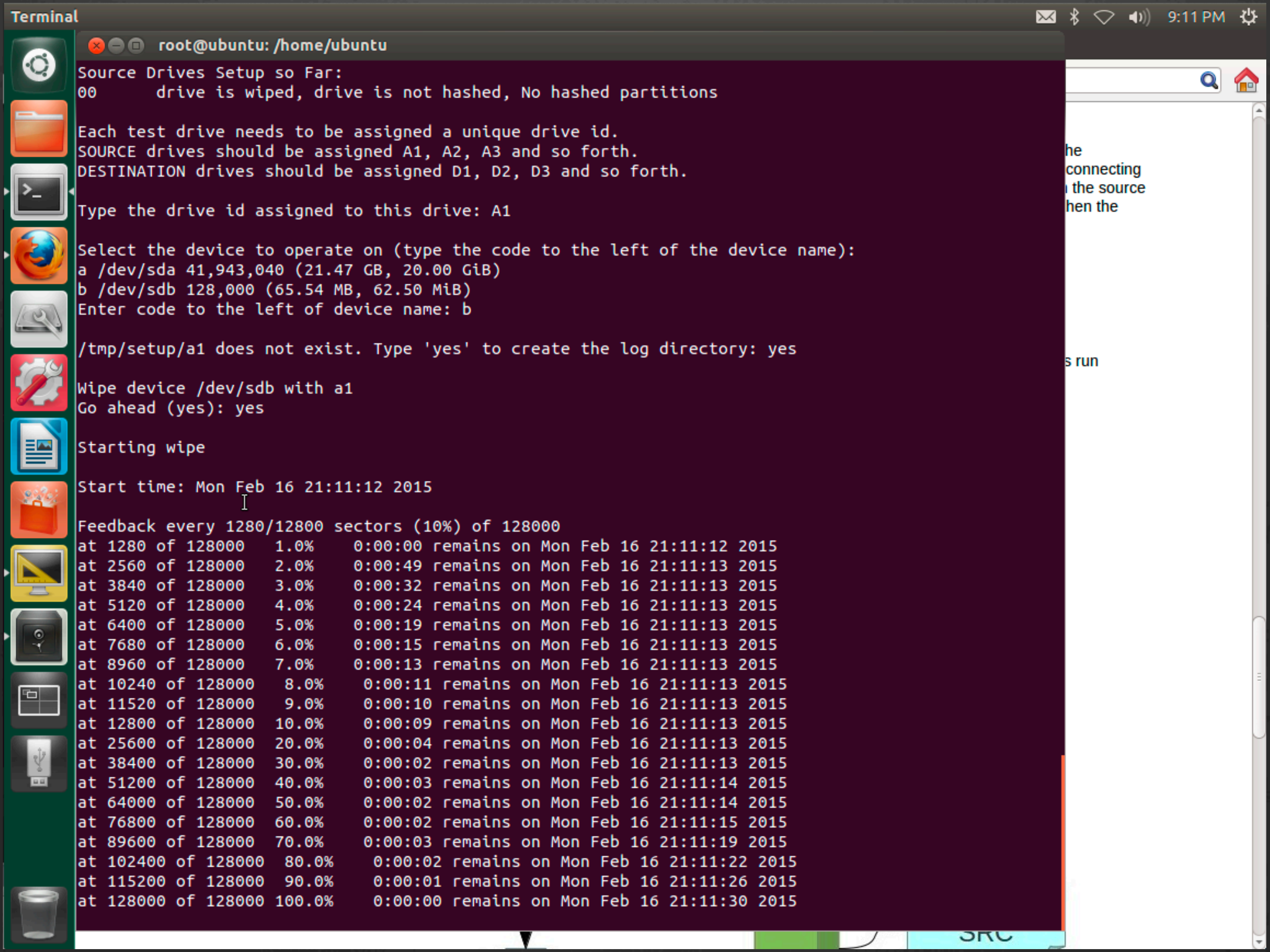


Federated Testing - Test a Disk Imaging Tool - Run Tests - Test Instructions - Mozilla Firefox
9:08 PM
Federated Testing - Test a Disk...
localhost/diskimaging/testinstructions.php?runtests=true&testcase=FT-DI-01-ATA28
Google

Running Test Case FT-DI-01-ATA28

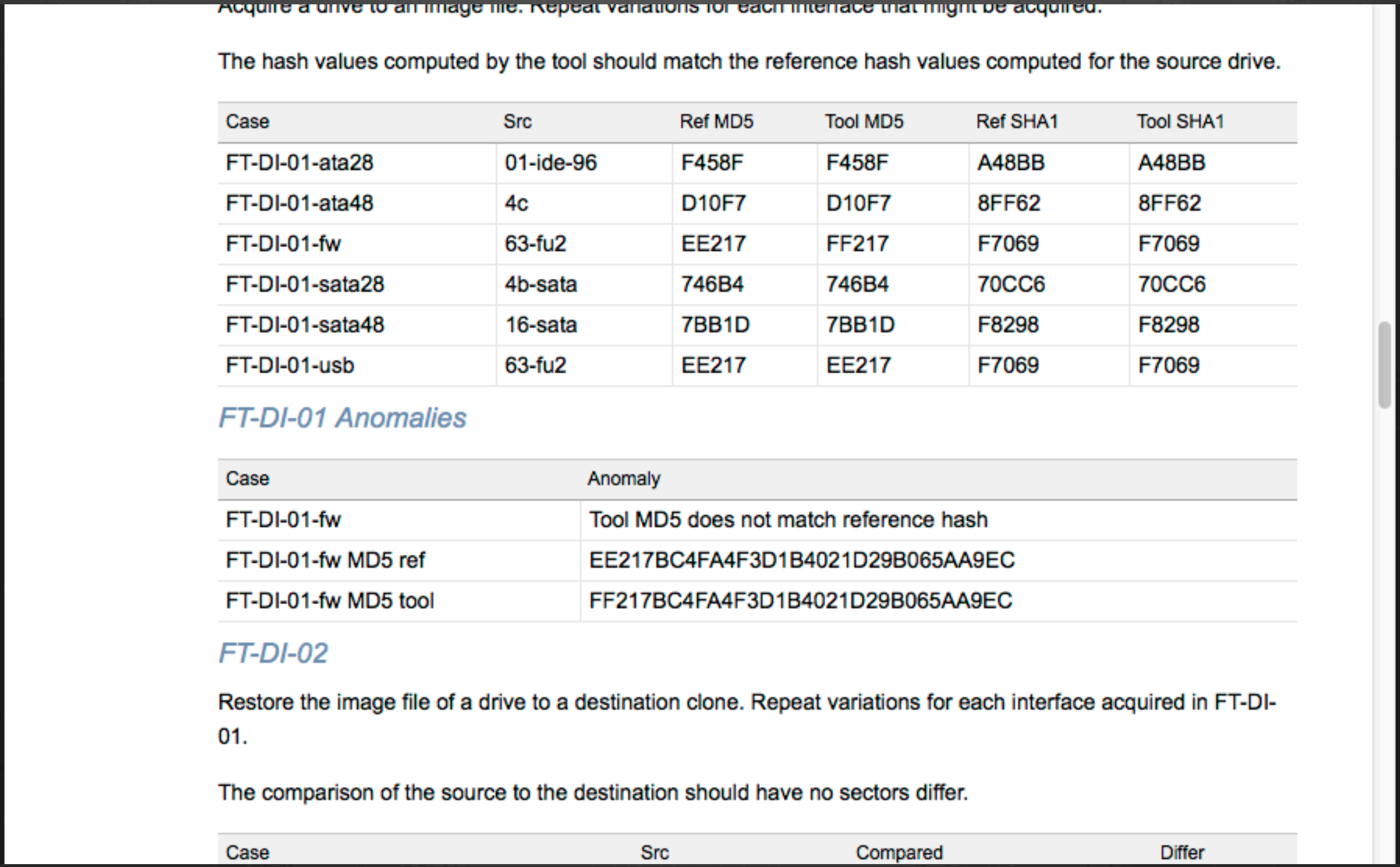
1. When you attach the **write blocker to the test PC**, you MUST use the **ATA cable** to force the computer to use the ATA interface for access to the drive (through the write blocker). As for connecting the blocker to the source drive, it is OK to use any interface to connect the write blocker with 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



```
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



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

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

Case	Src	Ref MD5	Tool MD5	Ref SHA1	Tool SHA1
FT-DI-01-ata28	01-ide-96	F458F	F458F	A48BB	A48BB
FT-DI-01-ata48	4c	D10F7	D10F7	8FF62	8FF62
FT-DI-01-fw	63-fu2	EE217	FF217	F7069	F7069
FT-DI-01-sata28	4b-sata	746B4	746B4	70CC6	70CC6
FT-DI-01-sata48	16-sata	7BB1D	7BB1D	F8298	F8298
FT-DI-01-usb	63-fu2	EE217	EE217	F7069	F7069

FT-DI-01 Anomalies

Case	Anomaly
FT-DI-01-fw	Tool MD5 does not match reference hash
FT-DI-01-fw MD5 ref	EE217BC4FA4F3D1B4021D29B065AA9EC
FT-DI-01-fw MD5 tool	FF217BC4FA4F3D1B4021D29B065AA9EC

FT-DI-02

Restore the image file of a drive to a destination clone. Repeat variations for each interface acquired in FT-DI-01.

The comparison of the source to the destination should have no sectors differ.

Case	Src	Compared	Differ

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
- Faster testing
- 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

Federated Testing for Disk Imaging Release Plan

- Release plan:
  - Incorporating changes based on feedback
  - Recording companion video tutorials
  - Prerelease available at www.cftt.nist.gov/federated_testing.cfm this March
  - Beta testing
  - Release version 1.0

Project Sponsors

- Department of Homeland Security, Science and Technology Directorate (Major funding)
- NIST/SPO (Program management)

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?