Forensic Tool Testing Results

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.

Project Sponsors

- NIST/OLES (Program management)
- National Institute of Justice (Major funding)
- FBI (Additional funding)
- Department of Defense, DCCI (Equipment and support)
- Homeland Security (Major funding)
- State & Local agencies (Technical input)
- Internal Revenue, IRS (Technical input)

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

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
Disk imaging	15	2
Software Blocker	9	0
Hardware Blocker	21	0
Mobile Devices	10	6
Drive erase/wipe	4	4

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
  - 4x4x2x3 = 96 runs -- at 3 hours/run -- 288 hours or 36 days or about 7 weeks

Selecting Test Cases

- When are you done?
  - One test for each assertion may not be enough.
  - One test for every combination of test parameters and parameter values is too many.
- Pair-wise test case -- usually enough to trigger most combination based faults
- Fault based testing -- what mistakes might the programmer make
- Some test cases are templates for a set of similar runs (case variations over some parameter, e.g., interface: ATA, USB, etc.)

Testing Acquisition Tools

- Use case variations to vary some parameters like --
  - Source interface: ATA28, ATA48, SATA, USB, FW, SCSI
  - Destination File system: FAT32, NTFS, HFS
  - Type of hidden area: HPA, DCO, HPA+DCO
  - Partition Type: FAT16, FAT32, NTFS, ext3
- Use pair-wise case selection to reduce total number of cases

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-88 Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology
- Write vs SECURE ERASE

Disk Wipe Requirements

- Method: WRITE or SECURE ERASE
- ERASE support: not all drives do it
- What to wipe: visible (yes) DCO/HPA ?
- HPA/DCO: remove or replace?
- Notify if there is a write error?
  - Yes, of course notify the user
  - Could be hard to test reliably - skip for now
- Multi-pass or verify? no - not testable

Wipe Test Issues

- Reporting final state of HPA/DCO: removed or in place
- Reporting Drive size with HPA
  - Linux may remove an HPA
  - Bridges and blockers too
- Reporting result of attempt to use ERASE on non-supporting drive
- What should drive be wiped with: zeros, ones, user specified pattern, random values?

Interesting Results

- HPA/DCO ignored
- HPA/DCO removed, but not wiped
- Erase implementation issues
- Tool fails if “erase time” not supported by the drive

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. Capture image

OS	File Systems				
WIN	FAT 12/16/32	NT	NTC		
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

non-ascii-file-names.html

Styles | Spacing | Lists

Deleted Files		Language	Active Files	
ASCII	Non-ASCII		ASCII	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	みつびし.txt	Japanese	Subaru-h.txt	すばる.txt
Mitsubishi-k.txt	ミツビシ.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	नान.txt
Gulab_jamun.txt	گلاب_جامن.txt	Urdu	Pakora.txt	پکوڑا.txt
Kabob.txt	چلوکباب.txt	Farsi	Walnut.txt	گردو.txt
Couscous.txt	كسكس.txt	Arabic	Tagine.txt	طاجين.txt
Hummus.txt	חומוס.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

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

Contacts

Jim Lyle
www.cftt.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