JAN. 07

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special REPORT

Test Results for Hardware Write Block Device: Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface)

www.ojp.usdoj.gov/nij

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Alberto R. Gonzales
Attorney General

Regina B. Schofield
Assistant Attorney General

David W. Hagy
Deputy Assistant Attorney General, Office of Justice Programs and Principal Deputy Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.ojp.usdoj.gov/nij

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

NIJ

JAN. 07

Test Results for Hardware Write Block Device: Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface)

NCJ 216983

NIJ

David W. Hagy

Deputy Assistant Attorney General, Office of Justice Programs and Principal Deputy Director, National Institute of Justice

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Office of Law Enforcement Standards of the National Institute of Standards and Technology under Interagency Agreement 2003–IJ–R–029.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Test Results for Hardware Write Block Device: Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface)

January 2007

NIST
National Institute of Standards and Technology
Technology Administration, 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, and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, Internal Revenue Service Criminal Investigation's Electronic Crimes Program, and the U.S. Department of Homeland Security's Bureau of U.S. Immigration and Customs Enforcement and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable 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. This approach to testing computer forensics 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 the Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface) write blocker against *Hardware Write Blocker (HWB) Assertions and Test Plan Version 1.0*, available on the CFTT Web site (http://www.cftt.nist.gov/HWB-ATP-19.pdf).This specification identifies the following top-level tool requirements::

- A hardware write block (HWB) device shall not transmit a command to a protected storage device that modifies the data on the storage device.
- An HWB device shall return the data requested by a read operation.
- An HWB device shall return without modification any access-significant information requested from the drive.
- Any error condition reported by the storage device to the HWB device shall be reported to the host.

Test results from other software packages and the CFTT tool methodology can be found on NIJ's computer forensics tool testing Web page, http://www.ojp.usdoj.gov/nij/topics/ecrime/cftt.htm

Test Results for Hardware Write Block Devices

Device Tested:	Tableau Forensic IDE Pocket Bridge T14 by Tableau[1]
Model:	T14
Serial No:	000ECC01000E232D
Firmware:	January 31, 2005 16:30:32
Host to Blocker Interface:	FireWire
Blocker to Drive Interface:	IDE
Supplier:	Tableau, LLC
Address:	N8 W22195 Johnson Drive, Suite 100 Waukesha, WI 53186 http://www.tableau.com/

1 Results Summary by Requirements

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device.
For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation.
For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive.
For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host.
For all test cases run, the HWB device always returned error codes from the protected drive without modification.

2 Test Case Selection

Because a protocol analyzer was not available for the interface between the blocker and the protected drive, the following test cases were appropriate: HWB-02, HWB-04, HWB-05, HWB-07, HWB-08 and HWB-09.

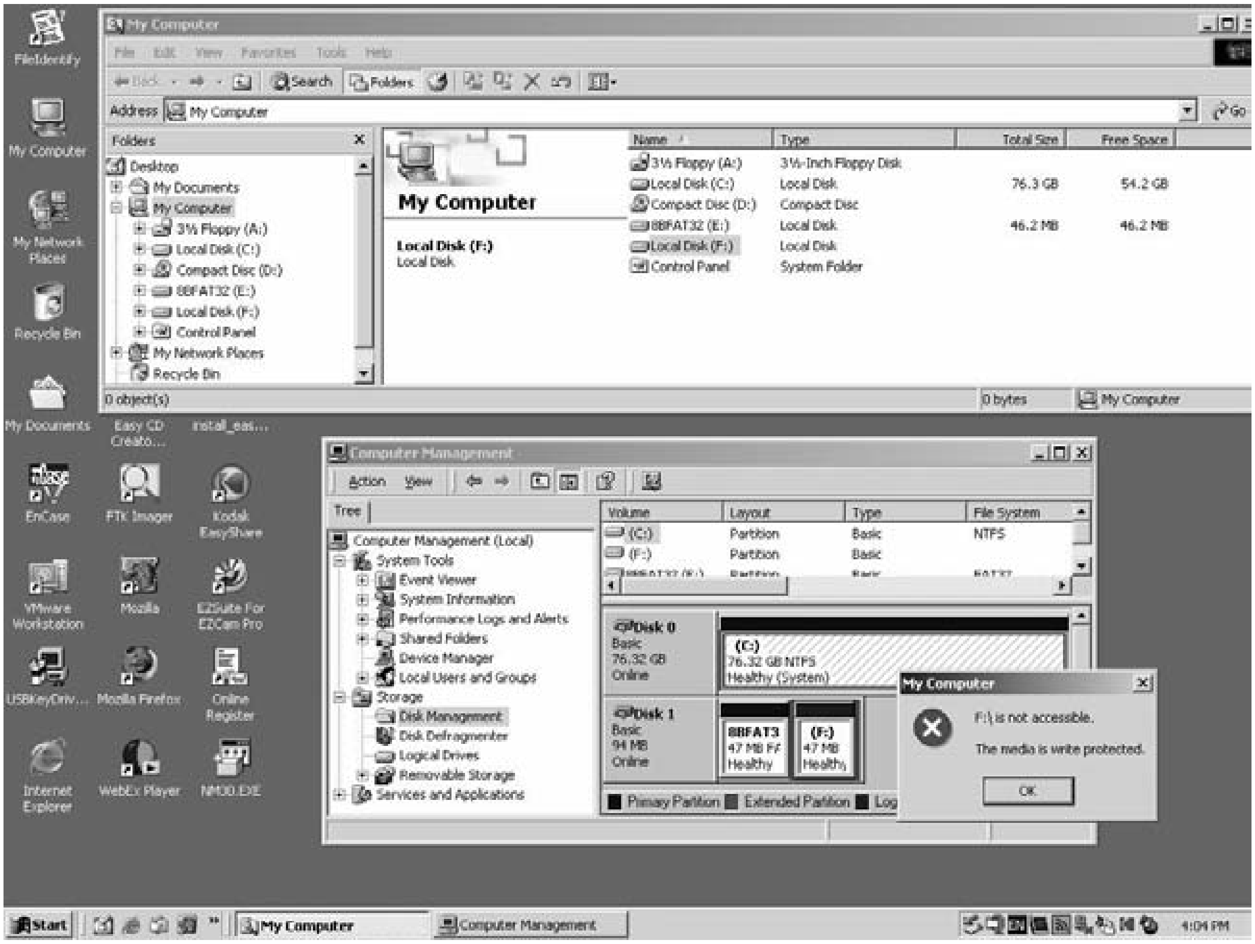
[1] Tableau produces this write block device for resale under various partner labels. See http://www.tableau.com for information on resellers.

For test case HWB-04, two variations were selected: file (attempt to use operating system commands to create and delete file system objects, such as files and directories, from a protected drive) and image (use an imaging tool to attempt to write to a protected drive).

For test case HWB-07, one variation was selected: ix (use a stand-alone imaging tool [IXimager] to read from a protected drive).

3 Observations

For test case HWB-04-file, the protected drive was set up with two partitions, FAT32 and NTFS. The NTFS partition was visible but not accessible to Windows 2000 (see Figure 1). It was therefore not possible to attempt to create or delete files and directories from the NTFS partition. However, the NTFS partition was accessible from Windows XP.



Name	Type	Total Size	Free Space
3½ Floppy (A:)	3½-Inch Floppy Disk		
Local Disk (C:)	Local Disk	76.3 GB	54.2 GB
Compact Disc (D:)	Compact Disc		
8BFAT32 (E:)	Local Disk	46.2 MB	46.2 MB
Local Disk (F:)	Local Disk		
Control Panel	System Folder		

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
(F:)	Partition	Basic	

Disk 0
Basic
76.32 GB
Online

(C:)
76.32 GB NTFS
Healthy (System)

Disk 1
Basic
94 MB
Online

8BFAT3
47 MB F/
Healthy

(F:)
47 MB
Healthy

My Computer

F:\ is not accessible.

The media is write protected.

OK

Figure 1. Screen Display From Test Case HWB-04-file.

4 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the hardware (test computers and hard drives) available for testing.

4.1 Test Computers

Two test computers were used: **Nancy** and **MrsPeel**. **Nancy** and **MrsPeel** have the following configuration:

FIC IC–VL67 (865G; S478; 800MHz)
Phoenix—Award BIOS version v6.00PG
Intel Pentium® 4 CPU
Plextor DVDR PX–716A, ATAPI CD/DVD–ROM drive
1.44MB floppy drive
Three IEEE 1394 ports
Four USB ports

4.2 Protocol Analyzer

A Data Transit bus protocol analyzer (Bus Doctor Rx) was used to monitor and record commands sent from the host to the write blocker. Two identical protocol analyzers were available for monitoring commands.

One of two Dell laptop computers (either Chip or Dale) was connected to each protocol analyzer to record commands observed by the protocol analyzer.

4.3 Hard Disk Drives

The hard disk drive used in testing is described below.

```
Drive label: 8B
Partition table Drive /dev/sda
00011/254/63 (max cyl/hd values)
00012/255/63 (number of cyl/hd)
201600 total number of sectors
Model (0EB-00CSF0      ) serial # (WD-WTAAV4044563)
 N   Start LBA Length    Start C/H/S End C/H/S   boot Partition type
 1 P 000000063 000096327 0000/001/01 0005/254/63      0B Fat32
 2 X 000096390 000096390 0006/000/01 0011/254/63      05 extended
 3 S 000000063 000096327 0006/001/01 0011/254/63      07 NTFS
 4 S 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 5 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 6 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
```

P primary partition (1-4)
S secondary (sub) partition
X primary extended partition (1-4)
x secondary extended partition

4.4 Support Software

The software in the following table was used to send commands to the protected drive. One widely used imaging tool, IXimager, was used to generate disk activity (reads and writes) consistent with a realistic scenario of an accidental modification of an unprotected hard drive during a forensic examination. This does not imply an endorsement of the imaging tool.

Program	Description
sendSCSI	A tool to send SCSI commands wrapped in the USB or IEEE 1394 (firewire) protocols to a drive.
FS–TST	Software from the FS–TST tools was used to generate errors from the hard drive by trying to read beyond the end of the drive. The FS–TST software was also used to setup the hard drives and print partition tables and drive size.
IXimager	An imaging tool (ILook IXimager Version 1.0, August 25, 2004) for test case 03-img.

5 Test Results

The main item of interest for interpreting the test results is determining the conformance of the device with the test assertions. This section lists each test assertion and identifies the information in the log files relevant to conformance with that assertion. Conformance with each assertion tested by a given test case is evaluated by examining the Blocker Input and Blocker Output boxes of the test report summary.

5.1 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 device tested.
Case Summary	Test case summary from *Hardware Write Blocker (HWB) Assertions and Test Plan Version 1.0.*
Assertions Tested	The test assertions tested by the test case from *Hardware Write Blocker (HWB) Assertions and Test Plan Version 1.0.*
Tester Name	Name or initials of person executing test procedure.
Test Date	Time and date that test was started.
Test Configuration	Identification of the following: 1. Label of the protected hard drive. 2. Interface between host and blocker. 3. Interface between blocker and protected drive. 4. Protocol analyzers monitoring each interface. 5. Laptop attached to each protocol analyzer. 6. Execution environment for tool sending commands from the host.
Hard Drives Used	Description of the protected hard drive.
Blocker Input	A list of commands sent from the host to the blocker. For test cases HWB-02 and HWB-07, a list of the commands sent is provided.

Heading	Description
	For test cases HWB-02 and HWB-04, an SHA1 value for the entire drive is provided for reference. For test case HWB-05, a string of known data from a given location is provided for reference.
Blocker Output	For test cases HWB-02 and HWB-04, an SHA1 value computed after commands are sent to the protected drive is given for comparison to the reference SHA1 value. For test case HWB-05, a string read from a given location is provided for comparison to known data. For test case HWB-08, the number of sectors determined for the protected drive and the partition table are provided. For test case HWB-09, any error return obtained by trying to access a nonexistent sector of the drive is provided.
Results:	Expected and actual results for each assertion tested.
Analysis:	Whether or not the expected results were achieved.

5.2 Test Details

Test Case HWB-02 Variation hwb-02 Tableau Forensic IDE Pocket Bridge T14	
Case Summary:	HWB-02 Identify modifying commands blocked by the HWB.
Assertions Tested:	HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.
Tester Name:	JRL
Test Date:	run start Sun Sep 11 15:58:06 2005 run finish Sun Sep 11 16:02:57 2005
Test Configuration:	HOST: MrsPeel HostToBlocker Monitor: Dale HostToBlocker PA: AA00111 HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: IDE Run Environment: Knoppix
Drives:	Protected drive: 8B 8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)
Blocker Input:	SHA of 8B is 92577F7B0A265FC883BBDFFBFB8E4E58E959B4D1 - Commands Sent to Blocker 210 SBP2 OP=READ(10) 2 SBP2 OP=WRITE(10) 1 SBP2 OP=WRITE(12) 1 SBP2 OP=WRITE BUFFER

<table>
<tr><th colspan="2">Test Case HWB-02 Variation hwb-02 Tableau Forensic IDE Pocket Bridge T14</th></tr>
<tr><td></td><td>1 SBP2 OP=WRITE LONG
1 SBP2 OP=WRITE SAME
2 SBP2 OP=WRITE/VERIFY
1 SBP2 OP=XDWRITE(10)
1 SBP2 OP=XDWRITEREAD(10)
1 SBP2 OP=XPWRITE(10)</td></tr>
<tr><td>Blocker Output:</td><td>CMD: ../../../diskhash.csh HWB-02 MrsPeel JRL /dev/sda 8B -after -new_log
92577F7B0A265FC883BBDFFBFB8E4E58E959B4D1 -</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-01 Modifying commands blocked</td><td>Modifying commands blocked</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

Test Case HWB-04 Variation HWB-04-file Tableau Forensic IDE Pocket Bridge T14	
Case Summary:	HWB-04 Attempt to modify a protected drive with forensic tools.
Assertions Tested:	HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.
Tester Name:	JRL
Test Date:	run start Sun Sep 11 14:56:19 2005 run finish Sun Sep 11 15:13:19 2005
Test Configuration:	HOST: Nancy HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: IDE Run Environment: W2K
Drives:	Protected drive: 8B 8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)
Blocker Input:	SHA of 8B is 92577F7B0A265FC883BBDFFBFB8E4E58E959B4D1 - Commands are sent to blocker by OS operations: @echo off REM %1 is the directory where alpha, beta & gamma are created REM Redirect the output to a logfile REM hwb-mod . X: > dir-setup.txt echo "mod: %1" mkdir %1\delta rmdir %1\gamma copy %1\beta\zeta.txt %1\alpha copy %1\beta\omega.txt %1\delta del %1\beta\zeta.txt dir %1 /b /s

<table>
<tr><th colspan="2">Test Case HWB-04 Variation HWB-04-file Tableau Forensic IDE Pocket Bridge T14</th></tr>
<tr><td>Blocker Output:</td><td>Results for FAT partition:
"mod: E:"
        0 file(s) copied.
        0 file(s) copied.
E:\beta\zeta.txt
E:\alpha
E:\beta
E:\gamma
E:\beta\zeta.txt
E:\beta\omega.txt
Results for NTFS partition:
"mod: F:"
The media is write protected.
The media is write protected.
Final SHA1 value:
CMD: ../../../diskhash.csh HWB-04-file MrsPeel JRL /dev/sda 8B -after -new_log
92577F7B0A265FC883BBDFFBFB8E4E58E959B4D1 -</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-01 Modifying commands blocked</td><td>Modifying commands blocked</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

<table>
<tr><th colspan="2">Test Case HWB-04 Variation HWB-04-img Tableau Forensic IDE Pocket Bridge T14</th></tr>
<tr><td>Case Summary:</td><td>HWB-04 Attempt to modify a protected drive with forensic tools.</td></tr>
<tr><td>Assertions Tested:</td><td>HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.</td></tr>
<tr><td>Tester Name:</td><td>JRL</td></tr>
<tr><td>Test Date:</td><td>run start Sun Sep 11 16:09:16 2005
run finish Sun Sep 11 16:24:32 2005</td></tr>
<tr><td>Test Configuration:</td><td>HOST: MrsPeel
HostToBlocker Monitor: none
HostToBlocker PA: none
HostToBlocker Interface: FW
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: IDE
Run Environment: IXimager</td></tr>
<tr><td>Drives:</td><td>Protected drive: 8B
8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)</td></tr>
<tr><td>Blocker Input:</td><td>SHA of 8B is 92577F7B0A265FC883BBDFFBFB8E4E58E959B4D1 -
Commands are sent to blocker by imaging tool</td></tr>
<tr><td>Blocker Output:</td><td>CMD: ../../../diskhash.csh HWB-04-img MrsPeel JRL /dev/sda 8B -after
92577F7B0A265FC883BBDFFBFB8E4E58E959B4D1 -</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-01 Modifying commands blocked</td><td>Modifying commands blocked</td></tr></table></td></tr>
</table>

Test Case HWB-04 Variation HWB-04-img Tableau Forensic IDE Pocket Bridge T14	
Analysis:	Expected results achieved

<table>
<tr><th colspan="2">Test Case HWB-05 Variation hwb-05 Tableau Forensic IDE Pocket Bridge T14</th></tr>
<tr><td>Case Summary:</td><td>HWB-05 Identify read commands allowed by the HWB.</td></tr>
<tr><td>Assertions Tested:</td><td>HWB-AM-02 If the host sends a read category operation to the HWB and no error is returned from the protected storage device to the HWB, then the data addressed by the original read operation are returned to the host.</td></tr>
<tr><td>Tester Name:</td><td>JRL</td></tr>
<tr><td>Test Date:</td><td>run start Sun Sep 11 15:47:26 2005
run finish Sun Sep 11 15:57:24 2005</td></tr>
<tr><td>Test Configuration:</td><td>HOST: MrsPeel
HostToBlocker Monitor: Dale
HostToBlocker PA: AA00111
HostToBlocker Interface: FW
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: IDE
Run Environment: Knoppix</td></tr>
<tr><td>Drives:</td><td>Protected drive: 8B
8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)</td></tr>
<tr><td>Blocker Input:</td><td>Commands Sent to Blocker
Read sector 32767 for the string: 00002/010/08 0000000327670</td></tr>
<tr><td>Blocker Output:</td><td>00002/010/08 0000000327670</td></tr>
<tr><td>Results:</td><td><table><tr><td>Assertion & Expected Result</td><td>Actual Result</td></tr><tr><td>AM-02 Read commands allowed</td><td>Read commands allowed</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

Test Case HWB-07 Variation HWB-07-ix Tableau Forensic IDE Pocket Bridge T14	
Case Summary:	HWB-07 Read a protected drive with forensic tools.
Assertions Tested:	HWB-AM-02 If the host sends a read category operation to the HWB and no error is returned from the protected storage device to the HWB, then the data addressed by the original read operation are returned to the host. HWB-AM-03 If the host sends an information category operation to the HWB and if there is no error on the protected storage device, then any returned access-significant information is returned to the host without modification.
Tester Name:	JRL
Test Date:	run start Sun Sep 11 16:25:48 2005 run finish Sun Sep 11 16:35:51 2005
Test Configuration:	HOST: MrsPeel HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none

<table>
<tr><th colspan="2"><b>Test Case HWB-07 Variation HWB-07-ix Tableau Forensic IDE Pocket Bridge T14</b></th></tr>
<tr><td></td><td>BlockerToDrive Interface: IDE
Run Environment: IXimager</td></tr>
<tr><td>Drives:</td><td>Protected drive: 8B
8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)</td></tr>
<tr><td>Blocker Input:</td><td>Commands Sent to Blocker
Commands are sent to blocker by imaging tool</td></tr>
<tr><td>Blocker Output:</td><td>Sep 11 16:29:18 iimager: User entered the Image Device Menu
Sep 11 16:29:25 iimager: User entered the Image Target Menu
Sep 11 16:29:37 iimager: User selected ILook Default Image Format
Sep 11 16:30:08 iimager: Image is being stored to /dev/sdb1
Sep 11 16:30:08 iimager: Beginning Image operation
Sep 11 16:30:08 iimager: Opened output file '/ILookImager/ILook.004/image001.asb'
Sep 11 16:30:08 iimager: Image is being stored to /ILook.004/image001.asb
Sep 11 16:30:08 iimager: Image is being stored to /dev/sdb1
Sep 11 16:30:08 iimager: Image is being stored to /ILook.004/image001.asb
Sep 11 16:30:08 iimager: Beginning Image operation for 103219200 bytes
Sep 11 16:30:16 iimager: Image Complete
Sep 11 16:30:16 iimager: Image was completed successfully.
Sep 11 16:30:16 iimager: Image Speed   : 12.90 MB/sec
Sep 11 16:30:27 iimager: User exited the Image Target Menu
Sep 11 16:30:27 iimager: User exited the Image Device Menu</td></tr>
<tr><td>Results:</td><td><table>
<tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr>
<tr><td>AM-02 Read commands allowed</td><td>Read commands allowed</td></tr>
<tr><td>AM-03 Access Significant Information unaltered</td><td>Access Significant Information unaltered</td></tr>
</table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

Test Case HWB-08 Variation hwb-08 Tableau Forensic IDE Pocket Bridge T14	
Case Summary:	HWB-08 Identify access significant information unmodified by the HWB.
Assertions Tested:	HWB-AM-03 If the host sends an information category operation to the HWB and if there is no error on the protected storage device, then any returned access-significant information is returned to the host without modification.
Tester Name:	JRL
Test Date:	run start Sun Sep 11 15:34:30 2005 run finish Sun Sep 11 15:36:20 2005
Test Configuration:	HOST: MrsPeel HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: FW BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: IDE Run Environment: Knoppix

<table>
<tr><th colspan="2">Test Case HWB-08 Variation hwb-08 Tableau Forensic IDE Pocket Bridge T14</th></tr>
<tr><td></td><td></td></tr>
<tr><td>Drives:</td><td>Protected drive: 8B
8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)</td></tr>
<tr><td>Blocker Output:</td><td>cmd: ../../../partab HWB-08 MrsPeel JRL /dev/sda 8B -all
201600 total number of sectors</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-03 Access Significant Information unaltered</td><td>Access Significant Information unaltered</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

<table>
<tr><th colspan="2">Test Case HWB-09 Variation hwb-09 Tableau Forensic IDE Pocket Bridge T14</th></tr>
<tr><td>Case Summary:</td><td>HWB-09 Determine if an error on the protected drive is returned to the host.</td></tr>
<tr><td>Assertions Tested:</td><td>HWB-AM-04 If the host sends an operation to the HWB and if the operation results in an unresolved error on the protected storage device, then the HWB shall return an error status code to the host.</td></tr>
<tr><td>Tester Name:</td><td>JRL</td></tr>
<tr><td>Test Date:</td><td>run start Sun Sep 11 15:36:51 2005
run finish Sun Sep 11 15:38:42 2005</td></tr>
<tr><td>Test Configuration:</td><td>HOST: MrsPeel
HostToBlocker Monitor: none
HostToBlocker PA: none
HostToBlocker Interface: FW
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: IDE
Run Environment: Knoppix</td></tr>
<tr><td>Drives:</td><td>Protected drive: 8B
8B is a WDC WD200EB-00CSF0 configured to report 201600 sectors (103 MB)</td></tr>
<tr><td>Blocker Output:</td><td>00011/254/63 (max cyl/hd values)
00012/255/63 (number of cyl/hd)
201600 total number of sectors
cmd: ../../../diskchg HWB-09 MrsPeel JRL /dev/sda -read 301600 0 32
Disk addr lba 301600 C/H/S 18/197/20 offset 0
Disk read error 0xFFFFFFFF at sector 18/197/20</td></tr>
<tr><td>Results:</td><td><table><tr><th>Assertion & Expected Result</th><th>Actual Result</th></tr><tr><td>AM-04 Error code returned</td><td>Error code returned</td></tr></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

About the National Institute of Justice

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
e-mail: *askncjrs@ncjrs.org*