September 2023

Test Results for Disk Imaging Tool:
Falcon-NEO2 Version: 1.0u1

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's (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology's (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 Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, and U.S. 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 tool: Falcon-NEO2 Version: 1.0u1 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 the DHS S&T-sponsored digital forensics webpage, http://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.) versions 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: Falcon-NEO2 Version: 1.0u1

Tests were Configured for the Following Write Block Scenarios:

Small (< 138GB) SATA drive with write blocker built-in to imaging device connected to PC by SATA interface
Large (> 138GB) SATA drive with write blocker built-in to imaging device connected to PC by SATA interface
SD drive with write blocker built-in to imaging device connected to PC by USB interface
USB drive with write blocker built-in to imaging device connected to PC by USB interface

Tool Description

Tool Name: Falcon-NEO2

Tool Version: 1.0u1

Vendor: Logicube

Testing Organization

Organization Conducting Test: Logicube
Contact: Mario Zelaya
Report Date: 9/13/2023
Authored by: Mario Zelaya
Reviewed by: Peter Manalo
Reviewed by date: 9/13/2023
Approved by: Gabi Abraham
Approved by Date: 9/13/2023

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

Results Summary

Logicube's Falcon-NEO2 met expectations for the different scenarios tested. The Falcon-NEO2 provides a log file in PDF, HTML, or XML once a task is completed. The log contains detailed information about the process such as the device's serial number, software version, duration time of the specified task, hash values for source and image (if verification option selected), and file system information for the source and destination along with model information for source and destination. The tool also allows the examiner to enter case information such as examiner's

name, case number, evidence number, etc. The Falcon-NEO2 was able to obtain images from a physical drive and a logical partition, clone a source to a destination, and hash a source drive.

Test Environment & Selected Cases

Hardware: ***Falcon-NEO2***
Firmware Version: ***1.0u1***
Kernel Version: ***5.10.46-logicube.08***

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-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-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-07-SATA28	Create a clone of a drive directly from a source drive of a given type using a given write blocker connected to a computer over a given interface. Test ability to create a clone during acquisition of given drive type with the given write blocker connected to a computer over the given interface.	completed
FT-DI-07-SATA48	Create a clone of a drive directly from a source drive of a given type using a given write blocker connected to a computer over a given interface. Test ability to create a clone during acquisition of given drive type with the given write blocker connected to a computer over the given interface.	completed
FT-DI-07-USB	Create a clone of a drive directly from a source drive of a given type using a given write blocker connected to a computer over a given interface. Test ability to create a clone during acquisition of given drive type with the given write blocker connected to a computer over the given interface.	completed
FT-DI-08-SD	Create a clone of removable media directly from source media of a given type using a given media reader connected to a computer over a given interface. Test ability to create a clone of removable media during acquisition of given media type with the given media reader connected to a computer over the given interface.	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 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	Reference Hash vs Tool Hash -SHA1
FT-DI-01-SATA28	a1	write blocker built-in to imaging device (SATA)	match	match
FT-DI-01-SATA48	a2	write blocker built-in to imaging device (SATA)	match	match
FT-DI-01-USB	a3	write blocker built-in to imaging device (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	Reference Hash vs Tool Hash – SHA1
FT-DI-03-SD	a4	write blocker built-in to imaging device (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	Reference Hash vs Tool Hash – SHA1
FT-DI-05-ExFAT	a5+1	match	match
FT-DI-05-Ext4	a7+1	match	match
FT-DI-05-FAT32	a8+1	match	match
FT-DI-05-NTFS	a6+1	match	match

Case Summary

Results are as expected.

FT-DI-07

Test Case Description

Create a clone of a drive directly from a source drive of a given type using a given write blocker connected to a computer over a given interface. Test ability to create a clone during acquisition of given drive type with the given write blocker connected to a computer over the given interface.

This test can be repeated to test acquisition of multiple drive types. This test tests the ability of the tool to clone a specific type of drive (the drive type tested is included in the test case name) 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 comparison of the source to the destination should have no sectors differ.

Test Case Results

The following table presents results for individual test cases.

Test Results for FT-DI-07 cases

Case	Src	Blocker (interface)	Compared	Differ
FT-DI-07-SATA28	a9	write blocker built-in to imaging device (SATA)	62533296	0
FT-DI-07-SATA48	a10	write blocker built-in to imaging device (SATA)	468862128	0
FT-DI-07-USB	a11	write blocker built-in to imaging device (USB)	61341696	0

Case Summary

Results are as expected.

FT-DI-08

Test Case Description

Create a clone of removable media directly from source media of a given type using a given media reader connected to a computer over a given interface. Test ability to create a clone of removable media during acquisition of given media type with the given media reader connected to a computer over the given interface.

This test can be repeated to test acquisition of different removable media types. This test tests the ability of the tool to clone a specific type of removable media (the removable media type tested is included in the test case name) 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 comparison of the source to the destination should have no sectors differ.

Test Case Results

The following table presents results for individual test cases.

Test Results for FT-DI-08 cases

Case	Src	Blocker (interface)	Compared	Differ
FT-DI-08-SD	a12	write blocker built-in to imaging device (USB)	62309376	0

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	Reference Hash vs Tool Hash – SHA1
FT-DI-14	a9	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	62533296 (29GiB)	1527D ...	AE37C ...	E0738 ...	3A996 ...
a10	sata	known	468862128 (223GiB)*	2CDC1 ...	97850 ...	8BFDE ...	A59D9 ...
a11	usb	known	61341696 (29GiB)	82591 ...	D3A7B ...	4D249 ...	D045B ...
a12	usb	known	62309376 (29GiB)	101F5 ...	4D87C ...	E9F60 ...	60DAB ...
a2	sata	known	468862128 (223GiB)*	C5E70 ...	B8464 ...	F906F ...	632B0 ...
a3	usb	known	60574592 (28GiB)	E3D4C ...	EF9F4 ...	74BC7 ...	2603B ...
a4	sd	known	3911680 (1GiB)	C8A76 ...	670B4 ...	22164 ...	99107 ...
a5+1	exfat	known	10485760 (5GiB)	6B159 ...	9A0B8 ...	E30E9 ...	F7058 ...
a6+1	ntfs	known	10485760 (5GiB)	7E8FF ...	C4202 ...	EB806 ...	D3ACE ...
a6+1	NTFS-FS	known	10485753 (4GiB)	4F398 ..	EEFAE ..	BE8EB ..	8C88C ..
a7+1	ext4	known	10485760 (5GiB)	050DD ...	07FBA ...	37297 ...	FB00A ...
a8+1	fat32	known	10485760 (5GiB)	2E00A ...	2752F ...	4B1AC ...	5E28A ...
a9	sata	known	62533296 (29GiB)	8CF88 ...	06487 ...	34B20 ...	994C4 ...

* 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	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a1	no	none	Wed Aug 30 16:40:35 2023
ft-di-01-sata48	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a2	no	none	Wed Aug 30 16:37:53 2023
ft-di-01-usb	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (USB)	a3	no	none	Wed Aug 30 18:20:04 2023
ft-di-03-sd	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (USB)	a4	no	none	Thu Aug 31 11:52:37 2023
ft-di-05-exfat	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a5	no	none	Thu Aug 31 12:32:59 2023
ft-di-05-ext4	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a7	no	none	Thu Aug 31 16:13:08 2023
ft-di-05-fat32	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a8	no	none	Thu Aug 31 19:14:19 2023
ft-di-05-ntfs	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a6	no	none	Thu Aug 31 13:37:15 2023
ft-di-07-sata28	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a9	none	d1	Fri Sep 1 16:06:08 2023
ft-di-07-sata48	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (SATA)	a10	none	d2	Wed Sep 6 12:58:32 2023
ft-di-07-usb	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (USB)	a11	none	d3	Wed Sep 6 17:56:09 2023
ft-di-08-sd	MARIO_ZELAYA	Falcon-Neo2	write blocker built-in to imaging device (USB)	a12	none	d4	Thu Sep 7 17:05:06 2023
ft-di-14	MARIO_ZELAYA	Falcon-Neo2	N/A	a9	none	none	Thu Sep 7 17:47:44 2023

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
diskcmp.c Linux Version 1.4 Created 04/08/22 at 12:27:48
diskwipe.c Linux Version 1.6 Created 04/08/22 at 12:26:03
zbios.c Linux Version 1.9 Created 04/08/22 at 11:51:01
zbios.h Linux Version 1.4 Created 04/08/22 at 11:48:35

Tool: @(#) ft-di-prt_test_report.py Version 1.24 created 05/23/18 at 16:08:06
OS: Linux Version 5.13.0-48-generic
Done: 2023-09-13 16:52:46.090747