March 21, 2005

Hardware Write Blocker (HWB) Assertions and Test Plan

Draft 1 for public comment of Version 1.0

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

Abstract[1]

This document defines test assertions and test cases for hardware write blocker (HWB) devices used in computer forensics investigations. These assertions have been derived from the associated HWB requirements (*Hardware Write Blocker Device (HWB) Specification Version 2.0 May 19, 2004*). The requirements were developed by a focus group of individuals who have been trained and are experienced in the use of hardware write blocking tools and have performed investigations that have depended on the results of these tools. As this document evolves through comments from the focus group and others, new versions will be posted to the web site at http://www.cftt.nist.gov/.

[1] **Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.**

Contents

List of Tables

121

1. Introduction

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. A capability is required to ensure that forensic tools consistently produce accurate, objective, and reproducible test results. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic tools by the development of functional specifications, test procedures, test criteria, test sets, test software, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools' capabilities. This approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing. This project is further described at http://www.cftt.nist.gov/.

The CFTT is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice; the NIST Office of Law Enforcement Standards (OLES) and the NIST Information Technology Laboratory (ITL); and is supported by other organizations, including the Federal Bureau of Investigation, the Department of Defense Cyber Crime Center, IRS-Criminal Investigation's Electronic Crimes Program, the Department of Homeland Security's Bureau of Immigration and Customs Enforcement and the U.S. Secret Service. Since all documents are posted on the web for public review, the entire computer forensics community has the opportunity to participate in the development of the specifications and test methods.

The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified, i.e., the examination or capture of digital data from the hard drives or other storage media of a seized computer must be performed so that the contents are not changed. The investigator follows a set of procedures designed to prevent the modification of original evidence. These procedures may include various write blocking techniques including the use of software tools or hardware devices to block modification of the contents of a drive.

2. Purpose

This document defines functional test assertions and test cases for hardware write blocker (HWB) devices used in computer forensics investigations. These assertions have been derived from the associated HWB requirements (*Hardware Write Blocker Device (HWB) Specification Version 2.0 May 19, 2004*) and are used in the generation of test cases and a test plan.

3. Scope

The scope of this specification is defined by the methods used for testing HWB devices. It is limited specifically as follows:

1. For ATA interfaces and devices, only the command sets from ATA-1 through ATA-7 specifications are tested [ATA-1, ATA-2, ATA-3, ATA-4, ATA-5, ATA-6, and ATA-7].

2. For SCSI interfaces and devices, only command sets applicable to the direct access class of storage devices are tested. These include the SCSI primary command sets, the SCSI block command sets, and the SCSI reduced block command sets [SPC-1, SPC-2, SPC-3, SPC-4, SBC-1, SBC-2, SBC, and SBC-1].

3. For USB interfaces and devices, only commands sets applicable to the mass storage device class storage devices are tested. These include the SCSI primary command sets, SCSI block command sets, and SCSI reduced block command sets.

4. For IEEE-1394 interfaces and devices, the command sets tested are the same as for testing SCSI devices.

4. Background

One of the core elements of forensic investigations is to never alter original evidence. A HWB device is one way of ensuring this requirement is met. A HWB is designed to prevent any modifying command from reaching a storage device while allowing information about the disk to remain available to the operating system and forensic tool.

Hardware Write Blocker Device (HWB) Specification Version 2.0 divides the full set of commands that can be sent to a storage device into four functional categories of operations: modifying, read, information, and other non-modifying. The modifying category is the most critical of the four as it refers to the main body of operations that must be blocked by a HWB device. Test cases are generally constructed by sending commands of specific categories and observing the result.

Commands for testing a HWB device can be sent by the host computer to a storage device by the BIOS, the operating system, file system operations, forensic tools, or a test harness. Certain actions such as boot up and shut down can cause modifying commands to be sent to storage devices. Because a HWB is placed between the host and the storage device it should prevent any modifying command from reaching the storage device.

A test harness was developed to execute the identified test cases so that HWB device behaviors could be observed. A protocol analyzer was also used to observe activity on the interface during HWB testing. A protocol analyzer is a device that connects directly to the interface and captures all activity that passes its connection point on that interface.

5. Assertions

This section lists assertions that all HWB tools shall meet. An assertion is a condition that must be tested to confirm conformance to a requirement. Each assertion specifies conditions that are to be

tested. Traceability matrices relating requirements to assertions and assertions to test cases are presented in Appendix C.

HWB-AM-01. The HWB shall not transmit any modifying category operation to the protected storage device.

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-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.

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.

6. Test Methodology

The general protocol for executing test cases involves sending commands from a host computer to a storage device protected by a HWB and observing the results.

6.1 Test Materials

An inventory of items used to carry out this testing is presented in Table 1. While some items are always required, other items are used if available to give more complete results.

Table 1 Software and Hardware Used for Testing

Item	**Comments**
Hardware Write Blocker (HWB) Device	The HWB device to be tested.
Storage Device	The drive or device protected by the HWB. The details of a particular test case may require that a storage device support a particular capability. For example, if testing a HWB with ATA drives then some drives used in testing must support 48 bit sector addressing to verify that an ATA *read DMA extended* command correctly returns the data requested.
Host computer	A platform for running the test harness.
Operating System	An environment for issuing commands to a protected storage device.

Protocol Analyzer	A device to directly observe commands on a bus. Depending on the requirements of a specific test case, the protocol analyzer allows identification of commands blocked by the HWB or documents commands generated from the host computer.
Monitor host	A computer for controlling a protocol analyzer.
Test Harness	• A basic command generator to generate each possible command code. • A write command generator to generate each defined write commands such that execution of the command would leave a unique signature on an unprotected drive (or a drive if the HWB fails to protect the drive). • A read command generator to generate each defined read command and verify that the data obtained is the actual content on the storage device. • An information command generator to obtain access significant information for validation. • An error command generator to generate a command that should return an error status. • A write command analysis tool to scan a drive for the signatures of the write command generator. • Tools to initialize a drive to a known state. • Tools to compute a SHA1 or other hash of a drive.
Forensic Acquisition/Imaging Tools	Common forensic applications used to generate I/O commands to the protected storage device.

6.2 Measuring Conformity to Assertions

This section describes the methodology for measurement of the conformity of HWB to assertions. Each assertion has one or more measurement methodologies defined. Each defined methodology depends on the combination of what must be measured and measurement tools available for each test case. The complete measurement of conformity requires two critical components: a method for generating commands on the protected bus and a method for determining the action of the HWB.

Some assertions may be measured in more than one way. For example, measuring HWB-AM-01 the assertion that the HWB does not send any modifying command to the protected storage device can be done in more than one way. A known sequence of commands can be sent from the host to the HWB protecting a storage device. Then either the commands sent from the HWB to the protected device can be monitored by a protocol analyzer or the protected device can be examined (either directly or by comparing a pre-test hash to a post-test hash) for changes. Both methods determine if the HWB protects the actual device used for the test, however using the protocol analyzer records the HWB action for all commands sent. For example, if a storage device that only supports up through the ATA-4 protocol was used in a test and the HWB under test only blocked

write commands defined up through the ATA-5 protocol then the HWB might (incorrectly) allow write commands defined in the ATA-5, 6 and 7 protocols to be transmitted to the storage device with no detectable change occurring to the device. The protocol analyzer, however if available, would report all commands transmitted by the HWB device.

Commands may be generated by a combination of operating system software, test harness software or by widely used forensic software. Some methods for generating commands may be limited in the completeness of the command set generated.

A protocol analyzer can capture all bus activity between the write block device and the protected storage device or between the test host and the HWB. If a protocol analyzer is not available for the input bus or output bus of a HWB under test, alternative measurement procedures are defined. The alternative measurement methodology may put some limitations on the test results.

If more complete command generation software or additional protocol analyzer components become available after a test report is issued for a device, the more complete tests can be executed and a supplement to the original report can be produced.

Four categories of measurement methodology are defined based on availability of command generators and protocol analyzers.

Operational: Neither a command generator nor a protocol analyzer is required for operational tests. In this method, widely used forensic tools and operating system environments generate commands. The main advantage of this method is that commands are generated by the actual conditions under which the HWB device functions. There are two limitations to this method: commands tested are limited to ones generated by operating systems and selected forensic applications used in the test and it is unknown which commands are actually generated. This category represents the minimal level of testing required to provide assurance that a write block device provides adequate protection from undesired change to a storage device.

Observational: If a protocol analyzer is available, then the observational methodology is used. This method runs the same tools to generate commands as the operational test but the protocol analyzer monitors the actual commands generated and records the behavior of the blocking device. This method documents the HWB behavior for all commends generated. The limitation of this method is the commands tested are limited to ones generated by operating systems and selected forensic applications used in the test. In other words, although the set of generated commands is known, the entire possible command set may not be generated.

Indirect: This methodology is used if only a command generator is available for the test case. This limits the scope of testing to commands that can produce an observable result on the storage device or return verifiable data to the host. For testing commands that write to a device or change the device configuration, this requires a sophisticated command generator that produces configuration and content changes that can be detected by examination of the storage device. For read and information commands, the returned data or information must be verifiable. If a protocol analyzer is available, it may optionally be used to record the actual commands sent from the host.

Detailed: This methodology is used if both a command generator and a protocol analyzer are available. This category of testing is only needed for determining the exact set of commands blocked by the HWB (assertions HWB-AM-01 and HWB-AM-05). Every possible command code is sent and the behavior of the blocking device is recorded by a protocol analyzer.

6.3 Measurement Methodology

This section describes the methodology for measuring conformity of the HWB device to each defined assertion. Not all measurement categories are required for every assertion.

6.3.1 HWB-AM-01

The HWB shall not transmit any modifying category operation to the protected storage device.

Detailed: The command generator sends all feasible command codes to the HWB device. The protocol analyzer records a trace of all command activity between the HWB device and the protected device. Any commands classified as modifying are reported.

Indirect: The command generator sends modifying commands designed to write specific information in known locations to the protected device. After a test run, the protected device is examined to determine if the data stored on the protected device was changed. Any changes are reported.

Observational: A variety of forensic tools running in commonly used operating system environments generate commands to do tasks that are known to write to a storage device and a protocol analyzer records a trace of all command activity between the blocking device and the protected device. Any commands classified as modifying are reported along with a trace of all commands actually generated.

Operational: A variety of forensic tools running in commonly used operating system environments generate commands to do tasks that are known to write to a storage device. A pre-test hash matching a post-test hash verifies that no changes occurred to the protected device.

6.3.2 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.

Detailed: Not applicable.

Indirect: The command generator sends all feasible read command codes to the blocking device to read known data from the protected device. The returned data is compared to known content already placed on the storage device. Any differences are reported.

Observational: A variety of forensic tools in commonly used operating system environments are used to generate commands to acquire a storage device. A protocol analyzer records a trace of all command activity between the HWB device and the protected device. A pre-test hash and a hash of data acquired through the HWB are used to verify that the protected device is accurately (the data on the storage device is acquired without modification) acquired. Either a second run allows the protocol analyzer to be attached between the host computer and the

HWB to record a trace of commands generated or a second protocol analyzer records a trace of all commands actually generated for reporting.

Operational: A variety of forensic tools in commonly used operating system environments are used to generate commands to acquire a storage device. A pre-test hash and a hash of data acquired through the HWB are used to verify that the protected device was accurately (the data on the storage device is acquired without modification) acquired.

6.3.3 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.

Detailed: Not applicable.

Indirect: The command generator sends all information category commands to a protected device of known size and configuration. The access significant information is checked against known values obtained without the HWB present.

Observational: Forensic tools in commonly used operating system environments are used to acquire a storage device. If the storage device is completely (all user accessible sectors) acquired this implies that the size of the device and any other access significant information is reported correctly to the host from the HWB. The protocol analyzer located between the host and the HWB records the actual commands generated.

Operational: Forensic tools in commonly used operating system environments are used to acquire a storage device. If the storage device is completely (all user accessible sectors) acquired this implies that the size of the device and any other access significant information is reported correctly to the host from the HWB.

6.3.4 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.

Detailed: Not applicable.

Indirect: A command generator attempts to read from an invalid sector and reports the result.

Observational: Not applicable.

Operational: Not applicable.

6.3.5 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.

Detailed: The command generator sends all feasible command codes to the blocking device. The protocol analyzer records the behavior of the HWB for each command sent from the host. It is placed between the host and the HWB.

Indirect: Not applicable.
Observational: Not applicable.
Operational: Not applicable.

7. Test Cases

This section describes nine test cases that use several methodologies to determine HWB device actions for commands that might change a storage device, and verify that if a storage device is protected with a HWB then data stored on a protected device and data about the device can be obtained.

7.1 Test Case Selection

The selection of test cases depends on the availability of a protocol analyzer and command generator software.

At least three of the nine defined test cases are always executed. Test case HWB-09 is always executed. If a protocol analyzer is available then test cases HWB-03 and HWB-06 are executed. If no protocol analyzer is available, test cases HWB-04 and HWB-07 are executed as alternatives to HWB-03 and HWB-06.

If a command generator corresponding to any of the test cases HWB-02, HWB-05 and HWB-08 is available, then the respective test case is executed. A protocol analyzer is not required, but if available, it may be used to record the commands sent from the host.

Test case HWB-01 is executed only if both a protocol analyzer and a command generator for the full command set are available.

7.2 Test Case Descriptions

This section describes each test case. The next section describes variations on some of the test cases.

Item	Description
Case number	A unique identifier for the test case.
Category	One of the four categories of test: detailed, indirect, observational or operational. The category indicates if the test uses a protocol analyzer (detailed and observational), a command generator (detailed and indirect) or neither (operational).
Test Summary	A brief statement describing the test case.
Comment	Additional information about the test case.
Assertions tested	The assertions measured by the test.
Variations	For tests that are repeated with a slight variation of some parameter, this general description of alternate versions of the test that are run. The details of each alternative are described separately.

Item	Description
Tools Required	A list of items needed for the test.
Test Setup and Procedure	A general list of steps to follow for the test. Detailed procedures are in a separately published *Setup and Procedures* document.
Expected Results	A description of successful test results.

416
417
418

Item	Description
Case number	HWB-01
Category	Detailed
Test Summary	Identify commands blocked by the HWB.
Comment	This test case may be omitted if no protocol analyzer is available.
Assertions tested	AM-01 and AM-05
Variations	The command set may be split into several runs with a different subset of the command space sent in each run. Each run is identified by a unique suffix appended to the case number.
Tools Required	Test Host Test drive (no specific content required) Monitor Host Protocol Analyzer Basic Command Generator Tool
Test Setup and Procedure	1. Select test materials. 2. Attach protocol analyzer between HWB and protected device. 3. Start monitor host and begin trace. 4. Start test host. 5. Execute command generator. 6. Shut down test host. 7. Stop trace. 8. Shut down monitor host and save result.
Expected Results	AM-01: No modifying commands are logged from the HWB to the protected device by the protocol analyzer. AM-05: HWB behavior for each command sent is recorded.

419
420

Item	Description
Case number	HWB-02
Category	Indirect
Test Summary	Identify modifying commands blocked by the HWB.
Comment	This test is an alternative to HWB-01 and is used if no protocol analyzer is available. This test is limited to testing commands implemented in the modification command generation tool. The generation tool is limited to commands that produce a result observable by a modification analysis tool. This test may be omitted if no modifying command generation tool is available.

Item	Description
Assertions tested	AM-01
Variations	The command space may be split into several runs with a different subset of the command space sent in each run. Each run is identified by a unique suffix appended to the case number.
Tools Required	Test Host Test drive with 48 bit address space (no specific content required) Modifying command generator tool Modification analysis tool FS-TST **diskwipe**
Test Setup and Procedure	1. Select test materials. 2. Start the test host (without the HWB). 3. Initialize the selected drive with FS-TST **diskwipe.** 4. Shut down the test host. 5. Attach the HWB. 6. Start the test host. 7. Execute Modifying command generator. 8. Execute Modification analysis tool and save results.
Expected Results	AM-01: No changes are detected on the protected drive by the modification analysis tool.

421
422

Item	Description
Case number	HWB-03
Category	Observational
Test Summary	Identify commands blocked by the HWB while attempting to modify a protected drive with forensic tools.
Comment	This test may be omitted if no protocol analyzer is available.
Assertions tested	AM-01 and AM-05
Variations	Attempt to write to a protected drive using forensic and file system applications. The applications and operating system environments are selected from those available at test run time. There should also be at least one variation of attempting to write to a protected drive from each of the following: writing to a drive from an imaging tool, changing file system content and if the protected interface is bootable, booting the protected drive. Variations are described in Section 7.4.1.
Tools Required	Test Host Monitor Host Multiple test drives Protocol Analyzer Selection of forensic acquisition tools
Test Setup and Procedure	1. Select test materials. 2. Set up selected variation. 3. Attach protocol analyzer between host and HWB. 4. Start monitor host and begin trace.

Item	Description
	5. Start test host. 6. Execute selected test case variation. 7. Shut down test host. 8. Stop trace, save result to identify modifying commands generated. 9. Shut down monitor host. 10. Attach protocol analyzer between HWB and protected drive. 11. Start monitor host and begin trace. 12. Start test host. 13. Execute selected variation. 14. Shut down test host. 15. Stop trace, save result to identify modifying commands blocked. **Alternate Procedure Using two Protocol Analyzers** 1. Select test materials. 2. Set up selected variation. 3. Attach one protocol analyzer between host and HWB. 4. Attach a second protocol analyzer between HWB and drive. 5. Start monitor hosts and begin trace. 6. Start test host. 7. Execute selected variation. 8. Shut down test host. 9. Stop traces, save result to identify modifying commands generated.
Expected Results	AM-01: No modifying commands are logged from the HWB to the protected device by the protocol analyzer. AM-05: HWB behavior for each command sent is recorded.

Item	Description
Case number	HWB-04
Category	Operational
Test Summary	Attempt to modify a protected drive with forensic tools.
Comment	This test is an alternative to HWB-03 if no protocol analyzer is available.
Assertions tested	AM-01
Variations	Attempt to write to a protected drive using forensic and file system applications. The applications and operating system environments are selected from those available at test run time. There should also be at least one variation of attempting to write to a protected drive from each of the following: writing to a drive from an imaging tool, changing file system content and if the protected interface is bootable, booting the protected drive. Variations are described in Section 7.4.1.

Item	Description
Tools Required	Test Host Multiple test drives Selection of forensic acquisition tools.
Test Setup and Procedure	1. Select test materials. 2. Set up selected variation. 3. Pre-test hash. 4. Start test host. 5. Execute variation. 6. Shut down test host. 7. Post-test hash.
Expected Results	AM-01 Pre-test hash is the same as the post-test hash.

425
426

Item	Description
Case number	HWB-05
Category	Indirect
Test Summary	Identify read commands allowed by the HWB.
Comment	If there is no read command generator available this case may be omitted.
Assertions tested	AM-02
Variations	The command space may be split into several runs with a different subset of the command space sent in each run. Each run is identified by a unique suffix appended to the case number.
Tools Required	Test Host Read Command Generator Tool
Test Setup and Procedure	1. Select test materials. 2. Start test host. 3. Execute read command generator. 4. Shut down test host. 5. Save results.
Expected Results	AM-02 All read commands return data known to be present on the storage device.

427
428

Item	Description
Case number	HWB-06
Category	Observational
Test Summary	Identify read and information commands used by forensic tools and allowed by the HWB.
Comment	If there is no protocol analyzer available then case HWB-07 may be executed as an alternative.
Assertions tested	AM-02, AM-03 & AM-05
Variations	Use imaging tools from at least two operating system environments to attempt to read from a protected drive. Variations

Item	Description
	are described in Section 7.4.2.
Tools Required	Test Host Monitor Host Protocol Analyzer Selection of forensic acquisition tools
Test Setup and Procedure	1. Select test materials. 2. Set up selected test case variation. 3. Attach protocol analyzer between host and HWB and begin trace. 4. Start test host. 5. Execute selected variation. 6. Shut down test host. 7. Stop trace, save result to identify read and information commands generated.
Expected Results	AM-02: Accurate (pre-test hash matches acquisition hash) acquisition of the sectors acquired from the protected drive. AM-03: Complete (all user accessible sectors) acquisition of the protected drive. AM-05: HWB behavior for each command sent is recorded.

Item	Description
Case number	HWB-07
Category	Operational
Test Summary	Read a protected drive with forensic tools.
Comment	This case is an alternative to HWB-06 to be executed if no protocol analyzer is available.
Assertions tested	AM-02 and AM-03
Variations	Use imaging tools from at least two operating system environments to attempt to read from a protected drive. The variations are described in Section 7.4.2.
Tools Required	Test Host Selection of forensic acquisition tools
Test Setup and Procedure	1. Select test materials. 2. Set up selected test case variation. 3. Start test host. 4. Execute selected variation. 5. Shut down test host. 6. Save results.
Expected Results	AM-02: Accurate (pre-test hash matches acquisition hash) acquisition of the sectors acquired from the protected drive. AM-03: Complete (all user accessible sectors) acquisition of the protected drive.

Item	Description
Case number	HWB-08
Category	Indirect
Test Summary	Verify that access significant information is unmodified by the HWB.
Comment	If there is no information command generator available this test case may be omitted.
Assertions tested	AM-03
Variations	The command space may be split into several runs with a different subset of the command space sent in each run. Each run is identified by a unique suffix appended to the case number.
Tools Required	Test host Information command generation tool
Test Setup and Procedure	1. Select test materials. 2. Start test host. 3. Execute information command generator. 4. Shut down test host. 5. Save results.
Expected Results	AM-03: All access significant information is correctly returned from the drive.

Item	Description
Case number	HWB-09
Category	Indirect
Test Summary	Determine if an error on the protected drive is returned to the host.
Comment	None
Assertions tested	AM-04
Variations	None
Tools Required	Test host Error generator
Test Setup and Procedure	1. Select test materials. 2. Start test host. 3. Execute error generator. 4. Shut down test host. 5. Save results.
Expected Results	AM-04: Error status returned to host from protected drive.

7.3 Test Case Resource Summary

Table 2 summarizes the resources (protocol analyzer and command generators) required for each test case and the assertions tested. In the **Analyzer Placement** columns, the label **H=>B** indicates the protocol analyzer monitors traffic from the host computer to the HWB. The column labeled **B=>D** indicates the protocol analyzer is placed between the HWB and the protected storage device.

Table 2 Summary of Test Cases

Traceability of Assertions to Test Cases						**Test Case Resource Attributes**						
Test Case	**Assertions Tested**					**Analyzer Placement**		**Generator Required**				
	01	**02**	**03**	**04**	**05**	**H=>B**	**B=>D**	**Basic**	**Write**	**Read**	**Info**	**Error**
01	●				●		●	●				
02	●					●[1]			●			
03	●				●	●[2]	●[2]					
04	●											
05		●				●[1]				●		
06		●	●		●	●						
07		●	●									
08			●			●[1]					●	
09				●		●[1]						●

Note 1: The protocol analyzer is not required for the test but may optionally be used to confirm that the commands sent from the host were actually sent from the host.
Note 2: The test requires that both the commands sent from the host and that the commands received by the protected device are reported. This can be measured either by running the test once with two protocol analyzers or by running the test twice with different placement of the protocol analyzer for each run.

7.4 Test Case Variations

This section describes variations on defined test cases. The objective of the test case variations is to generate as large a subset of the command space as possible from widely used forensic applications.

7.4.1 Modifying Variations (HWB-03 and HWB-04)

The objective of the modifying variations is to generate as many different modifying commands as practical. The modifying variations are divided into three groups: *boot*, *restore, file-system application* and *option switches*. A description of each variation follows:

7.4.1.1 Boot

The *boot* variation uses the boot and shutdown process of an operating system to attempt to modify a protected drive. Use the following procedure to set up a bootable drive for the test case. If the protected interface is not bootable, this variation may be omitted. Otherwise, at least one *boot* variation test case should be executed. Additional *boot* variation test cases may optionally be executed for other operating systems.

Perform the following steps to set up each boot variation:

1. Select an operating system.
2. Select a storage device of known size.
3. Select a host computer (this should be the same computer used in the write block test run).
4. Install the selected operating system on the selected storage device.
5. Shut down the computer.

7.4.1.2 Restore

The *restore* variation uses forensic imaging tools to attempt to write to a protected drive. This variation requires two or three drives: a protected drive, a drive to hold an execution environment with a forensic imaging tool and a drive to contain an image file. The execution environment and forensic imaging tool may be placed together on a single drive or the imaging tool might be on a bootable CD and the image file on a separate drive. Other combinations are possible. Two variations are defined: small target drive and large target drive. For ATA hard drives larger than about 138GB different instructions are required to read and write data than for smaller drives. The ATA standards define two sector address lengths: 28 bit sector addresses and 48 bit sector addresses. A small drive in this case is defined as one that can be addressed with 28 bit sector addressing and a large drive as one that must be addressed with 48 bit sector addressing.

Perform the following steps to set up an image for the restore:

1. Set up an image source drive that can be imaged. The drive should contain at least one valid partition with arbitrary content.
2. Set up an imaging environment for a selected imaging tool.
3. Use the imaging environment to create an image file of the entire source drive.
4. Use the imaging environment to create an image file of a partition on the source drive.
5. Set up the small drive to be protected by wiping the drive with FS-TST **diskwipe**.
6. Set up the large drive to be protected by wiping the drive with FS-TST **diskwipe**.

Perform the following steps to execute the variation for both target drives:

1. Attach the target drive to the HWB.
2. Boot the tool environment.
3. Attempt to restore the image to the target drive.

7.4.1.3 File system applications

The *file system application* variation uses file system manipulation commands to attempt to write to a protected drive. Two variations are defined: small target drive and large target drive. A small drive, in this case, is defined as one that can be addressed with 28 bit sector addressing and a large drive as one that must be addressed with 48 bit sector addressing. An operating system execution environment is also required.

Perform the following steps to set up the drives for the variation:

1. Set up both the target drives to be protected by wiping the drives with FS-TST **diskwipe**.
2. Create one target partition on the small drive.
3. Create two partitions on the large drive such that the second partition, the target, requires 48 bit sector addressing for access, i.e., make the first partition at least 140GB.
4. On each target partition create three directories, **alpha**, **beta** and **gamma**. In the **beta** directory create two files, **zeta** and **omega**. File content is arbitrary.

Do the following to execute the variation:

1. Protect the target drive.
2. Boot the execution environment.
3. Attempt to create a file in the **alpha** directory.
4. Attempt to delete the file **zeta** in the **beta** directory.
5. Attempt to delete the **gamma** directory.
6. Attempt to create a new directory called **delta**.
7. Attempt to copy the file **omega** to the **delta** directory.

7.4.1.4 HWB Option switches

If the HWB device has a method for setting different behaviors then each behavior setting shall be tried at least once in the proceeding tests.

7.4.2 Read and Information Variations (HWB-06 and HWB-07)

The objective of the read and information variations is to generate as many different read and information commands as practical. This is accomplished by using a variety of imaging tools to acquire a drive. This set of variations includes at least one windows environment imaging tool and one UNIX-like environment imaging tool. If the protected interface allows imaging from DOS and if there are DOS imaging tools available, then image the protected drive from DOS using BIOS access. Two imaging targets should be set up: a full drive that can be addressed with 28 bit sector addressing and second drive with a small partition that must be addressed with 48 bit sector addressing.

Perform the following steps to set up the variation:

1. Create an image source drive that can be imaged. The drive should contain at least one valid partition with arbitrary content.
2. Set up an imaging environment for a selected imaging tool.

Do the following to execute the variation:

1. Execute the imaging tool to image the protected drive.

Appendix A. References

[ATA-1] 0791M AT Attachment Interface for Disk Drives (ATA-1), X3T10/0791D, Revision 4c, 1991.
[ATA-2] 0948D AT Attachment Interface with Extensions (ATA-2), X3T10/0948D, Revision 4c, March 18, 1996.
[ATA-3] 2008D AT Attachment - 3 Interface (ATA-3), X3T13/2008D, Revision 7b January 27, 1997.
[ATA-4] 1153D AT Attachment - 4 with Packet Interface Extension (ATA/ATAPI - 4). X3T13/1153, Revision18, August 18, 1998.
[ATA-5] 1321D AT Attachment - 5 with Packet Interface (ATA/ATAPI - 5), X3T13/1321, Revision 3, February 29, 2000.
[ATA-6] 1410D AT Attachment - 6 with Packet Interface (ATA/ATAPI - 6) X3T13/1410, Revision 3, October 30, 2001.
[ATA-7] 1532D AT Attachment - 7 with Packet Interface (ATA/ATAPI - 7) X3T13/1532, Revision 4b, April 21, 2004.
[SBC-1] SBC SCSI-3 Block Commands, T10/996D, Revision 8c, November 13, 1997, [first generation disk drive command set]
[SBC-2]SBC-2 SCSI Block Commands – 2, T10/1417D, Revision 16, November 13, 2004, [second generation disk drive command set]
[RBC] RBC Reduced Block Commands, T10/1240-D, Revision 10a, August, 18, 1999, [simplified disk drive command set]
[RBC-1] RBC_AM1 Reduced Block Command Set Amendment 1 [first amendment to above standard]
[SPC-1] SPC SCSI-3 Primary Commands, T10/995D, Revision 11a, March 28, 1997, [first generation command set for all SCSI devices]
[SPC-2] SPC-2 SCSI Primary Commands – 2, T10/1236-D, Revision 20, July 18, 2001, [second generation command set for all SCSI devices]
[SPC-3] SPC-3 SCSI Primary Commands – 3, T10/1416-D, Revision 21c, January 15, 2005, [third generation command set for all SCSI devices]
[SPC-4] SPC-4 SCSI Primary Commands – 4, in preparation [fourth generation command set for all SCSI devices]
[SAT] T10/1711-D Revision 1a, SCSI / ATA Translation (SAT), 16 December 2004.

Note: the ATA references can be found at http://www.t13.org/ and the SCSI references can be found at http://www.t10.org/.

Appendix B. Command Category Assignments

This section presents command category assignments for the ATA and SCSI protocols. The following tables in this appendix give the category assignments for the ATA and SCSI command sets used to access secondary storage block devices. In the *category* column the letter *R* indicates a *read* category command, the letter *M* indicates a modifying category, the letter *I* indicates an *information* category and a blank indicates the command is not assigned to any of the three listed categories.

The commands in Table 3 are defined in the ATA specifications [ATA-1, ATA-2, ATA-3, ATA-4, ATA-5, ATA-6, and ATA-7]. In the columns labeled **1** through **7**, an *S* indicates that the command is supported in that version of the ATA specification. The commands in Table 4 are defined in the SCSI reduced block commands reference [RBC, RBC-1]. The commands in Table 5 and Table 6 are defined in the SCSI command references [SBC-1, SBC-2, SPC-1, SPC-2, SPC-3, and SPC-4]. In addition, the SCSI/ATA translation reference [SAT] defines translations from SCSI commands to ATA commands as might be found in HWB devices that translate from SCSI commands to ATA commands.

Please note that the following ATA standards have been withdrawn:
0791M AT Attachment Interface for Disk Drives (ATA-1) (Withdrawn 6 August 1999)
For historical purposes the last committee draft of the standard is maintained as X3T9.2/791Dr4c.
0948D AT Attachment Interface with Extensions (ATA-2) (Withdrawn in 2001)
For historical purposes the last committee draft of the standard is maintained as X3T9.2/948Dr4c.
2008D AT Attachment - 3 Interface (ATA-3) (Withdrawn in 2002)
For historical purposes the last committee draft of the standard is maintained as d2008r7b.

Table 3 ATA Command Category Assignments

Command Name	Category	Op Code	ATA Specification						
			1	2	3	4	5	6	7
READ BUFFER	R	E4h	S	S	S	S	S	S	S
READ DMA (W/ RETRY)	R	C8h	S	S	S	S	S	S	S
READ DMA (W/O RETRY)	R	C9h	S	S	S	S	-	-	-
READ DMA EXT	R	25h	-	-	-	-	-	S	S
READ DMA QUEUED	R	C7h	-	-	-	S	S	S	S
READ DMA QUEUED EXT	R	26h	-	-	-	-	-	S	S
READ LOG EXT	R	2Fh	-	-	-	-	-	S	S
READ LONG (W/ RETRY)	R	22h	S	S	S	-	-	-	-
READ LONG (W/O RETRY)	R	23h	S	S	S	-	-	-	-
READ MULTIPLE	R	C4h	S	S	S	S	S	S	S
READ MULTIPLE EXT	R	29h	-	-	-	-	-	S	S
READ SECTOR(S) (W/ RETRY)	R	20h	S	S	S	S	S	S	S
READ SECTOR(S) (WO/ RETRY)	R	21h	S	S	S	S	-	-	-
READ SECTOR(S) EXT	R	24h	-	-	-	-	-	S	S
READ STREAM DMA EXT	R	2Ah	-	-	-	-	-	-	S

Command Name	Category	Op Code	ATA Specification						
			1	2	3	4	5	6	7
READ STREAM EXT	R	2Bh	-	-	-	-	-	-	S
READ VERIFY SECTOR(S)	R	40h	S	S	S	S	S	S	S
READ VERIFY SECTOR(S)	R	41h	S	S	S	S	-	-	-
READ VERIFY SECTOR(S) EXT	R	42h	-	-	-	-	-	S	S
SMART READ LOG	R	B0h/D5h	-	-	-	-	S	S	S
CFA ERASE SECTORS	M	C0h	-	-	-	S	S	S	S
CFA TRANSLATE SECTOR	M	87h	-	-	-	S	S	S	S
CFA WRITE MULTIPLE WITHOUT ERASE	M	CDh	-	-	-	S	S	S	S
CFA WRITE SECTORS WITHOUT ERASE	M	38h	-	-	-	S	S	S	S
DEVICE CONFIGURATION SET	M	B1h/C3h	-	-	-	-	-	S	S
DOWNLOAD MICROCODE	M	92h	-	S	S	S	S	S	S
FLUSH CACHE	M	E7h	-	-	-	S	S	S	S
FLUSH CACHE EXT	M	EAh	-	-	-	-	-	S	S
FORMAT TRACK	M	50h	S	S	S	-	-	-	-
PACKET	M	A0h	-	-	S	S	S	S	S
SECURITY ERASE PREPARE	M	F3h	-	-	S	S	S	S	S
SECURITY ERASE UNIT	M	F4h	-	-	S	S	S	S	S
SECURITY SET PASSWORD	M	F1h	-	-	S	S	S	S	S
SMART WRITE LOG	M	B0h/D6h	-	-	-	-	S	S	S
WRITE BUFFER	M	E8h	S	S	S	S	S	S	S
WRITE DMA (W/ RETRY)	M	CAh	S	S	S	S	S	S	S
WRITE DMA (W/O RETRY)	M	CBh	S	S	S	S	-	-	-
WRITE DMA EXT	M	35h	-	-	-	-	-	S	S
WRITE DMA FUA EXT	M	3Dh	-	-	-	-	-	-	S
WRITE DMA QUEUED	M	CCh	-	-	-	S	S	S	S
WRITE DMA QUEUED EXT	M	36h	-	-	-	-	-	S	S
WRITE DMA QUEUED FUA EXT	M	3Eh	-	-	-	-	-	-	S
WRITE LOG EXT	M	3Fh	-	-	-	-	-	S	S
WRITE LONG (W/ RETRY)	M	32h	S	S	S	-	-	-	-
WRITE LONG (W/O RETRY)	M	33h	S	S	S	-	-	-	-
WRITE MULTIPLE	M	C5h	S	S	S	S	S	S	S
WRITE MULTIPLE EXT	M	39h	-	-	-	-	-	S	S
WRITE MULTIPLE FUA EXT	M	CEh	-	-	-	-	-	-	S
WRITE SAME	M	E9h	S	S	-	-	-	-	-
WRITE SECTOR(S) (W/ RETRY)	M	30h	S	S	S	S	S	S	S
WRITE SECTOR(S) (W/O RETRY)	M	31h	S	S	S	S	-	-	-
WRITE SECTOR(S) EXT	M	34h	-	-	-	-	-	S	S
WRITE STREAM DMA EXT	M	3Ah	-	-	-	-	-	-	S
WRITE STREAM EXT	M	3Bh	-	-	-	-	-	-	S
WRITE VERIFY	M	3Ch	S	S	S	-	-	-	-
DEVICE CONFIGURATION IDENTIFY	I	B1h/C2h	-	-	-	-	-	S	S
IDENTIFY DEVICE	I	ECh	S	S	S	S	S	S	S
READ NATIVE MAX ADDRESS	I	F8h	-	-	-	S	S	S	S

Command Name	Category	Op Code	ATA Specification						
			1	2	3	4	5	6	7
READ NATIVE MAX ADDRESS EXT	I	27h	-	-	-	-	-	S	S
ACKNOWLEDGE MEDIA CHANGE		DBh	S	S	-	-	-	-	-
BOOT - POST-BOOT		DCh	S	S	-	-	-	-	-
BOOT - PRE-BOOT		DDh	S	S	-	-	-	-	-
CFA REQUEST EXTENDED ERROR		03h	-	-	-	S	S	S	S
CHECK MEDIA CARD TYPE		D1h	-	-	-	-	-	S	S
CHECK POWER MODE		98h	S	S	S	-	-	-	-
CHECK POWER MODE		E5h	S	S	S	S	S	S	S
CONFIGURE STREAM		51h	-	-	-	-	-	-	S
DEVICE CONFIGURATION FREEZE LOCK		B1h/C1h	-	-	-	-	-	S	S
DEVICE CONFIGURATION RESTORE		B1h/C0h	-	-	-	-	-	S	S
DEVICE RESET		08h	-	-	S	S	S	S	S
EXECUTE DEVICE DIAGNOSTIC		90h	S	S	S	S	S	S	S
GET MEDIA STATUS		DAh	-	-	-	S	S	S	S
IDENTIFY DEVICE DMA		EEh	-	-	S	-	-	-	-
IDENTIFY PACKET DEVICE		A1h	-	-	S	S	S	S	S
IDLE		97h	S	S	S	-	-	-	-
IDLE		E3h	S	S	S	S	S	S	S
IDLE IMMEDIATE		95h	S	S	S	-	-	-	-
IDLE IMMEDIATE		E1h	S	S	S	S	S	S	S
INITIALIZE DEVICE PARAMETERS		91h	S	S	S	S	S	-	-
MEDIA EJECT		EDh	-	S	S	S	S	S	S
MEDIA LOCK		DEh	S	S	S	S	S	S	S
MEDIA UNLOCK		DFh	S	S	S	S	S	S	S
NOP		00h	S	S	S	S	S	S	S
RECALIBRATE		10h	-	S	S	-	-	-	-
RECALIBRATE (X = 1..F)		1Xh	S	-	-	-	-	-	-
SECURITY DISABLE PASSWORD		F6h	-	-	S	S	S	S	S
SECURITY FREEZE LOCK		F5h	-	-	S	S	S	S	S
SECURITY UNLOCK		F2h	-	-	S	S	S	S	S
SEEK		70h	-	S	S	S	S	S	-
SEEK (X = 1..F)		7Xh	S	-	-	-	-	-	-
SERVICE		A2h	-	-	S	S	S	S	S
SET FEATURES		EFh	S	S	S	S	S	S	S
SET FEATURES: 4 BYTES OF ECC APPLY ON READ LONG/WRITE LONG COMMANDS		EFh/BBh	S	S	S	-	-	-	-
SET FEATURES: DISABLE 8-BIT DATA TRANSFERS		EFh/81h	S	S	-	-	S	S	S
SET FEATURES: DISABLE ADVANCED POWER MANAGEMENT		EFh/85h	-	-	-	S	S	S	S
SET FEATURES: DISABLE ALL AUTOMATIC DEFECT REASSIGNMENT		EFh/84h	-	-	S	-	-	-	-
SET FEATURES: DISABLE AUTOMATIC		EFh/C2h	-	-	-	-	-	S	S

Command Name	Category	Op Code	ATA Specification						
			1	2	3	4	5	6	7
ACOUSTIC MANAGEMENT FEATURE SET									
SET FEATURES: DISABLE CFA POWER MODE 1		EFh/8Ah	-	-	-	-	S	S	S
SET FEATURES: DISABLE ECC		EFh/77h	S	S	S	-	-	-	-
SET FEATURES: DISABLE MEDIA STATUS NOTIFICATION		EFh/31h	-	-	-	S	S	S	S
SET FEATURES: DISABLE POWER-UP IN STANDBY FEATURE SET.		EFh/86h	-	-	-	-	S	S	S
SET FEATURES: DISABLE READ LOOK-AHEAD FEATURE		EFh/55h	S	S	S	S	S	S	S
SET FEATURES: DISABLE RELEASE INTERRUPT		EFh/DDh	-	-	-	S	S	S	S
SET FEATURES: DISABLE RETRY		EFh/33h	S	S	S	-	-	-	-
SET FEATURES: DISABLE REVERTING TO POWER ON DEFAULTS		EFh/66h	S	S	S	S	S	S	S
SET FEATURES: DISABLE SERVICE INTERRUPT		EFh/DEh	-	-	-	S	S	S	S
SET FEATURES: DISABLE WRITE CACHE		EFh/82h	S	S	S	S	S	S	S
SET FEATURES: ENABLE 8-BIT DATA TRANSFERS		EFh/01h	S	S	-	-	S	S	S
SET FEATURES: ENABLE ADVANCED POWER MANAGEMENT		EFh/05h	-	-	-	S	S	S	S
SET FEATURES: ENABLE ALL AUTOMATIC DEFECT REASSIGNMENT		EFh/04h	-	-	S	-	-	-	-
SET FEATURES: ENABLE AUTOMATIC ACOUSTIC MANAGEMENT FEATURE SET		EFh/42h	-	-	-	-	-	S	S
SET FEATURES: ENABLE CFA POWER MODE 1		EFh/0Ah	-	-	-	-	S	S	S
SET FEATURES: ENABLE ECC		EFh/88h	S	S	S	-	-	-	-
SET FEATURES: ENABLE MEDIA STATUS NOTIFICATION		EFh/95h	-	-	-	S	S	S	S
SET FEATURES: ENABLE POWER-UP IN STANDBY FEATURE SET.		EFh/06h	-	-	-	-	S	S	S
SET FEATURES: ENABLE READ LOOK-AHEAD FEATURE		EFh/AAh	S	S	S	S	S	S	S
SET FEATURES: ENABLE RELEASE INTERRUPT		EFh/5Dh	-	-	-	S	S	S	S
SET FEATURES: ENABLE RETRIES		EFh/99h	S	S	S	-	-	-	-
SET FEATURES: ENABLE REVERTING TO POWER ON DEFAULTS		EFh/CCh	S	S	S	S	S	S	S
SET FEATURES: ENABLE SERVICE INTERRUPT		EFh/5Eh	-	-	-	S	S	S	S
SET FEATURES: ENABLE WRITE CACHE		EFh/02h	S	S	S	S	S	S	S

Command Name	Category	Op Code	ATA Specification						
			1	2	3	4	5	6	7
SET FEATURES: POWER-UP IN STANDBY FEATURE SET DEVICE SPIN-UP.		EFh/07h	-	-	-	-	S	S	S
SET FEATURES: RESERVED FOR ADDRESS OFFSET RESERVED AREA BOOT METHOD TECHNICAL REPORT		EFh/09h	-	-	-	-	S	S	S
SET FEATURES: RESERVED FOR ADDRESS OFFSET RESERVED AREA BOOT METHOD TECHNICAL REPORT		EFh/89h	-	-	-	-	S	S	S
SET FEATURES: RESERVED FOR SERIAL ATA		EFh/10h	-	-	-	-	-	-	S
SET FEATURES: RESERVED FOR SERIAL ATA		EFh/90h	-	-	-	-	-	-	S
SET FEATURES: RESERVED FOR TECHNICAL REPORT		EFh/20h	-	-	-	-	-	-	S
SET FEATURES: RESERVED FOR TECHNICAL REPORT		EFh/21h	-	-	-	-	-	-	S
SET FEATURES: SET CACHE SEGMENTS TO SECTOR COUNT REGISTER VALUE		EFh/54h	S	S	S	-	-	-	-
SET FEATURES: SET DEVICE MAXIMUM AVERAGE CURRENT		EFh/9Ah	-	-	S	-	-	-	-
SET FEATURES: SET MAXIMUM HOST INTERFACE SECTOR TIMES		EFh/43h	-	-	-	-	-	-	S
SET FEATURES: SET MAXIMUM PREFETCH USING SECTOR COUNT REGISTER VALUE		EFh/ABh	S	S	S	-	-	-	-
SET FEATURES: SET TRANSFER MODE BASED ON VALUE IN SECTOR COUNT REGISTER		EFh/03h	S	S	S	S	S	S	S
SET FEATURES: VENDOR UNIQUE LENGTH OF ECC ON READ LONG/WRITE LONG COMMANDS		EFh/44h	S	S	S	-	-	-	-
SET MAX ADDRESS		F9h	-	-	-	S	S	S	S
SET MAX ADDRESS EXT		37h	-	-	-	-	-	S	S
SET MULTIPLE MODE		C6h	S	S	S	S	S	S	S
SLEEP		99h	S	S	S	-	-	-	-
SLEEP		E6h	S	S	S	S	S	S	S
SMART DISABLE OPERATIONS		B0h/D9h	-	-	S	S	S	S	S
SMART ENABLE OPERATIONS		B0h/D8h	-	-	S	S	S	S	S
SMART ENABLE/DISABLE ATTRIBUTE AUTOSAVE		B0h/D2h	-	-	S	S	S	S	S
SMART EXECUTE OFF-LINE IMMEDIATE		B0h/D4h	-	-	-	S	S	S	S
SMART READ ATTRIBUTE THRESHOLDS		B0h/D1h	-	-	S	S	-	-	-
SMART READ ATTRIBUTE VALUES		B0h/D0h	-	-	S	S	S	S	S
SMART RETURN STATUS		B0h/DAh	-	-	S	S	S	S	S

Command Name	Category	Op Code	ATA Specification						
			1	2	3	4	5	6	7
SMART SAVE ATTRIBUTE VALUES		B0h/D3h	-	-	S	S	S	S	-
STANDBY		96h	S	S	S	-	-	-	-
STANDBY		E2h	S	S	S	S	S	S	S
STANDBY IMMEDIATE		94h	S	S	S	-	-	-	-
STANDBY IMMEDIATE		E0h	S	S	S	S	S	S	S

622
623
624
625

626 Table 4 SCSI Reduced Block Commands Category Assignments

Command Name	Catagory	OpCode
READ (10)	R	28h
FORMAT UNIT	M	04h
WRITE (10)	M	2Ah
WRITE BUFFER	M	3Bh
READ CAPACITY	I	25h
INQUIRY		12h
MODE SELECT(6)		15h
MODE SENSE(6)		1Ah
PERSISTENT RESERVE IN		5Eh
PERSISTENT RESERVE OUT		5Fh
PREVENT/ALLOW MEDIUM REMOVAL		1Eh
RELEASE(6)		17h
REQUEST SENSE		03h
RESERVE(6)		16h
START STOP UNIT		1Bh
SYNCHRONIZE CACHE		35h
TEST UNIT READY		00h
VERIFY (10)		2Fh

627
628

629 Table 5 SCSI-3 Block Commands Category Assignments

Command Name	Catagory	Op Code
READ BUFFER	R	3Ch
READ DEFECT DATA (10)	R	37h
READ DEFECT DATA (12)	R	B7h
READ LONG	R	3Eh
READ(10)	R	28h
READ(12)	R	A8h
READ(6)	R	08h
XDREAD	R	52h

Command Name	Catagory	Op Code
COPY	M	18h
COPY AND VERIFY	M	3Ah
FORMAT UNIT	M	04h
REASSIGN BLOCKS	M	07h
REBUILD	M	81h
REGENERATE	M	82h
WRITE AND VERIFY	M	2Eh
WRITE BUFFER	M	3Bh
WRITE LONG	M	3Fh
WRITE SAME	M	41h
WRITE(10)	M	2Ah
WRITE(12)	M	AAh
WRITE(6)	M	0Ah
XDWRITE	M	50h
XDWRITE EXTENDED	M	80h
XPWRITE	M	51h
READ CAPACITY	I	25h
CHANGE DEFINITION		40h
COMPARE		39h
INQUIRY		12h
LOCK-UNLOCK CACHE		36h
LOG SELECT		4Ch
LOG SENSE		4Dh
MODE SELECT(10)		55h
MODE SELECT(6)		15h
MODE SENSE(10)		5Ah
MODE SENSE(6)		1Ah
MOVE MEDIUM		A7h
Obsolete		32h
Obsolete		0Bh
Obsolete		30h
Obsolete		01h
Obsolete		31h
PERSISTENT RESERVE IN		5Eh
PERSISTENT RESERVE OUT		5Fh
PRE-FETCH		34h
PREVENT-ALLOW MEDIUM REMOVAL		1Eh
READ ELEMENT STATUS		B4h
RECEIVE DIAGNOSTIC RESULTS		1Ch
RELEASE (10)		57h
RELEASE (6)		17h
REPORT LUNS		A0h
REQUEST SENSE		03h
RESERVE (10)		56h

Command Name	Catagory	Op Code
RESERVE (6)		16h
SEEK(10)		2Bh
SEND DIAGNOSTIC		1Dh
SET LIMITS(10)		33h
SET LIMITS(12)		B3h
START STOP UNIT		1Bh
SYNCHRONIZE CACHE		35h
TEST UNIT READY		00h
VERIFY		2Fh

630
631

632 Table 6 SCSI-3 Block Commands (Optical Media) Category Assignments

Command Name	Catagory	Op code
READ BUFFER	R	3Ch
READ DEFECT DATA (10)	R	37h
READ DEFECT DATA (12)	R	B7h
READ ELEMENT STATUS	R	B8h
READ GENERATION	R	29h
READ LONG	R	3Eh
READ UPDATED BLOCK	R	2Dh
READ(10)	R	28h
READ(12)	R	A8h
READ(6)	R	08h
COPY	M	18h
COPY AND VERIFY	M	3Ah
ERASE (10)	M	2Ch
ERASE (12)	M	ACh
FORMAT UNIT	M	04h
REASSIGN BLOCKS	M	07h
UPDATE BLOCK	M	3Dh
WRITE AND VERIFY (10)	M	2Eh
WRITE AND VERIFY (12)	M	AEh
WRITE BUFFER	M	3Bh
WRITE LONG	M	3Fh
WRITE(10)	M	2Ah
WRITE(12)	M	AAh
WRITE(6)	M	0Ah
READ CAPACITY	I	25h
CHANGE DEFINITION		40h
COMPARE		39h
INQUIRY		12h
LOCK-UNLOCK CACHE		36h
LOG SELECT		4Ch

Command Name	Catagory	Op code
LOG SENSE		4Dh
MEDIUM SCAN		38h
MODE SELECT(10)		55h
MODE SELECT(6)		15h
MODE SENSE(10)		5Ah
MODE SENSE(6)		1Ah
MOVE MEDIUM		A5h
Obsolete		32h
Obsolete		01h
Obsolete		0Bh
Obsolete		B2h
Obsolete		30h
Obsolete		B0h
Obsolete		31h
Obsolete		B1h
PERSISTENT RESERVE IN		5Eh
PERSISTENT RESERVE OUT		5Fh
PRE-FETCH		34h
PREVENT-ALLOW MEDIUM REMOVAL		1Eh
RECEIVE DIAGNOSTIC RESULTS		1Ch
RELEASE(10)		57h
RELEASE(6)		17h
REQUEST SENSE		03h
RESERVE(10)		56h
RESERVE(6)		16h
SEEK(10)		2Bh
SEND DIAGNOSTIC		1Dh
SET LIMITS (10)		33h
SET LIMITS (12)		B3h
START STOP UNIT		1Bh
SYNCHRONIZE CACHE		35h
TEST UNIT READY		00h
VERIFY (10)		2Fh
VERIFY (12)		AFh

633
634

Appendix C. Traceability Matrices

In this section describes the relationship between requirements and test assertions and also, the relationship between test assertions and test cases. A cell in Table 7 marked with • means that the assertion for the cell's row is derived from the requirement in the cell's column. A cell in Table 8 marked with a • means that the test case in the cell's row tests the assertion in the cell's column.

Requirements

HWB-RM-01 A HWB shall not, after receiving an *operation of any category* from the host nor at any time during its operation, transmit any *modifying category operation* to a protected storage device.

HWB-RM-02 A HWB, after receiving a *read category operation* from the host, shall return the data requested by the read operation.

HWB-RM-03 A HWB, after receiving an *information category operation* from the host, shall return a response to the host that shall not modify any access-significant information contained in the response.

HWB-RM-04 Any error condition reported by the storage device to the HWB shall be reported to the host.

Test Assertions

HWB-AM-01 The HWB shall not transmit any modifying category operation to the protected storage device.

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-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.

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.

Test Cases

HWB-01 Identify commands blocked by the HWB.

HWB-02 Identify modifying commands blocked by the HWB.

HWB-03 Identify commands blocked by the HWB while attempting to modify a protected drive with forensic tools.

HWB-04 Attempt to modify a protected drive with forensic tools.

HWB-05 Identify read commands allowed by the HWB.

HWB-06 Identify read and information commands used by forensic tools and allowed by the HWB.

HWB-07 Read a protected drive with forensic tools.

HWB-08 Identify access significant information unmodified by the HWB.
HWB-09 Determine if an error on the protected drive is returned to the host.

Table 7 Requirements and Assertions Traceability Matrix

		Requirements			
		RM-01	**RM-02**	**RM-03**	**RM-04**
Assertions	**AM-01**	●			
	AM-02		●		
	AM-03			●	
	AM-04				●
	AM-05	●			

Table 8 Assertions and Test Cases Traceability Matrix

		Assertions				
		AM-01	**AM-02**	**AM-03**	**AM-04**	**AM-05**
Test Cases	**HWB-01**	●				●
	HWB-02	●				
	HWB-03	●				●
	HWB-04	●				
	HWB-05		●			
	HWB-06		●	●		●
	HWB-07		●	●		
	HWB-08			●		
	HWB-09				●	

Appendix D. Optional Scheme for Variation Designations

This section describes a scheme for naming test case variations. Each variation is designated by a code of 5 characters appended to the test case ID to create a unique test case identifier. The following scheme is recommended, but not required:

HWB-WW-XYYYZ where

WW is the test case number.
X indicates the variation class as follows: **B** for boot, **R** for restore, **F** for file system application and **A** for image acquisition.
YYY identifies a unique aspect of the variation.
Z indicates an option switch setting if present.

Table 9 Examples of Test Case Variation Designations

Designation	Comments
HWB-03-BWXP	Boot variation for Windows XP.
HWB-03-RE28	Restore variation using EnCase to a drive with 28 bit sector addressing.
HWB-03-RI48	Restore variation using iLook to a drive with 48 bit sector addressing.
HWB-03-F28	File system application to a drive with 28 bit sector addressing.
HWB-03-F48	File system application to a drive with 48 bit sector addressing.
HWB-03-BWXP3	Device switch setting 3 for boot variation for Windows XP. The meaning of switch setting 3 would be defined in the test report.
HWB-06-AD28	Acquisition of a small drive from a DOS based imaging tool.
HWB-06-AW48	Acquisition of a partition on a large drive from a Windows based imaging tool.