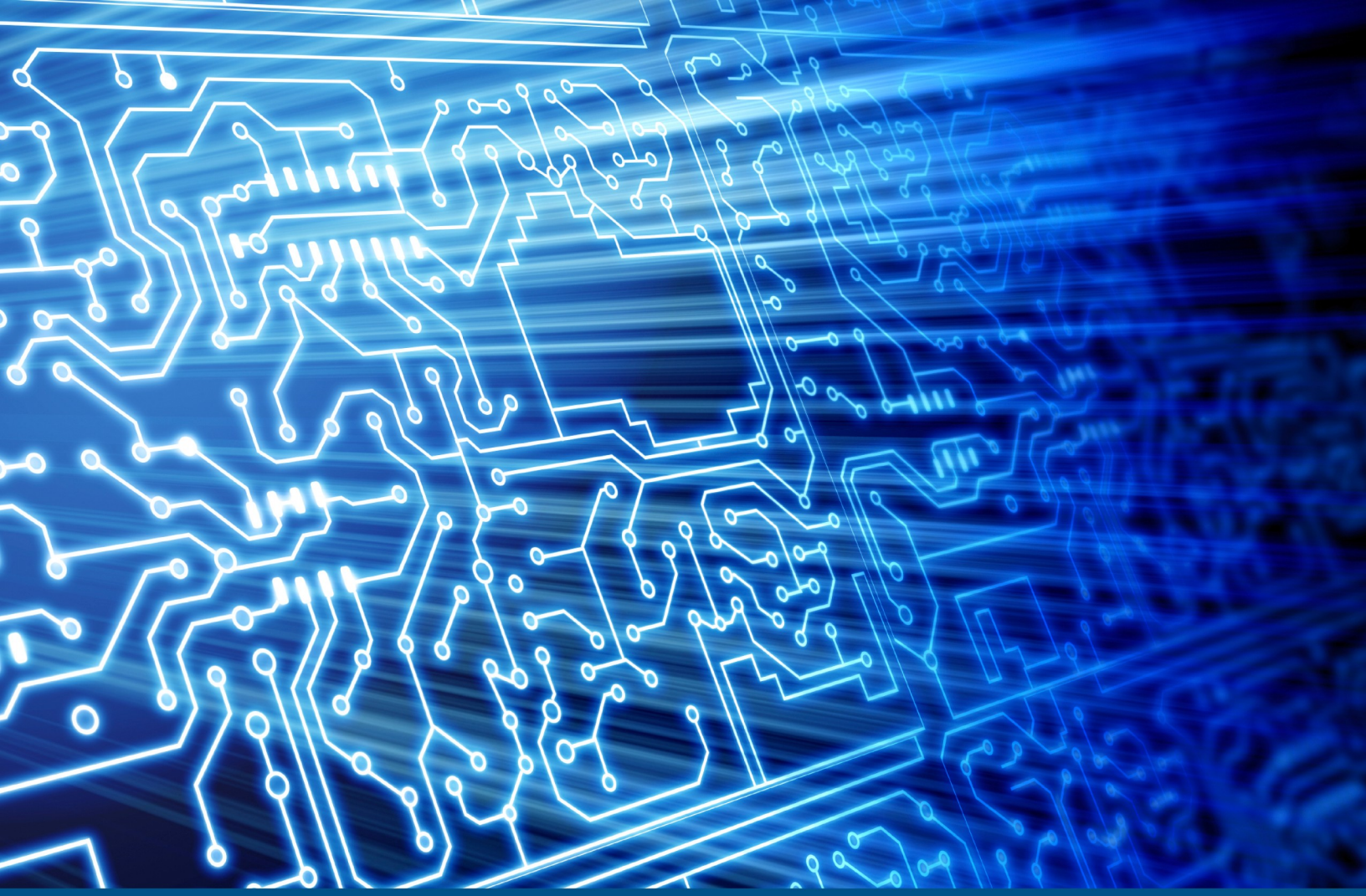

E3 Version 2.3

Test Results for Disk Imaging Tool

March 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.

March 2020

Test Results for Disk Imaging Tool:
E3 Version 2.3

Federated Testing Suite for Disk Imaging

Contents

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

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; 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 E3 Version 2.3 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, 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. **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: E3 Version 2.3

Tool Description

Tool Name: E3
Tool Version: 2.3
Operating System: Microsoft Windows 10 Enterprise 64-bit, version 1903, build 18362.356

Vendor Contact:

Vendor name:	Paraben Corporation
Address:	39344 John Mosby Hwy Ste 277 Aldie, VA 20105-2000 USA
Phone:	+1 (801) 796-0944

Testing Organization

Organization conducting test: Paraben Corporation
Contact: Amber@paraben.com
Report date: November 20, 2019
Authored by: Amber Schroader

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

Results Summary

The tool met expectations for the different imaging scenarios tested.

Test Environment & Selected Cases

Hardware:
Test/Analysis PC: MSI B360M Pro-VDH
FT-LOGS USB: Silicon Motion USB flash disk 1100 2GB (S/N: AA77DPGTK06O2TW4)
A1 Source Drive: HGST HTS 500 GB (S/N: 000ECC020035D0CA, Model: 545050A7E680)
A2 Source Drive: Western Digital Elements 1078 1 TB (S/N: 57583631413734445A543936)

Operating System: Microsoft Windows 10 Enterprise 64-bit, version 1903, build 18362.356

Write Blockers Used in Testing

Blocker Model	Firmware Version
WiebeTech USB WriteBlocker	0103
Tableau T35e	Sep 12 2011

Selected Test Cases

This table presents a brief description of each test case that was performed.

Test Case Status

Case	Description	Status
FT-DI-05-Ext2	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-FAT16	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

Test Result Details by Case

This section presents test results grouped by function.

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	SHA256
FT-DI-05-Ext2	a1+1	match	match	match
FT-DI-05-Ext4	a1+2	match	match	match
FT-DI-05-FAT16	a2+1	match	match	match
FT-DI-05-FAT32	a1+3	match	match	match
FT-DI-05-NTFS	a1+4	match	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+4	ntfs	known	209715200 (100GiB)	BA5B3 ...	F742E ...	DC001 ...	7FDB8 ...
a1+4	NTFS-FS	known	209715193 (99GiB)	CAC65 ...	E6F3E ...	5BD73 ...	F5A12 ...
a1+3	fat32	known	67108864 (32GiB)	DF117 ...	FCC60 ...	57A6D ...	A683B ...
a1+1	ext2	known	82411520 (39GiB)	C6030 ...	3F74B ...	D45DD ...	FA02B ...
a1+2	ext4	known	167772160 (80GiB)	EFFA5 ...	EE243 ...	878A7 ...	766FD ...
a2+1	fat16	known	8386560 (3GiB)	53249 ...	3BA56 ...	6FDAC ...	67CAB ...

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-05-ext2	LEE	Pcs1	Tableau T35e (USB)	a1	no	none	Fri Nov 1 16:58:23 2019
ft-di-05-ext4	LEE	Pcs1	Tableau T35e (USB)	a1	no	none	Sat Nov 2 10:06:43 2019
ft-di-05-fat16	LEE	Pcs1	WiebeTech USB WriteBlocker (USB)	a2	no	none	Fri Nov 1 11:18:53 2019
ft-di-05-fat32	LEE	Pcs1	Tableau T35e (USB)	a1	no	none	Thu Oct 31 14:34:27 2019
ft-di-05-ntfs	LEE	Pcs1	Tableau T35e (USB)	a1	no	none	Fri Nov 1 16:55:50 2019

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