



Computer Forensics Tool Testing

Jim Lyle

National Institute of Standards
and Technology





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.

Overview

- Mostly high level thoughts and a few details about testing at CFTT
- Conformance testing as used by CFTT
- Some challenges for writing requirements and test cases
- Selecting test cases
- Thoughts on testing acquisition tools, write blocker tools and disk wiping tools

Current Tasks

- Testing tools for:
 - ⊙ imaging, write blocking, drive wipe
 - ⊙ deleted file recovery, file carving
 - ⊙ mobile devices
- New specs for: tablet devices, File Carving
- Forensic tool catalog
- Federated testing

General CFTT Method: Conformance Testing

- Requirements specification
 - ⊙ Background & definitions
 - ⊙ Core behaviors for all tools
 - ⊙ Optional features and behaviors
- Test Assertions -- atomic tests
- Test Cases -- each case evaluates some subset of the assertions
- Test procedures -- how to run tests
- Test Reports

CFTT Reports (since Aug 2002)

Tool Type	Published	Testing/Drafting Report
Disk imaging	21	7
Software Blocker	9	0
Hardware Blocker	24	0
Mobile Devices	21	5
Drive erase/wipe	10	0
Deleted File Recovery	0	6
Total as of Nov 2012	85	18

Challenges to Creating a Specification

- Diversity of tool features
- May not be one correct behavior
 - ⊙ Write blocker behavior
 - ⊙ Deleted file recovery
 - ⊙ File Carving
- Some actions not exactly repeatable, e.g., memory acquire
- Needs to allow for evolution of technology

Challenges to Creating Test Cases

- Many errors only manifest if there is a specific set of conditions.
- Combinatorics -- testing enough combinations of parameters & possible values
- Example (creating a disk image)
 - ⊙ Partition: FAT, NTFS, ext3, HFS
 - ⊙ Physical: ATA, SCSI, USB, 1394
 - ⊙ Destination: image, clone
 - ⊙ Error: none, bad sector, out of space
 - ⊙ $4 \times 4 \times 2 \times 3 = 96$ runs -- at 3 hours/run -- 288 hours or 36 days or about 7 weeks

Federated Testing

- NIST develops specification, methods & test data
- Forensic labs do tool testing
- Test reports follow standardized format
- Reviewed Test reports posted to central web site

Generate Test Plan for Testing Drive Wipe Tools

Filling out and submitting this form generates a test plan for testing a drive wipe tool (either a hardware device or software running on a PC). The generated test plan is a set of test cases including for each case, (1) procedures for how to setup a test drive, (2) procedures for running the test case, and (3) how to evaluate the result.

You need to specify three things:

1. The name and version of the tool under test.
2. The interfaces that can be used to attach the drive to either a computer running a software erase tool or a hardware device that erases the drive.
3. A list of features that the tool supports and you want to test.






Tool Name and Version

Enter the tool name and version:

Interface Between Tool and Drive to Erase

The drive selected for erasing has to be attached to the device (or PC) that does the erasing by some interface. More than one interface could be supported by the tool.

Select all tool interfaces that need to be tested:

Interface	Need to Test
ATA 	<input type="checkbox"/>
SATA 	<input checked="" type="checkbox"/>
SCSI 	<input type="checkbox"/>
USB 	<input type="checkbox"/>
FireWire 	<input type="checkbox"/>

Tool Features to Test

Select the tool features you want to test.

Note that the ERASE command and the hidden sectors (HPA & DCO) are rendered in "grey" and cannot be selected. These features can only be used with the ATA and SATA interfaces. Testing these features is disabled unless either the ATA or SATA interface is first selected.

Feature	Need to Test
Wipe sectors via WRITE command	<input checked="" type="checkbox"/>
Wipe sectors via ERASE command	<input checked="" type="checkbox"/>
Wipe hidden sectors (DCO)	<input type="checkbox"/>
Wipe hidden sectors (HPA)	<input type="checkbox"/>
Remove DCO	<input type="checkbox"/>
Remove HPA	<input type="checkbox"/>
Detect attempt to use ERASE on unsupported drive	<input type="checkbox"/>

[Generate Test Case List](#)



Test Plan for Clean-it-up

Forensic Media Preparation Tool To Test: Clean-it-up

Interfaces to test:

- SATA28
- SATA48

Requirements to test:

- Wipe sectors via WRITE command
- Wipe sectors via ERASE command

Test Cases:

FMP-01-SATA28	Test Drive Setup	Test Procedures	Test Evaluation
FMP-01-SATA48	Test Drive Setup	Test Procedures	Test Evaluation
FMP-02-SATA28	Test Drive Setup	Test Procedures	Test Evaluation
FMP-02-SATA48	Test Drive Setup	Test Procedures	Test Evaluation

[Test Report Template](#)

Run Procedures for Test Case FMP-01-SATA48

32. Select a drive that does not support the secure erase command and that uses the SATA48 interface required by the variation.
33. If the tool under test requires a host computer to execute the test, then select and configure a test host as needed to support the tool.
34. Manually calibrate the system clock on test host if applicable.
35. Select an analysis host.
36. Manually calibrate the system clock on the analysis host.
37. Execute the following command:

```
logfmp FMP-01-SATA48 analysis-host operator drive test-host
```

38. Do an analysis of the initial state with dsumm.

```
dd bs=512 if=/dev/xxx | dsumm FMP-01-SATA48 analysis_host operator /dev/xxx label init.txt
```

39. Prepare to run the tool under test:
40. Configure tool under test and attach the test drive.
41. Select write mode if applicable.
42. If the tool under test creates a log file and offers a choice for log file name use tool-log.txt for the name.
43. Run tool under test.
44. Any tool parameter settings that are used need to be recorded in the testrun-note.txt file

Run HDAT2

45. Boot system with the hdat2 boot floppy.
46. Press 1 to bypass the decrementing startup file menu time. If 1 is not pressed, after a few seconds, the startup file menu becomes the command screen.
47. At the command screen, type HDAT2 and then press Enter.
48. At the Device List screen, select the destination drive using the up or down arrow keys to highlight the drive. Press Enter.
49. record size of drive as size_postwipe

CFReDS: Forensic Tool Test Data

- Data sets for tool testing
 - ◎ Deleted File Recovery
 - ◎ File Carving
 - ◎ String Search UNICODE text in русский
 - ◎ Search container files (e.g., zip or tar)
 - ◎ Memory images
 - ◎ Mobile device images
- Data sets for equipment check out
- Data sets for staff training
- Proficiency Testing and Skill Testing

Testing Acquisition Tools

● Primary issues

- ⊙ Clone a device
- ⊙ Acquire a device to an image file
- ⊙ Restore image file to a device

● Secondary issues

- ⊙ Partitions
- ⊙ Hidden areas
- ⊙ Reliably faulty drives

Testing Write Blockers

- Use cmd generator to send all possible I/O commands (even undefined commands)
- Monitor blocker output to characterize tool behavior (preferred measurement method)
- All writes must be blocked
- At least one read cmd must be allowed
- Just report on behavior for anything else
- Alternate test cases (using different measurements) if can't use generator or monitor



Forensic Media Preparation

- Disk wiping for internal reuse (not for disposal)
- For disposal see: NIST SP 800-88 Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology
- Write vs SECURE ERASE

DFR Testing Overview

- About 17 test cases defined (1 run for each file system family, 4 runs per case)
- Is particular file system supported
- Can active files be listed
- Support for non-ASCII file names
- Can deleted file names be recovered (maybe not)
- Recover contiguous content
- Recover fragmented content
- Identify overwritten content

Testing Supported File Systems

- Basic Case to identify supported file systems
- Test case –
 1. Create three files: A, B & C
 2. Delete file B
 3. Image file system

OS	File Systems				
WIN	FAT 12/16/32	NT	NTC	ExFAT	
Mac	HFS	OSX	OSX-J	OSX-C	OSX-JC
Linux	Ext2	Ext3	Ext4		

Supported File Systems: Results

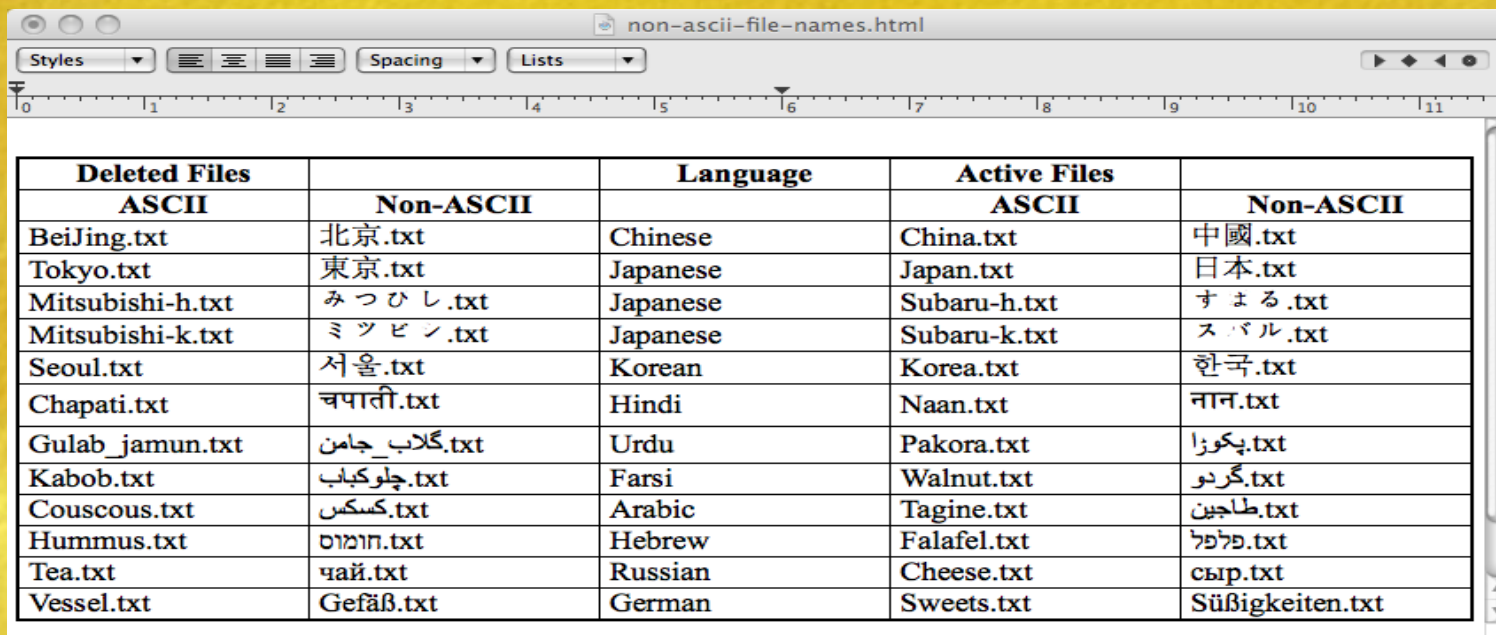
Tool	Active File List	Deleted File Name	Deleted File Content
Tool #1	FAT,HFS,OSX, OSXJ, EXT Nothing: OSXC, OSXCJ	FAT, NT No name: OSX, EXT	FAT, NT, ext2 (as lost file), Nothing: ext3/4, HFS, OSX/C/J
Tool #2	FAT, NT, HFS, OSX/C/J, EXT2/3 Nothing: ext4	FAT, NT No name: OSX, EXT	FAT, NT, EXT2 No content: NTC, OSX/J/C, EXT3/4
Tool #3	FAT, NT, HFS, OSX/C/J, EXT Nothing: OSXCJ	FAT, NT No name: OSX, EXT	FAT, NT, EXT2 No content: OXS/J/C, EXT3/4



Non-ASCII File Names

1. Create set of files with non-ASCII file names
 - ⦿ European diacritical marks
 - ⦿ Asian characters
 - ⦿ Right to left text
2. Delete some files
3. Run tools (#1, #2 & #3)

Non-ASCII File Names



The screenshot shows a web browser window titled "non-ascii-file-names.html". The browser interface includes a menu bar with "Styles", "Spacing", and "Lists" options, and a ruler at the top. The main content is a table with five columns: "Deleted Files ASCII", "Deleted Files Non-ASCII", "Language", "Active Files ASCII", and "Active Files Non-ASCII". The table lists various file names in different languages, including Chinese, Japanese, Korean, Hindi, Urdu, Farsi, Arabic, Hebrew, Russian, and German.

Deleted Files ASCII	Deleted Files Non-ASCII	Language	Active Files ASCII	Active Files Non-ASCII
BeiJing.txt	北京.txt	Chinese	China.txt	中國.txt
Tokyo.txt	東京.txt	Japanese	Japan.txt	日本.txt
Mitsubishi-h.txt	みつひし.txt	Japanese	Subaru-h.txt	すまると.txt
Mitsubishi-k.txt	ミツピン.txt	Japanese	Subaru-k.txt	スバル.txt
Seoul.txt	서울.txt	Korean	Korea.txt	한국.txt
Chapati.txt	चपाती.txt	Hindi	Naan.txt	نان.txt
Gulab_jamun.txt	گلاب_جامن.txt	Urdu	Pakora.txt	پکوزا.txt
Kabob.txt	چلوکباب.txt	Farsi	Walnut.txt	گردو.txt
Couscous.txt	كسكس.txt	Arabic	Tagine.txt	طاجين.txt
Hummus.txt	חמום.txt	Hebrew	Falafel.txt	פלפל.txt
Tea.txt	чай.txt	Russian	Cheese.txt	сыр.txt
Vessel.txt	Gefäß.txt	German	Sweets.txt	Süßigkeiten.txt

- Most tools rendered non-ASCII correctly for most file systems.
- Two tools had problem rendering Korean text from OSX
- One tool could not render non-ASCII file names from EXT2



Mobile Device Tools

- Stick around for Rick (after the break)

Summary

- Give tool opportunity to fail -- diverse test suite & fault based test cases
- Case templates that vary over a parameter -- this is useful as technology evolves
- Use pair-wise testing to allocate lots of parameters among a few test cases
- Have alternate cases with different measurement tools if first measurement method can't be used
- Make tool test data available to community via www.cfreds.nist.gov
- Make test methodology available to community via Federated Testing Project

Contacts

Jim Lyle

www.cftt.nist.gov

www.cfreds.nist.gov

cftt@nist.gov

Doug White

www.nsrl.nist.gov

nsrl@nist.gov

Sue Ballou, Office of Law Enforcement Standards

Steering Committee Rep. For State/Local Law Enforcement

susan.ballou@nist.gov