

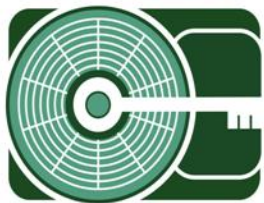
[MISDE]

September | 2006



Validation Testing of Guidance Software's FastBloc Field Edition (FE)

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.



TEST PLAN

Test Number: FastBlocFE-01
Test Title: Validation Testing of Guidance Software's FastBloc Field Edition (FE).
Test Date: 2/15/2006 to 2/17/2006

Purpose and Scope:

Guidance Software's FastBloc Field Edition (FE) is a hardware write-blocking device that enables the safe viewing and acquisition of subject media within a Windows environment. FastBloc FE is a USB/FireWire device that provides write-blocking capability to integrated drive electronics (IDE) enabled hard disk drives.

This test plan will test the ability of the FastBloc Field Edition (FE) to allow normal hard disk write-block operation to occur to source media. This test plan will evaluate two FastBloc FE devices and will consist of three test scenarios:

Requirements:

- 1) The FastBloc Field Edition (FE) should successfully compute an MD5 hash calculation of the source hard disk.
- 2) The FastBloc Field Edition (FE) should allow normal hard disk write-block operation to the source hard disk.
- 3) The FastBloc Field Edition (FE) should successfully compute an MD5 hash calculation that is consistent with the original MD5 hash calculation.

Description of Methodology:

The IDE enabled source disk will be attached to the FastBloc FE and an MD5 hash calculation will be performed using EnCase® v.5.04a for Windows. A write-operation will then be performed on the hard disk by attempting to add a file entitled "Test Document.doc" to the disk. The disk will then be powered down and restarted via the FastBloc FE to determine if the write operation was persistent. A subsequent MD5 hash calculation will be performed on the hard disk using EnCase v.5.04a for Windows.

The FastBloc FE must successfully protect the IDE hard disk from modification. In addition, the devices should allow for MD5 hash calculations to be performed, in this occurrence, using EnCase Forensic Edition Version .5.04a.

Expected Results:

- 1) The Guidance Software FastBloc FE will successfully calculate an MD5 hash value for the source IDE hard-disk.
- 2) The Guidance Software FastBloc FE write-block device will successfully prevent hard disk modification.



- 3) An MD5 hash performed on the source disk after the write attempt will match the original MD5 hash calculation of the source disk

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-01	Source Drive; FastBloc FE; EnCase v.5.04a	MD5 hash calculation performed on source drive	1	MD5 Hash calculation produced.
01-02	Source Drive; FastBloc FE; EnCase v.5.04a	Folder added to source drive; FastBloc powered down and restarted	2	No modification to protected hard disk
01-03	Source Drive; FastBloc FE; EnCase v.5.04a	MD5 hash calculation performed on source drive	3	MD5 Hash calculation produced.
01-04	N/A	Compare MD5 hash calculation values	3	MD5 calculation matches original MD5 hash calculated on drive.



Test Data Description:

Test Data Set:

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 FE (S/N 171479) MD5 hash value (before write attempt):

f2fe69015f701475863293a71ddda0d7

Guidance Software FastBloc FE (S/N 171479) MD5 hash value (after write attempt):

f2fe69015f701475863293a71ddda0d7

Guidance Software FastBloc FE (S/N 171483) MD5 hash value (before write attempt):

f2fe69015f701475863293a71ddda0d7

Guidance Software FastBloc FE (S/N 171483) MD5 hash value (after write attempt):

f2fe69015f701475863293a71ddda0d7



SUMMARY REPORT

Test Number: FastBlocFE-01
Test Title: Validation Testing of Guidance Software's FastBloc Field Edition (FE).
Test Date: 2/15/2006 to 2/17/2006

Test Description:

This test documents the ability of the FastBloc Field Edition (FE) 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 algorithm calculations.

Forensic Tool:

Title: FastBloc Field Edition (FE)
 Manufacturer: Guidance Software
 Model Number: F.G.-0501-000A
 Serial Number: 171479

Title: FastBloc Field Edition (FE)
 Manufacturer: Guidance Software
 Model Number: F.G.-0501-000A
 Serial Number: 171483

Test Results:

Test Number	Environment:	Actions:	Assigned Req't's	Expected Results:	Results:
01-01	Source Drive; FastBloc FE; EnCase v.5.04a for Windows	MD5 hash calculation performed on source drive	1	MD5 Hash calculation produced.	Pass
01-02	Source Drive; FastBloc FE; EnCase v.5.04a for Windows	Folder added to source drive. FastBloc powered down and restarted	2	No modification to protected hard disk	Pass
01-03	Source Drive; FastBloc FE; EnCase v.5.04a for Windows	MD5 hash calculation performed on source drive	3	MD5 Hash calculation produced.	Pass
01-04	N/A	Compare MD5 hash calculation values	3	MD5 calculation matches original MD5 hash calculated on drive.	Pass



Requirements:

- 1) The FastBloc Field Edition (FE) should successfully compute an MD5 hash calculation of the subject hard disk drive.
- 2) The FastBloc Field Edition (FE) should allow normal hard disk write-block operation to the subject hard drive.
- 3) The FastBloc Field Edition (FE) should successfully compute an MD5 hash calculation that is consistent with the original MD5 hash calculation.

Observations:

Hard disks can be hot-swapped in Windows only if the FastBloc FE unit is powered off before switching disks.

Limitations:

N/A

Recommendations:

N/A