



Apricorn Aegis Fortress Firmware Version 0401

Test Results for Write-Protected Drive

November 07, 2019



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/cyber-security-division>.

November 2019

Test Results for Write-Protected Drive:
Apricorn Aegis Fortress Firmware Version 0401

Federated Testing Suite for Hardware Write Blocking

Contents

Introduction.....	1
How to Read This Report	2
1 Device Description.....	3
2 Testing Organization.....	3
3 Results Summary	3
4 Test Environment.....	3
5 Test Result Details by Case	4
5.1 FT-HWB-USB	4
5.1.1 Test Case Description	4
5.1.2 Test Drive Description	4
5.1.3 Test Evaluation Criteria	4
5.1.4 Test Case Results	4
5.1.5 Case Summary	4
6 Appendix: Additional Details	5
6.1 FT-HWB-USB	5
6.1.1 USB 3	5
6.2 Test Setup & Analysis Tool Versions.....	6

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 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 read-only function of the Apricorn Aegis Fortress device firmware version 0401 using the CFTT Federated Testing Test Suite for Hardware Write Blocking, 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 Device Description**
The device name, version and vendor information 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 device meets expectations and provides a summary of any ways the device did not meet expectations. The section also provides any observations of interest about the device or about testing the device including any observed limitations on device use.
4. **Test Environment**
Description of hardware and software used in device testing.
5. **Test Result Details by Case**
6. Automatically generated test results that identify anomalies.
7. **Appendix: Additional details**
More information about each test case.

Federated Testing Test Results for Write-Protected Drive: Apricorn Aegis Fortress

1 Device Description

Device Name: Aegis Fortress
Firmware Version: 0401

Manufacturer Contact:

Manufacturer: Apricorn
Address: 12191 Kirkham Road
Poway, CA 92064
Tel: (800) 458-5448
WWW: <https://www.apricorn.com>

2 Testing Organization

Organization conducting test: Apricorn
Contact: Kevin Su
Report date: 6-26-2019
Authored by: Mark D.

3 Results Summary

The tested device performed as expected. Data on the device was unchanged by the attempted writes.

4 Test Environment

Hardware: tests were run using a computer with an ASUS ROG Strix B450-F Gaming motherboard.

Aegis Fortress, firmware version 0401. Put the drive in read-only mode before testing to repeat the tests.

5 Test Result Details by Case

This section presents test results grouped by case.

5.1 FT-HWB-USB

5.1.1 Test Case Description

Test a USB key or USB portable drive's ability to write-protect when Read-Only mode is enabled. Test the ability of the USB key or USB portable drive to block write commands from the ATA and SCSI command sets issued from a test computer.

5.1.2 Test Drive Description

Manufacturer, model & size of the test drive used for this test: Apricorn Fortress with 1TB capacity (A25-3PL256-1000F) configured in read-only mode.

5.1.3 Test Evaluation Criteria

The number of 'writes not blocked' should be 0.

5.1.4 Test Case Results

The following table presents results for the test case.

Test Results for FT-HWB-USB		
Computer to Drive Connection	Write Commands Sent	Writes Not Blocked
USB 3	36	0

5.1.5 Case Summary

Test drive unchanged.

6 Appendix: Additional Details

6.1 FT-HWB-USB

6.1.1 USB 3

```
/usr/lib/cgi-bin/test-hwb Thu Aug 15 14:12:56 2019
@(#) test-hwb.c Linux Version 1.3 created 05/17/18 at 15:05:48
compiled May 17 2018 15:06:05 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 -p /media/cftt/FT-LOGS/FT-HWB-usb/ Mark_D.
AMD-5 FT-HWB-usb usb3 usb /dev/sda
operator: Mark_D.
host: AMD-5
test case: FT-HWB-usb
connection type: usb3
drive/media type: usb
device: /dev/sda
device type (ATA or SCSI - /usr/lib/cgi-bin/test-hwb tries to guess):
    SCSI
```

Opcode	Command Name	Status	Lba/Sector	Result
30h	(ATA) WRITE SECTOR(S)	Sent	12288	Unchanged
CAh	(ATA) WRITE DMA	Sent	51712	Unchanged
CCh	(ATA) WRITE DMA QUEUED	Sent	52224	Unchanged
C5h	(ATA) WRITE MULTIPLE	Sent	50432	Unchanged
31h	(ATA) WRITE SECTOR(S) w/o retries	Sent	12544	Unchanged
CBh	(ATA) WRITE DMA w/o retries	Sent	51968	Unchanged
3Ch	(ATA) WRITE VERIFY	Sent	15360	Unchanged
34h	(ATA) WRITE SECTOR(S) EXT	Sent	13312	Unchanged
39h	(ATA) WRITE MULTIPLE EXT	Sent	14592	Unchanged
CEh	(ATA) WRITE MULTIPLE FUA EXT	Sent	52736	Unchanged
3Bh	(ATA) WRITE STREAM EXT	Sent	15104	Unchanged
35h	(ATA) WRITE DMA EXT	Sent	13568	Unchanged
3Dh	(ATA) WRITE DMA FUA EXT	Sent	15616	Unchanged
36h	(ATA) WRITE DMA QUEUED EXT	Sent	13824	Unchanged
3Eh	(ATA) WRITE DMA QUEUED FUA EXT	Sent	15872	Unchanged
3Ah	(ATA) WRITE STREAM DMA EXT	Sent	14848	Unchanged
38h	(ATA) CFA WRITE SECTORS W/O ERASE	Sent	14336	Unchanged
CDh	(ATA) CFA WRITE MULTIPLE W/O ERASE	Sent	52480	Unchanged
C0h	(ATA) CFA ERASE SECTORS	Sent	49152	Unchanged
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
2Eh	(SCSI) WRITE AND VERIFY 10	Sent	11792	Unchanged
AEh	(SCSI) WRITE AND VERIFY 12	Sent	44560	Unchanged
8Eh	(SCSI) WRITE AND VERIFY 16	Sent	36368	Unchanged
7Fh	(SCSI) WRITE AND VERIFY 32	Sent	32529	Unchanged
41h	(SCSI) WRITE SAME 10	Sent	16656	Unchanged
93h	(SCSI) WRITE SAME 16	Sent	37648	Unchanged

Opcode	Command Name	Status	Lba/Sector	Result
7Fh	(SCSI) WRITE SAME 32	Sent	32530	Unchanged
3Fh	(SCSI) WRITE LONG 10	Sent	16144	Unchanged
9Fh	(SCSI) WRITE LONG 16	Sent	40720	Unchanged
32h	(ATA) WRITE LONG	Sent	12800	Unchanged
33h	(ATA) WRITE LONG w/o retries	Sent	13056	Unchanged
45h	(ATA) WRITE UNCORRECTABLE EXT	Sent	17664	Unchanged

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

RESULTS: test drive unchanged

run start Thu Aug 15 14:12:56 2019
run finish Thu Aug 15 14:15:58 2019
elapsed time 0:3:2
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.

6.2 Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions
test-hwb.c Linux Version 1.3 created 05/17/18 at 15:05:48

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, released 5/25/2018