Computer Forensic Tool Testing at NIST

Jim Lyle

Information Technology Laboratory

AAFS

Seattle, 24 Feburary 2006

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
  - Test harness
  - Examples
- Questions and answers

Investigators Need …

Computer forensic investigators need tools that …

- Work as they should,
- Reference data to reduce analysis workload,
- Produce results admissible in court, and
- Are independently tested tools

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)

Why NIST/ITL is involved

- Mission: Assist federal, state & local agencies
- NIST is a neutral organization – not law enforcement or vendor
- NIST provides an open, rigorous process

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)

What is the NSRL?

National Software Reference Library (NSRL)

- Physical library of software, 6,000 products
- Database of known file signatures
- Reference Data Set (RDS)
  - 10,500,000 file signatures on CD (SHA-1, MD5)

Goals

- Automate the process of identifying known files on computers used in crimes
- Allow investigators to concentrate on files that could contain evidence (unknown and suspect files)

NSRL Software & Metadata

- Most popular, most desired software
- Currently 32 languages, used internationally
- Software is purchased commercially
- Software is donated under non-use policy
- List of contents available on website, **www.nsrl.nist.gov**
- Look for malicious files, e.g., hacker tools
- Identify duplicate files
- Allows positive identification of manufacturer, product, operating system, version, file name from file "signature"
- Data format available for forensic tool developers
- Published quarterly, free redistribution

The Problem for Investigators

Do forensic tools work as they should?

- Software tools must be …
  - Tested: accurate, reliable & repeatable
  - Peer reviewed
  - Generally accepted
- … by whom?
- Results of a forensic analysis must be admissible in court

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

Testing Style

- IV&V (Independent Verification & Validation)?
- Conformance Testing Model?
- Other Models? E.g., formal methods?

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 Assertions

- Each test assertion should be a single testable statement (or condition)
- Pre-condition: establish conditions for the test
- Action: the operation under test
- Post-condition: measurement of the results after the operation

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

Develop Test Harness

- A set of tools or procedures to measure the results of each test assertion
- Must be under strict version control
- Must measure the right parameter (validated)
- Must measure the parameter correctly (verified)

V&V of Test Harness

- May be a significant amount of work
- May have more detailed requirements than the forensic tool
- Test harness must be revalidated if changed

Example from Acquisition

- Requirement
- Test Assertion
- Test Case

Acquisition Requirements

- First draft: All digital data is acquired
- Problems:
  - Some sectors masked by HPA or DCO
  - Really want an accurate acquisition
  - What about I/O errors? Ignore for now
- Second Draft: several requirements
  - All visible sectors are acquired
  - All masked sectors are acquired
  - All acquired sectors are accurately acquired

More Requirements

- A requirement, simple at first glance, is really complex and becomes three requirements
- Three simple requirements are easier to measure
- Some tools might not see the masked (HPA, DCO) sectors
- A vocabulary with definitions helps the reader understand the exact meaning of terms in the requirements

Test Assertions

We now have one test assertion for each requirement:

- If a digital source is imaged then all visible sectors are acquired.
- If a digital source is imaged and there are hidden (HPA, DCO) sectors on the target, then all hidden sectors are acquired.
- If a digital source is imaged, then all acquired sectors are accurately acquired.

Measuring Assertions

- How to measure these assertions?
- Somewhat tool dependent
  - Tool may report number of sectors acquired
  - Tool may report a hash (MD5, SHA1) of acquired data
  - Tool may copy acquired data somewhere

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

Ready to Test Tools

- Everything ready to test a tool
  - Specification (requirements, test assertions & test cases, test procedures)
  - Validated test harness (user manual, validation plan, validation report)
- Steering committee selects tools to test
  - Most widely used tools selected
  - May be unfair to vendors

Tool Test Process

After Steering Committee selects a tool …

- Acquire tool & review documentation
- Select test cases
- Execute test cases
- Discuss unexpected results with vendor & other labs (CART, DCCI, RCMP, others)
- Produce test report (deliver to NIJ)
- NIJ reviews and posts test report

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

Current Activities

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

Challenges

- No standards or specifications for tools
- Arcane knowledge domain (e.g. DOS, BIOS, Windows drivers, Bus protocols)
- Reliably faulty hardware
- Many versions of each tool

Impact

- Release 18 (Feb 2001) - A US government organization was doing some testing and uncovered an issue under a specific set of circumstances.
- Linux doesn't use the last sector if odd
- 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)
- Draft of revised disk imaging posted
- 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
- Revised Disk Imaging

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

Test Reports in Progress

- Hardware write block devices: FastBloc IDE, DriveLock IDE, NoWrite, FireFly, UltraBlock SATA, WiebeTech FireWire and five more
- Disk imaging software: IXimager

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 Resources

- 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
- SWGDE guidelines for tool validation (www.swgde.org)

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

Mark Skall
Chief, Software Diagnostics & Conformance Testing Div.
www.itl.nist.gov/div897
skall@nist.gov

Sue Ballou, Office of Law Enforcement Standards
Steering Committee Rep. For State/Local Law Enforcement
susan.ballou@nist.gov