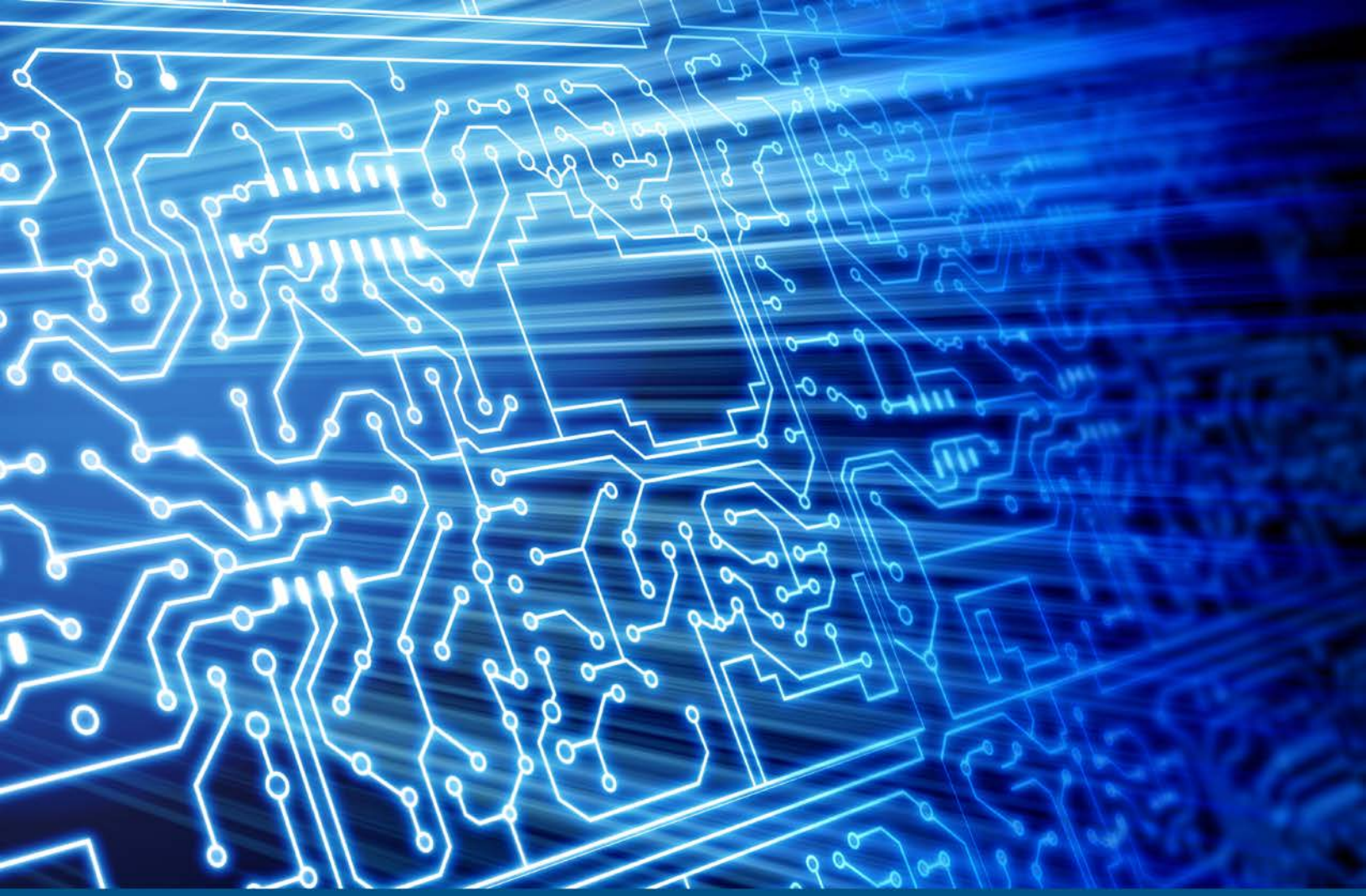

Tableau Forensic SATA/IDE Bridge T35u

Test Results for Hardware Write Block Device - Federated Testing Suite

October 17, 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 http://www.dhs.gov/science-and-technology/cyber-security-division.

October 2018

Test Results for Hardware Write Block Device:
Tableau Forensic SATA/IDE Bridge T35u
Firmware Version Sep 15 2015 11:19:41

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 (https://www.cftt.nist.gov/).

This document reports the results from testing the hardware write blocking function of the Tableau Forensic SATA/IDE Bridge T35u device firmware version Sep 15 2015 11:19:41 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 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 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: Tableau Forensic SATA/IDE Bridge T35u

1. Device Description

Device Name: Tableau Forensic SATA/IDE Bridge T35u
Firmware Version: Sep 15 2015 11:19:41

Manufacturer Contact:

Manufacturer:	OpenText Corporation
Address:	1055 E. Colorado Blvd. Pasadena, CA 91106-2375
Tel:	(866) 229-9199
WWW:	https://www.guidancesoftware.com/

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.

Forensic SATA/IDE Bridge T35u Firmware Version: Sep 15 2015 11:19:41
Serial Number: 000ecc55 003550ad

4. Test Result Details by Case

This section presents test results grouped by case.

4.1. FT-HWB-ATA/IDE

4.1.1. Test Case Description

Test a write blocker's ability to write-protect an ATA/IDE 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 ATA/IDE drive.

4.1.2. Test Drive Description

Manufacturer, model & size of the test drive used for this test: IBM, IC35L040AVER07-0, 40GB

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-ATA/IDE		
Computer to Blocker Connection	**Write Commands Sent**	**Writes Not Blocked**
USB 3	36	0

4.1.5. Case Summary

Test drive unchanged.

4.2. FT-HWB-SATA

4.2.1. 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.

4.2.2. Test Drive Description

Manufacturer, model & size of the test drive used for this test: Kingston, SVP100S264G, 64GB

4.2.3. Test Evaluation Criteria

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

4.2.4. 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	36	0

4.2.5. Case Summary

Test drive unchanged.

5. Appendix: Additional Details

5.1. FT-HWB-ATA/IDE

5.1.1. USB 3

```
/usr/lib/cgi-bin/test-hwb Tue Jul  3 13:14:31 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 -p /media/cftt/FT-LOGS/FT-HWB-ata/ GP
DEATH_STAR FT-HWB-ata usb3 ata /dev/sdc
operator: GP
host: DEATH_STAR
test case: FT-HWB-ata
connection type: usb3
drive/media type: ata
device: /dev/sdc

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 Tue Jul  3 13:14:31 2018
run finish Tue Jul  3 13:14:31 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. FT-HWB-SATA

5.2.1. USB 3

```
/usr/lib/cgi-bin/test-hwb Tue Jul  3 13:11:29 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 -p /media/cftt/FT-LOGS/FT-HWB-sata/ GP
DEATH_STAR FT-HWB-sata usb3 sata /dev/sdc
operator: GP
host: DEATH_STAR
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           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
```

```
Opcode  Command Name                    Status          Lba/Sector      Result
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 Tue Jul  3 13:11:29 2018
run finish Tue Jul  3 13:11:29 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.
```

5.3. 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