Testing Disk Imaging Tools

By

James Lyle

Presented At

The Digital Forensic Research Conference

DFRWS 2002 USA Syracuse, NY (Aug 6th - 9th)

NIST CFTT:
Testing Disk Imaging Tools

James R. Lyle

National Institute of Standards and Technology

Gaithersburg Md

Talk Overview

- Project Background
- Test methodology
- Creating the disk imaging specification
- Testing imaging tools
- Current CFTT status
- Future directions

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.

Goals of CFTT

Problem: Computer forensic investigators need tools that …

- Work well and
- Produce results admissible in court

Response: Establish a testing methodology by developing for forensic tools …

- Specifications
- Test procedures
- Test cases

Why is NIST involved?

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

Overview of Methodology

- CFTT directed by Steering Committee
- Functionality driven
- Specifications developed for specific categories of activities, e.g., disk imaging, hard drive write protect, etc.
- Test methodology developed for each category

Developing a Specification

After tool category selected by SC …

- Focus group (law enforcement + ITL) develop tool category specification
- Spec posted to web for public comment
- Comments incorporated
- Develop test environment

Tool Test Process

After SC selects a tool …

- Acquire tool & review documentation
- Select test cases
- Execute test cases
- Produce test report

Capabilities to test disk imaging

- Accuracy of copy
  - Compare disks
  - Initialize disk sectors to unique content
- Verify source disk unchanged
- Corrupt an image file
- Error handling: reliably faulty disk

Test Case Structure: Setup

1. Record details of source disk setup.
2. Initialize the source disk to a known value.
3. Hash the source disk and save hash value.
4. Record details of test case setup.
5. Initialize a destination disk.
6. If the test requires a partition, create and format a partition on the destination disk.
7. If the test uses an image file, partition and format a disk for the image file.

Test Case Structure: Run Tool

8. If required, setup I/O error
9. If required, create image file
10. If required, corrupt image file
11. Create destination

Test Case Structure: Measure

12. Compare Source to Destination
13. Rehash the Source

Disk Imaging Test Parameters

Parameter	Value
Functions	Copy, Image, Verify
Source interface	BIOS to IDE, BIOS to SCSI, ATA, ASPI, Legacy BIOS
Dst interface	
Relative size	Src=Dst, Src<Dst, Src>Dst
Errors	None, Src Rd, Dst Wt, Img R/W/C
Object type	Disk, FAT12/16/32, NT, Ext2
Remote access	Yes, no

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

Refining the Test Procedure

- During **dd** testing some results seemed to indicate that the Linux environment was making a change to the source disk.
- After investigation we found that the problem was actually the test procedure.

Current Status

- Test reports for Linux dd & SafeBack 2.18 in final review
- Developing test cases for software hard drive write protect specification
- Running EnCase tests

Future Tasks

- Deleted file recovery specification
- Hardware hard disk write protect device specification
- Testing other disk imaging tools