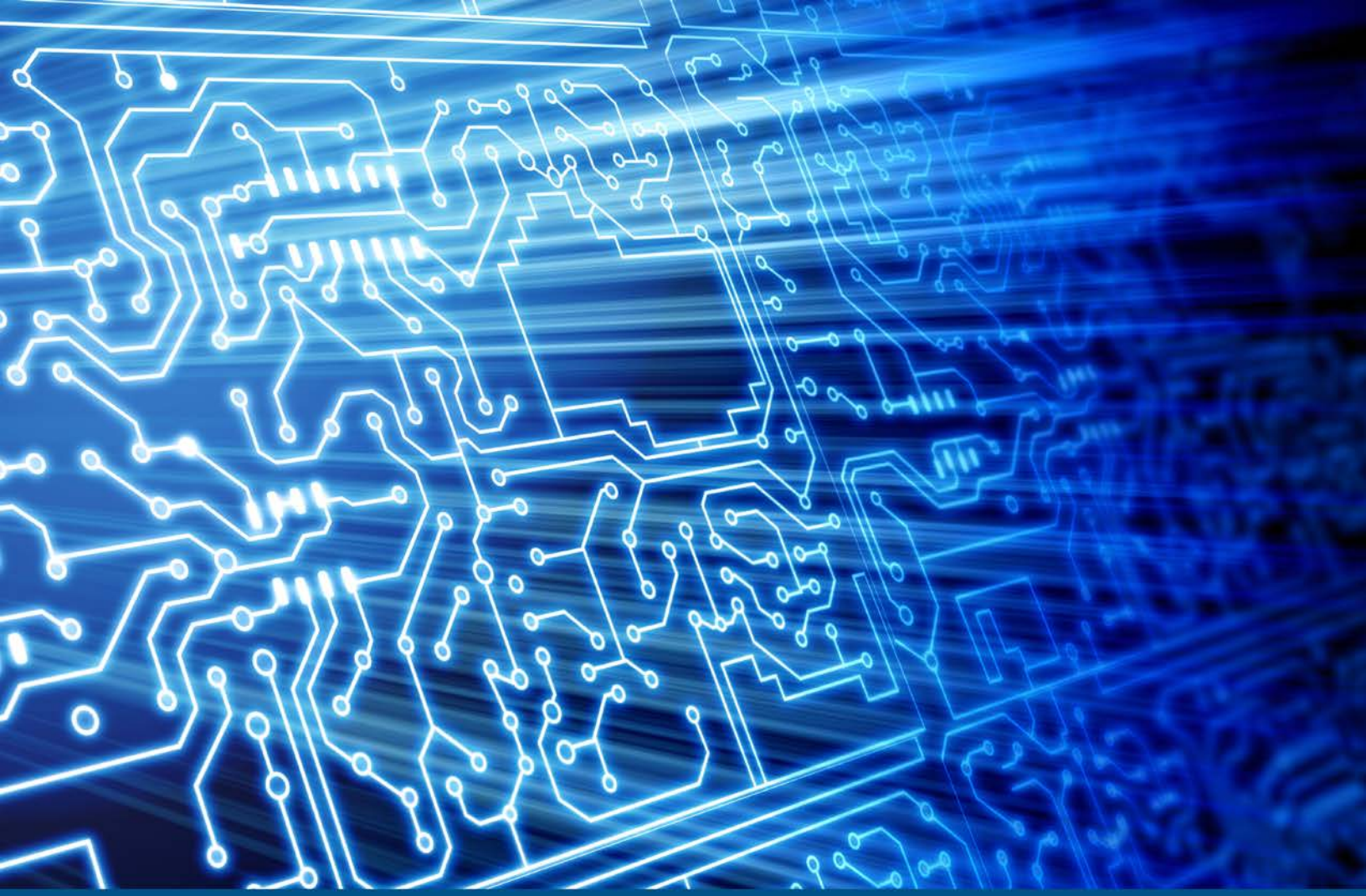

Image MASSter Solo-4 Forensic

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:
Image MASSter Solo-4 Forensic

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 Image MASSter Solo-4 Forensic 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 or at the Department of Homeland Security Web page, https://www.cyberfetch.org/public.

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 Image MASSter Solo-4 Forensic test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test Results for Digital Data Acquisition Tool

Tool Tested:	Imager MASSter Solo-4 Forensic
Software Version:	v4.10.29.0 x32
Firmware Version:	v1.33.0.0 x32
Supplier:	Intelligent Computer Solutions, Inc
Address:	10030 Remmet Ave. Chatsworth, CA 91311
Tel:	(888) 994-4678
Email:	salesmail@ics-iq.com
WWW:	http://www.ics-iq.com/

1 Results Summary

The Imager MASSter Solo-4 Forensic system is a portable data acquisition device. The unit provides native interface support for SAS, SATA and USB drives in addition to supporting PATA. The tool acquired the test media completely and accurately. The following restore anomaly was observed.

- In test case DA-10-encrypt the tool's "Encrypt Destination Files" setting was used to acquire a source drive to an encrypted image file. In DA-14-encrypt, the image file created in DA-10-encrypt was restored to a drive. When the restored drive was compared to the source, only 1,571,229 sectors out of 156,301,488 sectors matched. The vendor plans to address this issue in a future software release and recommends not using the "Encrypt Destination Files" setting until it is corrected.

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 Imager MASSter Solo-4 Forensic and the linked test cases selected for execution. Table 2 lists the features not available in Imager MASSter Solo-4 Forensic 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
Fill excess sectors on a clone device	17
Fill excess sectors on a clone acquisition	19
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 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, type of digital object acquired, image file format, and the way that sectors are hidden on a drive.

The following source interfaces were tested: USB, ATA28, ATA48, SATA28, SATA48, and SAS. These are noted as variations on test cases DA-01, DA-06, DA-08 and DA-14.

The following digital source types were tested: 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.

The following image file types are supported by the tool: E01, E01 compressed and encrypted. These were tested 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 Solo-4 Forensic test runs, see http://www.cftt.nist.gov/TBD.

Test Case Results	
Case	**Results**
01-sas	Expected Results
01-sata28	Expected Results
01-sata48	Expected Results
01-usb	Expected Results
02-cf	Expected Results
02-thumb	Expected Results
04	Expected Results
06-sas	Expected Results
06-sata28	Expected Results
06-sata48	Expected Results
06-usb	Expected Results
07-cf	Expected Results
07-thumb	Expected Results
08-ata28	Expected Results
08-ata48	Expected Results
08-dco	Expected Results
09-abort	Expected Results
09-skipbloc	Expected Results
09-skipsec	Expected Results
10-encrypt	Expected Results
10-E01	Expected Results
10-comp	Expected Results
12	Expected Results
14-sata28	Expected Results
14-sata48	Expected Results
14-cf	Expected Results
14-encrypt	Not Expected
14-sas	Expected Results
14-thumb	Expected Results
14-usb	Expected Results
17	Expected Results
19	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

Image MASSter Solo-4 Forensic is a custom hardware device. The tests were run on the Image MASSter Solo-4 Forensic unit running software version v4.10.29.0 x32 and firmware version v1.33.0.0 x32.

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 then the excess destination sectors are scanned and 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 Image MASSter Solo-4 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-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-19 measures the tool's ability to fill excess sectors on a clone acquisition. The expected result is that the tool writes benign data content to the excess sectors on the destination drive.

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-sas	01-sas	143638992	0
da-01-sata28	01-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-usb	38996496	0	0	38996496	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-sata	120103200	0

Message to User da-04		
Case	**SRC**	**Message**
da-04	01-sata	Source Drive is larger than the Destination drive. Do you wish to continue?

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-sas	01-SAS	N/A	N/A	96B00...	96B00...	N/A	N/A
da-06-sata28	01-SATA	N/A	N/A	49512...	49512...	1AA01...	1AA01...
da-06-sata48	16-SATA	7BB1D...	7BB1D...	N/A	N/A	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	776DF...	776DF...	N/A	N/A	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. Note that for test case da-09-abort a tool option was set to abort if a faulty sector is encountered. The tool aborts when the first 1024 sector block with a faulty sector is encountered at LBA 6,160,328. Only 6,159,360 sectors of the 120,103,200 total number of sectors on the drive were acquired, with 113,943,840 sectors not acquired. This is the expected tool behavior for the selected option.

Differences Between SRC & DST da-09			
Case	**SRC**	**Compared**	**Differ**
da-09-abort	ed-bad-cpr4	120103200	113943840
da-09-skipbloc	ed-bad-cpr4	120103200	35
da-09-skipsec	ed-bad-cpr4	120103200	35

Faulty Drives		
Case	**Drive**	**Faulty Sectors**
da-09-abort	ed-bad-cpr4	35
da-09-skipbloc	ed-bad-cpr4	35
da-09-skipsec	ed-bad-cpr4	35

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-09-abort	36198288	0	0	36198288	0
da-09-skipbloc	36146800	0	0	36146800	0
da-09-skipsec	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-E01	01-SATA	N/A	N/A	49512...	49512...	N/A	N/A
da-10-comp	01-SATA	N/A	N/A	49512...	49512...	N/A	N/A
da-10-encrypt	01-SATA	N/A	N/A	N/A	N/A	1AA01...	1AA01...

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	F6	Operation Failed. Please refer to logs for details.

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**
da-14-E01	01-sata	156301488	0
da-14-cf	c1-cf	503808	0
da-14-comp	01-sata	156301488	0
da-14-encrypt	01-sata	156301488	154730259
da-14-sas	01-sas	143638992	0
da-14-sata28	01-sata	156301488	0
da-14-sata48	16-sata	312581808	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-sata28	39511584	0	0	39511584	0
da-14-thumb	3495904	0	0	3495904	0
da-14-usb	38996496	0	0	38996496	0

5.11 DA-14 Anomalies

Anomalies Observed

Anomalies Observed in da-14	
Case	**Anomaly**
da-14-encrypt	Some sectors differ: [154730259]

5.12 DA-17

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

Differences Between SRC & DST da-17			
Case	**SRC**	**Compared**	**Differ**
da-17	01-sata	N/A	N/A

Message to User da-17		
Case	**SRC**	**Message**
da-17	01-sata	Operation Failed. Please refer to logs for more details.

5.13 DA-19

DA-19 Acquire a physical device to an unaligned clone, filling excess sectors.

Differences Between SRC & DST da-19			
Case	**SRC**	**Compared**	**Differ**
da-19	01-sata	156301488	0

Excess Sector Analysis					
Case	**Excess**	**Zero**	**Src Fill**	**Dst Fill**	**Other**
da-19	78140160	78140160	0	0	0

5.14 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	C1-CF	776DF...	776DF...	5B823...	5B823...	C7CF0...	C7CF0...

5.15 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	D5-THUMB	N/A	N/A	D6852...	2F1A9...	N/A	N/A

6 Summary of Administrative Data

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
01-sas	solo4	csr	01-SAS	06-SATA	Tue Nov 20 15:37:56 2012
01-sata28	solo4	csr	01-SATA	29-SATA	Tue Nov 6 15:04:04 2012
01-sata48	solo4	csr	16-SATA	43-SATA	Tue Nov 6 17:27:00 2012
01-usb	solo4	csr	63-FU2	50-IDE	Thu Nov 8 13:53:08 2012
02-cf	solo4	csr	C1-CF	C2-CF	Fri Nov 9 08:38:09 2012
02-thumb	solo4	csr	D5-THUMB	D6-THUMB	Fri Nov 9 10:29:15 2012
04	solo4	csr	01-SATA	6F	Fri Nov 9 14:47:30 2012
06-sas	solo4	csr	01-SAS	NONE	Wed Nov 21 07:34:21 2012
06-sata28	solo4	csr	01-SATA	NONE	Sat Nov 10 17:50:41 2012
06-sata48	solo4	csr	16-SATA	NONE	Sat Nov 10 17:48:45 2012
06-usb	solo4	csr	63-FU2	NONE	Sun Nov 11 13:59:21 2012
07-cf	solo4	csr	C1-CF	NONE	Sat Nov 10 16:59:21 2012
07-thumb	solo4	csr	D5-THUMB	NONE	Sat Nov 10 16:58:24 2012
08-ata28	solo4	csr	42	NONE	Sat May 18 09:32:41 2013
08-ata48	solo4	csr	4B	NONE	Fri May 17 14:02:18 2013
08-dco	solo4	csr	92	NONE	Fri May 17 09:17:40 2013
09-abort	solo4	csr	ED-BAD-CPR4	29-LAP	Fri Nov 16 17:18:17 2012
09-skipbloc	solo4	csr	ED-BAD-CPR4	7C-SATA	Sat Nov 17 13:02:11 2012
09-skipsec	solo4	csr	ED-BAD-CPR4	4D-SATA	Fri Nov 16 18:14:01 2012
10-E01	solo4	csr	01-SATA	NONE	Fri Nov 16 08:03:00 2012
10-comp	solo4	csr	01-SATA	NONE	Fri Nov 16 07:58:31 2012
10-encrypt	solo4	csr	01-SATA	NONE	Fri Nov 16 08:01:11 2012

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
12	solo4	csr	F6	NONE	Sat Nov 17 14:25:59 2012
14-E01	solo4	csr	01-SATA	25-SATA	Fri Nov 16 08:22:26 2012
14-cf	solo4	csr	C1-CF	C2-CF	Mon Nov 12 14:49:40 2012
14-comp	solo4	csr	01-SATA	06-SATA	Fri Nov 16 11:56:10 2012
14-encrypt	solo4	csr	01-SATA	29-LAP	Fri Nov 16 16:03:49 2012
14-sas	solo4	csr	01-SAS	02-SAS	Wed Nov 21 09:30:29 2012
14-sata28	solo4	csr	01-SATA	22-IDE	Sun Nov 11 17:14:47 2012
14-sata48	solo4	csr	16-SATA	16-LAP	Sun Nov 11 17:00:53 2012
14-thumb	solo4	csr	D5-THUMB	D6-THUMB	Mon Nov 12 14:50:58 2012
14-usb	solo4	csr	63-FU2	05-SATA	Tue Nov 13 11:51:52 2012
17	solo4	csr	01-SATA	57-IDE	Mon Nov 19 09:02:09 2012
19	solo4	csr	01-SATA	NONE	Mon Nov 19 11:29:34 2012
24	solo4	csr	C1-CF	NONE	Tue Nov 20 07:54:19 2012
25	solo4	csr	D5-THUMB	NONE	Wed Nov 21 16:42:36 2012