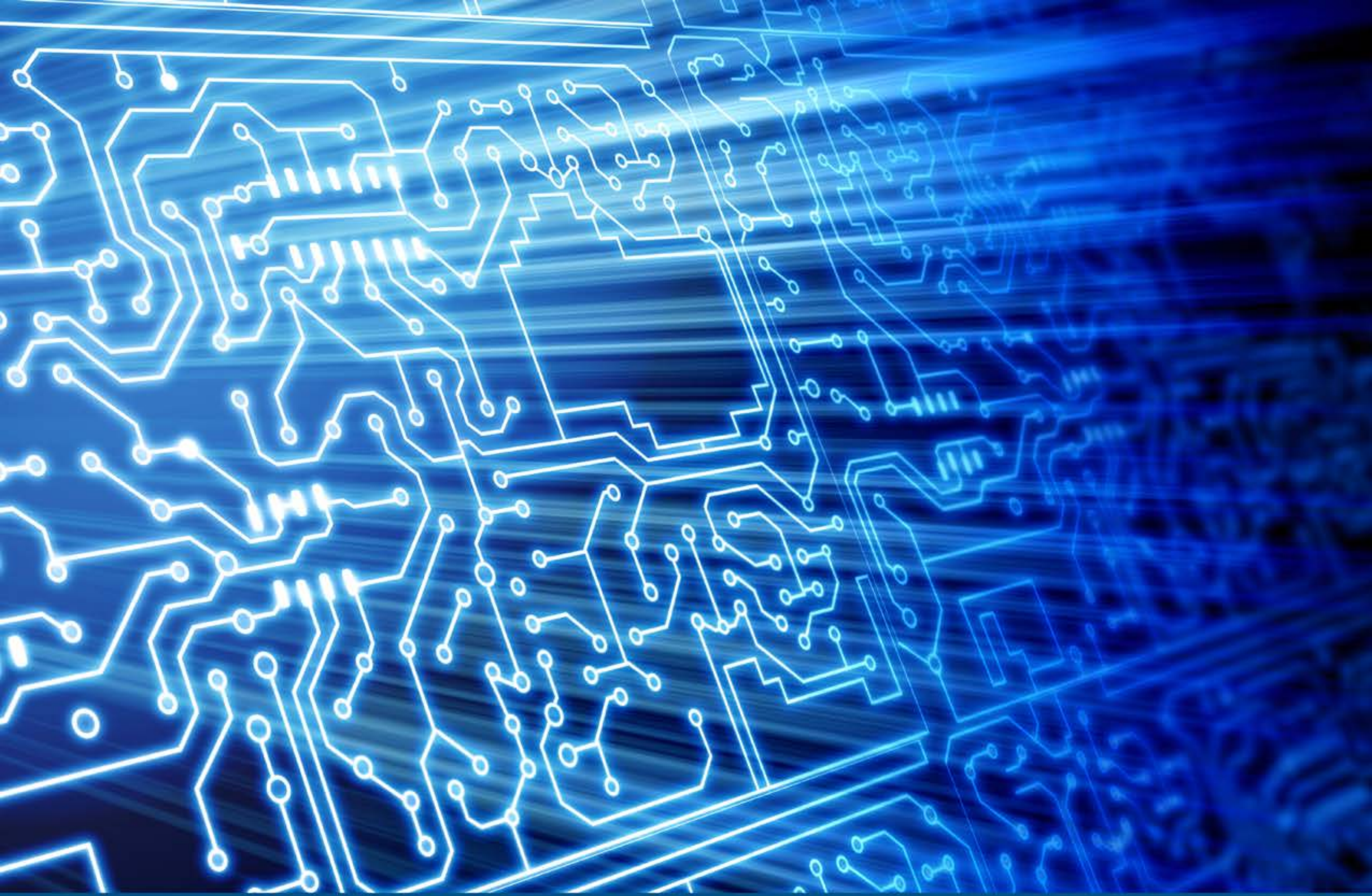

Falcon-NEO Version1.1

Test Results for Disk Imaging Tool – Federated Testing Suite

October 20, 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.

October 2018

Test Results for Disk Imaging Tool:
Falcon-NEO Version 1.1

Federated Testing Suite for Disk Imaging

Contents

Introduction 1
How to Read This Report 2
Tool Description 3
Testing Organization 3
Results Summary 4
Test Environment & Selected Cases 4
Selected Test Cases 5
Test Result Details by Case 6
FT-DI-01 6
Test Case Description 6
Test Evaluation Criteria 6
Test Case Results 6
Case Summary 6
FT-DI-03 7
Test Case Description 7
Test Evaluation Criteria 7
Test Case Results 7
Case Summary 7
FT-DI-05 8
Test Case Description 8
Test Evaluation Criteria 8
Test Case Results 8
Case Summary 8
FT-DI-13 9
Test Case Description 9
Test Evaluation Criteria 9
Test Case Results 9
Case Summary 9
Appendix: Additional Details 10
Test Drives and Partitions 10
Test Case Admin Details 11
Test Setup & Analysis Tool Versions 12

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 the Logicube Falcon-NEO Version 1.1 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 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, and vendor information 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: Logicube Falcon-NEO Version 1.1

Tests were Configured for the Following Write Block Scenarios:

Large (> 138GB) SATA drive with write blocker built-in to imaging device connected to imaging unit by SATA interface
SD Card with write blocker built-in to imaging device connected to imaging unit by USB interface (via SD Card reader)
USB drive with write blocker built-in to imaging device connected to imaging unit by USB interface

Tool Description

Tool Name: Logicube Falcon-NEO
Software Version: 1.1
Kernel Version: 4.9.51-logicube.15

Vendor Contact:

Vendor: Logicube

Address: 19755 Nordhoff Place
Chatsworth, CA 91311

Tel: (888) 494-8832

WWW: https://www.logicube.com/

Testing Organization

Organization conducting test: Computer & Digital Forensics Lab, Carver County Sheriff’s Office, Minnesota, U.S.A.
Contact: anucci@co.carver.mn.us
Report date: 8/3/2018
Authored by: Detective Angela Nucci

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

Results Summary

Logicube's Falcon-NEO met expectations while testing its imaging and hashing capabilities. The tool provides a log, once a task is completed, which includes detailed information about the process such as: duration time of imaging and verification, hash values for source and image (if verification option selected), serial number and file system information for the destination and source, and model information for source and destination. The tool also allows for the examiner to enter case information such as: examiner's name, case number, evidence number, etc. The Falcon-NEO was able to obtain images from a physical drive, and also from a logical partition.

Following are some of the limitations noted during testing:

- "Imaging" option allows for only MD5 and SHA1 hashes to be computed during the imaging and verification process when the "E01Capture" method is selected.
- "Hash/Verify" option allows for hashing of entire physical drives (single partitions cannot be selected). The tool will hash the source partition and verify it against the image during the imaging process if the option "partition to file" is selected during imaging. However, hashing a single partition is not currently an available option within "Hash/Verify." Logicube notes that a single partition can be hashed by selecting the specific LBA range belonging to the partition and that the LBA range for a specific partition can be seen by clicking on the "I" (information) button from within the drive details screen.
- When attempting to hash a drive (not an image file) "Hash/Verify" allows for MD5, SHA1, or SHA256 options, but only one can be selected at a time.
- "Hash/Verify" allows for image file hashing and verification, but only for image files created with Falcon-NEO.

Test Environment & Selected Cases

Hardware: Logicube Falcon-NEO
Software Version: 1.1
Kernel Version: 4.9.51-logicube.15

Write Blockers Used in Testing

Blocker Model	Firmware Version
write blocker built-in to imaging device	N/A

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-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-Ext4	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-13	Compute the hash value of the acquired data within an image file. Test the ability of the tool to re-compute 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). Only the SATA48 test was completed, as SATA drives smaller than 138GB are rarely seen in our laboratory.

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	write blocker built-in to imaging device (SATA)	match	match
FT-DI-01-USB	a2	write blocker built-in to imaging device (USB)	match	match

Case Summary

Results are as expected. To conduct the SATA48 test, a 160GB SATA drive was used. The tool was able to image the hard drive and verify both the MD5 and SHA1 checksums. The tool also computed a “partial hash” for each of the image segments (.e01, .e02, .e03, etc.). During the USB test, the tool also calculated a “partial hash” for the single .e01 image file generated.

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	a3	write blocker built-in to imaging device (USB); Staples SD Card reader model no: 16771	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	a4+1	match	match
FT-DI-05-Ext4	a5+1	match	match
FT-DI-05-FAT32	a6+1	match	match
FT-DI-05-NTFS	a7+1	match	match

Case Summary

Results are as expected. Tool log file will show a table with “Drive Information” indicating information on the source and destination drives. The table includes serial and model number along with file system information. However, the source drive does not reflect file system information and it shows as “NA.” Furthermore, the log includes a “Source Partition Information” table, which does include information on the file system for the source partition imaged.

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	a2	match	match

Case Summary

Results are as expected. The image obtained from source a2 was hashed and verified using Falcon-NEO's "Hash/Verify" option. When verifying an image previously created by Falcon-NEO, the tool allows you to hash and verify both: MD5 and SHA1 hashes. However, if attempting to hash a drive (not an image file), the tool will provide an option to hash using MD5, SHA1, or SHA256. Only one option can be selected at a time. It was also noted that the tool does not have an option for hashing a single partition within "Hash/Verify." However, Logicube notes that a single partition can be hashed by selecting the specific LBA range belonging to the partition and that the LBA range for a specific partition can be seen by clicking on the "I" (information) button from within the drive details screen.

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	312581808 (149GiB)*	2DA11 ...	982B9 ...	1BE53 ...	AA171 ...
a2	usb	known	7577600 (3GiB)	A8F40 ...	14151 ...	44A78 ...	11EAF ...
a3	sd	known	3909632 (1GiB)	20522 ...	3E57C ...	8AADD ...	68765 ...
a4	usb	known	1972224 (963MiB)	44473 ...	AC350 ...	AC03D ...	853CC ...
a4+1	exfat	known	1968128 (961MiB)	2B8BB ...	76A35 ...	03CCB ...	30C3D ...
a5	usb	known	7821312 (3GiB)	EE287 ...	45245 ...	6E8BF ...	549C2 ...
a5+1	ext4	known	7817216 (3GiB)	B1573 ...	74A6D ...	6B8BD ...	66459 ...
a6	usb	known	7821312 (3GiB)	67E3E ...	AFD3D ...	D6D19 ...	842BF ...
a6+1	fat32	known	7817216 (3GiB)	863EB ...	E809A ...	8BE73 ...	77DCF ...
a7	usb	known	7856127 (3GiB)	C40B0 ...	8D7AF ...	07FD4 ...	65ACA ...
a7+1	ntfs	known	7849984 (3GiB)	1F483 ...	3A2FF ...	B5219 ...	7C33D ...
a7+1	NTFS-FS	known	7849977 (3GiB)	79AB3 ..	008F0 ..	361D7 ..	08F4E ..

* 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		Date
ft-di-01-sata48	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (SATA)	a1	d1		Thu Jul 26 14:01:32 2018
ft-di-01-usb	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB)	a2	d2		Thu Jul 26 17:16:36 2018
ft-di-03-sd	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB); Staples SD Card reader model no: 16771	a3	d3		Thu Jul 26 17:46:41 2018
ft-di-05-exfat	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB)	a4	d4		Thu Jul 26 18:11:30 2018
ft-di-05-ext4	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB)	a5	d5		Tue Jul 31 09:57:05 2018
ft-di-05-fat32	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB)	a6	d6		Tue Jul 31 13:22:28 2018
ft-di-05-ntfs	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB)	a7	d7		Fri Aug 3 07:49:32 2018
ft-di-13	DETECTIVE ANGELA NUCCI	Logicube Falcon-NEO	write blocker built-in to imaging device (USB)	a2	d2		Thu Aug 2 10:14:51 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