January 9, 2009

Forensic Storage Media Preparation Tool Specification

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 one investigation does not inadvertently become included in another investigation. Before a storage device is used in an investigation the storage 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 requirements established by the Computer Forensic Tool Testing Project at the National Institute of Standards and Technology for the preparation of storage devices used in a forensic examination of digital data. These requirements are used to derive test assertions and test methods used to determine whether a specific tool meets the requirements. The 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 (CFTT) project at the National Institute of Standards and Technology (NIST) 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 information necessary for toolmakers to improve their tools, for users of these tools to make informed choices about acquiring and using computer forensic tools, and for interested parties to better understand a tool's capabilities. Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing. The materials and description of this project are located 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 investigation to the next. An investigator needs to ensure that data from an earlier investigation does not inadvertently become included 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 requirements established by the Computer Forensic Tool Testing Project at the National Institute of Standards and Technology for the preparation of digital storage devices used in a forensic examination of digital data. The storage device would be attached either to a computer or another electronic device for erasure.

These requirements are used to derive test assertions and test methods used to determine whether a specific tool meets the requirements. The assertions are described as general

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. The test assertions, test methods and test protocols are found in an accompanying document, *Forensic Media Preparation Tool Test Assertions and Test Plan*, located on the CFTT web site, http://www.cftt.nist.gov/.

3. Scope

This specification defines 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 digital media is being released, recycled or otherwise disposed of from an organization see NIST Special Publication SP 800-88, *Guidelines for Media Sanitization* (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf) for guidance.

These requirements only cover the final result of the tool operation. Desirable features that are problematic to test are not included. Omission of such features from these requirements does not imply that the features should not be implemented in actual tools. For example, one such desirable feature is for the tool to include a verify phase to check that the drive actually has been overwritten. However, to test that the tool can detect that part of a drive has not actually been overwritten would require that there exists a capability to either make the overwrite of original data fail or to allow modification of drive contents between the overwrite phase and the verify phase. Such a capability is unlikely and undesirable since it endangers the integrity of tool operation.

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 was already accessible.
- Although some tools may include features to detect improper storage device operation, the primary use of these tools is to overwrite the existing data on the storage device, not to determine if the storage device is working properly. In other words, testing if a tool can determine if a storage device is in working order is beyond the scope of these requirements.

4. Background

The storage device used to contain digital data or digital evidence during a forensic examination should be *initialized* to contain forensically benign data such as binary zeros. Other forensically benign data that may be used to overwrite storage include either a fixed data pattern or random data. Any residual data should be overwritten so that there is no possibility of inadvertent inclusion of unrelated data from a storage device into an investigation.

Digital storage devices can be initialized by either overwriting all data areas with forensically benign data or by using the built-in commands of a hard drive to erase all data. A digital storage device may be attached to a host computer by one of several interfaces. These include ATA (AT Attachment), SATA (Serial ATA), eSATA (External Serial ATA), SCSI (Small Computer System Interface), USB (Universal Serial Bus), and FireWire. For ATA and SATA hard drives, the SECURITY ERASE UNIT command (see http://www.t13.org) overwrites a hard drive. A similar command, ERASE, is defined for the SCSI interface (see http://www.t10.org). Additional discussion of disk drive sanitization and erasure can be found in *Tutorial on Disk Drive Data Sanitization* (http://cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf) and *CMRR Protocols for Disk Drive Secure Erase* (http://cmrr.ucsd.edu/people/Hughes/CmrrSecureEraseProtocols.pdf).

ATA hard drives may have hidden data areas that must be made visible by commands sent to the hard drive. A *device configuration overlay* (DCO) may be present that makes the drive appear smaller than the real drive capacity. In addition, a *host protected area* (HPA) may be defined either alone or on top of a DCO to create a hidden area on a hard drive. If a DCO or HPA is present on a storage device, then any command that tries to read or write data to a sector within the hidden area aborts with an indication of *invalid address*. Forensic media preparation tools may provide an optional feature to overwrite hidden areas of a drive.

5. Requirements

This section lists requirements for forensic media preparation.

5.1 Core Requirements

FMP-CR-01. All visible sectors shall be overwritten.

5.2 Requirements for Optional Features

Three optional features are identified: hidden area overwriting, overwrite command selection, and overwrite pattern selection.

5.2.1 Hidden area overwriting requirements

FMP-RO-01 If the tool supports overwriting hidden sectors, then all sectors contained in a hidden area shall be overwritten.

FMP-RO-02 If a hidden area exists on the storage device the tool may optionally remove the hidden area from the storage device.

5.2.2 Overwrite command selection requirements

Note that in these requirements the phrase *ERASE command* refers to both the ATA SECURITY ERASE UNIT command and the SCSI ERASE command.

FMP-RO-03 If the tool supports selection of a command for overwriting and the selected storage device supports an ERASE command for overwriting, then the tool shall allow selection of the ERASE command.

FMP-RO-04 If the ERASE command is selected and the disk drive does not support the command, then the tool shall indicate to the user that the command is not supported.

5.2.3 Overwrite pattern selection

FMP-RO-05 If an overwrite pattern is selected then the selected pattern is used for overwriting.