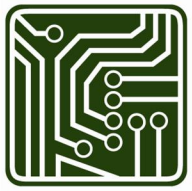
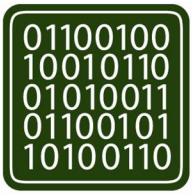
[MISDE]

January 2006





Sending Multiple dd Image Captures to a Single Hard Drive Using the Logicube Forensic MD5

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.

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

TEST PLAN

Test Number: Logicube_dd-01

Test Title: Sending multiple dd Image Captures to a Single Hard Disk Using Logicube Forensic MD5 Capturing System.

Test Date: 6/22/2006

Purpose and Scope:

Because of the increased amounts of data being seized from suspect computers, it is sometimes difficult for the investigator to dedicate a single cloned hard drive for every computer seized in an investigation. Moreover, storage capacity in recent years has improved tremendously, creating a problem for departments and organizations that do not have large amounts of data storage capacity available in the laboratory. This problem is further augmented by budget constraints, which requires investigators to fully use the storage that is readily available.

The Logicube Forensic MD5 data capturing system features an option known as dd image capture mode. DD mode is a Unix/Linux derived function allowing the investigator to capture a source hard drive to multiple viewable image files. The investigator can specify data from the source drive to be divided into file sizes of 650 MB, 2 GB, and 4 GB. This function was developed to allow archiving onto CD-R / R/W and DVD-R / R/W; however these files can also be stored to a single destination hard drive.

This test plan will determine if the dd image function of the Logicube Forensic MD5 will allow multiple hard disk images to be stored to a single destination disk. The analysis consists of four test scenarios:

Requirements:

1) The Logicube Forensic MD5 Capturing System in dd capture mode should allow normal capturing to occur from the destination hard disk.

2) The file structure of the first dd capture should allow files to be viewed using Encase® v.5.04a for Windows.

3) The Logicube Forensic MD5 Capturing System should allow normal capturing of a second dd Image to the destination hard disk without overwriting the first image.

4) The file structure of the dd capture should reveal multiple dd-based image files when viewed in EnCase Forensic Edition Version 5.04a for Windows

Description of Methodology:

The source disk will be connected to the Logicube Forensic MD5 data capturing system in the source position. The destination disk will be connected to the Logicube Forensic MD5 capturing system in the destination position. A 4 gigabyte (GB) dd capture will then be executed.

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

The destination drive will then be connected to the Guidance Software FastBloc FE write-block device and will be viewed using EnCase Forensic Edition Version 5.04a with Windows XP Professional SP2. The disk contents will be noted and the destination disk will be disconnected from the FastBloc device.

The destination disk will then be reattached to the Logicube Forensic MD5 capturing system in the destination position and a second 4 GB dd capture will then be performed. The destination drive will again be attached to the Guidance Software FastBloc FE write-block device and will be viewed using EnCase 5.04a for Windows. The disk contents will be viewed to determine whether the files associated with the first dd capture were overwritten or the files associated with the second dd capture were added to the destination drive.

The dd function of the Logicube Forensic MD5 must successfully write file sets in two separate and distinct capturing sessions onto one destination hard disk drive. These file sets should be able to be visible within Micorsoft Windows XP.

Expected Results:

1) The Logicube Forensic MD5 data capturing system will successfully perform a 4 GB dd Capture of the source hard disk to the destination disk.

2) The dd capture will successfully be viewed using the FastBloc FE write-block device and EnCase v.5.04a for windows.

3) The Logicube Forensic MD5 data capturing system will successfully perform a second 4 GB dd capture of the source drive to the destination disk.

4) The second dd capture, when viewed in EnCase v.5.04a for Windows should confirm two distinct hard disk drive captures contained within the same destination disk.

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

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-01	Source Drive, Destination Drive, Logicube Forensic MD5 in 4 GB dd Capture Setting	Complete Image of suspect/source drive to destination drive	1	Complete image copied to destination drive in 4 GB subfolders
01-02	Destination Drive; FastBloc FE, Encase v.5.04a	Destination drive structure viewed in Encase v.5.04a	2	Copied 4 GB subfolders (20.4 GB total) within destination drive are able to be recognized and viewed
01-03	Source Drive, Destination Drive, Logicube Forensic MD5 in 4 GB dd Capture Setting	2nd Image of suspect/source drive to destination drive	3	2nd dd image will be written to destination drive without overwriting of 1st dd capture
01-04	Destination Drive; FastBloc FE, Encase v.5.04a	Destination drive structure viewed in Encase v.5.04a	4	No modification to original capture; Two distinct captures able to be recognized

Test Data Description:

Test Data Set:

Western Digital WD204
Model WDC WD204BB (ATA)
MD5sum: 1015b34a41582bf0b760e8d3d3582bf1

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

SUMMARY REPORT

Test Number: Logicube_dd-01

Test Title: Validity Testing of Multiple dd Image Captures to a Hard Disk Using the Logicube Forensic MD5 Capturing System.

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

Test Description:

This test documents the ability of the Logicube Forensic MD5 capturing system to capture multiple source drives to a single destination drive using the system's dd capture mode. The analysis consists of four test scenarios:

Forensic Tool:

Title: Forensic MD5 Capturing System
Manufacturer: Logicube ®
Version: Firmware Version.6.0

Test Results:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:	Results:
01-01	Source Drive; Destination Drive; Logicube Forensic MD5 in 4 GB dd Capture Setting	Complete Image of suspect/source drive to destination drive	1	Complete image copied to destination drive in 4 GB subfolders	Pass
01-02	Destination Drive; FastBloc FE, Encase Forensic v.5.04a	Destination drive structure viewed in Encase v.5.04a	2	Copied 4 GB subfolders (20.4 GB total) within destination drive are able to be recognized and viewed	Pass
01-03	Source Drive; Destination Drive; Logicube Forensic MD5 in 4 GB dd Capture Setting	2nd Image of suspect/source drive to destination drive	3	2nd dd image will be written to destination drive without overwriting of 1st dd capture	Pass
01-04	Destination Drive; FastBloc FE; Encase Forensic v.5.04a	Destination drive structure viewed in Encase v.5.04a	4	No modification to original capture; Two distinct captures able to be recognized	Pass

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

Requirements:

1) The Logicube Forensic MD5 Capturing System should allow normal capturing to occur to the source hard drive in dd capture mode.

2) The file structure of the first dd capture should allow files to be viewed using Encase v.5.04a for Windows.

3) The Logicube Forensic MD5 Capturing System should allow normal capturing of a second dd Image to the source hard drive without overwriting the first image.

4) The file structure of the dd capture should reveal multiple DD image files when viewed in Encase v.5.04a for Windows.

Observations:

Upon capture each dd image, the Logicube Forensic MD5 automatically labeled folders on the destination drive as DDCAPTUR for the first image and DDCAPTU for the second image (see figures 2.1, 2.2).

In addition to copying image captures, the Logicube Forensic MD5 also copied a log file into each capture folder (see figure 1.2).

Limitations:

Upon capture of the 1st and 2nd image, a hash calculation was performed for each subfolder in the DDCAPTUR and DDCAPTU folder rather than an MD5 hash of the total drive. This is because the default setting on the Logicube Forensic MD5 in dd capture mode is for an MD5-FILE to be executed, which calculates MD5 hashes for each subfolder copied to the destination.

Recommendations:

To remedy this issue, the setting can be HWCRC32, which will calculate the entire destination drive, or MD5-DISK which will calculate only the entire dd image folder being copied.

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 File structure of destination disk after the first dd capture viewed within EnCase 5.04a

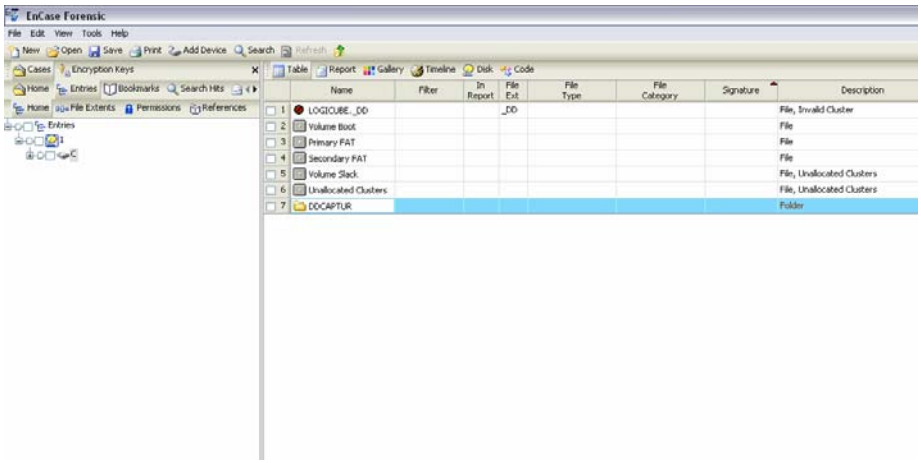
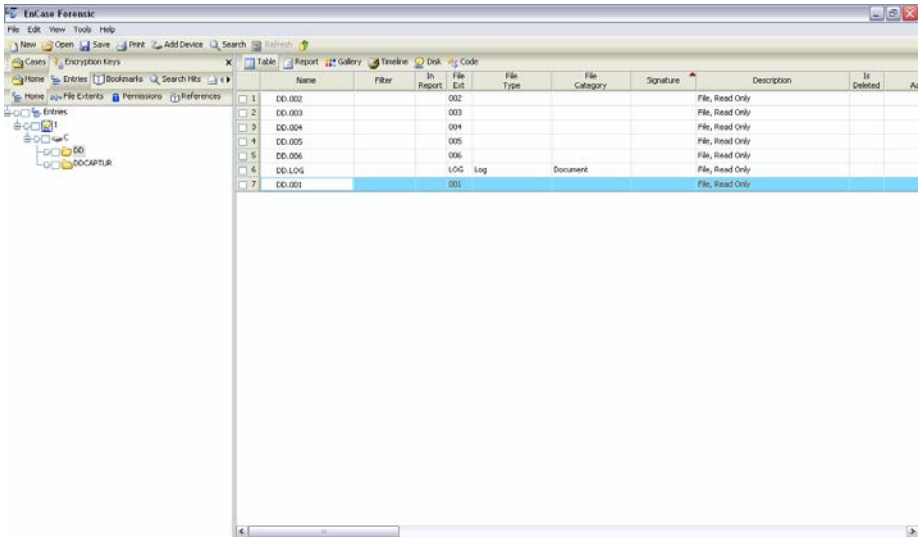


Figure 1.2 Contents of 1st dd Capture file folder.



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 1.3 File details for the files created on the destination disk by the Logicube Forensic MD5 Capturing System

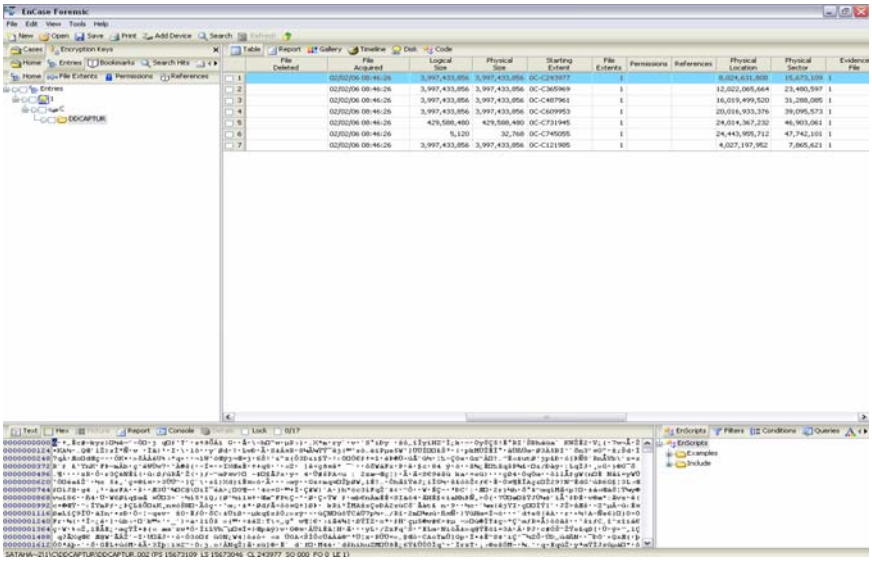
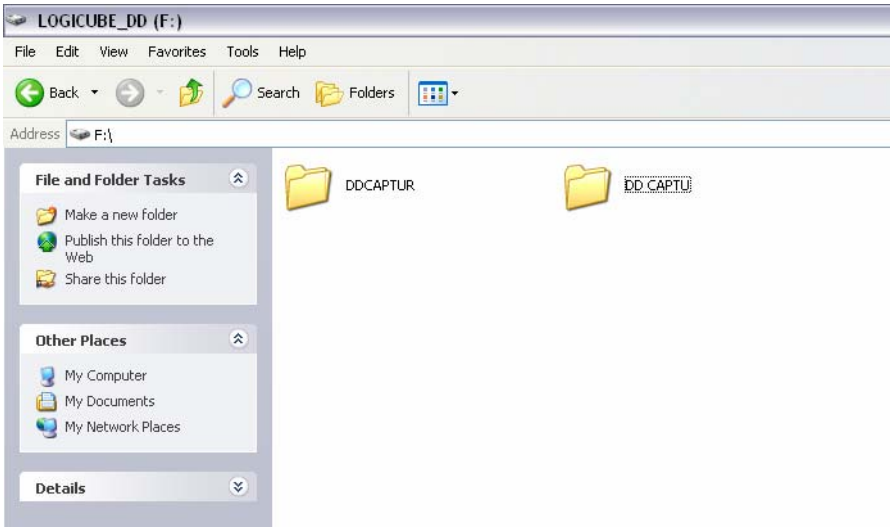


Figure 2.1 File structure of the destination disk after the second dd capture viewed in Windows Explorer.



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 2.2 Contents of the DDCAPTU (2nd dd capture) folder viewed in Windows Explorer.

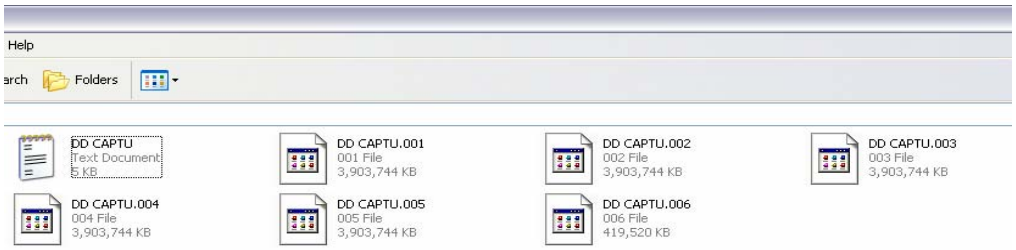
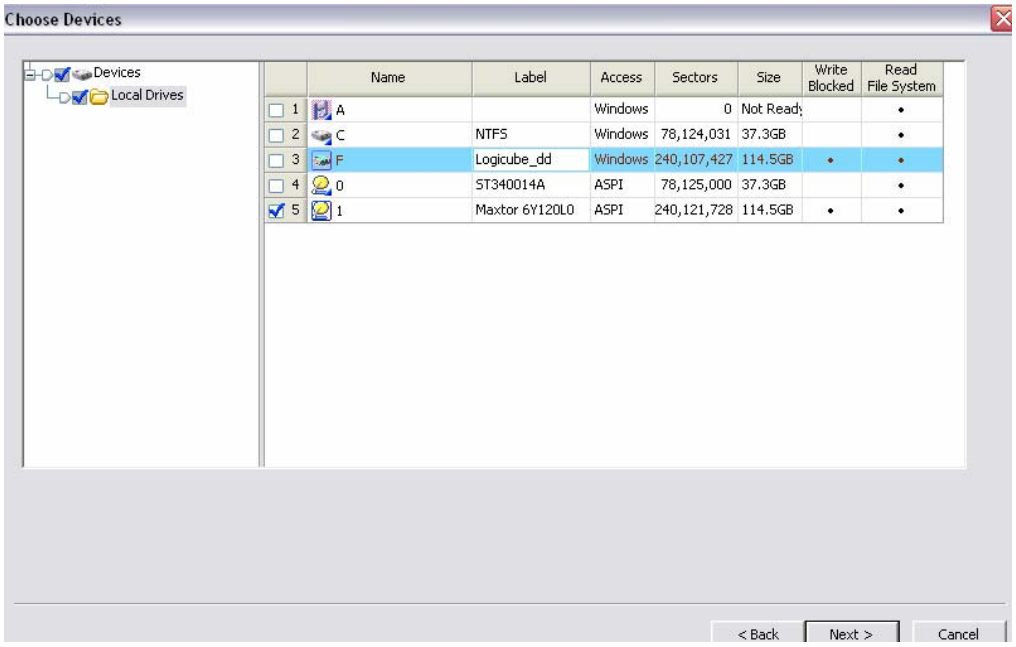


Figure 2.3 Label name automatically assigned to the dd capture destination disk by the Logicube Forensic MD5 (viewed in EnCase v.5.04a).



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