JUNE 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 T5 Forensic IDE Bridge (USB Interface)

www.ojp.usdoj.gov/nij

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

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 Acting 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
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

NIJ

JUNE 07

Test Results for Hardware Write Block Device: Tableau T5 Forensic IDE Bridge (USB Interface)

NCJ 218380

NIJ

David W. Hagy

Deputy Assistant Attorney General, Office of Justice Programs
and Acting 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 Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

Test Results for Hardware Write Block Device: Tableau T5 Forensic IDE Bridge (USB Interface)

June 2007

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

Contents

Introduction... 3

Test Results for Hardware Write Block Devices 4

1 Results Summary by Requirements 4
2 Test Case Selection 4
3 Testing Environment 5
3.1 Test Computers 5
3.2 Protocol Analyzer 5
3.3 Hard Disk Drives 6
3.4 Support Software 7
4 Test Results 7
4.1 Test Results Report Key 7
4.2 Test Details 9
4.2.1 HWB-01 9
4.2.2 HWB-03-file 11
4.2.3 HWB-03-img 12
4.2.4 HWB-05 13
4.2.5 HWB-06 14
4.2.6 HWB-08 15
4.2.7 HWB-09 16

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, the Internal Revenue Service Criminal Investigation Division'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 project 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 for 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 the **Tableau T5 Forensic IDE Bridge (USB Interface)** write blocker against the *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 shall return the data requested by a read operation.
- An HWB shall return without modification any access-significant information requested from the drive.
- Any error condition reported by the storage device to the HWB 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 T5 Forensic IDE Bridge*
Model:	T5
Serial No:	U004B009296,000ecc01000540e5
Firmware:	Oct 4 2004 15:28:51
Host to Blocker Interface:	USB
Blocker to Drive Interface:	ATA
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 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 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 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 device always returned error codes from the protected drive without modification.

2 Test Case Selection

Since a protocol analyzer was available for the interface between the blocker and the protected drive, the following test cases were appropriate: HWB–01, HWB–03, HWB–05, HWB–06, HWB–08, and HWB–09.

*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–03, two variations were selected: file (attempt to use operating system commands to create and delete files and directories from a protected drive) and image (use an imaging tool to attempt to write to a protected drive).

3 Testing Environment

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

3.1 Test Computers

Two test computers were used: **DixonHill** and **Charlie**.

Charlie has the following configuration:

Asus P4P8T Intel® (865G/ICH 5 chipsets, FSB 800/533/400MHz) Motherboard
AMIBIOS© American Megatrends Asus P4P8T–SP ACPI BIOS revision 1003
Intel Pentium® 4 CPU, 3GHZ
1 GB RAM
Plextor DVDR PX–716A, ATAPI CD/DVD-ROM drive
WDC WD800JB–00JJC0, 80 GB ATA disk drive
Five IEEE 1394 ports
Six USB ports
Memory Card reader

DixonHill has the following configuration:

Intel® D865PERL Motherboard
Intel Pentium® 4 CPU 2.4GHz
BE7X 1.08.00.048 BIOS
FE7X 1.05.00.063 Firmware
2048 MB RAM
ABIT R9200SE–T AGP graphics adapter
LSI MegaRAID SATA 150–4D SER523 REV B2 RAID controller
Lite-On DVDRW SHOW–1234 Drive
Floppy Drive
4 USB ports
1 IEEE 1394 FireWire port
4 slots for SATA RAID drives

3.2 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.

3.3 Hard Disk Drives

The hard disk drives that were used were selected from the ATA drives listed below. These hard drives were mounted in removable storage modules. The drives were set up in a variety of ways with the common partition types (FAT and NTFS) represented. The setup of each drive is documented 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
Non-IDE disk
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
```

```
Drive label: A8
Partition table Drive /dev/sda
00011/254/63 (max cyl/hd values)
00012/255/63 (number of cyl/hd)
201600 total number of sectors
Non-IDE disk
Model (0BB-00AUA1      ) serial # (WD-WMA6Y3401179)
 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
```

```
Drive label: BE
Partition table Drive /dev/sda
24320/254/63 (max cyl/hd values)
24321/255/63 (number of cyl/hd)
390721968 total number of sectors
Non-IDE disk
Model (00JB-00KFA0     ) serial # (     WD-WMAMR10220)
 N   Start LBA Length    Start C/H/S End C/H/S   boot Partition type
 1 P 000000063 039070017 0000/001/01 1023/254/63      0C Fat32X
 2 X 039070080 351646785 1023/000/01 1023/254/63      0F extended
 3 S 000000063 307194867 1023/001/01 1023/254/63      07 NTFS
 4 x 307194930 000016065 1023/000/01 1023/254/63      05 extended
 5 S 000000063 000016002 1023/001/01 1023/254/63      01 Fat12
 6 x 307210995 004096575 1023/000/01 1023/254/63      05 extended
 7 S 000000063 004096512 1023/001/01 1023/254/63      06 Fat16
 8 S 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
 9 P 000000000 000000000 0000/000/00 0000/000/00      00 empty entry
10 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

3.4 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 04-img.

4 Test Results

The main item of interest for interpreting the test results is determining the conformance of the device with the test assertions. 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.

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, model, and interface 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 applicable to the test case, selected 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 and completed.
Test Configuration	Identification of the following: 1. Host computer for executing the test case. 2. Laptop attached to each protocol analyzer. 3. Protocol analyzers monitoring each interface.

Heading	Description
	4. Interface between host and blocker. 5. Interface between blocker and protected drive. 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 case HWB–01, a list of each command code observed on the bus between the blocker and the protected drive and a count of the number of times the command was observed is provided. For test cases HWB–03 and HWB–06, a list of each command sent and the number of times the command was sent. For test case HWB–05, a string of known data from a given location is provided for reference.
Blocker Output	A list of commands observed by the protocol analyzer on the bus from the blocker to the protected drive. For test case HWB–01, a list of each command code observed on the bus between the blocker and the protected drive and a count of the number of times the command was observed is provided. Also, a count of the number of unique commands sent (from the Blocker Input box) and a count of the number of unique commands observed on the bus between the blocker and the protected drive. For test cases HWB–03 and HWB–06, a list of each command sent and the number of times the command was sent. 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.

4.2 *Test Details*

4.2.1 HWB–01

Test Case HWB-01 Variation hwb-01 Tableau T5 Forensic IDE Bridge (USB)	
Case Summary:	HWB-01 Identify commands blocked by the HWB.
Assertions Tested:	HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device. HWB-AM-05 The action that a HWB device takes for any commands not assigned to the modifying, read or information categories is defined by the vendor.
Tester Name:	Kbr
Test Date:	run start Wed Sep 20 17:10:55 2006 run finish Wed Sep 20 17:14:19 2006
Test Configuration:	HOST: dixon hill HostToBlocker Monitor: chip HostToBlocker PA: aa00155 HostToBlocker Interface: usb BlockerToDrive Monitor: dale BlockerToDrive PA: aa00111 BlockerToDrive Interface: ide Run Environment: helix1.5
Drives:	Protected drive: BE BE is a WDC WD2000JB-00KFA0 with 390721968 sectors (200 GB)
Blocker Input:	Commands Sent to Blocker

Count	Commands
1	BLANK
1	CHG
1	CLOS
1	COMPARE
1	COPY
1	COPY/VERIFY
1	ERASE
1	ERASE(10)
1	FORMAT
3	GET
1	INQUIRY
1	LK/UNLK
1	LOAD/UNLOAD
2	LOG
1	MECH
1	MEDIUM
4	MODE
1	PAUSE/RESUME
2	PERSISTENT
5	PLAY
2	PLY
1	PRE-FETCH
1	PREVENT/ALLOW
7	RD
13	READ
548	READ(10)
1	READ(12)
1	REASSIGN
1	RECEIVE
1	RECIEVE(6)
1	RECOVER
1	RELEASE(10)
1	RELEASE(6)
1	REPAIR
5	REPORT
1	REQ
228	REQUEST_SENSE
1	RESERVE(10)
1	RESERVE(6)
1	REZERO
65	Reserved
1	SCAN
1	SEEK(10)

Test Case HWB-01 Variation hwb-01 Tableau T5 Forensic IDE Bridge (USB)

1	SEEK(6)
9	SEND
1	SEND(6)
4	SET
1	SND
1	SPACE
6	SRCH
1	START/STOP
1	STOP
1	SYNCH
4	TEST
1	UPDATE
4	VERIFY
1	VERIFY(12)
1	VERIFY(6)
5	WRITE
7	WRITE(10)
1	WRITE(12)
1	WRITE/VERIFY
1	XDREAD(10)

63 commands sent

Blocker Output:

Commands Allowed by Blocker

Count	Commands
546	25=READ DMA EXT
4	42=READ/V W/ EXT
4	70=SEEK
1	E7=FLUSH CACHE

63 commands sent, 4 commands allowed

Results:

Assertion & Expected Result	Actual Result
AM-01 Modifying commands blocked	Modifying commands blocked
AM-05 HWB behavior recorded	HWB behavior recorded

Analysis: Expected results achieved

4.2.2 HWB-03-file

<table>
<tr><th colspan="2">Test Case HWB-03 Variation hwb-03-file Tableau T5 Forensic IDE Bridge (USB)</th></tr>
<tr><td>Case Summary:</td><td>HWB-03 Identify commands blocked by the HWB while attempting 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.
HWB-AM-05 The action that a HWB device takes for any commands not assigned to the modifying, read or information categories is defined by the vendor.</td></tr>
<tr><td>Tester Name:</td><td>kbr</td></tr>
<tr><td>Test Date:</td><td>run start Tue Sep 26 15:44:55 2006
run finish Tue Sep 26 15:52:58 2006</td></tr>
<tr><td>Test Configuration:</td><td>HOST: charlie
HostToBlocker Monitor: chip
HostToBlocker PA: aa00155
HostToBlocker Interface: usb
BlockerToDrive Monitor: dale
BlockerToDrive PA: aa00111
BlockerToDrive Interface: ide
Run Environment: WXP</td></tr>
<tr><td>Drives:</td><td>Protected drive: BE
BE is a WDC WD2000JB-00KFA0 with 390721968 sectors (200 GB)</td></tr>
<tr><td>Blocker Input:</td><td>Commands Sent to Blocker
<table>
<tr><th>Count</th><th>Commands</th></tr>
<tr><td>5</td><td>MODE</td></tr>
<tr><td>4</td><td>PREVENT/ALLOW</td></tr>
<tr><td>10</td><td>READ</td></tr>
<tr><td>40</td><td>READ(10)</td></tr>
<tr><td>50</td><td>REQUEST_SENSE</td></tr>
<tr><td>191</td><td>TEST</td></tr>
<tr><td>27</td><td>WRITE(10)</td></tr>
</table></td></tr>
<tr><td>Blocker Output:</td><td>Commands Allowed by Blocker
<table>
<tr><th>Count</th><th>Commands</th></tr>
<tr><td>39</td><td>25=READ DMA EXT</td></tr>
<tr><td>5</td><td>70=SEEK</td></tr>
</table></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>
<tr><td>AM-05 HWB behavior recorded</td><td>HWB behavior recorded</td></tr>
</table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

4.2.3 HWB-03-img

<table>
<tr><th colspan="2">Test Case HWB-03 Variation hwb-03-img Tableau T5 Forensic IDE Bridge (USB)</th></tr>
<tr><td>Case Summary:</td><td>HWB-03 Identify commands blocked by the HWB while attempting 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.
HWB-AM-05 The action that a HWB device takes for any commands not assigned to the modifying, read or information categories is defined by the vendor.</td></tr>
<tr><td>Tester Name:</td><td>kbr</td></tr>
<tr><td>Test Date:</td><td>run start Tue Sep 26 16:04:21 2006
run finish Tue Sep 26 16:19:05 2006</td></tr>
<tr><td>Test Configuration:</td><td>HOST: dixon hill
HostToBlocker Monitor: chip
HostToBlocker PA: aa00155
HostToBlocker Interface: usb
BlockerToDrive Monitor: dale
BlockerToDrive PA: aa00111
BlockerToDrive Interface: ide
Run Environment: IXimager</td></tr>
<tr><td>Drives:</td><td>Protected drive: BE
BE is a WDC WD2000JB-00KFA0 with 390721968 sectors (200 GB)</td></tr>
<tr><td>Blocker Input:</td><td>Commands Sent to Blocker
<table>
<tr><th>Count</th><th>Commands</th></tr>
<tr><td>553</td><td>READ(10)</td></tr>
<tr><td>1314</td><td>REQUEST_SENSE</td></tr>
<tr><td>1314</td><td>WRITE(10)</td></tr>
</table></td></tr>
<tr><td>Blocker Output:</td><td>Commands Allowed by Blocker
<table>
<tr><th>Count</th><th>Commands</th></tr>
<tr><td>286</td><td>25=READ DMA EXT</td></tr>
</table></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>
<tr><td>AM-05 HWB behavior recorded</td><td>HWB behavior recorded</td></tr>
</table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

4.2.4 HWB–05

<table>
<tr><th colspan="2">Test Case HWB-05 Variation hwb-05 Tableau T5 Forensic IDE Bridge (USB)</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 is returned to the host.</td></tr>
<tr><td>Tester Name:</td><td>kbr</td></tr>
<tr><td>Test Date:</td><td>run start Thu Sep 21 10:53:52 2006
run finish Thu Sep 21 10:57:00 2006</td></tr>
<tr><td>Test Configuration:</td><td>HOST: dixon hill
HostToBlocker Monitor: chip
HostToBlocker PA: aa00155
HostToBlocker Interface: usb
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: ide
Run Environment: helix1.5</td></tr>
<tr><td>Drives:</td><td>Protected drive: A8
A8 is a WDC WD200BB-00AUA1 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 000000032767</td></tr>
<tr><td>Blocker Output:</td><td>00002/010/08 000000032767</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></table></td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

4.2.5 HWB–06

<table>
<tr><th colspan="2">Test Case HWB-06 Variation hwb-06 Tableau T5 Forensic IDE Bridge (USB)</th></tr>
<tr><td>Case Summary:</td><td>HWB-06 Identify read and information commands used by forensic tools and 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 is 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.
HWB-AM-05 The action that a HWB device takes for any commands not assigned to the modifying, read or information categories is defined by the vendor.</td></tr>
<tr><td>Tester Name:</td><td>kbr</td></tr>
<tr><td>Test Date:</td><td>run start Tue Sep 26 17:27:14 2006
run finish Tue Sep 26 17:52:41 2006</td></tr>
<tr><td>Test Configuration:</td><td>HOST: dixon hill
HostToBlocker Monitor: chip
HostToBlocker PA: aa00155
HostToBlocker Interface: usb
BlockerToDrive Monitor: dale
BlockerToDrive PA: aa00111
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
<table>
<tr><th>Count</th><th>Commands</th></tr>
<tr><td>844</td><td>READ(10)</td></tr>
<tr><td>771</td><td>WRITE(10)</td></tr>
</table>
2 commands sent</td></tr>
<tr><td>Blocker Output:</td><td>Commands Allowed by Blocker
<table>
<tr><th>Count</th><th>Commands</th></tr>
<tr><td>778</td><td>C8=Read DMA</td></tr>
</table>
2 commands sent, 1 commands allowed</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>
<tr><td>AM-05 HWB behavior recorded</td><td>HWB behavior recorded</td></tr>
</table>
</td></tr>
<tr><td>Analysis:</td><td>Expected results achieved</td></tr>
</table>

4.2.6 HWB–08

Test Case HWB-08 Variation hwb-08 Tableau T5 Forensic IDE Bridge (USB)	
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:	kbr
Test Date:	run start Thu Sep 21 10:45:23 2006 run finish Thu Sep 21 10:47:11 2006
Test Configuration:	HOST: dixon hill HostToBlocker Monitor: none HostToBlocker PA: none HostToBlocker Interface: usb BlockerToDrive Monitor: none BlockerToDrive PA: none BlockerToDrive Interface: ide Run Environment: helix1.5
Drives:	Protected drive: BE BE is a WDC WD2000JB-00KFA0 with 390721968 sectors (200 GB)
Blocker Output:	cmd: /home/helix/partab hwb-08 dixon hill kbr /dev/sdb be -all 390721968 total number of sectors
Results:	see below
Analysis:	Expected results achieved

Results:

Assertion & Expected Result	**Actual Result**
AM-03 Access Significant Information unaltered	Access Significant Information unaltered

4.2.7 HWB–09

<table>
<tr><th colspan="2">Test Case HWB-09 Variation hwb-09 Tableau T5 Forensic IDE Bridge (USB)</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>kbr</td></tr>
<tr><td>Test Date:</td><td>run start Thu Sep 21 10:48:06 2006
run finish Thu Sep 21 10:50:09 2006</td></tr>
<tr><td>Test Configuration:</td><td>HOST: dixon hill
HostToBlocker Monitor: none
HostToBlocker PA: none
HostToBlocker Interface: usb
BlockerToDrive Monitor: none
BlockerToDrive PA: none
BlockerToDrive Interface: ide
Run Environment: helix1.5</td></tr>
<tr><td>Drives:</td><td>Protected drive: BE
BE is a WDC WD2000JB-00KFA0 with 390721968 sectors (200 GB)</td></tr>
<tr><td>Blocker Output:</td><td>24320/254/63 (max cyl/hd values)
24321/255/63 (number of cyl/hd)
390721968 total number of sectors
cmd: /home/helix/diskchg hwb-09 dixon hill kbr /dev/sdb -read 490721968 0 1
Disk addr lba 490721968 C/H/S 30546/7/38 offset 0
Disk read error 0xFFFFFFFF at sector 30546/7/38</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*