[MISDE]

September | 2006

Verification of the Functionality of the X-Late HardCopy ATA Hard Drive Data Capture Unit

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: HardCopyATA-01

Test Title: Verification of the Functionality of the X-Late HardCopy ATA Hard Drive Data Capture Unit

Test Date: 2/3/2006 to 2/7/2006

Purpose and Scope:

In addition to the Logicube Forensic MD5 Forensic Capturing System, the MISDE Laboratory possesses the X-Late HardCopy ATA Hard Drive Capturing System, which allows direct capture of ATA enabled hard disk drives.

This test plan will test the ability of the HardCopy ATA Hard Drive Data Capture Unit to effectively perform all of the commands and operations supported by the device.

Requirements:

1) The HardCopy ATA Hard Drive Data Capture Unit should allow for normal message digest (MD5) checksum operation to occur for the source drive.

2) The MD5 checksum of the source drive will be verified by comparing calculated MD5 hashes of the same drive using the Logicube® Forensic MD5 Capturing System

3) The HardCopy ATA Hard Drive Data Capture Unit should allow normal MD5 checksum operation to be calculated for the destination drive.

4) The MD5 checksum of the destination drive will be verified by comparing calculated MD5 hashes of the same drive by the Logicube Forensic MD5 Capturing System.

5) The HardCopy ATA Hard Drive Data Capture Unit should allow normal write-blocked cloning of the source drive to the destination disk.

6) The HardCopy ATA Hard Drive Data Capture Unit should allow a complete forensic wipe of the destination disk.

7) The HardCopy ATA Hard Drive Data Capture Unit should allow the destination disk to be formatted with a FAT-32 file system.

8) The HardCopy ATA Hard Drive Data Capture Unit should allow a binary (.BIN) image of the source disk to be written to the destination drive.

9) An MD5 calculation performed on the destination disk after an image is completed should match the MD5 checksum of the source disk.

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

Description of Methodology:

The suspect/source disk will be attached to the X-Line HardCopy™ Hard Drive Data Capture Unit in the READ ONLY SUSPECT DRIVE parallel ATA connection. The destination disk will then be connected to the HardCopy Data Capture Unit in the WRITE TO DESTINATION DRIVE connection. The unit will be controlled through the serial interface option within Windows XP for all proceeding operations, although serial connection is not necessary to execute commands for the device.

The HardCopy ATA Hard Drive Capturing Unit will then compute an MD5 hash of the source disk. Upon completion of the MD5 hash calculation, the source disk will be removed and a second MD5 hash will be calculated using the Logicube Forensic MD5 Capturing System to determine if the hash values are consistent.

A subsequent MD5 hash calculation will then be performed on the destination disk using the HardCopy Data Capturing Unit. Upon completion of the MD5 hash calculation, the disk drive will be removed and verification will occur with a second calculation of the destination disk using the Logicube Forensic MD5 Capturing System.

The source and destination disks will then be connected to HardCopy Capturing Device and the clone operation command will be executed. The destination disk will then be removed and viewed using Guidance Software's EnCase® Forensic Edition version 5.04a via FastBloc Field Edition (FE) to determine if the source disk was successfully cloned.

The destination disk will then be re-attached to the HardCopy Data Capture Unit and a wipe command will be executed. Upon completion of the wipe, the destination disk will be removed and viewed in EnCase Forensic Edition version 5.04a via FastBloc FE to determine if the all data from the destination disk was successfully wiped.

The destination disk will then be attached to the HardCopy Data Capture Unit and a format drive command will be executed. The disk will then be removed and viewed in EnCase Forensic Edition version 5.04a via FastBloc FE to determine if the device successfully formatted a FAT-32 file system to the destination drive.

The destination disk will then be connected to the HardCopy Data Capturing Unit and the image drive command will be executed. Upon completion of the image, the destination disk will be removed from the Hardcopy unit and viewed in EnCase Forensic Edition version 5.04a via FastBloc FE to determine if the image was successfully written to the destination disk. The destination disk will then be attached to the HardCopy Data Capturing Unit and a subsequent MD5 hash algorithm calculation will be executed to determine if the MD5 checksum of the destination disk matches that of the cloned/imaged source disk.

Expected Results:

1) The HardCopy ATA Hard Drive Capturing Unit will allow an MD5 checksum to be calculated for the source disk.

2) The HardCopy ATA Hard Drive Capturing Unit will allow an MD5 checksum to be calculated for the destination disk.

3) The MD5 hash calculations of the source and destination disks calculated by the HardCopy ATA Hard Drive Capturing Unit will match those produced by the Logicube Forensic MD5 Capturing System.

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

4) The HardCopy Capturing Unit will successfully clone the source disk onto the destination disk.

5) The HardCopy Data Capture Unit will successfully wipe all data from the destination disk.

6) The HardCopy Data Capture Unit will successfully format the destination disk with a FAT-32 file system.

7) The HardCopy Data Capture Unit's image function will allow a successful binary image (.BIN) to be written to the destination drive.

8) An MD5 calculation performed on the destination disk after successful clone/image should match that of the source disk.

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-01	Source Drive; HardCopy Data Capture Unit	MD5 hash calculation of the source drive	1	Successful MD5 calculation will be produced by device.
01-02	Source Drive; Logicube Forensic MD5 Capturing System	MD5 hash calculation of the source drive	2	MD5 calculation will match that of the HardCopy Data Capture Unit.
01-03	Destination Drive; HardCopy Data Capture Unit	MD5 hash calculation of destination drive	3	Successful MD5 calculation will be produced by device.
01-04	Destination Drive; Logicube Forensic MD5 Capturing System	MD5 hash calculation of destination drive	4	MD5 calculation will match that of the HardCopy Data Capture Unit.
01-05	Source Drive; Destination Drive; HardCopy Data Capture Unit	Source drive cloned to destination drive	5	Source drive will successfully be cloned to destination drive.
01-06	Destination Drive; FastBloc FE; Encase v.5.04a	Destination drive structure viewed in Encase v.5.04a	5	Clone of source drive will be visible on destination drive.
01-07	Destination Drive; HardCopy Data Capture Unit	Wipe of destination drive	6	Destination drive will successfully be wiped.
01-08	Destination Drive; FastBloc FE; Encase v.5.04a	Destination drive structure viewed in Encase v.5.04a	6	No data will be visible on destination drive. Only unused disk space will appear.
01-09	Destination Drive; HardCopy Data Capture Unit	Destination drive formatted using HardCopy Data Capture Unit	7	The destination drive will be successfully formatted.
01-10	Destination Drive; FastBloc FE; Encase	Destination drive structure viewed	7	The HardCopy formatted file system

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

	v.5.04a	in Encase v.5.04a		will be visible on the destination drive.
01-11	Source Drive; Destination Drive; FastBloc FE; Encase v.5.04a	Source drive imaged to destination drive	8	A successful image will be copied from the source to the destination drive.
01-12	Destination Drive; FastBloc FE; Encase v.5.04a	Destination drive structure viewed in Encase v.5.04a	8	Copied binary image file will be visible on destination drive.
01-13	Destination Disk; HardCopy Data Capture unit	MD5 hash calculation performed on destination disk	9	MD5 calculation of cloned/imaged destination disk will match that of the source disk.

Test Data Description:

Test Data Set:

Source:
Western Digital WD204
Model: WDC WD204BB)
Capacity: 20.4 GB
S/N: WMA4J1088649

MD5 hash values
Logicube Forensic MD5 hash value: 1015b34a41582bf0b760e8d3d3582bf1
HardCopy Data Capture Unit hash value: 1015b34a41582bf0b760e8d3d3582bf1

Destination:
Maxtor Diamondmax Plus 9
Model: 6Y120PO
Capacity: 120 GB ATA
S/N: Y327XZME

MD5 hash values (performed after image function execution)
Logicube Forensic MD5 hash value: d20d385e80e5e94da28582858d4ad218
HardCopy Data Capture Unit hash value: d20d385e80e5e94da28582858d4ad218

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: HardCopyATA-01

Test Title: Verification of the Functionality of the X-Late HardCopy ATA Hard Drive Data Capture Unit

Test Date: 2/3/2006 to 2/7/2006

Test Description:

This test documents the results of the functionality of the X-Late HardCopy ATA Hard Drive Data Capture Unit. The analysis consists of twelve test scenarios:

Forensic Tool:

Title: HardCopy™ ATA Hard Drive Data Capture Unit
Manufacturer: X-late Inc.
Version: 2.3B

Test Results:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:	Results:
01-01	Source Drive; HardCopy Data Capture Unit	MD5 hash calculation of suspect/source drive	1	Successful MD5 calculation will be produced by device	Pass
01-02	Suspect Drive; Logicube Forensic MD5 Capturing System	MD5 hash calculation of suspect/source drive	2	MD5 calculation will match that of the HardCopy Data Capture Unit	Pass
01-03	Destination Drive; HardCopy Data Capture Unit	MD5 hash calculation of destination drive	3	Successful MD5 calculation produced by device	Pass
01-04	Destination Drive; Logicube Forensic MD5 Capturing System	MD5 hash calculation of destination drive	4	MD5 calculation will match that of the HardCopy Data Capture Unit	Pass
01-05	Source Drive; Destination Drive; HardCopy Data Capture Unit	Source drive cloned to destination drive	5	Source drive will successfully be cloned to destination drive	Pass
01-06	Destination Drive; FastBloc FE; Encase v.5.04a for Windows	Destination drive structure viewed in Encase v.5.04a	5	Clone of source drive will be visible on destination drive	Pass
01-07	Destination Drive; HardCopy Data Capture Unit	Wipe of destination drive	6	Destination drive will successfully be wiped.	Pass

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

01-08	Destination Drive; FastBloc FE; Encase v.5.04a for Windows	Destination drive structure viewed in Encase v.5.04a	6	No data will be visible on destination drive. Only unused disk space will appear	Pass
01-09	Destination Drive; HardCopy Data Capture Unit	Destination drive formatted using HardCopy Data Capture Unit	7	The destination drive will be successfully formatted	Pass
01-10	Destination Drive; FastBloc FE; EnCase v.5.04a	Destination drive structure viewed in Encase v.5.04a	7	The HardCopy formatted file system will be visible on the destination drive	Pass
01-11	Source Drive; Destination Drive; HardCopy Data Capture unit	Source drive imaged to destination drive	8	A successful image will be copied from the source to the destination drive	Pass
01-12	Destination Drive; FastBloc FE; EnCase v.5.04a for Windows	Destination drive structure viewed in Encase v.5.04a	8	Copied binary image image file will be visible on destination drive	Pass
01-12	Destination Drive; HardCopy Data Capture Unit	MD5 hash calculation performed on destination drive	9	MD5 calculation will match that of source disk	**Fail* (see limitations 1:2)*

Requirements:

1) The HardCopy ATA Hard Drive Data Capture Unit should allow for normal MD5 checksum operation to occur for the source drive.

2) The MD5 checksum of the source drive will be verified by comparing calculated MD5 hashes of the same drive using the Logicube® Forensic MD5 Capturing System

3) The HardCopy ATA Hard Drive Data Capture Unit should allow normal MD5 checksum operation to be calculated for the destination drive.

4) The MD5 checksum of the destination drive will be verified by comparing calculated MD5 hashes of the same drive by the Logicube Forensic MD5 Capturing System.

5) The HardCopy ATA Hard Drive Data Capture Unit should allow normal write-blocked cloning of the source drive to the destination drive.

6) The HardCopy ATA Hard Drive Data Capture Unit should allow a complete forensic wipe of the destination drive.

7) The HardCopy ATA Hard Drive Data Capture Unit should allow the destination disk to be formatted with a FAT-32 file system.

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

8) The HardCopy ATA Hard Drive Data Capture Unit should allow a binary (.BIN) image of the source drive to be written to the destination drive.

9) An MD5 calculation performed on the destination disk after an image is completed should match the MD5 checksum of the source disk.

Observations:

N/A

Limitations:

1) When copying a source hard drive in Image mode, the files stored on the destination drive are written in binary format (.BIN). Because of this, the file structure of the source drive cannot be observed, only a raw data file (see figure 1.2).

2) It was discovered upon completion of a clone operation, the MD5 checksum of the destination disk differed from that of the source disk. (see test scenario 01-12). This is because the destination disk was much larger (120 GB) than the source disk (20.4 GB).

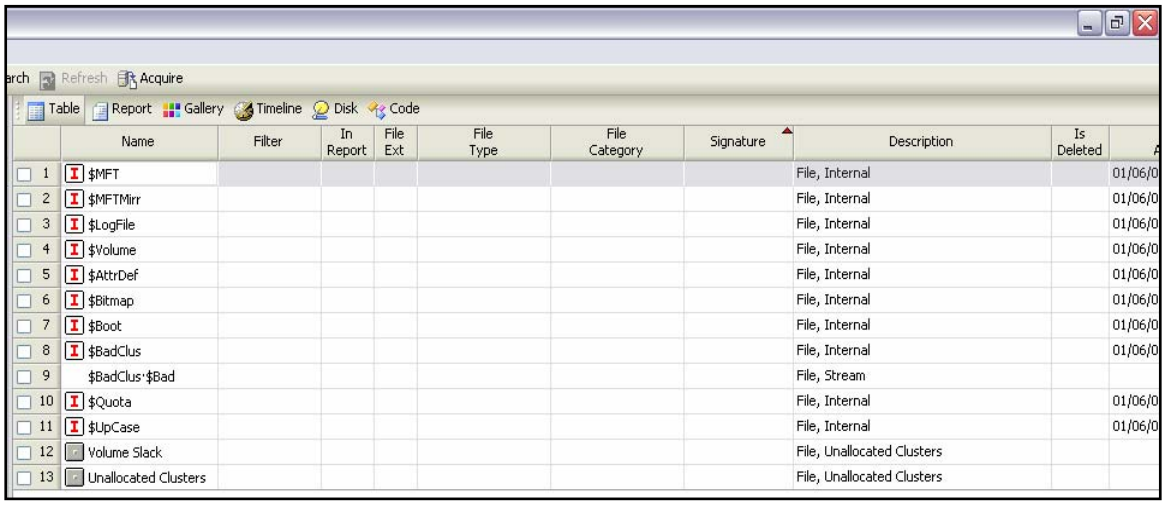
Recommendations:

1) To convert the binary (.BIN) file created from image mode, it is recommended to use a software extraction program such as IsoBuster v.1.9, which will extract the single .BIN file into a viewable file structure.

2) When performing an MD5 checksum on the destination disk after a clone or image, it is recommended to utilize the device's [blks] command, which allows the investigator to specify the specific number of sectors to be calculated.

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

Figure 1.1 File structure of formatted destination drive



	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	
1	$MFT							File, Internal		01/06/0
2	$MFTMirr							File, Internal		01/06/0
3	$LogFile							File, Internal		01/06/0
4	$Volume							File, Internal		01/06/0
5	$AttrDef							File, Internal		01/06/0
6	$Bitmap							File, Internal		01/06/0
7	$Boot							File, Internal		01/06/0
8	$BadClus							File, Internal		01/06/0
9	$BadClus:$Bad							File, Stream		
10	$Quota							File, Internal		01/06/0
11	$UpCase							File, Internal		01/06/0
12	Volume Slack							File, Unallocated Clusters		
13	Unallocated Clusters							File, Unallocated Clusters		

Figure 1.2 .BIN image file from image capture