The Contribution of Tool Testing to the Challenge of Responding to an IT Adversary

Jim Lyle

National Institute of Standards and Technology

23 October 2006

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
- Conformance testing forensic tools
- Testing Disk imaging tools and Write blocking devices
- Summary

Something Is Wrong

- Something is not quite right
- An investigation is started
  - What is going on?
  - Who is doing it?
  - How?
  - Is it criminal?
- Now what?

Challenges for the Investigator

- Technical
  - Hardware: Intel, AMD, Mac, Sun, …
  - Operating systems: DOS, Windows, Linux, FreeBSD, UNIX, …
  - File systems: FAT, NT, EXT, Mac, UNIX, …
  - Networks: TCP/IP, HTTP, FTP, email, IM, …
- Infrastructure

Investigators Need …

Computer forensic investigators need tools that …

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

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)

Origins of CFTT

- 1999 US law enforcement saw a need for independent assessment of forensic tools
- 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)
- SAMATE -- Software Assurance Metrics and Tool Evaluation (Paul E. Black)
- CFReDS -- Computer Forensics Reference Data Sets (Jim Lyle)
- Cell phone/PDA forensics (Richard Ayers, Computer Security Division)
- Incident Response Guidelines (Tim Grance, Computer Security Division)

Testing Model

- 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

Forensic Tools

- … 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?
- Testing by feature uses a set of tests for each feature: acquisition, searching, data recovery
- Examples: EnCase acquisition, iLook string search, FTK file recovery

Conformance Testing at CFTT

- A **specification** giving an unambiguous list of requirements,
- A **test plan** describing test cases to run, criteria for selecting test cases and criteria for conformity assessment,
- A set of **test tools** for creating test data and extracting test results,
- A set of **test procedures** to follow during test execution.

Developing a Specification

1. NIST develops a specification (requirements)
2. The specification is posted to the web for peer review
3. Relevant comments and feedback are incorporated
4. A test plan, test assertions and test cases, is developed.
5. The test plan is posted to the web for peer review
6. Relevant comments and feedback are incorporated
7. Final versions of the specification and test plan are posted
8. The test tools and test procedures are developed

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

Testing a Tool

1. Steering Committee selects tool to test.
2. NIST acquires the tool to be tested.
3. NIST reviews the tool documentation.
4. NIST selects relevant test cases depending on features supported by the tool.
5. NIST executes tests.
6. NIST produces test report.
7. Steering Committee reviews test report.
8. Vendor reviews test report.
9. NIJ posts test report to web.

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

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

Impact from Imaging Testing

- 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

Write Blocker Test Results

- Some blockers allowed an obsolete low level formatting command that command cannot modify drive contents with meaningful data but can erase the drive.
- Some blockers substituted a different read command for the command issued by the host.
- Some blockers cached the results of the IDENTIFY DEVICE command so that the number of sectors on the drive returned for the IDENTIFY DEVICE command was not updated to reflect a change in number of accessible sectors.

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

Available Specifications

- Disk Imaging (e.g., Safeback, EnCase, Ilook, Mares imaging tool)
- Deleted file recovery
- Write Block Software Tools (e.g., RCMP HDL, Pdblock, ACES)
- Write Block Hardware Devices (A-Card, FastBlock, NoWrite)

Specifications Under Development

- String Searching
- File carving

Available Test Reports

- Disk imaging: Sydex SafeBack 2.0, NTI Safeback 2.18, EnCase 3.20, GNU dd 4.0.36 (RedHat 7.1),FreeBSD 4.4 dd
- Software write block: RCMP HDL V0.4, V0.5, V0.7,V0.8, PDblock
- Write block devices: FastBloc, WiebeTech, Tableau, MyKey

Test Reports in Progress

- Disk imaging: IXimager, EnCase V4, EnCase V5, linen
- Additional Write blocker models

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

Summary

- The tool user to makes informed choices about tools.
- The tool vendors get feedback for tool improvement.
- Independently tested tools are less likely to be successfully challenged in court.
- The specification process highlights technical issues that need consensus.
- Diverse organizations can test forensic tools in a comparable way.
- First step toward development of international standards for forensic tools.
- Programs similar to CFTT can be established.

Contacts

Jim Lyle

www.cftt.nist.gov

cftt@nist.gov

Sue Ballou, Office of Law Enforcement Standards

susan.ballou@nist.gov