OCT 2010

*NIJ*

Special | **REPORT**

# Test Results for Forensic Media Preparation Tool: Disk Jockey PRO Forensic Edition (version 1.20)

*NIJ*

**OCT. 2010**

# Test Results for Forensic Media Preparation Tool: Disk Jockey PRO Forensic Edition (version 1.20)

# NIJ

**John H. Laub**
*Director, National Institute of Justice*

**September 2010**

## Test Results for Forensic Media Preparation Tool:
Disk Jockey PRO Forensic Edition (version 1.20)

NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce

## Contents

## Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice (DOJ), and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation (FBI), the U.S. Department of Defense Cyber Crime Center (DC3), U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program (IRS–CID), and the U.S. Department of Homeland Security's (DHS) Bureau of Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection, and U.S. Secret Service (USSS). The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensic tools is based on well–recognized methodologies for conformance and quality testing. The specifications and test methods are posted on the CFTT Web site (http://www.cftt.nist.gov/) for review and comment by the computer forensics community.

This document reports the results from testing Disk Jockey PRO Forensic Edition (Version 1.20), against the *Forensic Media Preparation Tool Test Assertions and Test Plan Version 1.0*, available at the CFTT Web site (http://www.cftt.nist.gov/fmp–atp–pc–01.pdf).

Test results for other devices and software packages using the CFTT tool methodology can be found on NIJ's computer forensics tool testing Web page, http://www.ojp.usdoj.gov/nij/topics/technology/electronic–crime/cftt.htm.

## How to Read This Report

This report is divided into four key sections. The first section is a summary of the results from the test runs. This section is sufficient for most readers to assess the suitability of the tool for the intended use. The remaining sections of the report describe how the tests were conducted and provide documentation of test case run details that support the report summary. Section 2 gives a justification for the selection of test cases from the set of possible cases that are defined in the test plan for forensic media preparation tools. The test cases are selected, in general, based on features offered by the tool. Section 3 lists hardware and software used to run the test cases with and provides links to additional information about the items used. Section 4 contains a description of each test case. The

description of each test run lists all test assertions used in the test case, the expected result and the actual result.

# Test Results for Forensic Media Preparation Tool

Tool Tested:        Disk Jockey Pro Forensic Edition
Version:            1.20
Run Environments:   Custom

Supplier:           Diskology
                    P.O. Box 733
                    Lincoln, CA 95648

Tel:                916 645–3196 phone
                    270 596–0522 fax
Email:              sales@diskology.com
WWW:                http://www.diskology.com/

# 1. Results Summary

In all the test cases run against Disk Jockey Forensic, all visible sectors were successfully overwritten. For the test cases that used drives containing an HPA or DCO, the tool behaved as designed by the vendor as follows:

- In the two single pass mode tests (FMP–03–DCO–2 & FMP–03–DCO–HPA–2), the HPA and DCO remained intact; hidden sectors were not overwritten.
- In DoD x7 pass mode, HPA hidden sectors were removed and overwritten (FMP–03–HPA–2).

The vendor clarified the tool behavior with the following statement:

> DATA ERASE DoD—This mode erases the data of the attached HDD by writing seven–passes per the standard established by the Department of Defense. NOTE: This mode will also remove (reset) any HPA or DCO settings before proceeding to erase/wipe the disk, therefore every usable sector of the disk, including any sectors formerly within an HPA or DCO area will also be erased/wiped.

> DATA ERASE 00x1—This mode completes a one–pass erase on the disk by writing 00h bytes in all sectors of the connected HDD. NOTE: This mode will not remove either an HPA or DCO area from the disk; nor will it erase/wipe any sectors in those areas.

## 2.  Test Case Selection

Disk Jockey Pro Forensic was tested for its ability to overwrite sectors. The prime function of the device is a hard drive duplication system for cloning a master drive to one or two target drives. The device optionally supports a secondary function to wipe one target drive. This test report covers only the results of testing the wipe function.

The tested device has two ports for attaching hard drives. The ports are labeled Source Disk and Destination Disk respectively. Drives attached to the Destination Disk port can be overwritten by selecting either a quick single pass that writes 00h to the disk or a DoD seven pass option. It should be noted that in addition the Source port is write protected, thus rendering the disk protected from the wipe command.

 The test cases selected were limited to only those test cases defined by *Forensic Media Preparation Tool Test Assertions and Test Plan Version 1.0* and applicable to features supported by this tool.

Since Disk Jockey Pro Forensic does not support a secure erase mode those tests were omitted. All selected test cases were *WRITE* tests (cases FMP–01 and FMP–03).

Three hidden sector test cases (FMP–03) were included among the cases selected. They were included to measure the tool behavior in conjunction with hidden sectors.

The following cases were used in testing:

- FMP–01–ATA28
- FMP–01–ATA48
- FMP–01–SATA28
- FMP–01–SATA48
- FMP–03–DCO–HPA–2
- FMP–03–DCO–2
- FMP–03–HPA–2

The following source interfaces were tested: ATA28, ATA48, SATA28, SATA48.

The table below shows the user parameter set for each test run, i.e., destination drive type, number of passes, and fill value. Refer to the tool documentation for additional information about these parameters. The following table documents the settings for each test case:

| Test Case | Destination Disk Type | Pass | Fill |
|-----------|----------------------|------|------|
| FMP-01-ATA28 | Desktop | 1 | 00h |
| FMP-01-ATA48 | Desktop | 7 | 00h |
| FMP-01-SATA28 | Desktop | 1 | 00h |

| Test Case | Destination Disk Type | Pass | Fill |
|---|---|---|---|
| FMP–01–SATA48 | Desktop | 7 | 00h |
| FMP–03–DCO–HPA–2 | Laptop | 1 | 00h |
| FMP–03–DCO–2 | Laptop | 1 | 00h |
| FMP–03–HPA–2 | Desktop | 7 | 00h |

# 3. Test Materials

## 3.1 Support Software

Several programs were used in the setup and analysis of the test drives. These include **hdat2** (download from: http://www.hdat2.com/download.html), **dsumm** (download from: http://www.cftt.nist.gov/) and **diskwipe** from **FS–TST Release 2.0** (download from: http://www.cftt.nist.gov/diskimaging/fs–tst20.zip).

The **hdat2** program is used to create, remove and document hidden areas on a drive.

The **diskwipe** program initializes a hard drive with known content.

The **dsumm** program analyzes the content of a hard drive and produces a summary of disk contents in terms of counts for each byte value present on the drive. For example, if a drive can contain 10GB (19531250 sectors of 512 bytes per sector) and the drive is wiped with zero bytes, then **dsumm** reports 10,000,000,000 zero bytes. The program also prints the first sector found with printable ASCII content.

## 3.2 Test Drive Creation

The following steps are used to setup a test drive:

1. The drive is initially filled with known content by the **diskwipe** program from FS–TST. The **diskwipe** program writes the sector address to each sector in both C/H/S and LBA format. The remainder of the sector bytes is set to a constant fill value unique for each drive. The fill value is noted in the **diskwipe** tool log file.
2. The **dsumm** program analyzes the drive contents. This documents the content of the drive. Each sector has unique content after the setup.
3. If the drive is intended for hidden area tests (FMP–03), an HPA, a DCO or both are created.
4. The drive size after creation of a hidden area is recorded.

## 3.3  Test Drive Analysis

The following steps are used to analyze a test drive after it has been wiped by the tool under test:

1. The size of the drive is recorded. This determines if the tool changes the size of a hidden area.
2. Any hidden areas still present on the drive are removed.
3. The **dsumm** program is run to determine the final content of the drive.

## 3.4  Test Drives

The following hard drives listed in the following table were used in testing. The column labeled **Test Case** identifies the test case. The column labeled **Sectors** is the size of the drive with no DCO or HPA. The column labeled **Model** is the model of the drive as returned by the ATA IDENTIFY DEVICE command. The column labeled **Serial #** is the serial number as returned by the ATA IDENTIFY DEVICE command.

| Test Case | Sectors | Model | Serial # |
|---|---|---|---|
| FMP–01–ATA28 | 80043264 | Maxtor 6Y040L0 | Y2SM68LE |
| FMP–01–ATA48 | 488397168 | WDC WD2500JB–00GVC0 | WD–WCAL78188039 |
| FMP–01–SATA28 | 234441648 | WDC WD1200JD–00GBB0 | WD–WMAES2049679 |
| FMP–01–SATA48 | 312581808 | ST3160815AS | 9RX7Y1DP |
| FMP–03–DCO–HPA–2 | 156301488 | Hitachi HTS541680J9AT00 | SB0241HGGAWN9E |
| FMP–03–DCO–2 | 234441648 | Hitachi HTS542512K9SA00 | 080914BB6200WBKPDL2G |
| FMP–03–HPA–2 | 312581808 | WDC WD1600JB–00GVC0 | WD–WMAL94865344 |

For FMP–03 test cases the layout of visible and hidden sectors is as follows. The column labeled **Test Case** identifies the test case. The column labeled **Size** is the number of visible sectors presented to the device for the test case. The column labeled **Hidden** is the size in sectors of the hidden area.

| Test Case | Size | Total | Hidden (DCO+HPA) |
|---|---|---|---|
| FMP–03–DCO–HPA–2 | 131301488 | 156301488 | 25000000 (10000000+15000000) |
| FMP–03–DCO–2 | 224441648 | 234441648 | 10000000 |
| FMP–03–HPA–2 | 297581808 | 312581808 | 15000000 |

# 4.  Test Results

The main item of interest for interpreting the test results is determining the conformance of the tool under test with the test assertions. Conformance with each assertion tested by a given test case is evaluated by examining the **Log Highlights** box of the test report summary.

## *4.1 Test Results Report Key*

A summary of the actual test results is presented in this report. The following table presents a description of each section of the test report summary.

| Heading | Description |
|---|---|
| First Line: | Test case ID, name, and version of tool tested. |
| Case Summary: | Test case summary from *Forensic Media Preparation Tool Test Assertions and Test Plan Version 1.0.* |
| Assertions: | The test assertions applicable to the test case, selected from *Forensic Media Preparation Tool Test Assertions and Test Plan Version 1.0.* |
| Tester Name: | Name or initials of person executing test procedure. |
| Analysis Host: | Host used to setup test drive and analyze final drive state. |
| Test Host: | Host computer executing the test. |
| Test Date: | Time and date that test was started. |
| Test Drive: | Drive erased by the tool under test. |
| Source Setup: | Report of the native drive size, the size of any hidden areas, the apparent size of the drive (as reported by an ATA IDENTIFY DEVICE command) and an analysis of initial drive contents. |
| Tool Settings: | Report of tool parameters set for each test run. |
| Log Highlights: | Report of the state of the drive after executing the tool under test, including the apparent drive size, size of hidden area and analysis of drive contents. The ASCII content of the first non–binary–zero sector is reported. |
| Results: | Expected and actual results for each assertion tested. |
| Analysis: | Whether or not the expected results were achieved. |

## *4.2 Test Details*

### 4.2.1 FMP–01–ATA28

| Test Case FMP-01-ATA28 Disk Jockey Pro Forensic Version 1.20 | |
|---|---|
| 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: | none |
| Test date: | Fri Oct 16 09:47:27 2009 |
| Test drive: | 57-IDE |
| Source Setup: | Initial setup size: 80043264 from total of 80043264 (with 0 hidden) IDE disk: Model (Maxtor 6Y040L0) serial # (Y2SM68LE) |

| | |
|---|---|
| **Test Case FMP-01-ATA28 Disk Jockey Pro Forensic Version 1.20** | |
| | Sector 0 is first sector with printable text |
| | ============= Start text ============= |
| | 00000/000/01 000000000000WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW |
| | ============= End text Sector 0 ============= |
| | 9 <new line> characters inserted for readability |
| | |
| | Totals for all sectors |
| | summary format: <count> <hex value> <(actual character if printable)> ... |
| |   80043264 00      80043264 20 ( )  160086528 2F (/) |
| |  579129549 30 (0)  180771021 31 (1)  141043689 32 (2) |
| |  141042889 33 (3)  138514684 34 (4)  138479164 35 (5) |
| |  123343870 36 (6)  113259050 37 (7)  103108778 38 (8) |
| |  102259114 39 (9) 38901026304 57 (W) |
| | Totals for non-ASCII sectors |
| | summary format: <count> <hex value> <(actual character if printable)> ... |
| | |
| | 40982151168 bytes, 80043264 sectors, 14 distinct values seen |
| | 80043264 sectors have printable text |
| | |
| Tool Settings: | rounds: x1 |
| Log Highlights: | Size after tool runs: 80043264 from total of 80043264 (with 0 hidden) |
| | Analysis of tool result -- |
| | Totals for all sectors |
| | summary format: <count> <hex value> <(actual character if printable)> ... |
| |  40982151168 00 |
| | Totals for non-ASCII sectors |
| | summary format: <count> <hex value> <(actual character if printable)> ... |
| |  40982151168 00 |
| | |
| | 40982151168 bytes, 80043264 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 | | |

## 4.2.2  FMP–01–ATA48

| | |
|---|---|
| **Test Case FMP-01-ATA48 Disk Jockey Pro Forensic Version 1.20** | |
| 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: | none |
| Test date: | Fri Oct 16 14:35:42 2009 |
| Test drive: | 29-IDE |
| Source Setup: | Initial setup size: 488397168 from total of 488397168 (with 0 hidden)<br>IDE disk: Model (WDC WD2500JB-00GVC0) serial # (WD-WCAL78188039)<br><br>Sector 0 is first sector with printable text<br>============= Start text =============<br>00000/000/01 000000000000))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))<br>))))))))))))))))))))))))))))))))))))<br>============= End text Sector 0 =============<br>9 &lt;new line&gt; characters inserted for readability<br><br>Totals for all sectors<br>summary format: &lt;count&gt; &lt;hex value&gt; &lt;(actual character if printable)&gt; ...<br>  488397168 00       488397168 20 ( ) 237361023648 29 ())<br>  976794336 2F (/)  2735169210 30 (0)  1278997882 31 (1)<br> 1192805876 32 (2)   933260747 33 (3)   905775911 34 (4)<br>  805865997 35 (5)   749775664 36 (6)   718765480 37 (7)<br>  716559080 38 (8)   707761849 39 (9)<br>Totals for non-ASCII sectors<br>summary format: &lt;count&gt; &lt;hex value&gt; &lt;(actual character if printable)&gt; ...<br><br>250059350016 bytes, 488397168 sectors, 14 distinct values seen<br>488397168 sectors have printable text |
| Tool Settings: | rounds: DoD x7 |
| Log Highlights: | Size after tool runs: 488397168 from total of 488397168 (with 0 hidden)<br>Analysis of tool result --<br>Totals for all sectors<br>summary format: &lt;count&gt; &lt;hex value&gt; &lt;(actual character if printable)&gt; ...<br>250059350016 F6<br>Totals for non-ASCII sectors<br>summary format: &lt;count&gt; &lt;hex value&gt; &lt;(actual character if printable)&gt; ...<br>250059350016 F6<br><br>250059350016 bytes, 488397168 sectors, 1 distinct values seen<br>No sectors have printable text |

| Results: | **Assertion & Expected Result** | **Actual Result** | |
|---|---|---|---|
| | FMP-CA-01 Visible sectors overwritten | as expected | |
| Analysis: | Expected results achieved | | |

## 4.2.3 FMP–01–SATA28

| Test Case FMP-01-SATA28 Disk Jockey Pro Forensic Version 1.20 | |
|---|---|
| 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: | none |
| Test date: | Thu Oct 22 14:39:43 2009 |
| Test drive: | 1C-SATA |
| Source Setup: | Initial setup size: 234441648 from total of 234441648 (with 0 hidden)<br>IDE disk: Model (WDC WD1200JD-00GBB0) serial # (WD-WMAES2049679)<br><br>Sector 0 is first sector with printable text<br>============= Start text =============<br>00000/000/01 000000000000<br>============= End text Sector 0 =============<br>1 \<new line\> character inserted for readability<br><br>Totals for all sectors<br>summary format: \<count\> \<hex value\> \<(actual character if printable)\> ...<br>  234441648 00    113938640928 1C     234441648 20 ( )<br>  468883296 2F (/)  1461085523 30 (0)  678339301 31 (1)<br>  497617498 32 (2)   407041791 33 (3)  391715334 34 (4)<br>  376075228 35 (5)   347651457 36 (6)  332766225 37 (7)<br>  332765657 38 (8)   332658242 39 (9)<br>Totals for non-ASCII sectors<br>summary format: \<count\> \<hex value\> \<(actual character if printable)\> ...<br><br>120034123776 bytes, 234441648 sectors, 14 distinct values seen<br>234441648 sectors have printable text |
| Tool Settings: | rounds: x1 |
| Log Highlights: | Size after tool runs: 234441648 from total of 234441648 (with 0 hidden)<br>Analysis of tool result --<br>Totals for all sectors<br>summary format: \<count\> \<hex value\> \<(actual character if printable)\> ...<br>120034123776 00<br>Totals for non-ASCII sectors<br>summary format: \<count\> \<hex value\> \<(actual character if printable)\> ...<br>120034123776 00<br><br>120034123776 bytes, 234441648 sectors, 1 distinct values seen<br>No sectors have printable text |
| Results: | **Assertion & Expected Result** \| **Actual Result**<br>FMP-CA-01 Visible sectors overwritten \| as expected |
| Analysis: | Expected results achieved |

## 4.2.4 FMP–01–SATA48

| | |
|---|---|
| **Test Case FMP-01-SATA48 Disk Jockey Pro Forensic Version 1.20** | |
| 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: | none |
| Test date: | Mon Oct 19 12:33:47 2009 |
| Test drive: | 43-SATA |
| Source Setup: | Initial setup size: 312581808 from total of 312581808 (with 0 hidden)<br>IDE disk: Model (ST3160815AS) serial # (9RX7Y1DP)<br><br>Sector 0 is first sector with printable text<br>============= Start text =============<br>00000/000/01 000000000000CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC<br>============= End text Sector 0 =============<br>9 <new line> characters inserted for readability<br><br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>   312581808 00       312581808 20 ( )    625163616 2F (/)<br>  1850492169 30 (0)   906528227 31 (1)   696435016 32 (2)<br>   541016511 33 (3)   522787395 34 (4)   514450557 35 (5)<br>   478352540 36 (6)   458495114 37 (7)   458481159 38 (8)<br>   449761088 39 (9) 151914758688 43 (C)<br>Totals for non–ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br><br>160041885696 bytes, 312581808 sectors, 14 distinct values seen<br>312581808 sectors have printable text |
| Tool Settings: | rounds: DoD x7 |
| Log Highlights: | Size after tool runs: 312581808 from total of 312581808 (with 0 hidden)<br>Analysis of tool result --<br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>160041885696 F6<br>Totals for non-ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>160041885696 F6<br><br>160041885696 bytes, 312581808 sectors, 1 distinct values seen<br>No sectors have printable text |
| Results: | **Assertion & Expected Result** — **Actual Result**<br>FMP-CA-01 Visible sectors overwritten — as expected |
| Analysis: | Expected results achieved |

## 4.2.5 FMP–03–DCO–HPA–2

| Test Case FMP-03-DCO-HPA-2 Disk Jockey Pro Forensic Version 1.20 | |
|---|---|
| Case Summary: | FMP-03. Overwrite hidden sectors using WRITE commands. |
| Assertions: | FMP-CA-01 All visible sectors shall be overwritten with the specified benign data.<br>FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data.<br>FMP-AO-02 A hidden area may optionally be removed from the storage device. |
| Tester Name: | csr |
| Analysis host: | frank |
| Test host: | none |
| Test date: | Thu Oct 29 16:45:33 2009 |
| Test drive: | 14-LAP |
| Source Setup: | Size with DCO: 146301488 74.91 GB (10000000 sectors in DCO)<br>Size with HPA: 131301488 67.23 GB (15000000 sectors in HPA)<br>Initial setup size: 131301488 from total of 156301488 (with 25000000 hidden)<br>IDE disk: Model (Hitachi HTS541680J9AT00) serial # (SB0241HGGAWN9E)<br><br>Sector 0 is first sector with printable text<br>============= Start text =============<br>00000/000/01 000000000000<br>============= End text Sector 0 =============<br>1 <new line> character inserted for readability<br><br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>  146301488 00     71102523168 14     146301488 20 ( )<br>  292602976 2F (/)    993890325 30 (0)    358021591 31 (1)<br>  285788447 32 (2)    254136647 33 (3)    248114389 34 (4)<br>  238370729 35 (5)    220867833 36 (6)    211263767 37 (7)<br>  211263764 38 (8)    196915244 39 (9)<br>Totals for non-ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br><br>74906361856 bytes, 146301488 sectors, 14 distinct values seen<br>146301488 sectors have printable text |
| Tool Settings: | rounds = x1 |
| Log Highlights: | Size after tool runs: 131301488 from total of 156301488 (with 25000000 hidden)<br>Analysis of tool result --<br><br>Sector 131301488 is first sector with printable text<br>============= Start text =============<br>08173/035/39 000131301488<br>============= End text Sector 131301488 =============<br>1 <new line> character inserted for readability<br><br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br> 67251361856 00    12150000000 14     25000000 20 ( )<br>   50000000 2F (/)   144914896 30 (0)    71835647 31 (1)<br>   43889901 32 (2)    47061285 33 (3)    47968552 34 (4)<br>   43681897 35 (5)    33810839 36 (6)    30896747 37 (7)<br>   43759142 38 (8)    42181094 39 (9)<br>Totals for non-ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br> 67226361856 00 |

| Test Case FMP-03-DCO-HPA-2 Disk Jockey Pro Forensic Version 1.20 | | |
|---|---|---|
| | 80026361856 bytes, 156301488 sectors, 14 distinct values seen<br>25000000 sectors have printable text | |
| Results: | **Assertion & Expected Result** | **Actual Result** |
| | FMP-CA-01 Visible sectors overwritten | as expected |
| | FMP-AO-01 Hidden sectors overwritten | DCO+HPA not overwritten |
| | FMP-AO-02 Hidden area final state is | in place |
| Analysis: | Expected results not achieved | |

## 4.2.6  FMP–03–DCO–2

| Test Case FMP-03-DCO-2 Disk Jockey Pro Forensic Version 1.20 | |
|---|---|
| Case Summary: | FMP-03. Overwrite hidden sectors using WRITE commands. |
| Assertions: | FMP-CA-01 All visible sectors shall be overwritten with the specified benign data.<br>FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data.<br>FMP-AO--02 A hidden area may optionally be removed from the storage device. |
| Tester Name: | csr |
| Analysis host: | frank |
| Test host: | none |
| Test date: | Thu Oct 29 09:01:53 2009 |
| Test drive: | 1D-LAP |
| Source Setup: | Size with DCO: 224441648 114.91 GB (10000000 sectors in DCO)<br>Initial setup size: 224441648 from total of 234441648 (with 10000000 hidden)<br>IDE disk: Model (Hitachi HTS542512K9SA00) serial # (080914BB6200WBKPDL2G)<br><br>Sector 0 is first sector with printable text<br>============= Start text =============<br>00000/000/01 000000000000<br>============= End text Sector 0 =============<br>1 <new line> character inserted for readability<br><br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>  224441648 00     109078640928 1D       224441648 20 ( )<br>  448883296 2F (/)   1412016107 30 (0)    648943731 31 (1)<br>  464424111 32 (2)    386665415 33 (3)    366881143 34 (4)<br>  361115515 35 (5)    335339466 36 (6)    320942106 37 (7)<br>  320928507 38 (8)    320460155 39 (9)<br>Totals for non--ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br><br>114914123776 bytes, 224441648 sectors, 14 distinct values seen<br>224441648 sectors have printable text |
| Tool Settings: | rounds = x1 |
| Log Highlights: | Size after tool runs: 224441648 from total of 234441648 (with 10000000 hidden)<br>Analysis of tool result --<br><br>Sector 224441648 is first sector with printable text<br>============= Start text =============<br>13970/215/54 000224441648<br>============= End text Sector 224441648 =============<br>1 <new line> character inserted for readability<br><br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>114924123776 00     4860000000 1D      10000000 20 ( )<br>   20000000 2F (/)   49069416 30 (0)   29395570 31 (1)<br>   33193387 32 (2)   20376376 33 (3)   24834191 34 (4)<br>   14959713 35 (5)   12311991 36 (6)   11824119 37 (7)<br>   11837150 38 (8)   12198087 39 (9)<br>Totals for non-ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>114914123776 00 |

| Test Case FMP-03-DCO-2 Disk Jockey Pro Forensic Version 1.20 | | | |
|---|---|---|---|
| | 120034123776 bytes, 234441648 sectors, 14 distinct values seen<br>10000000 sectors have printable text | | |
| Results: | **Assertion & Expected Result** | **Actual Result** | |
| | FMP-CA-01 Visible sectors overwritten | as expected | |
| | FMP-AO-01 Hidden sectors overwritten | DCO not overwritten | |
| | FMP-AO-02 Hidden area final state is | in place | |
| Analysis: | Expected results not achieved | | |

## 4.2.7 FMP–03–HPA–2

| Test Case FMP-03-HPA-2 Disk Jockey Pro Forensic Version 1.20 | |
|---|---|
| Case Summary: | FMP-03. Overwrite hidden sectors using WRITE commands. |
| Assertions: | FMP-CA-01 All visible sectors shall be overwritten with the specified benign data.<br>FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data.<br>FMP-AO-02 A hidden area may optionally be removed from the storage device. |
| Tester Name: | csr |
| Analysis host: | frank |
| Test host: | none |
| Test date: | Wed Oct 28 08:38:30 2009 |
| Test drive: | 53-IDE |
| Source Setup: | Size with HPA: 297581808 152.36 GB (15000000 sectors in HPA)<br>Initial setup size: 297581808 from total of 312581808 (with 15000000 hidden)<br>IDE disk: Model (WDC WD1600JB-00GVC0) serial # (WD-WMAL94865344)<br><br>Sector 0 is first sector with printable text<br>============= Start text =============<br>00000/000/01 000000000000SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS<br>============= End text Sector 0 =============<br>9 <new line> characters inserted for readability<br><br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>  312581808 00      312581808 20 ( )   625163616 2F (/)<br> 1850492169 30 (0)  906528227 31 (1)  696435016 32 (2)<br>  541016511 33 (3)  522787395 34 (4)  514450557 35 (5)<br>  478352540 36 (6)  458495114 37 (7)  458481159 38 (8)<br>  449761088 39 (9) 151914758688 53 (S)<br>Totals for non-ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br><br>160041885696 bytes, 312581808 sectors, 14 distinct values seen<br>312581808 sectors have printable text |
| Tool Settings: | rounds = DoD x7 |
| Log Highlights: | Size after tool runs: 312581808 from total of 312581808 (with 0 hidden)<br>Analysis of tool result --<br>Totals for all sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>160041885696 F6<br>Totals for non-ASCII sectors<br>summary format: <count> <hex value> <(actual character if printable)> ...<br>160041885696 F6<br><br>160041885696 bytes, 312581808 sectors, 1 distinct values seen<br>No sectors have printable text |

| Test Case FMP-03-HPA-2 Disk Jockey Pro Forensic Version 1.20 | | |
|---|---|---|
| Results: | **Assertion & Expected Result** | **Actual Result** |
| | FMP-CA-01 Visible sectors overwritten | as expected |
| | FMP-AO-01 Hidden sectors overwritten | as expected |
| | FMP-AO-02 Hidden area final state is | removed |
| Analysis: | Expected results achieved | |

## About the National Institute of Justice

A component of the Office of Justice Programs, NIJ is the research, development and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development and evaluation to enhance the administration of justice and public safety. NIJ's principal authorities are derived from the Omnibus Crime Control and Safe Streets Act of 1968, as amended (see 42 U.S.C. §§ 3721–3723).

The NIJ Director is appointed by the President and confirmed by the Senate. The Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the U.S. Department of Justice, and the needs of the field. The Institute actively solicits the views of criminal justice and other professionals and researchers to inform its search for the knowledge and tools to guide policy and practice.

### Strategic Goals

NIJ has seven strategic goals grouped into three categories:

### Creating relevant knowledge and tools

1. Partner with state and local practitioners and policymakers to identify social science research and technology needs.
2. Create scientific, relevant, and reliable knowledge—with a particular emphasis on terrorism, violent crime, drugs and crime, cost-effectiveness, and community-based efforts—to enhance the administration of justice and public safety.
3. Develop affordable and effective tools and technologies to enhance the administration of justice and public safety.

### Dissemination

4. Disseminate relevant knowledge and information to practitioners and policymakers in an understandable, timely and concise manner.
5. Act as an honest broker to identify the information, tools and technologies that respond to the needs of stakeholders.

### Agency management

6. Practice fairness and openness in the research and development process.
7. Ensure professionalism, excellence, accountability, cost-effectiveness and integrity in the management and conduct of NIJ activities and programs.

### Program Areas

In addressing these strategic challenges, the Institute is involved in the following program areas: crime control and prevention, including policing; drugs and crime; justice systems and offender behavior, including corrections; violence and victimization; communications and information technologies; critical incident response; investigative and forensic sciences, including DNA; less-than-lethal technologies; officer protection; education and training technologies; testing and standards; technology assistance to law enforcement and corrections agencies; field testing of promising programs; and international crime control.

In addition to sponsoring research and development and technology assistance, NIJ evaluates programs, policies, and technologies. NIJ communicates its research and evaluation findings through conferences and print and electronic media.

To find out more about the National Institute of Justice, please visit:

*http://www.ojp.usdoj.gov/nij*

or contact:

National Criminal Justice
 Reference Service
P.O. Box 6000
Rockville, MD 20849–6000
800–851–3420
*http://www.ncjrs.gov*