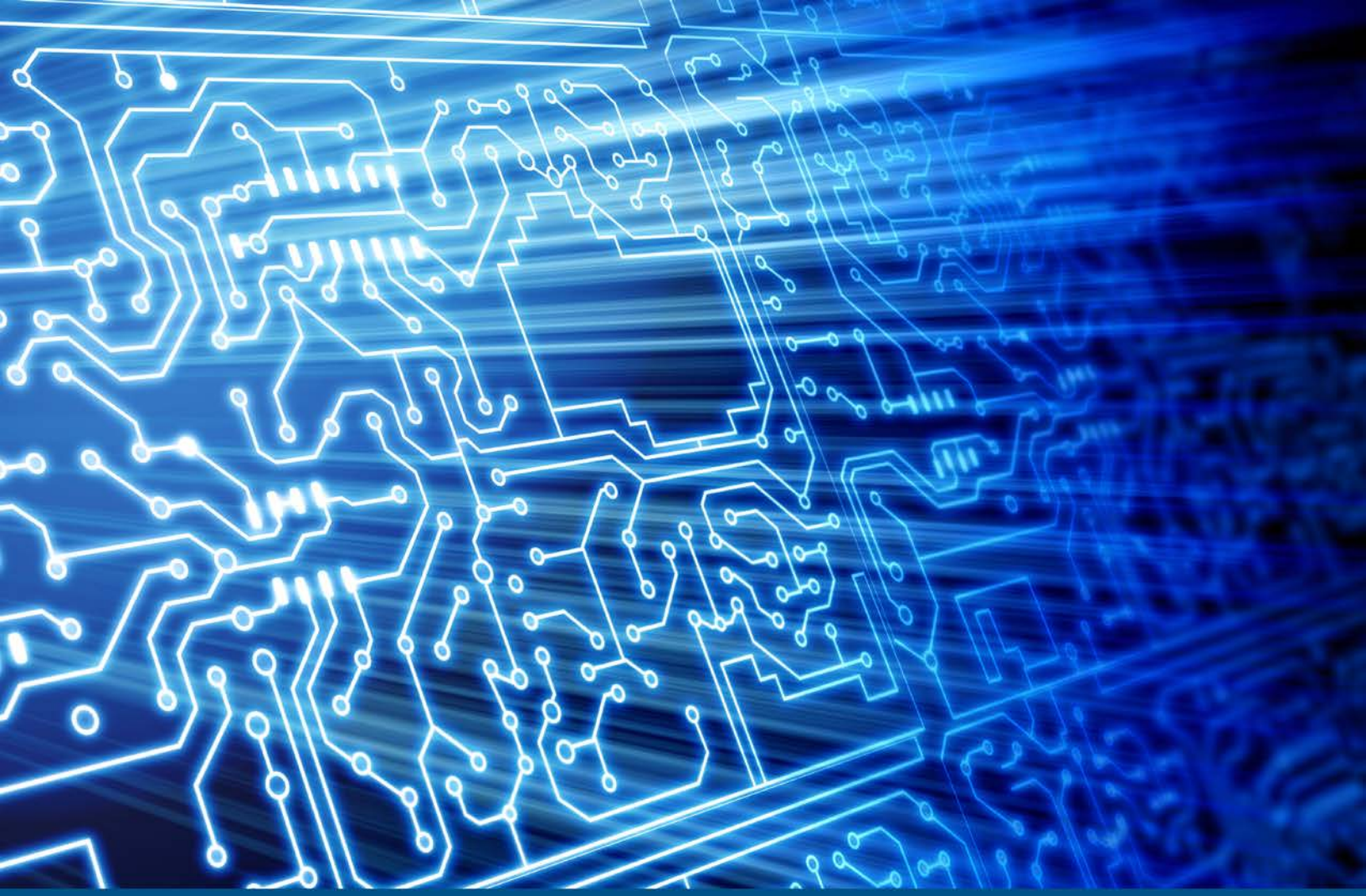

EnCase Forensic Version 7.12.01.18, Windows 7

Test Results for Disk Imaging Tool – Federated Testing Suite

August 13, 2018

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/science-and-technology/cyber-security-division.

August 2018

Test Results for Disk Imaging Tool:
EnCase Forensic Version 7.12.01.18, Windows 7

Federated Testing Suite for Disk Imaging

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 (NIST) Special Programs Office 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 (https://www.cftt.nist.gov/).

Federated Testing is an expansion of the CFTT program to provide forensic investigators and labs with test materials for tool testing and to support shared test reports. The goal of Federated Testing is to help forensic investigators to test the tools that they use in their labs and to enable sharing of tool test results. CFTT's Federated Testing Forensic Tool Testing Environment and included test suites can be downloaded from https://www.cftt.nist.gov/federated-testing.html and used to test forensic tools. The results can be optionally shared with CFTT, reviewed by CFTT staff, and then shared with the community.

This document reports the results from testing the disk imaging function of EnCase Forensic Version 7.12.01.18 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 1.1.

Test results from other tools can be found on DHS's computer forensics web page, https://www.dhs.gov/science-and-technology/nist-cftt-reports.

How to Read This Report

This report is organized into the following sections:

1. Tested Tool Description. The tool name, version, vendor information, support environment (e.g., operating system version, device firmware version, etc.) version are listed.
2. Testing Organization. Contact information and approvals.
3. Results Summary. This section identifies any significant anomalies observed in the test runs. This section provides a narrative of key findings identifying where the tool meets expectations and provides a summary of any ways the tool did not meet expectations. The section also provides any observations of interest about the tool or about testing the tool including any observed limitations or organization imposed restrictions on tool use.
4. Test Environment. Description of hardware and software used in tool testing in sufficient detail to satisfy the testing organization's policy and requirements.
5. Test Result Details by Case. Automatically generated test results that identify anomalies.
6. Appendix: Additional Details. Additional administrative details for each test case such as, who ran the test, when the test was run, computer used, etc.

Federated Testing Test Results for Disk Imaging Tool: EnCase Forensic Version 7.12.01.18

Tests were Configured for the Following Write Block Scenarios:

Large (> 138GB) SATA drive with Tableau T35u connected to PC by USB interface
Large (> 138GB) SATA drive with UltraBay 3d connected to PC by USB interface
USB drive with UltraBay 3d connected to PC by USB interface

Tool Description

Tool Name: EnCase Forensic
Tool Version: 7.12.01.18

Operating System: Windows 7

Vendor Contact:

Vendor name:	Guidance Software
Address:	1055 E. Colorado Blvd. Pasadena, CA 91106-2375
Phone:	866-229-9199
Web:	https://www.guidancesoftware.com/

Testing Organization

Organization conducting test: Missouri State Public Defender Digital Forensics Lab
Contact: Kate Davenport
Authored by: Kate Davenport

This test report was generated using CFTT's Federated Testing Forensic Tool Testing Environment, see Federated Testing Home Page.

Results Summary

The tool met expectations for different imaging scenarios successfully. One notable finding was observed. When a partition with an NTFS file system was acquired (test FT-DI-05-NTFS), the acquisition hashes created by EnCase did not match the reference hashes for the partition. However, when the image file was rehashed omitting the partition slack, the hash matched the reference hash for the acquired NTFS file system. EnCase acquired the file system and its contents completely, but not the partition slack.

Test Environment & Selected Cases

Hardware:

FRED (Digital Intelligence) S/N: F0133035941

Workstation B- Lenovo ThinkStation P510 Signature Edition

FT-LOGS- SanDisk Cruzer Glide 64 GB USB & Patriot 256 GB USB

A1 Source Drive- WD Black 500 GB S/N: WX41AB4CL9LF Model: WD5000BPKX-00HPJT0

A2 Source Drive- WD Black 500 GB S/N: WX41AB4CLHZ4 Model: WD5000BPKX-00HPJT0

A3 Source USB Drive- PNY 32 GB

A4 Source Drive- WD Caviar 250 GB S/N: WMART1348638 Model: WD2500AAJS-00VTA0

A5 Source Drive- WD Caviar 250 GB S/N: WMART1348638 Model: WD2500AAJS-00VTA0

D1 Destination Drive- WD Blue 250 GB S/N: WCC2F2233793 Model: WD2500AAKX-75U6AA0

D2 Destination Drive- Seagate Barracuda 80 GB S/N: 5LRC74XD Model: ST3808110AS

Operating System: Windows 7

Software: EnCase Forensic 7.12.01.18

Write Blockers Used in Testing

Blocker Model	Firmware Version
Tableau T35u	7.17
UltraBay 3d	Unknown

Federated Testing Version 1.1

Selected Test Cases

This table presents a brief description of each test case that was performed.

Test Case Status

Case	Description	Status
FT-DI-01-SATA48	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-01-SATA48	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-01-USB	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-05-FAT32	Acquire partition of a given type to an image file and compute selected hashes for the acquired data. Test the ability to read a given partition type accurately and correctly hash the data while creating an image file.	completed
FT-DI-05-NTFS	Acquire partition of a given type to an image file and compute selected hashes for the acquired data. Test the ability to read a given partition type accurately and correctly hash the data while creating an image file.	completed
FT-DI-05-NTFS-2	Acquire partition of a given type to an image file and compute selected hashes for the acquired data. Test the ability to read a given partition type accurately and correctly hash the data while creating an image file.	completed
FT-DI-10	Acquire a drive to an image file without enough space for the image file. Test the ability of the tool to notify the user that the image file is incomplete.	completed
FT-DI-13	Compute the hash value of the acquired data within an image file. Test the ability of the tool to recompute the hash of an existing image file.	completed
FT-DI-14	Compute the hash value of a drive (without creating an image file). Test the ability to read all data accurately and correctly hash the data.	completed

Test Result Details by Case

This section presents test results grouped by function.

FT-DI-01

Test Case Description

Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.

This test can be repeated to test acquisition of multiple drive types. This test tests the ability of the tool to acquire a specific type of drive (the drive type tested is included in the test case name) to an image file using a specific write blocker (applies only to tools that are used with hardware write blockers) and a certain interface connection between the test computer and the write blocker. The write blocker used and the interface connection between the test computer and the write blocker are listed for each test case in the table below. Two tests are required to test ATA or SATA drives, one to test drives smaller than 138GB (ATA28 & SATA28: 28-bit addressing) and one to test larger drives (ATA48 & SATA48: 48-bit addressing).

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases.

Test Results for FT-DI-01 cases

Case	Src	Blocker (interface)	Reference Hash vs Tool Hash	
			MD5	SHA1
FT-DI-01-SATA48	a1	Tableau T35u (USB)	match	match
FT-DI-01-SATA48	a2	UltraBay 3d (USB)	match	match
FT-DI-01-USB	a3	UltraBay 3d (USB)	match	match

Case Summary

Results are as expected.

FT-DI-05

Test Case Description

Acquire partition of a given type to an image file and compute selected hashes for the acquired data. Test the ability to read a given partition type accurately and correctly hash the data while creating an image file.

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases

Test Results for FT-DI-05 cases

Case	Src	Reference Hash vs Tool Hash	
		MD5	SHA1
FT-DI-05-FAT32	a4+1	match	match
FT-DI-05-NTFS	a4+2	**differ**	**differ**
FT-DI-05-NTFS-2	a5+2	match	n/a

Anomalies

The following table lists any observed anomalies and provides additional details.

Test Anomalies for FT-DI-05 cases

Case	Anomaly
FT-DI-05-NTFS	**Tool MD5 and SHA1 do not match reference hashes**
FT-DI-05-NTFS MD5 ref	15942BBA33AD9487AC5EA7CF335C97F2
FT-DI-05-NTFS MD5 ref-FS	364D5EC8B6B49C754332A6E0969C4825
FT-DI-05-NTFS MD5 tool	01568D5B8E5E2E52AD9CF1953C5C4740
FT-DI-05-NTFS SHA1 ref	382AB1CAB5E62AE2703DE7BA89A5FFE5686AD31C
FT-DI-05-NTFS SHA1 ref-FS	FE92972A356D4717672B3CFFEA7C135A22F198E4
FT-DI-05-NTFS SHA1 tool	289E1D16518F97599C68230FEF45666A4C07B89E

Case Summary

Results are as expected.

In test FT-DI-05-NTFS when EnCase was used to acquire an NTFS partition, the acquisition hashes created by EnCase did not match the reference hashes for the partition. However, when the image file was rehashed omitting the partition slack, test FT-DI-05-NTFS-2, the hash matched the reference hash for the acquired NTFS file system. These findings show that EnCase acquired the file system and its contents completely, but not the partition slack. This should be noted if using EnCase to acquire an NTFS partition.

FT-DI-10

Test Case Description

Acquire a drive to an image file without enough space for the image file. Test the ability of the tool to notify the user that the image file is incomplete.

Test Evaluation Criteria

The tool should issue a message indicating not enough space for the image file.

Test Case Results

The following table presents results for individual test cases.

Test Results for FT-DI-10 cases

Case	Message
FT-DI-10	The target drive must be at least 465.8 GB. Truncate the restore by 391.3 GB?

Case Summary

Results are as expected.

FT-DI-13

Test Case Description

Compute the hash value of the acquired data within an image file. Test the ability of the tool to recompute the hash of an existing image file.

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases.

Test Results for FT-DI-13 cases

Case	Src	Reference Hash vs Tool Hash	
		MD5	SHA1
FT-DI-13	a1	match	match

Case Summary

Results are as expected.

FT-DI-14

Test Case Description

Compute the hash value of a drive (without creating an image file). Test the ability to read all data accurately and correctly hash the data.

Test Evaluation Criteria

The hash values computed by the tool should match the reference hash values computed for the source drive.

Test Case Results

The following table presents results for individual test cases.

Test Results for FT-DI-14 cases

Case	Src	Reference Hash vs Tool Hash	
		MD5	SHA1
FT-DI-14	a1	match	match

Case Summary

Results are as expected.

Appendix: Additional Details

Test drives and Partitions

The following table presents the state of each source object, drive or partition, including reference hashes and known content.

Both drives and partitions are described in the table. Partitions are indicated in the *Drive* column by the notation **[drive] + [partition number]**. Where **[drive]** is the drive label and **[partition number]** is the partition number. For example, the first partition on drive A3 would be A3+1. The type column records either the drive type, e.g. SATA, USB, etc., or the partition type, e.g., NTFS, FAT32, etc., depending on whether a drive or a partition is being described.

Test Drives

Drive	Type	Content	Sectors	MD5	SHA1	SHA256	SHA512
a1	sata	known	976773168 (465GiB)*	A62A5 ...	EC829 ...	33100 ...	3EFD8 ...
a2	sata	known	976773168 (465GiB)*	2188C ...	6874F ...	E5EF7 ...	53B7F ...
a3	usb	known	61997056 (29GiB)	1EA0A ...	F95DD ...	45F43 ...	17105 ...
a4+1	fat32	known	62492787 (29GiB)	CDD35 ...	FCC99 ...	01B17 ...	55959 ...
a4+2	ntfs	known	62492850 (29GiB)	15942 ...	382AB ...	33976 ...	1998B ...
a4+2	NTFS-FS	known	62492848 (29GiB)	364D5 ..	FE929 ..	00D7B ..	5A0D7 ..
a5+2	ntfs	N/A	62492850 (29GiB)	5A584 ...	81262 ...	7CA6E ...	08817 ...
a5+2	NTFS-FS	N/A	62492848 (29GiB)	364D5 ..	FE929 ..	00D7B ..	5A0D7 ..

* Large 48-bit address drive

Test Case Admin Details

For each test run, the test computer, the tester, the source drive, the image file drive, the destination drive, and the date the test was run are listed.

Test Case Admin Details

Case	User	Host	Blocker (PC interface)	Src	Image	Dst	Date
ft-di-01-sata48	KED	Fred3	Tableau T35u (USB)	a1	d1	none	Tue Jan 31 10:09:24 2017
ft-di-01-sata48	KED	Fred3	UltraBay 3d (USB)	a2	no	none	Fri Feb 3 09:43:21 2017
ft-di-01-usb	KED	Fred3	UltraBay 3d (USB)	a3	no	none	Fri Feb 3 14:24:57 2017
ft-di-05-fat32	KED	Fred3	UltraBay 3d (USB)	a4	no	none	Thu Feb 23 10:33:56 2017
ft-di-05-ntfs	KED	Fred3	UltraBay 3d (USB)	a4	no	none	Thu Feb 23 10:34:52 2017
ft-di-05-ntfs-2	KED	B	Tableau T35u (USB)	a5	no	none	Thu Jul 27 06:33:04 2017
ft-di-10	KED	Fred3	N/A	a1	d2	none	Fri Feb 17 10:31:25 2017
ft-di-13	KED	Fred3	Tableau T35u (USB)	a1	no	none	Mon Feb 6 14:40:48 2017
ft-di-14	KED	Fred3	N/A	a1	none	none	Fri Feb 10 17:25:27 2017

Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions

cftt-di Version 1.20 created 07/05/16 at 14:56:34
cftt-di Version 1.19 created 06/02/16 at 11:27:15
diskcmp.c Linux Version 1.3 Created 03/20/13 at 14:23:34
diskwipe.c Linux Version 1.5 Created 03/20/13 at 14:23:34
zbios.c Linux Version 1.8 Created 07/14/13 at 20:49:31
zbios.h Linux Version 1.2 Created 03/20/13 at 14:23:33

Tool: @(#) ft-di-prt_test_report.py Version 1.19 created 06/02/16 at 11:27:53
OS: Linux Version 3.2.0-51-generic
Federated Testing Version 1.1, released 6/2/2016