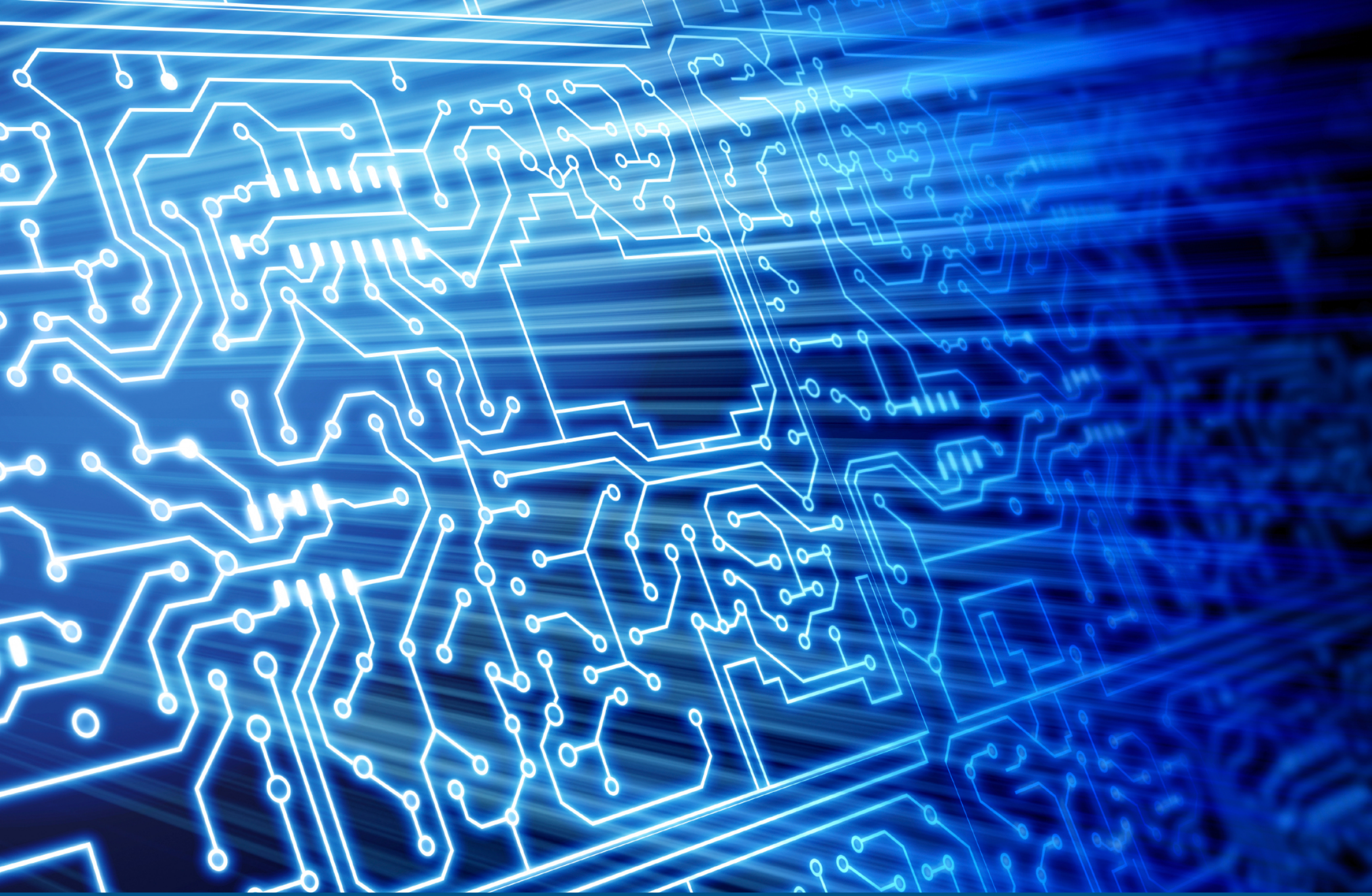

DFAS Pro Version 1.0.1.6 Build 052

Test Results for Disk Imaging Tool – Federated Testing Suite

April 21, 2019

Homeland Security

Science and Technology

This report was prepared for the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.

For additional information about ongoing DHS S&T cybersecurity projects, please visit the DHS Science and Technology Cyber Security Division Web site at http://www.dhs.gov/science-and-technology/cyber-security-division.

April 2019

Test Results for Disk Imaging Tool:
DFAS Pro Version 1.0.1.6 Build 052

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/).

This document reports the results from testing the disk imaging function of DFAS Pro Version 1.0.1.6 Build 052 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 3.1.

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 NIST's Federated Testing Home page, 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.

Test results from this and 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, 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: DFAS Pro Version 1.0.1.6 Build 052

Tests were Configured for the Following Write Block Scenarios:

Large (> 138GB) SATA drive with Tableau T35es connected to PC by USB interface
USB drive with Tableau T8R2 connected to PC by USB interface
SD card with Tableau T8R2 connected to PC by USB interface

Tool Description

Tool Name: DFAS Pro
Tool Version: 1.0.1.6 Build 052
Operating System: Windows 7 Ultimate 64-bit

Vendor Contact:

Vendor name:	Douzone Bizon
Address:	130, Beodeul 1-gil, Namsan-myeon, Chuncheon-si, Gangwon-do, South Korea
Phone:	+82-02-6233-2075
Email:	Duozone Bizon email address (forensic@douzone.com)
WWW:	D-Forensic Center (DFC) home page (http://www.dforensic.com)

Testing Organization

Organization conducting test: The Korea Convergence Security Association
Contact: President of the Association, Professor Hangbae Chang
(+82-2-820-5538, Professor Hangbae Chang's email address (hbchang@cau.ac.kr)
Report date: 26-OCT-2018

This test report was generated using CFTT's Federated Testing Forensic Tool Testing Environment, see NIST's Federated Testing Home page (https://www.cftt.nist.gov/federated-testing.html).

Results Summary

Except for the following anomalies, the tool functioned as expected and acquired each drive completely and accurately. For three of the tests, tests that involved the acquisition of physical devices (vs logical), the tool recorded the size of the acquired devices incorrectly in the tool-generated log files. For example, the tool recorded the size of the drive acquired in test FT-DI-01-USB as 15,342,075 sectors instead of 15,356,160 sectors.

Test Environment & Selected Cases

Hardware:
- Test/Analysis PC: MSI GS60 2QD
- FT-LOGS USB: SanDisk Blade 4GB (S/N: 20044320830534003 58F)
- A1 Source Drive: WD Caviar Blue 320GB (S/N: WD-WCAV2F671357)
- A2 Source Drive: Seagate Barracuda 1TB (S/N: Z1D5END1)
- A3 Source Drive: Sony TINY Series USB Flash Drive 8GB (S/N: 9B3001305040022672)
- A4 Source Media: SanDisk Ultra Micro SD Card 16GB (S/N: 7371ZR5AL6QE)
- Destination Drive: WDC WD2003FZEX 2TB (S/N: WD-WCC5C6HUR1NR)

Operating System: Windows 7 Ultimate 64-bit

Write Blockers Used in Testing

Blocker Model	Firmware Version
Tableau T35es	Aug 6 2010
Tableau T8R2	Mar 9 2011

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-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-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

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 T35es (USB)	match	match
FT-DI-01-USB	a3	Tableau T8R2 (USB)	match	match

Case Summary

The tool acquired the test drives completely and accurately but recorded the sizes of the acquired drives incorrectly. In test case FT-DI-01-SATA48 the tool incorrectly recorded the size of the acquired drive as 625,137,345 sectors instead of 625,142,448 sectors in the tool-generated log file. In test case FT-DI-01-USB the tool recorded the size of the acquired drive as 15,342,075 sectors instead of 15,356,160 sectors.

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	a4	Tableau T8R2 (USB)	match	match

Case Summary

The tool acquired the test media completely and accurately but recorded the size of the acquired media incorrectly. In test case FT-DI-03-SD the tool incorrectly recorded the size of the acquired media as 31,101,840 sectors instead of 31,116,288 sectors in the tool-generated log file.

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-NTFS	a2+1	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	625142448 (298GiB)*	96634 ...	88143 ...	21145 ...	242F7 ...
a2+1	ntfs	known	1953519616 (931GiB)*	35DD3 ...	76D42 ...	2BCB8 ...	CD281 ...
a2+1	NTFS-FS	known	1953519609 (931GiB)	180E7 ..	B9242 ..	7C5D3 ..	87FF6 ..
a3	usb	known	15356160 (7GiB)	59978 ...	AF578 ...	B519D ...	B7CB1 ...
a4	sd	known	31116288 (14GiB)	38CD2 ...	74AE9 ...	36A2D ...	EB2C1 ...

* 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	DFC	Testpc	Tableau T35es (USB)	a1	repository	none	Thu Sep 27 07:35:11 2018
ft-di-01-usb	DFC	Testpc	Tableau T8R2 (USB)	a3	repository	none	Thu Sep 27 07:53:29 2018
ft-di-03-sd	DFC	Testpc	Tableau T8R2 (USB)	a4	repository	none	Thu Sep 27 07:54:19 2018
ft-di-05-ntfs	DFC	Testpc	Tableau T35es (USB)	a2	repository	none	Thu Sep 27 07:39:36 2018

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 3.1, released 5/25/2018