Test Results for Disk Imaging Tool:
OSForensics Version 8.0.1007

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 (S&T), the National Institute of Justice, and the National Institute of Standards and Technology (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 Criminal Investigation Division Electronic Crimes Program, and the DHS 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 OSForensics Version 8.0.1007 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 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: OSForensics Version 8.0.1007

Tests were Configured for the Following Write Block Scenarios:

USB drive with write blocker built-in to imaging device connected to PC by USB interface

Tool Description

Tool Name: OSForensics
Tool Version: 8.0.1007

Vendor Contact:

Vendor:	Passmark Software Inc.
Address:	370 Convention Way, Level 2 Redwood City, California 94063
Tel:	(650) 216-2306
WWW:	https://osforensics.com /

Testing Organization

Organization conducting test: Passmark Software Inc.
Contact: jeffs@passmark.com
Report date: 2/27/2021
Authored by: Eric McClelland

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

Results Summary

OSForensics, version 8.0.1007, was utilized to acquire bit-for-bit content of stored electronic data (commonly referred to as "imaging") from a generic USB storage device containing known content. The USB drive used was prepared using the NIST CFTT Program digital forensics tool testing framework.

OSForensics, version 8.0.1007, accurately imaged the USB drive with known content and was able to successfully validate the resultant image file compared to the original source media used in testing. OSForensics met expectations and no errors were encountered while performing the imaging scenario.

Test Environment & Selected Cases

Hardware: 32 GB RAM, Intel i7-6700HQ CPU @ 2.6GHz, Dell Alienware 17 R3 Laptop Computer

A1 Source Drive: Generic USB Storage Drive with the following Sectors/Drive Size - 15728640 (7GiB)

Operating System: Microsoft Windows 10 Pro Version 10.0.19042 Build 19042Software: OSForensics Version 8.0.1007 write blocking functionality enabled to facilitate a write blocked connection between the workstation and the source drive being imaged.

Write Blockers Used in Testing

Blocker Model	Firmware Version
software write blocker	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-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

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 Advanced Technology Attachment (ATA) or Serial Advanced Technology Attachment (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-USB	a1	write blocker built-in to imaging device (USB)	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., New Technology File System (NTFS), File Allocation Table 32 (fat 32), etc., depending on whether a drive or a partition is being described.

Test Drives

Drive	Type	Content	Sectors	MD5	SHA1	SHA256	SHA512
a1	usb	known	152728640 (7GiB)	39B81 ...	64B9B ...	2F55B ...	3772E ...

* 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-usb	ERIC_MCCLELLD	Alienwarer17	software write blocker (USB)	a1	image-01-usb.e01	none	Sat Feb 27 12:12:24 2021

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 5, released 3/12/2020