August 2021

Test Results for Disk Imaging Tool:
DFT Version 1.0

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) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology (NIST) Special Programs Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense's Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, as well as the DHS 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 Website (https://www.cftt.nist.gov/).

This document reports the results from testing the disk imaging function of DFT Version 1.0 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 5.

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 http://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.

Test results from other tools can be found on DHS's computer forensics webpage, 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, and support environment version (e.g., operating system version) are listed.
2. Testing Organization. The name and contact information of the organization that performed the tests are listed.
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: DFT Version 1.0

Tests were Configured for the Following Write Block Scenarios:

Small (< 138GB) SATA drive with Tableau Forensic SATA/IDE Bridge T35U connected to PC by SATA interface

Large (> 138GB) SATA drive with Tableau Forensic SATA/IDE Bridge T35U connected to PC by SATA interface

SD drive with Samsung SD adapter for microSD connected to PC by USB interface

USB drive with Tableau Forensic USB Bridge T8-R2 connected to PC by USB interface

Tool Description

Tool Name: DFT
Tool Version: 1.0

Vendor Contact:
Vendor name: National Security Research Institute
Address: 1559, Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea, 34044
Phone: +82-42-870-2280, +82-42-870-2322
Email: hhu@nsr.re.kr, sylee@nsr.re.kr
Operating System: Microsoft Windows 10

Testing Organization

Organization conducting test: Digital Forensic & Cryptanalysis (DF&C) Lab., Kookmin University
Contact: Prof. Jongsung Kim
Report date: July 28, 2021
Authored by: Prof. Jongsung Kim

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 the different imaging scenarios tested.

Test Environment & Selected Cases

Hardware: Custom PC with USB 3, USB 2, SATA ports
PC1: AMD Ryzen 7 3700X CPU @ 3.6GHz
PC2: Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz
PC3: Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz
PC4: AMD Ryzen 7 3700X CPU @ 3.6GHz
PC5: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
PC6: Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz

Operating System:
PC1: Microsoft Windows 10 Pro 21H1 (19043.1083)
PC2: Microsoft Windows 10 Enterprise (10.0.19042 build 19042)
PC3: Microsoft Windows 10 Home (19042.1083)
PC4: Microsoft Windows 10 Pro version 1809 (17763.1577)
PC5: Microsoft Windows 10 Pro (10.0.18363 build 18363)
PC6: Microsoft Windows 10 Enterprise (10.0.19041 build 19041)

Write Blockers Used in Testing

Blocker Model	Firmware Version
Tableau Forensic SATA/IDE Bridge T35U	20.1
Samsung SD adapter for microSD	Unknown
Tableau Forensic USB Bridge T8-R2	7.02

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-SATA28	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-03-SD	Acquire removable media of a given type using a given media reader 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 removable media type accurately and correctly hash the data while creating an image file.	completed
FT-DI-05-ExFAT	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-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-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

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-SATA28	a5	Tableau Forensic SATA/IDE Bridge T35U (SATA)	match	match
FT-DI-01-SATA48	a1	Tableau Forensic SATA/IDE Bridge T35U (SATA)	match	match
FT-DI-01-USB	a21	Tableau Forensic USB Bridge T8-R2 (USB)	match	match

Case Summary

Results are as expected.

FT-DI-03

Test Case Description

Acquire removable media of a given type using a given media reader 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 removable media type accurately and correctly hash the data while creating an image file.

This test can be repeated to test acquisition of multiple removable media types. This test tests the ability of the tool to acquire a specific type of removable media (the removable media type tested is included in the test case name) to an image file using a specific media reader which may also be a write blocker and a certain interface connection between the test computer and the media reader. The media reader used and the interface connection between the test computer and the media reader are listed for each test case in the table below.

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-03 cases

Case	Src	Blocker (interface)	Reference Hash vs Tool Hash	
			MD5	SHA1
FT-DI-03-SD	a2	Samsung SD adapter for microSD (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-ExFAT	a16+1	match	match
FT-DI-05-FAT32	a26+1	match	match
FT-DI-05-NTFS	a3+1	match	match

Case Summary

Results are as expected.

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	Error: Volume size is too small

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	a5	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	1953525168 (931GiB)*	7C5E0...	88E0E...	4C4C5...	DB6D5 ...
a16+1	exfat	known	31537153 (15GiB)	268A6...	EEBC2...	A6DFB...	22732 ...
a2	sd	known	62333952 (29GiB)	61BDE...	636E3...	594F1...	7F111 ...
a21	USB	known	62656641 (29GiB)	5E495...	82B28...	0A330...	B16EA ...
a25	SATA	known	976773168 (465GiB)*	EBB6F...	FCAE8...	5E813...	17210 ...
a26+1	FAT32	known	16777216 (8GiB)	1FCE7...	197E0...	44A5E...	49133 ...
a26	USB	known	31299696 (14GiB)	F752C...	3A77A...	14B21...	9D1B6 ...
a3+1	NTFS	known	33554432 (16GiB)	1BCA2...	BEDCA...	B8655...	9D098 ...
a3+1	NTFS-FS	known	33554425 (15GiB)	8BCA7...	3D82F...	89C4A...	4C964 ..
a5	SATA	known	250069680 (119GiB)	90132...	81F92...	2B57A...	9A480 ...

* 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-sata28	DF&C	Test_Pc	Tableau Forensic SATA/IDE Bridge T35U (SATA)	a5	00	none	Thu Jul 15 15:42:58 2021
ft-di-01-sata48	DF&C	Test_Pc	Tableau Forensic SATA/IDE Bridge T35U (SATA)	a1	00	none	Thu Jul 15 15:43:27 2021
ft-di-01-usb	DF&C	Test_Pc	Tableau Forensic USB Bridge T8-R2 (USB)	a21	00	none	Thu Jul 15 15:44:24 2021
ft-di-03-sd	DF&C	Test_Pc	Samsung SD adapter for microSD (USB)	a2	00	none	Thu Jul 15 15:45:12 2021
ft-di-05-exfat	DF&C	Test_Pc	Tableau Forensic USB Bridge T8-R2 (USB)	a16	00	none	Thu Jul 15 15:45:34 2021
ft-di-05-fat32	DF&C	Test_Pc	Tableau Forensic USB Bridge T8-R2 (USB)	a26	00	none	Thu Jul 15 15:46:47 2021
ft-di-05-ntfs	DF&C	Test_Pc	Tableau Forensic USB Bridge T8-R2 (USB)	a3	00	none	Thu Jul 15 15:47:03 2021

ft-di-10	DF&C	Test_Pc	N/A	a25	00	none	Thu Jul 15 15:47:17 2021
ft-di-13	DF&C	Test_Pc	Tableau Forensic SATA/IDE Bridge T35U (SATA)	a5	00	none	Thu Jul 15 16:59:50 2021

Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions

cftt-di Version 1.25 created 05/23/18 at 15:58:45
diskwipe.c Linux Version 1.5 Created 03/20/13 at 14:23:34

Tool: @(#) ft-di-prt_test_report.py Version 1.24 created 05/23/18 at 16:08:06
OS: Linux Version 4.13.0-37-generic
Federated Testing Version 5, released 3/12/2020