F-Response

Extend Your Arsenal

F-Response® Validation Testing Report

Includes F-Response Field Kit, Consultant, and Enterprise
(Windows, Linux, and Apple OS X)
March 2009

Document Control

This is a controlled document produced by Agile Risk Management LLC ("AGILE"). The control and release of this document is the responsibility of the AGILE document owner. This includes any amendment that may be required.

Issue Control			
Issue	2.0	**Date**	March 24, 2009
Classification	Public	**Author**	M. Shannon
Document Title	F-Response Validation Testing Report		
Approved by	M. Shannon		
Released by	M. Shannon		

Owner Details	
Name	Matthew M Shannon
Office/Region	Agile Risk Management LLC Corporate Offices
Contact Number	1-800-317-5497
E-mail Address	mshannon@f-response.com

Revision History			
Issue	**Date**	**Author**	**Comments**
Draft 0.1	09/03/2008	Matthew Shannon	Initial Draft
Final 1.0	09/07/2008	Matthew Decker	Reviewed by
Final 1.0	09/08/2008	Matthew Shannon	Initial Final Document Release
Draft 1.1	01/15/2009	Matthew Shannon	Modified to include Linux and Apple OS X Testing Results
Final 2.0	03/24/2009	Matthew Decker	Reviewed by
Final 2.0	03/31/2009	Matthew Shannon	Second Final Document Release

Table of Contents

Testing Results Summary

The purpose of this testing is to validate the accuracy and reliability of F-Response software using the repeatable test method presented herein. The results of the testing are hereby published for independent validation and peer review.

F-Response uses a patent-pending process based on the well documented "iSCSI" industry standard to create a reliable, read-only connection between an examiner's computer and a computer under inspection. The function of the F-Response software tested herein is that an established F-Response iSCSI network connection is completely read-only, functioning much like a software write blocker albeit over a network connection. The testing validates that F-Response software protects the integrity of the data on the computer under inspection because it does not permit alteration of any data on the computer under inspection during the test.

The results of our testing confirm that the iSCSI network connection established by F-Response software does reliably and accurately create a read-only connection between an examiner's computer and a computer under inspection. Our testing uses generally accepted forensics techniques and tools to verify and validate the results. The scientific method presented is done so in accordance with the Daubert Principles (Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993) 509 U.S. 579, 589), and as such we submit that F-Response is suitable for use in acquiring data that is intended for use in a court of law.

Unless otherwise noted, all testing activities were performed against the F-Response application code base (F-Response Field Kit, Consultant, and Enterprise Edition), release 3.09 (Windows, Linux, and Apple OS X).

1 Introduction

1.1 Scope

The scope of this project was limited to the validation and testing of F-Response Field Kit, Consultant, and Enterprise Edition on the following platforms.

- Microsoft Windows
    - Windows 2000 Professional
    - Windows 2000 Server
    - Windows XP Professional
    - Windows XP Professional 64
    - Windows 2003 Server
    - Windows Vista Business
    - Windows Vista Business 64
    - Windows 2008 Server
    - Windows 2008 Server 64
    - Windows 7 (Build 7000)
    - Windows 7 (Build 7000) 64
- Linux
    - Fedora Core (4 – 10)
    - Ubuntu (6.04 – 8.10)
- Apple
    - OS X 10.4 PPC
    - OS X 10.5 Intel

1.2 Purpose

This document outlines the F-Response Software validation process, results, and methodology developed and executed by Agile Risk Management LLC. F-Response Software validation answers the following questions:

- Disk Validity
    - Does F-Response accurately present the remote Physical Disk(s)?
- Read Accuracy
    - Does F-Response correctly and accurately read data from the remote Physical Disk(s)?
- Write Prevention
    - Does F-Response effectively prevent write operations from occurring on the remote Physical Disk(s)?

1.3 Document Layout

This document will adhere to the following layout:

- Test Results
    - Presents a table representing the test results by operating system.
- Test Environment and Procedure
    - Presents the environment and procedure used in the testing process.
- Test Results Details
    - Presents the detailed results of the testing procedures, including screen captures.

2 Test Results

2.1 Disk Validity

Does F-Response effectively present the remote PhysicalDisk(s)?

In order to test the validity of the locally attached remote F-Response iSCSI disk, we collected the total disk size in sectors and the sector size using multiple local data collection sources. This provided a baseline to test against when the F-Response disk is attached to our local workstation for analysis. While not explicitly noted, the results of these tests were identical for each version of F-Response tested, Field Kit, Consultant, and Enterprise. The detailed process used to obtain these results is included in section 4 of this document.

Disk Validity Testing Results	Native (Local Machine)		Remote (F-Response Presented)		Result
Platform	Total Sectors	Sector Size	Total Sectors	Sector Size	
Windows 2000 Professional	16777216	512	16777216	512	PASS
Windows 2000 Server	16777216	512	16777216	512	PASS
Windows XP Professional	12582912	512	12582912	512	PASS
Windows XP Professional 64	16777216	512	16777216	512	PASS
Windows 2003 Standard Edition Server	16777216	512	16777216	512	PASS
Windows Vista Business	33554432	512	33554432	512	PASS
Windows Vista Business 64	33554432	512	33554432	512	PASS
Windows 2008 Enterprise Server	33554432	512	33554432	512	PASS
Windows 2008 Enterprise Server 64	33554432	512	33554432	512	PASS
Windows 7 (Build 7000)	33554432	512	33554432	512	PASS
Windows 7 (Build 7000) 64	50331648	512	50331648	512	PASS
Fedora Core 4	8388608	512	8388608	512	PASS
Fedora Core 5	16777216	512	16777216	512	PASS
Fedora Core 6	16777216	512	16777216	512	PASS
Fedora Core 7	16777216	512	16777216	512	PASS
Fedora Core 8	16777216	512	16777216	512	PASS
Fedora Core 9	16777216	512	16777216	512	PASS
Fedora Core 10	16777216	512	16777216	512	PASS
Ubuntu Server 6.06	16777216	512	16777216	512	PASS

Ubuntu Server 6.10	16777216	512	16777216	512	PASS
Ubuntu Server 7.04	16777216	512	16777216	512	PASS
Ubuntu Server 7.10	16777216	512	16777216	512	PASS
Ubuntu Server 8.04	16777216	512	16777216	512	PASS
Ubuntu Server 8.10	16777216	512	16777216	512	PASS
Apple OS X 10.4 PPC	117210240	512	117210240	512	PASS
Apple OS X 10.5 Intel	312581808	512	312581808	512	PASS

2.2 Read Accuracy

Does F-Response correctly and accurately read data from the remote PhysicalDisk(s)?

In order to test the read accuracy of the locally attached remote F-Response iSCSI disk, we obtained hash values for the individual files listed below, as well as a portion of the raw disk (Physical Sector 6291519) from the local F-Response disk. Both these hash values were then computed using select Computer Forensics software packages on their native operating system. While not explicitly noted, the results of these tests were identical for each version of F-Response tested, Field Kit, Consultant, and Enterprise.

Read Accuracy Testing Results	Native (Local Machine)		Remote (F-Response Presented)		Result
Platform	File Hash	Data Hash	File Hash	Data Hash	
Windows 2000 Professional	2ECC0CD4197C012F9D0FCFF7F78E1D34	BE7CF63AAC0AA8E140BA84F4CB0D6F01	2ecc0cd4197c012f9d0fcff7f78e1d34	BE7CF63AAC0AA8E140BA84F4CB0D6F01	PASS
Windows 2000 Server	2ECC0CD4197C012F9D0FCFF7F78E1D34	BE7CF63AAC0AA8E140BA84F4CB0D6F01	2ecc0cd4197c012f9d0fcff7f78e1d34	BE7CF63AAC0AA8E140BA84F4CB0D6F01	PASS
Windows XP Professional	C1B29B4E6EEA9510610DB2EC4D6DB160	2204D7C2DF92DA3D8AAFA7493014D707	c1b29b4e6eea9510610db2ec4d6db160	2204D7C2DF92DA3D8AAFA7493014D707	PASS
Windows XP Professional 64	eaad72a0cbd33f63d4cda5e933a5d6d8	184DF2E5F625495AB65C82C6E7CDDD76	eaad72a0cbd33f63d4cda5e933a5d6d8	184DF2E5F625495AB65C82C6E7CDDD76	PASS
Windows 2003 Standard Edition Server	971757832F7DD9516977985999F527CA	839B7586271A6E65262E86B12072C60C	971757832f7dd9516977985999f527ca	839B7586271A6E65262E86B12072C60C	PASS
Windows Vista Business	9E24B834DC6FC0634C28004721DF9D82	0BFD435DED2FFBD890062D36ABB6A830	9e24b834dc6fc0634c28004721df9d82	0BFD435DED2FFBD890062D36ABB6A830	PASS
Windows Vista Business 64	57dab7451bc4a63b71a1f6d258ef7c8b	6267A69C7D36AA761082E2D1175464E0	57dab7451bc4a63b71a1f6d258ef7c8b	6267A69C7D36AA761082E2D1175464E0	PASS
Windows 2008 Enterprise Server	9E24B834DC6FC0634C28004721DF9D82	0BFD435DED2FFBD890062D36ABB6A830	9e24b834dc6fc0634c28004721df9d82	0BFD435DED2FFBD890062D36ABB6A830	PASS
Windows 2008 Enterprise Server 64	9E24B834DC6FC0634C28004721DF9D82	82D205869C776D8C367B477E8438D1F1	9e24b834dc6fc0634c28004721df9d82	82D205869C776D8C367B477E8438D1F1	PASS
Windows 7 (Build 7000)	2B5291C6825C21D4190262E020AB1163	9401419A2FC1FAF919221BEEEDE7770A	2b5291c6825c21d4190262e020ab1163	9401419A2FC1FAF919221BEEEDE7770A	PASS
Windows 7 (Build 7000) 64	2B5291C6825C21D4190262E020AB1163	D7177B47DCF8F1E3E5BC59F153EE90FA	2b5291c6825c21d4190262e020ab1163	D7177B47DCF8F1E3E5BC59F153EE90FA	PASS
Fedora Core 4	a71e7abce43fb3a62066007d7ad2c0e6	935d7c4e010f79fb4d3947d191cb5d7e	a71e7abce43fb3a62066007d7ad2c0e6	935D7C4E010F79FB4D3947D191CB5D7E	PASS
Fedora Core 5	cd23994c39661cad3a4a2cf838ccbae5	53e6f1ddb08b4ce450efbc3fec822004	cd23994c39661cad3a4a2cf838ccbae5	53E6F1DDB08B4CE450EFBC3FEC822004	PASS
Fedora Core 6	69a9a365aefdc12877f386f06698ab03	85de51ffd49743cfd35aec25147b1036	69a9a365aefdc12877f386f06698ab03	85DE51FFD49743CFD35AEC25147B1036	PASS
Fedora Core 7	6f3169684750da15642e477efb0e30ff	c89330d2fbd6eaf20386e02534411192	6f3169684750da15642e477efb0e30ff	C89330D2FBD6EAF20386E02534411192	PASS
Fedora Core 8	1fd60eb534fd865502b85247c8a2e004	01c0bbffaf80c5ec9f0559f2148653af	1fd60eb534fd865502b85247c8a2e004	01C0BBFFAF80C5EC9F0559F2148653AF	PASS
Fedora Core 9	5dee0cbc019929ba25f5a1110f480fec	5f753ae907d950b782aa1e4dce3ba9e7	5dee0cbc019929ba25f5a1110f480fec	5F753AE907D950B782AA1E4DCE3BA9E7	PASS
Fedora Core 10	db9db7e9897eaa492a78c9e362124349	e83bc3df75b7b1bb0261a6154f919f1d	db9db7e9897eaa492a78c9e362124349	E83BC3DF75B7B1BB0261A6154F919F1D	PASS

Ubuntu Server 6.06	e451038f108519e121576c646c46f28c	a073b1a0cbb96938a1699823ba5e69af	e451038f108519e121576c646c46f28c	A073B1A0CBB96938A1699823BA5E69AF	PASS
Ubuntu Server 6.10	fe52708fbf10b81b018e609da78ca934	98b4de262ec42072ed15d28be723d2c2	fe52708fbf10b81b018e609da78ca934	98B4DE262EC42072ED15D28BE723D2C2	PASS
Ubuntu Server 7.04	fdbf5ae46257db439d38ca5dc911e4e7	07220c3f5a1bcaf89891fd0228288876	fdbf5ae46257db439d38ca5dc911e4e7	07220C3F5A1BCAF89891FD0228288876	PASS
Ubuntu Server 7.10	6e456bdb48be15d1dcb785f2a8376472	8cbbbc673901073134b9607aff7b9f84	6e456bdb48be15d1dcb785f2a8376472	8CBBBC673901073134B9607AFF7B9F84	PASS
Ubuntu Server 8.04	03c03d4413202be5fa08c4c90bf37ede	edfea877fc950eb110ef5666b31066c0	03c03d4413202be5fa08c4c90bf37ede	EDFEA877FC950EB110EF5666B31066C0	PASS
Ubuntu Server 8.10	aa609974b6773de6c90a2dbf08ad220c	deb34a7d1c1763f5831babe1056a2276	AA609974B6773DE6C90A2DBF08AD220C	DEB34A7D1C1763F5831BABE1056A2276	PASS
Apple OS X 10.4 PPC	58a9a08922bf15873c1c7fb75b829d7b	fddf4657481e5d1f5a733e76fe2496bf	58A9A08922BF15873C1C7FB75B829D7B	FDDF4657481E5D1F5A733E76FE2496BF	PASS
Apple OS X 10.5 Intel	45b608d8d62fa464d3d5055b5e9a09a0	2d281550d07074ec8625bb7942d17e7c	45B608D8D62FA464D3D5055B5E9A09A0	2D281550D07074EC8625BB7942D17E7C	PASS

2.3 Write Prevention

Does F-Response accurately prevent write operations from occurring on the remote PhysicalDisk(s)?[1]

In order to test the write prevention capabilities of F-Response , we attempted to perform write operations using both the file system create file and delete file commands, as well as through direct writing to arbitrary locations on the F-Response connected disk. In all cases F-Response silently prevented the write operations. In each case, the local system would return a "success" message, however no actual changes occurred on the remote F-Response disk. While not explicitly noted, the results of these tests were identical for each version of F-Response tested, Field Kit, Consultant, and Enterprise. The detailed process used to obtain these results is included in section 4 of this document.

Write Prevention Testing	Action				Result
Platform	File Deletion		Data Modification		
	System Response	Actual Result	System Response	Actual Result	
Windows 2000 Professional	SUCCESS	BLOCKED	SUCCESS	BLOCKED	PASS
Windows 2000 Server	SUCCESS	BLOCKED	SUCCESS	BLOCKED	PASS
Windows XP Professional	SUCCESS	BLOCKED	SUCCESS	BLOCKED	PASS
Windows XP Professional 64	SUCCESS	BLOCKED	SUCCESS	BLOCKED	PASS
Windows 2003 Standard Edition Server	SUCCESS	BLOCKED	SUCCESS	BLOCKED	PASS
Windows Vista Business	BLOCKED	BLOCKED	SUCCESS	BLOCKED	PASS
Windows Vista Business 64	BLOCKED	BLOCKED	SUCCESS	BLOCKED	PASS
Windows 2008 Enterprise Server	BLOCKED	BLOCKED	SUCCESS	BLOCKED	PASS
Windows 2008 Enterprise Server 64	BLOCKED	BLOCKED	SUCCESS	BLOCKED	PASS
Windows 7 (Build 7000)	BLOCKED	BLOCKED	SUCCESS	BLOCKED	PASS
Windows 7 (Build 7000) 64	BLOCKED	BLOCKED	SUCCESS	BLOCKED	PASS
Fedora Core 4	NA	NA	SUCCESS	BLOCKED	PASS
Fedora Core 5	NA	NA	SUCCESS	BLOCKED	PASS

[1] All write operations are prevented, however select write operations are held in memory where necessary to improve operations. No write operations reach the physical disk. Full details of the write tests performed are available in section 4 of this document.

Fedora Core 6	NA	NA	SUCCESS	BLOCKED	PASS
Fedora Core 7	NA	NA	SUCCESS	BLOCKED	PASS
Fedora Core 8	NA	NA	SUCCESS	BLOCKED	PASS
Fedora Core 9	NA	NA	SUCCESS	BLOCKED	PASS
Fedora Core 10	NA	NA	SUCCESS	BLOCKED	PASS
Ubuntu Server 6.06	NA	NA	SUCCESS	BLOCKED	PASS
Ubuntu Server 6.10	NA	NA	SUCCESS	BLOCKED	PASS
Ubuntu Server 7.04	NA	NA	SUCCESS	BLOCKED	PASS
Ubuntu Server 7.10	NA	NA	SUCCESS	BLOCKED	PASS
Ubuntu Server 8.04	NA	NA	SUCCESS	BLOCKED	PASS
Ubuntu Server 8.10	NA	NA	SUCCESS	BLOCKED	PASS
Apple OS X 10.4 PPC	NA	NA	SUCCESS	BLOCKED	PASS
Apple OS X 10.5 Intel	NA	NA	SUCCESS	BLOCKED	PASS

3 Test Environment

3.1 Test Environment Software

The following represents a complete listing of the software used to validate F-Response.

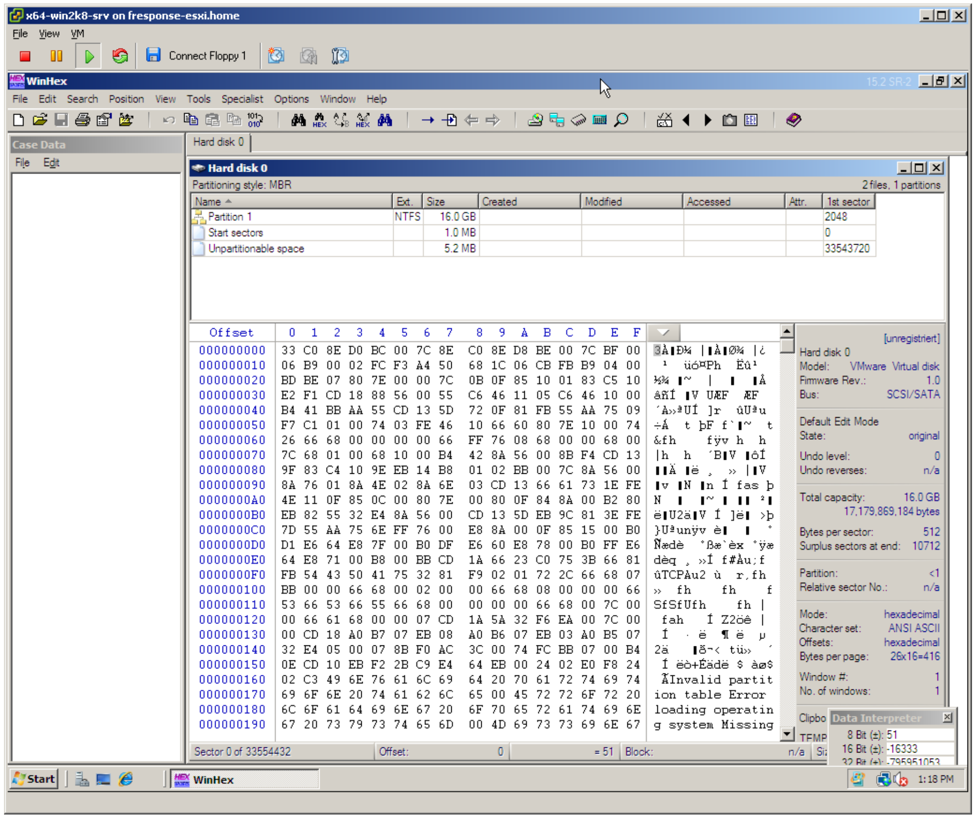
Application	Version	Company	Used for	Platform
Forensic Acquisition Utilities (FAU)	1.3.0.2363	GMG	Used in testing Write Prevention in Windows	Windows XP Professional SP3
F-Response (FK, CE, EE)	3.09	Agile Risk Management LLC	Providing remote forensically sound disk access.	Multiple (See Scope Section)
GNU Tools (md5, dd, dmesg)	2.3.5+ (glibc)	Linux	Baseline data collection on the Linux target platform.	Linux (See Scope Section)
Encase Forensic	6.13	Guidance Software Inc.	Verifying capacity, read accuracy.	Windows XP Professional SP3
MacForensicsLab	2.5.4	SubRosaSoft Inc.	Verifying capacity, read accuracy.	Apple OS X 10.5,10.4
Microsoft iSCSI Initiator	2.08	Microsoft	Required to attach F-Response Disk to Windows	Windows XP Professional SP3
VM Ware ESX Server 3i	3.5.0. 123629	VMWare Inc.	Hosting F-Response Test Virtual Machines	VMWare ESXi Hypervisor
X-Ways Forensics/Winhex[2]	15.0 SR-2	X-Ways Technology AG	Verifying capacity, read accuracy.	Windows XP Professional SP3

[2] X-Ways permission granted for use of demonstration licensed version.

4 Test Result Details[3]

4.1 Obtain Baseline (Windows)

Step 1, Open X-Ways WinHex and select the first physical disk, record the provided total number of bytes and sector size. Divide the total number of bytes by the sector size to obtain the sector count. Record the provided values.


x64-win2k8-srv on fresponse-esxi.home
File View VM
Connect Floppy 1
WinHex
15.2 SR-2
File Edit Search Position View Tools Specialist Options Window Help
Case Data
File Edit
Hard disk 0
Start
WinHex
1:18 PM

Hard disk 0

Partitioning style: MBR — 2 files, 1 partitions

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
Partition 1	NTFS	16.0 GB					2048
Start sectors		1.0 MB					0
Unpartitionable space		5.2 MB					33543720

```
   Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000   33 C0 8E D0 BC 00 7C 8E  C0 8E D8 BE 00 7C BF 00   3À▮Ð¼ |▮À▮Ø¾ |¿
000000010   06 B9 00 02 FC F3 A4 50  68 1C 06 CB FB B9 04 00    ¹  üó¤Ph  Ëû¹
000000020   BD BE 07 80 7E 00 00 7C  0B 0F 85 10 01 83 C5 10   ½¾ ▮~  |  ▮  ▮Å
000000030   E2 F1 CD 18 88 56 00 55  C6 46 11 05 C6 46 10 00   âñÍ ▮V UÆF  ÆF
000000040   B4 41 BB AA 55 CD 13 5D  72 0F 81 FB 55 AA 75 09   ´A»ªUÍ ]r  ûUªu
000000050   F7 C1 01 00 74 03 FE 46  10 66 60 80 7E 10 00 74   ÷Á  t þF f`▮~  t
000000060   26 66 68 00 00 00 00 66  FF 76 08 68 00 00 68 00   &fh    fÿv h  h
000000070   7C 68 01 00 68 10 00 B4  42 8A 56 00 8B F4 CD 13   |h  h  ´B▮V ▮ôÍ
000000080   9F 83 C4 10 9E EB 14 B8  01 02 BB 00 7C 8A 56 00   ▮▮Ä ▮ë ¸  » |▮V
000000090   8A 76 01 8A 4E 02 8A 6E  03 CD 13 66 61 73 1E FE   ▮v ▮N ▮n Í fas þ
0000000A0   4E 11 0F 85 0C 00 80 7E  00 80 0F 84 8A 00 B2 80   N  ▮  ▮~ ▮ ▮▮ ²▮
0000000B0   EB 82 55 32 E4 8A 56 00  CD 13 5D EB 9C 81 3E FE   ë▮U2ä▮V Í ]ë▮ >þ
0000000C0   7D 55 AA 75 6E FF 76 00  E8 8A 00 0F 85 15 00 B0   }Uªunÿv è▮  ▮  °
0000000D0   D1 E6 64 E8 7F 00 B0 DF  E6 60 E8 78 00 B0 FF E6   Ñæd è °ßæ`èx °ÿæ
0000000E0   64 E8 71 00 B8 00 BB CD  1A 66 23 C0 75 3B 66 81   dèq ¸ »Í f#Àu;f
0000000F0   FB 54 43 50 41 75 32 81  F9 02 01 72 2C 66 68 07   ûTCPAu2 ù  r,fh
000000100   BB 00 00 66 68 00 02 00  00 66 68 08 00 00 00 66   »  fh    fh    f
000000110   53 66 53 66 55 66 68 00  00 00 00 66 68 00 7C 00   SfSfUfh    fh  |
000000120   00 66 61 68 00 00 07 CD  1A 5A 32 F6 EA 00 7C 00    fah   Í Z2öê  |
000000130   00 CD 18 A0 B7 07 EB 08  A0 B6 07 EB 03 A0 B5 07    Í  · ë  ¶ ë  µ
000000140   32 E4 05 00 07 8B F0 AC  3C 00 74 FC BB 07 00 B4   2ä   ▮ð¬< tü»  ´
000000150   0E CD 10 EB F2 2B C9 E4  64 EB 00 24 02 E0 F8 24    Í ëò+Éäd ë $ àø$
000000160   02 C3 49 6E 76 61 6C 69  64 20 70 61 72 74 69 74    ÃInvalid partit
000000170   69 6F 6E 20 74 61 62 6C  65 00 45 72 72 6F 72 20   ion table Error
000000180   6C 6F 61 64 69 6E 67 20  6F 70 65 72 61 74 69 6E   loading operatin
000000190   67 20 73 79 73 74 65 6D  00 4D 69 73 73 69 6E 67   g system Missing
```

Sector 0 of 33554432 | Offset: 0 | = 51 | Block: n/a | Si

[unregistriert]
Hard disk 0
Model: VMware Virtual disk
Firmware Rev.: 1.0
Bus: SCSI/SATA

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Total capacity: 16.0 GB
17,179,869,184 bytes

Bytes per sector: 512
Surplus sectors at end: 10712

Partition: <1
Relative sector No.: n/a

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 26x16=416

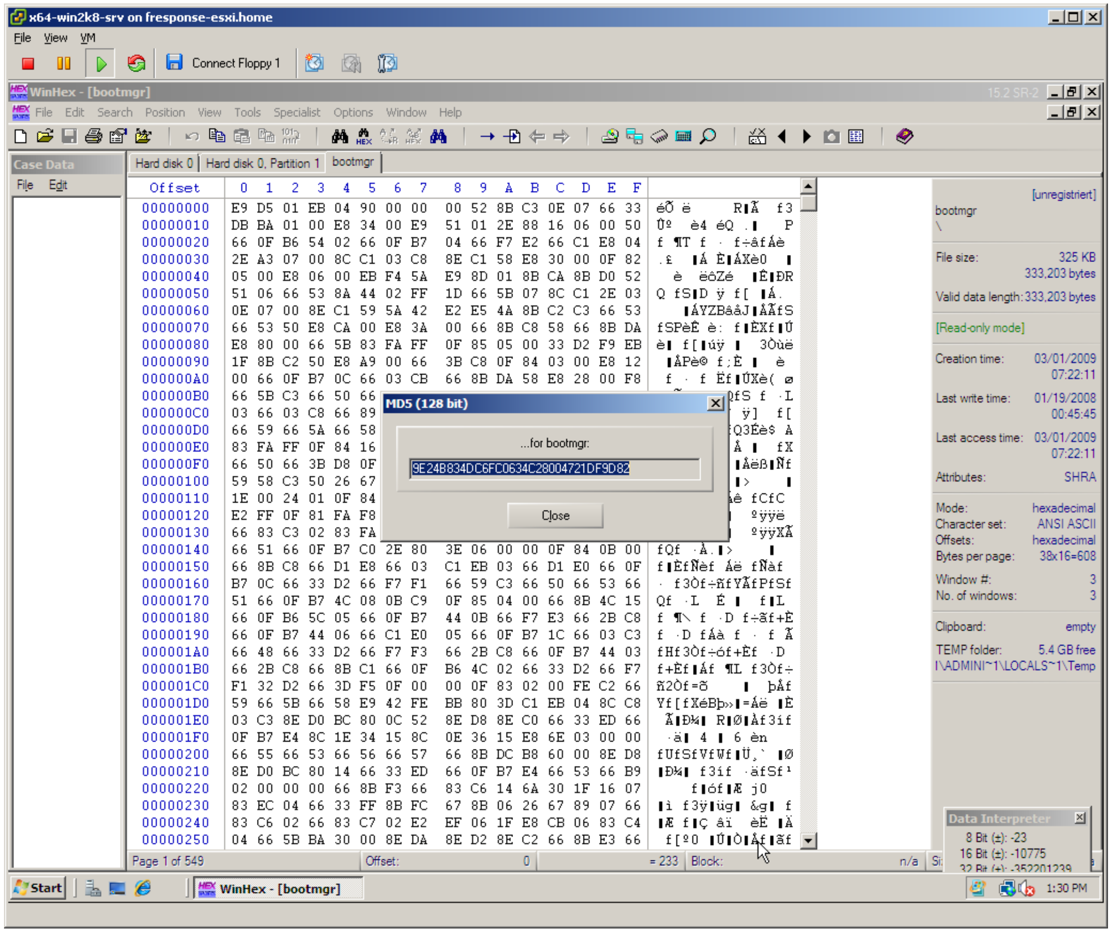
Window #: 1
No. of windows: 1

Clipbo
TEMP

Data Interpreter
8 Bit (±): 51
16 Bit (±): -16333
32 Bit (±): -795951053

[3] All testing details assume the F-Response disk has been properly connected using one of the many supported iSCSI Initiator software products, as this process is detailed in numerous training manuals and quick start guides available on the F-Response website (www.f-response.com) it will not be duplicated herein. In addition while only one baseline collection effort is contained herein, this process was repeated for all platforms identified under the Scope section of this document.

Step 2, Obtain file hash value and data hash value, select a system file, double click on it, and select Tools->Compute Hash, select md5 hash and record this value.



MD5 (128 bit)

...for bootmgr:

9E24B834DC6FC0634C28004721DF9D82

Close

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  E9 D5 01 EB 04 90 00 00  00 52 8B C3 0E 07 66 33
00000010  DB BA 01 00 E8 34 00 E9  51 01 2E 88 16 06 00 50
00000020  66 0F B6 54 02 66 0F B7  04 66 F7 E2 66 C1 E8 04
00000030  2E A3 07 00 8C C1 03 C8  8E C1 58 E8 30 00 0F 82
00000040  05 00 E8 06 00 EB F4 5A  E9 8D 01 8B CA 8B D0 52
00000050  51 06 66 53 8A 44 02 FF  1D 66 5B 07 8C C1 2E 03
00000060  0E 07 00 8E C1 59 5A 42  E2 E5 4A 8B C2 C3 66 53
00000070  66 53 50 E8 CA 00 E8 3A  00 66 8B C8 58 66 8B DA
00000080  E8 80 00 66 5B 83 FA FF  0F 85 05 00 33 D2 F9 EB
00000090  1F 8B C2 50 E8 A9 00 66  3B C8 0F 84 03 00 E8 12
000000A0  00 66 0F B7 0C 66 03 CB  66 8B DA 58 E8 28 00 F8
000000B0  66 5B C3 66 50 66
000000C0  03 66 03 C8 66 89
000000D0  66 59 66 5A 66 58
000000E0  83 FA FF 0F 84 16
000000F0  66 50 66 3B D8 0F
00000100  59 58 C3 50 26 67
00000110  1E 00 24 01 0F 84
00000120  E2 FF 0F 81 FA F8
00000130  66 83 C3 02 83 FA
00000140  66 51 66 0F B7 C0 2E 80  3E 06 00 00 0F 84 0B 00
00000150  66 8B C8 66 D1 E8 66 03  C1 EB 03 66 D1 E0 66 0F
00000160  B7 0C 66 33 D2 66 F7 F1  66 59 C3 66 50 66 53 66
00000170  51 66 0F B7 4C 08 0B C9  0F 85 04 00 66 8B 4C 15
00000180  66 0F B6 5C 05 66 0F B7  44 0B 66 F7 E3 66 2B C8
00000190  66 0F B7 44 06 66 C1 E0  05 66 0F B7 1C 66 03 C3
000001A0  66 48 66 33 D2 66 F7 F3  66 2B C8 66 0F B7 44 03
000001B0  66 2B C8 66 8B C1 66 0F  B6 4C 02 66 33 D2 66 F7
000001C0  F1 32 D2 66 3D F5 0F 00  00 0F 83 02 00 FE C2 66
000001D0  59 66 5B 66 58 E9 42 FE  BB 80 3D C1 EB 04 8C C8
000001E0  03 C3 8E D0 BC 80 0C 52  8E D8 8E C0 66 33 ED 66
000001F0  0F B7 E4 8C 1E 34 15 8C  0E 36 15 E8 6E 03 00 00
00000200  66 55 66 53 66 56 66 57  66 8B DC B8 60 00 8E D8
00000210  8E D0 BC 80 14 66 33 ED  66 0F B7 E4 66 53 66 B9
00000220  02 00 00 00 66 8B F3 66  83 C6 14 6A 30 1F 16 07
00000230  83 EC 04 66 33 FF 8B FC  67 8B 06 26 67 89 07 66
00000240  83 C6 02 66 83 C7 02 E2  EF 06 1F E8 CB 06 83 C4
00000250  04 66 5B BA 30 00 8E DA  8E D2 8E C2 66 8B E3 66
```

Page 1 of 549 | Offset: 0 | = 233 | Block: | n/a

[unregistriert]
bootmgr
\

File size: 325 KB
333,203 bytes
Valid data length: 333,203 bytes

[Read-only mode]

Creation time: 03/01/2009 07:22:11
Last write time: 01/19/2008 00:45:45
Last access time: 03/01/2009 07:22:11
Attributes: SHRA

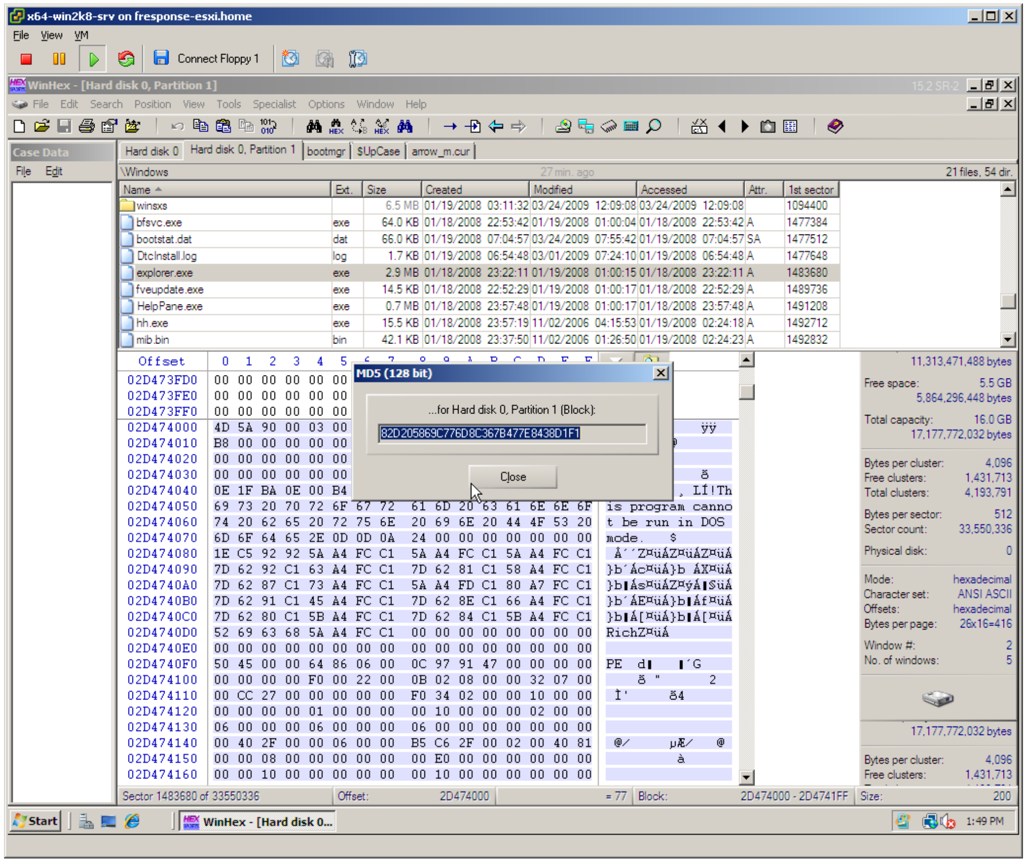
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 38x16=608

Window #: 3
No. of windows: 3

Clipboard: empty
TEMP folder: 5.4 GB free
I\ADMINI~1\LOCALS~1\Temp

Data Interpreter
8 Bit (±): -23
16 Bit (±): -10775
32 Bit (±): -352201239

Step 4, Select a single sector on the disk, select Tools->Compute Hash (MD5 128 bit), record the resulting hash value.



x64-win2k8-srv on fresponse-esxi.home
File View VM
Connect Floppy 1
WinHex - [Hard disk 0, Partition 1]
15.2 SR-2
File Edit Search Position View Tools Specialist Options Window Help
Case Data
File Edit
Hard disk 0 | Hard disk 0, Partition 1 | bootmgr | $UpCase | arrow_m.cur

\Windows — 27 min. ago — 21 files, 54 dir.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
winsxs		6.5 MB	01/19/2008 03:11:32	03/24/2009 12:09:08	03/24/2009 12:09:08		1094400
bfsvc.exe	exe	64.0 KB	01/18/2008 22:53:42	01/19/2008 01:00:04	01/18/2008 22:53:42	A	1477384
bootstat.dat	dat	66.0 KB	01/19/2008 07:04:57	03/24/2009 07:55:42	01/19/2008 07:04:57	SA	1477512
DtcInstall.log	log	1.7 KB	01/19/2008 06:54:48	03/01/2009 07:24:10	01/19/2008 06:54:48	A	1477648
explorer.exe	exe	2.9 MB	01/18/2008 23:22:11	01/19/2008 01:00:15	01/18/2008 23:22:11	A	1483680
fveupdate.exe	exe	14.5 KB	01/18/2008 22:52:29	01/19/2008 01:00:17	01/18/2008 22:52:29	A	1489736
HelpPane.exe	exe	0.7 MB	01/18/2008 23:57:48	01/19/2008 01:00:17	01/18/2008 23:57:48	A	1491208
hh.exe	exe	15.5 KB	01/18/2008 23:57:19	11/02/2006 04:15:53	01/19/2008 02:24:18	A	1492712
mib.bin	bin	42.1 KB	01/18/2008 23:37:50	11/02/2006 01:26:50	01/19/2008 02:24:23	A	1492832

```
  Offset    0  1  2  3  4  5
02D473FD0  00 00 00 00 00 00
02D473FE0  00 00 00 00 00 00
02D473FF0  00 00 00 00 00 00
02D474000  4D 5A 90 00 03 00                                   ÿÿ
02D474010  B8 00 00 00 00 00                                   @
02D474020  00 00 00 00 00 00
02D474030  00 00 00 00 00 00                                    ð
02D474040  0E 1F BA 0E 00 B4                               , LÍ!Th
02D474050  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
02D474060  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
02D474070  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode.   $
02D474080  1E C5 92 92 5A A4 FC C1  5A A4 FC C1 5A A4 FC C1   Å´´Z¤üÁZ¤üÁZ¤üÁ
02D474090  7D 62 92 C1 63 A4 FC C1  7D 62 81 C1 58 A4 FC C1  }b´Ác¤üÁ}b ÁX¤üÁ
02D4740A0  7D 62 87 C1 73 A4 FC C1  5A A4 FD C1 80 A7 FC C1  }b▮Ás¤üÁZ¤ýÁ▮§üÁ
02D4740B0  7D 62 91 C1 45 A4 FC C1  7D 62 8E C1 66 A4 FC C1  }b´ÁE¤üÁ}b▮Áf¤üÁ
02D4740C0  7D 62 80 C1 5B A4 FC C1  7D 62 84 C1 5B A4 FC C1  }b▮Á[¤üÁ}b▮Á[¤üÁ
02D4740D0  52 69 63 68 5A A4 FC C1  00 00 00 00 00 00 00 00  RichZ¤üÁ
02D4740E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02D4740F0  50 45 00 00 64 86 06 00  0C 97 91 47 00 00 00 00  PE  d▮   ▮´G
02D474100  00 00 00 00 F0 00 22 00  0B 02 08 00 00 32 07 00      ð "      2
02D474110  00 CC 27 00 00 00 00 00  F0 34 02 00 00 10 00 00   Ì'      ð4
02D474120  00 00 00 00 01 00 00 00  00 10 00 00 00 02 00 00
02D474130  06 00 00 00 06 00 00 00  06 00 00 00 00 00 00 00
02D474140  00 40 2F 00 00 06 00 00  B5 C6 2F 00 02 00 40 81   @⁄      µÆ⁄   @
02D474150  00 00 08 00 00 00 00 00  00 E0 00 00 00 00 00 00          à
02D474160  00 00 10 00 00 00 00 00  00 10 00 00 00 00 00 00
```

MD5 (128 bit)

...for Hard disk 0, Partition 1 (Block):

82D205869C776D8C367B477E8438D1F1

Close

11,313,471,488 bytes
Free space: 5.5 GB
5,864,296,448 bytes
Total capacity: 16.0 GB
17,177,772,032 bytes

Bytes per cluster: 4,096
Free clusters: 1,431,713
Total clusters: 4,193,791

Bytes per sector: 512
Sector count: 33,550,336

Physical disk: 0

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 26x16=416

Window #: 2
No. of windows: 5

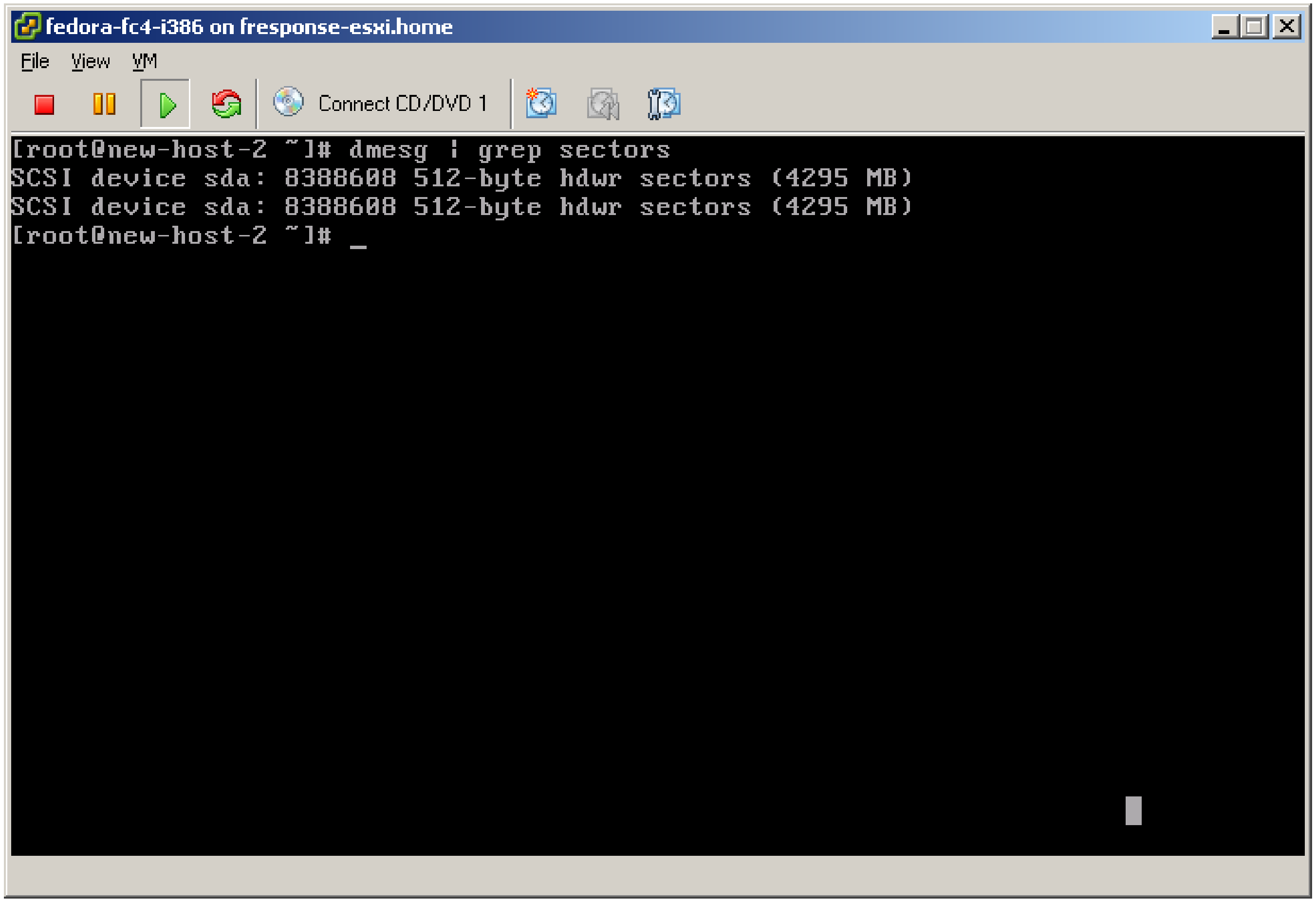
17,177,772,032 bytes

Bytes per cluster: 4,096
Free clusters: 1,431,713

Sector 1483680 of 33550336 | Offset: 2D474000 | = 77 | Block: 2D474000 - 2D4741FF | Size: 200

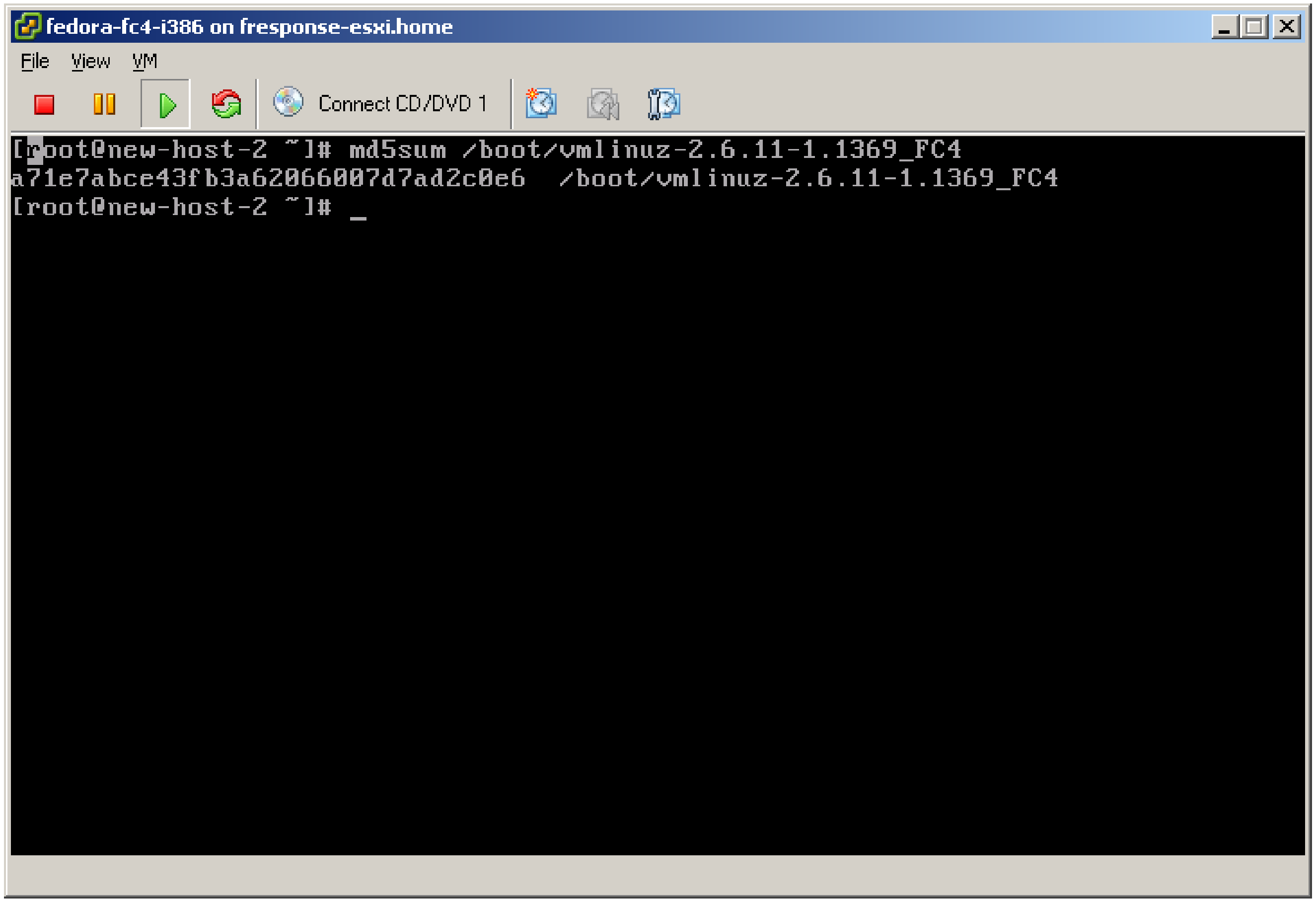
4.2 Obtain Baseline (Linux)

Step 1, Use “dmesg | grep sectors” to return the total number of sectors on the attached disk(s) and sector size.



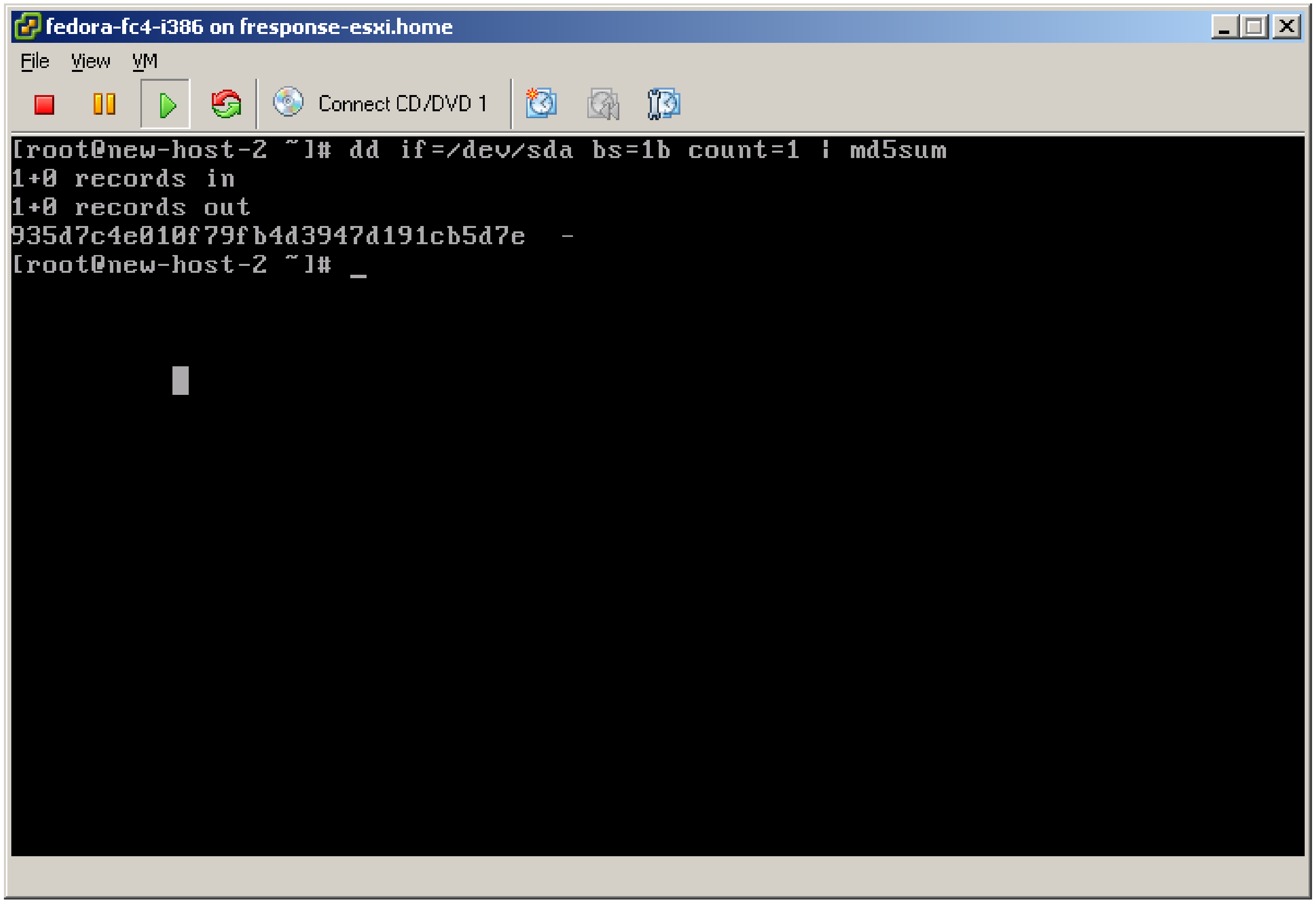
```
[root@new-host-2 ~]# dmesg ¦ grep sectors
SCSI device sda: 8388608 512-byte hdwr sectors (4295 MB)
SCSI device sda: 8388608 512-byte hdwr sectors (4295 MB)
[root@new-host-2 ~]# _
```

Step 2, Use "md5sum </path/to/file>" to return generate the hash of a relevant system file.



```
[root@new-host-2 ~]# md5sum /boot/vmlinuz-2.6.11-1.1369_FC4
a71e7abce43fb3a62066007d7ad2c0e6  /boot/vmlinuz-2.6.11-1.1369_FC4
[root@new-host-2 ~]# _
```

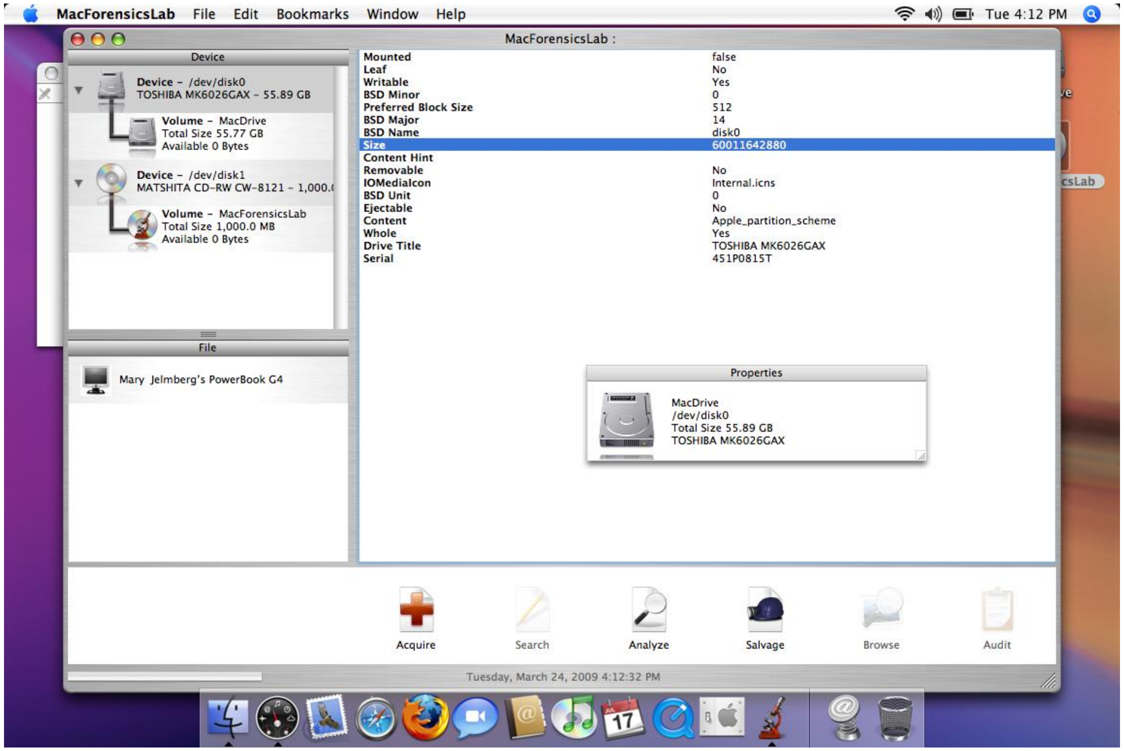
Step 3, Use “dd if=/dev/<disk> bs=1b count=1 | md5sum” to return generate the hash of a single sector on the disk.



```
[root@new-host-2 ~]# dd if=/dev/sda bs=1b count=1 | md5sum
1+0 records in
1+0 records out
935d7c4e010f79fb4d3947d191cb5d7e  -
[root@new-host-2 ~]# _
```

4.3 Obtain Baseline (Apple OS X)

Step 1, Use the SubRosaSoft MacForensicsLab to obtain total disk size in bytes and sector size in bytes.



Device – /dev/disk0
TOSHIBA MK6026GAX – 55.89 GB

Volume – MacDrive
Total Size 55.77 GB
Available 0 Bytes

Device – /dev/disk1
MATSHITA CD-RW CW-8121 – 1,000.(

Volume – MacForensicsLab
Total Size 1,000.0 MB
Available 0 Bytes

Mary Jelmberg's PowerBook G4

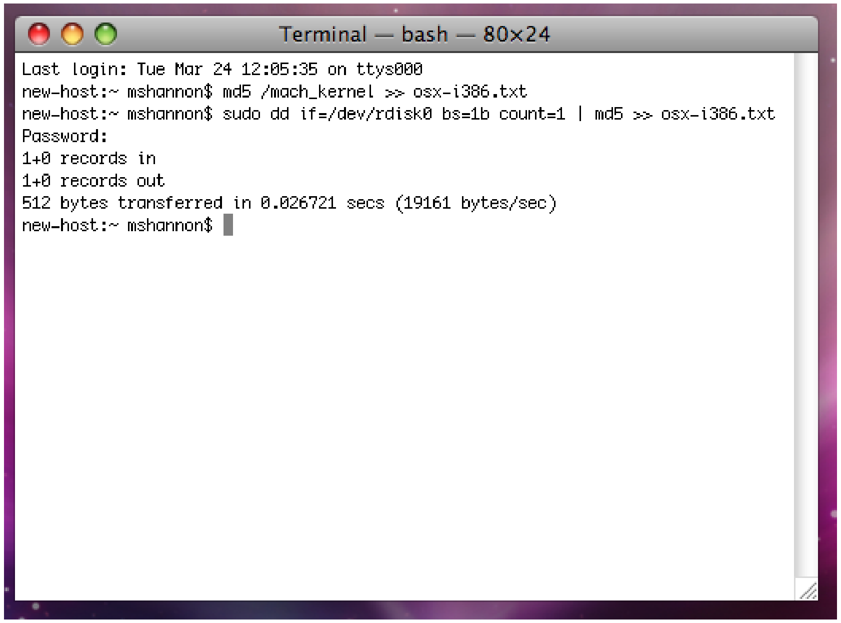
Mounted	false
Leaf	No
Writable	Yes
BSD Minor	0
Preferred Block Size	512
BSD Major	14
BSD Name	disk0
Size	60011642880
Content Hint	
Removable	No
IOMediaIcon	Internal.icns
BSD Unit	0
Ejectable	No
Content	Apple_partition_scheme
Whole	Yes
Drive Title	TOSHIBA MK6026GAX
Serial	451P0815T

Properties

MacDrive
/dev/disk0
Total Size 55.89 GB
TOSHIBA MK6026GAX

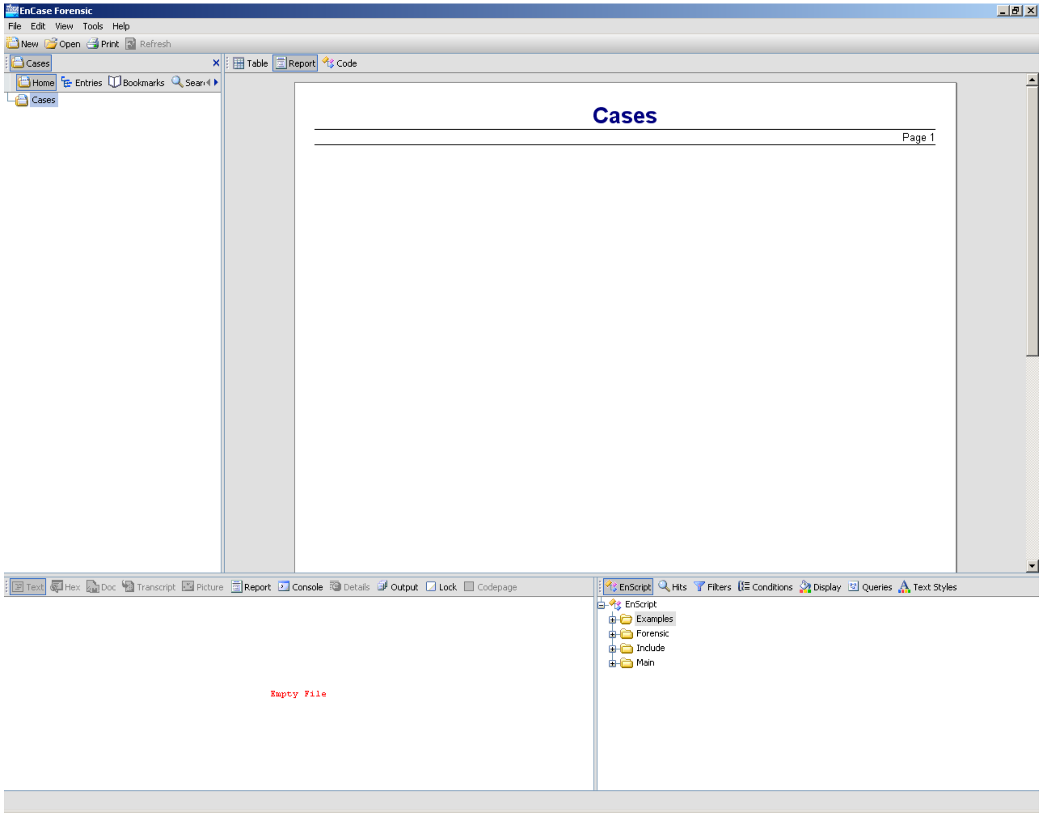
Tuesday, March 24, 2009 4:12:32 PM

Step 2, Open a Terminal window in Apple OS X and use the following commands to obtain file and data hashes "md5 <path/to/file>" and "dd if=/dev/rdisk0 bs=1b count=1 | md5".

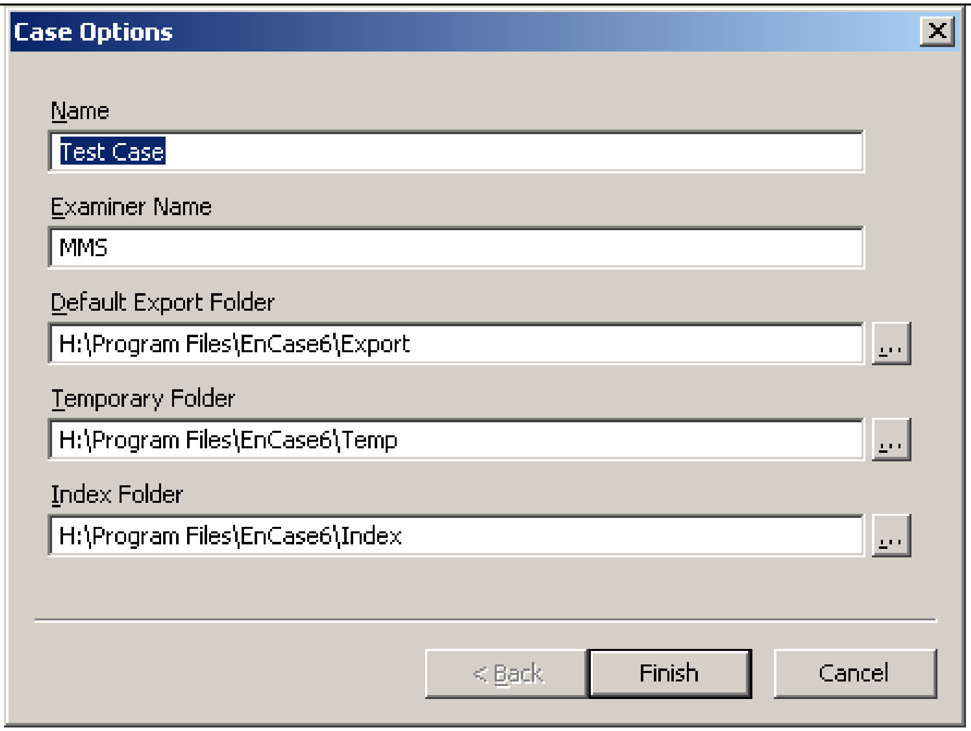


```
Last login: Tue Mar 24 12:05:35 on ttys000
new-host:~ mshannon$ md5 /mach_kernel >> osx-i386.txt
new-host:~ mshannon$ sudo dd if=/dev/rdisk0 bs=1b count=1 | md5 >> osx-i386.txt
Password:
1+0 records in
1+0 records out
512 bytes transferred in 0.026721 secs (19161 bytes/sec)
new-host:~ mshannon$ 
```

4.4 Disk Validity Testing – Encase


EnCase Forensic
File Edit View Tools Help
New Open Print Refresh
Cases
Home Entries Bookmarks Search
Cases
Table Report Code
Cases
Page 1
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage
Empty File
EnScript Hits Filters Conditions Display Queries Text Styles
EnScript
Examples
Forensic
Include
Main

Step 1, Open Encase Forensic Edition.



Case Options

Name
Test Case

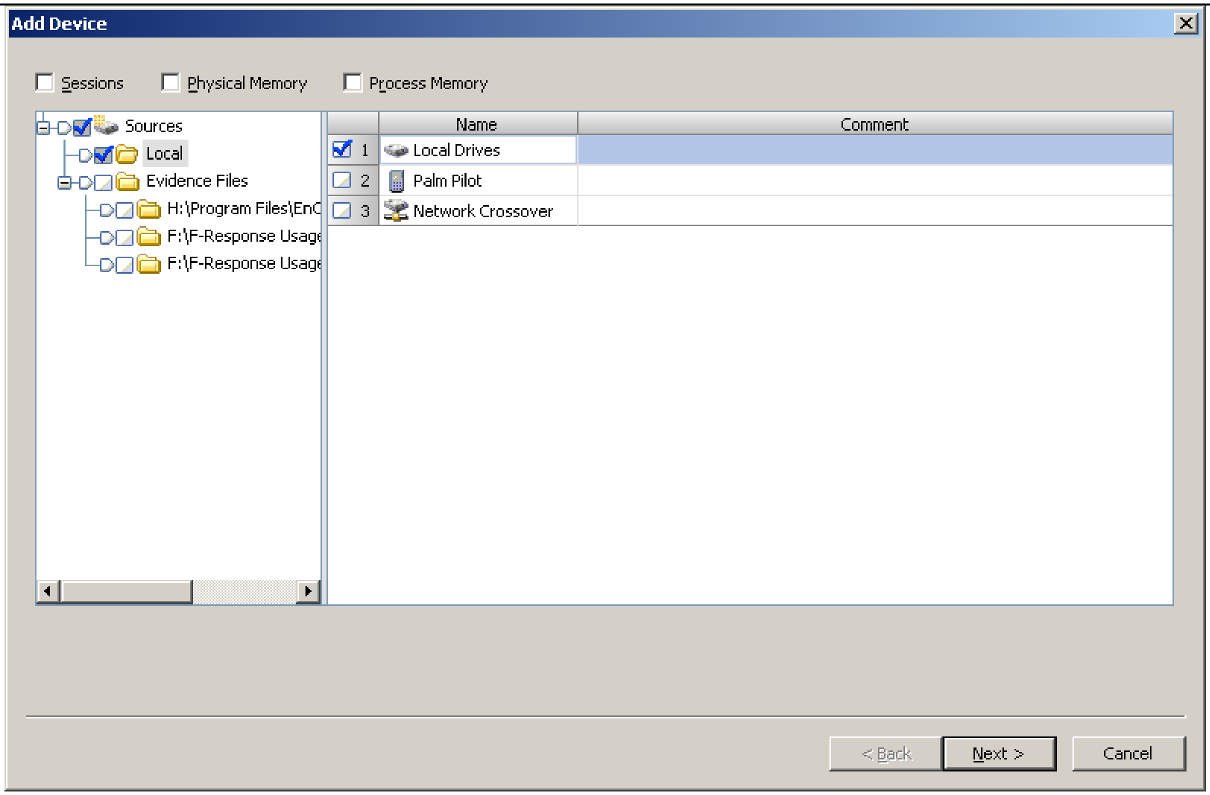
Examiner Name
MMS

Default Export Folder
H:\Program Files\EnCase6\Export

Temporary Folder
H:\Program Files\EnCase6\Temp

Index Folder
H:\Program Files\EnCase6\Index

Step 2, Create a new Encase Case File.



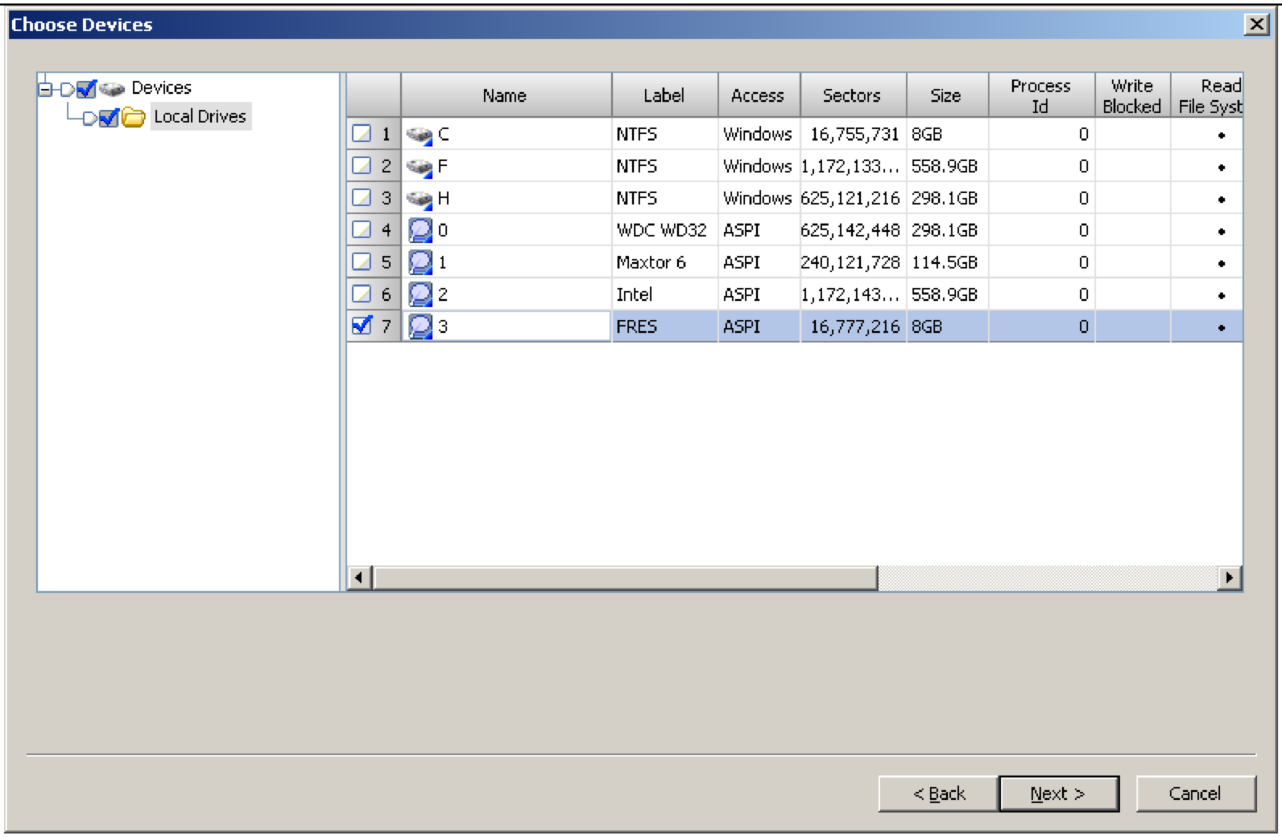
Add Device

□ Sessions □ Physical Memory □ Process Memory

- ☑ Sources
  - ☑ Local
  - □ Evidence Files
    - □ H:\Program Files\EnC
    - □ F:\F-Response Usag
    - □ F:\F-Response Usag

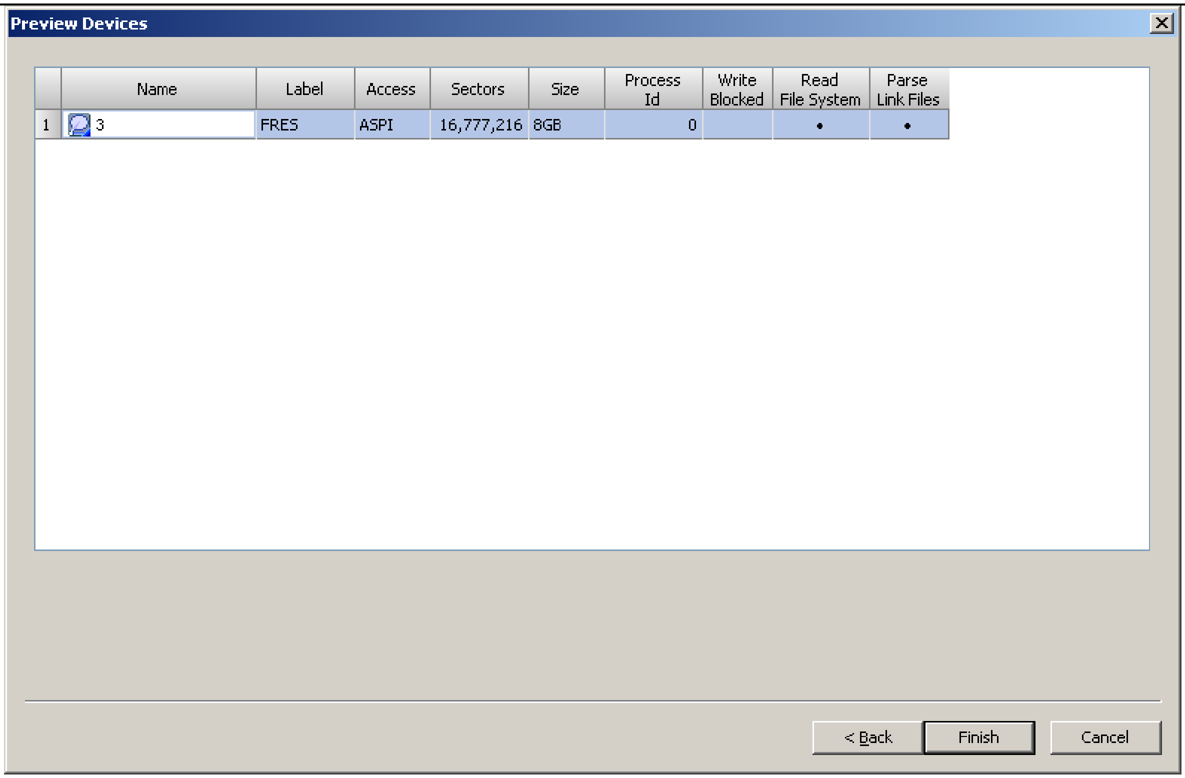
		Name	Comment
☑	1	Local Drives	
□	2	Palm Pilot	
□	3	Network Crossover	

Step 3, File->Add Device, select Local Drives



		Name	Label	Access	Sectors	Size	Process Id	Write Blocked	Read File Syst
☐	1	C	NTFS	Windows	16,755,731	8GB	0		•
☐	2	F	NTFS	Windows	1,172,133...	558.9GB	0		•
☐	3	H	NTFS	Windows	625,121,216	298.1GB	0		•
☐	4	0	WDC WD32	ASPI	625,142,448	298.1GB	0		•
☐	5	1	Maxtor 6	ASPI	240,121,728	114.5GB	0		•
☐	6	2	Intel	ASPI	1,172,143...	558.9GB	0		•
☑	7	3	FRES	ASPI	16,777,216	8GB	0		•

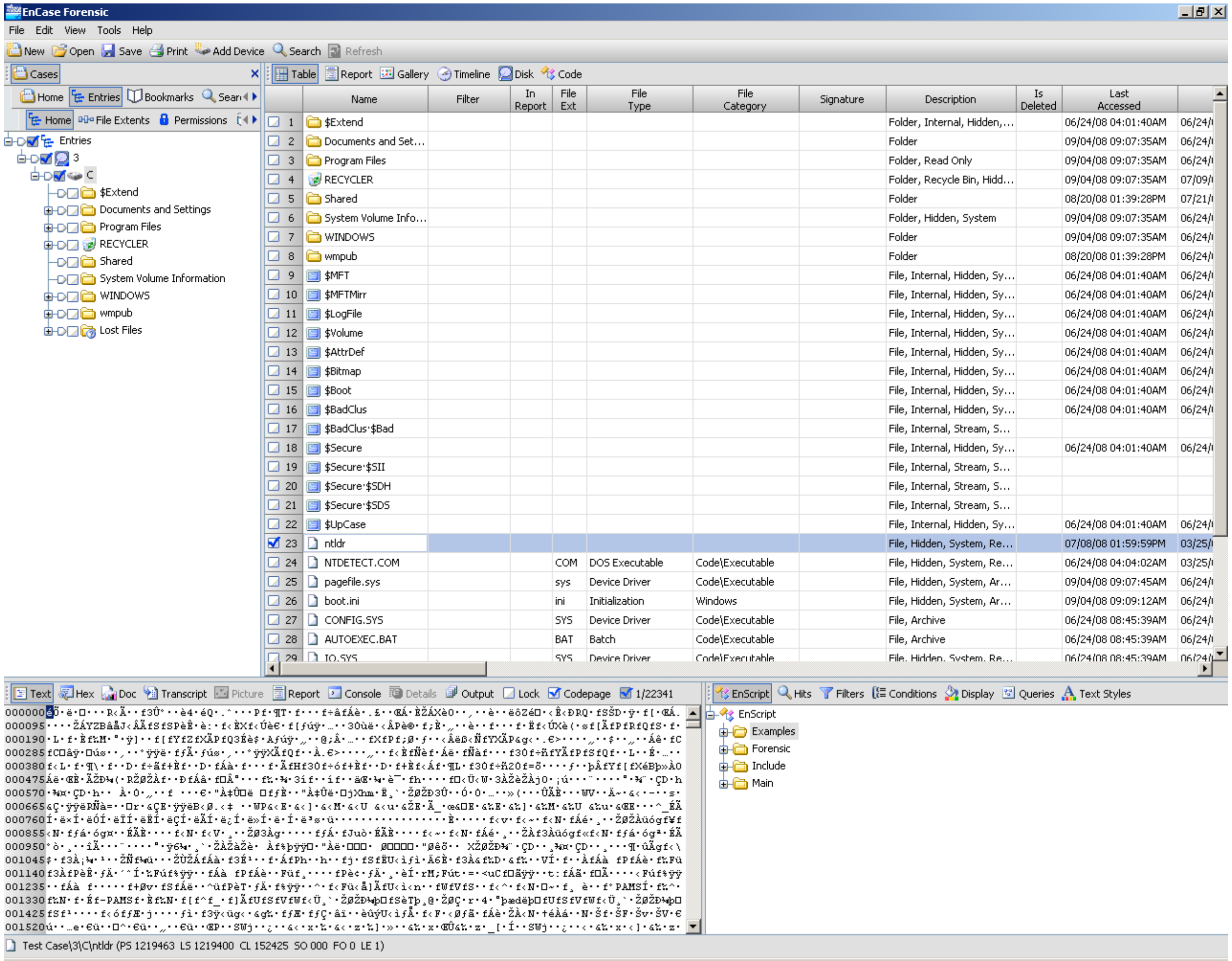
Step 4, Select FRES (F-Response Disk), Note Total Sectors.



	Name	Label	Access	Sectors	Size	Process Id	Write Blocked	Read File System	Parse Link Files
1	3	FRES	ASPI	16,777,216	8GB	0		•	•

Step 5, Press Next and Finish

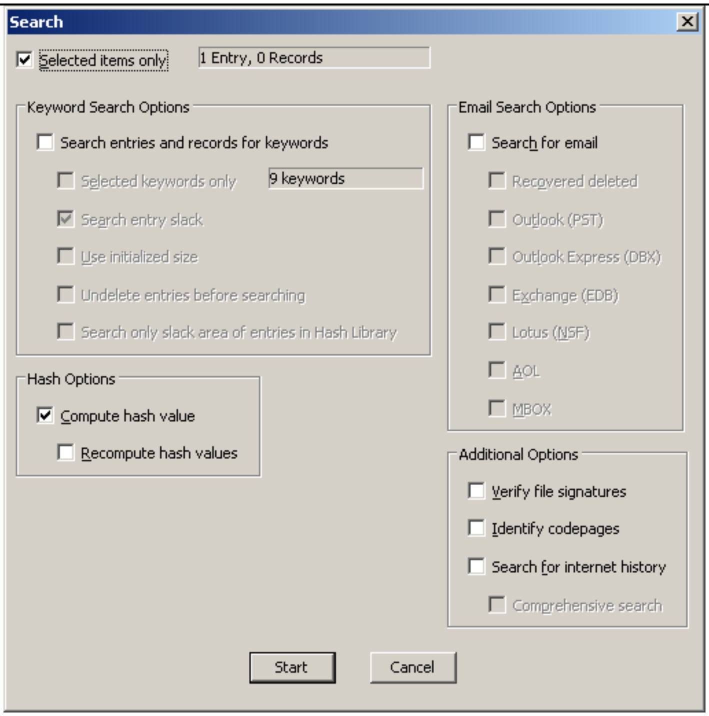
4.5 Read Accuracy Testing – Encase, X-Ways


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks Search
Home File Extents Permissions
Entries
3
C
$Extend
Documents and Settings
Program Files
RECYCLER
Shared
System Volume Information
WINDOWS
wmpub
Lost Files
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 1/22341
EnScript Hits Filters Conditions Display Queries Text Styles
EnScript
Examples
Forensic
Include
Main

		Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	
☐	1	$Extend							Folder, Internal, Hidden,…		06/24/08 04:01:40AM	06/24/
☐	2	Documents and Set…							Folder		09/04/08 09:07:35AM	06/24/
☐	3	Program Files							Folder, Read Only		09/04/08 09:07:35AM	06/24/
☐	4	RECYCLER							Folder, Recycle Bin, Hidd…		09/04/08 09:07:35AM	07/09/
☐	5	Shared							Folder		08/20/08 01:39:28PM	07/21/
☐	6	System Volume Info…							Folder, Hidden, System		09/04/08 09:07:35AM	06/24/
☐	7	WINDOWS							Folder		09/04/08 09:07:35AM	06/24/
☐	8	wmpub							Folder		08/20/08 01:39:28PM	06/24/
☐	9	$MFT							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	10	$MFTMirr							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	11	$LogFile							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	12	$Volume							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	13	$AttrDef							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	14	$Bitmap							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	15	$Boot							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	16	$BadClus							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	17	$BadClus·$Bad							File, Internal, Stream, S…			
☐	18	$Secure							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☐	19	$Secure·$SII							File, Internal, Stream, S…			
☐	20	$Secure·$SDH							File, Internal, Stream, S…			
☐	21	$Secure·$SDS							File, Internal, Stream, S…			
☐	22	$UpCase							File, Internal, Hidden, Sy…		06/24/08 04:01:40AM	06/24/
☑	23	ntldr							File, Hidden, System, Re…		07/08/08 01:59:59PM	03/25/
☐	24	NTDETECT.COM			COM	DOS Executable	Code\Executable		File, Hidden, System, Re…		06/24/08 04:04:02AM	03/25/
☐	25	pagefile.sys			sys	Device Driver	Code\Executable		File, Hidden, System, Ar…		09/04/08 09:07:45AM	06/24/
☐	26	boot.ini			ini	Initialization	Windows		File, Hidden, System, Ar…		09/04/08 09:09:12AM	06/24/
☐	27	CONFIG.SYS			SYS	Device Driver	Code\Executable		File, Archive		06/24/08 08:45:39AM	06/24/
☐	28	AUTOEXEC.BAT			BAT	Batch	Code\Executable		File, Archive		06/24/08 08:45:39AM	06/24/
☐	29	IO.SYS			SYS	Device Driver	Code\Executable		File, Hidden, System, Re…		06/24/08 08:45:39AM	06/24/

Test Case\3\C\ntldr (PS 1219463 LS 1219400 CL 152425 SO 000 FO 0 LE 1)

Step 1, Check File Hashing selected file from F-Response presented disk.



Search

☑ Selected items only — 1 Entry, 0 Records

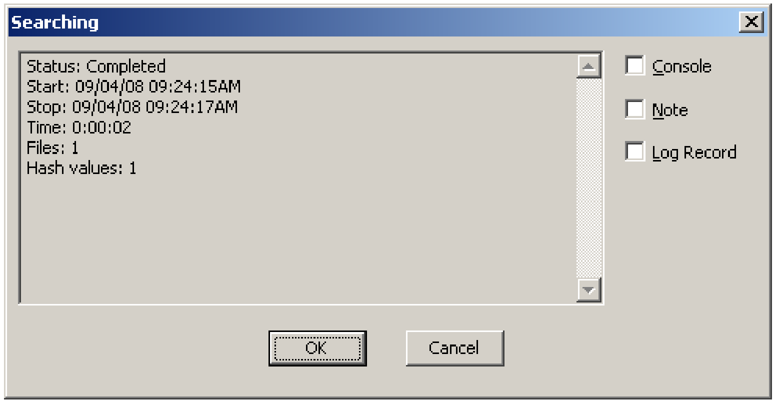
Keyword Search Options
- □ Search entries and records for keywords
- □ Selected keywords only — 9 keywords
- ☑ Search entry slack
- □ Use initialized size
- □ Undelete entries before searching
- □ Search only slack area of entries in Hash Library

Hash Options
- ☑ Compute hash value
- □ Recompute hash values

Email Search Options
- □ Search for email
- □ Recovered deleted
- □ Outlook (PST)
- □ Outlook Express (DBX)
- □ Exchange (EDB)
- □ Lotus (NSF)
- □ AOL
- □ MBOX

Additional Options
- □ Verify file signatures
- □ Identify codepages
- □ Search for internet history
- □ Comprehensive search

Step 2, Select Menu item Tools->Search, check Compute hash value and Selected items only

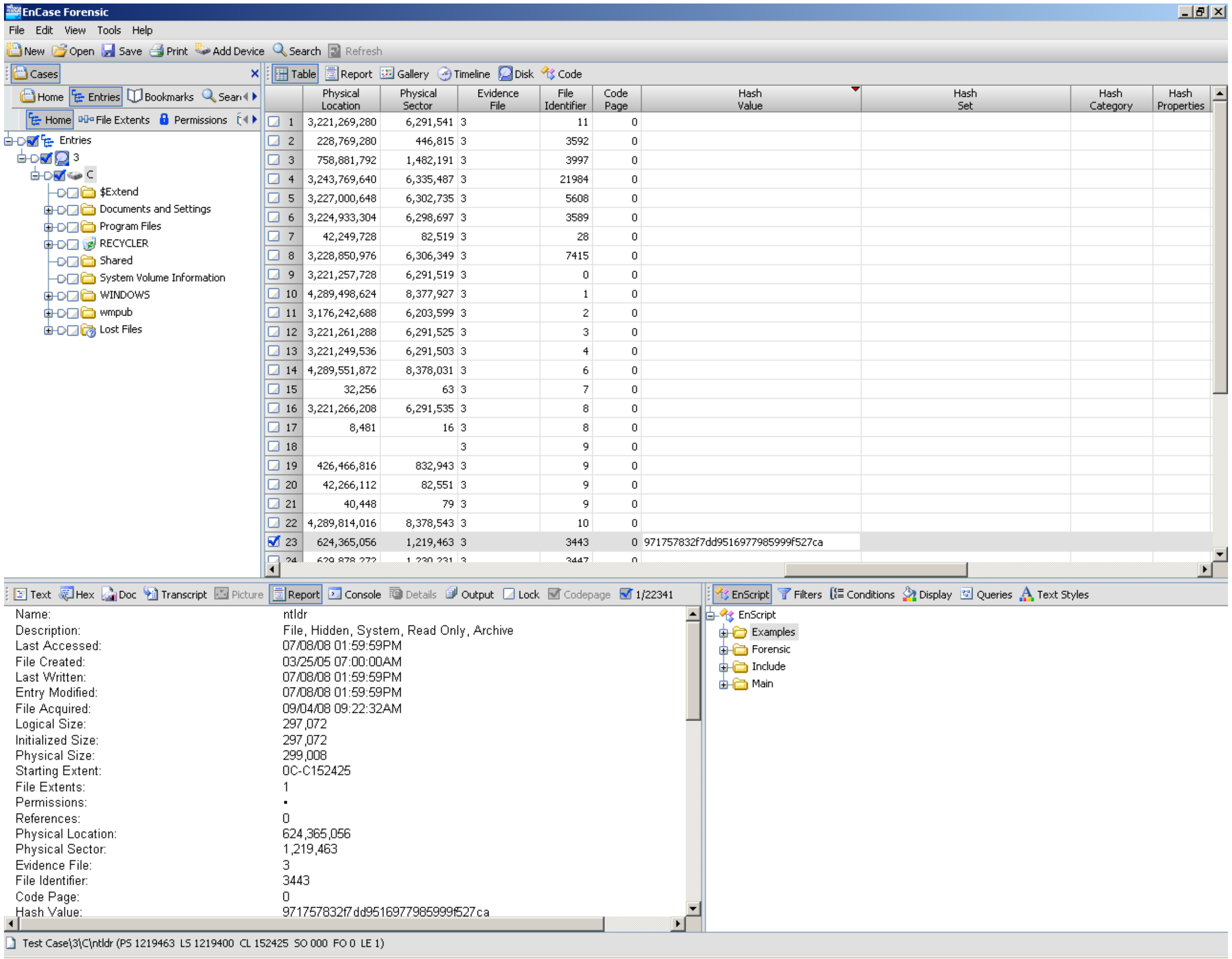


Searching

```
Status: Completed
Start: 09/04/08 09:24:15AM
Stop: 09/04/08 09:24:17AM
Time: 0:00:02
Files: 1
Hash values: 1
```

- □ Console
- □ Note
- □ Log Record

Step 3, Press OK when Searching is complete.

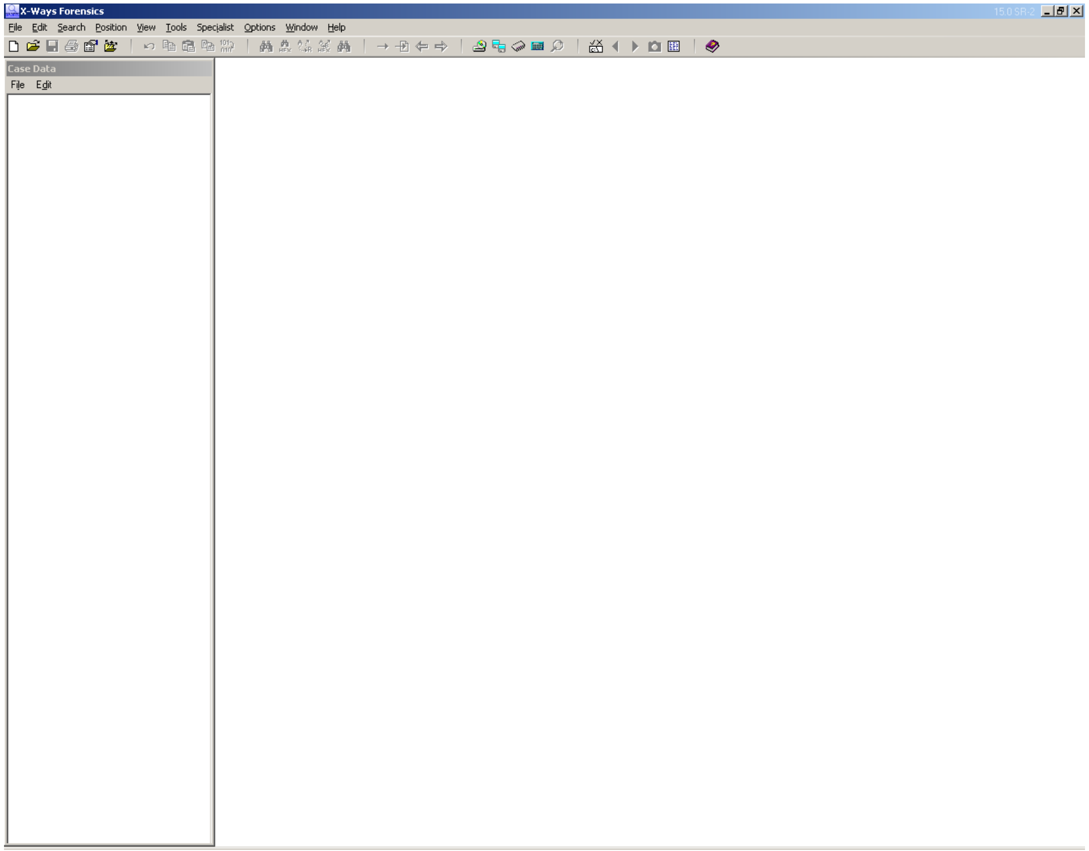

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search
Home File Extents Permissions
Entries
3
C
$Extend
Documents and Settings
Program Files
RECYCLER
Shared
System Volume Information
WINDOWS
wmpub
Lost Files
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 1/22341
EnScript Filters Conditions Display Queries Text Styles
EnScript
Examples
Forensic
Include
Main

		Physical Location	Physical Sector	Evidence File	File Identifier	Code Page	Hash Value	Hash Set	Hash Category	Hash Properties
□	1	3,221,269,280	6,291,541	3	11	0				
□	2	228,769,280	446,815	3	3592	0				
□	3	758,881,792	1,482,191	3	3997	0				
□	4	3,243,769,640	6,335,487	3	21984	0				
□	5	3,227,000,648	6,302,735	3	5608	0				
□	6	3,224,933,304	6,298,697	3	3589	0				
□	7	42,249,728	82,519	3	28	0				
□	8	3,228,850,976	6,306,349	3	7415	0				
□	9	3,221,257,728	6,291,519	3	0	0				
□	10	4,289,498,624	8,377,927	3	1	0				
□	11	3,176,242,688	6,203,599	3	2	0				
□	12	3,221,261,288	6,291,525	3	3	0				
□	13	3,221,249,536	6,291,503	3	4	0				
□	14	4,289,551,872	8,378,031	3	6	0				
□	15	32,256	63	3	7	0				
□	16	3,221,266,208	6,291,535	3	8	0				
□	17	8,481	16	3	8	0				
□	18			3	9	0				
□	19	426,466,816	832,943	3	9	0				
□	20	42,266,112	82,551	3	9	0				
□	21	40,448	79	3	9	0				
□	22	4,289,814,016	8,378,543	3	10	0				
☑	23	624,365,056	1,219,463	3	3443	0	971757832f7dd9516977985999f527ca			
□	24	629,878,272	1,230,231	3	3447	0				

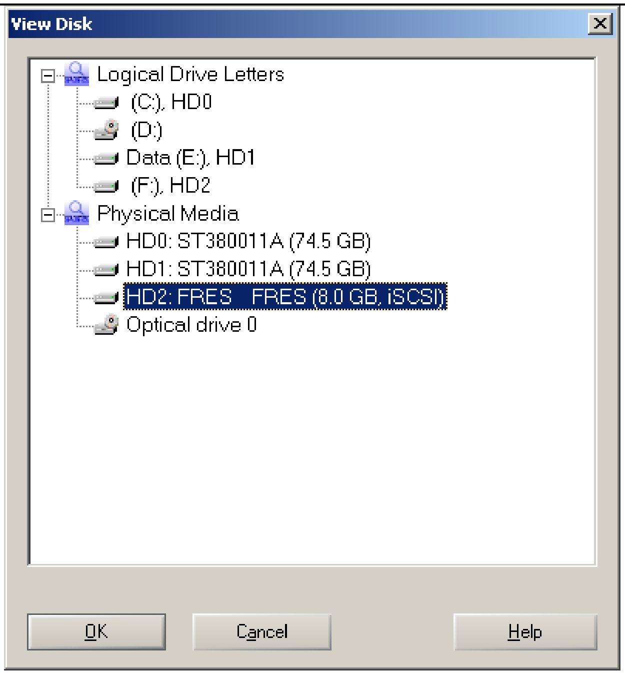
Name: ntldr
Description: File, Hidden, System, Read Only, Archive
Last Accessed: 07/08/08 01:59:59PM
File Created: 03/25/05 07:00:00AM
Last Written: 07/08/08 01:59:59PM
Entry Modified: 07/08/08 01:59:59PM
File Acquired: 09/04/08 09:22:32AM
Logical Size: 297,072
Initialized Size: 297,072
Physical Size: 299,008
Starting Extent: 0C-C152425
File Extents: 1
Permissions: •
References: 0
Physical Location: 624,365,056
Physical Sector: 1,219,463
Evidence File: 3
File Identifier: 3443
Code Page: 0
Hash Value: 971757832f7dd9516977985999f527ca

Test Case\3\C\ntldr (PS 1219463 LS 1219400 CL 152425 SO 000 FO 0 LE 1)

Step 4, Review and record the resulting hash value.


X-Ways Forensics
File Edit Search Position View Tools Specialist Options Window Help
Case Data
File Edit

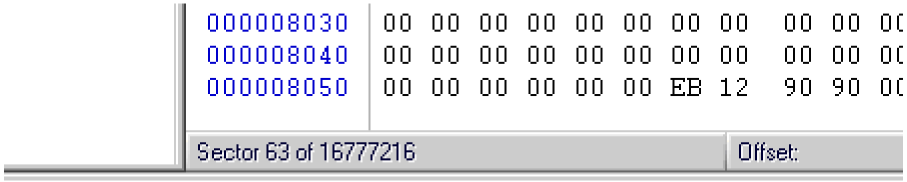
Step 5, Open X-Ways Forensics



View Disk

- Logical Drive Letters
  - (C:), HD0
  - (D:)
  - Data (E:), HD1
  - (F:), HD2
- Physical Media
  - HD0: ST380011A (74.5 GB)
  - HD1: ST380011A (74.5 GB)
  - HD2: FRES   FRES (8.0 GB, iSCSI)
  - Optical drive 0

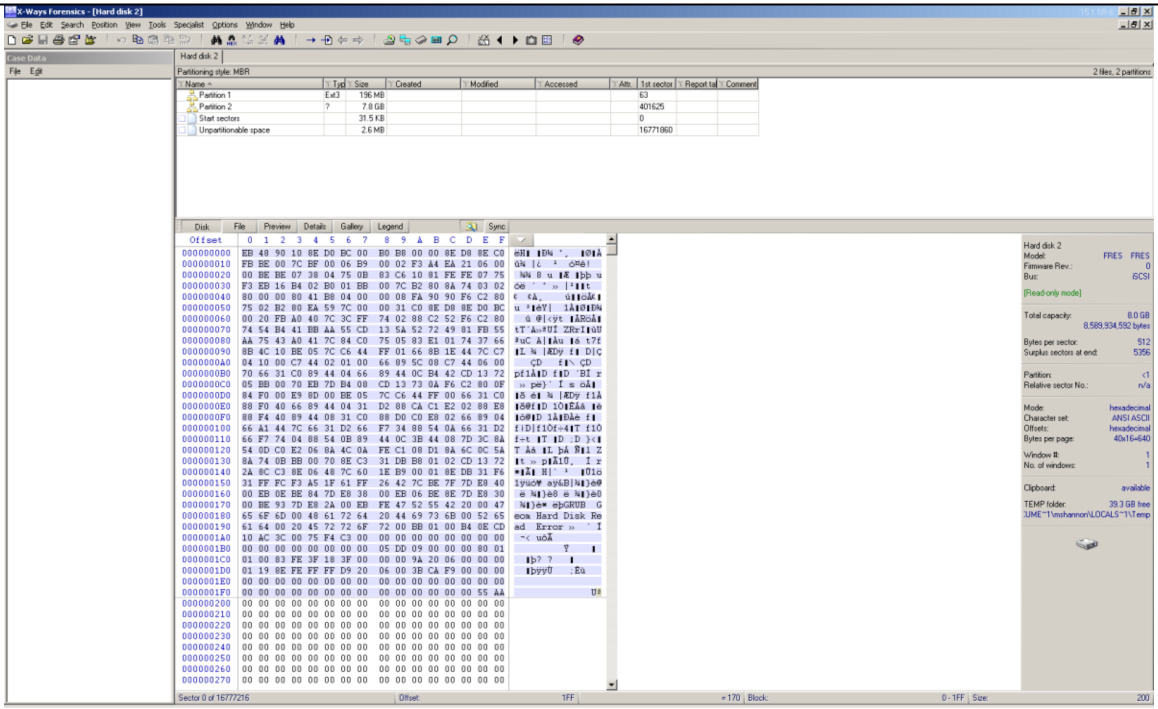
Step 2, Select Tools->Open Disk, Select the FRES disk, press OK



```
000008030  00 00 00 00 00 00 00 00  00 00 0(
000008040  00 00 00 00 00 00 00 00  00 00 0(
000008050  00 00 00 00 00 00 EB 12  90 90 0(
```

Sector 63 of 16777216   Offset:

Step 3, Note total sector size.



X-Ways Forensics - [Hard disk 2]
File Edit Search Position View Tools Specialist Options Window Help
Case Data
File Edit
Hard disk 2
Disk File Preview Details Gallery Legend Sync

Partitioning style: MBR

2 files, 2 partitions

Name	Typ	Size	Created	Modified	Accessed	Attr.	1st sector	Report tal	Comment
Partition 1	Ext3	196 MB					63		
Partition 2	?	7.8 GB					401625		
Start sectors		31.5 KB					0		
Unpartitionable space		2.6 MB					16771860		

```
   Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000  EB 48 90 10 8E D0 BC 00  B0 B8 00 00 8E D8 8E C0
000000010  FB BE 00 7C BF 00 06 B9  00 02 F3 A4 EA 21 06 00
000000020  00 BE BE 07 38 04 75 0B  83 C6 10 81 FE FE 07 75
000000030  F3 EB 16 B4 02 B0 01 BB  00 7C B2 80 8A 74 03 02
000000040  80 00 00 80 41 B8 04 00  00 08 FA 90 90 F6 C2 80
000000050  75 02 B2 80 EA 59 7C 00  00 31 C0 8E D8 8E D0 BC
000000060  00 20 FB A0 40 7C 3C FF  74 02 88 C2 52 F6 C2 80
000000070  74 54 B4 41 BB AA 55 CD  13 5A 52 72 49 81 FB 55
000000080  AA 75 43 A0 41 7C 84 C0  75 05 83 E1 01 74 37 66
000000090  8B 4C 10 BE 05 7C C6 44  FF 01 66 8B 1E 44 7C C7
0000000A0  04 10 00 C7 44 02 01 00  66 89 5C 08 C7 44 06 00
0000000B0  70 66 31 C0 89 44 04 66  89 44 0C B4 42 CD 13 72
0000000C0  05 BB 00 70 EB 7D B4 08  CD 13 73 0A F6 C2 80 0F
0000000D0  84 F0 00 E9 8D 00 BE 05  7C C6 44 FF 00 66 31 C0
0000000E0  88 F0 40 66 89 44 04 31  D2 88 CA C1 E2 02 88 E8
0000000F0  88 F4 40 89 44 08 31 C0  88 D0 C0 E8 02 66 89 04
000000100  66 A1 44 7C 66 31 D2 66  F7 34 88 54 0A 66 31 D2
000000110  66 F7 74 04 88 54 0B 89  44 0C 3B 44 08 7D 3C 8A
000000120  54 0D C0 E2 06 8A 4C 0A  FE C1 08 D1 8A 6C 0C 5A
000000130  8A 74 0B BB 00 70 8E C3  31 DB B8 01 02 CD 13 72
000000140  2A 8C C3 8E 06 48 7C 60  1E B9 00 01 8E DB 31 F6
000000150  31 FF FC F3 A5 1F 61 FF  26 42 7C BE 7F 7D E8 40
000000160  00 EB 0E BE 84 7D E8 38  00 EB 06 BE 8E 7D E8 30
000000170  00 BE 93 7D E8 2A 00 EB  FE 47 52 55 42 20 00 47
000000180  65 6F 6D 00 48 61 72 64  20 44 69 73 6B 00 52 65
000000190  61 64 00 20 45 72 72 6F  72 00 BB 01 00 B4 0E CD
0000001A0  10 AC 3C 00 75 F4 C3 00  00 00 00 00 00 00 00 00
0000001B0  00 00 00 00 00 00 00 00  05 DD 09 00 00 00 80 01
0000001C0  01 00 83 FE 3F 18 3F 00  00 00 9A 20 06 00 00 00
0000001D0  01 19 8E FE FF FF D9 20  06 00 3B CA F9 00 00 00
0000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA
000000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000250  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000260  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000270  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Hard disk 2
Model: FRES FRES
Firmware Rev.: 0
Bus: iSCSI
[Read-only mode]

Total capacity: 8.0 GB
8,589,934,592 bytes

Bytes per sector: 512
Surplus sectors at end: 5356

Partition: <1
Relative sector No.: n/a

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 40x16=640

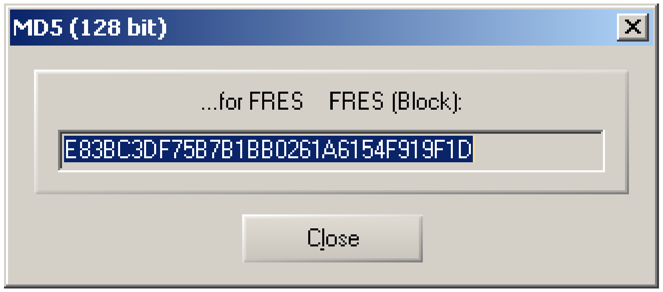
Window #: 1
No. of windows: 1

Clipboard: available

TEMP folder: 39.3 GB free
:UME~1\mshannon\LOCALS~1\Temp

Sector 0 of 16777216 | Offset: 1FF | = 170 | Block: 0 - 1FF | Size: 200

Step 4, Select the sector of disk hashed previously during the baseline gathering phase. Press Ctrl-F2 to bring up the hashing dialog.

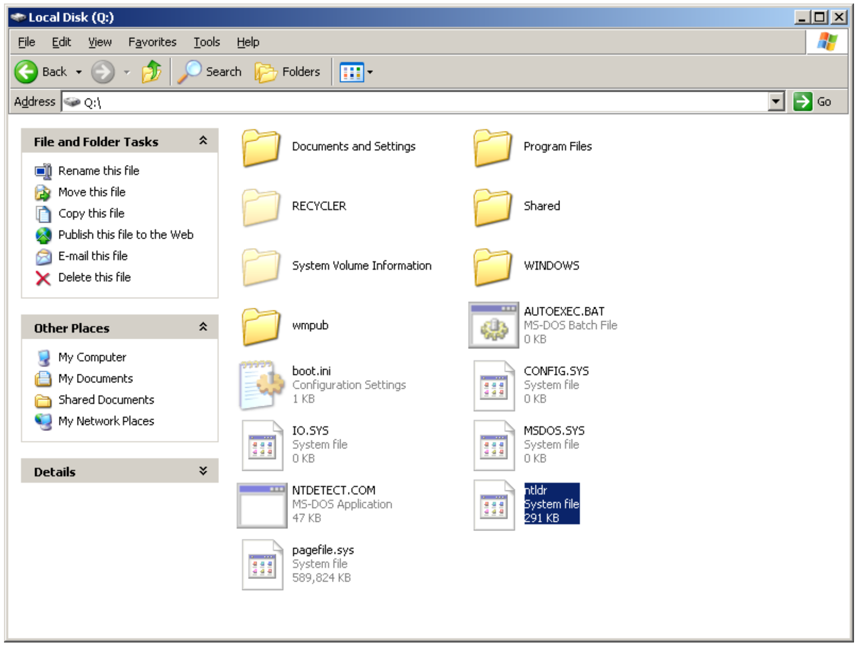


...for FRES FRES (Block):

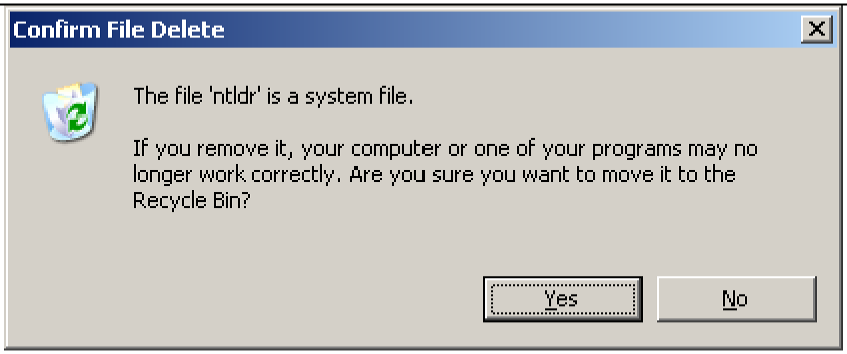
E83BC3DF75B7B1BB0261A6154F919F1D

Step 5, Select MD5 as the hashing type and press Ok, record and compare resulting hash with hash obtained during baseline operation.

4.6 Write Prevention Testing – Windows



Step 1, Open newly mounted F-Response Disk, select the ntldr or bootmgr file.

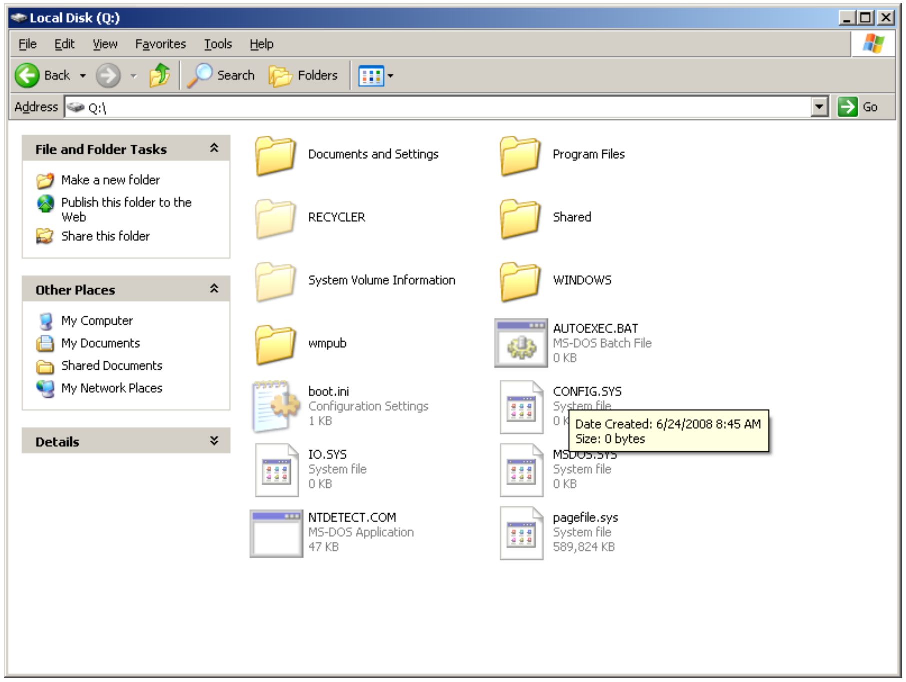


Confirm File Delete

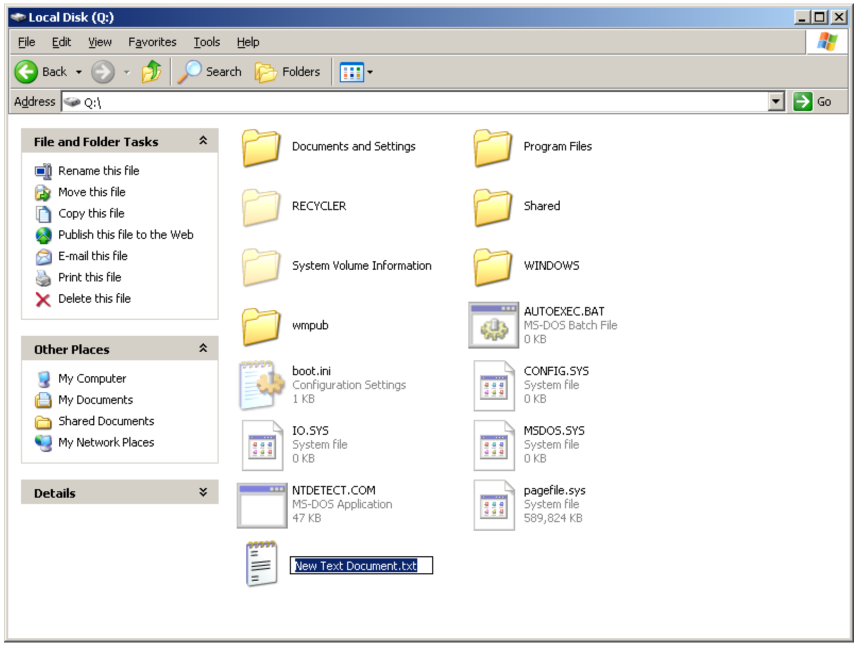
The file 'ntldr' is a system file.

If you remove it, your computer or one of your programs may no longer work correctly. Are you sure you want to move it to the Recycle Bin?

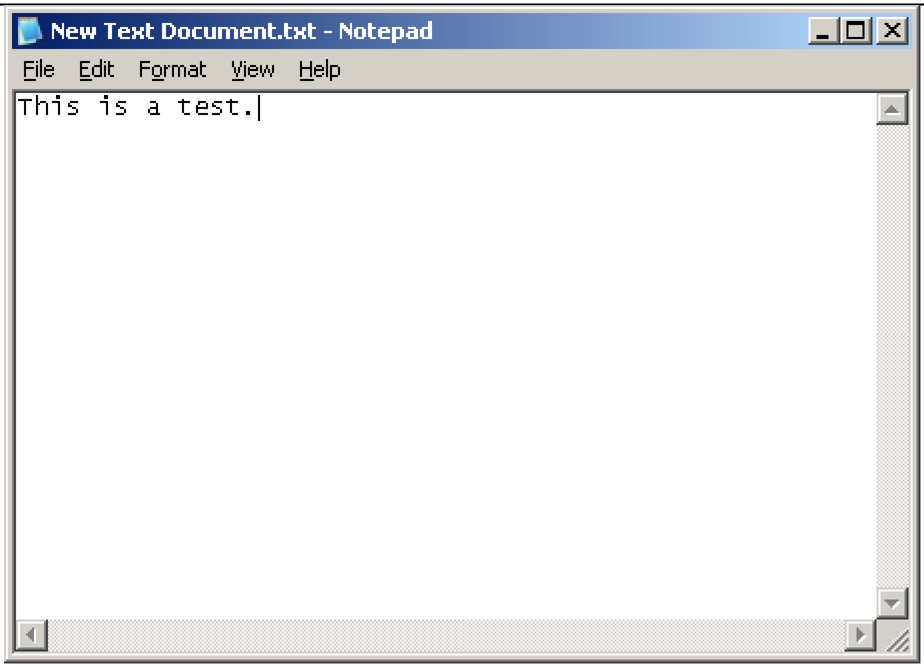
Step 2, Right click and select delete. Press Yes to delete



Step 3, Confirm system response of File deleted successfully.

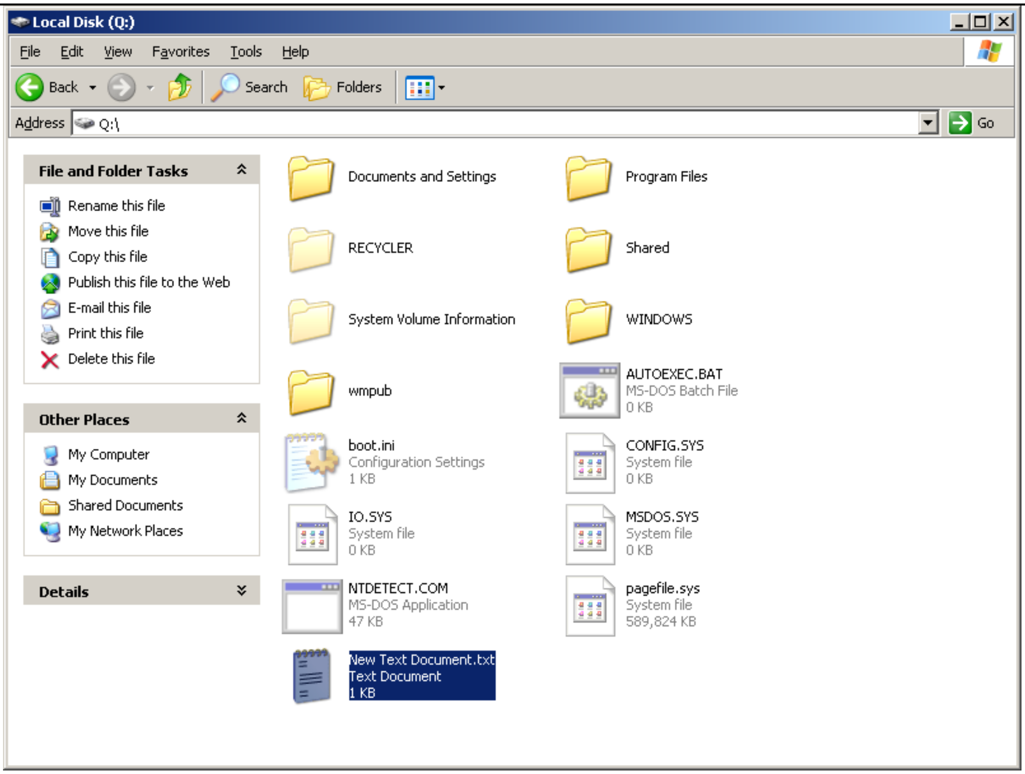


Step 4, Create new file, right click and create new Text Document.

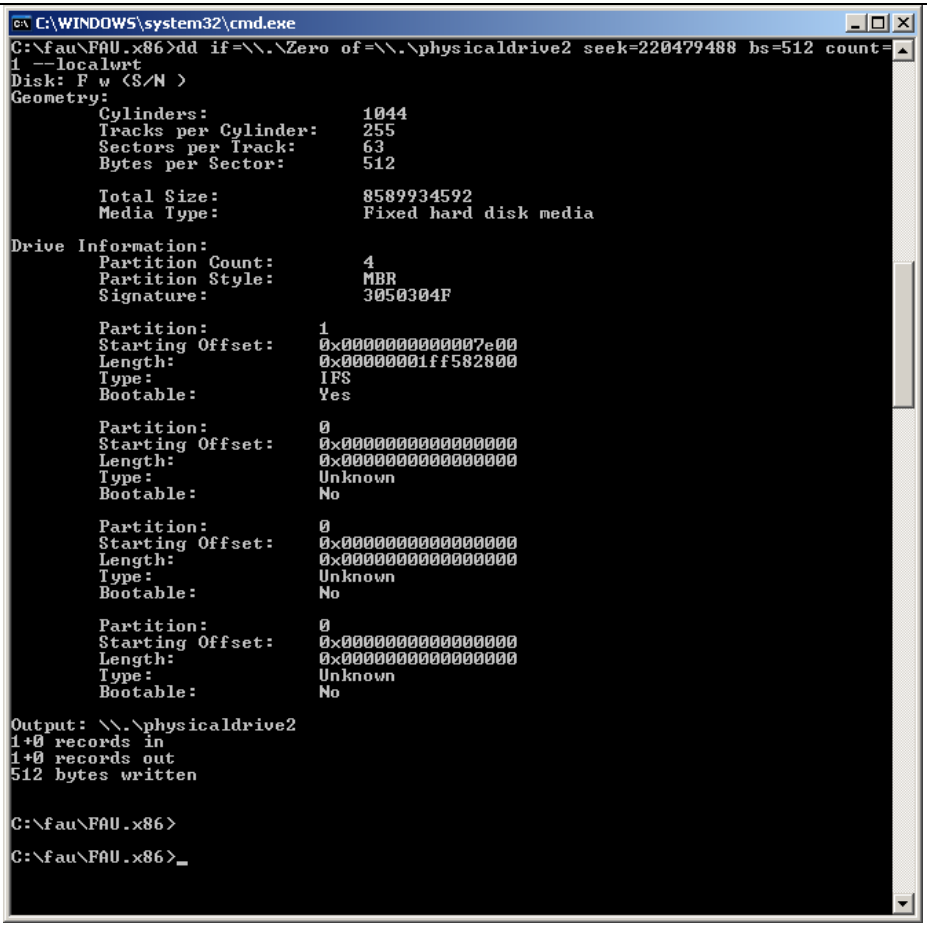


This is a test.

Step 5, Open new text document, add arbitrary content, save and close.

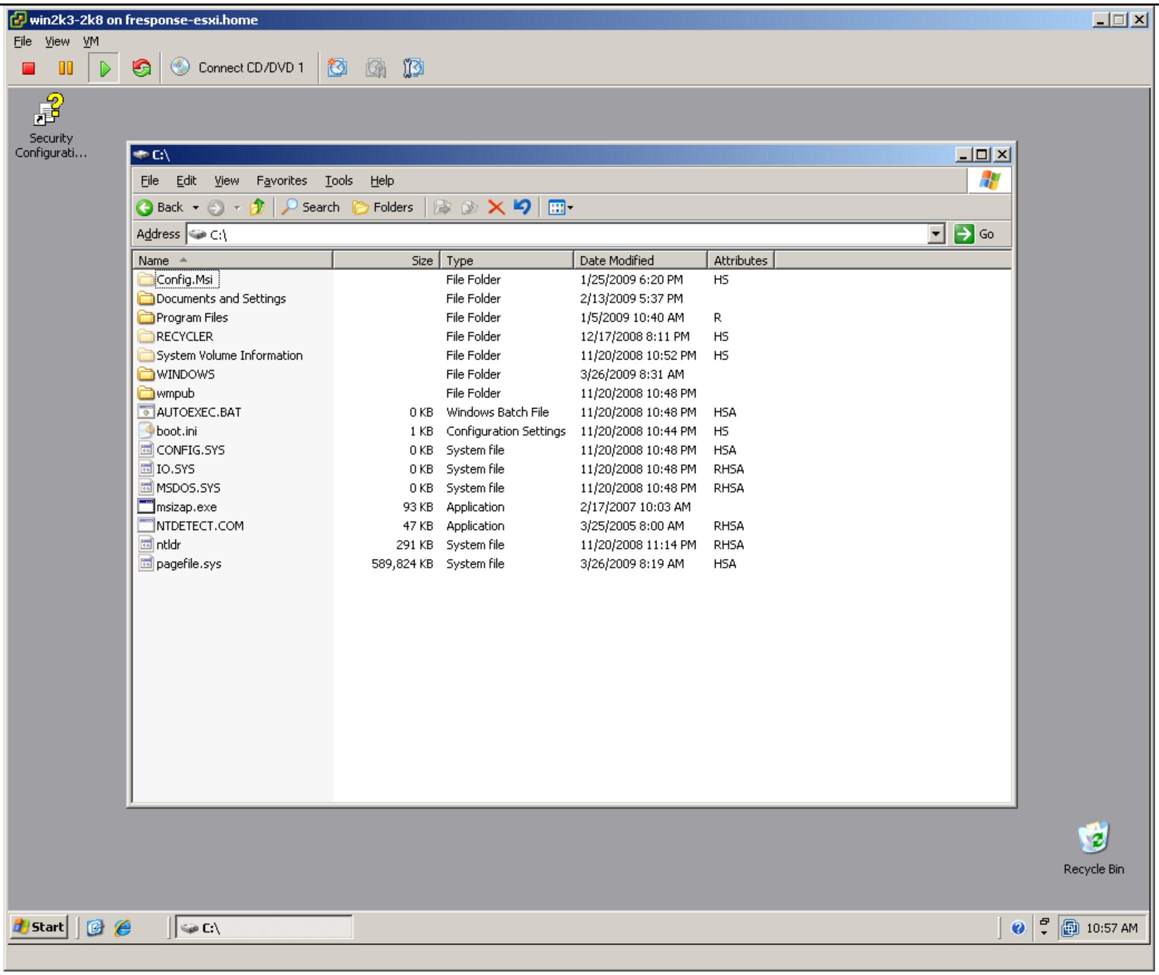

Local Disk (Q:)
File Edit View Favorites Tools Help
Back Search Folders
Address Q:\ Go
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Print this file
Delete this file
Other Places
My Computer
My Documents
Shared Documents
My Network Places
Details
Documents and Settings
Program Files
RECYCLER
Shared
System Volume Information
WINDOWS
wmpub
AUTOEXEC.BAT MS-DOS Batch File 0 KB
boot.ini Configuration Settings 1 KB
CONFIG.SYS System file 0 KB
IO.SYS System file 0 KB
MSDOS.SYS System file 0 KB
NTDETECT.COM MS-DOS Application 47 KB
pagefile.sys System file 589,824 KB
New Text Document.txt Text Document 1 KB

Step 6, Confirm system response of File created successfully.



```
C:\fau\FAU.x86>dd if=\\.\Zero of=\\.\physicaldrive2 seek=220479488 bs=512 count=
1 --localwrt
Disk: F w (S/N )
Geometry:
        Cylinders:                1044
        Tracks per Cylinder:      255
        Sectors per Track:        63
        Bytes per Sector:         512

        Total Size:               8589934592
        Media Type:               Fixed hard disk media

Drive Information:
        Partition Count:          4
        Partition Style:          MBR
        Signature:                3050304F

        Partition:            1
        Starting Offset:      0x0000000000007e00
        Length:               0x00000001ff582800
        Type:                 IFS
        Bootable:             Yes

        Partition:            0
        Starting Offset:      0x0000000000000000
        Length:               0x0000000000000000
        Type:                 Unknown
        Bootable:             No

        Partition:            0
        Starting Offset:      0x0000000000000000
        Length:               0x0000000000000000
        Type:                 Unknown
        Bootable:             No

        Partition:            0
        Starting Offset:      0x0000000000000000
        Length:               0x0000000000000000
        Type:                 Unknown
        Bootable:             No

Output: \\.\physicaldrive2
1+0 records in
1+0 records out
512 bytes written


C:\fau\FAU.x86>

C:\fau\FAU.x86>_
```

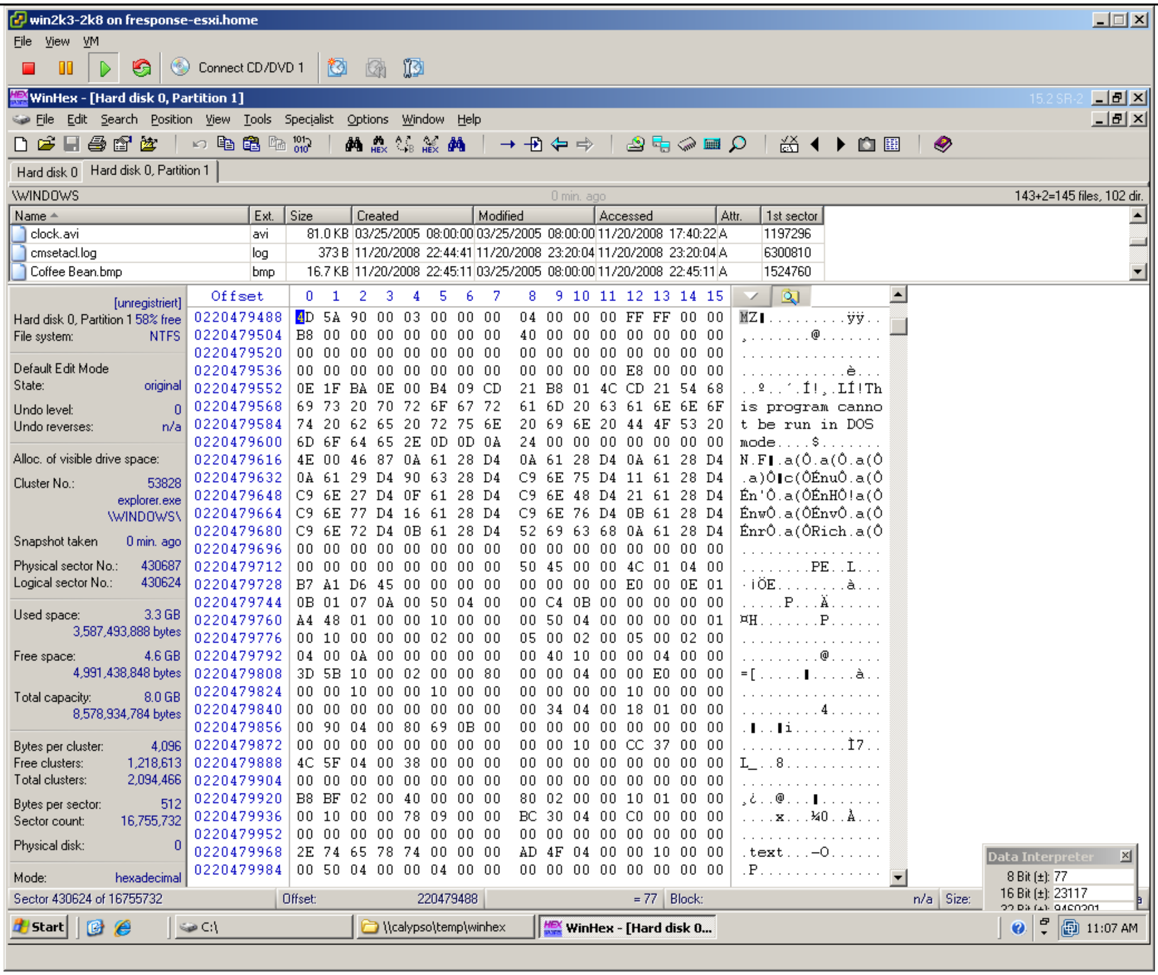
Step 7, Open FAU DD, use DD command to write zeros to arbitrary sector on disk.



Address C:\

Name	Size	Type	Date Modified	Attributes
Config.Msi		File Folder	1/25/2009 6:20 PM	HS
Documents and Settings		File Folder	2/13/2009 5:37 PM	
Program Files		File Folder	1/5/2009 10:40 AM	R
RECYCLER		File Folder	12/17/2008 8:11 PM	HS
System Volume Information		File Folder	11/20/2008 10:52 PM	HS
WINDOWS		File Folder	3/26/2009 8:31 AM	
wmpub		File Folder	11/20/2008 10:48 PM	
AUTOEXEC.BAT	0 KB	Windows Batch File	11/20/2008 10:48 PM	HSA
boot.ini	1 KB	Configuration Settings	11/20/2008 10:44 PM	HS
CONFIG.SYS	0 KB	System file	11/20/2008 10:48 PM	HSA
IO.SYS	0 KB	System file	11/20/2008 10:48 PM	RHSA
MSDOS.SYS	0 KB	System file	11/20/2008 10:48 PM	RHSA
msizap.exe	93 KB	Application	2/17/2007 10:03 AM	
NTDETECT.COM	47 KB	Application	3/25/2005 8:00 AM	RHSA
ntldr	291 KB	System file	11/20/2008 11:14 PM	RHSA
pagefile.sys	589,824 KB	System file	3/26/2009 8:19 AM	HSA

Step 7, Return to F-Response testing computer, confirm no data changes have occurred.



win2k3-2k8 on fresponse-esxi.home

WinHex - [Hard disk 0, Partition 1]

Hard disk 0 | Hard disk 0, Partition 1

\WINDOWS — 0 min. ago — 143+2=145 files, 102 dir.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
clock.avi	avi	81.0 KB	03/25/2005 08:00:00	03/25/2005 08:00:00	11/20/2008 17:40:22	A	1197296
cmsetacl.log	log	373 B	11/20/2008 22:44:41	11/20/2008 23:20:04	11/20/2008 23:20:04	A	6300810
Coffee Bean.bmp	bmp	16.7 KB	11/20/2008 22:45:11	03/25/2005 08:00:00	11/20/2008 22:45:11	A	1524760

	[unregistriert]
Hard disk 0, Partition 1	58% free
File system:	NTFS
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Alloc. of visible drive space:	
Cluster No.:	53828
	explorer.exe
	\WINDOWS\
Snapshot taken	0 min. ago
Physical sector No.:	430687
Logical sector No.:	430624
Used space:	3.3 GB
	3,587,493,888 bytes
Free space:	4.6 GB
	4,991,438,848 bytes
Total capacity:	8.0 GB
	8,578,934,784 bytes
Bytes per cluster:	4,096
Free clusters:	1,218,613
Total clusters:	2,094,466
Bytes per sector:	512
Sector count:	16,755,732
Physical disk:	0
Mode:	hexadecimal

```
  Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
0220479488   4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00   MZ▮.........ÿÿ..
0220479504   B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00   ¸.......@.......
0220479520   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0220479536   00 00 00 00 00 00 00 00  00 00 00 00 E8 00 00 00   ............è...
0220479552   0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
0220479568   69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F   is program canno
0220479584   74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20   t be run in DOS 
0220479600   6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00   mode....$.......
0220479616   4E 00 46 87 0A 61 28 D4  0A 61 28 D4 0A 61 28 D4   N.F▮.a(Ô.a(Ô.a(Ô
0220479632   0A 61 29 D4 90 63 28 D4  C9 6E 75 D4 11 61 28 D4   .a)Ô▮c(ÔÉnuÔ.a(Ô
0220479648   C9 6E 27 D4 0F 61 28 D4  C9 6E 48 D4 21 61 28 D4   Én'Ô.a(ÔÉnHÔ!a(Ô
0220479664   C9 6E 77 D4 16 61 28 D4  C9 6E 76 D4 0B 61 28 D4   ÉnwÔ.a(ÔÉnvÔ.a(Ô
0220479680   C9 6E 72 D4 0B 61 28 D4  52 69 63 68 0A 61 28 D4   ÉnrÔ.a(ÔRich.a(Ô
0220479696   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0220479712   00 00 00 00 00 00 00 00  50 45 00 00 4C 01 04 00   ........PE..L...
0220479728   B7 A1 D6 45 00 00 00 00  00 00 00 00 E0 00 0E 01   ·¡ÖE........à...
0220479744   0B 01 07 0A 00 50 04 00  00 C4 0B 00 00 00 00 00   .....P...Ä......
0220479760   A4 48 01 00 00 10 00 00  00 50 04 00 00 00 00 01   ¤H.......P......
0220479776   00 10 00 00 00 02 00 00  05 00 02 00 05 00 02 00   ................
0220479792   04 00 0A 00 00 00 00 00  00 40 10 00 00 04 00 00   .........@......
0220479808   3D 5B 10 00 02 00 00 80  00 00 04 00 00 E0 00 00   =[.....▮.....à..
0220479824   00 00 10 00 00 10 00 00  00 00 00 00 10 00 00 00   ................
0220479840   00 00 00 00 00 00 00 00  00 34 04 00 18 01 00 00   .........4......
0220479856   00 90 04 00 80 69 0B 00  00 00 00 00 00 00 00 00   .▮..▮i..........
0220479872   00 00 00 00 00 00 00 00  00 00 10 00 CC 37 00 00   ............Ì7..
0220479888   4C 5F 04 00 38 00 00 00  00 00 00 00 00 00 00 00   L_..8...........
0220479904   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0220479920   B8 BF 02 00 40 00 00 00  80 02 00 00 10 01 00 00   ¸¿..@...▮.......
0220479936   00 10 00 00 78 09 00 00  BC 30 04 00 C0 00 00 00   ....x...¼0..À...
0220479952   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0220479968   2E 74 65 78 74 00 00 00  AD 4F 04 00 00 10 00 00   .text...O......
0220479984   00 50 04 00 00 04 00 00  00 00 00 00 00 00 00 00   .P..............
```

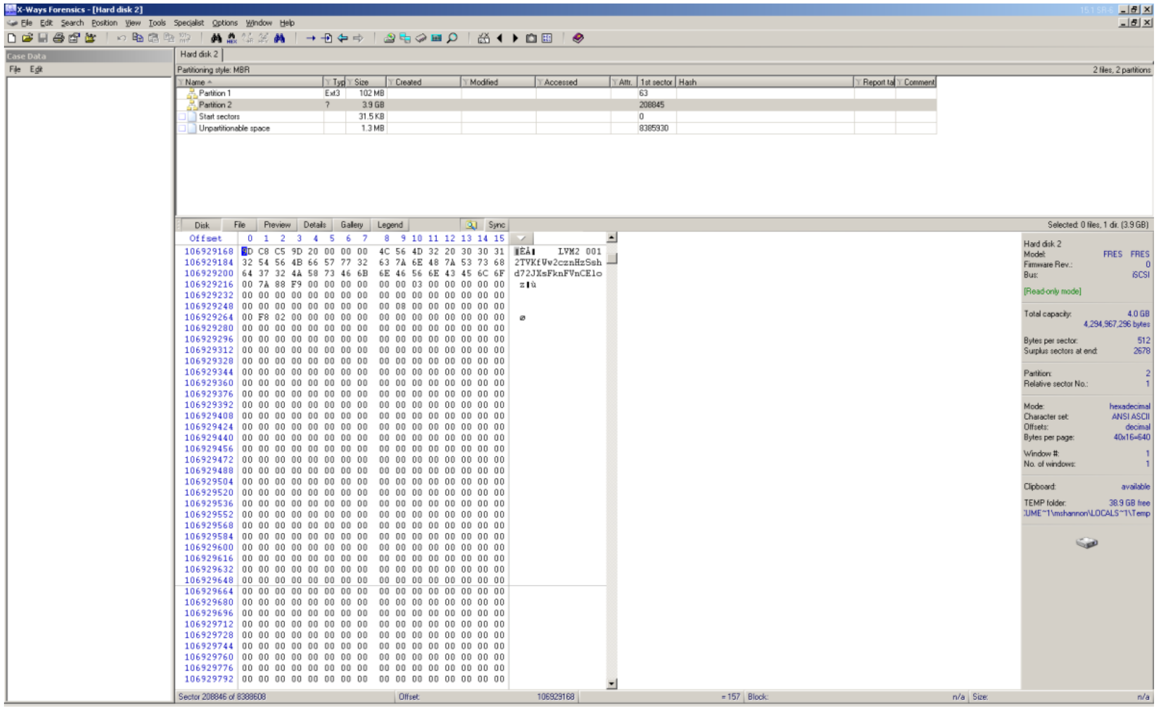
Data Interpreter
8 Bit (±): 77
16 Bit (±): 23117

Sector 430624 of 16755732 | Offset: 220479488 | = 77 | Block: n/a | Size:

Start | C:\ | \\calypso\temp\winhex | WinHex - [Hard disk 0... | 11:07 AM

Step 8, Use Winhex to review selected sector and confirm zeroing operation was unsuccessful.

4.7 Write Prevention Testing – Linux, Apple OS X



X-Ways Forensics - [Hard disk 2]

Hard disk 2

Partitioning style: MBR

2 files, 2 partitions

Name	Typ	Size	Created	Modified	Accessed	Attr.	1st sector	Hash	Report ta	Comment
Partition 1	Ext3	102 MB					63			
Partition 2	?	3.9 GB					208845			
Start sectors		31.5 KB					0			
Unpartitionable space		1.3 MB					8385930			

Selected: 0 files, 1 dir. (3.9 GB)

```
   Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
106929168   9D C8 C5 9D 20 00 00 00  4C 56 4D 32 20 30 30 31  ▮ÈÅ▮    LVM2 001
106929184   32 54 56 4B 66 57 77 32  63 7A 6E 48 7A 53 73 68  2TVKfWw2cznHzSsh
106929200   64 37 32 4A 58 73 46 6B  6E 46 56 6E 43 45 6C 6F  d72JXsFknFVnCElo
106929216   00 7A 88 F9 00 00 00 00  00 00 03 00 00 00 00 00   z▮ù
106929232   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929248   00 00 00 00 00 00 00 00  00 08 00 00 00 00 00 00
106929264   00 F8 02 00 00 00 00 00  00 00 00 00 00 00 00 00   ø
106929280   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929296   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929312   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929328   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929344   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929360   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929376   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929392   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929408   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929424   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929440   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929456   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929472   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929488   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929504   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929520   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929536   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929552   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929568   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929584   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929600   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929616   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929632   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929648   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929664   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929680   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929696   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929712   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929728   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929744   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929760   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929776   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
106929792   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Sector 208846 of 8388608 | Offset: 106929168 | = 157 | Block: n/a | Size: n/a

Hard disk 2
Model: FRES FRES
Firmware Rev.: 0
Bus: iSCSI
[Read-only mode]

Total capacity: 4.0 GB
4,294,967,296 bytes

Bytes per sector: 512
Surplus sectors at end: 2678

Partition: 2
Relative sector No.: 1

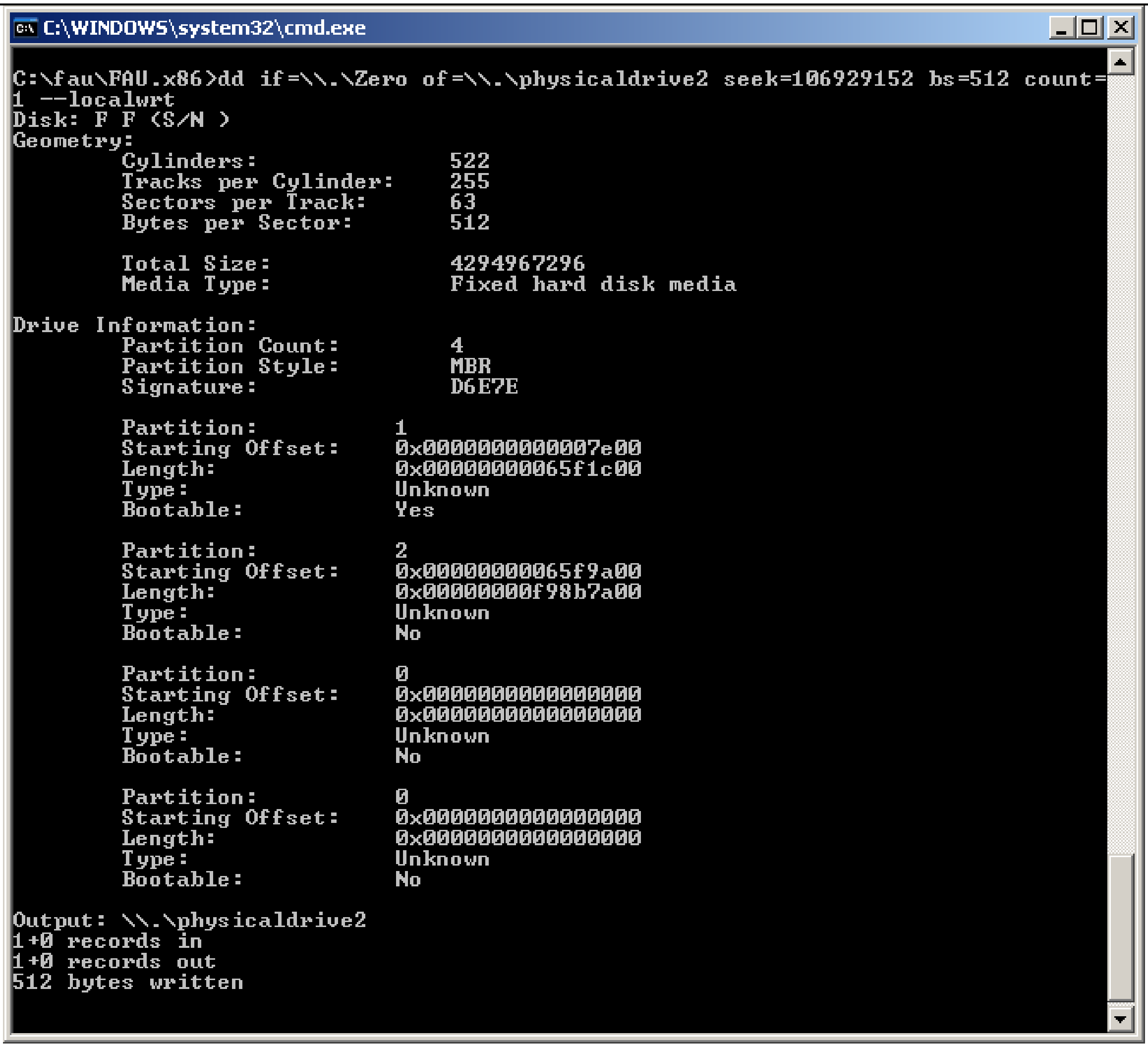
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 40x16=640

Window #: 1
No. of windows: 1

Clipboard: available

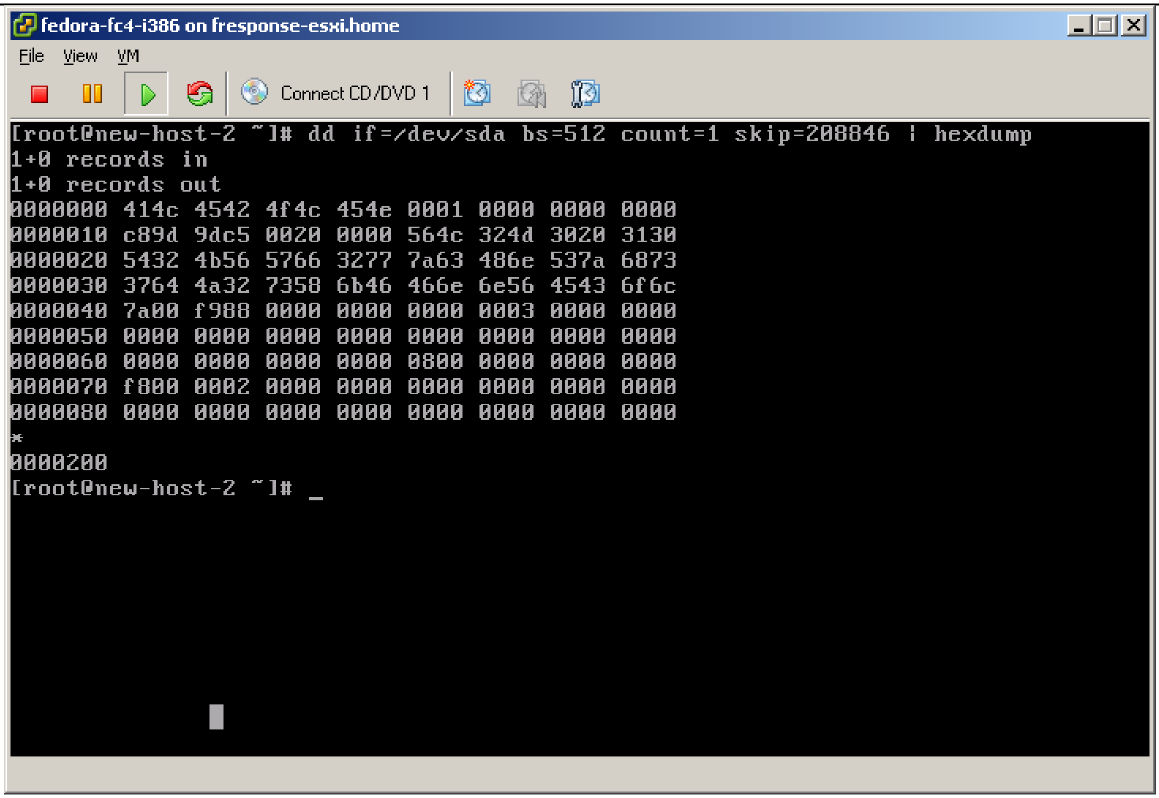
TEMP folder: 38.9 GB free
:UME~1\mshannon\LOCALS~1\Temp

Step 1, Open the attached disk using X-Ways, record the value of one arbitrary sector of information.



```
C:\fau\FAU.x86>dd if=\\.\Zero of=\\.\physicaldrive2 seek=106929152 bs=512 count=
1 --localwrt
Disk: F F (S/N )
Geometry:
        Cylinders:              522
        Tracks per Cylinder:    255
        Sectors per Track:      63
        Bytes per Sector:       512

        Total Size:             4294967296
        Media Type:             Fixed hard disk media

Drive Information:
        Partition Count:        4
        Partition Style:        MBR
        Signature:              D6E7E

        Partition:          1
        Starting Offset:    0x0000000000007e00
        Length:             0x00000000065f1c00
        Type:               Unknown
        Bootable:           Yes

        Partition:          2
        Starting Offset:    0x00000000065f9a00
        Length:             0x00000000f98b7a00
        Type:               Unknown
        Bootable:           No

        Partition:          0
        Starting Offset:    0x0000000000000000
        Length:             0x0000000000000000
        Type:               Unknown
        Bootable:           No

        Partition:          0
        Starting Offset:    0x0000000000000000
        Length:             0x0000000000000000
        Type:               Unknown
        Bootable:           No

Output: \\.\physicaldrive2
1+0 records in
1+0 records out
512 bytes written
```

Step 2, Use DD to output zeros to the selected arbitrary sector.



```
[root@new-host-2 ~]# dd if=/dev/sda bs=512 count=1 skip=208846 | hexdump
1+0 records in
1+0 records out
0000000 414c 4542 4f4c 454e 0001 0000 0000 0000
0000010 c89d 9dc5 0020 0000 564c 324d 3020 3130
0000020 5432 4b56 5766 3277 7a63 486e 537a 6873
0000030 3764 4a32 7358 6b46 466e 6e56 4543 6f6c
0000040 7a00 f988 0000 0000 0000 0003 0000 0000
0000050 0000 0000 0000 0000 0000 0000 0000 0000
0000060 0000 0000 0000 0000 0800 0000 0000 0000
0000070 f800 0002 0000 0000 0000 0000 0000 0000
0000080 0000 0000 0000 0000 0000 0000 0000 0000
*
0000200
[root@new-host-2 ~]# _
```

Step 3, On the original disk, dump the sector in question using dd and hexdump, compare the resulting values to confirm no writes have taken place.

Appendix A. Contacts

A.1 Agile Risk Management LLC

2202 N West Shore Blvd, Suite 200
Tampa, FL 33607

Table 1: Agile Risk Management LLC Contacts

Contact	Title	Contact Information
Matthew Shannon	Principal	mshannon@f-response.com
Matthew Decker	Principal	mjdecker@f-response.com

Appendix B. Legal Notices

B.1 Trademarks

F-Response® is a registered trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

B.2 Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

B.3 Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.