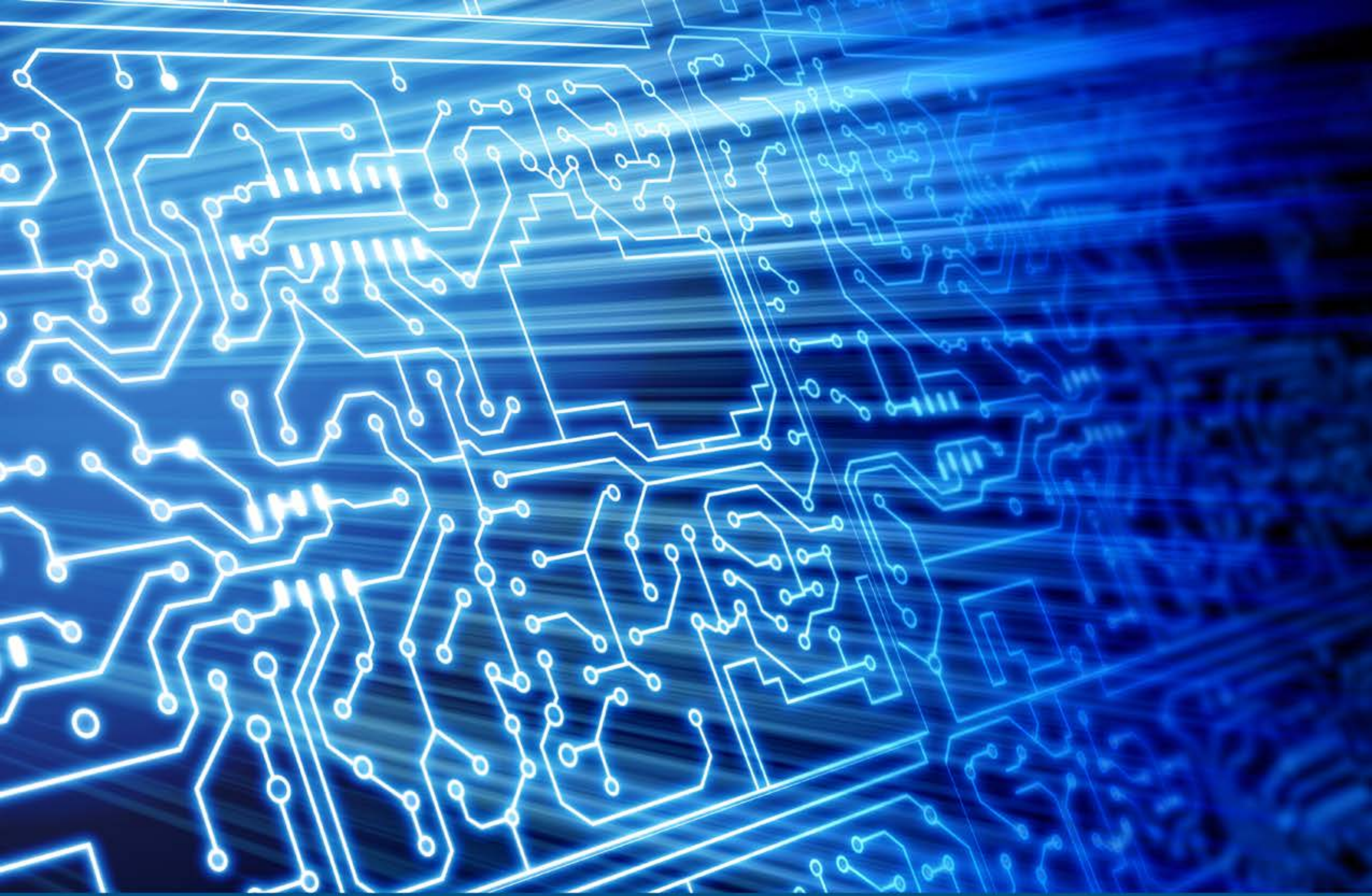

MacQuisition 2013R2

Test Results for Digital Data Acquisition Tool

July 23, 2014

Homeland Security

Science and Technology

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

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

July 2014

Test Results for Digital Data Acquisition Tool:
MacQuisition 2013R2

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), the National Institute of Justice, and the National Institute of Standards and Technology Law Enforcement Standards Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Web site (http://www.cftt.nist.gov/).

This document reports the results from testing MacQuisition 2013R2 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 MacQuisition 2013R2 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test Results for Digital Data Acquisition Tool

Tool Tested:	MacQuisition
Software Version:	2013R2
Runtime Environment	MacQuisition USB
Supplier:	BlackBag Technologies
Address:	300 Piercy Road San Jose, CA 95138
Tel:	(408) 844-8890
WWW:	https://www.blackbagtech.com

1 Results Summary

MacQuisition 2013R2 is a USB-based live data acquisition, data collection, and forensic imaging tool. The tool boots and collects data from various models of Macintosh computers. MacQuisition 2013R2 was only tested for its forensic imaging ability. The tool acquired the test media completely and accurately. When acquiring a hard drive with known faulty sectors, the tool wrote forensically benign content to the image in place of the faulty sectors.

For more detailed results 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 MacQuisition 2013R2 and the linked test cases selected for execution. Table 2 lists the features not available in MacQuisition 2013R2 and the test cases not executed.

Table 1. Selected Test Cases

Supported Optional Feature	Cases selected for execution
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
Detect a corrupted (or changed) image file	24 & 25

Table 2. Omitted Test Cases

Unsupported Optional Feature	Cases omitted (not executed)
Create a clone during acquisition	01
Create an unaligned clone from a digital source	02
Create cylinder aligned clones	03, 15, 21 & 23
Create a truncated clone from a physical device	04
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 an image file	14 & 17
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
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, the type of digital object acquired and image file format.

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

The following digital source types were tested: partitions (FAT16, FAT32, FAT32X, EXFAT, NTFS, EXT2, EXT3, EXT4, SWAP, hidden, OSX, OSXC, OSXCJ, OSXJ and OSXU), secure digital (SD), 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 case DA-07.

In addition to raw (.dd), the following image file types are supported by the tool: Expert Witness .E01 (uncompressed, empty block compression, fast compression and best compression) and Apple Disk Image (.dmg). 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 MacQuisition 2013R2 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

Test case Results	
Case	**Results**
06-fw	Expected Results
06-sata28	Expected Results

Test case Results	
Case	**Results**
06-sata48	Expected Results
06-usb	Expected Results
07-sd	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-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-e01bc	Expected Results
10-e01ebc	Expected Results
10-e01fc	Expected Results
12	Expected Results
24	Expected Results
25	Expected Results

4 Testing Environment

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

4.1 *Execution Environment*

Tests were run from the MacQuisition USB key.

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 MacQuisition 2013R2 test runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files-v3.html.

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-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-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-fw	63-FU2	EE217…	EE217…	F7069…	F7069…	N/A	N/A
da-06-sata28	07-SATA	2EAF7…	2EAF7…	655E9…	655E9…	N/A	N/A
da-06-sata48	0D-SATA	1FA7C…	1FA7C…	BAAD8…	BAAD8…	N/A	N/A
da-06-usb	63-FU2	EE217…	EE217…	F7069…	F7069…	N/A	N/A

5.2 DA-07

DA-07 Acquire a digital source of type DS to an image file.

Hash Matches da-07							
Case-DS	**SRC**	**Ref MD5**	**Tool MD5**	**Ref SHA1**	**Tool SHA1**	**Ref SHA256**	**Tool SHA256**
da-07-cf	C1-CF	776DF…	776DF…	5B823…	5B823…	N/A	N/A
da-07-exFAT	49-SATA	E8578…	E8578…	3D44F…	3D44F…	N/A	N/A
da-07-ext2	01-IDE	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	8B24F…	8B24F…	074BA…	074BA…	N/A	N/A
da-07-f32	01-IDE	BFF7D…	BFF7D…	B861D…	B861D…	CAE3A…	CAE3A…
da-07-f32x	01-IDE	B5BFD…	B5BFD…	30BA6…	30BA6…	N/A	N/A
da-07-hidden	01-IDE	5A165…	5A165…	D10BD…	D10BD…	N/A	N/A
da-07-nt	01-IDE	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-sd	A1-SD	E9250…	E9250…	FBA5D…	FBA5D…	N/A	N/A
da-07-swap	01-IDE	275AC…	275AC…	DFC37…	DFC37…	N/A	N/A
da-07-thumb	D5-THUMB	C8435…	C8435…	D6852…	D6852…	N/A	N/A

5.3 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	36146800	0	0	36146800	0

5.4 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	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A
da-10-e01	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A
da-10-e01bc	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A
da-10-e01ebc	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A
da-10-e01fc	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A

5.5 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	0b-sata	Warning: Destination device 'disk1s2' does not have enough space available for this image.

5.6 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	63-FU2	EE217...	EE217...	F7069...	F7069...	N/A	N/A

5.7 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	C1-CF	776DF...	044E3...	5B823...	79F1C...	N/A	N/A

6 Summary of Administrative Data

Summary of Administrative Data					
Case	**Host**	**Who**	**Source**	**Destination**	**Date**
06-fw	palpatine	csr	63-FU2	NONE	Sun Feb 9 08:37:30 2014
06-sata28	palpatine	csr	07-SATA	NONE	Fri Feb 7 09:09:41 2014
06-sata48	palpatine	csr	0D-SATA	NONE	Fri Feb 7 10:14:28 2014
06-usb	palpatine	csr	63-FU2	NONE	Sun Feb 9 08:30:56 2014
07-cf	palpatine	csr	C1-CF	NONE	Sun Feb 16 10:18:19 2014
07-exFAT	palpatine	csr	49-SATA	NONE	Sun Feb 16 10:31:29 2014
07-ext2	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:07:30 2014
07-ext3	palpatine	csr	49-SATA	NONE	Sun Feb 16 10:31:29 2014
07-ext4	palpatine	csr	49-SATA	NONE	Sun Feb 16 10:31:29 2014
07-f16	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:04:49 2014
07-f32	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:07:30 2014
07-f32x	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:12:58 2014
07-hidden	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:12:58 2014
07-nt	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:22:44 2014
07-osx	palpatine	csr	4B-SATA	NONE	Sun Feb 16 13:36:03 2014
07-osxc	palpatine	csr	4B-SATA	NONE	Sun Feb 16 13:42:30 2014
07-osxcj	palpatine	csr	4B-SATA	NONE	Sun Feb 16 13:51:07 2014
07-osxj	palpatine	csr	4B-SATA	NONE	Sun Feb 16 13:40:17 2014
07-osxu	palpatine	csr	4B-SATA	NONE	Sun Feb 16 13:50:00 2014
07-sd	palpatine	csr	A1-SD	NONE	Sun Feb 16 09:59:13 2014
07-swap	palpatine	csr	01-IDE	NONE	Sun Feb 16 12:12:58 2014
07-thumb	palpatine	csr	D5-THUMB	NONE	Sun Feb 16 09:35:38 2014
09	palpatine	csr	ED-BAD-CPR4	2A-SATA	Thu Feb 6 14:43:48 2014
10-dmg	palpatine	csr	63-FU2	NONE	Mon Feb 10 05:04:49 2014
10-e01	palpatine	csr	63-FU2	NONE	Mon Feb 10 04:20:03 2014
10-e01bc	palpatine	csr	63-FU2	NONE	Mon Feb 10 12:12:17 2014
10-e01ebc	palpatine	csr	63-FU2	NONE	Mon Feb 10 10:53:01 2014
10-e01fc	palpatine	csr	63-FU2	NONE	Mon Feb 10 11:33:49 2014
12	palpatine	csr	0B-SATA	NONE	Sun Feb 16 14:06:28 2014
24	palpatine	csr	63-FU2	NONE	Sun Feb 9 11:15:56 2014
25	palpatine	csr	C1-CF	NONE	Wed Feb 19 14:26:31 2014