[MISDE]

September | 2006

Functionality Test of Tableau® UltraBlock™ Forensic USB Bridge Device

MARSHALL
INFORMATION SECURITY
& DIGITAL EVIDENCE

MISDE

Marshall University
Forensic Science Center
1401 Forensic Science Dr.
Huntington, WV 25701
Phone: 304/690-4363
Fax: 304/690-4360

http://forensics.marshall.edu/MISDE

Disclaimer of Liability:

With respect to this document, neither the Marshall University Forensic Science Center nor any of its employees, makes any warranty, express or implied, including the warranty of fitness for a particular purpose, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed. Any mention of commercial products within the following documents is intended for information purposes only and is not intended to be used as a substitute and/or replacement for an external laboratory's own test validation. It is advised to independently verify any information prior to reliance thereon.

Redistribution Policy:

MISDE grants permission for the redistribution and use of the following posted document created by MISDE, provided that the following conditions are met.

1) Redistributions of documents, or parts of the documents, must retain the MUFSC/MISDE cover and disclaimer of liability page.
2) Neither the name of the Marshall University Forensic Science Center nor the Information Security and Digital Evidence Laboratory (MISDE) may be used to endorse or promote products derived from the following document.
3) Any reference or quote obtained from the following MISDE document must be properly annotated in the document that the reference is contained therein.

MARSHALL UNIVERSITY
FORENSIC SCIENCE CENTER
MISDE Laboratory
Official Document

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

TEST PLAN

Test Number: USBwriteblock-01

Test Title: Functionality Test of Tableau® UltraBlock™ Forensic USB Bridge Device

Test Date: 2/16/2006

Purpose and Scope:

To safely acquire and analyze universal serial bus (USB) enabled devices, the MISDE Laboratory possesses the Tableau® UltraBlock™ Forensic USB Bridge Device. The UltraBlock™ is a hardware-based write blocker that allows USB mass storage devices (i.e. flash drives, thumb drives, external USB hard drives, etc.) to be connected to a computer for forensic acquisition and examination.

This test plan will test the ability of the UltraBlock™ USB device to accurately read data from a USB mass storage device without data being inadvertently modified during acquisition and/or examination. This test consists of four scenarios:

Requirements:

1) The UltraBlock™ USB write-block device should successfully recognize a USB mass storage device in a Windows environment.

2) The UltraBlock™ USB write-block device should successfully block all write attempts to the USB mass storage device.

3) An MD5 hash algorithm should be calculated before and after a write attempt to USB device.

4) The MD5 hash calculations of the USB flash device should match .

Description of Methodology:

The Tableau® UltraBlock™ USB Writeblock device will be connected to a Dell Optiplex GX270 PC (3.20 GHz, Windows XP 32 Bit, Service pack 2, 1.0GB DDR RAM) using USB 2.0 connection. The source media, a 64 MB Dell/Lexar® SmartFlash ™ USB thumb Device (see figure 1.1) will be attached to the USB 2.0 port of the UltraBlock device (see figure 1.2). The UltraBlock™ device will be powered on and an MD5 hash calculation will be performed using EnCase® Forensic Edition Version 5.04a for Windows (see figure 2.1). Upon completion of the MD5 hash algorithm calculation, the device will be viewed in Windows Explorer. A folder entitled “Test Document.doc” will attempted be transferred to the UltraBlock™ attached USB thumb drive (see figure 2.2). The UltraBlock™ USB Bridge will then be powered down and restarted. The USB thumb device will again be viewed within Windows explorer to determine if the attempted write was successful (figure 2.3). An MD5 hash calculation will be performed once again on the USB thumb device while attached to UltraBlock™ Forensic USB Bridge (see figure 2.4).

Expected Results:

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

1) The Tableau UltraBlock™ Forensic USB Bridge will successfully calculate an MD5 hash value for the attached USB thumb device.

2) The Tableau UltraBlock™ Forensic USB Bridge will successfully prevent modification to the attached USB thumb device.

3) An MD5 hash performed on the USB thumb disk after the write attempt will match the original MD5 hash calculation of the USB thumb device before a write attempt was completed.

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-01	USB thumb device; Tableau UltraBlock™ Forensic USB Bridge	Drive recognized in Windows	1	Drive will be visible in Windows explorer
01-02	USB thumb device; Tableau UltraBlock™ Forensic USB Bridge; EnCase® v.5.04a for Windows	MD5 hash calculation performed on USB thumb device	3	MD5 Hash calculation will be produced.
01-03	USB thumb device; Tableau UltraBlock™ Forensic USB Bridge	Write attempt to USB thumb device	2	No modification will be made to protected USB thumb device.
01-04	USB thumb device; Tableau UltraBlock™ Forensic USB Bridge; EnCase® v.5.04a for Windows	MD5 hash calculation performed on USB thumb device	3	MD5 Hash calculation produced.
01-04	N/A	Comparison of MD5 calculations before and after write attempt	4	MD5 calculations should match

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Test Data Description:

USB device info (as reported by Tableau® UltraBlock™ Forensic USB bridge):

Mfg name: Lexar®
Product name: Digital Film
Serial Number: 03
Firmware rev: /W1.
USB speed: 12mbps
USB Class Info: class=8 subclass=6 protocol=50
Int Node ID: 1
USB address: 2
SCSI class disk: 0

USB Tech info (as reported by Tableau® UltraBlock™ Forensic USB bridge):

Device mfg name: LEXR PLUG DRIVE
Device model name: LEXR PLUG DRIVE
Device serial number: 03
Vendor ID: 5dc
Product ID: 80
Class 8
Subclass: 6
Protocol: 50
USB Revision: 1
Configurations supported by device: 1
Max Power: 90ma

MD5 hash value (before write attempt): 7516D73D43E4F2BCDDF6720E45963393

MD5 hash value (after write attempt): 7516D73D43E4F2BCDDF6720E45963393

EnCase® Forensic Edition v5.04a Hash Statistics (before write attempt to USB device):

Status: Completed
Start: 02/16/06 13:26:43
Stop: 02/16/06 13:27:56
Time: 0:01:13
Name: USB thumb drive viewed in UltraBlock
Start Sector: 0
Stop Sector: 125,951
Hash Value: 7516D73D43E4F2BCDDF6720E45963393

EnCase® Forensic Edition v5.04a Hash Statistics (after write attempt to USB device):

Status: Completed
Start: 02/16/06 13:42:39
Stop: 02/16/06 13:43:53
Time: 0:01:14
Name: USB thumb drive viewed in UltraBlock (after write attempt)
Start Sector: 0
Stop Sector: 125,951
Hash Value: 7516D73D43E4F2BCDDF6720E45963393

MARSHALL UNIVERSITY
FORENSIC SCIENCE CENTER
MISDE Laboratory
Official Document

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

SUMMARY REPORT

Test Number: USBwriteblock-01

Test Title: Functionality Test of Tableau ® UltraBlock ™ Forensic USB Bridge Device

Test Date: 2/14/2006

Test Description:

This test documents the results of the functionality of the Tableau ® UltraBlock Forensic USB Bridge. The analysis consists of five scenarios:

Forensic Tool:

Title: UltraBlock™ Forensic USB Bridge
Manufacturer: Tableau® (Digital Intelligence)
Model Number: Model T8
Serial Number: T005Co17391

Test Results:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:	Results:
01-01	USB 64 MB thumb device; Tableau UltraBlock™ Forensic USB Bridge	Drive recognized in Windows	1	Device will be visible in Windows explorer	Pass
01-02	USB 64 MB thumb device; Tableau UltraBlock™ Forensic USB Bridge; EnCase ® v.5.04a for Windows	MD5 hash calculation performed on USB thumb device	3	MD5 Hash calculation will be produced.	Pass
01-03	USB 64 MB thumb device; Tableau® UltraBlock™ Forensic USB Bridge	Write attempt to USB thumb device	2	No modification will be made to protected USB thumb device.	Pass
01-04	USB thumb device; Tableau ® UltraBlock ™ Forensic USB Bridge; EnCase® v.5.04a for	MD5 hash calculation performed on USB thumb device	3	MD5 Hash calculation will be	Pass

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

	Windows			produced.	
01-05	N/A	Comparison of MD5 calculations before and after write attempt	4	MD5 hash calculations should match	Pass

Requirements:

1) The UltraBlock™ USB write-block device should successfully recognize a USB mass storage device in a Windows environment.

2) The UltraBlock™ USB write-block device should successfully block all write attempts to the USB mass storage device.

3) An MD5 hash algorithm should be calculated before and after a write attempt to USB device

4) The MD5 hash calculations of the USB flash device should match.

Observations:

N/A

Limitations:

During the test procedure a failure to dismount UltraBlock™ USB bridge before powering down in some cases caused an improper recognition of the device on the next powerup during the test procedure

Recommendations:

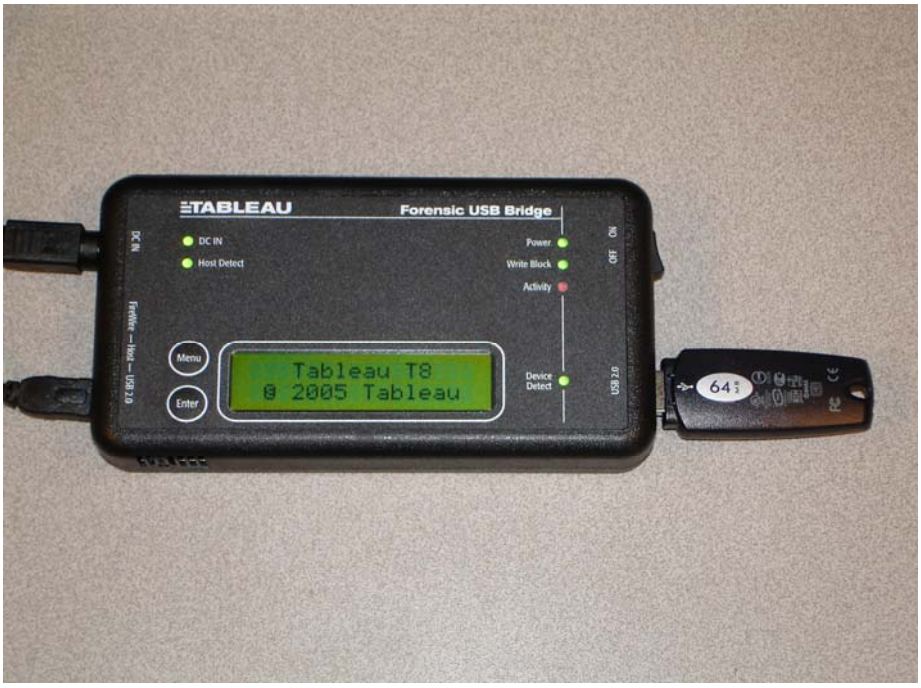
It is recommended to safely remove the hardware by clicking on the safe dismount icon on the lower right portion of the Windows system tray.

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 1.1- Dell/Lexar® 64 MB USB thumb device used for analysis

Figure 1.2 USB thumb drive attached to UltraBlock™ USB bridge.



1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 2.1 Hash statistics of USB thumb device before write attempt

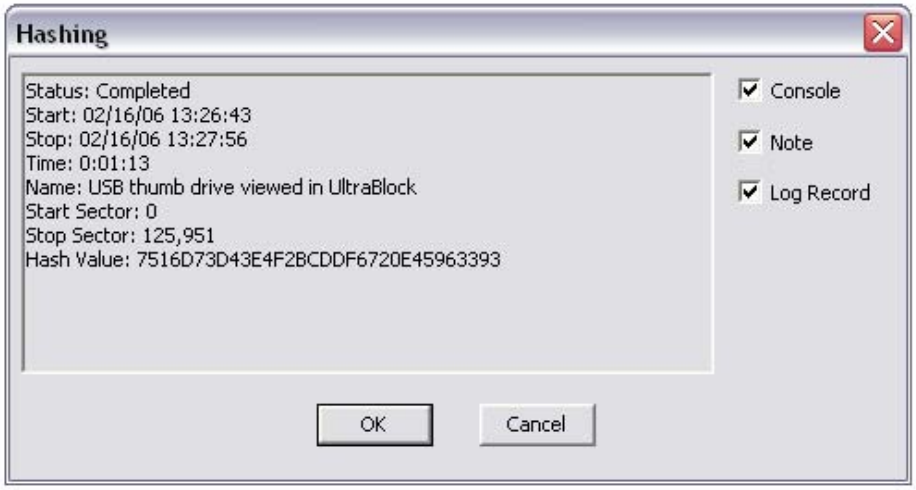


Figure 2.2 Write attempt to USB flash device attached to UltraBlock™ Forensic USB Bridge

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 2.3 Contents of USB thumb drive after write attempt viewed in Windows Explorer

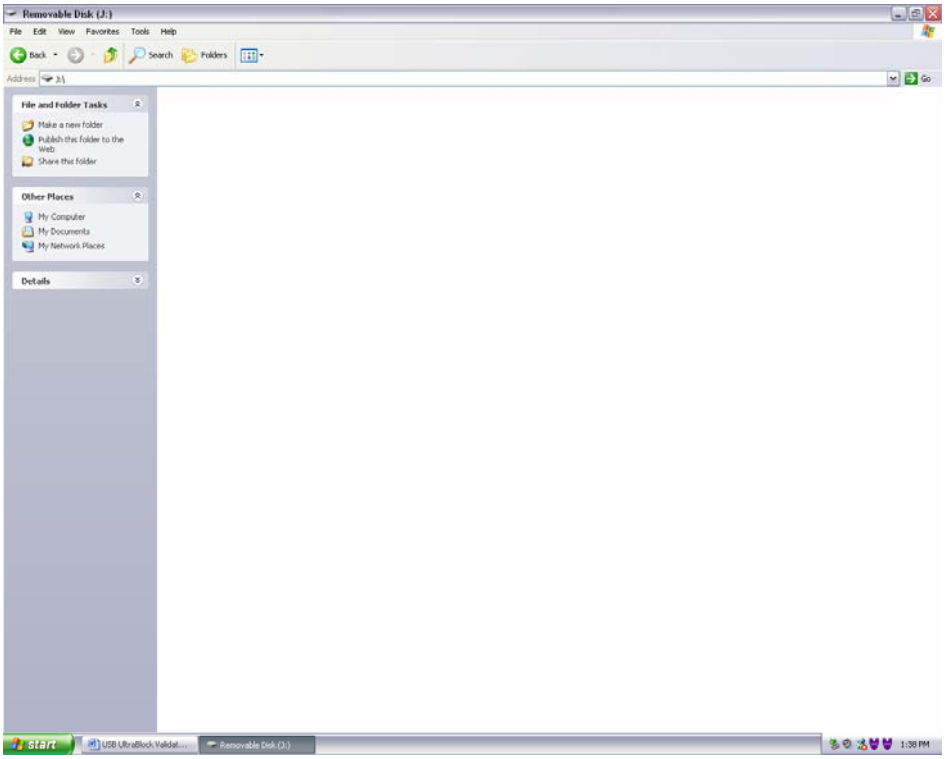


Figure 2.4 Hash statistics of USB thumb device after write attempt