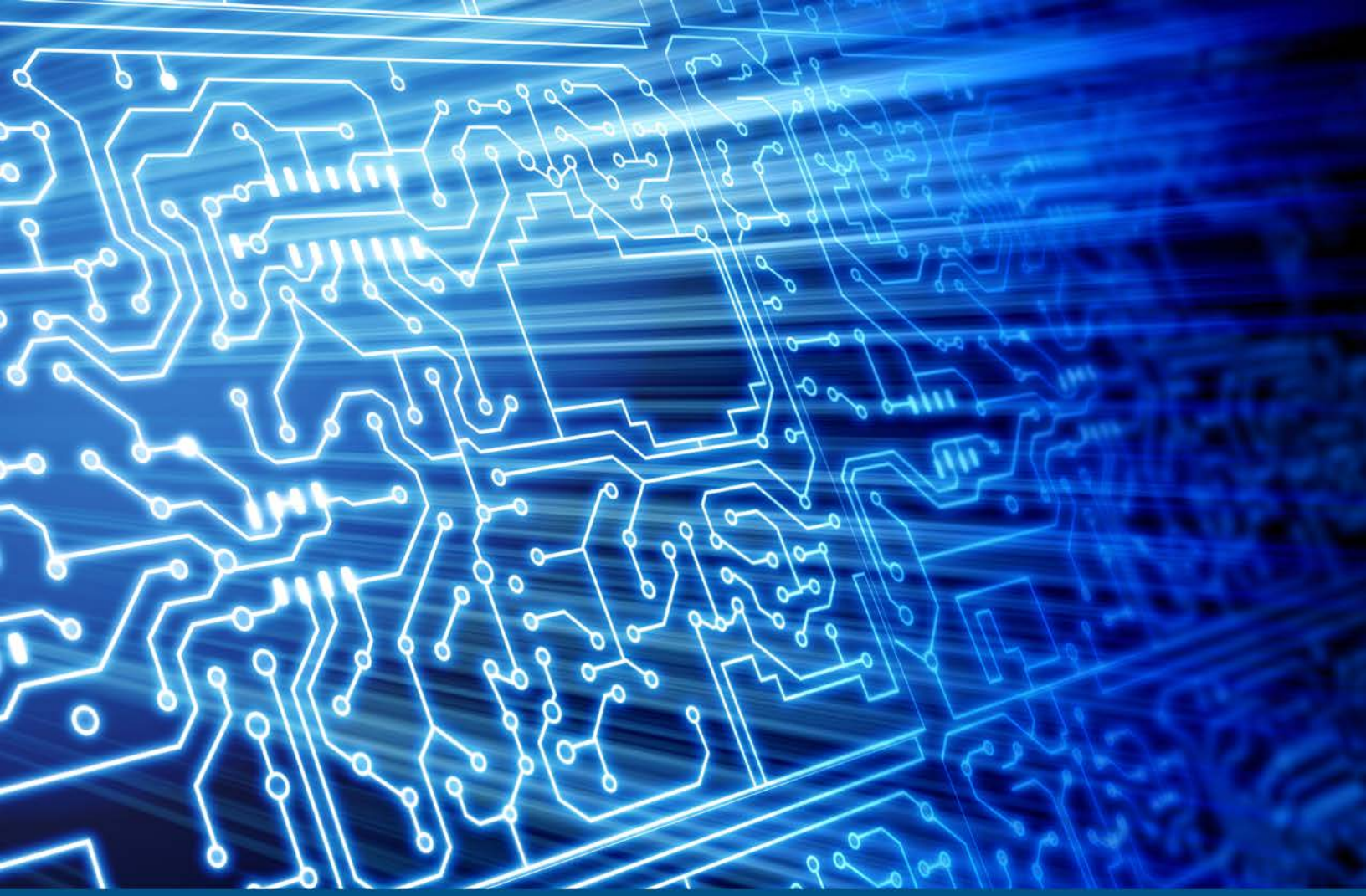

IXImager v3.0.Nov.12.12

Test Results for Digital Data Acquisition Tool

November 18, 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 http://www.dhs.gov/cyber-research.

November 2013

Test Results for Digital Data Acquisition Tool:
IXImager v3.0.Nov.12.12

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

Contents

Introduction 1
How to Read This Report 1
1 Results Summary 2
2 Test Case Selection 2
3 Results by Test Case-Variation 3
4 Testing Environment 5
4.1 Execution Environment 5
4.2 Support Software 5
4.3 Test Drive Creation 5
4.3.1 Source Drive 5
4.3.2 Media Drive 6
4.3.3 Destination Drive 6
4.4 Test Drive Analysis 6
4.5 Note on Test Drives 6
5 Test Results 7
5.1 DA-01 8
5.2 DA-02 9
5.3 DA-04 9
5.4 DA-06 9
5.5 DA-07 9
5.6 DA-08 10
5.7 DA-09 10
5.8 DA-10 10
5.9 DA-12 10
5.10 DA-14 10
5.11 DA-17 11
5.12 DA-24 11
5.13 DA-25 12
5.14 DA-25 Observation 12
6 Summary of Administrative Data 12

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 IXImager v3.0.Nov.12.12 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 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 IXImager v3.0.Nov.12.12 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test Results for Digital Data Acquisition Tool

Tool Tested:	IXImager
Software Version:	v3.0 Nov 12 2012
Runtime Environment	IXImager boot CD-ROM
Supplier:	Perlustro, L.P.
Tel:	(901) 202-5207
Email:	solutions@perlustro.com
WWW:	http://www.perlustro.com/

1 Results Summary

IXImager is a bootable forensics imaging and analysis system that runs from CD-ROM or flash media. When acquiring a hard drive with 35 known faulty sectors, the tool wrote forensically benign content to the image in place of the faulty sectors. The tool acquired all visible and hidden sectors completely and accurately from the test media. For more test result details 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 IXImager and the linked test cases selected for execution. Table 2 lists the features not available in IXImager 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
Create a clone from an image file	14 & 17
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 a n image file	16
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 media and the type of digital object acquired.

The following source interfaces were tested: USB, ATA28, ATA48, FW, SATA28, SATA48, SCSI, and SAS. These are noted as variations on test cases DA-01, DA-06 and DA-14.

The following digital source types were tested: partitions (OSX, OSXJ, OSXC, OSXCJ, OSXU, EXT2, EXT3, EXT4, SWAP, FAT16, FAT32, FAT32X, HIDDEN, exFAT and NTFS), compact flash (CF) and thumb drive (Thumb). These digital source types are noted as variations on test cases DA-02, DA–07 and DA-14.

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

Test Case Results	
Case	**Results**
01-sata28	Expected Results
01-sata48	Expected Results
01-scsi	Expected Results
01-usb	Expected Results
02-cf	Expected Results
02-thumb	Expected Results
04	Expected Results
06-ata28	Expected Results
06-ata48	Expected Results
06-fw	Expected Results
06-sas	Expected Results
06-sata28	Expected Results
06-sata48	Expected Results

Test Case Results	
Case	**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-f32	Expected Results
07-f32x	Expected Results
07-fat16	Expected Results
07-hidden	Expected Results
07-ntfs	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
08-ata28	Expected Results
08-ata48	Expected Results
08-dco	Expected Results
09	Expected Results
10-encrypt	Expected Results
12	Expected Results
14-ata28	Expected Results
14-ata48	Expected Results
14-cf	Expected Results
14-encrypt	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-ntfs	Expected Results
14-osx	Expected Results
14-osxc	Expected Results
14-osxcj	Expected Results
14-osxj	Expected Results

Test Case Results	
Case	**Results**
14-osxu	Expected Results
14-sas	Expected Results
14-sata28	Expected Results
14-sata48	Expected Results
14-scsi	Expected Results
14-swap	Expected Results
14-thumb	Expected Results
14-usb	Expected Results
17	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

IXImager is bootable forensics image and analysis system. The tests were run from the IXImager v3.0 Nov 12 2012 boot 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 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 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 IXImager v3.0 Nov 12 2012 test runs, see http://www.cftt.nist.gov/TBD.

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-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.

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-sas	01-sas	143638992	0
da-01-sata28	07-sata	156301488	0
da-01-sata48	16-sata	312581808	0
da-01-scsi	E0	17938985	0
da-01-usb	63-FU2	117304992	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-01-scsi	21163351	0	0	21163351	0
da-01-fw	38996496	0	0	38996496	0
da-01-usb	2798208	0	0	2798208	0
da-01-ata28	40360	0	0	40360	0
da-01-sas	12662496	0	0	12662496	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-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	01-ide-58	78177792	0

Message to User da-04		
Case	**SRC**	**Message**
da-04	01-ide-58	Error! Your Target device has run out of free space!

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	N/A	N/A	888E2...	888E2...	N/A	N/A
da-06-ata48	4C	N/A	N/A	8FF62...	8FF62...	N/A	N/A
da-06-fw	63-FU2	N/A	N/A	F7069...	F7069...	N/A	N/A
da-06-sas	01-SAS	N/A	N/A	96B00...	96B00...	N/A	N/A
da-06-sata28	4B-SATA	N/A	N/A	70CC6...	70CC6...	N/A	N/A
da-06-sata48	16-SATA	N/A	N/A	F8298...	F8298...	N/A	N/A
da-06-scsi	E0	N/A	N/A	4A694...	4A694...	N/A	N/A
da-06-usb	63-FU2	N/A	N/A	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	N/A	N/A	5B823...	5B823...	N/A	N/A
da-07-exFAT	49-SATA	N/A	N/A	3D44F...	3D44F...	N/A	N/A
da-07-ext2	43	N/A	N/A	283BC...	283BC...	N/A	N/A
da-07-ext3	49-SATA	N/A	N/A	FDF0F...	FDF0F...	N/A	N/A
da-07-ext4	49-SATA	N/A	N/A	F28A7...	F28A7...	N/A	N/A
da-07-f32	43	N/A	N/A	72462...	72462...	N/A	N/A
da-07-f32x	43	N/A	N/A	379C1...	379C1...	N/A	N/A
da-07-fat16	43	N/A	N/A	443CC...	443CC...	N/A	N/A
da-07-hidden	43	N/A	N/A	9D0C9...	9D0C9...	N/A	N/A
da-07-ntfs	43	N/A	N/A	73EB2...	73EB2...	N/A	N/A
da-07-osx	4B-SATA	N/A	N/A	3DE70...	3DE70...	N/A	N/A
da-07-osxc	4B-SATA	N/A	N/A	2D630...	2D630...	N/A	N/A
da-07-osxcj	4B-SATA	N/A	N/A	29EA0...	29EA0...	N/A	N/A

Hash Matches da-07							
Case-DS	**SRC**	**Ref MD5**	**Tool MD5**	**Ref SHA1**	**Tool SHA1**	**Ref SHA256**	**Tool SHA256**
da-07-osxj	4B-SATA	N/A	N/A	37311...	37311...	N/A	N/A
da-07-osxu	4B-SATA	N/A	N/A	D102A...	D102A...	N/A	N/A
da-07-swap	43	N/A	N/A	F5B06...	F5B06...	N/A	N/A
da-07-thumb	D5-THUMB	N/A	N/A	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	SHA1	D76F9...	5A753...	5A753...
da-08-ata48	4B	HPA	SHA1	2D50D...	F4099...	F4099...
da-08-dco	92	DCO	SHA1	55A3C...	63E6F...	63E6F...

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	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	0	0	36198288	0

5.8 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-encrypt	63-FU2	N/A	N/A	F7069...	F7069...	N/A	N/A

5.9 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	07-sata	It appears your target device is smaller then your source device. If you choose to continue this operation, when your target device becomes full you will need to change the output media to complete this operation.

5.10 DA-14

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

Differences Between SRC & DST da-14			
Case-Image	**SRC**	**Compared**	**Differ**

Differences Between SRC & DST da-14			
Case-Image	**SRC**	**Compared**	**Differ**
da-14-ata28	43	78125000	0
da-14-ata48	4C	390721968	0
da-14-cf	c1-cf	503808	0
da-14-encrypt	63-FU2	117304992	0
da-14-exFAT	49-sata	10485760	0
da-14-ext2	43	10490382	0
da-14-ext3	49-sata	5863725	0
da-14-ext4	49-sata	7807590	0
da-14-f16	43	2104452	0
da-14-f32	43	8401932	0
da-14-f32x	43	20980827	0
da-14-fw	63-FU2	117304992	0
da-14-hidden	43	4192902	0
da-14-ntfs	43	27712062	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-sas	01-sas	143638992	0
da-14-sata28	4B-sata	156301488	0
da-14-sata48	16-sata	312581808	0
da-14-scsi	E0	17938985	0
da-14-swap	43	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-fw	2798208	0	0	2798208	0
da-14-sas	12662496	0	0	12662496	0
da-14-sata28	78140160	0	0	78140160	0
da-14-ata28	40360	0	0	40360	0
da-14-thumb	3495904	0	0	3495904	0
da-14-scsi	21163351	0	0	21163351	0

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	4B-sata	78165360	0

Message to User da-17		
Case	**SRC**	**Message**
da-17	4B-sata	Your target device has run out of free space!

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	N/A	N/A	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	4B-SATA	N/A	N/A	70CC6...	33885...	N/A	N/A

5.14 DA-25 Observation

Observed Behavior

Observed in da-25	
Case	**Behavior**
da-25	SHA1 mismatch [70CC6...] vs [33885...]

6 Summary of Administrative Data

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
01-ata28	CheFong	csr	43	02-IDE	Wed Nov 28 07:27:28 2012
01-ata48	nihilus	csr	4C	33-SATA	Wed Nov 28 07:24:13 2012
01-fw	CheFong	csr	63-FU2	30-SATA	Wed Nov 28 14:38:40 2012
01-sas	CheFong	csr	01-SAS	06-SATA	Tue Nov 27 13:06:21 2012
01-sata28	Palpatine	csr	07-SATA	25-SATA	Wed Nov 28 18:39:48 2012
01-sata48	nihilus	csr	16-SATA	41-SATA	Thu Nov 29 14:49:13 2012
01-scsi	Frank	csr	E0	9E	Tue Nov 27 16:06:19 2012
01-usb	CheFong	csr	63-FU2	6F	Wed Nov 28 10:33:02 2012
02-cf	nihilus	csr	C1-CF	C2-CF	Mon Dec 3 12:10:46 2012
02-thumb	CheFong	csr	D5-THUMB	D6-THUMB	Mon Dec 3 12:18:57 2012
04	Palpatine	csr	01-IDE-58	7B	Mon Dec 10 08:25:54 2012
06-ata28	nihilus	csr	43	NONE	Sat Dec 1 10:02:38 2012
06-ata48	nihilus	csr	4C	NONE	Sat Dec 1 11:44:06 2012
06-fw	nihilus	csr	63-FU2	NONE	Sat Dec 1 13:47:39 2012
06-sas	CheFong	csr	01-SAS	NONE	Fri Nov 30 15:39:29 2012
06-sata28	nihilus	csr	4B-SATA	NONE	Fri Nov 30 12:57:01 2012
06-sata48	CheFong	csr	16-SATA	NONE	Fri Nov 30 14:26:31 2012
06-scsi	Frank	csr	E0	NONE	Thu Nov 29 17:51:26 2012
06-usb	nihilus	csr	63-FU2	NONE	Sat Dec 1 12:36:32 2012
07-cf	CheFong	csr	C1-CF	NONE	Tue Dec 4 07:35:13 2012
07-exFAT	CheFong	csr	49-SATA	NONE	Wed Dec 5 15:03:54 2012
07-ext2	CheFong	csr	43	NONE	Thu Dec 6 12:10:56 2012
07-ext3	CheFong	csr	49-SATA	NONE	Wed Dec 5 15:03:54 2012
07-ext4	CheFong	csr	49-SATA	NONE	Wed Dec 5 15:03:54 2012
07-f32	CheFong	csr	43	NONE	Thu Dec 6 12:07:28 2012
07-f32x	CheFong	csr	43	NONE	Thu Dec 6 12:10:56 2012
07-fat16	CheFong	csr	43	NONE	Thu Dec 6 12:13:23 2012
07-hidden	CheFong	csr	43	NONE	Thu Dec 6 12:27:31 2012
07-ntfs	CheFong	csr	43	NONE	Thu Dec 6 12:15:27 2012
07-osx	CheFong	csr	4B-SATA	NONE	Thu Dec 6 13:10:56 2012
07-osxc	CheFong	csr	4B-SATA	NONE	Thu Dec 6 13:10:56 2012
07-osxcj	CheFong	csr	4B-SATA	NONE	Thu Dec 6 13:10:56 2012
07-osxj	CheFong	csr	4B-SATA	NONE	Thu Dec 6 13:10:56 2012
07-osxu	CheFong	csr	4B-SATA	NONE	Thu Dec 6 13:10:56 2012
07-swap	CheFong	csr	43	NONE	Thu Dec 6 12:17:31 2012
07-thumb	CheFong	csr	D5-THUMB	NONE	Tue Dec 4 07:41:37 2012
08-ata28	Chefong	csr	42	NONE	Sun May 19 10:57:33 2013
08-ata48	chefong	csr	4B	NONE	Sat May 18 10:53:29 2013
08-dco	Chefong	csr	92	NONE	Wed Jun 12 10:29:42 2013

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
09	nihilus	csr	ED-BAD-CPR4	29-LAP	Mon Dec 10 07:35:45 2012
10-encrypt	CheFong	csr	63-FU2	NONE	Mon Dec 10 07:57:08 2012
12	nihilus	csr	07-SATA	NONE	Tue Jan 29 12:06:03 2013
14-ata28	nihilus	csr	43	08-IDE	Sun Dec 2 11:00:47 2012
14-ata48	CheFong	csr	4C	33-SATA	Sat Dec 1 16:07:22 2012
14-cf	CheFong	csr	C1-CF	NONE	Tue Dec 4 07:41:37 2012
14-encrypt	CheFong	csr	63-FU2	61-FU2	Mon Dec 10 13:31:52 2012
14-exFAT	Chefong	csr	49-SATA	9E	Sat Dec 8 14:41:59 2012
14-ext2	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-ext3	CheFong	csr	49-SATA	9E	Sat Dec 8 11:14:03 2012
14-ext4	CheFong	csr	49-SATA	9E	Sat Dec 8 11:14:03 2012
14-f16	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-f32	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-f32x	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-fw	nihilus	csr	63-FU2	6F	Sat Dec 1 15:34:00 2012
14-hidden	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-ntfs	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-osx	CheFong	csr	4B-SATA	08-IDE	Sun Dec 9 10:42:03 2012
14-osxc	CheFong	csr	4B-SATA	08-IDE	Sun Dec 9 10:42:03 2012
14-osxcj	CheFong	csr	4B-SATA	08-IDE	Sun Dec 9 10:42:03 2012
14-osxj	CheFong	csr	4B-SATA	08-IDE	Sun Dec 9 10:42:03 2012
14-osxu	CheFong	csr	4B-SATA	08-IDE	Sun Dec 9 10:42:03 2012
14-sas	CheFong	csr	01-SAS	83	Sat Dec 1 16:08:17 2012
14-sata28	CheFong	csr	4B-SATA	19-SATA	Sat Dec 1 16:09:47 2012
14-sata48	nihilus	csr	16-SATA	41-SATA	Sat Dec 1 15:36:16 2012
14-scsi	Frank	csr	E0	8F	Fri Nov 30 17:03:34 2012
14-swap	CheFong	csr	43	6D	Fri Dec 7 15:57:54 2012
14-thumb	CheFong	csr	D5-THUMB	D6-THUMB	Tue Jan 8 08:54:56 2013
14-usb	nihilus	csr	63-FU2	61-FU2	Sun Dec 2 09:28:10 2012
17	nihilus	csr	4B-SATA	02-IDE	Tue Dec 11 15:01:14 2012
24	nihilus	csr	43	NONE	Wed Dec 12 12:25:32 2012
25	nihilus	csr	4B-SATA	NONE	Mon Dec 17 10:44:15 2012