August 2016

Test Results for Disk Imaging Tool: X-Ways Forensics Version 18.8

Federated Testing Test 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 (http://www.cftt.nist.gov/).

This document reports the results from testing the disk imaging function of X-Ways Forensics Version 18.8 using the CFTT Federated Testing Test Suite for Disk Imaging, Version 1.0.

The Federated Testing Test Suite for Disk Imaging is flexible to allow a forensic lab to trade-off the time required to test every tool feature versus testing just the imaging tool features used by a specific lab. This report reflects testing the features that some forensic labs are likely to use on a day-to-day basis.

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: X-Ways Forensics Version 18.8

Tests were Configured for the Following Write Block Scenarios:

Small (< 138GB) ATA drive with WiebeTech ComboDock connected to PC by USB interface
Large (> 138GB) ATA drive with Tableau Model T35es-R2 connected to PC by FireWire interface
Small (< 138GB) SATA drive with Tableau Model T3U connected to PC by FireWire interface
Large (> 138GB) SATA drive with Tableau Model T3U connected to PC by FireWire interface
SD drive with Digital Intelligence UltraBlock USB 3.0 Card Reader connected to PC by USB interface

Tool Description

Tool Name: X-Ways Forensics
Tool Version: 18.8

Operating System: Windows 7

Vendor Contact:

Vendor name:	X-Ways Software Technology AG
Address:	PO box 62 02 08 50695 Cologne Germany
Phone:	+49 221-449 079 80
Web:	https://www.x-ways.net/
E-mail:	mail@x-ways.com

Testing Organization

Organization responsible for test: DHS S&T Cyber Security Division.
Contact: cftt@nist.gov

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: Dell Optiplex 980 PC with USB 2 and FireWire 400 ports.

Operating system: Windows 7

Write Blockers Used in Testing

Blocker Model	Firmware Version
WiebeTech ComboDock	N/A
Tableau Model T35es-R2	Jan 23 2013 12:20:26
Tableau Model T3U	Apr 11 2006 18:47:46
Digital Intelligence UltraBlock USB 3.0 Card Reader	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-ATA28	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-ATA48	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-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	completed

	ability to read a given drive type accurately and correctly hash the data while creating an image file.	
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-03-SD	Acquire removable media of a given type using a given media reader or 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 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
FT-DI-01-ATA28	a1	WiebeTech ComboDock (USB)	match
FT-DI-01-ATA48	a3	Tableau Model T35es-R2 (FireWire)	match
FT-DI-01-SATA28	a2	Tableau Model T3U (FireWire)	match
FT-DI-01-SATA48	a4	Tableau Model T3U (FireWire)	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 or 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 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 that 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
FT-DI-03-SD	a5	Digital Intelligence UltraBlock USB 3.0 Card Reader (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	a2+1	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	ata	known	156301488 (74GiB)	921C6 ...	1072D ...	94853 ...	E7C14 ...
a2	sata	known	117231408 (55GiB)	83253 ...	59C5C ...	932DB ...	6933D ...
a2+1	ntfs	known	39104480 (18GiB)	E9076 ...	A4F0B ...	0859B ...	EAF3C ...
a2+1	NTFS-FS	known	39104472 (18GiB)	EA8AD ..	A4943 ..	3A284 ..	9D6D2 ..
a3	ata	known	312581808 (149GiB)*	E2FED ...	A4389 ...	A2661 ...	21C54 ...
a4	sata	known	312581808 (149GiB)*	FD3E7 ...	8D1B1 ...	27C15 ...	16BF2 ...
a5	sd	known	1998848 (976MiB)	28D5C ...	98ED5 ...	2B93E ...	4E9FD ...

* 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.

Case	Host	Blocker (PC interface)	Src	Image	Dst	Date
ft-di-01-ata28	Seven	WiebeTech ComboDock (USB)	a1	11	none	Thu Apr 28 08:39:04 2016
ft-di-01-ata48	Seven	Tableau Model T35es-R2 (FireWire)	a3	11	none	Thu Apr 28 08:41:15 2016
ft-di-01-sata28	Seven	Tableau Model T3U (FireWire)	a2	11	none	Thu Apr 28 08:42:10 2016
ft-di-01-sata48	Seven	Tableau Model T3U (FireWire)	a4	11	none	Thu Apr 28 08:43:09 2016
ft-di-03-sd	Seven	Digital Intelligence UltraBlock USB 3.0 Card Reader (usb)	a5	11	none	Thu Apr 28 08:44:40 2016

ft-di-05-ntfs	Seven		a2	11	none	Thu Apr 28 08:45:23 2016

Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions

cftt-di Version 1.16 created 11/24/15 at 11:10:20
diskwipe.c Linux Version 1.5 Created 03/20/13 at 14:23:34

Tool: @(#) ft-di-prt_test_report.py Version 1.18 created 05/03/16 at 13:25:45
OS: Darwin Version 12.6.0