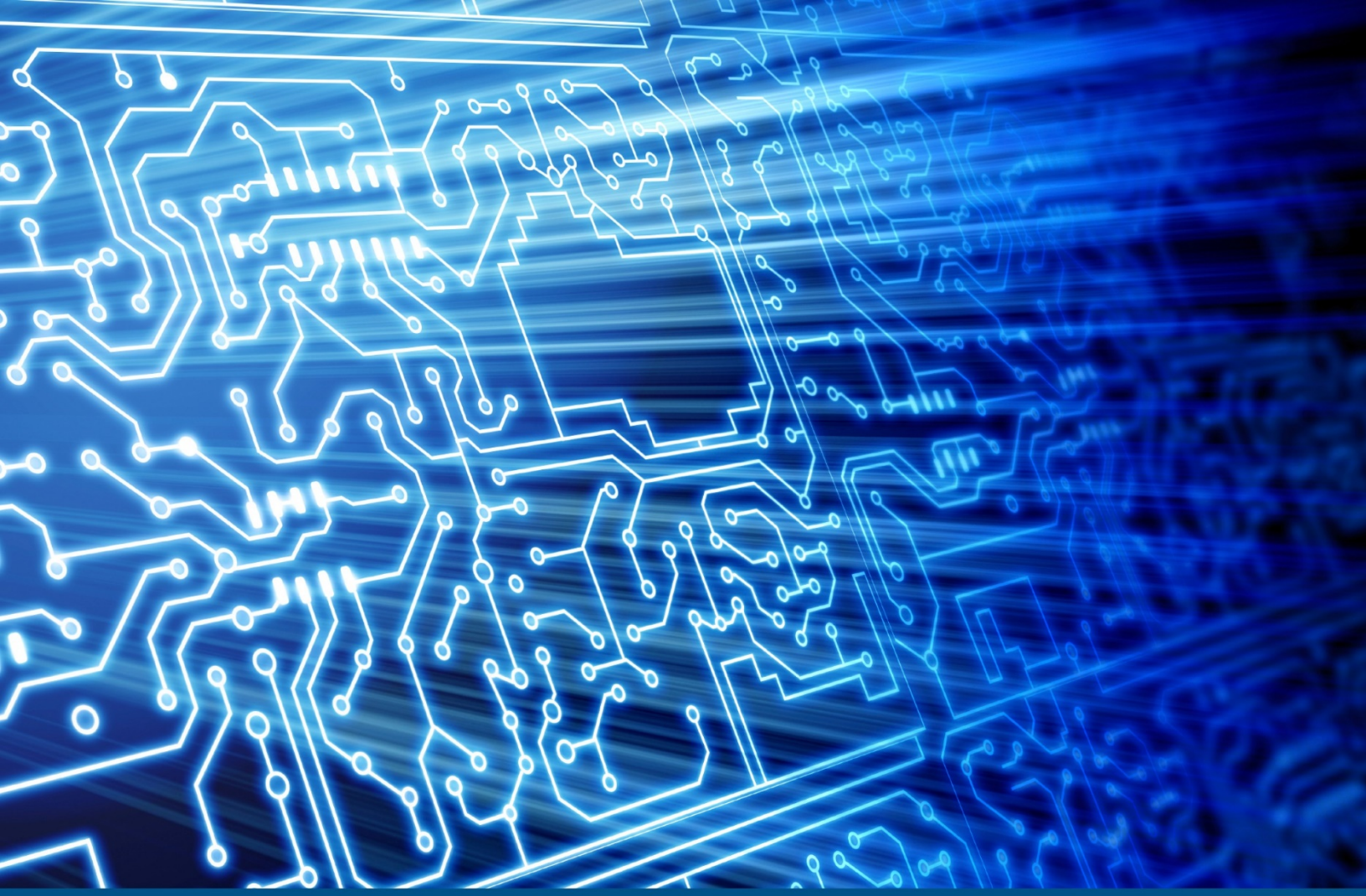

Test Results for Disk Imaging Tool:
FTK Imager Version 4.3.0.18

Federated Testing Suite for Disk Imaging

June 2020

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 https://www.dhs.gov/science-and-technology/cybersecurity

June 2020

Test Results for Disk Imaging Tool:
FTK Imager Version 4.3.0.18

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 Science and Technology Directorate (DHS S&T), 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 FTK Imager Version 4.3.0.18 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 4.

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.

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: FTK Imager Version 4.3.0.18

Tool Description

Tool Name: FTK Imager
Tool Version: 4.3.0.18
Release Date: 2020-02-04
File Name: AccessData_FTK_Imager-_4.3.0.exe
MD5: 04638f87a1fcd7da657b008f142b8382
Download Link: https://accessdata.com/product-download/ftk-imager-version-4-3-0
Operating System: Microsoft Windows 7 Ultimate, version: 6.1.7601 SP 1, build 7601

Vendor Contact:

Vendor name:	AccessData
Address:	603 East Timpanogos Circle, Building H, Floor 2, Suite 2300 Orem, UT 84097
Phone:	(801) 377-5410
Web:	https://accessdata.com

Testing Organization

Organization conducting test: Metro Washington Field Office, Office of Criminal Investigations, US Food and Drug Administration
Contact: stephan.reimers@fda.hhs.gov
Report date: February 28, 2020
Authored by: SR

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

Results Summary

AccessData FTK Imager, Version 4.3.0.18, was tested under a few testing scenarios to acquire bit-for-bit content of electronically stored information (a process known as “imaging”) from select hard disk drives containing known content. The tests were performed using the NIST CFTT Program digital forensics tool testing framework. Under the testing conditions, FTK Imager, Version 4.3.0.18, accurately and consistently imaged hard disk drives without apparent issue.
Furthermore, FTK Imager, Version 4.3.0.18, was able to accurately validate the contents of known electronically stored information from hard disk drive media.

The tool met expectations for the different imaging scenarios tested.

Test Environment & Selected Cases

Hardware: 64 GB RAM, Intel i7-3930K CPU @ 3.20GHz, Digital Intelligence FRED Forensic Workstation computer (S/N F0143037106)
A1 Source Drive: WDC WD80 model OJD-19JN (S/N: WD-WCAM96993422)
A2 Source Drive: WDC WD16 model 00BEKT-0 (S/N: WD-WXD1A50C8886)
A3 Source Drive: Hitachi model HTS54161 (S/N: SB3D0CAWJH1V6D)

Operating System: Microsoft Windows 7 Ultimate (Version: 6.1.7601 SP 1 Build 7601)

Write Blockers Used in Testing

Blocker Model	Firmware Version
Tableau T35689iu Forensic Combo Bridge	May 22, 2013
Tableau T35es Forensic SATA/IDE Bridge	Jan 23, 2013

Selected Test Cases

Tests were configured for the following write block scenarios:

1. Small (< 138GB) SATA drive with Tableau T35689iu Forensic Combo Bridge connected through an internal USB interface embedded in a test computer.
2. Large (> 138GB) SATA drive with Tableau T35689iu Forensic Combo Bridge connected through an internal USB interface embedded in a test computer.

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-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 ascertains 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	a1	Tableau T35689iu Forensic Combo Bridge (USB)	match	match
FT-DI-01-SATA48	a2	Tableau T35689iu Forensic Combo Bridge (USB)	match	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	SHA1
FT-DI-13	a3	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	a3	match	match

Case Summary

Results are as expected.

Appendix: Additional Details

Test Computer Information

OS Name: Microsoft Windows 7 Ultimate
Version: 6.1.7601 Service Pack 1 Build 7601
Other OS Description: Not Available
OS Manufacturer: Microsoft Corporation
System Name: SCERS_FRED_PC
System Manufacturer: System manufacturer
System Model: System Product Name
System Type: x64-based PC
Processor: Intel(R) Core(TM) i7-3930K CPU @ 3.20GHz, 3201 MHz, 6 Core(s), 12 Logical Processor(s)
BIOS Version/Date: American Megatrends Inc. 4505, 12/5/2013
SMBIOS Version: 2.7
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume6
Locale: United States
Hardware Abstraction Layer: Version = "6.1.7601.17514"
User Name: scers_fred_pc\scers_fred
Time Zone: Eastern Standard Time
Installed Physical Memory (RAM): 64.0 GB
Total Physical Memory: 63.9 GB
Available Physical Memory: 56.1 GB
Total Virtual Memory: 126 GB
Available Virtual Memory: 83.6 GB
Page File Space: 61.8 GB
Page File: C:\pagefile.sys

* Generated by msinfo32.exe

Test Drives and Partitions

Test Drive Specifications

Drive specifications were obtained by running the software tool Tableau Imager 1.2.0.0013-r2z9

Drive Test Label: a1
Vendor: WDC WD80
Model: 0JD-19JN
Revision: 1C05
Serial Number: WD-WCAM96993422
Bus: SATA

Device: Direct Access
Capacity: 80.0 GB (80,026,361,856 bytes)
Removable Media: No
Cylinders: 9729
Tracks per Cylinder: 255
Sector per Track: 63
Bytes per Sector: 512
HPA Supported: Yes
HPA in Use: No
DCO Supported: Yes
DCO in Use: No
Security Supported: Yes
Security in Use: No
Reported Capacity: 80.0 GB (80,026,361,856 bytes)
HPA Capacity: 80.0 GB (80,026,361,856 bytes)
DCO Capacity: 80.0 GB (80,026,361,856 bytes)

Drive Test Label: a2
Vendor: WDC WD16
Model: 00BEKT-0
Revision: 1A01
Serial Number: WD-WXD1A50C8886
Bus: SATA
Device: Direct Access
Capacity: 160.0 GB (160,041,885,696 bytes)
Removable Media: No
Cylinders: 19457
Tracks per Cylinder: 255
Sector per Track: 63
Bytes per Sector: 512
HPA Supported: Yes
HPA in Use: No
DCO Supported: Yes
DCO in Use: No
Security Supported: Yes
Security in Use: No
Reported Capacity: 160.0 GB (160,041,885,696 bytes)
HPA Capacity: 160.0 GB (160,041,885,696 bytes)
DCO Capacity: 160.0 GB (160,041,885,696 bytes)

Drive Test Label: a3
Vendor: Hitachi
Model: HTS54161

Revision: C70P
Serial Number: SB3D0CAWJH1V6D
Bus: SATA
Device: Direct Access
Capacity: 120.0 GB (120,034,123,776 bytes)
Removable Media: No
Cylinders: 14593
Tracks per Cylinder: 255
Sector per Track: 63
Bytes per Sector: 512
HPA Supported: Yes
HPA in Use: No
DCO Supported: Yes
DCO in Use: No
Security Supported: Yes
Security in Use: No
Reported Capacity: 120.0 GB (120,034,123,776 bytes)
HPA Capacity: 120.0 GB (120,034,123,776 bytes)
DCO Capacity: 120.0 GB (120,034,123,776 bytes)

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	312581808 (149GiB)*	A27A3 ...	7CF4B ...	04436 ...	FCD66 ...
a3	sata	known	234441648 (111GiB)	C08A5 ...	79642 ...	AC7A3 ...	E1C46 ...
a3+2	osxj	known	58442456 (27GiB)	AA82E ...	10F1E ...	78A08 ...	CDC35 ...
a3+3	fat32	known	58180312 (27GiB)	0C5EB ...	6852C ...	D2CFA ...	696C9 ...
a3+4	exfat	known	29221224 (13GiB)	A1B03 ...	39761 ...	AA188 ...	E8E89 ...

Note: * 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	SR	Scersfredpc	Tableau T35689iu Forensic Combo Bridge (USB)	a1	image-01-sata28.e01	none	Wed Feb 26 22:12:37 2020
ft-di-01-sata48	SR	Scersfredpc	Tableau T35689iu Forensic Combo Bridge (USB)	a2	image-01-sata48.e01	none	Wed Feb 26 22:13:43 2020
ft-di-13	SR	Scersfredpc	Tableau T35689iu Forensic Combo Bridge (USB)	a3	image-01-sata28-a3.e01	none	Wed Feb 26 22:07:04 2020
ft-di-14	SR	Scersfredpc	N/A	a3	none	none	Wed Feb 26 22:07:54 2020

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
VMWare Workstation Pro, ver 15.5.1 build-15018455

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 4, released 9/27/2019