[MISDE]

September | 2006

Validation Testing of Guidance Software's FastBloc Laboratory Edition (LE)

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: FastBlocLE-01

Test Title: Validation Testing of FastBloc Laboratory Edition (LE).

Test Date: 2/28/2006 to 3/2/2006

Purpose and Scope:

Guidance Software's FastBloc® Laboratory Edition (LE) is a hardware write-blocking device that enables the safe viewing and acquisition of source media within a Windows, Linux, or DOS-based environment. FastBloc LE is an IDE write-blocker that installs directly to the secondary IDE channel on the computer's motherboard.

This test plan will test the ability of the FastBloc Laboratory Edition (LE) to allow normal hard disk write-block operation to occur to source media. This test plan will consist of four test scenarios:

Requirements:

1) The FastBloc Laboratory Edition (LE) will successfully recognize an IDE enabled drive within a Windows environment.

2) The FastBloc Laboratory Edition (LE) should successfully compute a message digest (MD5) hash algorithm calculation of the source hard disk drive.

3) The FastBloc Laboratory Edition (LE) should allow normal hard disk write-block operation to the source hard drive.

4) The FastBloc Laboratory Edition (LE) should successfully compute an MD5 hash calculation that is consistent with the original MD5 hash calculation.

Description of Methodology:

The subject ATA hard disk drive will be connected to the FastBloc LE via the external IDE channel. A hardware MD5 hash calculation will be performed using EnCase v.5.04a for Windows. A write-operation will then be performed on the hard disk. The hard disk will be shutdown and restarted via the FastBloc LE and the file system viewed to determine if the write-operation was persistent. A subsequent MD5 calculation will be performed on the hard disk using Encase Forensic Edition version 5.04a.

The FastBloc LE must successfully protect the IDE hard disk drive from modification. In addition, the devices should allow for MD5 hash calculations to be performed using EnCase Forensic Edition v.5.04a.

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

Expected Results:

1) The IDE-enabled source hard disk will successfully be recognized in Windows while attached to the Guidance Software FastBloc LE.

2) The Guidance Software FastBloc LE will successfully calculate an MD5 hash value for the source IDE hard-disk.

3) The Guidance Software FastBloc LE write-block device will successfully prevent hard disk modification.

4) An MD5 hash performed on the disk after the write attempt will match the original MD5 hash calculation of the hard disk drive.

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-02	Source drive; FastBloc LE	Source drive attached to FastBloc LE write blocking device	1	Hard disk drive will be recognized within Windows.
01-02	Source drive; FastBloc LE; EnCase v.5.04a for Windows	MD5 hash calculation performed on subject drive	2	MD5 Hash calculation produced.
01-03	Source drive; FastBloc LE: Windows Explorer	Folder added to subject drive. Windows powered down and restarted	3	No modification to protected hard disk
01-04	Source Drive; FastBloc LE; EnCase v.5.04a for Windows	MD5 hash calculation performed on source drive	4	MD5 calculation matches original MD5 hash calculated on drive.

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

Test Data Description:

Test Data (see figure 1:1):

Seagate Barracuda ATA III
Model: ST320414A
Serial Number: 7eC0AS9Y
Part Number: 9R3004-301
Firmware Number: 3.05
20 Gigabyte Ultra ATA HDD

Drive Parameters:
Cylinders: 16383
Heads: 16
Sectors: 63
Addressable Sectors: 39,102,336

Installed Software:
Windows XP 32 Bit O/S w/ SP2
Microsoft Office 2003 Pro
Dell GX270 Drivers and Utilities Disk

Guidance Software FastBloc LE MD5 hash value (before write attempt):
F2FE69015F701475863293A71DDDA0D7

Guidance Software FastBloc LE MD5 hash value (after write attempt):
F2FE69015F701475863293A71DDDA0D7

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: FastBloc LE-01

Test Title: Validation Testing of Guidance Software's FastBloc Laboratory Edition (LE)

Test Date: 2/28/2006 to 3/1/2006

Test Description:

This test documents the ability of the FastBloc Laboratory Edition (LE) to successfully prevent write-attempts to a subject IDE hard drive. The test will additionally document the hardware's ability to produce consistent MD5 hash calculations.

Forensic Tool:

Title: FastBloc Laboratory Edition (LE)
Manufacturer: Guidance Software
Model Number: F.G.-0500-000A
Serial Number: 702516

Test Results:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-02	Source drive; FastBloc LE	Source drive attached to FastBloc LE write blocking device	1	Hard disk drive will be recognized within Windows.
01-02	Source drive; FastBloc LE; EnCase v.5.04a for Windows	MD5 hash calculation performed on subject drive	2	MD5 Hash calculation produced.
01-03	Source drive; FastBloc LE: Windows Explorer	Folder added to subject drive. Windows powered down and restarted	3	No modification to protected hard disk
01-04	Source Drive; FastBloc LE; EnCase v.5.04a for Windows	MD5 hash calculation performed on source drive	4	MD5 calculation matches original MD5 hash calculated on drive.

Requirements:

5) The FastBloc Laboratory Edition (LE) will successfully recognize an IDE enabled drive within a Windows environment.

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

6) The FastBloc Field Edition (LE) should successfully compute an MD5 hash calculation of the source hard disk drive.

7) The FastBloc Field Edition (LE) should allow normal hard disk write-block operation to the source hard drive.

8) The FastBloc Field Edition (LE) should successfully compute an MD5 hash calculation that is consistent with the original MD5 hash calculation.

Observations:

When performing a write-attempt operation, the disk cache of Microsoft Windows XP retained the file “test-document.doc” when examined using Windows explorer (see figure 1.4). Alternatively, after a shutdown and reboot of the system, the file was cleared from the disk cache and no modification was made to the protected hard disk (see figure 1.5).

Limitations:

N/A

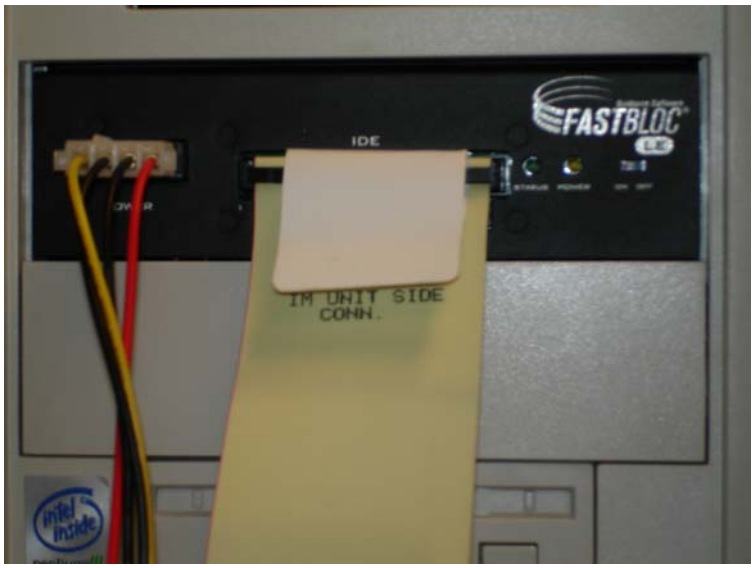
Recommendations:

N/A

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

Figure 1.1 Seagate Barracuda 18.6 GB laboratory validation hard disk attached to FastBloc LE.

Figure 1.2 Shown here is the Guidance Software FastBloc® Laboratory Edition (LE) S/N# 702515



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

Figure 1.3 EnCase Forensic Edition v.5.04a hash statistics of Seagate 18.6 GB hard disk attached to FastBloc LE before a write attempt operation.

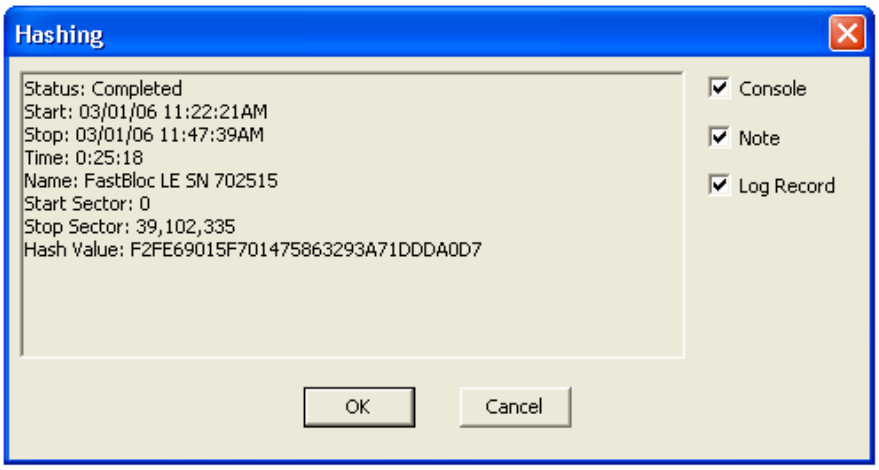
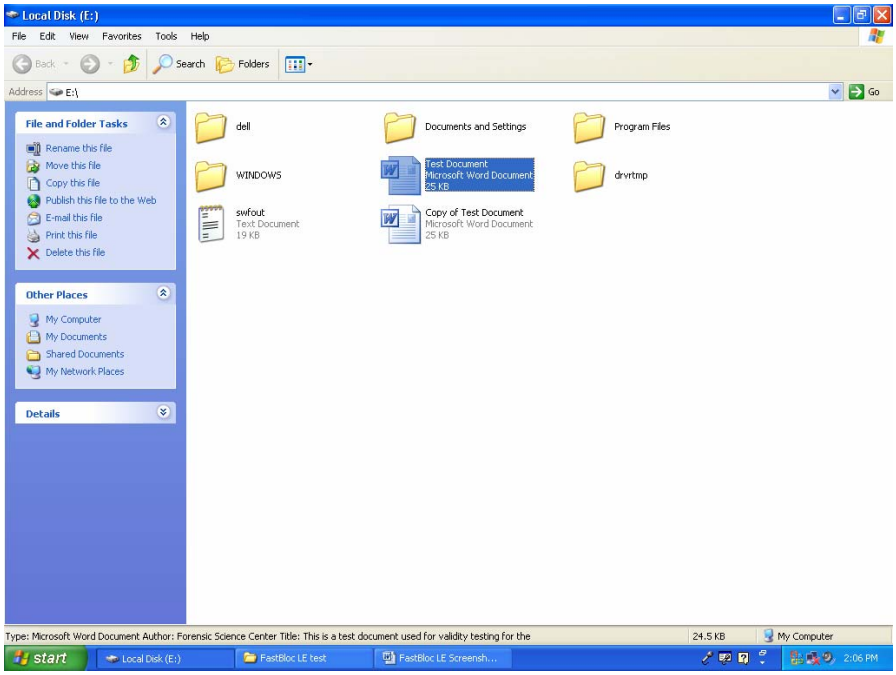


Figure 1.4 Write attempt operation performed on Seagate ® 18.6 GB hard disk attached to FastBloc® LE.



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

Figure 1.5 Structure of Seagate ® 18.6 GB hard disk drive after write attempt operation and rebooting of Windows XP.

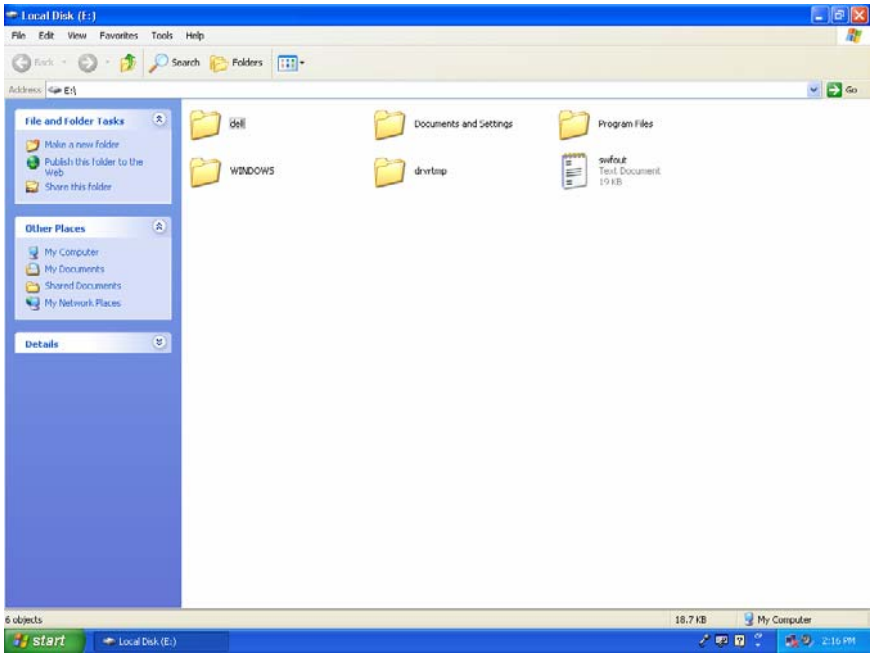


Figure 1.6 EnCase Forensic Edition v.5.04a hash statistics of Seagate 18.6 GB hard disk attached to FastBloc LE before a write attempt operation.