January 9, 2008

Forensic Media Preparation Tool Test Assertions and Test Plan

Draft 1 for Public Comment of Version 1.0

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

Abstract

Storage devices, such as disk drives, are often reused from one investigation to the next. An investigator needs to ensure that data from an earlier investigation does not inadvertently become included in another investigation. Before a storage device is used in an investigation the device needs to be prepared in a forensically sound manner for use by overwriting the user data areas with forensically benign data.

This paper defines test assertions and a test plan for testing tools and devices used in the preparation of storage devices used in a forensic examination of digital data. These test assertions are derived from *Forensic Storage Media Preparation Tool Specification, Version 1.0*. The test plan can be used to determine whether a specific tool meets the requirements. The test assertions describe specific statements of conditions that can be checked after a test is executed. Each assertion generates one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

As this document evolves updated versions will be posted at http://www.cftt.nist.gov

TABLE OF CONTENTS

1. Introduction

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. A means is required to ensure that forensic tools consistently produce accurate, repeatable and objective test results. The goal of the Computer Forensic Tool Testing project at the National Institute of Standards and Technology is to establish a methodology for testing computer forensic tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results of this working methodology provides helpful information toolmakers can use to improve their tools, so that users of these tools can make informed choices about acquiring and using computer forensic tools, and for interested parties to better understand a tools given capabilities. Our 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 Computer Forensic Tool Testing 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 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, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and the U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

2. Purpose

Storage devices, such as disk drives, are often reused from one forensic investigation to the next. An investigator needs to ensure that data from an earlier investigation does not inadvertently become included with the current investigation. Before a storage device is used in an investigation the device needs to be *prepared* for reuse in a forensically sound manner by overwriting the user data areas with benign (intended) data.

This paper defines test assertions and a test plan for testing tools and devices used in the preparation of storage devices used in a forensic examination of digital data. These test assertions are derived from *Forensic Storage Media Preparation Tool Specification, Version 1.0*. The test plan is used to determine whether a specific tool conforms to the requirements.

These requirements are used to then derive test assertions and test methods that determine whether a specific tool meets stated requirements. The test assertions describe specific statements of conditions that can be checked after a test is executed. Each assertion generates one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

3. Scope

The test assertions and test cases defined in this document are based on requirements for tools that overwrite or erase storage devices intended for reuse within an organization. These requirements are not for recycling or disposal of digital media. If a digital storage device is being released, recycled or otherwise disposed of from an organization then NIST Special Publication SP 800-88, *Guidelines for Media Sanitization* (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf) should be referenced.

Forensic media preparation for internal reuse within an organization assumes the following:

- An active effort to recover overwritten data is not occurring. In other words, since the digital storage device is staying within the same organization any data on the device would be accessible anyway.
- The use of these tools is not to determine if the storage device is working properly. In other words, trying to determine if a storage device is in working order is beyond the scope of these requirements.

4. Test Assertions

This section lists test assertions for forensic media preparation. The test assertions are divided into two groups: core test assertions that apply to all tools and optional feature test assertions that only apply if the tool under test supports some optional tool feature.

4.1 Core Test Assertions

Forensic media preparation tools overwrite the existing data present on the storage device with forensically benign data. The data used may be either defined by the tool or optionally selected by the user via the optional overwrite pattern selection feature.

FMP-CA-01. All visible sectors shall be overwritten with the specified benign data.

4.2 Optional Feature Test Assertions

Three optional features are identified: hidden area overwriting, overwrite command selection, and overwrite pattern selection. Evaluation of overwrite pattern selection is included in evaluation of assertion FMP-CA-01 a separate assertion is not defined.

4.2.1 Hidden area overwriting assertions

A hidden area may be present on a storage device either as a *host protected area* (HPA), a *device configuration overlay* (DCO) or a combination of both. A tool may make some, all or none of the hidden sectors visible by removing an HPA only, both HPA and DCO or not removing either from the storage device. After a tool finishes a hidden area may have been either removed or restored to its initial configuration.

FMP-AO-01. If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data.

FMP-AO-02. A hidden area may optionally be removed from the storage device.

4.2.2 Overwrite command selection assertions

Overwriting can be accomplished primarily in one of two ways. Either the tool is using some kind of WRITE command to overwrite each sector or the tool is using a command built into the hard drive, such as the ATA SECURITY ERASE UNIT command or the SCSI ERASE command, to overwrite the drive. Note that the ATA SECURITY ERASE UNIT command is executed in one of two modes: *normal erase mode* and *extended erase mode*. A disk drive may support either one or both modes.

Note that the SECURITY ERASE UNIT command defined in the ATA protocol is not required to erase sectors within a DCO or HPA. However, a tool may be designed to remove a hidden area before executing an ERASE command. The tool may then optionally restore the hidden area after the command is finished.

FMP-AO-03. If the tool supports overwrite command selection and an ERASE command is selected then all visible sectors are overwritten.

FMP-AO-04. If an overwrite command is selected and the storage device does not support the command then the user is notified.

4.3 Evaluating Conformance to Test Assertions

This section discusses evaluating conformance to the test assertions.

Forensic media preparation tools overwrite the existing data present on the storage device with forensically benign data. Examples of overwriting with forensically benign data include the following:

- Replace each byte of original data with binary zeros.
- Replace each byte of original data with a constant byte value.

- Replace multiple bytes of original data with a fixed pattern.
- Replace multiple bytes of original data with a varying pattern.
- Replace each byte of original data with a random byte value.
- Use some other scheme such that there is no general relationship between the original byte and the replacement byte and no meaning, either observed or implied can be associated with the replacement content.

4.3.1 FMP-CA-01

All visible sectors shall be overwritten with the specified benign data.

The general protocol for evaluating the overwriting of a storage device is as follows:

1. Initialize the test drive with the **diskwipe** program from the FS-TST package available from http://www.cftt.nist.gov/diskimaging/fs-tst20.zip.
2. Run the forensic media preparation tool.
3. Analyze the test drive by counting the number of times each possible byte value (from 0x00 through 0xFF) appears.
4. Perform an analysis to determine if the results are consistent with the tool specification.
5. If the tool allows specification of an overwrite pattern, the contents of the drive after executing the tool shall be consistent with the specified pattern.

4.3.2 FMP-AO-01

If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data.

The protocol for evaluating wiping of a storage device with a hidden area is as follows:

1. Initialize the test drive with the **diskwipe** program from the FS-TST package available from http://www.cftt.nist.gov/diskimaging/fs-tst20.zip.
2. Create a hidden area on the test drive.
3. Run the forensic media preparation tool.
4. Evaluate FMP-AO-02 to determine the final state of the hidden area left by the tool under test.
5. Analyze the test drive by counting the number of times each possible byte value (from 0x00 through 0xFF) appears.
6. Determine by analysis if the results are consistent with the tool specification.

4.3.3 FMP-AO-02

A hidden area may optionally be removed from the storage device.

To evaluate the final state of the hidden area, determine the number of visible sectors on the test drive.

4.3.4 FMP-AO-03

If the tool supports overwrite command selection and an ERASE command is selected then all visible sectors are overwritten.

Follow the protocol for evaluating FMP-CA-01 (if there is no hidden area) or FMP-AO-01 (if there is a hidden area) as appropriate.

4.3.5 FMP-AO-04

If an overwrite command is selected and the storage device does not support the command then the user is notified.

When attempting to use an ERASE command on a drive that does not support the ERASE command, note the tool's behavior.

5. Test Cases

Five test cases are defined as follows:

FMP-01. Overwrite visible sectors using WRITE commands.
FMP-02. Overwrite visible sectors using an ERASE command.
FMP-03. Overwrite hidden sectors using WRITE commands.
FMP-04. Overwrite hidden sectors using an ERASE command.
FMP-05. Detect drive not supporting ERASE command.

Not all test cases apply to all tools. Some tools support the write command while others use the erase command. A tool that supports both may or may not allow selection by the user. Some hard drives support the secure erase while others do not. The command used by the tool may not be documented for the tool. Based on the tools available at the end of 2008, most tools use a WRITE command to overwrite the storage device and do not support the ERASE command. Therefore test cases FMP-01 and FMP-03 should be used if the tool documentation makes no mention of the ERASE command.

A test case may be executed more than once with some relevant parameter varied to increase test coverage. This is called a test case variation. The variations executed depend on tool features supported. There are several categories of parameters that can lead to variations: interface type (e.g., ATA, SATA, eSATA, FireWire or USB), storage device size (for ATA and SATA drives with either 28 bit addressing or 48 bit addressing), type of ERASE command supported (normal mode or extended mode), hidden area type (e.g., device configuration overlay or host protected area), wipe pattern (as offered by the tool), number of wipe passes (1 or more) and wipe verification. Each tool option should be selected at least once for some test case and also not selected for at least one test case. Note that some features such as number of wipe passes or wipe verification are not addressed by any test assertions and are therefore these features of the tool under test are not checked for conformance to any specification. However, using these features ensures that their selection does not affect the assertions being tested.

Each test case is described in a box as follows:

Item	Description
Case number:	A unique identifier for the test case.
Test Summary:	A brief description of the test case.
Assertions Tested:	A list of the test assertions evaluated by the test case.
Variations:	A test case may be run more than once with some test parameters taking on different values.
Comments:	Additional information about the test case.
Test Setup:	Write a unique non-zero value to each sector of the test drive.
Expected Results:	Every sector of the test drive is overwritten.

5.1 Overwrite visible sectors using WRITE commands.

Item	Description
Case number:	FMP-01
Test Summary:	Overwrite visible sectors using WRITE commands.
Assertions Tested:	FMP-CA-01 All visible sectors shall be overwritten with the specified benign data.
Variations:	(interface) ATA28 (28 bit addressing) ATA48 (48 bit addressing) SATA28 (28 bit addressing) SATA48 (48 bit addressing) SCSI USB FireWire
Comments:	
Test Setup:	Write a unique non-zero value to each sector of the test drive.
Expected Results:	Every sector of the test drive is overwritten.

5.2 Overwrite visible sectors using an ERASE command.

Item	Description
Case number:	FMP-02
Test Summary:	Overwrite visible sectors using an ERASE command.
Assertions Tested:	FMP-AO-03 If the tool supports overwrite command selection and an ERASE command is selected then all visible sectors are overwritten.

Item	Description
Variations:	(interface, command) interface = ATA28 (28 bit addressing) ATA48 (48 bit addressing) SATA28 (28 bit addressing) SATA48 (48 bit addressing) SCSI Command = N (ATA SECURITY ERASE UNIT normal mode) X (ATA SECURITY ERASE UNIT normal mode) S (SCSI ERASE command)
Comments:	
Test Setup:	Test drive must support an ERASE command. Write a unique non-zero value to each sector of the test drive.
Expected Results:	Every sector of the test drive is overwritten.

5.3 Overwrite hidden sectors using WRITE commands.

Item	Description
Case number:	FMP-03
Test Summary:	Overwrite hidden sectors using WRITE commands.
Assertions Tested:	FMP-CA-01 All visible sectors shall be overwritten with the specified benign data. FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data. FMP-AO-02 A hidden area may optionally be removed from the storage device.
Variations:	(hidden area) HPA DCO DCO+HPA
Comments:	
Test Setup:	Write a unique non-zero value to each sector of the test drive. Create a hidden area on the test drive.
Expected Results:	Every sector of the test drive is overwritten. Status of hidden area is documented.

5.4 Overwrite hidden sectors using an ERASE command.

Item	Description
Case number:	FMP-04
Test Summary:	Overwrite hidden sectors using an ERASE command.
Assertions Tested:	FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data. FMP-AO-02 A hidden area may optionally be removed from the storage device. FMP-AO-03 If the tool supports overwrite command selection and an ERASE command is selected then all visible sectors are overwritten.
Variations:	(hidden area) HPA DCO DCO+HPA
Comments:	
Test Setup:	Test drive must support an ERASE command. Write a unique non-zero value to each sector of the test drive. Create a hidden area on the test drive.
Expected Results:	Every sector of the test drive is overwritten. Status of hidden area is documented.

5.5 Detect drive not supporting ERASE command.

Item	Description
Case number:	FMP-05
Test Summary:	Detect drive not supporting ERASE command.
Assertions Tested:	FMP-AO-04 If an overwrite command is selected and the storage device does not support the command then the user is notified.
Variations:	None
Comments:	
Test Setup:	Test drive must not support an ERASE command. Write a unique non-zero value to each sector of the test drive.
Expected Results:	Every sector of the test drive is overwritten.

Appendix A. Traceability Matrices

Test Assertions

FMP-CA-01 All visible sectors shall be overwritten with the specified benign data.
FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data.
FMP-AO-02 A hidden area may optionally be removed from the storage device.
FMP-AO-03 If the tool supports overwrite command selection and an ERASE command is selected then all visible sectors are overwritten.
FMP-AO-04 If an overwrite command is selected and the storage device does not support the command then the user is notified.

Table 1 Requirements to Assertions

	Test Assertions					
Requirements[1]		CA-01	AO-01	AO-02	AO-03	AO-04
	CR-01	•				
	RO-01		•			
	RO-02			•		
	RO-03				•	
	RO-04					•
	RO-05	•				

Test Cases

FMP-01. Overwrite visible sectors using WRITE commands.
FMP-02. Overwrite visible sectors using an ERASE command.
FMP-03. Overwrite hidden sectors using WRITE commands.
FMP-04. Overwrite hidden sectors using an ERASE command.
FMP-05. Detect drive not supporting ERASE command.

Table 2 Test Assertions to Test Cases

	Test Assertions					
Test Cases		CA-01	AO-01	AO-02	AO-03	AO-04
	FMP-01	•				
	FMP-02				•	
	FMP-03	•	•	•		
	FMP-04		•	•	•	
	FMP-05					•

[1] See Forensic Storage Media Preparation Tool Specification, Version 1.0 for description of requirements.