



DCFLDD 1.3.4-1

Test Results for Digital Data Acquisition Tool

December 27, 2013



**Homeland
Security**

Science and Technology

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

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

December 2013

**Test Results for Digital Data Acquisition Tool:
DCFLDD 1.3.4-1**

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	7
5 Test Results.....	7
5.1 DA-01	8
5.2 DA-02	8
5.3 DA-04	9
5.4 DA-06	9
5.5 DA-07	9
5.6 DA-09	9
5.7 DA-09 Anomalies	10
5.8 DA-12	10
5.9 DA-14	10
5.10 DA-17	11
6 Summary of Administrative Data	11

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 DCFLDD 1.3.4-1 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 DCFLDD 1.3.4-1 test runs, see <http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html>.

Test Results for Digital Data Acquisition Tool

Tool Tested: DCFLDD
Software Version: 1.3.4-1 19 Dec 2006
Runtime Environment: Ubuntu Desktop 12.10 Linux

Supplier: Sourceforge.net

Email: nickharbour@gmail.com
WWW: <http://dcfldd.sourceforge.net/>

1 Results Summary

DCFLDD is an enhanced version of GNU dd with features useful for forensics and security. Based on the dd program found in the GNU Coreutils package, dcfldd has the following additional features: hashing on-the-fly, status output, flexible disk wipes, image/wipe verify, multiple outputs, split output and piped output and logs. DCFLDD was tested only for its disk imaging capabilities and, except for the following anomaly the tool acquired the test media completely and accurately.

- When a drive with faulty sectors was imaged (test case DA-09) the tool failed to completely acquire all readable sectors near the location of the faulty sectors. In test case DA-09, a source drive with faulty sectors was cloned to a target drive. Readable sectors that were near faulty sectors on the source drive were not acquired. The tool wrote zeros to the target drive in place of these sectors.
- When a drive with faulty sectors was imaged (test case DA-09) the data cloned to the target drive became misaligned after faulty sectors were encountered on the source drive. For example, sector 6,160,448 on the target drive contained the contents of sector 6,160,392 from the source, sector 6,160,449 on the target contained the contents of source sector 6,160,393, and so on. The size of the offset or misalignment between the data on the source and target drives grew as more faulty sectors were encountered on the source.

Refer to sections 3 and 5 for more details.

2 Test Case Selection

Test cases used to test disk imaging tools are defined in *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0*. To test a tool, test cases are selected from the *Test Plan* document based on the features offered by the tool. Not all test cases or test assertions are appropriate for all tools. There is a core set of base cases (e.g., DA-06 and DA-07) that are executed for every tool tested. Tool features guide the selection of additional test cases. If a given tool implements some feature then the test cases linked to the implemented features are run. Table 1 lists the supported features of DCFLDD and the linked test cases selected for execution. Table 2 lists the features not available in DCFLDD 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
Insufficient space for image file	12
Create a clone from an image file	14 & 17

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
Create an image of a drive with hidden sectors	08
Create an image file in more than one format	10
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
Detect a corrupted (or changed) image file	24 & 25
Convert an image file from one format to another	26

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

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

The following digital source types were tested: partitions (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 DCFLDD 1.3.4-1 test runs, see <http://www.cfft.nist.gov/CFTT-Test-Run-Raw-Files-v3.html>.

Test Results Summary	
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-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-nt	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-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
07-f32x	Expected Results
07-hidden	Expected Results
07-nt	Expected Results
07-swap	Expected Results
07-thumb	Expected Results
09	Not Expected Results
12	Expected Results
14-ata28	Expected Results
14-ata48	Expected Results
14-cf	Expected Results

Test Results Summary	
Case	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-sata28	Expected Results
14-sata48	Expected Results
14-swap	Expected Results
14-thumb	Expected Results
14-usb	Expected Results
17	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 tool was executed in the Ubuntu Desktop 12.10 Linux (3.5.0-25-generic #39-Ubuntu SMP Mon Feb 25 19:02:34 UTC 2013 i686 i686 i686 GNU/Linux) environment.

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 DCFLDD 1.3.4-1 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 (AI) 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-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.

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	01-ide-96	78165360	0
da-01-ata48	4c	390721968	0
da-01-fw	63-FU2	117304992	0
da-01-sata28	4b-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-fw	43531488	0	0	43531488	0
da-01-ata28	117647712	0	0	117647712	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-exFAT	49-sata	10485760	0
da-02-ext2	43	10490382	0
da-02-ext3	49-sata	5863725	0
da-02-ext4	49-sata	7807590	0
da-02-f16	43	2104452	0
da-02-f32	43	8401932	0
da-02-f32x	43	20980827	0
da-02-hidden	43	4192902	0

Differences Between SRC & DST da-02			
Case-DS	SRC	Compared	Differ
da-02-nt	43	27712062	0
da-02-swap	43	4208967	0
da-02-thumb	d5-thumb	505856	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	58633344	0

Message to User da-04		
Case	SRC	Message
da-04	43	[75% of 38146Mb] 58633216 blocks (28629Mb) written. 00:16:53 remaining.dcfldd.: No space left on device

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...	N/A	N/A	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-sata28	4B-SATA	746B4...	746B4...	N/A	N/A	N/A	N/A
da-06-sata48	16-SATA	7BB1D...	7BB1D...	F8298...	F8298...	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-exfat	49-SATA	E8578...	E8578...	N/A	N/A	N/A	N/A
da-07-ext2	43	C7A84...	C7A84...	283BC...	283BC...	N/A	N/A
da-07-ext3	49-SATA	A2517...	A2517...	N/A	N/A	N/A	N/A
da-07-ext4	49-SATA	567F2...	567F2...	F28A7...	F28A7...	N/A	N/A
da-07-f16	43	N/A	N/A	N/A	N/A	EFEF3...	EFEF3...
da-07-f32	43	N/A	N/A	72462...	72462...	N/A	N/A
da-07-f32x	43	5980C...	5980C...	N/A	N/A	N/A	N/A
da-07-hidden	43	N/A	N/A	9D0C9...	9D0C9...	N/A	N/A
da-07-nt	43	5D42F...	5D42F...	73EB2...	73EB2...	N/A	N/A
da-07-swap	43	4B602...	4B602...	F5B06...	F5B06...	N/A	N/A
da-07-thumb	D5-THUMB	N/A	N/A	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	113942872

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	(120103200)	24	520	36197744	0

5.7 DA-09 Anomalies

Anomalies observed.

Anomalies Observed in da-09	
Case	Anomaly
da-09	Some sectors differ: [113942872], 113941720 sectors displaced in 14 shifts

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	43	[78% of 38146Mb] 61681408 blocks (30117Mb) written. 00:03:34 remaining.dcfldd:: No space left on device

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-ata28	01-ide-96	78165360	0
da-14-ata48	4c	390721968	0
da-14-cf	c1-cf	503808	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-nt	43	27712062	0
da-14-sata28	4b-sata	156301488	0
da-14-sata48	16-sata	312581808	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-ata48	97675200	0	0	97675200	0
da-14-fw	2798208	0	0	2798208	0
da-14-ata28	41937840	0	0	41937840	0
da-14-thumb	3495904	0	0	3495904	0

5.10DA-17

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

Differences Between SRC & DST da-17			
Case	SRC	Compared	Differ
da-17	01-ide-96	39102336	0

Message to User da-17		
Case	SRC	Message
da-17	01-ide-96	[50% of 38166Mb] 9775360 blocks (19092Mb) written. 00:44:54 remaining.dcfldd:: No space left on device

6 Summary of Administrative Data

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

Summary of Administrative Data					
Case	Host	Who	Source	Destination	Date
01-ata28	DeathStar	csr	01-IDE-96	23-IDE	Fri Mar 8 18:49:54 2013
01-ata48	CheFong	csr	4C	27-IDE	Sat Mar 9 17:51:24 2013
01-fw	DeathStar	csr	63-FU2	84-FU2	Thu Mar 14 15:35:11 2013
01-sata28	CheFong	csr	4B-SATA	06-SATA	Sun Mar 10 14:59:44 2013
01-sata48	Chefong	csr	16-SATA	43-SATA	Tue Mar 12 12:47:29 2013
01-usb	DeathStar	csr	63-FU2	61-FU2	Tue Mar 12 21:19:25 2013
02-cf	DeathStar	csr	C1-CF	C2-CF	Wed Mar 20 15:48:25 2013
02-exFAT	Chefong	csr	49-SATA	8B	Mon Mar 25 17:28:51 2013
02-ext2	Chefong	csr	43	7B	Tue Mar 26 12:24:04 2013
02-ext3	Chefong	csr	49-SATA	8B	Mon Mar 25 17:28:51 2013
02-ext4	Chefong	csr	49-SATA	8B	Mon Mar 25 17:28:51 2013
02-f16	Chefong	csr	43	7B	Wed Mar 27 14:48:34 2013
02-f32	Chefong	csr	43	7B	Wed Mar 27 14:20:27 2013
02-f32x	Chefong	csr	43	7B	Wed Mar 27 14:22:50 2013
02-hidden	Chefong	csr	43	7B	Wed Mar 27 11:00:22 2013
02-nt	Chefong	csr	43	7B	Tue Mar 26 18:05:44 2013
02-swap	Chefong	csr	43	7B	Wed Mar 27 11:01:21 2013
02-thumb	Deathstar	csr	D5-THUMB	D6-THUMB	Wed Mar 20 10:29:22 2013
04	Chefong	csr	43	90	Wed Jun 5 08:02:47 2013
06-ata28	Chefong	csr	01-IDE-96	NONE	Fri Mar 15 09:34:35 2013
06-ata48	Chefong	csr	4C	NONE	Sat Mar 16 09:06:35 2013
06-fw	Chefong	csr	63-FU2	NONE	Sat Mar 16 14:19:35 2013
06-sata28	Chefong	csr	4B-SATA	NONE	Sat Mar 16 11:57:35 2013
06-sata48	Chefong	csr	16-SATA	NONE	Sat Mar 16 12:50:35 2013
06-usb	Chefong	csr	63-FU2	NONE	Fri Mar 29 08:19:46 2013
07-cf	Chefong	csr	C1-CF	NONE	Mon Mar 18 17:09:35 2013
07-exfat	Chefong	csr	49-SATA	NONE	Mon Mar 18 16:09:35 2013
07-ext2	Chefong	csr	43	NONE	Mon Mar 18 16:09:35 2013
07-ext3	Chefong	csr	49-SATA	NONE	Mon Mar 18 16:09:35 2013
07-ext4	Chefong	csr	49-SATA	NONE	Mon Mar 18 16:09:35 2013
07-f16	Chefong	csr	43	NONE	Mon Mar 18 16:09:35 2013
07-f32	Chefong	csr	43	NONE	Mon Mar 18 16:09:35 2013
07-f32x	Chefong	csr	43	NONE	Mon Mar 18 16:09:35 2013
07-hidden	Chefong	csr	43	NONE	Tue Mar 26 15:45:10 2013
07-nt	Chefong	csr	43	NONE	Mon Mar 18 16:09:35 2013
07-swap	Chefong	csr	43	NONE	Mon Mar 18 16:09:35 2013
07-thumb	Chefong	csr	D5-THUMB	NONE	Mon Mar 18 17:09:35 2013
09	CheFong	csr	ED-BAD-CPR4	05-SATA	Thu Mar 7 09:37:28 2013
12	Chefong	csr	43	NONE	Tue May 21 09:36:59 2013
14-ata28	CheFong	csr	01-IDE-96	6D	Tue Mar 19 17:03:10 2013
14-ata48	DeathStar	csr	4C	2C-SATA	Tue Mar 19 13:47:34 2013

Summary of Administrative Data					
Case	Host	Who	Source	Destination	Date
14-cf	DeathStar	csr	C1-CF	C2-CF	Tue Mar 19 09:02:07 2013
14-exFAT	CheFong	csr	49-SATA	8B	Mon Mar 25 12:31:10 2013
14-ext2	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-ext3	CheFong	csr	49-SATA	8B	Mon Mar 25 15:31:10 2013
14-ext4	CheFong	csr	49-SATA	8B	Mon Mar 25 15:41:10 2013
14-f16	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-f32	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-f32x	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-fw	Chefong	csr	63-FU2	6D	Wed Mar 20 16:03:41 2013
14-hidden	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-nt	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-sata28	DeathStar	csr	4B-SATA	29-SATA	Tue Mar 19 17:06:36 2013
14-sata48	Chefong	csr	16-SATA	22-LAP	Wed Mar 20 16:00:44 2013
14-swap	Chefong	csr	43	29-SATA	Thu Mar 28 13:29:50 2013
14-thumb	DeathStar	csr	D5-THUMB	D6-THUMB	Tue Mar 19 09:08:29 2013
14-usb	Chefong	csr	63-FU2	61-FU2	Fri Mar 29 08:22:24 2013
17	Chefong	csr	01-IDE-96	8B	Sun Mar 24 12:15:35 2013