October 4, 2004

Digital Data Acquisition Tool Specification

Draft 1 for Public Review of Version 4.0

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

Contents

1.0 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, 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 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.

2.0 Purpose

This document defines requirements for digital media acquisition tools used in computer forensics investigations. This is a major revision of the original disk imaging specification, *Disk Imaging Tool Specification*, Version 3.1.6. The original specification covered the tools and technologies widely available at the time the specification was drafted (October 2001) for the acquisition of digital data from computer hard drives and has been effective for producing test reports evaluating critical features of the disk imaging tools of that time. However, technology and imaging tools have evolved requiring a revision to the specification. The ubiquity and variety of storage media is reflected in the change of title from *Disk Imaging Tool Specification* to *Digital Data Acquisition Tool Specification*. The primary goals of this revision are to expand the coverage of the specification to new storage technologies and to expand the coverage to new acquisition tool features. Secondary goals of the revision are to update terminology to add flexibility and more concise wording of requirements and to allow easier incorporation of new technologies. In addition, to improve layout and legibility and to be consistent with more recent specifications, test assertions and test cases have been moved to a separate document to be released later.

The requirements in this document are used to derive assertions to be tested. The assertions are described as general statements of conditions that are checked after a test is executed. Each assertion is checked in one or more test cases that specify detailed initial conditions, test scenarios, and expected test results.

These requirements were initially developed by a focus group of individuals who were expert in the use of disk acquisition tools and have performed investigations that depend on the results of these tools. As this document evolves through comments from the focus group and others, new versions will be posted at http://www.cftt.nist.gov/.

3.0 Scope

The scope of this specification is limited to software tools and hardware devices that acquire data from digital storage media that can be accessed as a file system by a computer. Not included are tools that image storage media directly from other digital devices such as cell phones, pagers, or PDAs.

The proper or improper use of a tool is not within the scope of this specification.

4.0 Background

NIJ Special Report 199408, “Forensic Examination of Digital Evidence: A Guide for Law Enforcement” presents a guideline for handling digital evidence as part of the criminal investigation process. The report states that digital evidence is processed in four steps: assessment, acquisition, examination, and documenting and reporting. This specification addresses tool functions for acquisition.

The digital media acquisition process begins with the identification of a *digital source*. It could be a physical device such as a hard disk drive from a computer, a memory card from a camera, a flash memory device or any of the various removable digital media available for storing digital data. The digital source may alternatively be a logical drive on a physical device. The ideal goal of the imaging process is to perform a complete and accurate acquisition of the digital source.

After the digital source is identified it is attached to a computer interface for acquisition. Some tool execution environments modify any attached storage device during the startup boot process and during the shutdown process. Acquisition of digital source attached to such a system often uses a write blocker to protect the digital source from modification.

After the digital source is attached to a computer interface an *acquisition tool* reads the data from the device and saves the data in an accessible form called a *destination object*. The destination object is usually one or more image files representing all the data acquired from the digital source. The destination object could alternatively be a clone of the source, either an exact bit-for-bit copy of the original (an *unaligned clone*), or it could be a bit-stream duplicate except for minor changes as required to align partitions on cylinder boundaries (a *cylinder-aligned clone*). The main distinction between a clone and

an image is that an image is accessed through a tool, but a clone is accessed as a normal file system mounted by the computer.

The two critical measurable attributes of the acquisition process are *completeness* and *accuracy*. Completeness measures if the all the data was acquired, and accuracy measures if the data was correctly acquired.

To access the digital source the physical device needs to be connected to the computer by a physical interface and then the acquisition tool needs to read the device by some protocol. For example, a hard drive might be attached by the ATA[1] interface and then accessed either through the BIOS interrupt 0x13 commands or accessed directly by the ATA commands. The combination of physical interface and access method is the *access interface*. Examples of some access interfaces include the following: legacy BIOS, extended BIOS, ATA, SATA, SCSI, ASPI, USB, IEEE 1394, RAID, and remotely over a network. For some interfaces there exists more than one version of the interface with differences that are significant to the acquisition process. For example, ATA-3 does not allow 48 bit disk addresses, but ATA-6 allows 48 bit disk addresses.

One component of digital imaging is determining the true size of the digital source. Hard drives built to the later ATA specifications may allow the creation of inaccessible or hidden areas, such as a host protected area or a device configuration overlay. A drive that has 80GB of space may be reconfigured to appear to have less space. An attempt to read from the hidden area results in an access error until the drive is reconfigured back to the original size.

5.0 Definitions

For the purposes of this specification, the following terms and definitions apply. Definitions for other hard disk drive related terms can be found in ANSI INCITS 361-2002 “AT Attachment - 6 with Packet Interface.”

Table 1 Acronyms Used in this Specification

Acronym	Expanded Term
ANSI	American National Standards Institute
ASPI	Advanced SCSI Programming Interface
ATA	AT-Attachment
BIOS	Basic Input Output System
IEEE	Institute of Electrical and Electronics Engineers
INCITS	International Committee for Information Technology Standards
RAID	Redundant Array of Independent Disks
SATA	Serial ATA
SCSI	Small Computer System Interface
USB	Universal Serial Bus

[1] See Table 1 Acronyms Used in this Specification for an explanation of any acronyms used in the text.

Access interface: The combination of a physical interface (how the device is physically attached) and an access method (command set or protocol) that is used by an acquisition tool to access the digital source. An access interface is visible to the acquisition tool either by default or as a user selectable interface.

Accurate acquisition: If for every bit of a destination object that corresponds to an accessible bit of a digital source, the value of the bit on the digital source is equal to the value of the corresponding bit in the destination object and for every bit of a destination object that corresponds to an inaccessible bit on the digital source, the destination object contains a benign fill. (The comparison is made after any necessary decryption or decompression.) See also **complete acquisition.**

Acquisition: The process of using an access interface to read digital data from a digital source and to create a destination object.

Acquisition tool: A program or hardware device used to read a digital source and then create either an image file or a clone of a digital source. An acquisition tool is also known as an imaging tool.

Benign fill: Values used to either replace data from a digital source that were inaccessible (such as from an unreadable sector) or values used to fill excess space during creation of a clone of a digital source. The fill must be benign in the sense that it could not be mistaken to have investigative value. The fill should be either a constant value such as zero, or text indicating that the data is not from the digital source.

Bit-stream duplicate: A bit-for-bit digital copy of a digital object such as a document, file, partition, graphic image, physical disk, or similar digital object.

Clone destination: Physical media used to receive either an unaligned clone or a cylinder-aligned clone.

Complete acquisition: If for every bit of the digital source there is a corresponding bit in the destination object and for every bit representing acquired data in the destination object there is a corresponding bit in the digital source. Note that for the case of a destination object that is an image file there may be descriptive data in the image file in addition to the data acquired from the digital source. See also **accurate acquisition.**

Cylinder-aligned clone: A bit-stream duplicate restored to physical media of the data acquired from a digital source except for minor changes as required to align partitions on cylinder boundaries. The cylinder-aligned clone allows for changes in file system metadata (such as partition table entries) and the addition of benign fill to produce a restored hard drive with partitions aligned on cylinder boundaries, a partition table updated to reflect the partition adjustments, and updated partition boot sectors. See also **unaligned clone.**

Destination object: Either an image file, an unaligned clone or a cylinder-aligned clone.

Digital source: A container of digital data that can be acquired by an acquisition tool. Examples of some digital sources include the following: physical drive, removable physical media, logical drive (also called a partition), or block of contiguous sectors. Examples of digital media include the following: hard disk drive, floppy disk, flash media, compact disk, digital versatile disk, and zip disk.

Execution environment: The collection of services provided by the operating system to support execution of the acquisition tool.

Hidden data sectors: The sectors in the current configuration of a drive that cannot be accessed by read and write commands without changing the drive configuration. For example, any sectors in a host protected area would be hidden data sectors. See also **visible data sectors.**

Image destination: A location for placement of an image file.

Image file: A file or set of files created from a digital source that contains the information necessary to create a bit-stream duplicate of the data acquired from the digital source. In addition to a native or default image file format, some tools optionally create compressed image files, encrypted image files, or the image file format of other tools. An image file that is a collection of files is referred to as a *multi-file image*.

Resolved error: When a tool issues an I/O request that returns failure or error status and the tool retries the operation or issues an alternate I/O request and is able to accomplish the intended result of the original request without a failure or error status return. See also **unresolved error**.

Truncated clone: An unaligned or aligned partial clone of a digital source created on a clone destination too small to contain all the data from the digital source.

Unaligned clone: A bit-stream duplicate restored to physical media of the data acquired from the digital source from both visible and hidden data sectors. However, the clone may need to be configured such that sectors hidden on the digital source are visible on the clone. See also **cylinder-aligned clone.**

Unresolved error: When a tool issues an I/O request that returns failure or error status and the tool retries the operation or issues an alternate I/O request, but still is not successful. If the tool retries the operation or issues an alternate I/O request and is able to accomplish the intended result of the original request without a failure or error status return then the error is *resolved.* See also **resolved error**.

Visible data sectors: The sectors in the current configuration of a drive that are accessible by read and write commands in the current drive configuration. See also **hidden data sectors.**

6.0 Requirements

The requirements are in two sections. The first section lists requirements that all acquisition tools shall meet. The second section lists requirements that the tool shall meet on the condition that specified features or options are offered by the tool.

6.1 Requirements for mandatory features

All acquisition tools shall meet these requirements.

DI-RM-01. The tool shall be able to acquire a digital source using each access interface visible to the tool.

DI-RM-02. The tool shall be able to create either a clone of a digital source, or an image of a digital source, or provide the capability for the user to select and then create either a clone or an image of a digital source.

DI-RM-03. The tool shall operate in at least one execution environment and shall be able to acquire digital sources in each execution environment.

DI-RM-04. The tool shall completely acquire all visible data sectors from the digital source.

DI-RM-05. The tool shall completely acquire all hidden data sectors from the digital source.

DI-RM-06. All data sectors acquired by the tool from the digital source shall be accurately acquired.

DI-RM-07. If there are unresolved errors reading from a digital source then the tool shall notify the user of the error type and the error location.

DI-RM-08. If there are unresolved errors reading from a digital source then the tool shall use a benign fill in the destination object in place of the inaccessible data.

6.2 Requirements for optional features

An acquisition tool may offer additional features beyond the basic requirements defined above. The tool may offer any combination of the following optional features:

- Create an image file in a specified format either by default or selected from a list of supported formats.
- Check the integrity of an image file by detecting if the image file has changed since the image file was created.
- Create a multi-file image.
- Create a multi-file image across multiple destination devices.
- Create a clone of a subset of an image file.
- Create a clone from the digital source.
- Create a clone from an image file.
- Create an unaligned clone.
- Create a cylinder-aligned clone.
- Divide the digital source into one or more blocks, compute a hash value for each block and then log the hash values.
- Set the content of any excess sectors during clone creation.
- Log descriptive information about the acquisition.
- Acquire an unprotected digital source without modification of the source.

Please note that DI-RM-02 requires that while a tool may create every possible destination object, the tool has to create at least one type of destination object. In other words, some requirements from either section 6.2.1 or section 6.2.2 have to apply to the tool.

6.2.1 Image file

The requirements in this section only apply if the tool offers features related to image files. Requirements DI-RO-04 through DI-RO-07 apply only if the tool offers additional image file features: multi-file images, integrity checking, image file format conversion or destination device switching.

DI-RO-01. If the tool offers image file creation and image file creation is selected and a supported image format is selected then the tool shall create an image file in the selected format such that the created image file contains all the data acquired by the tool.

DI-RO-02. If the tool offers image file creation and image file creation is selected and if there is an error writing an image file then the tool shall notify the user of the condition.

DI-RO-03. If the tool offers image file creation and image file creation is selected and if there is insufficient space on the image destination device to contain the image file then the tool shall notify the user of the condition.

DI-RO-04. If the tool offers image file creation and image file creation is selected and if the tool offers multi-file image creation and the tool offers selection of image file size then the tool shall create a multi-file image with files of the requested size such that the resulting multi-file image contains the same data as acquired by the tool.

DI-RO-05. If the tool offers image file creation and image file creation is selected and if the tool offers image file integrity checking and image file integrity checking is selected then the tool shall notify the user either that there have been no changes to the image file if the image file has not changed or the tool shall notify the user of the affected locations if an image file has been changed.

DI-RO-06. If the tool offers conversion of an image file from one format to another then the tool shall convert a source image file from its image file format to a selected target image file format such that the converted image file contains the same data as represented in the original image file.

DI-RO-07. If the tool offers destination device switching and if space on the image destination is exhausted during image file creation then the tool shall allow switching the destination device and continuation of the image file on the replacement device such that the resulting multi-file image represents the same data as acquired by the tool.

6.2.2 Clone creation

The requirements in this section apply only if the tool offers a clone creation feature. Requirement DI-RO-08 applies only if the tool also offers clone creation with the acquisition. Requirement DI-RO-09 applies only if the tool also supports image files. Requirement DI-RO-10 applies only if the tool also offers creation of a clone of a subset of the source. Requirement DI-RO-11 applies only if the tool supports unaligned clones. Requirement DI-RO-12 applies only if the tool supports cylinder-aligned clones.

DI-RO-08. If the tool offers clone creation during an acquisition and clone creation is selected then the tool shall create a clone from the digital source.

DI-RO-09. If the tool offers clone creation from an image file and clone creation is selected then the tool shall create a clone from the image file.

DI-RO-10. If the tool offers creation of a partial clone that is a subset of the original data acquired and the feature is selected then the tool shall create a clone of the specified subset of the acquired image.

DI-RO-11. If the tool offers unaligned clone creation and unaligned clone creation is selected then the tool shall create an unaligned clone.

DI-RO-12. If the tool offers cylinder-aligned clone creation and cylinder-aligned clone creation is selected then the tool shall create a cylinder-aligned clone.

DI-RO-13. If the tool offers clone creation and clone creation is selected and there are excess sectors on the clone destination then the tool shall as a default behavior or by user request either make no modification to the excess sectors or write a benign fill to the excess sectors as specified by the user.

DI-RO-14. If the tool offers clone creation and clone creation is selected and there is insufficient space on the clone destination to contain all the sectors acquired from the source then the tool shall notify the user and create a truncated clone using all available sectors of the clone destination.

DI-RO-15. If the tool offers clone creation and clone creation is selected and there is a write error creating the clone then the tool shall notify the user that a write error occurred.

6.2.3 Block hashes

The requirements in this section only apply if the tool offers block hash logging feature.

DI-RO-16. If the tool offers block hash logging and block hash logging is selected then the tool shall log correct hashes for blocks of the requested size from the digital source.

6.2.4 Logging

The requirements in this section only apply if the tool offers a log file creation feature.

DI-RO-17. If the tool offers log file creation then the tool shall log at least one of the following items: tool version, tool settings, acquisition date, acquisition time, device size (visible area), device size (all user

accessible sectors), device manufacturer, device model number, device serial number, partition table, amount of data acquired, and user comments.

6.2.5 Unprotected acquisitions

The requirements in this section apply to tools that offer acquisition without requiring write protection of the digital source.

DI-RO-18. If the tool offers acquisition of a digital source that is unprotected by a write block tool or device then an unprotected source shall not be modified during the acquisition process.