[MISDE]

September | 2006

Validation Testing of the Logicube Serial-ATA (SATA) cloning adapter

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: SATA_adapter-01

Test Title: Validation Testing of the Logicube Serial-ATA (SATA) cloning adapter

Test Date: 1/26/2006

Purpose and Scope:

Test plan will test the validity of write-block and MD5 hash calculation of Serial ATA (SATA) hard drives using the Logicube serial ATA cloning adapter. The analysis will consist of five tests:

1) Hash calculation performed on SATA drive using the Logicube® Forensic MD5 with SATA cloning adapter attached.

2) MD5 Hash calculated in Encase Forensic Edition version 5.04a using the SATA adapter and the FastBloc® Field Edition (FE) write blocking device.

3) Write block capability verified with FastBloc® FE

4) MD5 Hash calculated in Encase 5.04a using SATA adapter and FastBloc® Laboratory Edition (LE) write blocking device.

5) Write block capability verified with FastBloc® LE.

Methodology:

SATA drive equipped with SATA cloning adapter will be attached to various write-blocking devices to test the validity and consistency of hash calculations.

Expected Results:

1) SATA drive equipped with adapter should consistently produce same MD5 calculation using various types of write-blocking hardware.
2) Write-block (FastBloc FE and LE) should block any modification made to SATA drive

Test Data Description:

Serial-ATA (SATA) Test Drive:
Maxtor Diamondmax 10
Model: 6B200HO
S/N: B41AV2BH
200GB SATA Hard Drive
Equipped w/ Logicube® SATA cloning adapter

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 Title: Hash Calculation using Logicube Forensic MD5 Device.

Test Date: 1/26/2006

Test Description:

This test procedure calculated the MD5 checksum of the Maxtor Diamondmax 200GB SATA with attached Logicube SATA cloning adapter. The Logicube Forensic MD5 Hard Drive Capture system, configured to Hardware MD5 setting, was used to perform calculation.

Test Result:

PASSED. A successful MD5 checksum was calculated and reported by the device.

Forensic Tools:

Logicube Forensic MD5 Capturing Device
Logicube SATA Cloning Adapter

Test Notes:

The SATA drive (with attached SATA cloning adapter) was attached to the Logicube MD5 capturing device in the source drive position. A MD5 computation was successfully executed and yielded the following results:

MD5sum: F2B1C86D14BFB584328EFEAE476BEB15
Cylinders: 395136
Heads: 16
Sectors: 63
Total Sectors: 3982970888
Drive Size 189.9 GB
Total # of Sectors: 398,297,087

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 Title: Hash calculation in Encase 5.04a using SATA adapter and FastBloc Field Edition (FE) write blocking device.

Test Date: 1/26/2006

Test Description:

This test procedure calculated the MD5 checksum of the Maxtor Diamondmax 200GB SATA with attached Logicube SATA cloning adapter. Guidance Software's FastBloc FE was used in conjunction with Encase 5.04 to attempt an MD5 computation which matched that of the Logicube MD5 calculation

Test Result:

PASSED. A successful MD5 checksum was calculated and matched the calculation of the previous Logicube MD5.

Forensic Tools:

Encase Forensic v.5.04a
Guidance Software FastBloc FE write-blocker
Logicube SATA Cloning Adapter

Test Notes:

The SATA drive was attached to the FastBloc FE via the SATA adapter. An MD5 hash operation was performed on the hard disk drive using Encase Forensic 5.04a. A MD5 computation was successfully executed and yielded the following results:

MD5sum: F2B1C86D14BFB584328EFEAE476BEB15
Start: 1/26/06 11:28:33
Stop: 1/26/06 14:18:59
Time: 2:50:26
Start Sector: 0
Stop Sector: 398297087
Drive Size 189.9 GB

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 Title: Write Block verification using SATA adapter and FastBloc Field Edition (FE) write blocking device.

Test Date: 1/27/2006

Test Description:

This test procedure determined if write-blocking capability existed when using the SATA cloning adapter in conjunction with the FastBloc FE write blocker. A file folder (see figure 1.1) labeled “SATA write protection test” was placed onto the write-blocked local disk. A power-down of the suspect drive and the write-blocking device was performed, and then restarted.

Test Result:

PASSED. The folder was no longer visible on the write-blocked drive (see figure 1.2).

Forensic Tools:

Guidance Software FastBloc FE write-block device
Logicube SATA Cloning Adapter

Test Notes:

The disk cache of Microsoft Windows XP retained the file folder within the write-blocked drive, making it seem as if write-blocking were not present. However, a power down and power up of the FastBloc write blocker verified that the only viewable alteration to the drive was the disappearance of the test folder.

A system shutdown was not necessary to wipe the file folder from the write-blocked drive. Since FastBloc FE is a USB device; Windows XP automatically demounted and remounted the drive, thereby clearing the cache.

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

SUMMARY REPORT

Test Title: Hash calculation in Encase 5.04a using SATA adapter and FastBloc Laboratory Edition (LE) write blocking device.

Test Date: 1/27/2006

Test Description:

This test procedure calculated the MD5 checksum of the Maxtor Diamondmax 200GB SATA with attached Logicube SATA cloning adapter. Guidance Software's FastBloc LE was used in conjunction with Encase 5.04a to attempt an MD5 computation which matched that of the Logicube MD5 calculation.

Test Result:

PASSED. A successful MD5 checksum was calculated and matched the calculation from the previous Logicube MD5.

Forensic Tools:

Encase Forensic v.5.04a
Guidance Software FastBloc FE write-block device
Logicube SATA Cloning Adapter

Test Notes:

The SATA drive with attached SATA cloning adapter was attached to the FastBloc LE. Encase 5.04 was then opened and the hash option was selected from the EDIT menu. A MD5 computation was successfully executed and yielded the following results:

MD5sum: F2B1C86D14BFB584328EFEAE476BEB15
Start: 1/27/06 9:00:58
Stop: 1/27/06 14:01:42
Time: 5:00:44
Stop Sector: 398297087
Drive Size 189.9 GB

** It is also imperative to notate the time difference between the FastBloc devices. The FE hashed the drive in a total time of 2:50:26 while the LE hashed the same drive at a much slower rate of 5:00:44.*

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

SUMMARY REPORT

Test Title: Write Block verification using SATA adapter and FastBloc Laboratory Edition (LE) write blocking device.

Test Date: 1/27/2006

Test Description:

This test procedure determined if write-blocking capability existed when using the SATA cloning adapter in conjunction with the FastBloc LE write blocker. A file folder (see figure 2.1) labeled "SATA write protection test (FastBloc LE)" was placed onto the write-blocked local disk. A shutdown/restart of Windows XP was performed and restarted. The write-blocked drive was viewed again upon restart.

Test Result:

PASSED. The folder was no longer visible on the write-blocked drive (see figure 2.2).

Forensic Tools:

Guidance Software FastBloc Laboratory Edition (LE) write-block device
Logicube SATA Cloning Adapter

Test Notes:

The disk cache of Microsoft Windows XP retained the file folder within the write-blocked drive, making it seem as if write-blocking were not present. However, a shutdown of Windows XP was performed and restarted. Upon restart, the write-blocked drive was viewed again. There was no indication of the written folder, which infers that the drive is write-blocked.

Unlike the FastBloc FE write-block device, system shutdown was necessary to wipe the file folder from the write-blocked drive. This is because Fastbloc LE is mounted on the motherboard's secondary IDE channel and does not unmount itself when the unit is powered down. Although attempts to refresh indicate that the drive could be written to (as items did not disappear), a shutdown/startup of Windows will successfully clean the cache and verify the write-blocker in conjunction with the SATA cloning adapter.

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

Figure 1.1 File Folder entitled “SATA write protection test” added to Maxtor drive attached to FastBloc FE & Logicube SATA adapter

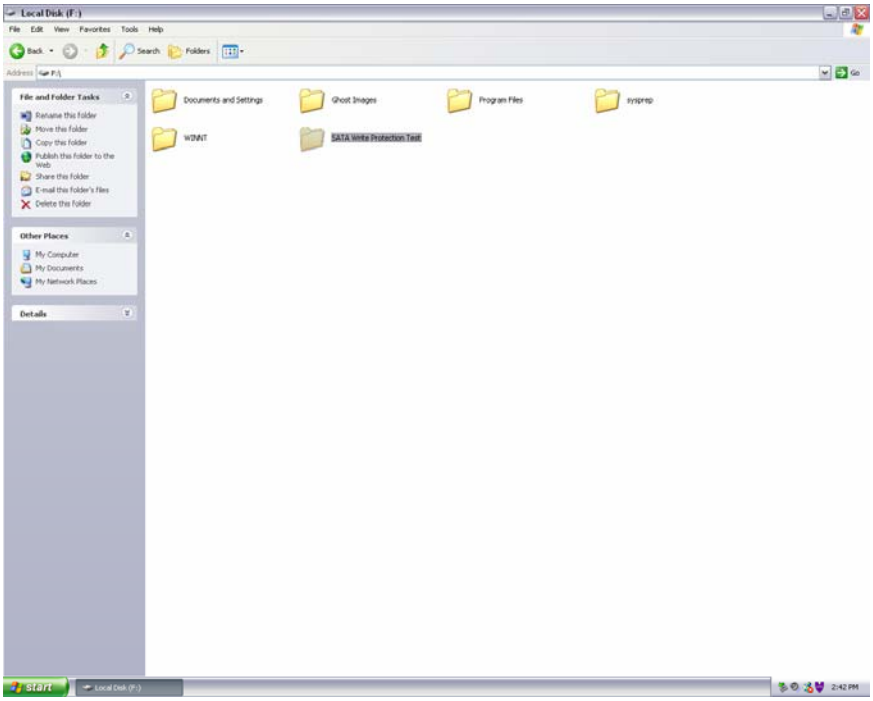
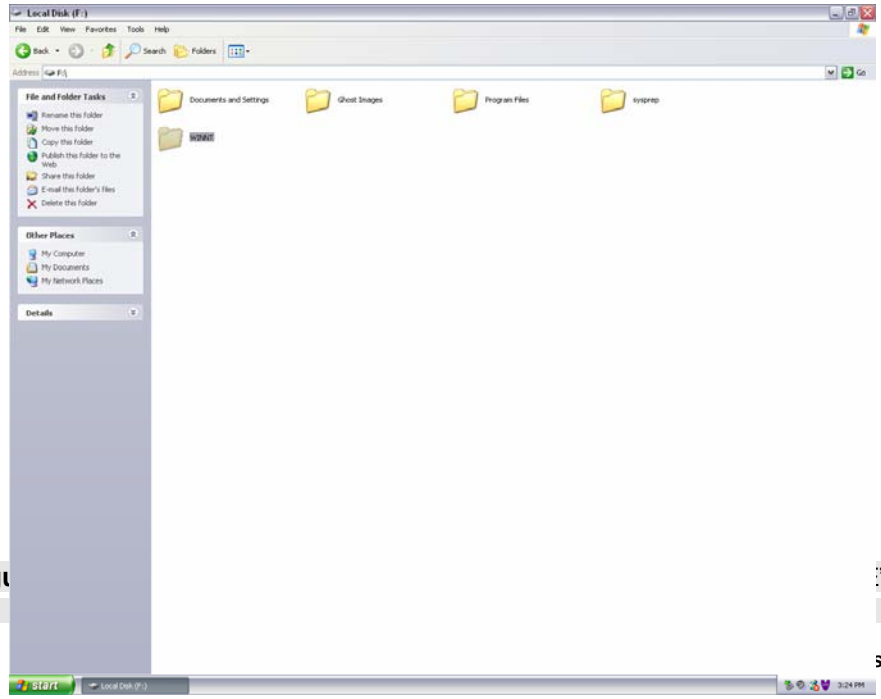


Figure 1.2 File folder cleaned from cache after unmounting and mounting of same drive



Figu :” to

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

SATA drive attached to FastBloc LE & Logicube SATA adapter

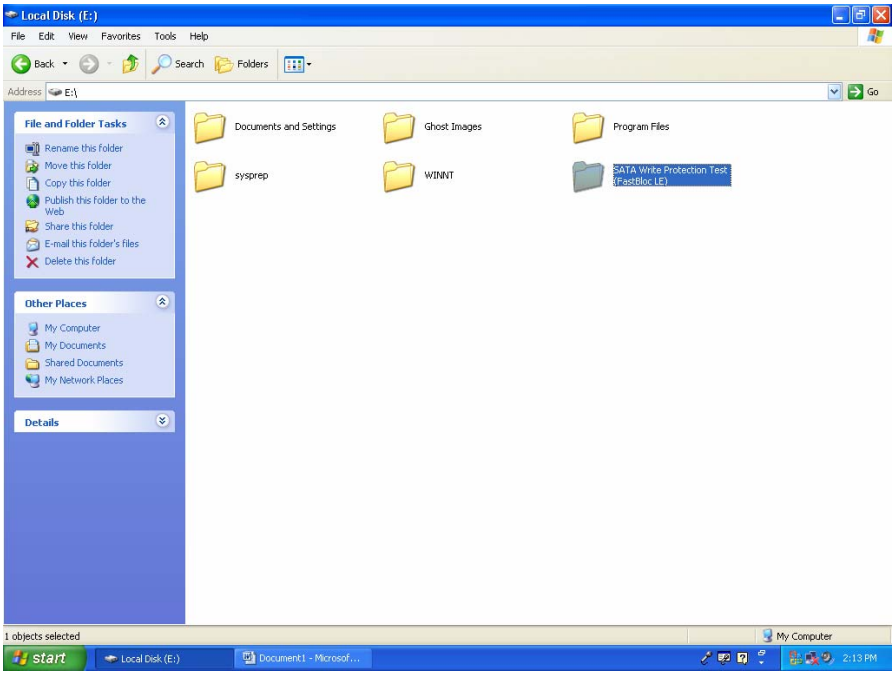


Figure 2.2 File folder cleaned from cache after rebooting of computer and mounting of same drive