Computer Forensics Tool Testing at NIST

Jim Lyle

Information Technology Laboratory

8 May 2017

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 and NSRL projects
- Questions and answers

Outline of an Investigation

- Get proper authorization
- Seize evidence (Hard drives, floppies …)
- Create duplicates for analysis
- Analyze the duplicates
  - Exclude known benign files
  - Examine obvious files
  - Search for hidden evidence
- Report results

Investigators Need …

Computer forensic investigators need tools that …

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

Goals of CF at NIST

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

Project Sponsors

- NIST/OLES (Program management)
- NIJ (Major funding)
- FBI (Additional funding)
- DCCC (Equipment and support)
- Homeland Security (Technical input)
- State & Local agencies (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**

Computer Forensics in ITL

- Located in Software Diagnostics and Conformance Testing (SDCT) Division
  - Includes development of specifications and conformance tests for use by agencies and industry
  - Work is funded by Federal agencies and NIST internal funds
- Homeland Security support of agencies investigating terrorist activities

A 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

CFTT Presentation Overview

- Project Tasks
- Current activities
- Challenges
- Testing Hard Drive Imaging Tools
- Benefits of CFTT

Project Tasks

- Identify forensics functions e.g.,
  - disk imaging,
  - hard drive write protect,
  - deleted file recovery
- Develop specification for each function
- Peer review of specification
- Test methodology for each function
- Test Tools (by function) & Report results

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, Windows drivers)
- Reliably faulty hardware
- Many versions of each tool

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 function selected by SC …

- Focus group (law enforcement + NIST) develop tool function 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

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

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

Test Logging

- Log everything, automatically if practical
- Hardware, Software, Versions
- Time/date
- Operator

Compare Logging I

- Tool version
- Date/time compiled
- Command line
- Run date/time

```
Z:\ss\DISKCMP.EXE @(#) diskcmp.cpp Version 3.1 Created 10/11/01 at 12:40:22
compiled on Oct 11 2001 at 12:45:27
@(#) support lib zbios.cpp Version 3.1 created 10/11/01 at 12:40:23
support lib compiled Oct 11 2001 at 12:45:36
@(#) zbios.h Version 3.1 Created 10/11/01 at 12:40:24
cmd: Z:\ss\DISKCMP.EXE 01 Cadfael 80 F6 81 92 /new_log /comment SN
run start Sat Oct 19 13:09:25 2002
run finish Sat Oct 19 15:16:06 2002
elapsed time 2:6:41
```

Compare Logging II

- Drive documentation

```
Source Drive 0x80, BIOS: Extensions Present
Interrupt 13  bios  1023/254/63 (max cyl/hd values)
Interrupt 13  ext  16383/016/63 (number of cyl/hd)
40188960 total number of sectors from the BIOS
IDE disk: Model (IBM-DTLA-307020) serial # (YHDYHLD2691)
Max number of user addressable sectors 40188960
Destination Drive 0x81, BIOS: Extensions Present
Interrupt 13  bios  1023/254/63 (max cyl/hd values)
Interrupt 13  ext  16383/016/63 (number of cyl/hd)
58633344 total number of sectors BIOS
IDE disk: Model (WDC WD300BB-00CAA0) serial # (WD-WMA8H2140350)
Max number of user addressable sectors 58633344
```

Compare Logging III

- Note sectors compared, match & differ
- State of excess sectors (dst fill => undisturbed)

```
Sectors compared: 40188960
Sectors match:    40188960
Sectors differ:          0

Source 18444384 fewer than destination
Zero fill:                 0
Src Byte fill (F6):        0
Dst Byte fill (92): 18444384
Dst fill range:  40188960-58633343
```

Legacy BIOS Quirks

- Some may under report drive size
- Example, Quantum SIROCCO1700A has 3335472 sectors 3309/16/63 spc 1008
- BIOS: 3,330,432 sectors with geometry 826/64/63 spc 4032
- BIOS under reports by 1.25 logical cyls and 5 physicals

Compare Logging IV

```
Source Drive 0x80, BIOS: Legacy
Interrupt 13  bios  0825/063/63 (max cyl/hd values)
Interrupt 13  ext  00826/064/63 (number of cyl/hd)
3330432 total number of sectors reported via interrupt 13 from the BIOS
IDE disk: Model (QUANTUM SIROCCO1700A) serial # (111610113604)
Max number of user addressable sectors reported by ATA identify device command 3335472
--------------------------------------
Destination Drive 0x81, BIOS: Legacy
Interrupt 13  bios  0825/063/63 (max cyl/hd values)
Interrupt 13  ext  00826/064/63 (number of cyl/hd)
3330432 total number of sectors reported via interrupt 13 from the BIOS
IDE disk: Model (QUANTUM SIROCCO1700A) serial # (111615915652)
Max number of user addressable sectors reported by ATA identify device command 3335472
----------------------------------------
Sectors compared:  3335472
Sectors match:     3334463
Sectors differ:      1009
Bytes differ:      494363
Diffs range 36460, 3334464-3335471
```

Bad Sector Error Log

```
 Make sector at LBA 36460 appear bad
return code 00010 on command 00002 from disk 00080
at address 00009/00002/00047
Bios disk geometry: 00825/00063/00063
Monitor BIOS interrupt 13h (disk service)
baddisk  compiled on 10/11/01 at 12:43:50
@(#) Version 3.1 Created 10/11/01 at 12:41:45
Now (10/16/01 at 15:21:01) Going . . .  TSR
 -------------------------------
return code 00010 on command 00010 from disk 00080
at address 00009/00002/00047
Bios disk geometry: 00825/00063/00063
Monitor BIOS interrupt 13h (disk service)
baddisk  compiled on 10/11/01 at 12:43:50
@(#) Version 3.1 Created 10/11/01 at 12:41:45
Now (10/16/01 at 15:21:02) Going . . .  TSR
```

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

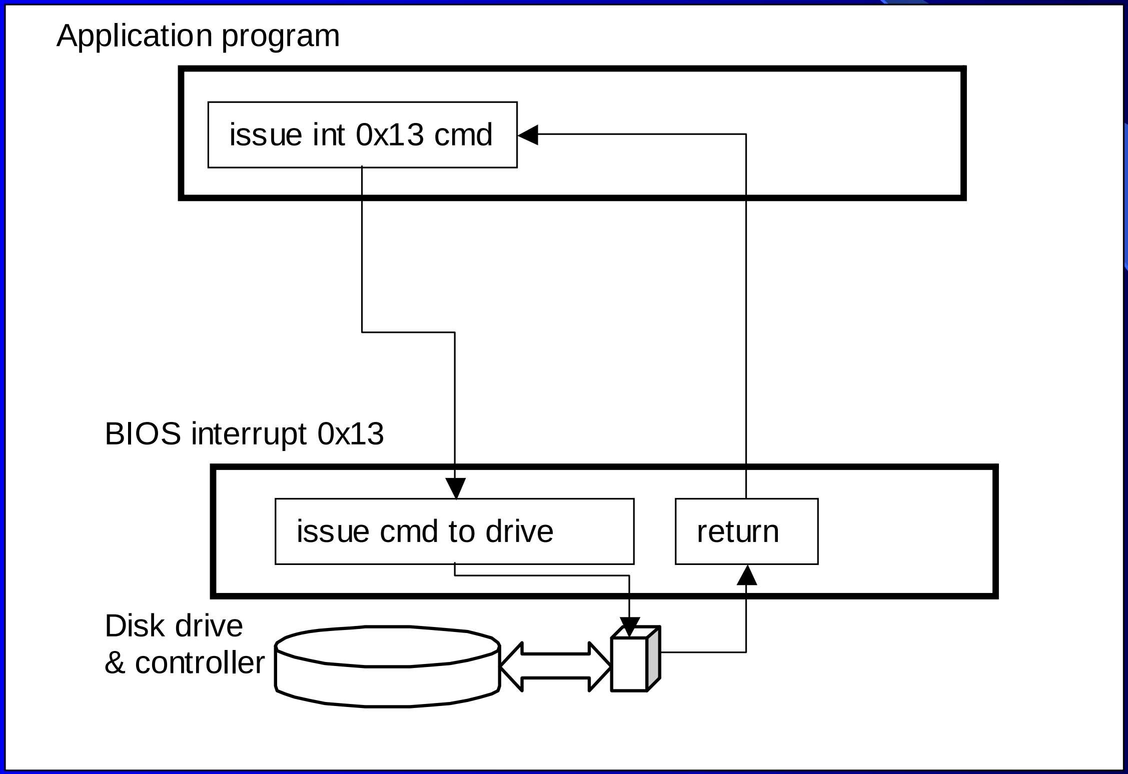
Refining the Test Procedure

- 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.

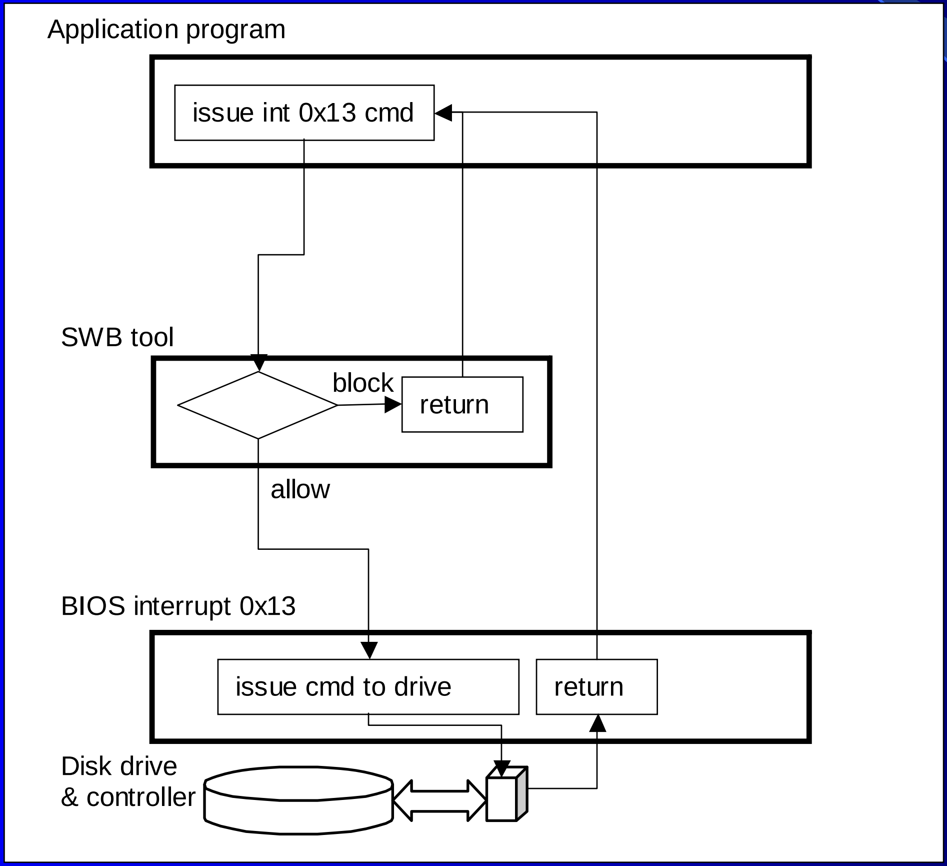
Hard Drive Write Protect

- Can be done either in hardware or software
- Software write protection limited to specific environment: BIOS access or device driver
- Hardware write protection more general

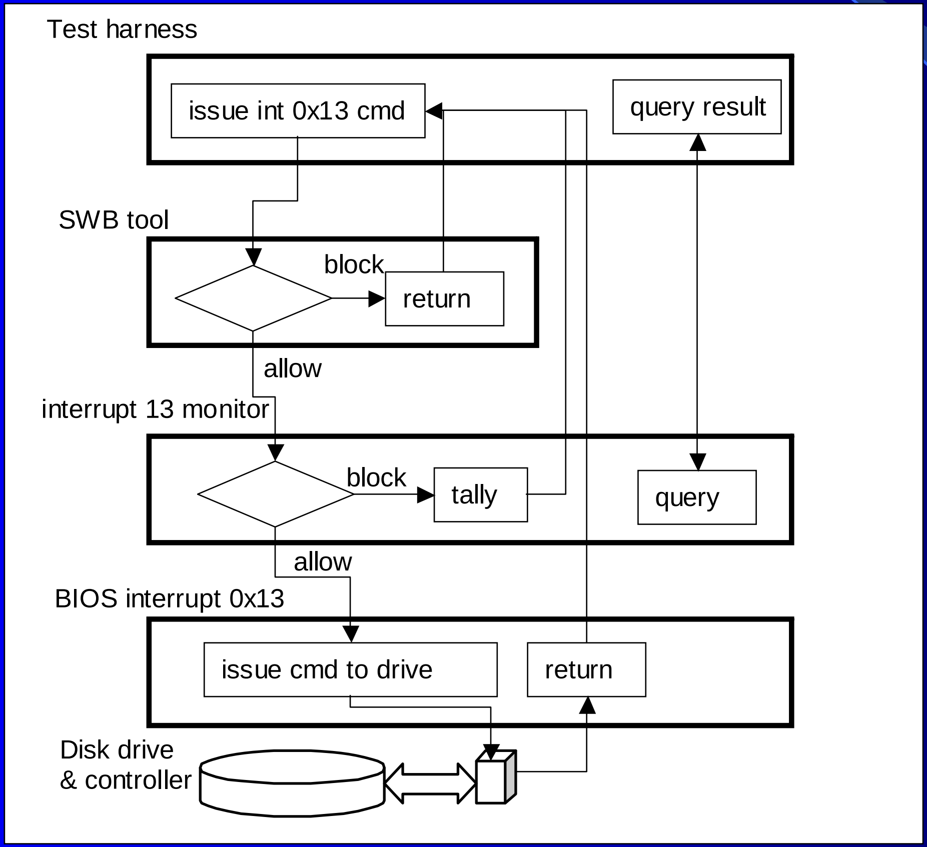
Hard Drive BIOS Access



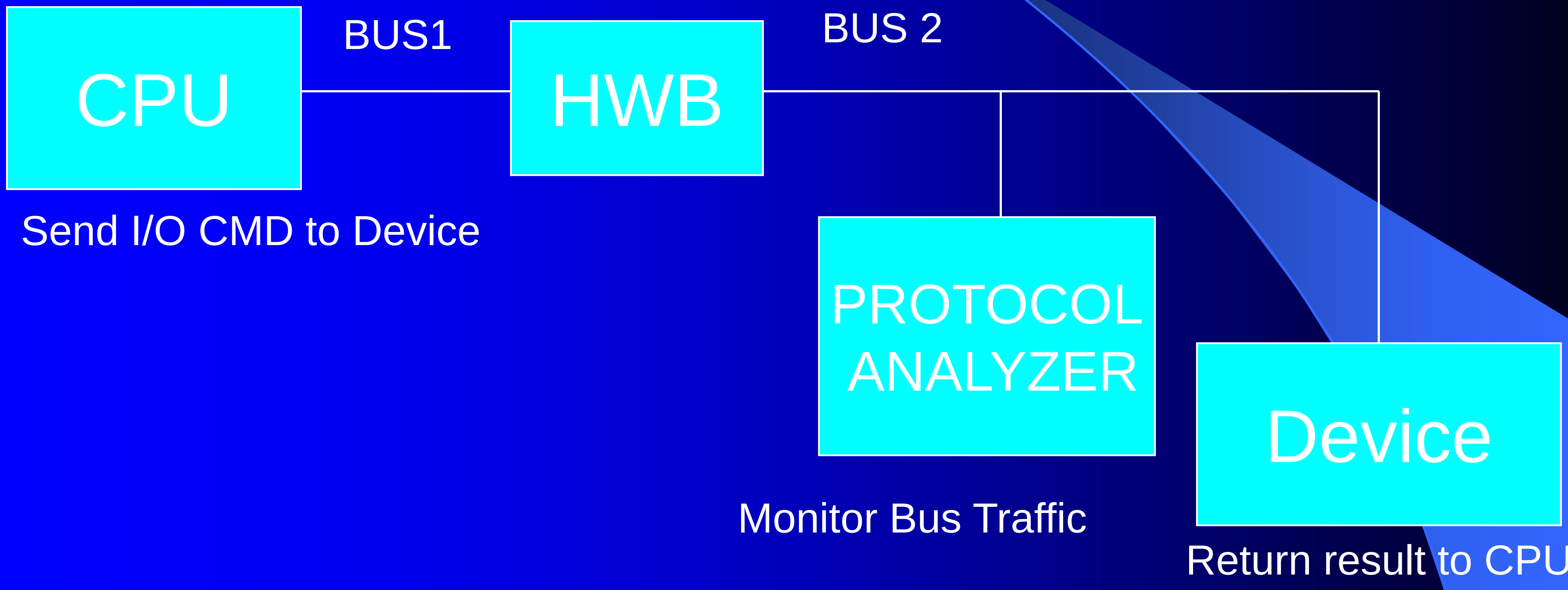
SWB Tool Operation



Test Harness Operation



HWB Testing



Send I/O CMD to Device

Monitor Bus Traffic

Return result to CPU

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)
- Write Block Software Tools (e.g., RCMP HDL, Pdblock, ACES)
- Write Block Hardware Devices (A-Card, FastBlock, NoWrite) – not final

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 V0.8

Test Reports in Production

- RCMP HDL V0.4
- RCMP HDL V0.5
- RCMP HDL V0.7

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

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