[MISDE]

September | 2006

Functionality Test of the Logicube® Forensic Talon Capturing System

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: TALON-01

Test Title: Functionality Test of the Logicube® Forensic Talon Capturing System

Test Date: 5/19/2006

Purpose and Scope:

The Logicube Forensic Talon Capturing Device is a drive-to-drive duplication device that allows the contents of a source (suspect) drive to be accurately copied over to a destination drive, while causing no alteration to the original evidence. The successor of the Forensic MD5 device, the Talon is capable of acquisition speeds of up to 4 GB per minute.

This test plan will test the ability of the Logicube Forensic Talon Capturing Device to accurately & effectively perform all of the operations and commands supported by the device.

Requirements:

1) The Logicube Forensic Talon should successfully perform a secure hash algorithm calculation (SHA-256) on a parallel-ATA (PATA) hard disk drive.

2) The Logicube Forensic Talon should successfully perform a secure hash algorithm calculation (SHA-256) on a serial-ATA (SATA) hard disk drive.

3) The Logicube Forensic Talon should successfully perform a PATA to PATA native drive capture/duplication.

4) The Logicube Forensic Talon should successfully perform a SATA to SATA drive capture/duplication.

5) The Logicube Forensic Talon should successfully perform a SATA to PATA (or vice-versa) drive capture/duplication.

6) The Logicube Forensic Talon should successfully perform a 650 MB dd-style image file capture of a source/suspect hard disk drive.

7) The Logicube Forensic Talon (engaged in USB mode) should successfully perform a capture of a hard disk drive via the integral USB port.

8) The Logicube Forensic Talon should successfully perform a binary keyword search on a PATA-enabled hard disk drive in the source position.

9) The Logicube Forensic Talon should successfully perform a wipeclean function on a PATA-enabled hard disk drive in the destination position.

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

10) The Logicube Forensic Talon should successfully verify the authenticity of a report stored on the CompactFlash card using the audit trail function.

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

Description of Methodology:

An 18.6 GB parallel-ATA (PATA) hard disk drive will be attached to the Logicube Forensic Talon in the source position (see figure 2.1). A secure hash algorithm (SHA) 256 calculation will be performed on the source disk using the SHA-256 function of the Talon. Upon completion of the calculation, a 160 GB zero-wiped PATA disk will be attached to the Talon in the destination position. A native capture will be executed from the PATA source to the PATA destination disk. Upon completion of the PATA disk capture, a 200 GB (18.6 GB HPA) serial-ATA (SATA) hard disk will be attached to the Talon in the source position. A SHA-256 calculation will then be performed on the disk. Upon conclusion of the calculation, a zero-wiped SATA disk will be attached to the Talon in the destination position. A native capture will be executed from the SATA source to the SATA destination.

The 160 GB wiped PATA disk will then be re-attached to the Talon in the destination position; with the 18.6 GB SATA disk left intact in the source position. A native capture will then be executed from the SATA source to the PATA destination.

Leaving both SATA and PATA disks intact, a 650 MB dd-image capture will be selected and performed on the two disks. Upon completion of the capture, the destination drive will then be connected to the Guidance Software ® FastBloc 2 FE write-block device and will be viewed using EnCase Forensic Edition Version 5.05c with Windows XP Professional SP2 (see figure 3.1). The disk contents will be noted and the destination disk will be disconnected from the FastBloc device (see figure 3.2, 3.3).

The Talon device (with 160 GB PATA disk attached in destination position) will be connected to a source/suspect PC using the integrated mini-USB Write-PROtect adapter in drive analysis operation mode. The destination PATA disk will be acquired and viewed using EnCase Forensic Edition Version 5.05c.

With the 160 GB PATA hard disk attached in the destination position, a keyword search will be performed on the disk. A keyword list containing the keywords “forensic” and “MISDE” (see figure 5.1) will be searched for on the destination drive. Upon completion of the keyword search, the logfile “listfile.txt” located on the Talon CompactFlash will be examined and the number of search hits notated.

Upon completion of prior testing, the 64 MB CompactFlash Card will be removed from the Talon device and connected to a PC via USB 2.0. The log file entitled “PATAPATA.txt” will be altered using Microsoft Notepad. After alteration of the text file, the CompactFlash card will be reinserted into the Talon and an Audit Trail Checksum Authentication will be executed to determine if the device will verify that the file “PATAPATA.txt” was indubitably altered.

Subsequent to all prior testing, the PATA disk (in the destination position) will be wiped using the WipeClean™ function of the Forensic Talon. The erase process will be executed without a source drive present, and will write zero-filled sectors to the destination drive using programmed I/O (input/output). In addition, a Logicube digital signature (a default setting) will be written to the destination drive on the first sector of each logical cylinder boundary across the entire drive.

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

Expected Results:

1) The Logicube Forensic Talon will successfully perform a secure hash algorithm calculation (SHA-256) on a parallel-ATA (PATA) hard disk drive.

2) The Logicube Forensic Talon will successfully perform a secure hash algorithm calculation (SHA-256) on a serial-ATA (SATA) hard disk drive.

3) The Logicube Forensic Talon will successfully perform a PATA to PATA native drive capture/duplication.

4) The Logicube Forensic Talon will successfully perform a SATA to SATA drive capture/duplication.

5) The Logicube Forensic Talon will successfully perform a SATA to PATA (or vice-versa) drive capture/duplication.

6) The Logicube Forensic Talon will successfully perform a 650 MB dd-style image file capture of a source/suspect hard disk drive.

7) The Logicube Forensic Talon (engaged in USB mode) will successfully perform a capture of a hard disk drive via the integral USB port.

8) The Logicube Forensic Talon will successfully perform a binary keyword search on a PATA-enabled hard disk drive in the source position.

9) The Logicube Forensic Talon will successfully perform a wipeclean function on a PATA-enabled hard disk drive in the destination position.

10) The Logicube Forensic Talon will successfully verify the authenticity of a report stored on the CompactFlash card using the audit trail function.

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-01	Logicube Forensic Talon System; 18.6 GB PATA disk drive in source position	SHA-256 hash calculation performed on source PATA disk	1	SHA-256 Hash calculation will be produced.
01-02	Logicube Forensic Talon System; 18.6 GB PATA disk drive in source position; 160 GB zero-wiped PATA drive in destination position	Native capture executed from PATA source to the PATA destination disk	3	Source disk will be successfully copied to destination disk.
01-03	Logicube Forensic	SHA-256 hash	2	SHA-256 Hash

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

	Talon System; 18.6 GB SATA disk drive in source position	calculation performed on source PATA disk		calculation will be produced.
01-04	Logicube Forensic Talon System; 18.6 GB SATA disk drive in source position; 200 GB zero-wiped SATA drive in destination position	Native capture executed from SATA source to the SATA destination disk	4	Source disk will be successfully copied to destination disk.
01-05	Logicube Forensic Talon System; 18.6 GB SATA disk drive in source position; 160 GB zero-wiped PATA drive in destination position	Native capture executed from SATA source to the PATA destination disk	5	Source SATA disk will be successfully copied to destination PATA disk
01-06	Logicube Forensic Talon System (in dd capture mode); 18.6 GB PATA disk drive in source position; 160 GB PATA disk in destination position	650 MB dd image will be copied from source disk to destination disk	6	Source disk will be successfully copied to destination disk.
01-07	160 GB PATA destination disk; EnCase Forensic Edition v.5.05c for Windows; Guidance Software FastBloc 2 FE write blocking device	Disk structure of destination disk viewed after 650 MB dd capture	6	Disk structure of dd image is partitioned into 650 MB fragments.
01-08	Logicube Forensic Talon System (in USB capture mode); 160 GB PATA disk in destination position; WritePROtect boot floppy	PC disk drive will be copied to PATA destination disk via integrated USB 2.0 connection.	7	Source disk will be successfully copied to destination disk via USB 2.0 connection
01-09	Logicube Forensic Talon System (keyword search mode); 160 GB PATA disk in destination position.	Keywords “forensic” and “MISDE” will be searched for on destination drive	8	Search hits will be found and stored on CompactFlash Card file “listfile.txt”
01-10	64 MB CompactFlash Card (included with Talon); Digital Intelligence UltraBlock Forensic Card Reader (Read/Write Enabled);	CompactFlash file “PATAPATA.txt” will be altered in Microsoft Notepad. Audit trail checksum function will be performed by	9	Audit Trail function will detect that CompactFlash file “PATAPATA.txt” was altered

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

	Logicube Forensic Talon (audit trail mode)	Logicube Talon.		
01-11	Logicube Forensic Talon System (WipeClean™ mode); 160 GB PATA disk in destination position.	160 GB PATA disk will be wiped w/ Logicube digital signature added to last 12 bytes of each sector	10	Disk will be successfully wiped by WipeClean™ function

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

Test Data Description:

Laboratory Test PATA Drive (See Figure 1.2):

Seagate Barracuda ATA III Ultra ATA HDD
Model: ST320414A
Serial Number: 7eC0AS9Y
Part Number: 9R3004-301
Firmware Number: 3.05
Capacity: 20.0 GB (18.6 GB viewable disk space)
Speed: 7200 rpm
Avg. Seek Time: 8.5 m/s
Jumper Setting: Single Master

Drive Parameters (non-DOS / Windows translation)
Cylinders: 16383
Heads: 16
Sectors: 63
Total Addressable Sectors: 39,102,336

Drive Parameters (DOS translation)
Cylinders: 1023
Heads: 256
Sectors: 63
Total Addressable Sectors: 39,102,336

Installed Software:
Microsoft Windows XP Professional 32 Bit O/S w/ Service pack 2
Microsoft Office 2003 Professional
Dell Optiplex GX270 Drivers and Utilities Disk

Zero-Wiped PATA Drive As Reported by Talon:

Model: Maxtor 6Y160P0
Capacity: 160 GB (152.7 GB Reported)
C: 317632
H: 16
S: 63
Total Physical Sectors: 320173056
UDMA Mode 6 is supported!
RPM=0
Seek= 6 m/s
S.M.A.R.T. is supported!
MD5 hash calculation: adda58096f65d59dce198cbe95143770

Examination PC used for USB Capture (see figure 4.2, 4.3):

Dell Optiplex GX270
Pentium 4 3.2 GHz Processor

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

1.00 GB RAM
40 GB PATA HDD
120 GB PATA Slave HDD (Primary Slave Drive)
Windows XP 32 bit w/ SP2
Dell GX270 Drivers and Utilities Disk Installed

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

SUMMARY REPORT

Test Number: TALON-01

Test Title: Functionality Test of the Logicube® Forensic Talon Capturing System

Test Date: 5/10/2006

Test Description:

This test plan will test the ability of the Logicube Forensic Talon Capturing Device to effectively perform all of the operations and commands supported by the device.

Forensic Tool:

Title: Forensic Talon Capturing System
Manufacturer: Logicube®
Model Number: F-TALON
Serial Number: 15287
Software: V2.35 (Jun 07 2006 11:39:01)
Firmware: V 1.0

Test Results:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:	Results
01-01	Logicube Forensic Talon System; 18.6 GB PATA disk drive in source position	SHA-256 hash calculation performed on source PATA disk	1	SHA-256 Hash calculation will be produced.	Pass
01-02	Logicube Forensic Talon System; 18.6 GB PATA disk drive in source position; 160 GB zero-wiped PATA drive in destination position	Native capture executed from PATA source to the PATA destination disk	3	Source disk will be successfully copied to destination disk.	Pass
01-03	Logicube Forensic Talon System; 18.6 GB SATA disk drive in source position	SHA-256 hash calculation performed on source SATA disk	2	SHA-256 Hash calculation will be produced.	Pass
01-04	Logicube Forensic Talon System; 18.6 GB SATA disk drive in source position; 200 GB zero-wiped SATA drive	Native capture executed from SATA source to the SATA destination disk	4	Source disk will be successfully copied to destination disk.	Pass

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

	in destination position				
01-05	Logicube Forensic Talon System; 18.6 GB SATA disk drive in source position; 160 GB zero-wiped PATA drive in destination position	Native capture executed from SATA source to the PATA destination disk	5	Source SATA disk will be successfully copied to destination PATA disk	Pass
01-06	Logicube Forensic Talon System (in dd capture mode); 18.6 GB PATA disk drive in source position; 160 GB PATA disk in destination position	650 MB dd image will be copied from source disk to destination disk	6	Source disk will be successfully copied to destination disk.	Pass
01-07	160 GB PATA destination disk; EnCase Forensic Edition v.5.05c for Windows; Guidance Software FastBloc 2 FE write blocking device	Disk structure of destination disk viewed after 650 MB dd capture	6	Disk structure of dd image is partitioned into 650 MB fragments.	Pass
01-08	Logicube Forensic Talon System (in USB capture mode); 160 GB PATA disk in destination position; WritePROtect boot floppy	PC disk drive will be copied to PATA destination disk via integrated USB 2.0 connection.	7	Source disk will be successfully copied to destination disk via USB 2.0 connection	**Fail** (see limitations)
01-09	Logicube Forensic Talon System (keyword search mode); 160 GB PATA disk in destination position.	Keywords “forensic” and “MISDE” will be searched for on destination drive	8	Search hits will be found and stored on CompactFlash Card file “listfile.txt”	Pass
01-10	64 MB CompactFlash Card (included with Talon); Digital Intelligence UltraBlock Forensic Card Reader (Read/Write Enabled); Logicube Forensic Talon (audit trail mode)	CompactFlash file “PATAPATA.txt” will be altered in Microsoft Notepad. Audit trail checksum function will be performed by Logicube Talon.	9	Audit Trail function will detect that CompactFlash file “PATAPATA.txt” was altered	Pass
01-11	Logicube Forensic Talon System (WipeClean™ mode); 160 GB PATA disk in destination position.	160 GB PATA disk will be wiped w/ Logicube digital signature added to last 12 bytes of each sector	10	Disk will be successfully wiped by WipeClean™ function	Pass

Requirements:

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

1) The Logicube Forensic Talon should successfully perform a secure hash algorithm calculation (SHA-256) on a parallel-ATA (PATA) hard disk drive.

2) The Logicube Forensic Talon should successfully perform a secure hash algorithm calculation (SHA-256) on a serial-ATA (SATA) hard disk drive.

3) The Logicube Forensic Talon should successfully perform a PATA to PATA native drive capture/duplication.

4) The Logicube Forensic Talon should successfully perform a SATA to SATA drive capture/duplication.

5) The Logicube Forensic Talon should successfully perform a SATA to PATA (or vice-versa) drive capture/duplication.

6) The Logicube Forensic Talon should successfully perform a 650 MB dd-style image file capture of a source/suspect hard disk drive.

7) The Logicube Forensic Talon (engaged in USB mode) should successfully perform a capture of a hard disk drive via the integral USB port.

8) The Logicube Forensic Talon should successfully perform a binary keyword search on a PATA-enabled hard disk drive in the source position.

9) The Logicube Forensic Talon should successfully perform a wipeclean function on a PATA-enabled hard disk drive in the destination position.

10) The Logicube Forensic Talon should successfully verify the authenticity of a report stored on the CompactFlash card using the audit trail function.

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

Observations:

During testing of the Talon, it was found that the CompactFlash memory card (see figure 1.4) reported a total capacity of 256 MB, contrary to the 64 MB capacity that the manufacturer label reports. This reported capacity was authenticated by Guidance Software EnCase Forensic Edition v.5.05 for Windows.

Limitations:

*Testing was unable to produce a stable image while the unit was engaged in USB mode. The bootable client would only report a data transfer rate of 2 MB/Min (see figure 4.4) and would time-out after a few moments. The root cause to this problem is unknown at the current time.

Unlike its predecessor, the Forensic MD5, which allowed computation of both CRC-32 & MD5 hash algorithms, early versions of the Forensic Talon will only compute a SHA-256 hash calculation. This lack of functionality with the Talon caused a limitation with validity in the respect that none of the SHA-256 calculations could be verified by another hardware or software test tool.

Because functionality of the Talon in USB mode is dependent of the PC number pad (see figure 4.3), the absence of a numeric keypad on the source PC (such as a laptop) limits performing functions with the device.

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 Shown is the Logicube® Forensic Talon Capturing System

Figure 1.2 Parallel-ATA (PATA) & Serial-ATA (SATA) disks used for testing

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

Figure 1.3 Logicube Talon External Connections

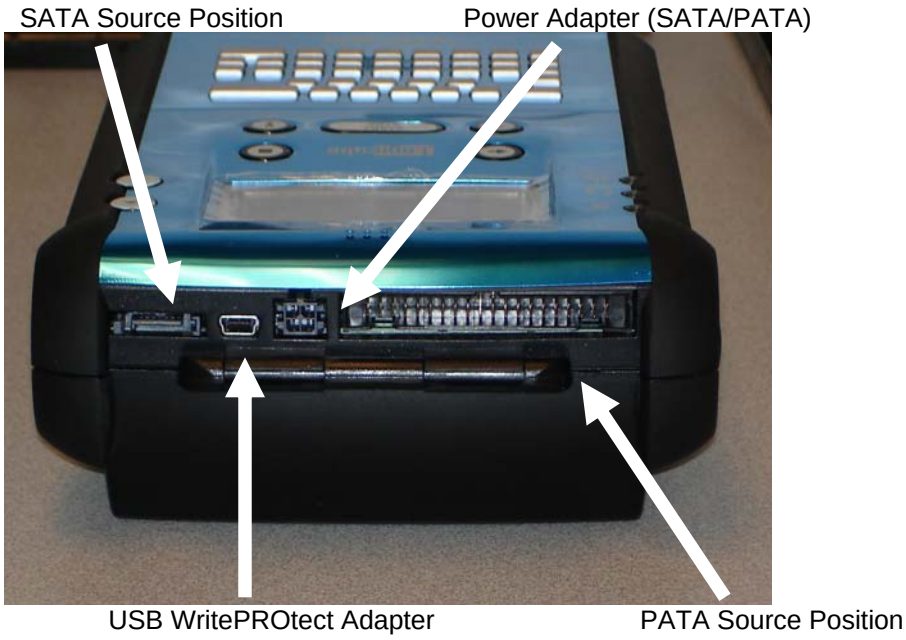
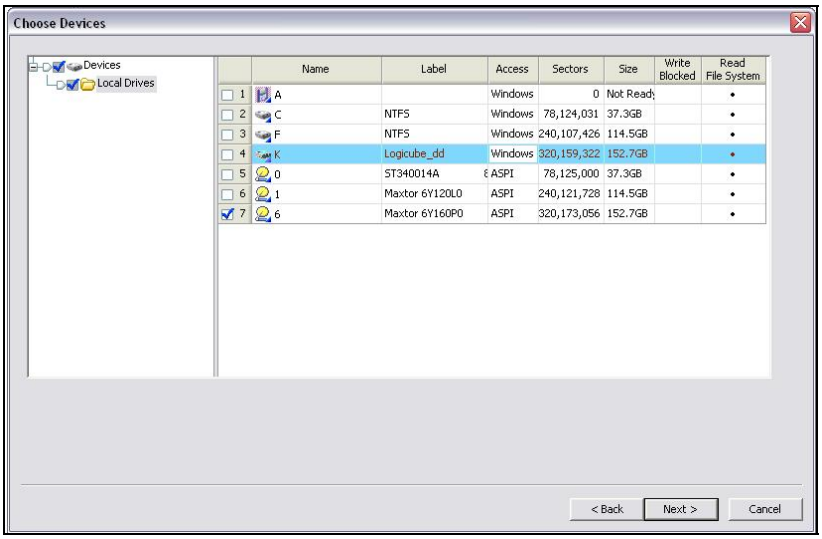


Figure 1.4 64 megabyte (256 MB reported) CompactFlash memory card

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

Figure 2.1 18.6 GB PATA disk drive connected to source position

Figure 3.1 DD Image Capture viewed in EnCase Forensic Edition v.5.05c for Windows



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

Figure 3.2 DD capture folder contained on disk viewed in EnCase Forensic Edition v.5.05c for Windows

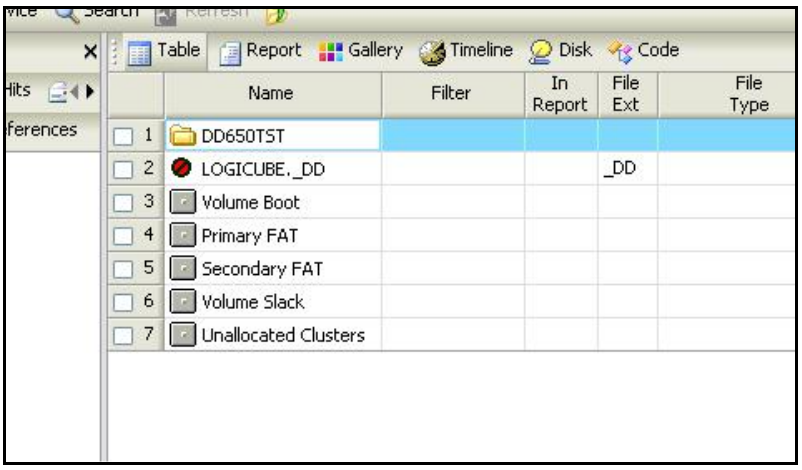
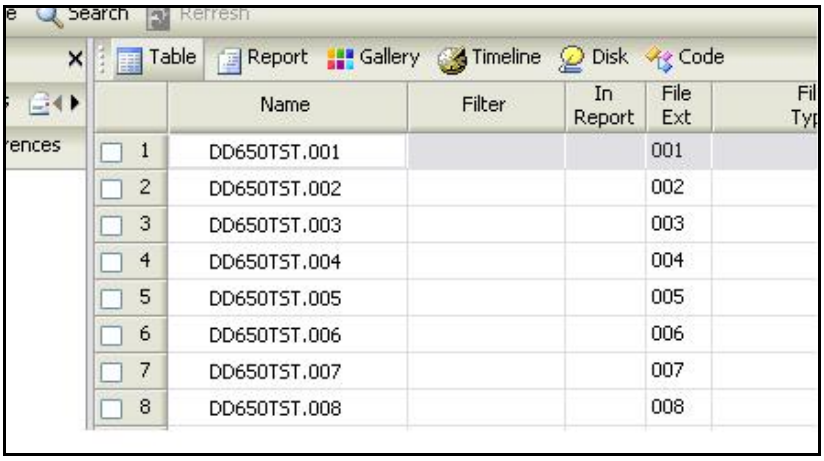


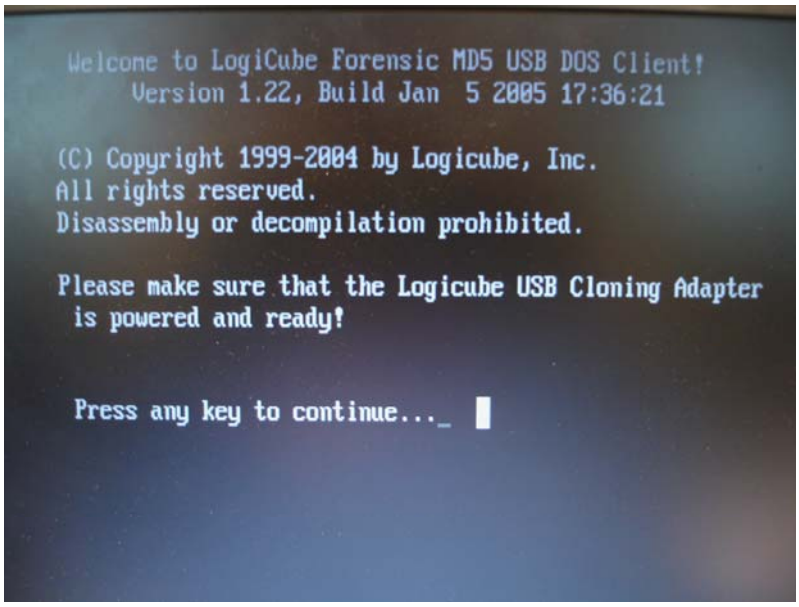
Figure 3.3 650 MB dd subfolders viewed in EnCase Forensic Edition v.5.05c for Windows.



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

Figure 4.1 Logicube Talon set in USB capture mode

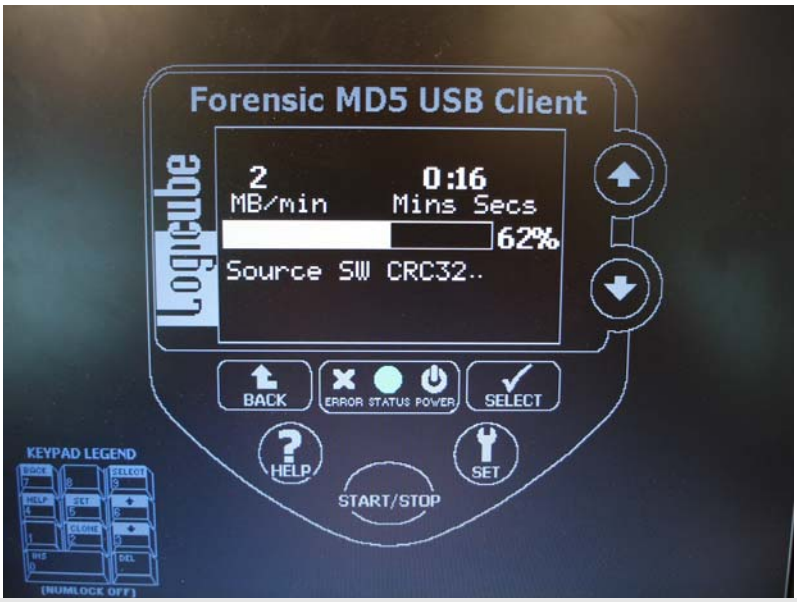
Figure 4.2 USB Cloning Adapter DOS startup screen (using WritePROtect Floppy)



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

Figure 4.3 USB Cloning Adapter Virtual Interface (using WritePROtect Floppy)

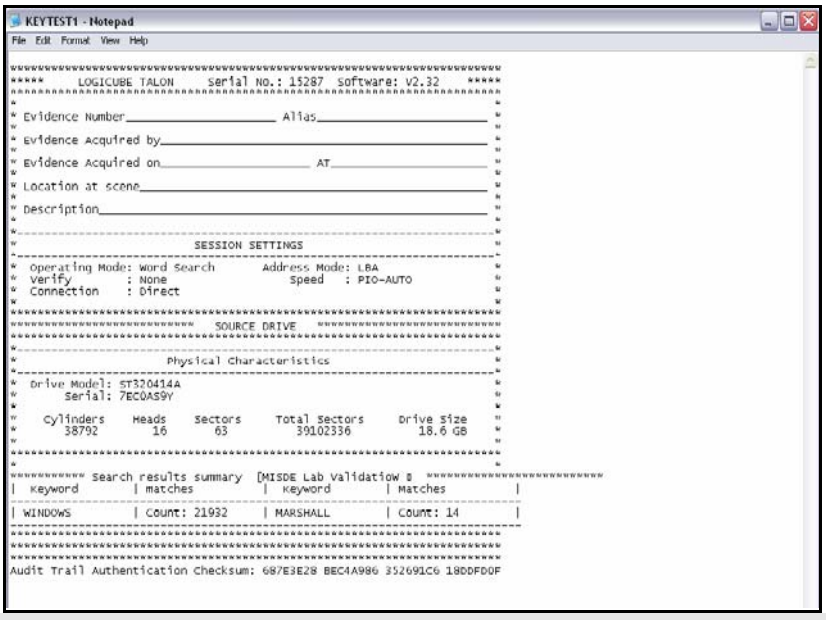
Figure 4.4 USB Cloning Adapter Virtual Interface in capture mode (using boot floppy)



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

Figure 5.1 Keyword search performed on 18.6 GB PATA test disk drive.

Figure 5.2 Log file (keylist1.txt) from keyword search performed on 18.6 GB PATA test disk



KEYTEST1 - Notepad

File Edit Format View Help

```
********************************************************************************
*****     LOGICUBE TALON     Serial No.: 15287  Software: V2.32     *****
********************************************************************************
*                                                                              *
* Evidence Number_____________________ Alias_____________________              *
*                                                                              *
* Evidence Acquired by_____________________________________________            *
*                                                                              *
* Evidence Acquired on_____________________ AT_____________________            *
*                                                                              *
* Location at scene________________________________________________            *
*                                                                              *
* Description______________________________________________________            *
*                                                                              *
*------------------------------------------------------------------------------*
*                          SESSION SETTINGS                                    *
*------------------------------------------------------------------------------*
*  Operating Mode: Word Search       Address Mode: LBA                         *
*  Verify        : None                  Speed   : PIO-AUTO                    *
*  Connection    : Direct                                                      *
*                                                                              *
********************************************************************************
*****************************   SOURCE DRIVE   *********************************
********************************************************************************
*------------------------------------------------------------------------------*
*                        Physical Characteristics                              *
*------------------------------------------------------------------------------*
*  Drive Model: ST320414A                                                      *
*       Serial: 7EC0AS9Y                                                       *
*                                                                              *
*    Cylinders     Heads     Sectors     Total Sectors     Drive Size          *
*        38792        16          63          39102336          18.6 GB       *
*                                                                              *
********************************************************************************
*                                                                              *
************ Search results summary  [MISDE Lab Validation 8  ****************************
|  Keyword        | matches          |  Keyword        | Matches          |
--------------------------------------------------------------------------------
| WINDOWS         | Count: 21932     | MARSHALL        | Count: 14        |
--------------------------------------------------------------------------------
********************************************************************************
********************************************************************************
********************************************************************************
Audit Trail Authentication Checksum: 687E3E2B BEC4A986 352691C6 18DDFD0F
```

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

Figure 5.3 Log file (listfile.txt) from keyword search performed on 18.6 GB PATA test disk