MAY 2013

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special **REPORT**

Test Results for Digital Data Acquisition Tool: FTK Imager CLI 2.9.0_Debian

nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Eric H. Holder, Jr.
Attorney General

Mary Lou Leary
Acting Assistant Attorney General

Greg Ridgeway
Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

NIJ

MAY 2013

Test Results for Digital Data Acquisition Tool: FTK Imager CLI 2.9.0_Debian

NCJ 242138

NIJ

Greg Ridgeway
Acting Director, National Institute of Justice

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Office of Law Enforcement Standards of the National Institute of Standards and Technology under Interagency Agreement 2003–IJ–R–029.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

May 2013

Test Results for Digital Data Acquisition Tool:
FTK Imager CLI 2.9.0_Debian

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

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology Law Enforcement Standards Office (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, and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and 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.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. The specifications and test methods are posted on the CFTT Web site (http://www.cftt.nist.gov/) for review and comment by the computer forensics community.

This document reports the results from testing FTK Imager CLI 2.9.0_Debian against the *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0*, available at the CFTT Web site (http://www.cftt.nist.gov/DA-ATP-pc-01.pdf).

Test results from other tools can be found on NIJ's computer forensics tool testing Web page, http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/cftt.htm.

How to Read This Report

This report is divided into five sections. The first section is a summary of the results from the test runs. This section is sufficient for most readers to assess the suitability of the tool for the intended use. The remaining sections of the report describe how the tests were conducted, discuss any anomalies that were encountered and provide documentation of test case run details that support the report summary. Section 2 gives justification for the selection of test cases from the set of possible cases defined in the test plan for Digital Data Acquisition tools. The test cases are selected, in general, based on features offered by the tool. Section 3 describes in more depth any anomalies summarized in the first section. Section 4 lists hardware and software used to run the test cases with links to additional information about the items used. Section 5 contains a description of each test case run. The description of each test run lists all test assertions used in the test case, the

expected result and the actual result. Please refer to the vendor documentation for guidance on using the tool.

Test Results for Digital Data Acquisition Tool

Tool Tested:	FTK Imager CLI
Software Version:	2.9.0 Debian
Runtime Environment(s)	Debian Live 6.0.4 and Ubuntu 10.04 LTS
Supplier:	AccessData
Address:	384 South 400 West, Suite 200 Lindon, UT 84042 USA
Tel:	1-801-377-5410
Fax:	1-801-765-4370
E-mail:	support@accessdata.com
WWW:	http://accessdata.com/

1 Results Summary

AccessData's FTK Imager CLI v2.9 Debian is designed to image and restore hard drives and other secondary storage. It uses the Debian command line interface to image, clone and restore acquired data. Except for the case where a drive with faulty sectors was imaged (test case DA-09), the tool acquired all sectors of the test media completely and accurately. In test cases DA-04 and DA-17 that measure how a tool behaves when the destination media has insufficient space for a clone or restore task, the tool failed to display a message indicating that the destination drive had insufficient space.

Refer to sections 3.1 and 3.2 for additional details on test cases DA-04, DA-17 and DA-09.

2 Test Case Selection

Test cases used to test disk imaging tools are defined in *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0*. To test a tool, test cases are selected from the *Test Plan* document based on the features offered by the tool. Not all test cases or test assertions are appropriate for all tools. There is a core set of base cases (e.g., DA-06 and DA-07) that are executed for every tool tested. Tool features guide the selection of additional test cases. If a given tool implements a feature, then the test cases linked to that feature are run. Table 1 lists the testable features of FTK Imager CLI v2.9 Debian and the linked test cases selected for execution. Table 2 lists the features not available in FTK Imager CLI v2.9 Debian and the test cases not executed.

Table 1. Selected Test Cases

Supported Optional Feature	Cases Selected for Execution
Create a clone during acquisition	01
Create an unaligned clone from a digital source	02

Supported Optional Feature	Cases Selected for Execution
Create a truncated clone from a physical device	04
Base Cases	06 & 07
Read error during acquisition	09
Create an image file in more than one format	10
Insufficient space for image file	12
Create a clone from an image file	14 & 17
Detect a corrupted (or changed) image file	24 & 25
Convert an image file from one format to another	26

Table 2. Omitted Test Cases

Unsupported Optional Feature	Cases Omitted (Not Executed)
Create cylinder aligned clones	03, 15, 21 & 23
Device I/O error generator available	05, 11 & 18
Create an image of a drive with hidden sectors	08
Destination Device Switching	13
Create a clone from a subset of an image file	16
Fill excess sectors on a clone acquisition	19
Fill excess sectors on a clone device	20, 21, 22 & 23

Some test cases have different forms to accommodate parameters within test assertions. These variations cover the acquisition interface to the source media, the type of digital object acquired and image file format.

The following source interfaces were tested: USB, ATA28, ATA48, FW, SATA28, SATA48 and SCSI. These are noted as variations on test cases DA-01 and DA-06.

The following digital source types were tested: partitions (FAT16, FAT32, NTFS, EXT3, EXT4), compact flash (CF) and thumb drive (Thumb). These digital source types are noted as variations on test cases DA-02 and DA–07.

The following image file types are supported by the tool: SMART ew-compressed, E01 and encrypted. These were tested as alternate image file formats and are noted as variations on test case DA-10.

3 Results by Test Assertion

A test assertion is a verifiable statement about a single condition after an action is performed by the tool under test. A test case usually checks a group of assertions after the action of a single execution of the tool under test. Test assertions are defined and linked to test cases in *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0*. Table 3 summarizes the test results for all the test cases by assertion. The column labeled **Assertions Tested** gives the text of each assertion. The column labeled **Tests** gives the

number of test cases that use the given assertion. The column labeled **Anomaly** gives the section number in this report where any observed anomalies are discussed.

Table 3. Assertions Tested

Assertions Tested	Tests	Anomaly
AM-01 The tool uses access interface SRC-AI to access the digital source.	33	
AM-02 The tool acquires digital source DS.	33	
AM-03 The tool executes in execution environment XE.	62	
AM-04 If clone creation is specified, the tool creates a clone of the digital source.	14	
AM-05 If image file creation is specified, the tool creates an image file on file system type FS.	19	
AM-06 All visible sectors are acquired from the digital source.	32	3.2
AM-08 All sectors acquired from the digital source are acquired accurately.	32	
AM-09 If unresolved errors occur while reading from the selected digital source, the tool notifies the user of the error type and location within the digital source.	1	3.2
AM-10 If unresolved errors occur while reading from the selected digital source, the tool uses a benign fill in the destination object in place of the inaccessible data.	1	
AO-01 If the tool creates an image file, the data represented by the image file is the same as the data acquired by the tool.	18	
AO-02 If an image file format is specified, the tool creates an image file in the specified format.	3	
AO-04 If the tool is creating an image file and there is insufficient space on the image destination device to contain the image file, the tool shall notify the user.	1	
AO-05 If the tool creates a multi-file image of a requested size then all the individual files shall be no larger than the requested size.	18	
AO-06 If the tool performs an image file integrity check on an image file that has not been changed since the file was created, the tool shall notify the user that the image file has not been changed.	1	
AO-07 If the tool performs an image file integrity check on an image file that has been changed since the file was created, the tool shall notify the user that the image file has been changed.	1	
AO-08 If the tool performs an image file integrity check on an image file that has been changed since the file was created, the tool shall notify the user of the affected locations.	1	
AO-09 If the tool converts a source image file from one format to a target image file in another format, the acquired data represented in the target image file is the same as the acquired data in the source image file.	9	
AO-11 If requested, a clone is created during an acquisition of a	14	

Assertions Tested	Tests	Anomaly
digital source.		
AO-12 If requested, a clone is created from an image file.	18	
AO-13 A clone is created using access interface DST-AI to write to the clone device.	32	
AO-14 If an unaligned clone is created, each sector written to the clone is accurately written to the same disk address on the clone that the sector occupied on the digital source.	31	
AO-17 If requested, any excess sectors on a clone destination device are not modified.	16	
AO-19 If there is insufficient space to create a complete clone, a truncated clone is created using all available sectors of the clone device.	2	
AO-20 If a truncated clone is created, the tool notifies the user.	2	3.1
AO-23 If the tool logs any log significant information, the information is accurately recorded in the log file.	62	
AO-24 If the tool executes in a forensically safe execution environment, the digital source is unchanged by the acquisition process.	33	

Two test assertions only apply in special circumstances. The assertion AO-22 is checked only for tools that create block hashes. The assertion AO-24 is only checked if the tool is executed in a run time environment that does not modify attached storage devices, such as MS-DOS. In normal operation, an imaging tool is used in conjunction with a write block device to protect the source drive. Table 4 lists the assertions that were not tested, usually due to the tool not supporting some optional feature, e.g., creation of cylinder-aligned clones.

Table 4. Assertions Not Tested

Assertions Not Tested
AM-07 All hidden sectors are acquired from the digital source.
AO-03 If there is an error while writing the image file, the tool notifies the user.
AO-10 If there is insufficient space to contain all files of a multi-file image and if destination device switching is supported, the image is continued on another device.
AO-15 If an aligned clone is created, each sector within a contiguous span of sectors from the source is accurately written to the same disk address on the clone device relative to the start of the span as the sector occupied on the original digital source. A span of sectors is defined to be either a mountable partition or a contiguous sequence of sectors not part of a mountable partition. Extended partitions, which may contain both mountable partitions and unallocated sectors, are not mountable partitions.
AO-16 If a subset of an image or acquisition is specified, all the subset is cloned.

Assertions Not Tested
AO-18 If requested, a benign fill is written to excess sectors of a clone.
AO-21 If there is a write error during clone creation, the tool notifies the user.
AO-22 If requested, the tool calculates block hashes for a specified block size during an acquisition for each block acquired from the digital source.

3.1 Creating truncated clones

Test case DA-04 measured FTK Imager CLI v2.9 Debian's behavior when asked to acquire a physical device to a truncated clone. Test case DA-17 tested the behavior for creating truncated clones from image files. In both cases the tool did not inform the user that a truncated clone had been created. The tests ended without any message informing the user that the destination drive was smaller than the source. The tool does not log progress information, to the screen or to file, during a clone operation. It appears that the message logging function of the tool is limited by scope to image acquisitions only.

3.2 Faulty sectors

When cloning a drive with faulty sectors, test case DA-09, the tool stopped the acquisition at the first faulty sector. No notification was given to the user.

4 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the selected test execution environments, computers available for testing, using the support software, and notes on other test hardware.

4.1 *Execution Environment*

The tool was executed in the Debian Live 6.0.4 and Ubuntu 10.04 LTS environments.

4.2 *Test Computers*

Two computers were used to run the tool: **DeathStar and Frank**.

DeathStar has the following configuration:

TCP Custom Built
Processor, Intel Core i5-2500 3.3GHZ
Super Writemaster CDRW/DVD
BIOS Version ASUS EFI Version 9.16.2011

Frank has the following configuration:

Latitude D800
Processor, Intel Pentium 4 3.40GHZ
Assembly, Floppy Drive, 1.44M, 3.5"

Samsung CDRW/DVD
BIOS Version Inter Version BF865105

4.3 Support Software

A package of programs to support test analysis, FS-TST Release 2.0, was used. The software can be obtained from: http://www.cftt.nist.gov/diskimaging/fs-tst20.zip.

4.4 Test Drive Creation

There are three ways that a hard drive may be used in a tool test case: as a source drive that is imaged by the tool, as a media drive that contains image files created by the tool under test, or as a destination drive on which the tool under test creates a clone of the source drive. In addition to the operating system drive formatting tools, some tools (**diskwipe** and **diskhash**) from the FS-TST package are used to setup test drives.

4.4.1 Source Drive

The setup of most source drives follows the same general procedure, but there are several steps that may be varied depending on the needs of the test case.

1. The drive is filled with known data by the **diskwipe** program from FS-TST. The **diskwipe** program writes the sector address to each sector in both C/H/S and LBA format. The remainder of the sector bytes is set to a constant fill value unique for each drive. The fill value is noted in the **diskwipe** tool log file.
2. The drive may be formatted with partitions as required for the test case.
3. An operating system may optionally be installed.
4. A set of reference hashes is created by the FS-TST **diskhash** tool. These include both SHA1 and MD5 hashes. In addition to full drive hashes, hashes of each partition may also be computed.
5. If the drive is intended for hidden area tests (DA-08), an HPA, a DCO or both may be created. The **diskhash** tool is then used to calculate reference hashes of just the visible sectors of the drive.

The source drives for DA-09 are created such that there is a consistent set of faulty sectors on the drive. Each of these source drives is initialized with **diskwipe** and then their faulty sectors are activated. For each of these source drives, a duplicate drive with no faulty sectors serves as a reference drive for comparison.

4.4.2 Media Drive

To setup a media drive, the drive is formatted with one of the supported file systems. A media drive may be used in several test cases.

4.4.3 Destination Drive

To setup a destination drive, the drive is filled with known data by the **diskwipe** program from FS-TST. Partitions may be created if the test case involves restoring from the image of a logical acquire.

4.5 Test Drive Analysis

For test cases that create a clone of a physical device, e.g., DA-01, DA-04, etc., the destination drive is compared to the source drive with the **diskcmp** program from the FS-TST package; for test cases that create a clone of a logical device, i.e., a partition, e.g., DA-02, DA-20, etc., the destination partition is compared to the source partition with the **partcmp** program. For a destination created from an image file, e.g., DA-14, the destination is compared, using either **diskcmp** (for physical device clones) or **partcmp** (for partition clones), to the source that was acquired to create the image file. Both **diskcmp** and **partcmp** note differences between the source and destination. If the destination is larger than the source, it is scanned and the excess destination sectors are categorized as either undisturbed (still containing the fill pattern written by **diskwipe**), zero filled or changed to something else.

For test case DA-09, imaging a drive with known faulty sectors, the program **ana-bad** is used to compare the faulty sector reference drive to a cloned version of the faulty sector drive.

For test cases such as DA-06 and DA-07, any acquisition hash computed by the tool under test is compared to the reference hash of the source to check that the source is completely and accurately acquired.

4.6 Note on Test Drives

The testing uses several test drives from a variety of vendors. The drives are identified by an external label that consists of a two-digit hexadecimal value and an optional tag, e.g., 25-SATA. The combination of hex value and tag serves as a unique identifier for each drive. The two digit hex value is used by the FS-TST **diskwipe** program as a sector fill value. The FS-TST compare tools, **diskcmp** and **partcmp,** count sectors that are filled with the source and destination fill values on a destination that is larger than the original source.

5 Test Results

The main item of interest for interpreting the test results is determining the conformance of the tool under test with the test assertions. Conformance with each assertion tested by a given test case is evaluated by examining the **Log Highlights** box of the test report.

5.1 Test Results Report Key

The following table presents an explanation of each section of the test details in section 5.2. The Tester Name, Test Host, Test Date, Drives, Source Setup and Log Highlights sections for each test case are populated by excerpts taken from the log files produced by the tool under test and the FS-TST tools that were executed in support of test case setup and analysis.

Heading	Description
First Line:	Test case ID, name and version of tool tested.
Case Summary:	Test case summary from *Digital Data Acquisition Tool*