May 19, 2004

Hardware Write Blocker Device (HWB) Specification

Version 2.0 May 19, 2004

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

Abstract[1]

This document defines functional requirements for hardware write blocker (HWB) devices used in computer forensics investigations. It does not define requirements for protecting storage devices from misuse, either intentional or not intentional. It defines the requirements for ensuring that data on a storage device is not altered and that data from and about the storage device can be obtained.

These requirements will be used to derive test assertions, test cases, and a test plan. The test assertions, test cases, and test plan will be published as a separate document. 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 our 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

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, 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; NIST's Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL); and is supported by other organizations, including the Federal Bureau of Investigation, the Department of Defense Cyber Crime Center, and the Department of Homeland Security's Bureau of Immigration and Customs Enforcement and 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.

1.1 Overview

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.

1.2 Change Summary

Several changes based on comments received were made to Version 1.0 to produce Version 2.0 of this specification.

1. Removed requirements for optional features.
2. Performed stylistic editorial changes.
3. Clarified that "misuse" of a storage device is out of scope.
4. Reframed concept of "command" to more generic/flexible concept of "command operations".
5. Redefined command operation categories.
6. Clarified general HWB functions (protect and access).
7. Reframed requirements to account for:
    - command operation categorizations

- flexibility for variations in design and implementation of HWB devices

For Example:

- Version 1.0 requirement RM-01 was reworded to cover not only blocking modifying commands sent from the host, but also to not allow the device to generate any modifying commands.
- Version 1.0 requirements RM-02 and RM-03 were combined and modified to allow the HWB device to consolidate read (and other non-modifying) requests.

8. Removed redundant terminology ("firmware").
9. Introduced new terms where necessary ("access-significant information"). This is descriptive information about a drive that if changed by the HWB device would affect the ability to access information on the device. For example, if the number of sectors was underreported, software that accessed the device might not try to access all information stored on the device.
10. Added new requirements that:
    - protect "access-significant information" from change by the HWB
    - make sure the host has access to any available error information
11. Clarified the use of examples for command category operations instead of using exhaustive command set listings.
12. Added a *Command Operation Categories* section.

2 Purpose

This document defines functional requirements for hardware write blocker (HWB) devices used in computer forensics investigations. It does not define requirements for protecting storage devices from misuse, either intentional or not intentional. It defines the requirements for ensuring that data on a storage device is not altered and that data from and about the storage device can be obtained.

These requirements will be used to derive test assertions, test cases, and a test plan. The test assertions, test cases, and test plan will be published as a separate document. 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 our web site at http://www.cftt.nist.gov.

3 Background Information

Data is written to or read from a storage device via commands that are issued by the computer and transmitted from the computer's interface connection to the storage device's interface connection. A hardware write blocker (HWB) is a hardware device that attaches to a computer system with the primary purpose of intercepting and preventing (or ‘blocking’) any modifying command operation from ever reaching the storage device. Physically, the device is connected between the computer and a storage device. Some of its functions include monitoring and filtering any activity that is transmitted or received between its interface connections to the

computer and the storage device.

The interface connections do not have to be the same type. For example, the computer connection to a HWB could be using a SCSI interface while the HWB connection to the hard disk could be using an IDE interface. Any assumptions that are made about either the data that the HWB is protecting or about the functions of the HWB itself are based entirely on the notion that the capabilities of the HWB are limited by the capabilities of its interfaces.

4 Terminology

Included here are definitions that define key terms or variations of key terms used in this specification. Most definitions are from the Working draft document (WD) of the Millennial Edition of the American National Standard Dictionary of Information Technology (ANSDIT), developed by the American National Standards Institute (ANSI), National Committee for Information Technology Standards (NCITS), the Technical Committee on Vocabulary, K5. The ANSDIT has been harmonized with ISO/IEC-2382, Information Technology Vocabulary (ITV). [http://www.ncits.org/tc_home/k5htm/Ansdit.htm]

access-significant information: Information contained within the response to an *information category operation* that is significant to locating and accessing data stored on the device. For example, the total number of sectors reported for a given storage device is significant to locating all data on the device.

command: (1)An order for an action to take place. (2) A control signal. … [ANSI]

firewire: A colloquial term referring to an external bus standard that supports data transfer rates of up to 400Mbps (IEEE Standard 1394a) and 800Mbps (IEEE Standard 1394b). The term ‘FireWire’ was trademarked by Apple.

Integrated Drive Electronics/AT Attachment (IDE/AT) Interface: A colloquial term for interface standards developed by T13. Technical Committee T13 is responsible for all interface standards relating to the AT Attachment (ATA) storage interface utilized as the disk drive interface on personal and mobile computers. T13 is a Technical Committee for the InterNational Committee on Information Technology Standards (INCITS) **[**http://www.incits.org/**].** INCITS is accredited by, and operates under rules approved by, the American National Standards Institute [ANSI] [http://www.ansi.org/].

interface: A shared boundary defined by the characteristics of that boundary. The interface may be described at the physical level, at the software level, or as purely logic operations. For example, characteristics of the boundary may include the identification of any physical interconnections, description of signal exchanges across the boundary, or specification of functions performed on each side of the boundary. [ANSI]

modification: (1) An addition or change to stored data or a deletion of stored data. …[ANSI]

read: To obtain data from an input device, from a storage device, or from a data medium. [ANSI]

storage device: A functional unit into which data can be placed, in which they can be retained, and from which they can be retrieved. [ANSI]

protected storage device: A storage device whose interface is connected to a HWB.

Small Computer System Interface (SCSI): A colloquial term for interface standards developed by T10. Technical Committee T10 is responsible for SCSI Storage Interfaces and SCSI architecture standards (SAM, SAM-2, and SAM-3), which are used by SCSI, SAS, Fibre Channel, SSA, IEEE 1394, USB, and ATAPI. T10 is also responsible for many SCSI command set standards (e.g., SPC, SPC-2, SPC-3, SBC, SBC-2, SSC, SSC-2, SSC-3, MMC, MMC-2, MMC-3, MMC-4, RBC, etc.). T10 is a Technical Committee of the InterNational Committee on Information Technology Standards (INCITS) [http://www.incits.org]. INCITS is accredited by, and operates under rules that are approved by, the American National Standards Institute (ANSI) [http://www.ansi.org].

transmit: To send from one location for reception elsewhere. ... [ANSI]

Universal Serial Bus (USB): A colloquial term referring to external bus standards that support data transfer rates of up to 480 Mbps for high-speed connection of peripheral equipment to microcomputers.

write: To send data to an output unit, to a storage device, or to a data medium. [ANSI]

5 Scope

The scope of this specification is limited to hardware devices that protect the contents of a computer hard drive or other storage media. The specifications are general and are based on the following assumptions.

1. Operations that could modify data on the storage device are controllable at the interface level (i.e., outside of the storage device itself). Any possible operations that can take place inside of the storage device that are not accessible or controllable via the interface functionality are outside the scope of this specification.

2. Any backward compatibility of a given HWB device is based primarily on the backward compatibility of its implemented interfaces. If the interface specifications mandate certain backward compatibilities, the assumption is that those backward compatibilities exist.

3. All devices are in a working computer system configuration. At a very minimum, a device is considered as being in a "working" state if it is connected to a powered-on host system and

can receive interface commands and issue a response for those commands.

4. Any changes to the computer system configuration to install the HWB must be technically sound and compatible with the respective interface specifications. An example of changes to the configuration would be the installation of a PCI-SCSI adapter card to support a SCSI-IDE HWB device.

5. The HWB is being used in a non-hostile environment. The assumption is that the environment in which these devices are used is controlled by individuals that are adhering to the intended use of the device. Preventing misuse of the storage device is outside the scope of this document.

6. The scope of the specification will be limited to the following interfaces: ATA, SCSI, USB, and Firewire.

6 Command Operation Categories

Each interface command represents one or more distinct operations. Every operation must exist in only one category. The commands of each interface and their associated operations can be partitioned into the following *command operation categories*:

- **Modifying :** Any operation that:
    1. directly causes a modification
    2. could ***potentially*** cause a modification
    3. is a necessary pre-requisite for a modification
    4. is undefined in the interface specifications
    5. changes how the storage device is presented to the host
    6. changes any of the storage device's configurable parameters
- **Read:** Any operation that requests data which is stored at specific locations on a storage device's medium and returns that data to the host. A read operation requests one or more blocks of data from the storage device's medium. Each block of data is specified by a location on the medium and a length.
- **Information:** Any operation that requests data which is not stored on a storage device's medium and returns that data to the host.
- **Other Non-Modifying:** Any operation not existing in any of the other operation categories that requests the storage device to perform a nondestructive action.

Examples of ATA and SCSI interface *command operations* are given in the appendix.

Categorization and Grouping of Command Operations

The categorization of interface commands was partitioned into operations to account for the fact that some commands have multiple sub-commands associated with them that perform various functions. These command operations were grouped into mutually exclusive groups or

categories. These categorizations were performed serially starting first with the assignment of operations to the Modifying category, then, respectively, to the Read, Information, and Other Non-Modifying categories. Thus, with each subsequent categorization, the number of unassigned operations available for classification was reduced until all operations had been categorized. This categorization sought to account for command operations not only in the current interface specification revisions, but also those in previous versions.

7 Mandatory Requirements

General hardware write blocker (HWB) functions could be described as: a HWB should not allow modifying command operations to be transmitted to a storage device and should allow retrieval of all accessible data on the storage device.

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.

Appendix - Interface Command Examples

The tables below are listings of some ATA and SCSI command operations. A HWB device should block modifying command operations. Testing command operations in each category will be discussed in the test plan for HWB.

Table 1 ATA Examples

Command Operation Name	Operation Code	Category
WRITE SECTOR(S) (w/ retry)	0x30	Modifying
READ SECTOR(S) (w/ retry)	0x20	Read
IDENTIFY DEVICE	0xEC	Information
IDLE	0xE3	Other Non-Modifying

Table 2 SCSI Examples

Command Operation Name	Operation Code	Category
WRITE (10)	0x2A	Modifying
READ (10)	0x28	Read
INQUIRY	0x12	Information
START STOP UNIT	0x1B	Other Non-Modifying