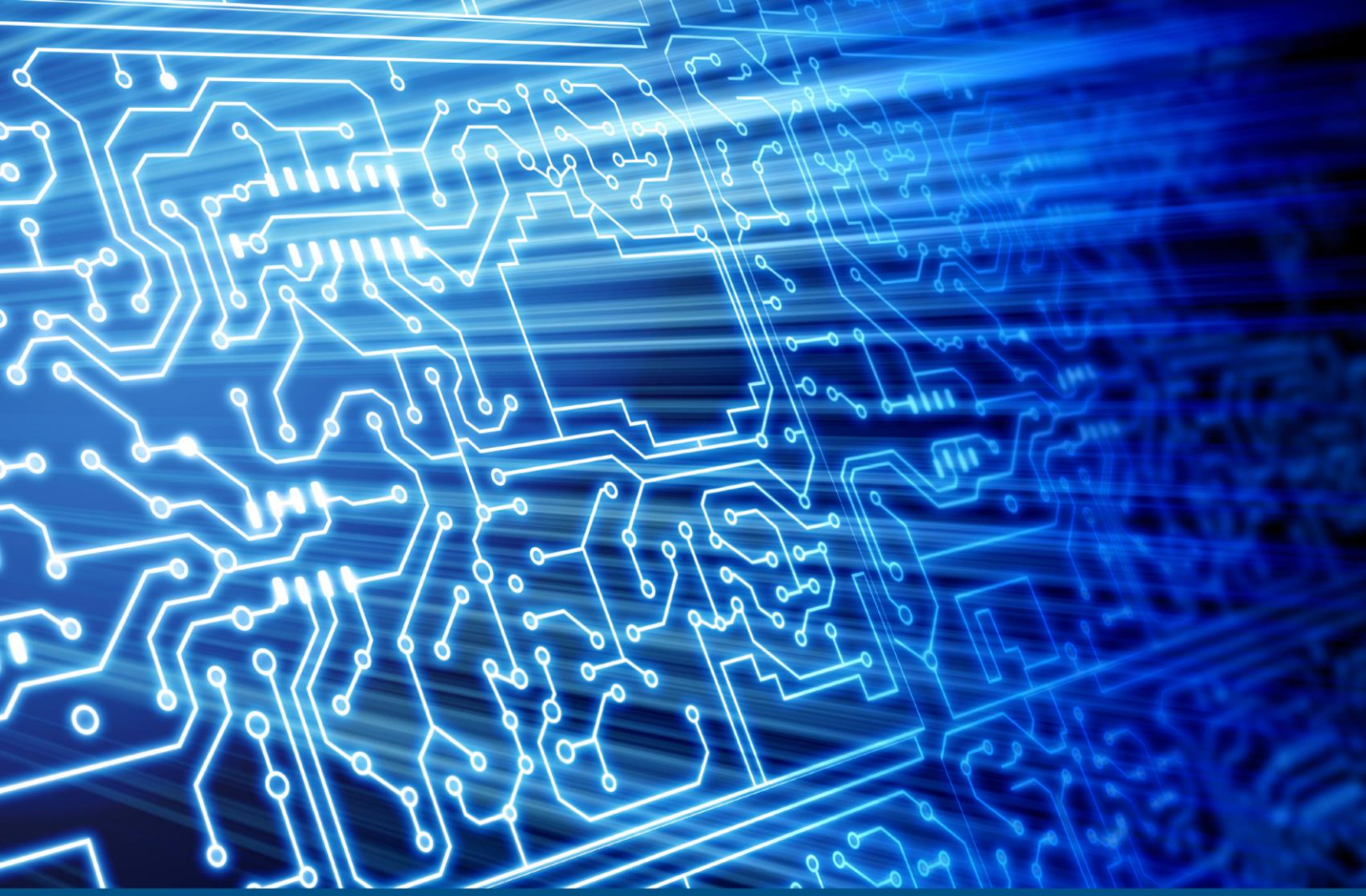

Computer Forensic Tool v3.4.1

Test Results for Disk Imaging Tool – Federated Testing Suite

February 12, 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.

February 2018

Test Results for Disk Imaging Tool:
Computer Forensic Tool (CFT) Version 3.4.1

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 CFT Version 3.4.1 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 2.1.

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: CFT Version 3.4.1

Tests were Configured for the Following Write Block Scenarios:

Small (< 138GB) SATA drive with Tableau T35es Forensic Bridge connected to PC by USB interface
Large (> 138GB) SATA drive with Tableau T35es Forensic Bridge connected to PC by USB interface
USB drive with Tableau T8 USB Forensic Bridge connected to PC by USB interface
SD card with Tableau T8 USB Forensic Bridge connected to PC by USB interface

Tool Description

Tool Name: Computer Forensic Tool (CFT)
Tool Version: 3.4.1
Operating System: Windows 10 Enterprise 64bit

Vendor Contact:

Vendor name:	National Security Research Institute
Address:	1559, Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea, 34044
Phone:	+82-42-870-2275, +82-42-870-2280
Email:	kibom@nsr.re.kr, hhu@nsr.re.kr

Testing Organization

Organization conducting test: ***Digital Forensic Research Center, Korea University***
Contact: ***Prof. Sangjin Lee***
Report date: 15-SEP-2017

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

Results Summary

The tested tool functioned as expected with no anomalies.

Test Environment & Selected Cases

Hardware: ***Custom PC with USB 3, USB 2, SATA ports***

Operating System: ***Windows 10 Enterprise 64bit***

Write Blockers Used in Testing

Blocker Model	Firmware Version
Tableau T8 USB Forensic Bridge	Apr 2 2013 16
Tableau T35es Forensic Bridge	Jan 23 2013 12:20:26

Federated Testing Version 2.1

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-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-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	completed

	given partition type accurately and correctly hash the data while creating an image file.	
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
FT-DI-01-SATA28	a1	Tableau T35es Forensic Bridge (USB)	match
FT-DI-01-SATA48	a2	Tableau T35es Forensic Bridge (USB)	match
FT-DI-01-USB	a3	Tableau T8 USB Forensic Bridge (USB)	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 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 media.

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
FT-DI-03-SD	a4	Tableau T8 USB Forensic Bridge (USB)	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
FT-DI-05-NTFS	a5+1	match

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
FT-DI-13	a3	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	156301488 (74GiB)	921C6 ...	1072D ...	94853 ...	E7C14 ...
a2	sata	known	976773168 (465GiB)*	2188C ...	6874F ...	E5EF7 ...	53B7F ...
a3	usb	known	3279872 (1GiB)	413A5 ...	8E0B9 ...	EA07F ...	BCA05 ...
a4	sd	known	31116288 (14GiB)	38CD2 ...	74AE9 ...	36A2D ...	EB2C1 ...
a5+1	ntfs	known	390042 (190MiB)	2B176 ...	48C6C ...	E3B3C ...	5707E ...
a5+1	NTFS-FS	known	390040 (190MiB)	A0013 ..	EF8AB ..	93AEC ..	5E166 ..

* 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	DFRC	Tpc	Tableau T35es Forensic Bridge (USB)	a1	91	none	Wed Sep 13 17:51:08 2017
ft-di-01-sata48	DFRC	Tpc	Tableau T35es Forensic Bridge (USB)	a2	91	none	Sat Sep 9 12:05:03 2017
ft-di-01-usb	DFRC	Tpc	Tableau T8 USB Forensic Bridge (USB)	a3	91	none	Wed Sep 13 17:55:03 2017
ft-di-03-sd	DFRC	Tpc	Tableau T8 USB Forensic Bridge (USB)	a4	91	none	Thu Sep 7 18:31:53 2017
ft-di-05-ntfs	DFRC	Tpc	Tableau T8 USB Forensic Bridge (USB)	a5	91	none	Sat Sep 9 14:15:15 2017
ft-di-13	DFRC	Tpc	Tableau T8 USB Forensic Bridge (USB)	a3	91	none	Wed Sep 13 17:56:26 2017

Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions

cftt-di Version 1.21 created 07/25/17 at 13:44:47
diskwipe.c Linux Version 1.5 Created 03/20/13 at 14:23:34

Tool: @(#) ft-di-prt_test_report.py Version 1.20 created 07/05/16 at 14:57:20
OS: Linux Version 3.2.0-51-generic
Federated Testing Version 2.1, released 7/27/2017