Computer Forensics:

Tool Testing
&
National Software Reference Library

Barbara Guttman
Information Technology Laboratory
3/11/2003

Outline

- Overview of computer forensics
- CFTT – Computer Forensics Tool Testing
- NSRL – National Software Reference Library

3/3/2003
A Shocking Revelation . . .

- Computers can be involved in crime ...
- As a victim
- As a weapon
- As a witness
- As a record
- As contraband

Outline of an Investigation

- Get proper authorization
- Seize evidence (Hard drives, floppies ...)
- Create duplicates for analysis
- Search the duplicates
  - Exclude known benign files
  - Examine obvious files
  - Search for hidden evidence
- Act on results
Investigators Need ...

- Computer forensic investigators need tools that ...
- Work well and
- Produce results admissible in court

What is the Problem?
What are NSRL and CFTT?

Automate the process to find evidence (NSRL)
Verify that tools work as expected (CFTT)
Get results accepted in court (CFTT)

---

Goals of CF at NIST

- Establish methodology for testing computer forensic tools
- Provide international standard reference data that tool makers and investigators can use in an investigations
Why NIST/ITL is involved

- NIST (OLES, ITL/SDCT)
- DoJ (NIJ, FBI)
- DoD (DCCC)
- TREASURY (USCS, USSS)
- National State/Local Agencies
- Software Vendors

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

3/3/2003
A Problem for Investigators

- Results of a forensic analysis must be admissible in court
- Software tools must be ...
  - Tested
  - Peer reviewed
  - Generally accepted
- ... by whom?

3/3/2003

CFTT Goal

- To ensure that computer forensics tools work as expected by law enforcement community
- Help law enforcement meet requirements of scientific evidence and expert testimony
- Allow results to be accepted in court
- Improve vendor software

3/3/2003
Project Tasks

- Identify tool categories e.g.,
  - disk imaging,
  - hard drive write protect,
  - deleted file recovery
- Develop standards for each category
- Peer review of standards
- Test methodology for each category
- Report results

Current Activities

Evaluating test methodology for ...
- Hard drive imaging tools
- Software hard drive write protect
- Hardware hard drive write protect
- Deleted file recovery
Testing Hard Disk Drive Imaging Tools

Need to verify...

- Source disk not changed
- Copied information is accurate
- Behavior if source is smaller than destination
- Behavior if source is larger than destination

Setup Source
Wipe
Load OS
Hash
Testing Hard Disk Drive Imaging Tools

- Select Source
- Wipe Destination
- Run Tool
- Compare Src : Dst
- Hash Source

3/3/2003

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
- EnCase
- iLook
- CFTT is a topic of discussion at various forensic meetings and criminal cases
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
What is the NSRL?

- National Software Reference Library (NSRL)
  - Physical library of software, 4000 products
  - SQL Server database of known file signatures
  - Reference Data Set (RDS)
    - Extract of database on CD: 12,000,000 file signatures
- 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)

Addressing Law Enforcement Needs

- LE needed an unbiased organization
- LE needed traceability for the NSRL contents
- No repositories of original software available for reproducing data
- NSRL needs to work with many CF tools
**Scope of the NSRL**

- NIST has collected software for 2 years
- Software is recorded as the original source for known files and stored as a part of the NSRL
- Versions of OS, DBMS, photo editors, word processors, network browsers, compilers...
- Data formats, data dictionary and project status information is available on the website for RDS users and industry reference

---

**What is the RDS?**

![Image of NSRL Reference Data Set](image-url)
What is the RDS?

- Reference set of file profiles
  - Each profile includes file name, file size, 4 file signatures (SHA1, MD5, CRC32), application name, operating system, etc.
  - Extracted from files on original software CDs, diskettes, and network downloads
  - A single application has between 50 and 10,000 separate file profiles

How to Use the RDS

- Eliminate as many known files as possible from the examination process using automated means
- Look for files that should be installed, but are not (incomplete deletion of pirated software)
- Look for files that could be suspect (hash matches, but name does not)
  - Discover files that do not contain expected contents (.exe file containing a bomb schematic, facility map)
- Look for "bad" files (e.g., hacker tools)
- Provide rigorously verified data for forensic investigations

3/3/2003
RDS Field Use Example

You are looking for facility maps on a computer which is running Windows NT 4.0 Workstation.

Windows NT 4.0 operating system software contains over 6753 images which are known gifs, icons, jpeg files, etc.

By using the RDS and an analysis program the investigator would not have to look at these files to complete his investigation.
Hash Examples

<table>
<thead>
<tr>
<th>Filename</th>
<th>Bytes</th>
<th>SHA-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT4\ALPHA\notepad.exe</td>
<td>68368</td>
<td>F1F284D5D7570199ED9C44A05AC146B9D204EAE67</td>
</tr>
<tr>
<td>NT4\I386\notepad.exe</td>
<td>45328</td>
<td>3C4E15A29014358C61548A981A4AC85731679E37</td>
</tr>
<tr>
<td>NT4\HPR\notepad.exe</td>
<td>66832</td>
<td>3330995684DBA665BE0B962308F2E21378998E69</td>
</tr>
<tr>
<td>NT4\PPC\notepad.exe</td>
<td>68880</td>
<td>47B974F2E4D5656D75DEB492D8C17B1BFD3FB23</td>
</tr>
<tr>
<td>WINNT31.WKS\I386\notepad.exe</td>
<td>57252</td>
<td>2E0849CF327709FC46B705EEAB5E57380F5B1F67</td>
</tr>
<tr>
<td>WINNT31.SRV\I386\notepad.exe</td>
<td>57252</td>
<td>2E0849CF327709FC46B705EEAB5E57380F5B1F67</td>
</tr>
</tbody>
</table>

3/3/2003

NSRL Accomplishments

- RDS CD 5 releases:
  - From 1 million to 12 million files
  - Free redistribution
- Incorporate into vendor products
- Used by FBI, DCCC, Secret Service, Customs Service

3/3/2003
Contacts

Jim Lyle
www.cftt.nist.gov
cftt@nist.gov

Barbara Guttman
bguttman@nist.gov

Doug White
www.nsrl.nist.gov
nsrl@nist.gov