

Test Results for Hardware Write Block Tool: Guidance Software Tableau Forensic Firmware Version T35U

Tool Description

Tool Name: Tableau Forensic
Firmware Version: T35U
Tool Manufacturer: Guidance Software

Testing Organization

Organization conducting test: *BGSU*.
Contact: S. Roy (sanroy@bgsu.edu)
Report date: *Dec 5th 2018*.
Authored by: *Quinton*.
Reviewed by: *Ashley, Blake*.
Reviewed by date: *Dec 5th 2018*.
Approved:
Approved by date:

This test report was generated using CFTT's Federated Testing Forensic Tool Testing Environment, see [Federated Testing Home Page](#).

How to Read This Report

This report is organized into the following sections:

1. Tested Tool Description. Guidance Software, Tableau Forensics, T35U
2. Testing Organization. Contact information and approvals.
3. How to Read This Report (this section).
4. 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.

5. Test Environment. Description of hardware and software used in tool testing in sufficient detail to satisfy the testing organization's policy and requirements.
6. Test Result Details by Case. Automatically generated test results that identify anomalies.
7. Appendix: Additional details. Additional details for each test case.

Results Summary

The tool was able to block writes as expected. The software was unable to find any places on the hard drive that it was able to write to. The CFTT iso was able to quickly run its tests without any issues

Test Environment

Hardware: *640 GB Hard Drive, Dell Computer, Tableau Forensics Hard-Ware Write blocker. 16GB Sandisk USB for logs*

Software: *Virtualbox VM 3GB RAM allocated, 2 CPU cores, NIST CFTT ISO loaded from Desktop*

Tableau Forensic Firmware Version: T35U

Test Result Details by Case

This section presents test results grouped by case.

FT-HWB-ATA/IDE

/media/cftt/FT-LOGS/FT-HWB-ata is missing

FT-HWB-SATA

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.

Test Drive Description

Manufacturer, model & size of the test drive used for this test: Western Digital 640 GB drive for Apple Computers

Test Evaluation Criteria

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

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	36	0

Case Summary

Test drive unchanged.

Appendix: Additional Details

FT-HWB-SATA

USB 3

```
/usr/lib/cgi-bin/test-hwb Wed Dec 5 19:09:05 2018
@(#) 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-sata/ AGBGQC
020_Lab_Computer FT-HWB-sata usb3 sata /dev/sdc
operator: AGBGQC
host: 020_Lab_Computer
test case: FT-HWB-sata
connection type: usb3
drive/media type: sata
device: /dev/sdc
device type (ATA or SCSI - /usr/lib/cgi-bin/test-hwb tries to guess):
    ATA
48-bit Address Feature Set:      NOT SUPPORTED
```

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
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 Wed Dec 5 19:09:05 2018
run finish Wed Dec 5 19:09:05 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.

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

Done: 2018-12-05 19:10:10.559847

Federated Testing Version 3.1, released 5/25/2018

END of REPORT