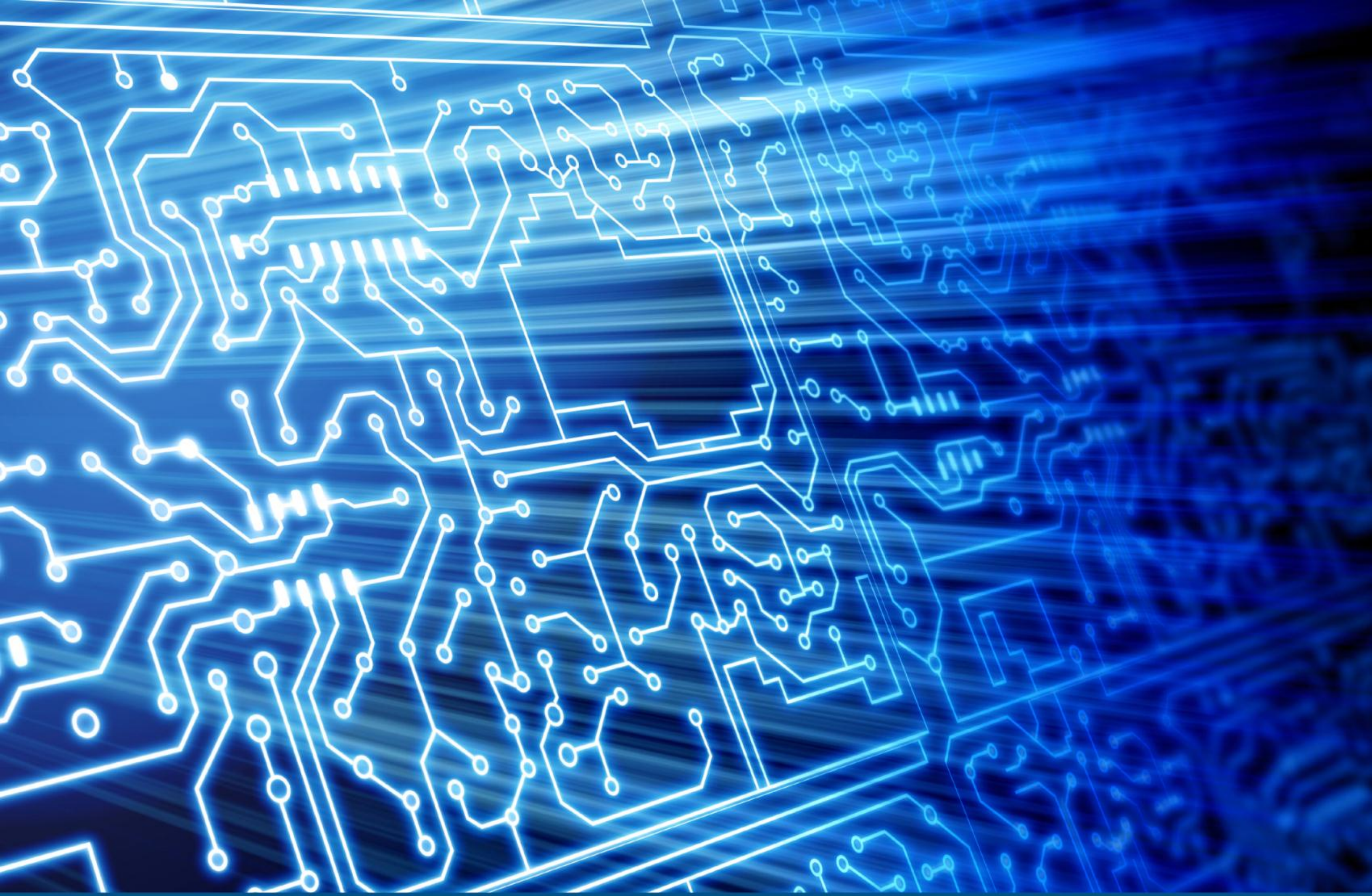

Fast Disk Acquisition System (FDAS) 2.0.2

Test Results for Digital Data Acquisition Tool

July 22, 2013

Homeland Security
Science and Technology

This report was prepared for the Department of Homeland Security Science and Technology Directorate Cyber Security Division by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.

For additional information about the Cyber Security Division and ongoing projects, please visit www.cyber.st.dhs.gov.

July 2013

Test Results for Digital Data Acquisition Tool:
FDAS version 2.0.2

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), the National Institute of Justice (NIJ), 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. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Web site (http://www.cftt.nist.gov/).

This document reports the results from testing FDAS version 2.0.2 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 identifies any significant anomalies observed in 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 test case selection, results by test case, the test environment and test details. 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 lists each test case run and the overall result. Section 4 lists hardware and software used to run the test cases with links to additional information about the items used. Section 5 presents for each test case the expected result data used to measure the success of the test and the actual data reported by the tool.

Test Results for Digital Data Acquisition Tool

Tool Tested:	FDAS version 2.0.2
Software Version:	2.0.2
Runtime Environment	Custom

Supplier: CyanLine LLC.

Address:
CyanLine LLC.
12 Christopher Way, STE 200,
Eatontown, NJ 07724.

Tel:	(732) 982-8510
Email:	info@cyanline.com
WWW:	http://cyanline.com

1 Results Summary

FDAS Fast Disk Acquisition System from CyanLine is a portable all in one acquisition tool. Connect a source drive to the unit and then it transfers the image directly to storage media internal to the device. FDAS also provides source drive write blocking. Except for the following anomalies, the tool acquired the test media completely and accurately.

- When a drive with faulty sectors was imaged (test cases DA-09-option1 & DA-09-option2) the tool failed to completely acquire all readable sectors near the location of the faulty sectors. Option 1 tries to skip around faulty sectors and omitted 422 readable sectors. Option 2 retries reading faulty sectors (at the expense of slower acquisition speed) and omitted 10 readable sectors.
- The tool failed to acquire sectors in a hidden area of a hard drive (test cases DA-08-DCO, DA-08-ATA28 & DA-08-ATA48).

Refer to sections3 and 5 for more details.

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 some feature then the test cases linked to the implemented features are run. Table 1 lists the supported features of FDAS version 2.0.2 and the linked test cases selected for execution. Table 2 lists the features not available in FDAS version 2.0.2 and the test cases not executed.

Table 1. Selected Test Cases

Supported Optional Feature	Cases selected for execution
Base Cases	06 & 07
Create an image of a drive with hidden sectors	08
Read error during acquisition	09
Create an image file in more than one format	10
Insufficient space for image file	12

Table 2. Omitted Test Cases

Unsupported Optional Feature	Cases omitted (not executed)
Create a clone during acquisition	01
Create an unaligned clone from a digital source	02
Create a truncated clone from a physical device	04
Create cylinder aligned clones	03, 15, 21 & 23
Device I/O error generator available	05, 11 & 18
Destination Device Switching	13
Create a clone from a subset of an image file	16
Create a clone from an image file	14 & 17
Fill excess sectors on a clone acquisition	19
Fill excess sectors on a clone device	20, 21, 22 & 23
Detect a corrupted (or changed) image file	24 & 25
Convert an image file from one format to another	26

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

The following source interfaces were tested: USB, ATA28, ATA48, FW, Mac TARGET mode, SATA28, and SATA48. These are noted as variations on test cases DA-06 and DA-07.

The following digital source types were tested: compact flash (CF) and thumb drive (Thumb). These digital source types are noted as variations on test case DA–07.

The following image file types are supported by the tool and were varied in testing: Expert Witness (.E01), and raw (.dd).

3 Results by Test Case-Variation

The following table summarizes the test results for each test run. Complete details can be examined at http://www.cftt.nist.gov/TBD.

Test Results Summary	
Case	**Results**
06-Target	Expected Results

Test Results Summary	
Case	**Results**
06-ata28	Expected Results
06-ata48	Expected Results
06-fw	Expected Results
06-sata28	Expected Results
06-sata48	Expected Results
06-usb	Expected Results
07-cf	Expected Results
07-thumb	Expected Results
08-ata28	Not Expected Results
08-ata48	Not Expected Results
08-dco	Not Expected Results
09-option1	Not Expected Results
09-option2	Not Expected Results
10-e01	Expected Results
12	Expected Results

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

Tests were run on the FDAS hardware unit running software version 2.0.2.

4.2 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.

4.3 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.

4.3.1 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.

4.3.2 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.

4.3.3 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.

4.4 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 **anabad** 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 a corresponding reference hash of the source to check that the source is completely and accurately acquired.

4.5 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

This section presents the expected data that the tested tool should report along with the actual data reported by the tool.

Test case DA-06 measures the tool’s ability to create a complete and accurate image over a specified access interface (AI). The test is repeated for each access interface supported by the tool. The expected result is for a hash value reported by the tool to match a reference hash value for the imaged source.

Test case DA-07 measures the tool’s ability to create a complete and accurate image from a specified digital source (DS). Some examples of digital sources are flash media, thumb drives, and hard drive partitions. The test is repeated for each digital source supported by the tool. The expected result is for a hash value reported by the tool to match a reference hash value for the imaged source.

Test case DA-08 measures the tool’s ability to acquire hidden sectors in either a Device Configuration Overlay (DCO) or a Host Protected Area (HPA). Reference hashes are provided for both the full test drive and just the visible area. The hash reported by the tool identifies if the hidden area is acquired.

Test case DA-09 measures the tool’s behavior if faulty sectors are encountered. The source drive content is compared to the acquired content and the number of differences noted.

Test case DA-10 measures the tool’s ability to create a complete and accurate image in an alternate image file format. The expected result is for a hash value reported by the tool to match a reference hash value for the imaged source.

Test case DA-12 measures the tool’s ability to create an image file where there is insufficient space. The expected result is for the tool to (1) copy source sectors to the image file until there is no free space left on the destination and (2) the tool notifies the user that the entire source has not been copied.

5.1 DA-06

DA-06 Acquire a physical device using access interface AI to an image file.

Hash Matches da-06

Case-AI	SRC	Ref MD5	Tool MD5	Ref SHA1	Tool SHA1	Ref SHA256	Tool SHA256
da-06-Target	01-SATA	0A49B…	0A49B…	N/A	N/A	N/A	N/A
da-06-ata28	43	BC39C…	BC39C…	N/A	N/A	N/A	N/A
da-06-ata48	4C	D10F7…	D10F7…	N/A	N/A	N/A	N/A
da-06-fw	63-FU2	EE217…	EE217…	N/A	N/A	N/A	N/A

Hash Matches da-06							
Case-AI	SRC	Ref MD5	Tool MD5	Ref SHA1	Tool SHA1	Ref SHA256	Tool SHA256
da-06-sata28	4B-SATA	746B4...	746B4...	N/A	N/A	N/A	N/A
da-06-sata48	0D-SATA	1FA7C...	1FA7C...	N/A	N/A	N/A	N/A
da-06-usb	63-FU2	EE217...	EE217...	N/A	N/A	N/A	N/A

5.2 DA-07

DA-07 Acquire a digital source of type DS to an image file.

Hash Matches da-07							
Case-DS	SRC	Ref MD5	Tool MD5	Ref SHA1	Tool SHA1	Ref SHA256	Tool SHA256
da-07-cf	C1-CF	776DF...	776DF...	N/A	N/A	N/A	N/A
da-07-thumb	D5-THUMB	C8435...	C8435...	N/A	N/A	N/A	N/A

5.3 DA-08

DA-08 Acquire a physical drive with hidden sectors to an image file.

Hash Matches da-08						
Case-AI	SRC	Hidden	Algorithm	Partial Acquire	Tool Hash	All Acquired
da-08-ata28	42	HPA	MD5	9BF3C...	9BF3C...	F4B9A...
da-08-ata48	2D-IDE	HPA	MD5	D6790...	D6790...	B7E8F...
da-08-dco	92	DCO	MD5	52596...	52596...	E095D...

5.4 DA-08 Anomalies

Anomalies Observed

Anomalies Observed in da-08	
Case	Anomaly
da-08-ata28	Hidden area (HPA) not acquired
da-08-ata48	Hidden area (HPA) not acquired
da-08-dco	Hidden area (DCO) not acquired

5.5 DA-09

DA-09 Acquire a digital source that has at least one faulty data sector.

Differences Between SRC & DST da-09				
Case	SRC	Faulty Sectors	Compared	Differ
da-09-option1	ed-bad-cpr4	35	120103200	457
da-09-option2	ed-bad-cpr4	35	120103200	42

5.6 DA-09 Anomalies

Anomalies Observed

Anomalies Observed in da-09	
Case	Anomaly
da-09-option1	Some sectors differ: [457]
da-09-option2	Some sectors differ: [42]

5.7 DA-10

DA-10 Acquire a digital source to an image file in an alternate format.

Hash Matches da-10							
Case	**SRC**	**Ref MD5**	**Tool MD5**	**Ref SHA1**	**Tool SHA1**	**Ref SHA256**	**Tool SHA256**
da-10-e01	43	BC39C...	BC39C...	N/A	N/A	N/A	N/A

5.8 DA-12

DA-12 Attempt to create an image file where there is insufficient space.

Message to User da-12		
Case	**SRC**	**Message**
da-12	4B-SATA	The tool would not allow the imaging process to begin when there was insufficient space to store the image file. The tool displayed, "No options avail Op Cmpt – Shutdown?"

5.9 Administrative Summary

The following table is a list of administrative data about each test case run.

Administrative Summary					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
06-Target	fdas	csr	01-SATA	NONE	Mon Feb 11 15:40:29 2013
06-ata28	fdas	csr	43	NONE	Sun Feb 10 13:28:01 2013
06-ata48	fdas	csr	4C	NONE	Sun Feb 10 13:32:49 2013
06-fw	fdas	csr	63-FU2	NONE	Sat Feb 9 09:27:57 2013
06-sata28	fdas	csr	4B-SATA	NONE	Sat Feb 9 11:06:14 2013
06-sata48	fdas	csr	0D-SATA	NONE	Sat Feb 9 15:35:35 2013
06-usb	fdas	csr	63-FU2	NONE	Sat Feb 9 09:11:06 2013
07-cf	fdas	csr	C1-CF	NONE	Sat Feb 9 08:58:03 2013
07-thumb	fdas	csr	D5-THUMB	NONE	Sat Feb 9 08:27:39 2013
08-ata28	fdas	csr	42	NONE	Wed May 8 12:54:47 2013
08-ata48	fdas	csr	2D-IDE	NONE	Tue May 7 10:10:00 2013
08-dco	fdas	csr	92	NONE	Tue May 7 09:01:28 2013
09-option1	fdas	csr	ED-BAD-CPR4	6F	Sat Feb 9 15:45:37 2013
09-option2	fdas	csr	ED-BAD-CPR4	29-LAP	Fri Feb 8 13:58:53 2013
10-e01	fdas	csr	43	NONE	Mon Feb 11 12:01:11 2013
12	fdas	csr	4B-SATA	NONE	Wed Jun 26 13:25:11 2013