Testing Tools to Erase Hard Drives for Reuse

Jim Lyle & Craig Russell
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.

Testing Drive Wipe Tools at CFTT

- Computer Forensic Tool Testing project at NIST
- Develop materials for testing forensic tools . . .
  - Tool Requirements
  - Test Plans
  - Test data www.cfreds.nist.gov (also see Simson Garfinkel; Brian *Carrier* *http://dftt.sourceforge.net/*)
  - Tool test reports submitted to NIJ
- Anyone can use our test methodology to test tools as needed

Drive Wiping

- Remove all data from a drive
- DCO & HPA
  - Tool designer may opt to ignore, i.e., “if hidden area there then it’s not used”
  - Tool designer may decide “every thing must go”
- Command used: WRITE or SECURE ERASE
- Number of overwrite passes (WRITE command)
- Overwrite pattern

Number of Passes

- DoD standard 5220.22-M for clearing and sanitizing magnetic media recommends the approach *"Overwrite all addressable locations with a character, its complement, then a random character and verify"* for clearing and sanitizing information on a writable media.

- **Technology has changed and according to NIST Special Publication 800-88 Guidelines for Media Sanitization:**

" … the change in track density and the related changes in the storage medium have created a situation where the acts of clearing and purging the media have converged. That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack."

Easy Wiping via WRITE

- The easy way to wipe a drive in UNIX (Linux, FreeBSD, etc)

```
dd if=/dev/zero of=/dev/xxx
```

Where /dev/xxx is the name of the device to erase

Other dd options can be added to taste

- There are limitations and costs
  - Skips DCO, maybe HPA, if present
  - Ties up a computer (maybe for hours)
  - Ignores remapped faulty sectors

Easy Wiping via ERASE

- Use CMRR free tool: http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml
- Drive must be attached to ATA or SATA interface
- Uses SECURE ERASE to wipe drive
- PC BIOS often issues SECURITY FREEZE LOCK

Options for Wiping

- Use write commands to overwrite each visible sector
  - Only wipes visible sectors, ignores DCO & HPA
  - DCO & HPA can be removed first
- For ATA & SATA can use SECURE ERASE
  - Also wipes (accessible) remapped bad sectors
  - Must remove DCO & HPA first (Some drives implement SECURE ERASE to erase HPA too)
- Destroy or degauss the drive

Wipe Tool Features

- Choice of WRITE or ERASE command
- Number of overwrites
- Verification pass
- Overwrite pattern: Constant byte, random byte, random sequence
- Removal and wiping for HPA or DCO
- Interface: ATA, SATA, SCSI, USB & FireWire
- Hardware device or Software tool

CFTT Disk Wipe Requirements

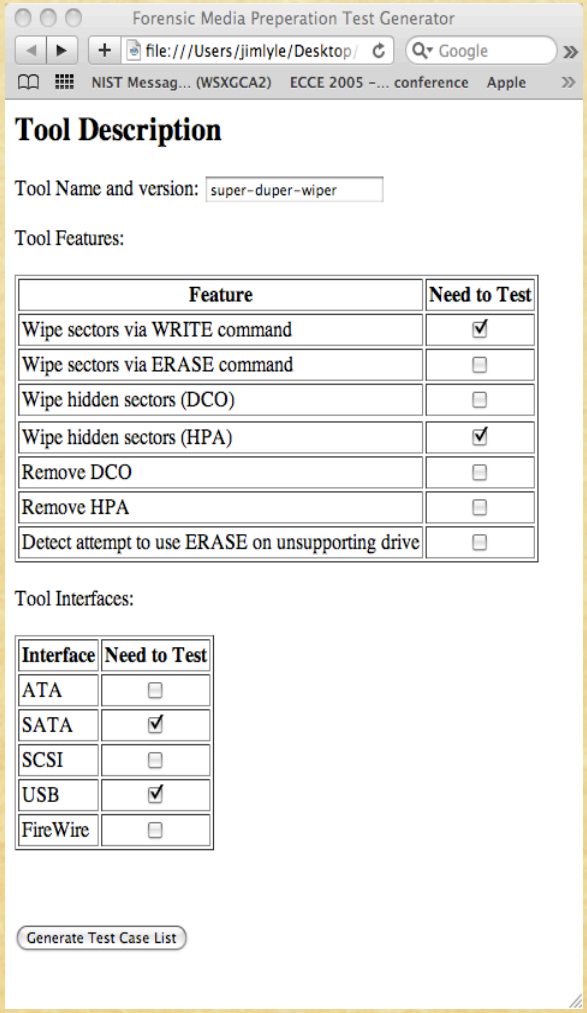
- Wipe method: WRITE or ERASE
- HPA & DCO wipe and removal
- User notification if ERASE selected but not supported by the drive
- Features (may be selected, but) not verified:
  - Multi-pass
  - Verify
  - randomness

Test Cases

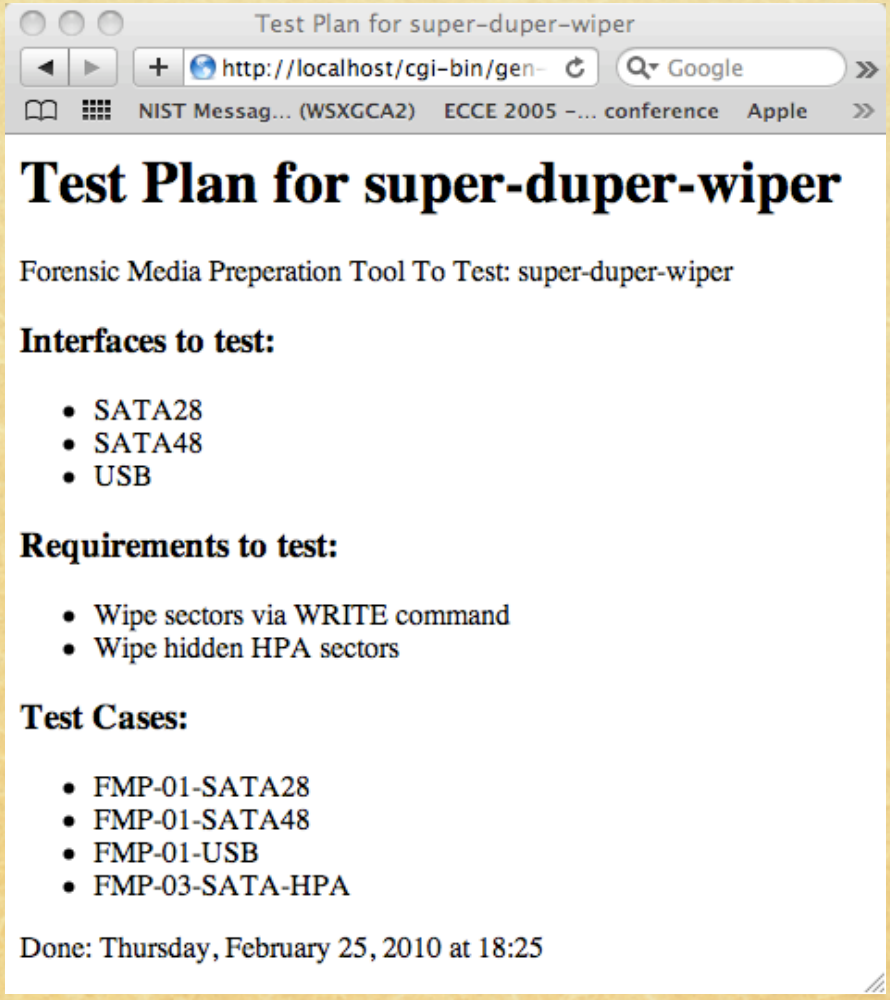
Test Cases	
1.	Use WRITE on visible sectors
2.	Use ERASE on visible sectors
3.	Use WRITE on HPA/DCO
4.	Use ERASE on HPA/DCO
5.	Try to use ERASE on unsupported drive

- Run 1 &2 for each interface: ATA, SATA, USB, etc
- Run 2, 4 & 5 only if SECURE ERASE supported
- Run 3 & 4 only on SATA & ATA interface

Test Case Selection Tool



Generated Test Plan



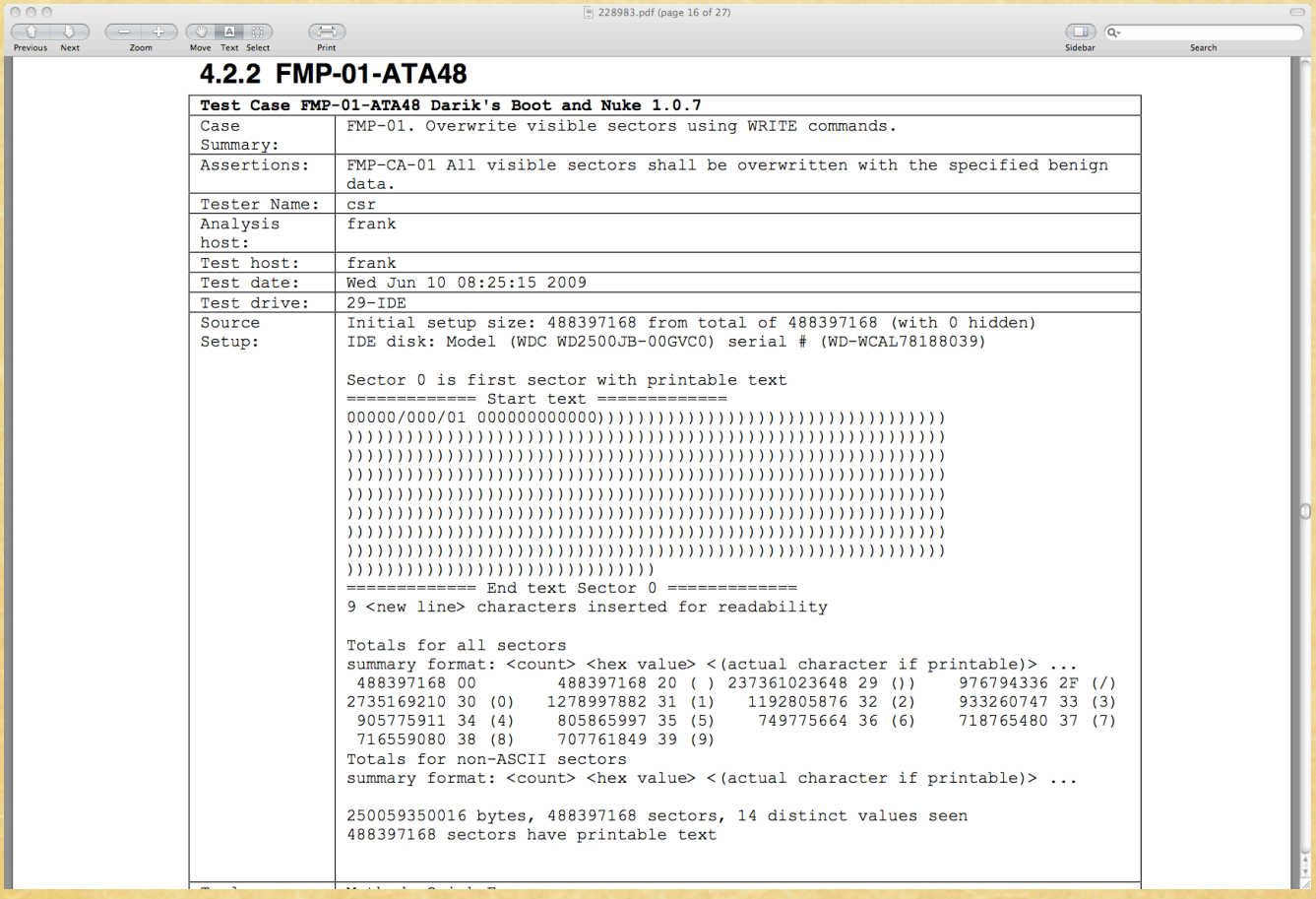
Running a Test Case

1. Remove DCO/HPA
2. Use NIST tool to fill each sector:
   00000/000/01 000000000000xxx ...
3. Optional: add DCO/HPA (cases 3 & 4)
4. Run wipe tool under test
5. Examine result with more NIST tools: DCO/HPA state, drive content

Test Support Tools

- DISKWIPE – put initial content on drive
- DSUMM – disk summary, count number of times each byte value is seen
- RANSUM – identify runs of wiped sectors and runs of unchanged sectors
- One freeware program HDAT2 (not NIST written) to manipulate DCO & HPA

Case Setup



4.2.2 FMP-01-ATA48

Test Case FMP-01-ATA48 Darik's Boot and Nuke 1.0.7	
Case Summary:	FMP-01. Overwrite visible sectors using WRITE commands.
Assertions:	FMP-CA-01 All visible sectors shall be overwritten with the specified benign data.
Tester Name:	csr
Analysis host:	frank
Test host:	frank
Test date:	Wed Jun 10 08:25:15 2009
Test drive:	29-IDE

Source Setup:

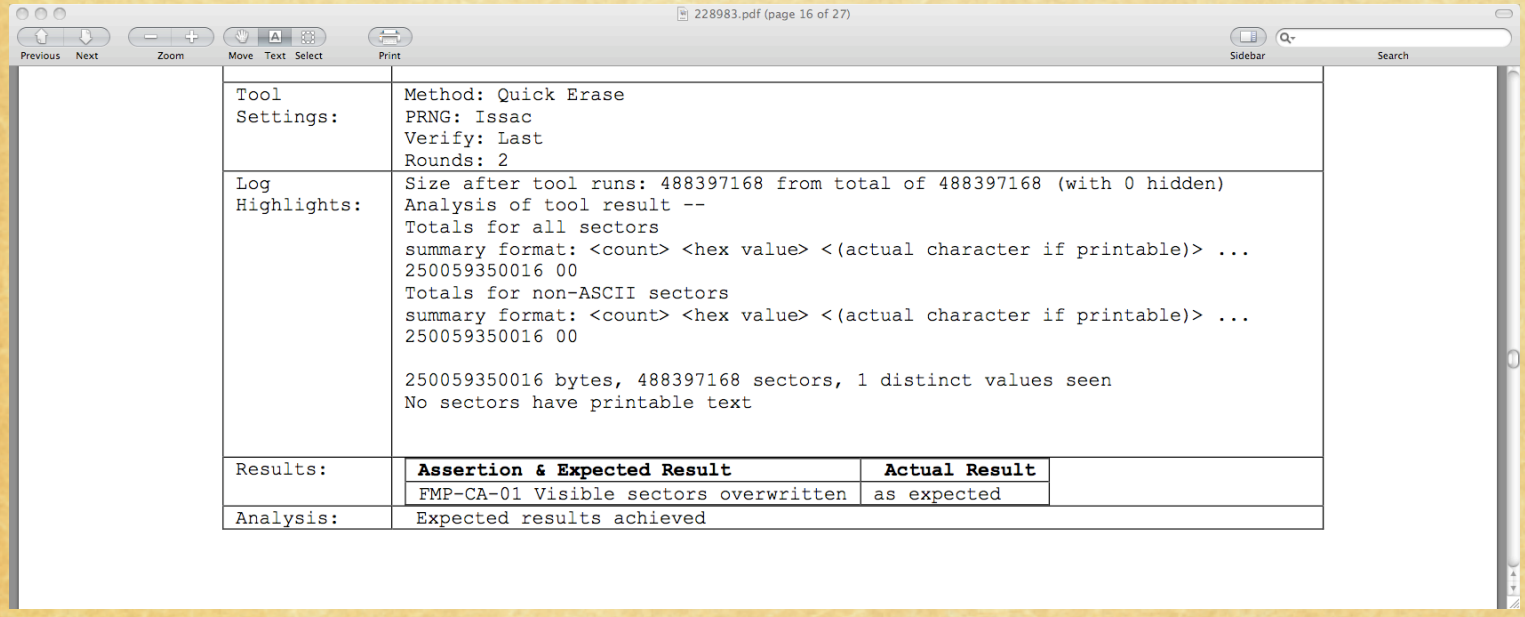
```
Initial setup size: 488397168 from total of 488397168 (with 0 hidden)
IDE disk: Model (WDC WD2500JB-00GVC0) serial # (WD-WCAL78188039)

Sector 0 is first sector with printable text
============= Start text =============
00000/000/01 000000000000)))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
))))))))))))))))))))))))))))))))
============= End text Sector 0 =============
9 <new line> characters inserted for readability

Totals for all sectors
summary format: <count> <hex value> <(actual character if printable)> ...
 488397168 00          488397168 20 ( ) 237361023648 29 ())    976794336 2F (/)
2735169210 30 (0)   1278997882 31 (1)   1192805876 32 (2)    933260747 33 (3)
 905775911 34 (4)    805865997 35 (5)    749775664 36 (6)    718765480 37 (7)
 716559080 38 (8)    707761849 39 (9)
Totals for non-ASCII sectors
summary format: <count> <hex value> <(actual character if printable)> ...

250059350016 bytes, 488397168 sectors, 14 distinct values seen
488397168 sectors have printable text
```

Test Result



Tool Settings:	Method: Quick Erase PRNG: Issac Verify: Last Rounds: 2
Log Highlights:	Size after tool runs: 488397168 from total of 488397168 (with 0 hidden) Analysis of tool result -- Totals for all sectors summary format: <count> <hex value> <(actual character if printable)> ... 250059350016 00 Totals for non-ASCII sectors summary format: <count> <hex value> <(actual character if printable)> ... 250059350016 00 250059350016 bytes, 488397168 sectors, 1 distinct values seen No sectors have printable text
Results:	**Assertion & Expected Result** / **Actual Result** FMP-CA-01 Visible sectors overwritten / as expected
Analysis:	Expected results achieved

Erase Toshiba with HPA

Initial setup size:
375721968 from total of 390721968 (with 15000000 hidden)
IDE disk: Model (TOSHIBA MK2049GSY) serial # (788DT0FLT)

Size after tool runs:
375721968 from total of 390721968 (with 15000000 hidden)

Analysis of tool result –

200049647616 bytes, 390721968 sectors, 14 distinct values seen 15000000 sectors have printable text

Sector 375721968 is first sector with printable text

Results

- HPA not erased and not removed

Erase Hitachi with HPA

Initial setup size:
365721968 from total of 390721968 (with 25000000 hidden)
IDE disk: Model (Hitachi HTS722020K9SA00) serial #

Size after tool runs:
365721968 from total of 390721968 (with 25000000 hidden)

Analysis of tool result -- 200049647616 00
200049647616 bytes, 390721968 sectors, 1 distinct values seen

Results

- HPA set to zeros
- HPA left in place

Reading a CFTT Report

- Results Summary section has everything most people need to read.
- Test Case Selection section describes why we selected each case. May be useful for deeper understanding or if someone wants to do their own testing.
- Test Materials describes the drives used, support tools used, setup procedures and analysis procedures. Not useful unless . . .
  - Assess validity of testing
  - Want to do your own
- Test Details – don't go here! We include it to allow verification of what is reported in the Results Summary.

Results Over 6 Tools

Drive eRazer	Voom Hard Copy II	Boot & Nuke
Disk Jockey PRO FE	Omniclone 2Xi	TD1

- All visible sectors wiped – all tools
- HPA removed but not wiped
- HPA wiped but not removed (ERASE)
- Remove and wipe both HPA & DCO
- HPA & DCO ignored
- HPA & DCO ignored in 1 pass mode, removed & wiped in "DoD 7 pass" mode
- Scratch drive required with some writing to the scratch drive

Project Sponsors (aka Steering Committee)

- National Institute of Justice (Major funding)
- FBI (Additional funding)
- Department of Defense, DCCI (Equipment and support)
- Homeland Security (Major funding)
- State & Local agencies (Technical input)
- Internal Revenue, IRS (Technical input)
- NIST/OLES (Program management)

Contact Information

Jim Lyle
jlyle@nist.gov

Craig Russell
craig.russel@nist.gov

Sue Ballou, Office of Law Enforcement Standards
Steering Committee representative for State/Local Law Enforcement
Susan.ballou@nist.gov

http://www.cftt.nist.gov cftt@nist.gov