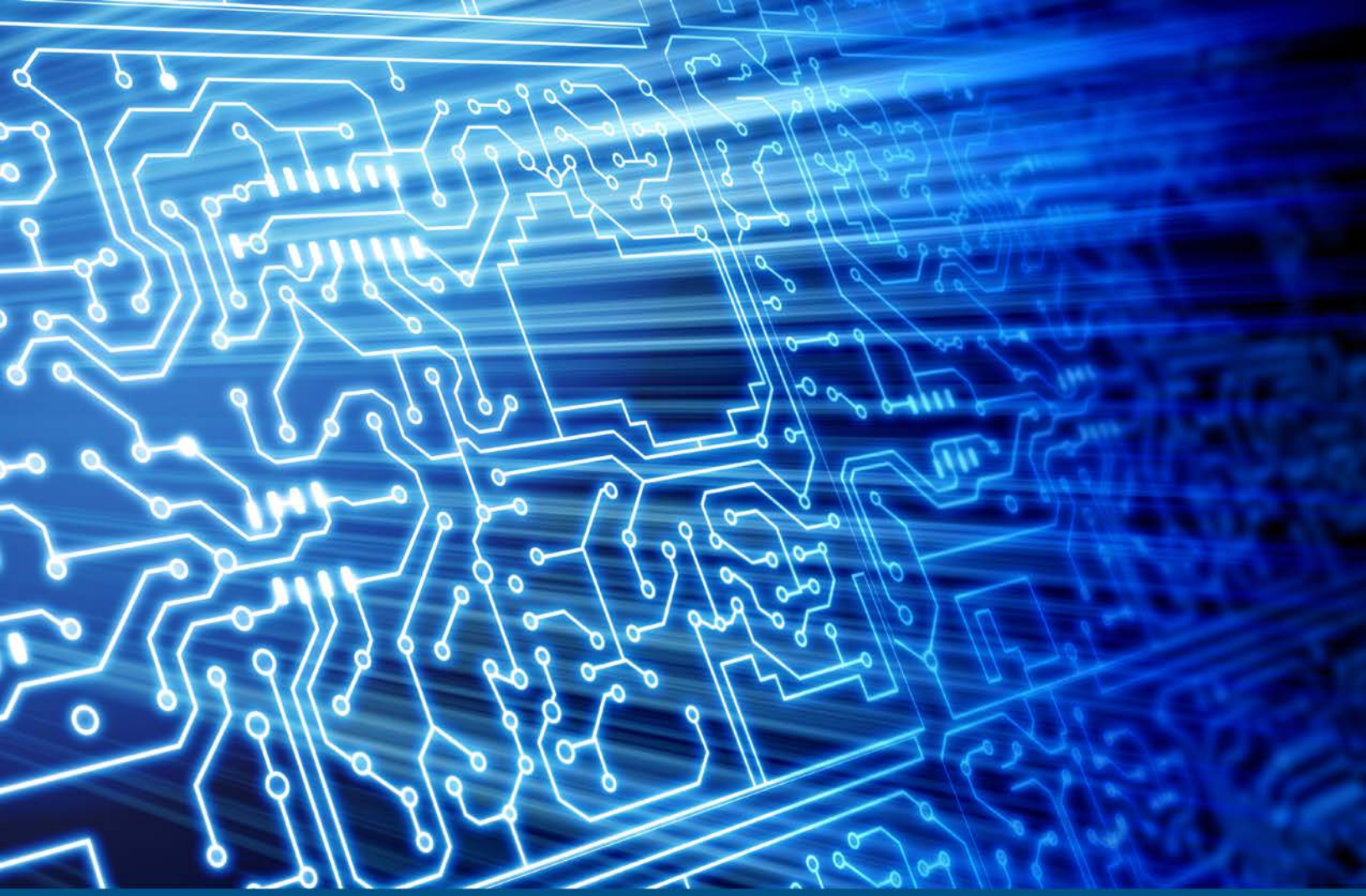

Tableau TD3 Forensic Imager 1.3.0

Test Results for Digital Data Acquisition Tool

July 23, 2014

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 2014

Test Results for Digital Data Acquisition Tool:
Tableau TD3 Forensic Imager version 1.3.0

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, and the National Institute of Standards and Technology Law Enforcement Standards Office and Information Technology Laboratory. 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 the Tableau TD3 Forensic Imager version 1.3.0 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 the DHS S&T-sponsored digital forensics web page, http://www.cyberfetch.org/.

How to Read This Report

This report is divided into six 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. Section 6 presents administrative data for each test case run. To download a zip file containing the raw log files for the Tableau TD3 Forensic Imager version 1.3.0 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test Results for Digital Data Acquisition Tool

Tool Tested:	Tableau TD3 Forensic Imager
Version:	1.3.0
Supplier:	Guidance Software, Inc.
Address:	1055 E. Colorado Blvd. Pasadena, CA 91106
Tel:	1 (866) 229-9199
WWW:	http://www.guidancesoftware.com/

1 Results Summary

The Tableau TD3 Forensic Imager is a modular multi-function standalone device. The TD3 Forensic Imager was only tested for its forensic imaging ability. Except for one test case, the tool acquired all visible and hidden sectors completely and accurately from the test media. In test case DA-09-standard100 when the tool was executed with Error Granularity set to *Standard* and faulty sectors were encountered, readable sectors in the same 64-sector imaging block as the faulty sectors were replaced by zeros in the created clone. This is the intended tool behavior as specified by the tool vendor. When Error Granularity was set to *Exhaustive* (default), all readable sectors were acquired by the tool and zeros were written to the clone in place of the faulty sectors (test cases DA-09-exh100, DA-09-exhdonot and DA-09-exhtryonce).

Note on test case DA-08-DCO, imaging a drive containing a Device Configuration Overlay or DCO. The tool does not automatically remove DCOs from source drives but is designed to alert the user when a DCO exists. A user may cancel the duplication process and manually remove the DCO using the "HPA/DCO Disable" menu option. In test case DA-08-DCO the "HPA/DCO Disable" menu option was exercised to remove the DCO and all sectors of the source drive were successfully acquired.

For more detailed results on all test cases see section 5.

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 Tableau TD3

version 1.3.0 and the linked test cases selected for execution. Table 2 lists the features not available in Tableau TD3 version 1.3.0 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
Create a truncated clone from a physical device	04
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
Detect a corrupted (or changed) image file	24 & 25

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
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
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 drive, the type of digital object acquired, the way that sectors are hidden on a drive and image file format. Image file segment size was varied for test cases DA-06 and DA-07. Error Granularity (*Standard* or *Exhaustive*) and Error Retry (*do not retry*, *retry once*, and *retry 100 times*) settings were varied for four DA-09 test case variations.

The following source interfaces were tested: FW, USB, PATA and SATA. These are noted as variations on test cases DA-01 and DA-06.

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

In addition to EnCase Evidence File Format (.e01), the following image file types are supported by the tool: EnCase Evidence File Format Version 2 (.ex01) and raw (.dd).

3 Results by Test Case-Variation

The following table lists the test outcome by test case-variation. For a complete explanation of the test case results, see Section 5. To download a zip file containing the raw log files for the Tableau TD3 version 1.3.0 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test case Results	
Case	**Results**
01-ata28	Expected Results
01-ata48	Expected Results
01-fw	Expected Results
01-sata28	Expected Results
01-sata48	Expected Results
01-usb	Expected Results
02-cf	Expected Results
02-sd	Expected Results
02-thumb	Expected Results
04	Expected 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-sd	Expected Results
07-thumb	Expected Results
08-ata28	Expected Results
08-sata48	Expected Results
08-dco	Expected Results
09-exh100	Expected Results
09-exhdonot	Expected Results
09-exhtryonce	Expected Results
09-standard100	Unexpected Results
10-dd	Expected Results
10-ex01	Expected Results
12	Expected Results
24	Expected Results
25	Expected Results

4 Testing Environment

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

4.1 *Execution Environment*

The Tableau TD3 Forensic Imager is a custom hardware device. The tests were run on the Tableau TD3 Forensic Imager unit running version 1.3.0 of the imager software.

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 **diskcmp** is used to compare a clone of the faulty sector drive to a reference drive. The reference drive is a copy of the faulty sector drive with readable sectors where the faulty sector drive has faulty sectors.

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 results for each test case along with the actual results produced by the tool. To download a zip file containing the raw log files for the Tableau TD3 version 1.3.0 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test case DA-01 measures the tool's ability to acquire a physical device source using a specified access interface and to create a complete and accurate clone of the source to a destination drive. The test is repeated for each access interface supported by the tool. The

expected result is measured by checking that all source sectors match corresponding destination sectors in a sector-by-sector comparison.

Test case DA-02 measures the tool's ability to acquire a digital source (DS) to a clone of the same type. 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 all source sectors to match corresponding destination sectors in a sector-by-sector comparison.

Test case DA-04 measures the tool's ability to acquire a physical device to a smaller physical device. The expected result is for the tool to (1) copy source sectors to the destination 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 to the destination.

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

Test case DA-24 measures the tool's ability to verify a valid image file. 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-25 measures the tool's ability to detect a corrupted image. The expected result is for a hash value reported by the tool should not match that of the reference hash value for the imaged source.

5.1 DA-01

DA-01 Acquire a physical device using access interface AI to an unaligned clone.

Differences Between SRC & DST da-01			
Case-AI	**SRC**	**Compared**	**Differ**
da-01-ata28	43	78125000	0
da-01-ata48	4c	488397168	0
da-01-fw	63-fu2	117304992	0
da-01-sata28	07-sata	156301488	0
da-01-sata48	16-sata	312581808	0
da-01-usb	63-fu2	117304992	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-01-ata28	41978200	0	0	41978200	0

5.2 DA-02

DA-02 Acquire a digital source of type DS to an unaligned clone.

Differences Between SRC & DST da-02			
Case-DS	**SRC**	**Compared**	**Differ**
da-02-cf	c1-cf	503808	0
da-02-sd	a1-sd	246016	0
da-02-thumb	d5-thumb	505856	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-02-thumb	3495904	0	0	3495904	0

5.3 DA-04

DA-04 Acquire a physical device to a truncated clone.

Differences Between SRC & DST da-04			
Case	**SRC**	**Compared**	**Differ**
da-04	43	19925880	0

Message to User da-04		
Case	**SRC**	**Message**
da-04	43	Destination disk is too small. Do you want to truncate the duplication to size of the destination disk?

5.4 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-ata28	01-IDE-96	F458F...	F458F...	A48BB...	A48BB...	N/A	N/A
da-06-ata48	4C	D10F7...	D10F7...	8FF62...	8FF62...	N/A	N/A
da-06-fw	63-FU2	EE217...	EE217...	F7069...	F7069...	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	07-SATA	2EAF7...	2EAF7...	655E9...	655E9...	N/A	N/A
da-06-sata48	16-SATA	7BB1D...	7BB1D...	F8298...	F8298...	N/A	N/A
da-06-usb	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A

5.5 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...	5B823...	5B823...	N/A	N/A
da-07-sd	A1-SD	E9250...	E9250...	FBA5D...	FBA5D...	N/A	N/A
da-07-thumb	D5-THUMB	C8435...	C8435...	D6852...	D6852...	N/A	N/A

5.6 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...	F4B9A...	F4B9A...
da-08-dco	92	DCO	MD5	52596...	E095D...	E095D...
da-08-sata48	1E-SATA	HPA	MD5	3655F...	8E1CF...	8E1CF...

5.7 DA-09

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

Differences Between SRC & DST da-09			
Case	**SRC**	**Compared**	**Differ**
da-09-exh100	ed-bad-cpr4	120103200	35
da-09-exhdonot	ed-bad-cpr4	120103200	35
da-09-exhtryonce	ed-bad-cpr4	120103200	35
da-09-standard100	ed-bad-cpr4	120103200	1216

Faulty Drives		
Case	**Drive**	**Faulty Sectors**
da-09-exh100	ed-bad-cpr4	35
da-09-exhdonot	ed-bad-cpr4	35
da-09-exhtryonce	ed-bad-cpr4	35
da-09-standard100	ed-bad-cpr4	35

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-09-exh100	36198288	0	0	36198288	0
da-09-exhdonot	36198288	0	0	36198288	0
da-09-exhtryonce	36198288	0	0	36198288	0
da-09-standard100	36198288	0	0	36198288	0

5.8 *DA-09 Anomalies*

Anomalies Observed

Anomalies Observed in da-09	
Case	**Anomaly**
da-09-standard100	Some sectors differ: [1216]

5.9 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-dd	43	BC39C...	BC39C...	888E2...	888E2...	N/A	N/A
da-10-ex01	43	BC39C...	BC39C...	888E2...	888E2...	N/A	N/A

5.10 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	43	Source image will not fit in destination filesystem. Aborting.

5.11 DA-24

DA-24 Verify a valid image.

Hash Matches da-24							
Case	**SRC**	**Ref MD5**	**Tool MD5**	**Ref SHA1**	**Tool SHA1**	**Ref SHA256**	**Tool SHA256**
da-24	43	BC39C...	BC39C...	888E2...	888E2...	N/A	N/A

5.12 DA-25

DA-25 Detect a corrupted image.

Hash Matches da-25							
Case	**SRC**	**Ref MD5**	**Tool MD5**	**Ref SHA1**	**Tool SHA1**	**Ref SHA256**	**Tool SHA256**
da-25	43	BC39C...	4B0CD...	888E2...	AF1C5...	N/A	N/A

6 Summary of Administrative Data

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
01-ata28	palpatine	csr	43	6D	Mon Dec 9 09:54:25 2013
01-ata48	palpatine	csr	4C	2C-SATA	Wed Dec 11 10:13:40 2013
01-fw	palpatine	csr	63-FU2	61-FU2	Thu Dec 12 14:01:14 2013
01-sata28	palpatine	csr	07-SATA	50-SATA	Sun Dec 15 10:19:26 2013
01-sata48	palpatine	csr	16-SATA	22-LAP	Wed Dec 18 10:08:57 2013
01-usb	palpatine	csr	63-FU2	61-FU2	Fri Dec 13 13:46:05 2013
02-cf	palpatine	csr	C1-CF	C2-CF	Mon Dec 23 10:10:09 2013
02-sd	palpatine	csr	A1-SD	A2-SD	Fri Jan 3 10:48:53 2014
02-thumb	palpatine	csr	D5-THUMB	D6-THUMB	Tue Dec 24 13:38:25 2013
04	palpatine	csr	43	66	Mon Dec 23 07:39:42 2013
06-ata28	palpatine	csr	01-IDE-96	NONE	Thu Jan 2 07:36:39 2014
06-ata48	palpatine	csr	4C	NONE	Thu Jan 2 08:06:39 2014
06-fw	palpatine	csr	63-FU2	NONE	Fri Jan 3 09:45:01 2014
06-sata28	palpatine	csr	07-SATA	NONE	Thu Jan 2 09:46:39 2014
06-sata48	palpatine	csr	16-SATA	NONE	Thu Jan 2 10:21:39 2014
06-usb	palpatine	csr	63-FU2	NONE	Fri Jan 3 09:45:01 2014
07-cf	palpatine	csr	C1-CF	NONE	Thu Jan 2 13:45:13 2014
07-sd	palpatine	csr	A1-SD	NONE	Thu Jan 2 09:46:39 2014
07-thumb	palpatine	csr	D5-THUMB	NONE	Thu Jan 2 14:00:13 2014
08-ata28	palpatine	csr	42	39-SATA	Thu May 22 10:14:28 2014
08-dco	palpatine	csr	92	39-SATA	Thu May 22 13:41:47 2014

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
08-sata48	palpatine	csr	1E-SATA	39-SATA	Thu May 22 08:38:33 2014
09-exh100	palpatine	csr	ED-BAD-CPR4	30-SATA	Thu Dec 26 07:33:55 2013
09-exhdonot	palpatine	csr	ED-BAD-CPR4	30-SATA	Thu Dec 26 14:34:50 2013
09-exhtryonce	palpatine	csr	ED-BAD-CPR4	72-SATA-SSD	Fri Dec 27 10:34:25 2013
09-standard100	palpatine	csr	ED-BAD-CPR4	72-SATA-SSD	Fri Dec 27 15:56:22 2013
10-dd	palpatine	csr	43	NONE	Tue Dec 31 11:13:12 2013
10-ex01	palpatine	csr	43	NONE	Tue Dec 31 11:13:30 2013
12	palpatine	csr	43	NONE	Tue Dec 31 10:12:23 2013
24	palpatine	csr	43	NONE	Mon Jan 6 08:56:56 2014
25	palpatine	csr	43	NONE	Mon Jan 6 12:49:22 2014