October 29, 2003

DRAFT

Hardware Write Blocker Device (HWB)

Specification

Version 1.0

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

Table Of 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 and objective 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 participates 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 using a software tool or hardware device to block modification of the contents of a drive.

2 Purpose

This document defines functional requirements for hardware write blocker (HWB) devices used in computer forensics investigations.

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 are experts 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 commands 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. 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. [See Addendum for examples of interface commands]

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]

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.

firmware: An ordered set of instructions and associated data stored in a manner that they are considered part of the hardware configuration as distinct from the software that is dynamically loaded as needed; for example, microprograms stored in read-only memory. Firmware may be implemented in hardware logic or stored in read-only memory; it may be addressed as part of the memory address space or be entirely separate. [ANSI]

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/]. [see Addendum for ATA interface commands]

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]. [see Addendum for SCSI interface commands]

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 (ie, 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.

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

6 Requirements

General hardware write blocker (HWB) functions could be described as: a HWB should not allow modifying commands to be transmitted to a storage device and should allow non-modifying commands to be transmitted a storage device.

Non-modifying commands are those that either read or gather information from a storage device. Modifying commands are all others including those that write to a storage device. Examples of ATA and SCSI interface commands are given in the addendum.

6.1 Requirements for Mandatory Features

HWB-RM-01 A HWB shall block modifying commands to a protected storage device.

HWB-RM-02 A HWB shall allow non-modifying commands to be transmitted to a protected storage device.

HWB-RM-03 A non-modifying command that enters the HWB shall be equivalent to the command that exits the HWB.

HWB-RM-04 The response that is transmitted from the protected storage device to the HWB shall be equivalent to what is transmitted from the HWB to the computer.

6.2 Requirements for Optional Features

The following requirements define optional device features. If a HWB device provides the capability defined, then the tool will be tested as if the requirement were mandatory. If the device does not provide the capability defined, the requirement will not apply.

HWB-RO-01 A HWB shall provide the capability to have a storage device either protected or not protected.

HWB-RO-02 A HWB shall provide the capability to protect a storage device's firmware.

HWB-RO-03 A HWB shall provide the capability to indicate a successful response for blocked commands.

HWB-RO-04 A HWB shall provide the capability to indicate a failed response for blocked commands.

HWB-RO-05 A HWB shall provide the capability to indicate that it is operational.

Addendum - Interface Command Examples

These tables are listings of some ATA and SCSI commands. A HWB device should block modifying commands and not block non-modifying commands. Testing commands in the configuration category will be discussed in the test plan for HWB.

ATA

Command	Hex Code	Category
CFA Erase Sectors	Coh	Modifying
CFA Request Extended Error Code	03h	Non-modifying
CFA Translate Error	87h	Non-modifying
CFA Write Multiple Without Erase	CDh	Modifying
CFA Write Sectors Without Erase	38h	Modifying
Check Power Mode	E5h	Non-modifying
Device Reset	08h	Configuration
Download Microcode	92h	Modifying
Execute Device Diagnostic	90h	Non-modifying
Flush Cache	E7h	Modifying
Get Media Status	DAh	Non-modifying
Identify Device	ECh	Non-modifying
Identify Packet Device	A1h	Non-modifying
Idle	E3h	Non-modifying
Idle Immediate	E1h	Non-modifying
Initialize Device Parameters	91h	Configuration
Media Eject	EDh	Non-modifying
Media Lock	DEh	Non-modifying
Media Unlock	DFh	Non-modifying
NOP	00h	Non-modifying
Packet	A0h	Non-modifying
Read Buffer	E4h	Non-modifying
Read DMA	C8h	Non-modifying
Read DMA Queued	C7h	Non-modifying
Read Multiple	C4h	Non-modifying
Read Native Max Address	F8h	Non-modifying
Read Sector(s)	20h	Non-modifying
Read Verify Sector(s)	40h	Non-modifying
Security Disable Password	F6h	Configuration
Security Erase Prepare	F3h	Configuration
Security Erase Unit	F4h	Modifying
Security Freeze Lock	F5h	Modifying
Security Set Password	F1h	Modifying
Security Unlock	F2h	Configuration
Seek	70h	Non-modifying

Service	A2h	Configuration
Set Features	EFh	Configuration
Set Max Address	F9h	Configuration
Set Max Set Password	F9h	Configuration
Set Max Lock	F9h	Configuration
Set Max Unlock	F9h	Configuration
Set Max Freeze Lock	F9h	Configuration
Set Multiple Mode	C6h	Configuration
Sleep	E6h	Configuration
SMART Disable Operations	B0h	Configuration
SMART Enable/Disable Attribute Autosave	B0h	Configuration
SMART Enable Operations	B0h	Configuration
SMART Execute Off-line Immediate	B0h	Configuration
SMART Read Data	B0h	Non-modifying
SMART Read Log	B0h	Non-modifying
SMART Return Status	B0h	Non-modifying
SMART Save Attribute Values	B0h	Modifying
SMART Write Log	B0h	Modifying
Standby	E2h	Non-modifying
Standby Immediate	E0h	Non-modifying
Write Buffer	E8h	Modifying
Write DMA	CAh	Modifying
Write DMA Queued	CCh	Modifying
Write Multiple	C5h	Modifying
Write Sector(s)	30h	Modifying

SCSI

Length	Command	Hex Code	Category
6	Change Definition	40h	Configuration
6	Compare	39h	Non-modifying
6	Copy	18h	Modifying
6	Copy and Verify	3Ah	Modifying
6	Erase	19h	Modifying
10	Erase	2Ch	Modifying
6	Format Unit	04h	Modifying
6	Inquiry	12h	Non-modifying
6	Lock/Unlock Cache	36h	Non-modifying
6	Log Select	4Ch	Modifying
6	Log Sense	4Dh	Modifying
6	Mode Select	15h	Configuration
10	Mode Select	55h	Configuration
6	Mode Sense	1Ah	Non-modifying
10	Mode Sense	5Ah	Non-modifying
6	Pre-Fetch	34H	Configuration

Length	Command	Hex Code	Category
6	Prevent/Allow Medium Removal	1Eh	Non-modifying
6	Read Block Limits	05H	Non-modifying
6	Read Buffer	3Ch	Non-modifying
6	Read Capacity	25h	Non-modifying
10	Read Defect Data	37h	Non-modifying
6	Read Generation	29h	Non-modifying
6	Read Long	3Eh	Non-modifying
6	Read Reverse	0Fh	Non-modifying
6	Read Updated Block	2Dh	Non-modifying
6	Read	08h	Non-modifying
10	Read	28h	Non-modifying
6	Reassign Blocks	07h	Modifying
6	Receive Diagnostic Results	1Ch	Non-modifying
6	Recover Buffered Data	14h	Non-modifying
6	Release	17h	Non-modifying
6	Request Sense	03h	Non-modifying
6	Reserve	16h	Non-modifying
6	Rezero Unit	01h	Configuration
10	Search Data Equal	31h	Non-modifying
10	Search Data High	30h	Non-modifying
10	Search Data Low	32h	Non-modifying
6	Seek	0Bh	Non-modifying
10	Seek	2Bh	Non-modifying
6	Send Diagnostic	1Dh	Non-modifying
10	Set Limits	33h	Configuration
6	Set Window	24h	Configuration
6	Space	11h	Configuration
6	Start/Stop Unit	1Bh	Non-modifying
6	Synchronize Cache	35h	Configuration
6	Test Unit Ready	00h	Non-modifying
6	Verify	13h	Non-modifying
10	Verify	2Fh	Non-modifying
10	Write and Verify	2Eh	Modifying
6	Write Buffer	3Bh	Modifying
6	Write Filemarks	10h	Modifying
6	Write Long	3Fh	Modifying
6	Write Same	41h	Modifying
6	Write	0Ah	Modifying
10	Write	2Ah	Modifying