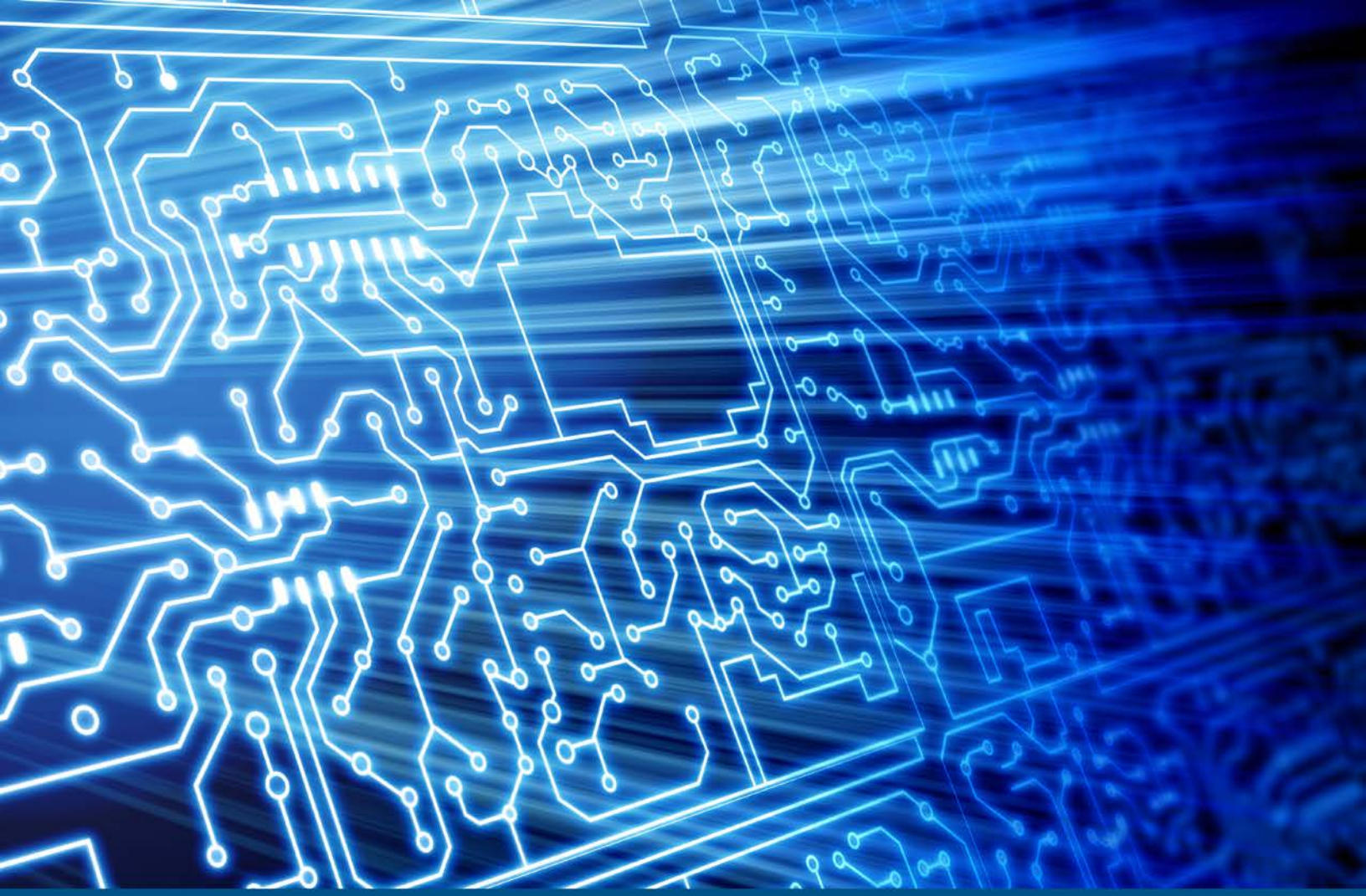

USB WriteBlocker

Test Results for Hardware Write Block Device - Federated Testing Suite

October 14, 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
DHS's Cyber Security Program.

October 2018

Test Results for Hardware Write Block Device:
USB WriteBlocker

Federated Testing Suite for Hardware Write Blocking

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.

This document reports the results from testing the hardware write blocking function of the CRU USB WriteBlocker using the CFTT Federated Testing Test Suite for Hardware Write Blocking, Version 3.1-1.

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 NIST's Software Quality Group 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.

How to Read This Report

This report is organized into the following sections:

1. Tested Device Description. The tool name, version and vendor information are listed.
2. 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 on tool use.
3. Test Environment. Description of hardware and software used in tool testing.
4. Test Result Details by Case. Automatically generated test results that identify anomalies.
5. Appendix: Additional details. Additional details for each test case.

Test Results for Hardware Write Block Device: CRU USB WriteBlocker

1. Device Description

Device Name: CRU USB WriteBlocker

Manufacturer Contact:

Manufacturer:	CRU Acquisition Group
Address:	1000 SE Tech Center Dr Suite 160 Vancouver, WA 98683
Tel:	(800) 260-9800
WWW:	CRU Associates Website

2. Results Summary

The tested device functioned as expected with no anomalies.

3. Test Environment

Hardware:
Custom PC with 4 USB 3, 8 USB 2, 3 eSATA, 2 FireWire 800 and 2 FireWire 400 ports.

CRU USB WriteBlocker
Serial Number: 001228802

4. Test Result Details by Case

This section presents test results grouped by case.

4.1. FT-HWB-USB

4.1.1. Test Case Description

Test a write blocker's ability to write-protect an USB drive. This test can be repeated to test multiple types of connections (interfaces) between a computer and the write blocker. Test the ability of the write blocker to block write commands from the ATA and SCSI command sets issued from a test computer from modifying an USB drive.

4.1.2. Test Drive Description

Manufacturer, model & size of the test drive used for this test: Kingston, DataTraveler G4, 16GB

4.1.3. Test Evaluation Criteria

For each computer to blocker connection tested, the number of ‘writes not blocked’ should be 0.

4.1.4. Test Case Results

The following table presents results for the test case.

Test Results for FT-HWB-USB		
Computer to Blocker Connection	**Write Commands Sent**	**Writes Not Blocked**
USB 2	5	0

4.1.5. Case Summary

Test drive unchanged.

5. Appendix: Additional Details

5.1. FT-HWB-USB

5.1.1. USB 2

```
/usr/lib/cgi-bin/test-hwb Fri Jul  6 12:18:48 2018
@(#) test-hwb.c Linux Version 1.4 created 06/27/18 at 10:56:14
compiled Jun 27 2018 10:56:31 with gcc Version 5.4.0 20160609
@(#) wrapper.c Linux Version 1.5 support lib created 08/03/17 at 13:05:44
@(#) ataraw.c Linux Version 1.3 support lib created 08/03/17 at 13:05:44
@(#) ataraw.h Linux Version 1.3 created 08/03/17 at 13:06:12
cmd: /usr/lib/cgi-bin/test-hwb -bh -sg -p /media/cftt/FT-LOGS/FT-HWB-usb/ GP
SCIMITAR FT-HWB-usb usb2 usb /dev/sda
operator: GP
host: SCIMITAR
test case: FT-HWB-usb
connection type: usb2
drive/media type: usb
device: /dev/sda
*** forcing only SCSI commands to be sent... ***


Opcode  Command Name                  Status          Lba/Sector      Result
0Ah     (SCSI) WRITE 6                Sent            2576            Unchanged
2Ah     (SCSI) WRITE 10               Sent            10768           Unchanged
AAh     (SCSI) WRITE 12               Sent            43536           Unchanged
8Ah     (SCSI) WRITE 16               Sent            35344           Unchanged
7Fh     (SCSI) WRITE 32               Sent            32528           Unchanged

5 writes sent, 0 write(s) not blocked, 0 write commands unsupported.

RESULTS: test drive unchanged

run start Fri Jul  6 12:18:48 2018
run finish Fri Jul  6 12:18:48 2018
elapsed time 0:0:0
Normal exit

Status Key:
Sent -  the ioctl used to send this command returned without error and the
ATA error bit (if applicable) was not set.
Not supported -  the ioctl used to send this command return with an error
status or the command completed with the ATA error bit set.
Test terminated -  the test was terminated for dangerous commands because 3
or more previous commands were not blocked.

Result Key:
Unchanged -  no changes to the test drive were detected.
Not Blocked -  sending this command resulted in a change to the test drive.
This command was NOT blocked!
n/a -  Not applicable.
```

5.2. Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions
test-hwb.c Linux Version 1.4 created 06/27/18 at 10:56:14

Tool: @(#) ft_hwb_prt_test_report.py Version 1.2 created 04/26/18 at 10:11:19
OS: Linux Version 4.13.0-37-generic
Federated Testing Version 3.1-1, released 06/27/2018