Computer Forensic Tool Testing at NIST

Jim Lyle

Information Technology Laboratory

Digital Forensics Forum

21 May 2007

NIST United States Department of Commerce
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.

Outline

- Overview of computer forensics at NIST
- Description of CFTT project
  - Specifications
  - Test assertions
  - Anomalies
- Questions and answers

Where is CFTT?

- US government, executive branch
- Department of Commerce (DOC)
- National Institute of Standards and Technology (NIST)
- Information Technology Lab (ITL)
- Software Diagnostics and Conformance Testing Division (SDCT)
- Computer Forensics: Tool Testing Project (CFTT)
- Also, the Office of Law Enforcement Standards (OLES) at NIST provides project input

Goals of CF at NIST/ITL

- Establish methodology for testing computer forensic tools (CFTT)
- Provide international standard reference data that tool makers and investigators can use in investigations (NSRL, CFReDS)

Project Sponsors (aka Steering Committee)

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

Other Related Projects at NIST

- NSRL -- Hash (MD5, SHA1) file signature data base, updated 4 times a year (Doug White)
- PDAs and Cell Phones, NIST Computer Security Division (Rick Ayers)
- SAMATE -- Software Assurance Metrics and Tool Evaluation (Paul E. Black)
- CFReDS -- Computer Forensics Reference Data Sets (Jim Lyle)

Forensic Tool Features

- … are like a Swiss army knife
  - Blade knife for cutting
  - Punch for making holes
  - Scissors for cutting paper
  - Cork screw for opening Chianti
- Forensic tools can do one or more of …
  - Image a disk (digital data acquisition)
  - Search for strings
  - Recover deleted files

Testing a Swiss Army Knife

- How should tools with a variable set of features be tested? All together or by features?
- Test by feature has a set of tests for each feature: acquisition, searching, recovery
- Examples: EnCase acquisition, iLook string search, FTK file recovery

Conformance Testing

- Start with a standard or specification
- Develop Test Assertions
- Develop Test Suite
- Identify testing labs to carry out tests

If certification desired

- Identify certification authority
- Identify funding

CFTT Model: Test Report

To produce a CFTT test report we need …

- Forensic tool under test (don’t forget there may be several versions and releases)
- Set of test cases (Defined in a test case doc)
- Validated measurement tools (test harness, user manual, design document, test harness requirements, V&V plan for test harness and V&V report for the test harness)
- Test assertions (define what should be measured in a test assertion document)
- Specification (Defines tool feature requirements)
- Resolution of comments document

Creating a Specification

- Specification (informal) vs Standard (Formal ISO process)
- Steering committee selects topic
- NIST does research: tools, vendors, users
- NIST drafts initial specification
- Post specification on web for public comment
- Resolve comments, post final version

Writing the Specification

- Specification for a single forensic function
- Describe technical background, define terms.
- Identify core requirements all tools must meet.
- Identify requirements for optional features related to the function being specified.

Develop Test Cases

- A test case is an execution of the tool under test
- Each test case should be focused on a specific test objective
- Each test case evaluates a set of test assertion

Core Acquisition Requirements

- All visible sectors are acquired
- All hidden sectors are acquired
- All acquired sectors are accurately acquired
- Benign fill of faulty sectors
- Error conditions

Requirements for Optional Features

- Clone creation
- Verify image integrity
- Image file format conversion
- Partition aligned clone creation

Test Case

- A test case for disk imaging
  - Create a target test drive (visible sectors only)
  - Calculate a hash of the test drive
  - Image the test drive with the tool under test
- Based on how tool reports results, measure results
- Sound forensic practice is often not good testing practice

Evaluating Test Results

If a test exhibits an anomaly …

1. Look for hardware or procedural problem
2. Anomaly seen before
3. If unique, look at more cases
4. Examine similar anomalies

Test Case Example: Setup

- Setup NTFS partition
  - MD5: 92b27b30bee8b0ffba8c660fa1590d49
  - 27744192 sectors
  - Each sector filled with sector LBA & disk ID
- Acquire partition
  - Total Sectors:27,744,191
  - 494A6ED8A827AD9B5403E0CC89379956
- Rehash (minus last sector) -- still no match

Example Continued

- Restore image to NTFS partition
- Compare to original
  - Sectors differ: 47
- Restore was in Windows XP …
- Restore again, unpower drive, no system shutdown. Compare to original
  - Sectors differ: 8
  - Diffs range: 27744184-27744191

Example Resolution

- Examine the eight sectors
  - Last sector not imaged
  - Other seven are a second copy of seven sectors starting at offset 27744120 -- Know this because each sector is tagged with LBA
- Verification:

```
xena:/Users/jimmy root# dd bs=512 if=/dev/disk2s11 of=~jimmy/nt.dd
xena.local(1009)==> dd if=nt.dd bs=512 skip=27744120 count=7 of=end.dd
xena.local(1012)==> dd if=nt.dd bs=512 count=27744184 of=chunk.dd
xena.local(1013)==> cat chunk.dd end.dd | md5
494a6ed8a827ad9b5403e0cc89379956
xena.local(1022)==> md5 nt.dd
MD5 (nt.dd) = 92b27b30bee8b0ffba8c660fa1590d49
```

Current Activities

- Hard drive imaging tools
- Software hard drive write protect
- Hardware hard drive write protect
- Deleted file recovery
- String Searching

Acquisition Anomalies

- Last sector of partition or drive acquire skipped in Linux 2.4
- Some sectors contiguous to a faulty sectors filled rather than acquired
- In a legacy BIOS acquisition (DOS), last partial cylinder not acquired
- Last partial cylinder of drive not used in a restore

Impact

- Release 18 (Feb 2001) - A US government organization was doing some testing and uncovered an issue under a specific set of circumstances.
- Several vendors have made product or documentation changes
- CFTT cited in some high profile court cases

Available Specifications

- Hard Drive Imaging (e.g., Safeback, EnCase, Ilook, Mares imaging tool)
- Write Block Software Tools (e.g., RCMP HDL, Pdblock, ACES)
- Write Block Hardware Devices (A-Card, FastBloc, NoWrite)

Specifications Under Development

- String searching
- Deleted file recovery
- Cell phone acquisition tools

Available Test Reports

- Sydex SafeBack 2.0
- NTI Safeback 2.18
- EnCase 3.20
- GNU dd 4.0.36 (RedHat 7.1)
- FreeBSD 4.4 dd
- RCMP HDL V0.4, V0.5, V0.7,V0.8
- Pdblock: v2.0, v2.1 & pd_lite
- IXimager

Available Imaging Test Reports

- IXimager (Version 2.0, Feb-01 2006), April 2007
- dd Provided with FreeBSD 4.4, January 2004
- SafeBack 2.18, June 2003
- EnCase 3.20, June 2003
- SafeBack 2.0, April 2003
- Red Hat Linux dd Version: 7.1 GNU fileutils 4.0.36, August 2002

Test Reports Later this Year

- DCCIdd (at NIJ for posting)
- EnCase 4.22a (Drafting report)
- Linen 5.05f (Drafting report)
- EnCase 5.05f (Under test)
- Encase 6.??/Linen 6.?? (Next in queue)
- FTK, X-ways, Talon starting soon

Available Testing Software

- FS-TST – tools to test disk imaging: drive wipe, drive compare, drive hash (SHA1), partition compare. (DCCI uses these tools)
- SWBT – tools to test interrupt 13 software write blockers

Benefits of CFTT

Benefits of a forensic tool testing program

- Users can make informed choices
- Neutral test program (not law enforcement)
- Reduce challenges to admissibility of digital evidence
- Tool creators make better tools

Other Testing Activities

- PDAs and Cell Phones, NIST Computer Security Division (Rick Ayers)
- DCCI (Department of Defense) not publicly available (Mark Hirsh)
- DFTT on source forge (Brian Carrier) just test data, not a test program
- Individual forensic labs -- to meet ASCLAD LAB accreditation criteria

Resources: Testing

- IEEE Standard 829, IEEE Standard for Software Test Documentation
- Conformance testing: http://www.itl.nist.gov/div897/ctg/conformProject.html
- ISO/IEC Guide 2:1996, Standardization and Related Activities – General Vocabulary
- IEEE Standard 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology
- ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories
- www.swgde.org -- guidelines for tool validation

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