March 2020

Test Results for Hardware Write Block Device: Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection (Linux)

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) Science and Technology Directorate (S&T), 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, and U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, as well as 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 website (https://www.cftt.nist.gov/).

This document reports the results from testing the hardware write blocking function of the Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection using the CFTT Federated Testing Test Suite for Hardware Write Blocking, Version 4.

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.
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:** Automatically generated test results that identify anomalies.
6. **Appendix: Additional details:** Additional details for each test case.

Federated Testing Test Results for Hardware Write Block Device: Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter

1 Device Description

Device Name: SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection

Manufacturer Contact:

Manufacturer:	Coolgear Inc
Address:	5120 110th Avenue North Clearwater, Florida 33760
Tel:	(888) 688-2188
WWW:	https://www.coolgear.com/

2 Testing Organization

Organization conducting test: Nova Southeastern University
Contact: lh1490@mynsu.nova.edu
Report date: February 15th, 2020
Authored by: Lazaro Herrera

3 Results Summary

The Coolgear tool is a consumer-grade USB to SATA / IDE device that contains two independent switches for 'write-protecting' media that can be procured for roughly $50 USD. The tool contains features that make it difficult to accidentally switch from 'write-protect' to 'write' mode (device must be powered off and powered back on). The manufacturer claims the write-protect functionality is guaranteed under Windows and makes no claims about any write-protect security under Linux. The testing documented by this report proves that the device is not forensically sound under Linux environments. In the testing, using an Ubuntu Linux environment, the device failed to block several write commands when write-protecting a SATA drive. Further testing may confirm or disprove manufacturer claims on Windows forensics viability.

4 Test Environment

Hardware:

Computer #1: Windows 10 Machine with AMD Ryzen 7 2700x processor, 16Gb of DDR4 RAM. Used to forensically clean devices using Roadkil's Diskwipe.

Computer #2: Small portable mini-itx machine for running CFTT Federated Testing Test Suite for Hardware Write Blocking (Portable_Forensics_1).

Hard Drive: 320GB Seagate Momentus 5400.5 SATA Hard Drive was used.
Note: 2.5" drives can be connected through USB only, 3.5" require a power brick.

Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection Tool
Used for both imaging and testing (hardware was moved between devices).
Device should have switches moved to 'lock' before being switched on.

Software:

Roadkil's Diskwipe
Used for performing quick zero wipes on hardware.
Images taken after every wipe to remove software as a variable.

FTK Imager Lite 3.1.1.8
Extracted from Caine 11.0 Windows Live Tooling.
Used for taking images before and after testing.

5 Test Result Details by Case

This section presents test results grouped by case.

5.1 FT-HWB-SATA

5.1.1 Test Case Description

Test a write blocker's ability to write-protect a SATA 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 a SATA drive.

5.1.2 Test Drive Description

Manufacturer, model & size of the test drive used for this test:

Manufacturer: Seagate
Model: Momentus 5400.5
Size: 320GB

5.1.3 Test Evaluation Criteria

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

5.1.4 Test Case Results

The following table presents results for the test case.

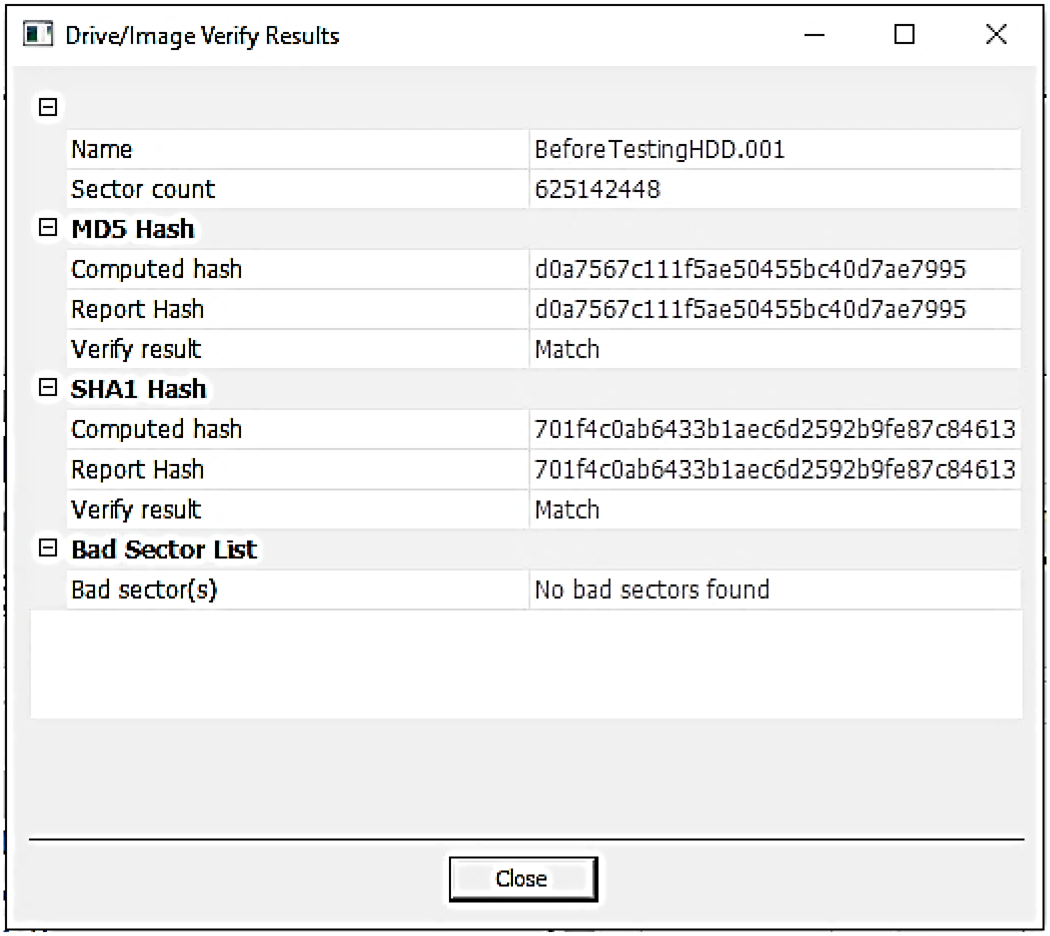
Test Results for FT-HWB-SATA

Computer to Blocker Connection	**Write Commands Sent**	**Writes Not Blocked**
USB 3	31	**10**

5.1.5 Case Summary

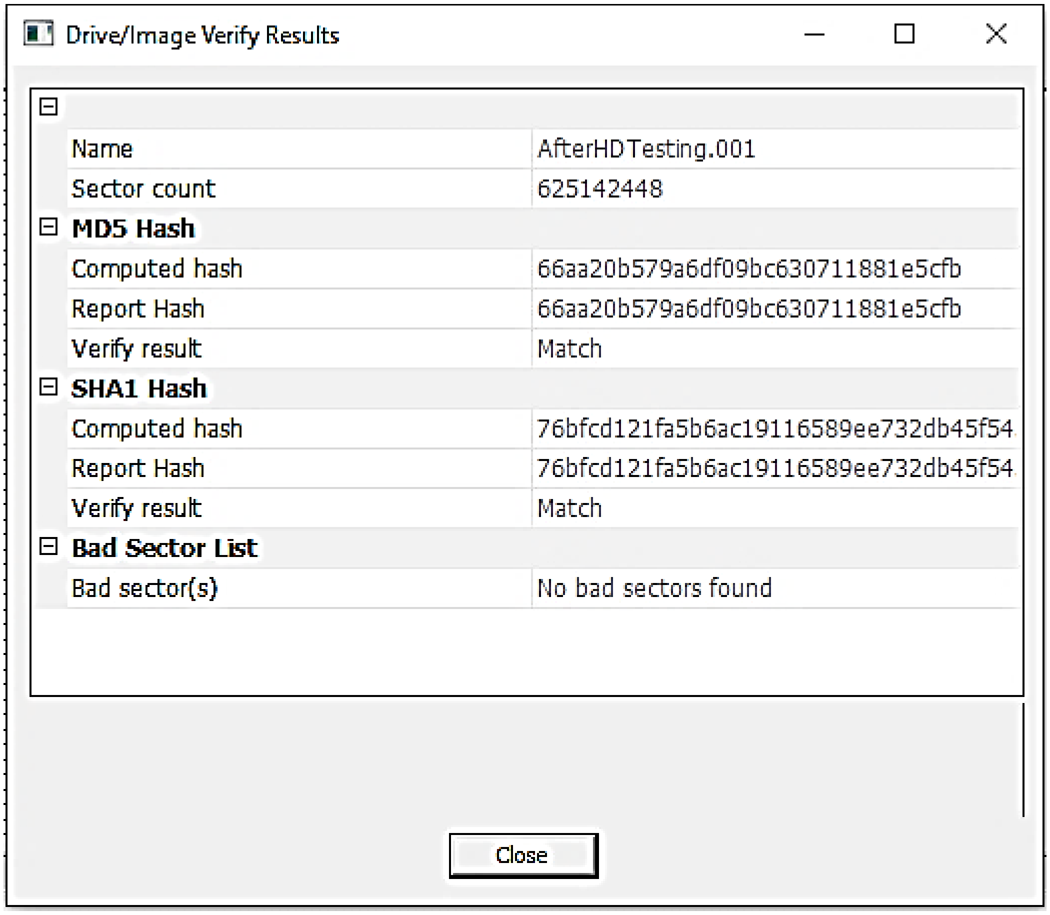
Blocker DID NOT block all writes.

As can be seen below, it is clear that the hashes (MD5 and SHA1) of the drive have changed during testing.



Drive/Image Verify Results

Name	BeforeTestingHDD.001
Sector count	625142448
MD5 Hash	
Computed hash	d0a7567c111f5ae50455bc40d7ae7995
Report Hash	d0a7567c111f5ae50455bc40d7ae7995
Verify result	Match
SHA1 Hash	
Computed hash	701f4c0ab6433b1aec6d2592b9fe87c84613
Report Hash	701f4c0ab6433b1aec6d2592b9fe87c84613
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found



Name	AfterHDTesting.001
Sector count	625142448
MD5 Hash	
Computed hash	66aa20b579a6df09bc630711881e5cfb
Report Hash	66aa20b579a6df09bc630711881e5cfb
Verify result	Match
SHA1 Hash	
Computed hash	76bfcd121fa5b6ac19116589ee732db45f54
Report Hash	76bfcd121fa5b6ac19116589ee732db45f54
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Full before and after logs for FTK Imager and full images can be furnished upon request.

Additionally, research shows (WARNING: EXTERNAL LINK) some reviewers have used Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection devices as an alternative to forensics-grade hardware with Linux.

6 Appendix: Additional Details

6.1 FT-HWB-SATA

6.1.1 USB 3

```
/usr/lib/cgi-bin/test-hwb Sat Feb 15 02:58:12 2020
@(#) 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 -p /media/cftt/FT-LOGS/FT-HWB-sata/
Lazaro_Herrera Portable_Forensics_1 FT-HWB-sata usb3 sata /dev/sdc
operator: Lazaro_Herrera
host: Portable_Forensics_1
test case: FT-HWB-sata
connection type: usb3
drive/media type: sata
device: /dev/sdc

 Opcode  Command Name                    Status             Lba/Sector  Result

 30h     (ATA) WRITE SECTOR(S)           Sent               12288       Not Blocked
 CAh     (ATA) WRITE DMA                 Sent               51712       Not Blocked
 CCh     (ATA) WRITE DMA QUEUED          Sent               52224       Unchanged
 C5h     (ATA) WRITE MULTIPLE            Sent               50432       Not Blocked
 31h     (ATA) WRITE SECTOR(S)           Sent               12544       Not Blocked
               w/o retries
 CBh     (ATA) WRITE DMA w/o retries     Sent               51968       Not Blocked
 3Ch     (ATA) WRITE VERIFY              Sent               15360       Unchanged
 34h     (ATA) WRITE SECTOR(S) EXT       Sent               13312       Not Blocked
 39h     (ATA) WRITE MULTIPLE EXT        Sent               14592       Not Blocked
 CEh     (ATA) WRITE MULTIPLE FUA EXT    Sent               52736       Not Blocked
 3Bh     (ATA) WRITE STREAM EXT          Sent               15104       Unchanged
 35h     (ATA) WRITE DMA EXT             Sent               13568       Not Blocked
 3Dh     (ATA) WRITE DMA FUA EXT         Sent               15616       Not Blocked
 36h     (ATA) WRITE DMA QUEUED EXT      Sent               13824       Unchanged
 3Eh     (ATA) WRITE DMA QUEUED FUA      Sent               15872       Unchanged
               EXT
 3Ah     (ATA) WRITE STREAM DMA EXT      Sent               14848       Unchanged
 38h     (ATA) CFA WRITE SECTORS W/O     Sent               14336       Unchanged
         ERASE
 CDh     (ATA) CFA WRITE MULTIPLE W/O    Sent               52480       Unchanged
               ERASE
 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
 7Fh     (SCSI) WRITE SAME 32            Sent               32530       Unchanged
 Opcode  Command Name                    Status            Lba/Sector  Result
 3Fh     (SCSI) WRITE LONG 10            Test terminated!  16144       n/a
 9Fh     (SCSI) WRITE LONG 16            Test terminated!  40720       n/a
 32h     (ATA) WRITE LONG                Test terminated!  12800       n/a
 33h     (ATA) WRITE LONG w/o retries    Test terminated!  13056       n/a
 45h     (ATA) WRITE UNCORRECTABLE EXT   Test terminated!  17664       n/a

31 writes sent, 10 write(s) not blocked, 0 write commands unsupported.

RESULTS: blocker DID NOT block all writes

run start Sat Feb 15 02:58:12 2020
run finish Sat Feb 15 03:03:25 2020
elapsed time 0:5:13
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 1.4 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 4, released 9/27/2019