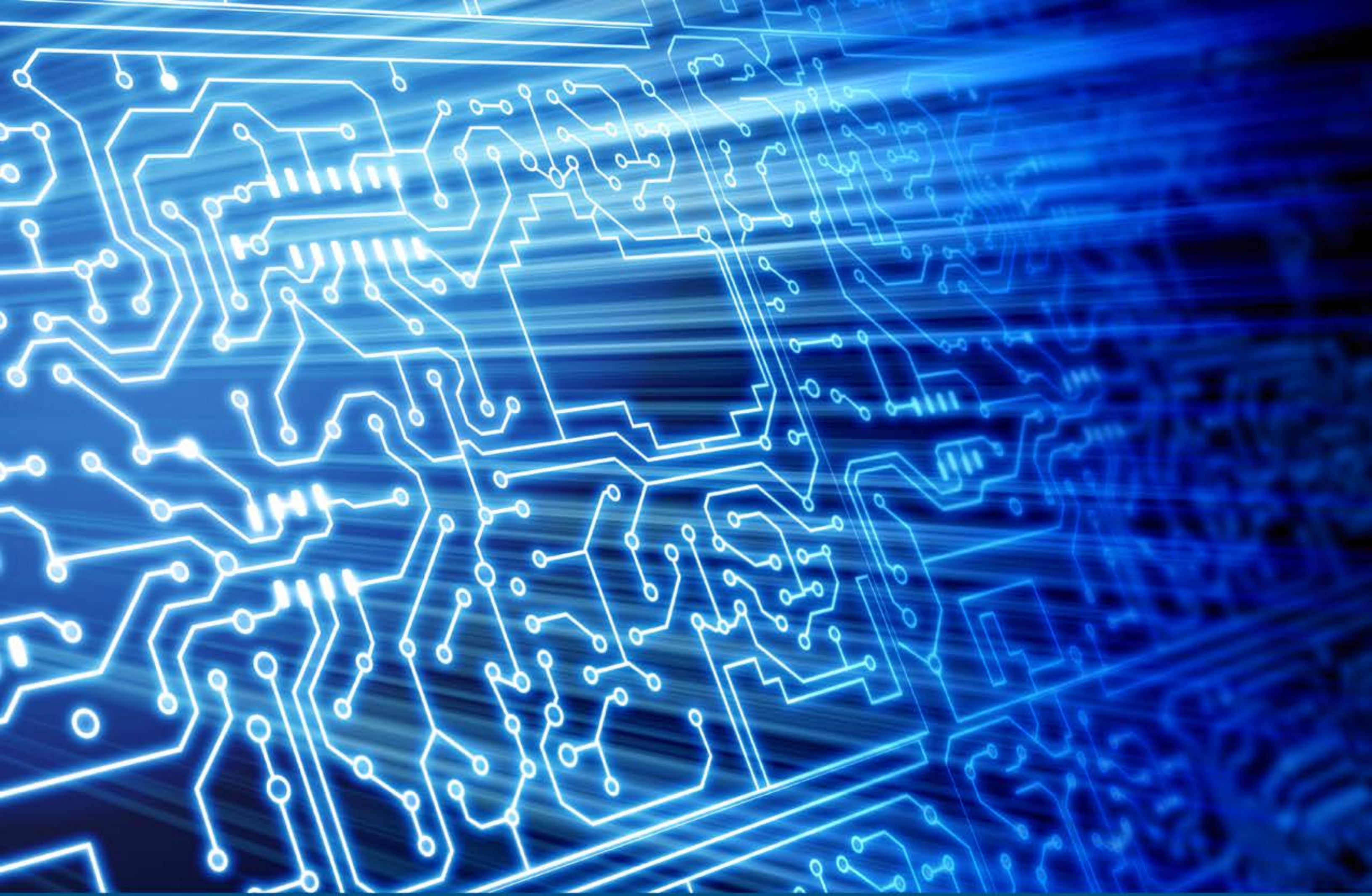

Paladin 4.0

Test Results for Digital Data Acquisition Tool

May 19, 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.

May 2014

Test Results for Digital Data Acquisition Tool:
Paladin 4.0

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 (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 Paladin 4.0 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 Paladin 4.0 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test Results for Digital Data Acquisition Tool

Tool Tested:	Paladin
Software Version:	4.0
Runtime Environment	Paladin 4.0 CD
Supplier:	Sumuri LLC
Address:	P.O. Box 252 Wyoming, Delaware 19934
Tel:	(302) 507-0015
Email:	sales@sumuri.com
WWW:	http://sumuri.com

1 Results Summary

Paladin 4.0 is a modified Live Linux distribution designed to simplify the process of creating forensic images in a forensically sound manner. Paladin 4.0 is designed to image, clone and restore data from hard drives and other secondary storage. Except for the following anomaly, the tool acquired the test media completely and accurately. The tool wrote only the contents of the first image segment when restoring a segmented raw (.dd) image to a clone. The clone operation completed after writing the first 2 GB segment of the image. Data from the four remaining segments were not written to the clone (test case DA-14-SCSI).

An additional observation was made for clone operations where the destination device or partition was larger than the source. When Paladin 4.0 was used to clone a smaller drive to a larger one or a smaller partition to a larger one, the tool wrote 32 sectors of 0's followed by a sector of unknown content to the end of the larger drive or partition. Of the excess sectors on the destination drive or partition, only the last 33 sectors were written to by the tool. This behavior is seen in test cases DA-01, DA-02 and DA-09.

For more result 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 Paladin 4.0 and the linked test cases selected for execution. Table 2 lists the features not available in Paladin 4.0 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
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
Create an image of a drive with hidden sectors	08
Device I/O error generator available	05, 11 & 18
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: FW, SCSI, USB, PATA, and SATA. These are noted as variations on test cases DA-01, DA-06, and DA-14.

The following digital source types were tested: partitions (FAT16, FAT32, FAT32X, EXFAT, NTFS, EXT2, EXT3, EXT4, SWAP, hidden, OSX, OSXC, OSXCJ, OSXJ and OSXU), compact flash (CF) and thumb drive (Thumb). There are two FAT 32 variations testing acquisition of both FAT 32 partition codes 0x0B (FAT32) and 0x0C (FAT32X). These digital source types are noted as variations on test cases DA-02, DA–07 and DA-14.

In addition to raw (.dd), the following image file types are supported by the tool: Expert Witness (.E01), EnCase Evidence File Format Version 2 (.ex01), Apple Disk Image (.dmg) and SMART (.s01). These were tested as alternate as alternate image file formats and are noted as variations on test case DA-10.

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 Paladin 4.0 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-scsi	Expected Results
01-usb	Expected Results
02-cf	Expected Results
02-exFAT	Expected Results
02-ext2	Expected Results
02-ext3	Expected Results
02-ext4	Expected Results
02-f16	Expected Results
02-f32	Expected Results
02-f32x	Expected Results
02-hidden	Expected Results
02-ntfs	Expected Results
02-osxcj	Expected Results
02-swap	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-scsi	Expected Results
06-usb	Expected Results
07-cf	Expected Results
07-exFAT	Expected Results
07-ext2	Expected Results
07-ext3	Expected Results
07-ext4	Expected Results
07-f16	Expected Results
07-f32	Expected Results

Test case Results	
Case	**Results**
07-f32x	Expected Results
07-hidden	Expected Results
07-nt	Expected Results
07-osx	Expected Results
07-osxc	Expected Results
07-osxcj	Expected Results
07-osxj	Expected Results
07-osxu	Expected Results
07-swap	Expected Results
07-thumb	Expected Results
09	Expected Results
10-dmg	Expected Results
10-e01	Expected Results
10-ex01	Expected Results
10-s01	Expected Results
14-ata28	Expected Results
14-ata48	Expected Results
14-cf	Expected Results
14-dmg	Expected Results
14-e01	Expected Results
14-ex01	Expected Results
14-exFAT	Expected Results
14-ext2	Expected Results
14-ext3	Expected Results
14-ext4	Expected Results
14-f16	Expected Results
14-f32	Expected Results
14-f32x	Expected Results
14-fw	Expected Results
14-hidden	Expected Results
14-nt	Expected Results
14-osx	Expected Results
14-osxc	Expected Results
14-osxcj	Expected Results
14-osxj	Expected Results
14-osxu	Expected Results
14-s01	Expected Results
14-sata28	Expected Results
14-sata48	Expected Results
14-scsi	Unexpected Results
14-swap	Expected Results
14-thumb	Expected Results
14-usb	Expected Results

Test case Results	
Case	**Results**
17	Expected Results
24	Expected Results
25	Expected Results
26-dd2dmg	Expected Results
26-dd2e01	Expected Results
26-dd2ex01	Expected Results
26-dd2s01	Expected Results
26-dmg2dd	Expected Results
26-e012dd	Expected Results
26-ex012dd	Expected Results
26-s012dd	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*

Tests were run from the Paladin 4.0 CD.

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 Paladin 4.0 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-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-14 measures the tool’s ability to create a clone from an image
file to a destination. The expected result is for all source sectors to match corresponding destination sectors in a sector-by-sector comparison.

Test case DA-17 measures the tool’s ability to create a clone from an image file when the destination is smaller than the source used to create the image file. 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-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.

Test case DA-26 measures the tool’s ability to convert an image to an alternate image format. The expected result is for a hash value reported by the tool should 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	390721968	0
da-01-fw	63-fu2	117304992	0
da-01-sata28	07-sata	156301488	0
da-01-sata48	16-sata	312581808	0
da-01-scsi	2A	17783249	0
da-01-usb	63-FU2	117304992	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-01-ata28	52792	32	0	52759	1
da-01-fw	43531488	32	0	43531455	1
da-01-scsi	21319087	32	0	21319054	1

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-ext2	01-ide-96	10490382	0

Differences Between SRC & DST da-02			
Case-DS	**SRC**	**Compared**	**Differ**
da-02-ext4	49-sata	7807590	0
da-02-f16	01-ide-96	2104452	0
da-02-f32	01-ide-96	8401932	0
da-02-f32x	01-ide-96	20980827	0
da-02-hidden	01-ide-96	4192902	0
da-02-nt	01-ide-96	27744192	0
da-02-osx	4b-sata	10485536	0
da-02-osxc	4b-sata	4194304	0
da-02-osxcj	4b-sata	4194304	0
da-02-osxj	4b-sata	20971520	0
da-02-osxu	4b-sata	6291456	0
da-02-swap	01-ide-96	4208967	0
da-02-thumb	d5-thumb	505856	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-02-ext2	2088450	28877	0	2059522	8
da-02-ext4	2637210	139	0	2637066	2
da-02-f16	2168775	32	0	2168742	1
da-02-f32x	1429785	32	0	1429752	1
da-02-nt	3711015	32	0	3710982	1
da-02-osxc	1985216	32	0	1985183	1
da-02-osxcj	1985216	32	0	1985183	1
da-02-osxj	2012336	39	0	2012295	2
da-02-osxu	2093304	64290	0	2028241	580
da-02-thumb	3495904	32	0	3495871	1

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	f6	19925880	0

Message to User da-04		
Case	**SRC**	**Message**
da-04	f6	Something wrong. Check the live logs.

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	43	BC39C...	BC39C...	888E2...	888E2...	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
da-06-sata28	01-SATA	0A49B...	0A49B...	49512...	49512...	N/A	N/A
da-06-sata48	16-SATA	7BB1D...	7BB1D...	F8298...	F8298...	N/A	N/A
da-06-scsi	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	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**

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-exFAT	49-SATA	E8578…	E8578…	3D44F…	3D44F…	N/A	N/A
da-07-ext2	01-IDE-96	3BE24…	3BE24…	4E0A1…	4E0A1…	N/A	N/A
da-07-ext3	49-SATA	A2517…	A2517…	FDF0F…	FDF0F…	N/A	N/A
da-07-ext4	49-SATA	567F2…	567F2…	F28A7…	F28A7…	N/A	N/A
da-07-f16	01-IDE-96	8B24F…	8B24F…	074BA…	074BA…	N/A	N/A
da-07-f32	01-IDE-96	BFF7D…	BFF7D…	B861D…	B861D…	N/A	N/A
da-07-f32x	01-IDE-96	B5BFD…	B5BFD…	30BA6…	30BA6…	N/A	N/A
da-07-hidden	01-IDE-96	5A165…	5A165…	D10BD…	D10BD…	N/A	N/A
da-07-nt	01-IDE-96	92B27…	92B27…	0FBA4…	0FBA4…	N/A	N/A
da-07-osx	4B-SATA	AEEAC…	AEEAC…	3DE70…	3DE70…	N/A	N/A
da-07-osxc	4B-SATA	D7311…	D7311…	2D630…	2D630…	N/A	N/A
da-07-osxcj	4B-SATA	F9F89…	F9F89…	29EA0…	29EA0…	N/A	N/A
da-07-osxj	4B-SATA	8BF36…	8BF36…	37311…	37311…	N/A	N/A
da-07-osxu	4B-SATA	E7E35…	E7E35…	D102A…	D102A…	N/A	N/A
da-07-swap	01-IDE-96	275AC…	275AC…	DFC37…	DFC37…	N/A	N/A
da-07-thumb	D5-THUMB	C8435…	C8435…	D6852…	D6852…	N/A	N/A

5.6 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	ed-bad-cpr4	120103200	35

Faulty Drives

Case	Drive	Faulty Sectors
da-09	ed-bad-cpr4	35

Excess Sector Analysis

Case	Excess	Zero	Src Fill	Dst Fill	Other
da-09	36198288	32	0	36198255	1

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-dmg	42	F4B9A…	F4B9A…	5A753…	5A753…	N/A	N/A
da-10-e01	42	F4B9A…	F4B9A…	5A753…	5A753…	N/A	N/A
da-10-ex01	42	F4B9A…	F4B9A…	5A753…	5A753…	N/A	N/A
da-10-s01	42	F4B9A…	F4B9A…	5A753…	5A753…	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	63-FU2	something wrong. Check the Live logs.

5.9 DA-14

DA-14 Create an unaligned clone from an image file.

Differences Between SRC & DST da-14			
Case-Image	**SRC**	**Compared**	**Differ**
da-14-F32	01-ide-96	8401932	0
da-14-ata28	43	78125000	0
da-14-ata48	4C	390721968	0
da-14-cf	c1-cf	503808	0
da-14-dmg	42	78165360	0
da-14-e01	42	78165360	0
da-14-ex01	42	78165360	0
da-14-exFAT	49-sata	10485760	0
da-14-ext2	01-ide-96	10490382	0
da-14-ext3	49-sata	5863725	0
da-14-ext4	49-sata	7807590	0
da-14-f16	01-ide-96	2104452	0
da-14-f32x	01-ide-96	20980827	0
da-14-fw	63-FU2	117304992	0
da-14-hidden	01-ide-96	4192902	0
da-14-nt	01-ide-96	27744192	0
da-14-osx	4b-sata	10485536	0
da-14-osxc	4b-sata	4194304	0
da-14-osxcj	4b-sata	4194304	0
da-14-osxj	4b-sata	20971520	0
da-14-osxu	4b-sata	6291456	0
da-14-s01	42	78165360	0
da-14-sata28	01-sata	156301488	0
da-14-sata48	16-sata	312581808	0
da-14-scsi	2A	17783249	13687249
da-14-swap	01-ide-96	4208967	0
da-14-thumb	d5-thumb	505856	0
da-14-usb	63-FU2	117304992	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-14-F32	1863477	0	0	1863477	0
da-14-ata28	41978200	0	0	41978200	0
da-14-dmg	41937840	0	0	41937840	0
da-14-ex01	41937840	0	0	41937840	0
da-14-exFAT	2809856	4096	0	2805760	0
da-14-ext2	1895670	28401	0	1867206	15
da-14-ext3	2522142	37158	0	2484914	16
da-14-ext4	2682792	36142	0	2646640	2
da-14-f16	1895670	0	0	1895670	0
da-14-f32x	1381590	0	0	1381590	0
da-14-fw	43531488	0	0	43531488	0
da-14-nt	3711015	0	0	3711014	1
da-14-osx	1891464	14	0	1891448	2
da-14-osxc	1883264	0	0	1883264	0
da-14-osxcj	1883264	0	0	1883264	0
da-14-osxj	5756168	14	0	5756152	2
da-14-osxu	2117208	65262	0	2051167	584
da-14-sata28	4534992	0	0	4534992	0
da-14-sata48	78140160	0	0	78140160	0
da-14-scsi	2142631	0	0	2142631	0
da-14-scsi-2	2142631	0	0	2142631	0
da-14-thumb	3495904	0	0	3495904	0

5.10 DA-14 Anomalies

Anomalies Observed

Anomalies Observed in da-14	
Case	**Anomaly**
da-14-scsi	Some sectors differ: [13687249]

5.11 DA-17

DA-17 Create a truncated clone from an image file.

Differences Between SRC & DST da-17			
Case	SRC	Compared	Differ
da-17	43	19925880	0

Message to User da-17		
Case	SRC	Message
da-17	43	something wrong. check the system logs.

5.12 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

5.13 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...	E8270...	888E2...	15B8F...	N/A	N/A

5.14 DA-25

Observation

Observed in da-25	
Case	Behavior
da-25	MD5 mismatch [BC39C...] vs [E8270...]
da-25	SHA1 mismatch [888E2...] vs [15B8F...]

5.15 DA-26

DA-26 Convert an image to an alternate image file format.

Hash Matches da-26							
Case	SRC	Ref MD5	Tool MD5	Ref SHA1	Tool SHA1	Ref SHA256	Tool SHA256
da-26-dd2dmg	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-dd2e01	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-dd2ex01	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-dd2s01	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-dmg2dd	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-e012dd	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-ex012dd	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A
da-26-s012dd	2A	91E0A...	91E0A...	F5F9F...	F5F9F...	N/A	N/A

6 Summary of Administrative Data

Summary of Administrative Data					
Case	Host	Who	Source	Destination	Date

Summary of Administrative Data

Case	Host	Who	Source	Destination	Date
01-ata28	DeathStar	csr	43	7B	Wed Apr 3 12:57:30 2013
01-ata48	Chefong	csr	4C	27-IDE	Wed Apr 3 14:57:46 2013
01-fw	Chefong	csr	63-FU2	84-FU2	Fri Apr 5 10:49:04 2013
01-sata28	DeathStar	csr	07-SATA	25-SATA	Wed Apr 3 16:08:29 2013
01-sata48	Chefong	csr	16-SATA	22-LAP	Thu Apr 4 11:50:03 2013
01-scsi	frank	csr	2A	8F	Sat Apr 6 09:14:48 2013
01-usb	DeathStar	csr	63-FU2	61-FU2	Thu Apr 4 13:14:04 2013
02-cf	Palpatine	csr	C1-CF	C2-CF	Mon Apr 15 11:43:24 2013
02-ext2	palpatine	csr	01-IDE-96	69-SATA	Fri Oct 25 17:58:32 2013
02-ext4	Joe	csr	49-SATA	23-LAP	Wed Aug 7 08:00:11 2013
02-f16	palpatine	csr	01-IDE-96	69-SATA	Fri Oct 25 18:15:27 2013
02-f32	DeathStar	csr	01-IDE-96	29-SATA	Thr Apr 11 10:15:44 2013
02-f32x	DeathStar	csr	01-IDE-96	29-SATA	Thr Apr 11 10:15:44 2013
02-hidden	DeathStar	csr	01-IDE-96	29-SATA	Thr Apr 11 10:15:44 2013
02-nt	palpatine	csr	01-IDE-96	69-SATA	Fri Oct 25 18:05:33 2013
02-osx	palpatine	csr	4B-SATA	8B	Tue Oct 22 13:18:50 2013
02-osxc	palpatine	csr	4B-SATA	23-LAP	Mon Oct 28 10:31:36 2013
02-osxcj	palpatine	csr	4B-SATA	23-LAP	Mon Oct 28 10:31:36 2013
02-osxj	palpatine	csr	4B-SATA	23-LAP	Mon Oct 28 10:31:36 2013
02-osxu	palpatine	csr	4B-SATA	23-LAP	Mon Oct 28 10:31:36 2013
02-swap	DeathStar	csr	01-IDE-96	29-SATA	Thr Apr 11 10:15:44 2013
02-thumb	Palpatine	csr	D5-THUMB	D6-THUMB	Mon Apr 15 09:43:51 2013
04	Palpatine	csr	F6	66	Thu Apr 18 12:33:42 2013
06-ata28	DeathStar	csr	43	NONE	Mon Apr 15 09:28:18 2013
06-ata48	palpatine	csr	4C	NONE	Sat Apr 6 15:55:19 2013
06-fw	DeathStar	csr	63-FU2	NONE	Sat Apr 6 13:51:48 2013
06-sata28	DeathStar	csr	01-SATA	NONE	Sun Apr 7 10:15:44 2013
06-sata48	Chefong	csr	16-SATA	NONE	Sat Apr 6 10:53:56 2013
06-scsi	frank	csr	2A	NONE	Sat Apr 6 16:05:45 2013
06-usb	DeathStar	csr	63-FU2	NONE	Sat Apr 6 15:49:00 2013
07-cf	Palpatine	csr	C1-CF	NONE	Wed Apr 3 09:47:48 2013
07-exFAT	Palpatine	csr	49-SATA	NONE	Tue Apr 2 15:39:04 2013
07-ext2	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-ext3	Palpatine	csr	49-SATA	NONE	Tue Apr 2 15:39:04 2013
07-ext4	Palpatine	csr	49-SATA	NONE	Tue Apr 2 15:39:04 2013
07-f16	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-f32	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-f32x	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-hidden	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-nt	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-osx	Palpatine	csr	4B-SATA	NONE	Tue Apr 2 16:52:07 2013
07-osxc	Palpatine	csr	4B-SATA	NONE	Tue Apr 2 16:52:07 2013
07-osxcj	Palpatine	csr	4B-SATA	NONE	Tue Apr 2 16:52:07 2013
07-osxj	Palpatine	csr	4B-SATA	NONE	Tue Apr 2 16:52:07 2013
07-osxu	Palpatine	csr	4B-SATA	NONE	Tue Apr 2 16:52:07 2013
07-swap	Palpatine	csr	01-IDE-96	NONE	Tue Apr 2 12:27:16 2013
07-thumb	Palpatine	csr	D5-THUMB	NONE	Wed Apr 3 09:47:48 2013
09	Palpatine	csr	ED-BAD-CPR4	72-SATA-SSD	Wed Apr 3 12:08:38 2013
10-dmg	Palpatine	csr	42	NONE	Sun Apr 21 11:59:27 2013
10-e01	Palpatine	csr	42	NONE	Sun Apr 21 11:59:27 2013
10-ex01	Palpatine	csr	42	NONE	Sun Apr 21 11:59:27 2013
10-s01	Palpatine	csr	42	NONE	Sun Apr 21 11:59:27 2013
12	Palpatine	csr	63-FU2	NONE	Tue Aug 13 12:28:06 2013
14-F32	palpatine	csr	01-IDE-96	6A-SATA	Sun Oct 20 12:59:02 2013
14-ata28	DeathStar	csr	43	6D	Mon Apr 15 10:55:12 2013
14-ata48	palpatine	csr	4C	1C-LAP	Sat Apr 13 12:50:37 2013
14-cf	Palpatine	csr	C1-CF	C2-CF	Mon Apr 15 12:02:28 2013
14-dmg	Palpatine	csr	42	6F	Tue Apr 23 08:32:37 2013
14-e01	palpatine	csr	42	02-IDE	Tue Apr 23 09:41:49 2013
14-ex01	Palpatine	csr	42	6F	Tue Apr 23 13:55:41 2013
14-exFAT	palpatine	csr	49-SATA	8F	Sat Oct 19 10:54:07 2013
14-ext2	palpatine	csr	01-IDE-96	6A-SATA	Sun Oct 20 12:59:02 2013
14-ext3	palpatine	csr	49-SATA	66	Sat Oct 19 14:24:44 2013

Summary of Administrative Data

Case	Host	Who	Source	Destination	Date
14-ext4	palpatine	csr	49-SATA	66	Sat Oct 19 15:58:12 2013
14-f16	palpatine	csr	01-IDE-96	29-SATA	Wed Apr 10 10:48:25 2013
14-f32x	MISSING	csr	01-IDE-96	29-SATA	Wed Apr 10 10:48:25 2013
14-fw	DeathStar	csr	63-FU2	84-FU2	Fri Apr 12 12:37:57 2013
14-hidden	palpatine	csr	01-IDE-96	29-SATA	Wed Apr 10 10:48:25 2013
14-nt	palpatine	csr	01-IDE-96	6A-SATA	Sun Oct 20 12:59:02 2013
14-osx	palpatine	csr	4B-SATA	8B	Tue Oct 22 07:06:21 2013
14-osxc	Palpatine	csr	4B-SATA	23-LAP	Thu Apr 18 10:14:26 2013
14-osxcj	Palpatine	csr	4B-SATA	23-LAP	Thu Apr 18 10:14:26 2013
14-osxj	palpatine	csr	4B-SATA	8B	Sun Oct 20 09:50:09 2013
14-osxu	palatine	csr	4B-SATA	8B	Sat Oct 19 17:12:43 2013
14-s01	palpatine	csr	42	02-IDE	Tue Apr 23 13:53:40 2013
14-sata28	DeathStar	csr	01-SATA	7B-SATA	Sat Apr 13 13:58:22 2013
14-sata48	palpatine	csr	16-SATA	27-IDE	Sat Apr 13 12:53:13 2013
14-scsi	Palpatine	csr	2A	66	Mon Apr 15 13:24:15 2013
14-swap	palpatine	csr	01-IDE-96	29-SATA	Wed Apr 10 10:48:25 2013
14-thumb	Palpatine	csr	D5-THUMB	D6-THUMB	Mon Apr 15 10:36:43 2013
14-usb	DeathStar	csr	63-FU2	61-FU2	Thu Apr 11 09:41:53 2013
17	Palpatine	csr	43	66	Tue Aug 13 14:50:26 2013
24	palpatine	csr	43		Fri Apr 19 11:51:19 2013
25	palpatine	csr	43	NONE	Fri Apr 19 12:46:43 2013
26-dd2dmg	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-dd2e01	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-dd2ex01	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-dd2s01	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-dmg2dd	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-e012dd	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-ex012dd	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013
26-s012dd	palpatine	csr	2A	NONE	Fri Apr 19 20:18:39 2013