F-RESPONSE NOW/UNIVERSAL™ VALIDATION TESTING REPORT

INCLUDES F-RESPONSE DISCOVERYSHARES™, PHYSICAL DEVICES, PARTITIONS, AND MEMORYSHARES™

December 2014

DOCUMENT CONTROL

This is a controlled document produced by F-Response (“F-RESPONSE”). The control and release of this document is the responsibility of the F-RESPONSE document owner. This includes any amendment that may be required.

Issue Control			
Issue	1.2	Date	December 1, 2014
Classification	Public	Author	M. Shannon
Document Title	F-Response Now/Universal Validation Testing Report		
Approved By	M. Shannon		
Released By	M. Shannon		

Owner Details	
Name	Matthew M. Shannon
Office Region	F-Response Corporate Offices
Contact Number	1-800-317-5497
Email Address	mshannon@f-response.com

Revision History			
Issue	Date	Author	Comments
1.1	October 21, 2014	M Shannon	Updated to reflect product branding.
1.2	December 11, 2014	M Shannon	Updated to reflect addition of compression and Linux based examiner software.

TABLE OF CONTENTS

TESTING RESULTS SUMMARY

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

F-Response Now/Universal™ uses a patent-pending process to create a reliable, read-only connection between an examiner's computer and a computer under inspection. The function of the F-Response Now/Universal™ Response software tested herein is that an established F-Response Now/Universal™ network connection is completely read-only, functioning much like a software write blocker albeit over a network connection. The testing validates that F-Response Now/Universal™ 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 network connection established by F-Response Now/Universal™ 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 Now/Universal™ 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 Now/Universal™ application code base (F-Response Now/Universal™ Discovery, Digital Forensics, and Incident Response Class Appliances), release 1.0.72-5 (Windows, Linux, and Apple OS X).

INTRODUCTION

SCOPE

The scope of this project was limited to the validation and testing of F-Response Now/Universal™ DiscoveryShares™, Physical Devices, and Partitions on the following platforms.

- Microsoft Windows
  - Windows 7 32bit
  - Windows 8.1 64bit
  - Windows Server 2012 64bit
- Linux
  - 3.1x Linux Kernel 32bit
  - 3.1x Linux Kernel 64bit
- Apple OSX
  - Apple OSX 10.8

PURPOSE

This document outlines the F-Response Now/Universal™ Software validation process, results, and methodology developed and executed by F-Response. F-Response Now/Universal™ Software validation answers the following questions:

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

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.

TEST RESULTS

DISK VALIDITY

Does F-Response Now/Universal™ accurately present the remote PhysicalDisk(s)?

In order to test the validity of the locally attached remote F-Response Now/Universal™ physical 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 Now/Universal™ disk is attached to our local workstation for analysis. 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 NOW/UNIVERSAL™PRESENTED)		RESULT	
PLATFORM	Total Sectors	Sector Size	Total Sectors	Sector Size	Windows Examiner	Linux Examiner
WINDOWS 7 X86	83886080	512	83886080	512	Pass	Pass
WINDOWS 8.1 X64	67108864	512	67108864	512	Pass	Pass
WINDOWS SERVER 2012 X64	83886080	512	83886080	512	Pass	Pass
LINUX 3.1 KERNEL X86	83886080	512	83886080	512	Pass	Pass
LINUX 3.1 KERNEL X64	83886080	512	83886080	512	Pass	Pass
APPLE OSX 10.8	83886080	512	83886080	512	Pass	Pass

READ ACCURACY

Does F-Response Now/Universal™ correctly and accurately read data from the remote PhysicalDisk(s), Partitions, and DiscoveryShares™?

In order to test the read accuracy of the locally attached remote F-Response Now/Universal™ physical disks, DiscoveryShares™, and partitions, we obtained hash values for the individual files listed below, as well as a portion of the raw disk (Physical Sector 0) from the local F-Response Now/Universal™ device(physical disks and partitions only). Both these hash values were then computed using select Computer Forensics software packages on their native operating system.

READ ACCURACY TESTING RESULTS	**NATIVE (LOCAL MACHINE)**		**REMOTE (F-RESPONSE NOW/UNIVERSAL™ PRESENTED)**		**RESULT**	
PLATFORM	File Hash	Data Hash	File Hash	Data Hash	Windows Examiner	Linux Examiner
WINDOWS 7 X86 (DISCOVERYSHARE™)	8B88EBBB05A0E56B7DCC708498C02B3E	N/A	8B88EBBB05A0E56B7DCC708498C02B3E	N/A	Pass	Pass
WINDOWS 8.1 X64 (DISCOVERYSHARE™)	ACDBE1ED38167C8B01B8F63161BB2CEA	N/A	ACDBE1ED38167C8B01B8F63161BB2CEA	N/A	Pass	Pass
WINDOWS SERVER 2012 X64 (DISCOVERYSHARE™)	928791755FDDEA721B053535EF84FA17	N/A	928791755FDDEA721B053535EF84FA17	N/A	Pass	Pass
LINUX 3.1 KERNEL X86 (DISCOVERYSHARE™)	835F8651D266F285C96F5AD2E4066243	N/A	835F8651D266F285C96F5AD2E4066243	N/A	Pass	Pass
LINUX 3.1 KERNEL X64 (DISCOVERYSHARE™)	A66ED71FF10AECA7C7DA78751F49D2AC	N/A	A66ED71FF10AECA7C7DA78751F49D2AC	N/A	Pass	Pass
APPLE OSX 10.8 (DISCOVERYSHARE™)	565140D56B9893751A53B12A190CEE6C	N/A	565140D56B9893751A53B12A190CEE6C	N/A	Pass	Pass
WINDOWS 7 X86	8B88EBBB05A0E56B7DCC708498C02B3E	C9A5A6878D97B48CC965C1E41859F034	8B88EBBB05A0E56B7DCC708498C02B3E	C9A5A6878D97B48CC965C1E41859F034	Pass	Pass
WINDOWS 8.1 X64	ACDBE1ED38167C8B01B8F63161BB2CEA	C9A5A6878D97B48CC965C1E41859F034	ACDBE1ED38167C8B01B8F63161BB2CEA	C9A5A6878D97B48CC965C1E41859F034	Pass	Pass
WINDOWS SERVER 2012 X64	928791755FDDEA721B053535EF84FA17	C9A5A6878D97B48CC965C1E41859F034	928791755FDDEA721B053535EF84FA17	C9A5A6878D97B48CC965C1E41859F034	Pass	Pass
LINUX 3.1 KERNEL X86	835F8651D266F285C96F5AD2E4066243	C9A5A6878D97B48CC965C1E41859F034	835F8651D266F285C96F5AD2E4066243	C9A5A6878D97B48CC965C1E41859F034	Pass	Pass

LINUX 3.1 KERNEL X64	A66ED71FF10AECA7C7DA78751F49D2AC	C9A5A6878D97B48CC965C1E41859F034	A66ED71FF10AECA7C7DA78751F49D2AC	C9A5A6878D97B48CC965C1E41859F034	Pass	Pass
APPLE OSX 10.8	565140D56B9893751A53B12A190CEE6C	C9A5A6878D97B48CC965C1E41859F034	565140D56B9893751A53B12A190CEE6C	C9A5A6878D97B48CC965C1E41859F034	Pass	Pass

WRITE PREVENTION

Does F-Response Now/Universal™ accurately prevent write operations from occurring on the remote PhysicalDisk(s), partitions, and DiscoveryShares™?[1]

In order to test the write prevention capabilities of F-Response Now/Universal™, 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 Now/Universal™ connected disk. In all cases F-Response Now/Universal™ prevented the write operations. In some cases, the local system would return a "success" message, however no actual changes occurred on the remote F-Response Now/Universal™ disk. The detailed process used to obtain these results is included in section 4 of this document.

WRITE PREVENTION TESTING RESULTS	**F-RESPONSE NOW/UNIVERSAL PRESENTED DISCOVERY SHARE**		**F-RESPONSE NOW/UNIVERSAL PRESENTED DISK**		**RESULT**	
SUBJECT PLATFORM	File Deletion		Data Modification		Windows Examiner	Linux Examiner
	System Response	Actual Result	System Response	Actual Result		
WINDOWS 7 X86	Blocked	Blocked	Success	Blocked	Pass	Pass
WINDOWS 8.1 X64	Blocked	Blocked	Success	Blocked	Pass	Pass
WINDOWS SERVER 2012 X64	Blocked	Blocked	Success	Blocked	Pass	Pass
LINUX 3.1 KERNEL X86	Blocked	Blocked	Success	Blocked	Pass	Pass
LINUX 3.1 KERNEL X64	Blocked	Blocked	Success	Blocked	Pass	Pass
APPLE OSX 10.8	Blocked	Blocked	Success	Blocked	Pass	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.

TEST ENVIRONMENT

TEST ENVIRONMENT SOFTWARE

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

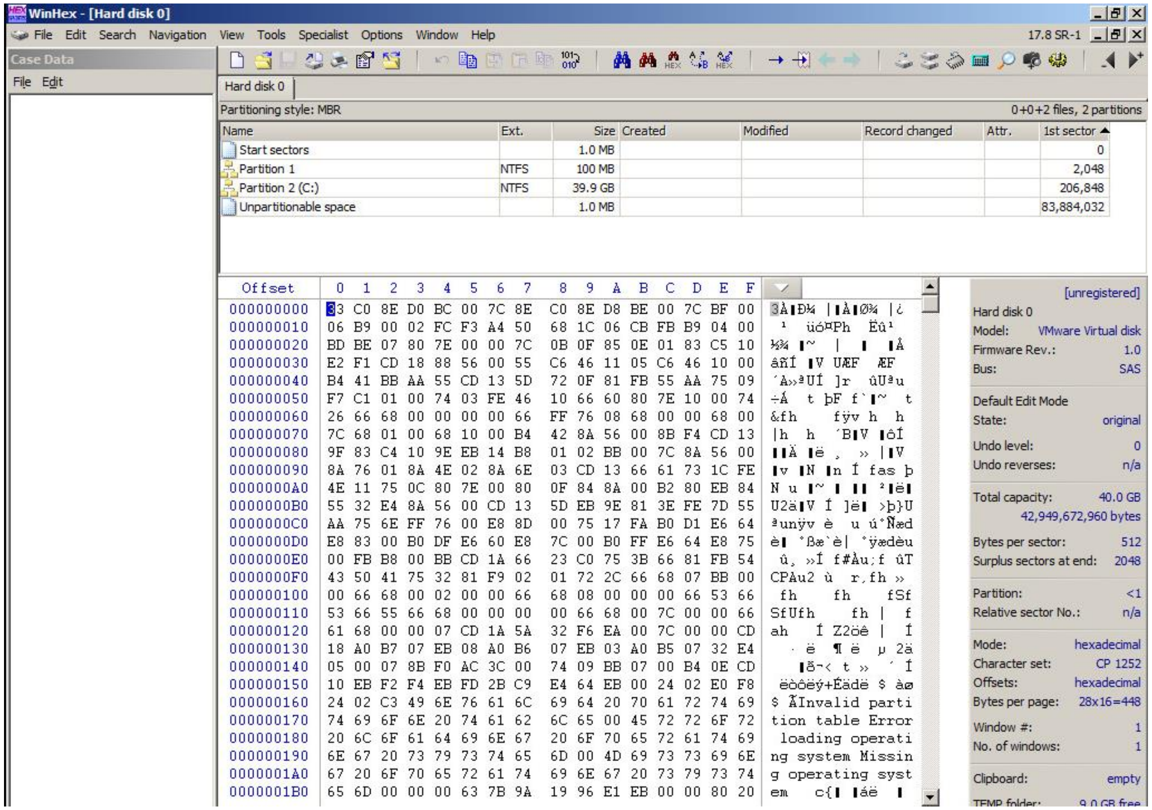
Application	Version	Company	Used for	Platform
F-Response Now/Universal™	1.0.74.5	F-Response	Providing remote forensically sound disk access.	Multiple (See Scope Section)
GNU Tools (md5, dd, dmesg)	2.3.5+ (glibc)	Linux	Baseline data collection on the Linux/OS X target platform.	Linux (See Scope Section)
Vmware VSphere	5.0	VMWare Inc.	Hosting F-Response Now/Universal™ Virtual Test Machines	VMWare Hypervisor
X-Ways Forensics/Winhex[2]	17	X-Ways Technology AG	Verifying capacity, read accuracy.	Windows 7 x86

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

TEST RESULT DETAILS[3]

OBTAIN BASELINE (WINDOWS)

Step 1, Open X-Ways WinHex go to Tools->Open Disk 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.


WinHex - [Hard disk 0]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-1
Case Data
File Edit
Hard disk 0

Partitioning style: MBR — 0+0+2 files, 2 partitions

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector ▲
Start sectors		1.0 MB					0
Partition 1	NTFS	100 MB					2,048
Partition 2 (C:)	NTFS	39.9 GB					206,848
Unpartitionable space		1.0 MB					83,884,032

```
   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 0E 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 1C FE   ▌v ▌N ▌n Í fas þ
0000000A0  4E 11 75 0C 80 7E 00 80  0F 84 8A 00 B2 80 EB 84   N u ▌~ ▌ ▌▌ ²▌ë▌
0000000B0  55 32 E4 8A 56 00 CD 13  5D EB 9E 81 3E FE 7D 55   U2ä▌V Í ]ë▌ >þ}U
0000000C0  AA 75 6E FF 76 00 E8 8D  00 75 17 FA B0 D1 E6 64   ªunÿv è  u ú°Ñæd
0000000D0  E8 83 00 B0 DF E6 60 E8  7C 00 B0 FF E6 64 E8 75   è▌ °ßæ`è| °ÿædèu
0000000E0  00 FB B8 00 BB CD 1A 66  23 C0 75 3B 66 81 FB 54    û¸ »Í f#Àu;f ûT
0000000F0  43 50 41 75 32 81 F9 02  01 72 2C 66 68 07 BB 00   CPAu2 ù  r,fh »
000000100  00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66    fh    fh    fSf
000000110  53 66 55 66 68 00 00 00  00 66 68 00 7C 00 00 66   SfUfh    fh |  f
000000120  61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD   ah   Í Z2öê |  Í
000000130  18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4      · ë  ¶ ë  µ 2ä
000000140  05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD      ▌ð¬< t »  ´ Í
000000150  10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8    ëòôëý+Éädë $ àø
000000160  24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69   $ ÃInvalid parti
000000170  74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72   tion table Error
000000180  20 6C 6F 61 64 69 6E 67  20 6F 70 65 72 61 74 69    loading operati
000000190  6E 67 20 73 79 73 74 65  6D 00 4D 69 73 73 69 6E   ng system Missin
0000001A0  67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74   g operating syst
0000001B0  65 6D 00 00 00 63 7B 9A  19 96 E1 EB 00 00 80 20   em   c{▌ ▌áë  ▌
```

[unregistered]

Hard disk 0
Model: VMware Virtual disk
Firmware Rev.: 1.0
Bus: SAS

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Total capacity: 40.0 GB
42,949,672,960 bytes

Bytes per sector: 512
Surplus sectors at end: 2048

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

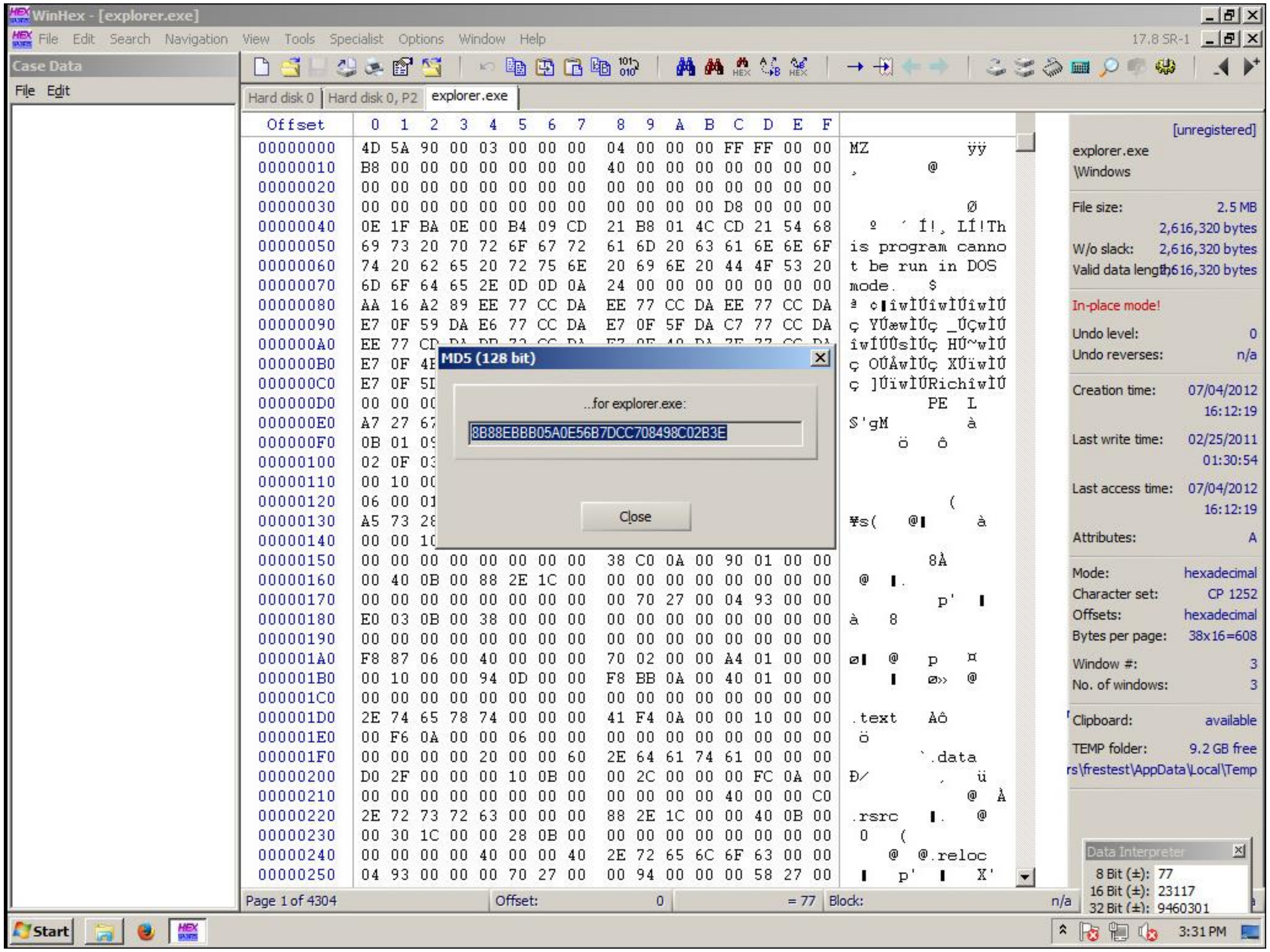
Mode: hexadecimal
Character set: CP 1252
Offsets: hexadecimal
Bytes per page: 28x16=448

Window #: 1
No. of windows: 1

Clipboard: empty
TEMP folder: 9.0 GB free

[3] All testing details assume the F-Response Now/Universal Resource has been properly connected using one of the many editions of F-Response Now/Universal software products, as this process is detailed in numerous training manuals and quick start guides available on the F-Response Now/Universal website (www.F-Response Now/Universal.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 explorer.exe:

8B88EBBB05A0E56B7DCC708498C02B3E

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00
00000010  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000030  00 00 00 00 00 00 00 00  00 00 00 00 D8 00 00 00
00000040  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68
00000050  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F
00000060  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20
00000070  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00
00000080  AA 16 A2 89 EE 77 CC DA  EE 77 CC DA EE 77 CC DA
00000090  E7 0F 59 DA E6 77 CC DA  E7 0F 5F DA C7 77 CC DA
000000A0  EE 77 CD
000000B0  E7 0F 4
000000C0  E7 0F 5
000000D0  00 00 00
000000E0  A7 27 67
000000F0  0B 01 09
00000100  02 0F 03
00000110  00 10 00
00000120  06 00 01
00000130  A5 73 28
00000140  00 00 10
00000150  00 00 00 00 00 00 00 00  38 C0 0A 00 90 01 00 00
00000160  00 40 0B 00 88 2E 1C 00  00 00 00 00 00 00 00 00
00000170  00 00 00 00 00 00 00 00  00 70 27 00 04 93 00 00
00000180  E0 03 0B 00 38 00 00 00  00 00 00 00 00 00 00 00
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0  F8 87 06 00 40 00 00 00  70 02 00 00 A4 01 00 00
000001B0  00 10 00 00 94 0D 00 00  F8 BB 0A 00 40 01 00 00
000001C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0  2E 74 65 78 74 00 00 00  41 F4 0A 00 00 10 00 00
000001E0  00 F6 0A 00 00 06 00 00  00 00 00 00 00 00 00 00
000001F0  00 00 00 00 20 00 00 60  2E 64 61 74 61 00 00 00
00000200  D0 2F 00 00 00 10 0B 00  00 2C 00 00 00 FC 0A 00
00000210  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 C0
00000220  2E 72 73 72 63 00 00 00  88 2E 1C 00 00 40 0B 00
00000230  00 30 1C 00 00 28 0B 00  00 00 00 00 00 00 00 00
00000240  00 00 00 00 40 00 00 40  2E 72 65 6C 6F 63 00 00
00000250  04 93 00 00 00 70 27 00  00 94 00 00 00 58 27 00
```

Page 1 of 4304 | Offset: 0 | = 77 | Block: n/a

[unregistered]
explorer.exe
\Windows

File size: 2.5 MB
2,616,320 bytes
W/o slack: 2,616,320 bytes
Valid data length: 2,616,320 bytes

In-place mode!
Undo level: 0
Undo reverses: n/a

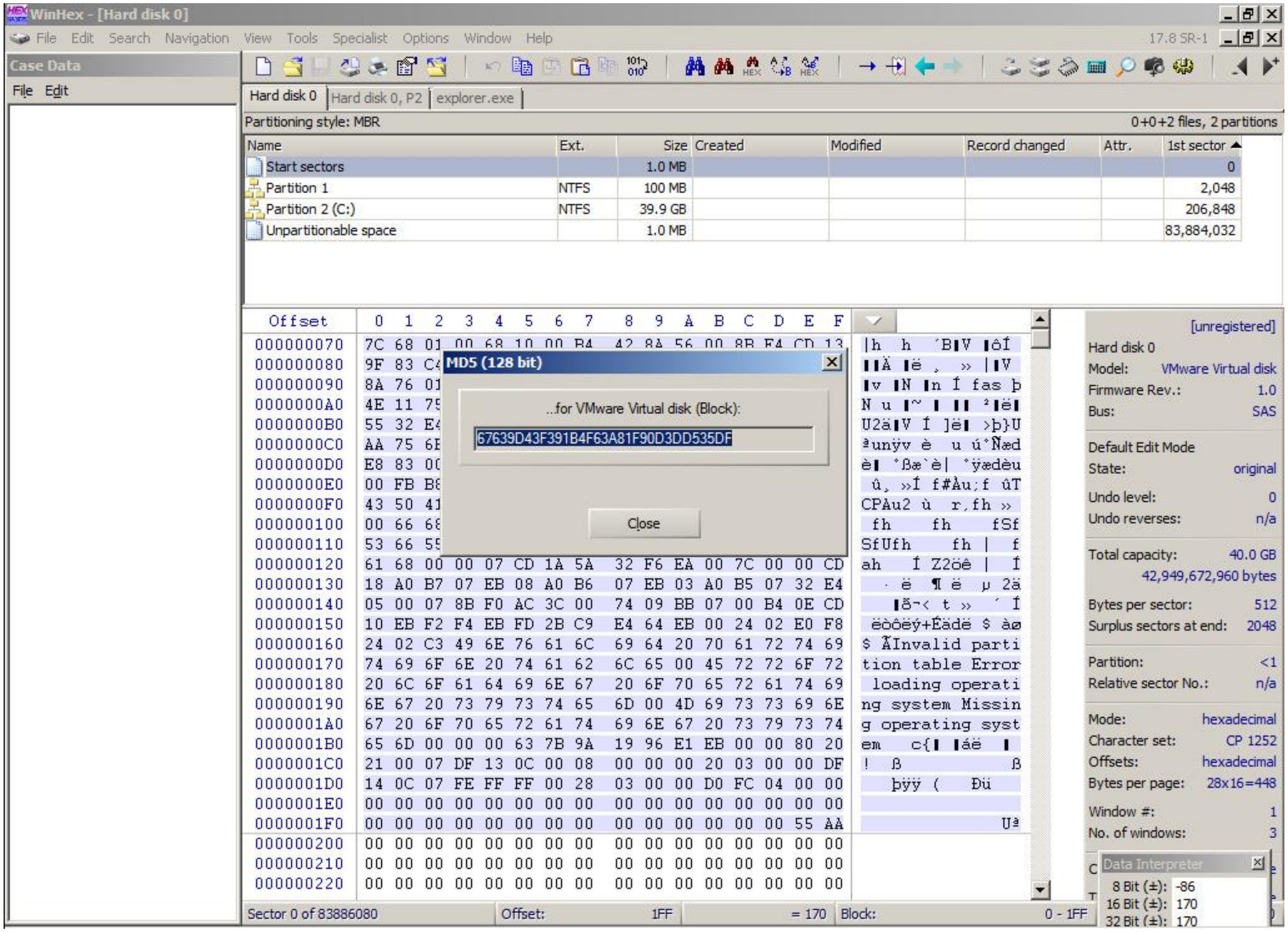
Creation time: 07/04/2012 16:12:19
Last write time: 02/25/2011 01:30:54
Last access time: 07/04/2012 16:12:19
Attributes: A

Mode: hexadecimal
Character set: CP 1252
Offsets: hexadecimal
Bytes per page: 38x16=608
Window #: 3
No. of windows: 3
Clipboard: available
TEMP folder: 9.2 GB free
rs\frestest\AppData\Local\Temp

Data Interpreter
8 Bit (±): 77
16 Bit (±): 23117
32 Bit (±): 9460301

3:31 PM

Step 3, Select a single sector on the disk, select Tools->Compute Hash (MD5 128 bit), record the resulting hash value.



Partitioning style: MBR

0+0+2 files, 2 partitions

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Start sectors		1.0 MB					0
Partition 1	NTFS	100 MB					2,048
Partition 2 (C:)	NTFS	39.9 GB					206,848
Unpartitionable space		1.0 MB					83,884,032

MD5 (128 bit)

...for VMware Virtual disk (Block):

67639D43F391B4F63A81F90D3DD535DF

Close

```
   Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
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                                             ▌▌Ä ▌ë ¸  » |▌V
000000090    8A 76 01                                             ▌v ▌N ▌n Í fas þ
0000000A0    4E 11 75                                             N u ▌~ ▌ ▌▌ ²▌ë▌
0000000B0    55 32 E4                                             U2ä▌V Í ]ë▌ >þ}U
0000000C0    AA 75 6E                                             ªunÿv è  u ú˚Ñæd
0000000D0    E8 83 00                                             è▌ ˚ßæ`è| ˚ÿædèu
0000000E0    00 FB B8                                              û¸ »Í f#Àu;f ûT
0000000F0    43 50 41                                             CPAu2 ù  r,fh »
000000100    00 66 68                                              fh    fh    fSf
000000110    53 66 55                                             SfUfh    fh |  f
000000120    61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD   ah   Í Z2öê |  Í
000000130    18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4      · ë  ¶ ë  µ 2ä
000000140    05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD       ▌ð¬< t »   ´ Í
000000150    10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8    ëòôëý+Éädë $ àø
000000160    24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69   $ ÃInvalid parti
000000170    74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72   tion table Error
000000180    20 6C 6F 61 64 69 6E 67  20 6F 70 65 72 61 74 69    loading operati
000000190    6E 67 20 73 79 73 74 65  6D 00 4D 69 73 73 69 6E   ng system Missin
0000001A0    67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74   g operating syst
0000001B0    65 6D 00 00 00 63 7B 9A  19 96 E1 EB 00 00 80 20   em   c{▌ ▌áë   ▌
0000001C0    21 00 07 DF 13 0C 00 08  00 00 00 20 03 00 00 DF   !  ß            ß
0000001D0    14 0C 07 FE FF FF 00 28  03 00 00 D0 FC 04 00 00      þÿÿ (   Ðü
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                 Uª
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
```

Sector 0 of 83886080 | Offset: 1FF | = 170 | Block: 0 - 1FF

Hard disk 0
Model: VMware Virtual disk
Firmware Rev.: 1.0
Bus: SAS

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Total capacity: 40.0 GB
42,949,672,960 bytes

Bytes per sector: 512
Surplus sectors at end: 2048

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

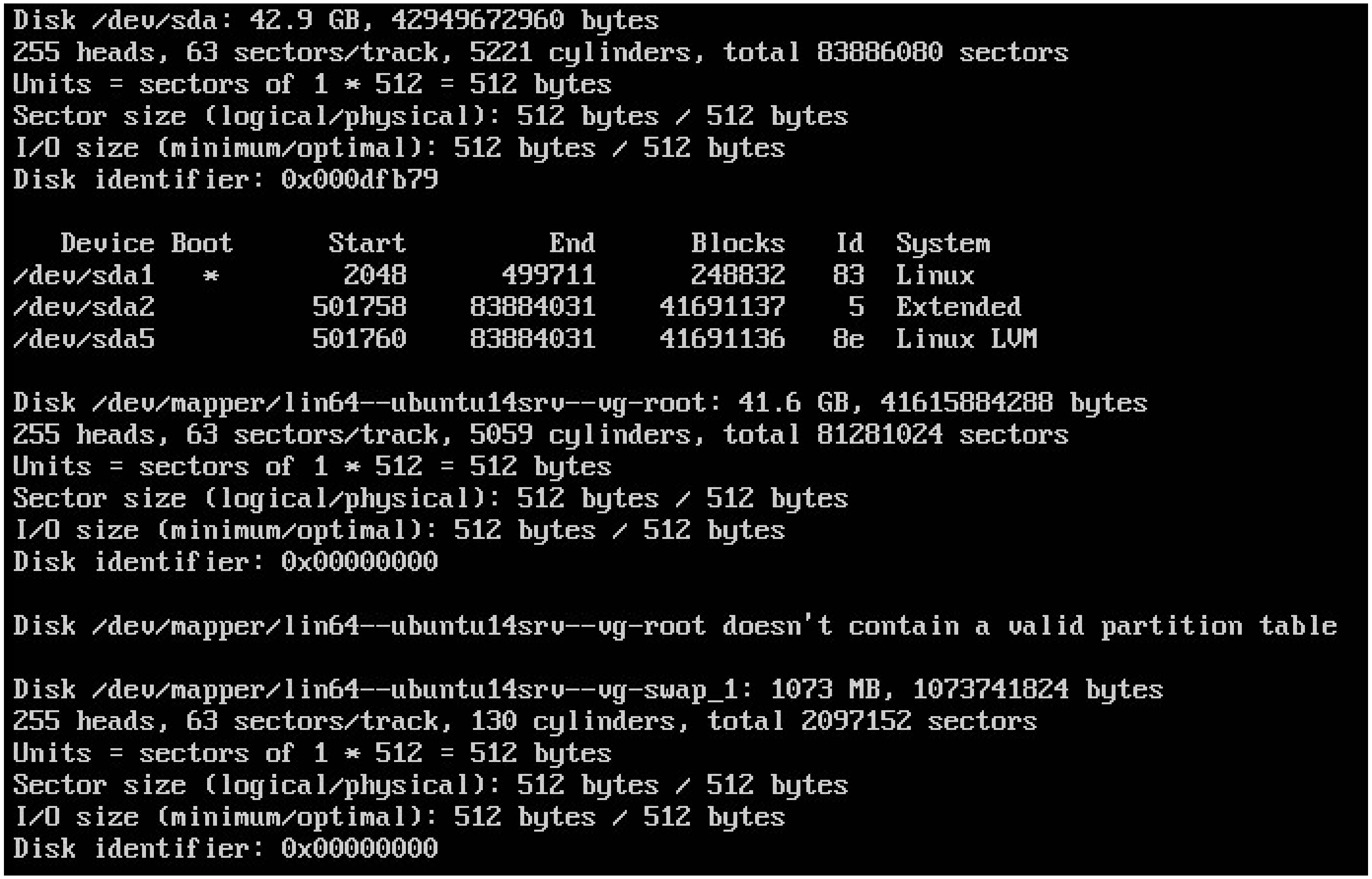
Mode: hexadecimal
Character set: CP 1252
Offsets: hexadecimal
Bytes per page: 28x16=448

Window #: 1
No. of windows: 3

8 Bit (±): -86
16 Bit (±): 170
32 Bit (±): 170

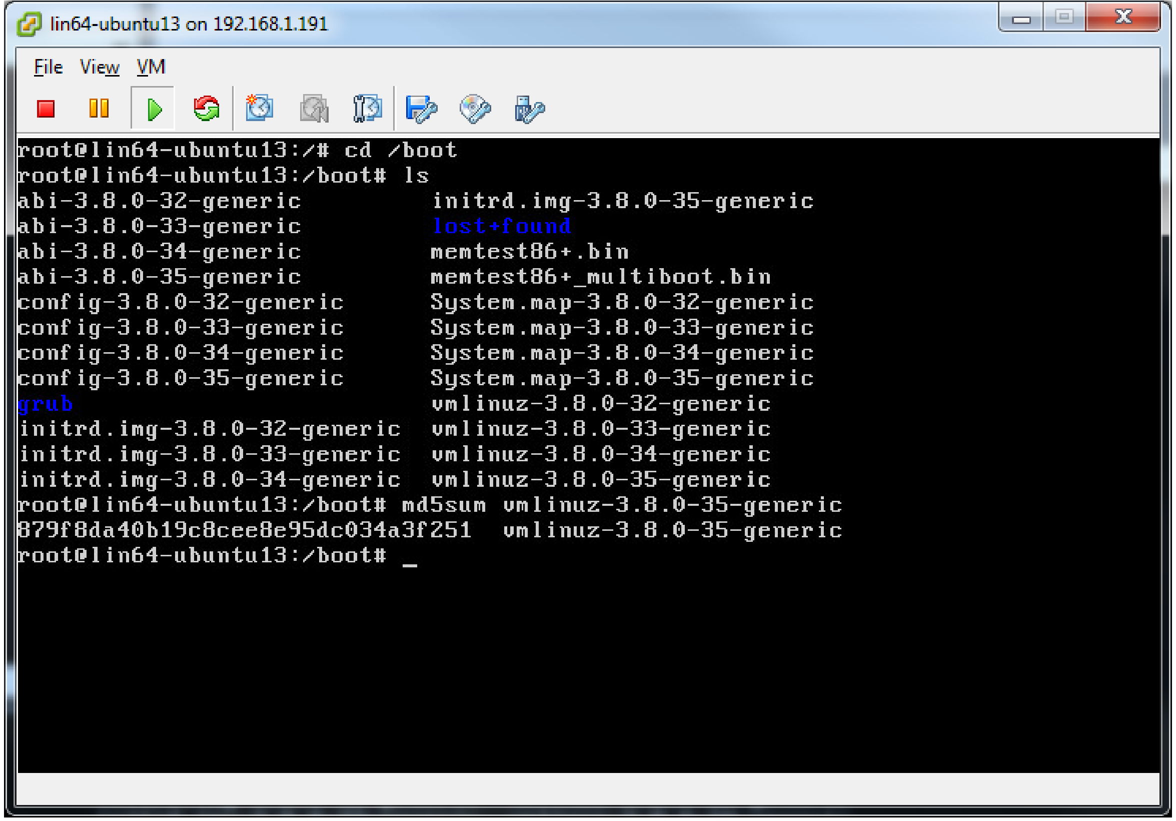
OBTAIN BASELINE (LINUX)

Step 1, Use "fdisk –l | more" to return the total capacity and bytes per sector on the attached disk(s).



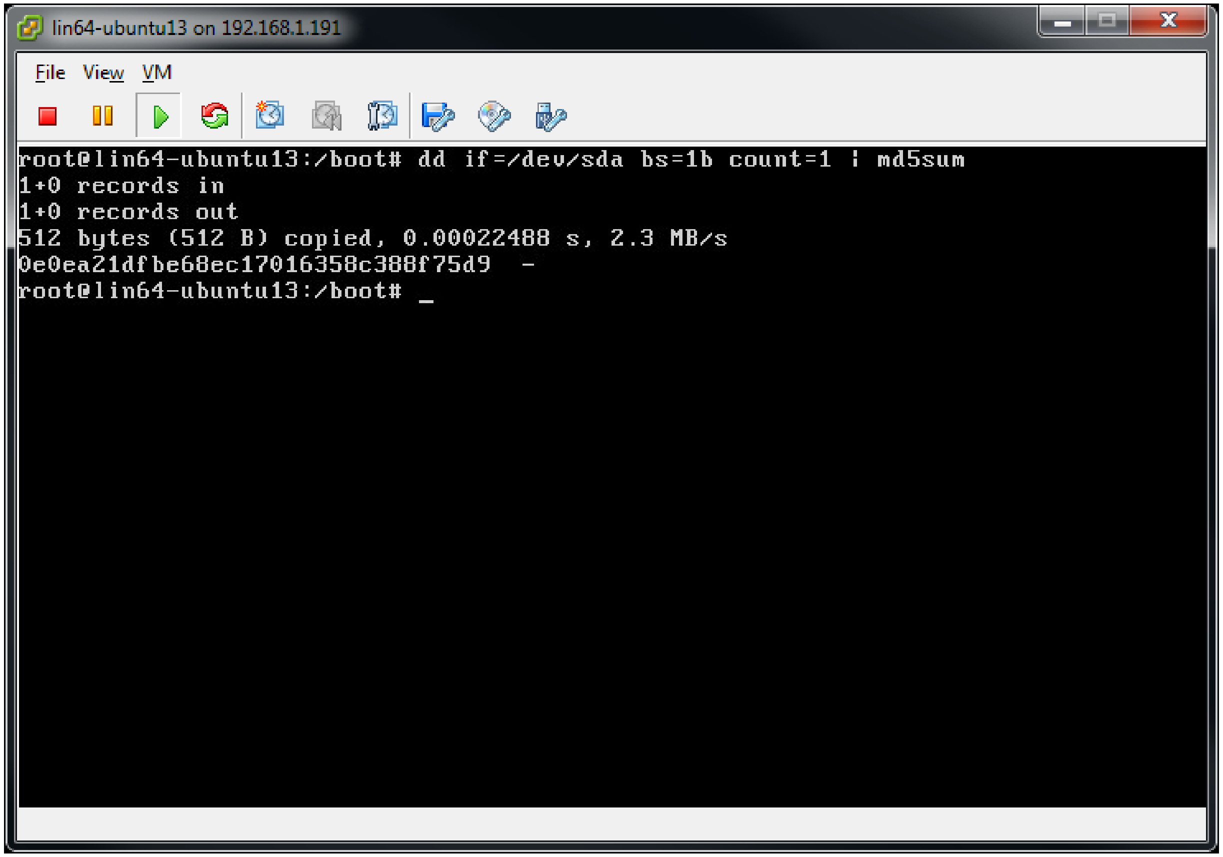
```
Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders, total 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000dfb79

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048      499711      248832   83  Linux
/dev/sda2          501758    83884031    41691137    5  Extended
/dev/sda5          501760    83884031    41691136   8e  Linux LVM

Disk /dev/mapper/lin64--ubuntu14srv--vg-root: 41.6 GB, 41615884288 bytes
255 heads, 63 sectors/track, 5059 cylinders, total 81281024 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/lin64--ubuntu14srv--vg-root doesn't contain a valid partition table

Disk /dev/mapper/lin64--ubuntu14srv--vg-swap_1: 1073 MB, 1073741824 bytes
255 heads, 63 sectors/track, 130 cylinders, total 2097152 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

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



```
root@lin64-ubuntu13:/# cd /boot
root@lin64-ubuntu13:/boot# ls
abi-3.8.0-32-generic         initrd.img-3.8.0-35-generic
abi-3.8.0-33-generic         lost+found
abi-3.8.0-34-generic         memtest86+.bin
abi-3.8.0-35-generic         memtest86+_multiboot.bin
config-3.8.0-32-generic      System.map-3.8.0-32-generic
config-3.8.0-33-generic      System.map-3.8.0-33-generic
config-3.8.0-34-generic      System.map-3.8.0-34-generic
config-3.8.0-35-generic      System.map-3.8.0-35-generic
grub                         vmlinuz-3.8.0-32-generic
initrd.img-3.8.0-32-generic  vmlinuz-3.8.0-33-generic
initrd.img-3.8.0-33-generic  vmlinuz-3.8.0-34-generic
initrd.img-3.8.0-34-generic  vmlinuz-3.8.0-35-generic
root@lin64-ubuntu13:/boot# md5sum vmlinuz-3.8.0-35-generic
879f8da40b19c8cee8e95dc034a3f251  vmlinuz-3.8.0-35-generic
root@lin64-ubuntu13:/boot# _
```

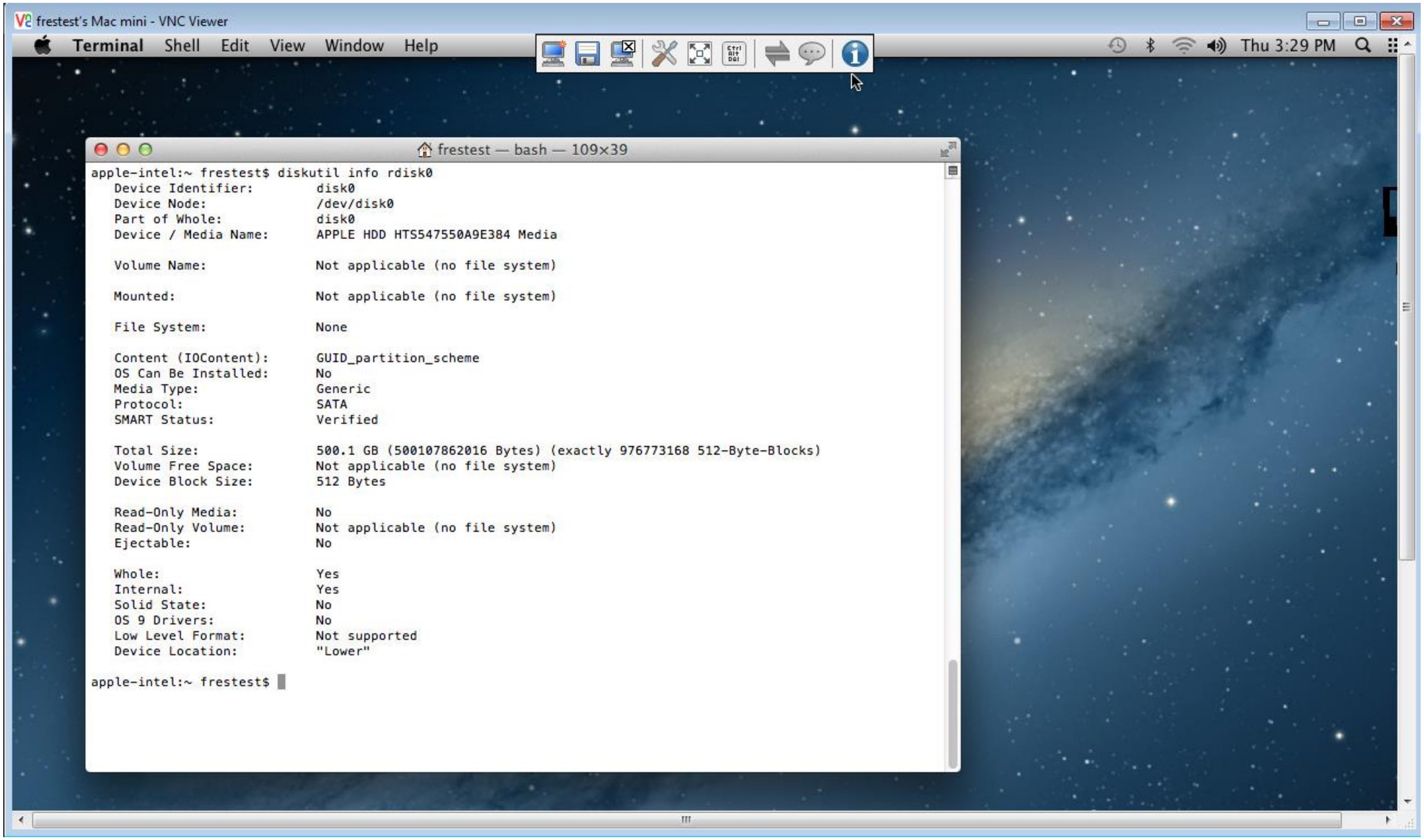
Step 3, Use "dd if=/dev/<disk> bs=1b count=1 | md5sum" to generate the hash of a single sector on the disk.



```
root@lin64-ubuntu13:/boot# dd if=/dev/sda bs=1b count=1 | md5sum
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.00022488 s, 2.3 MB/s
0e0ea21dfbe68ec17016358c388f75d9  -
root@lin64-ubuntu13:/boot# _
```

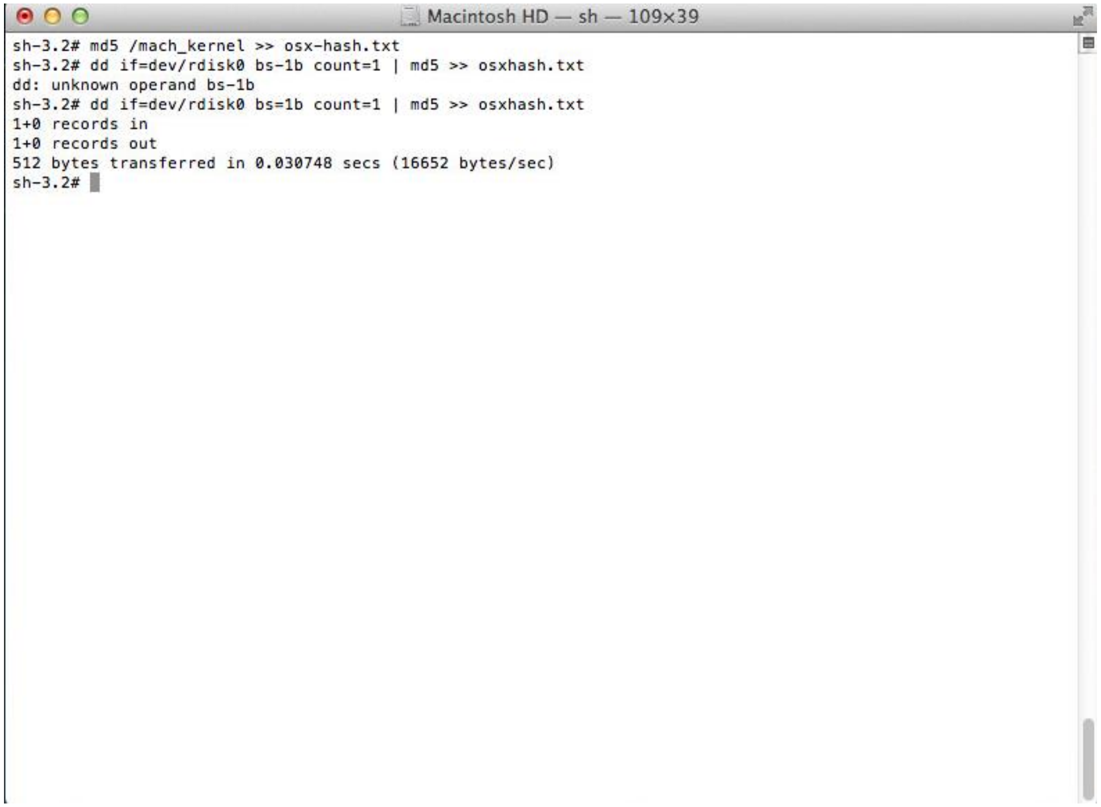
OBTAIN BASELINE (APPLE OS X)

Step 1, Open a terminal window in Apple OS X and type "diskutil info rdisk0" to obtain total disk size in bytes and sector size in bytes.



```
apple-intel:~ frestest$ diskutil info rdisk0
   Device Identifier:        disk0
   Device Node:              /dev/disk0
   Part of Whole:            disk0
   Device / Media Name:      APPLE HDD HTS547550A9E384 Media

   Volume Name:              Not applicable (no file system)

   Mounted:                  Not applicable (no file system)

   File System:              None

   Content (IOContent):      GUID_partition_scheme
   OS Can Be Installed:      No
   Media Type:               Generic
   Protocol:                 SATA
   SMART Status:             Verified

   Total Size:               500.1 GB (500107862016 Bytes) (exactly 976773168 512-Byte-Blocks)
   Volume Free Space:        Not applicable (no file system)
   Device Block Size:        512 Bytes

   Read-Only Media:          No
   Read-Only Volume:         Not applicable (no file system)
   Ejectable:                No

   Whole:                    Yes
   Internal:                 Yes
   Solid State:              No
   OS 9 Drivers:             No
   Low Level Format:         Not supported
   Device Location:          "Lower"

apple-intel:~ frestest$ 
```

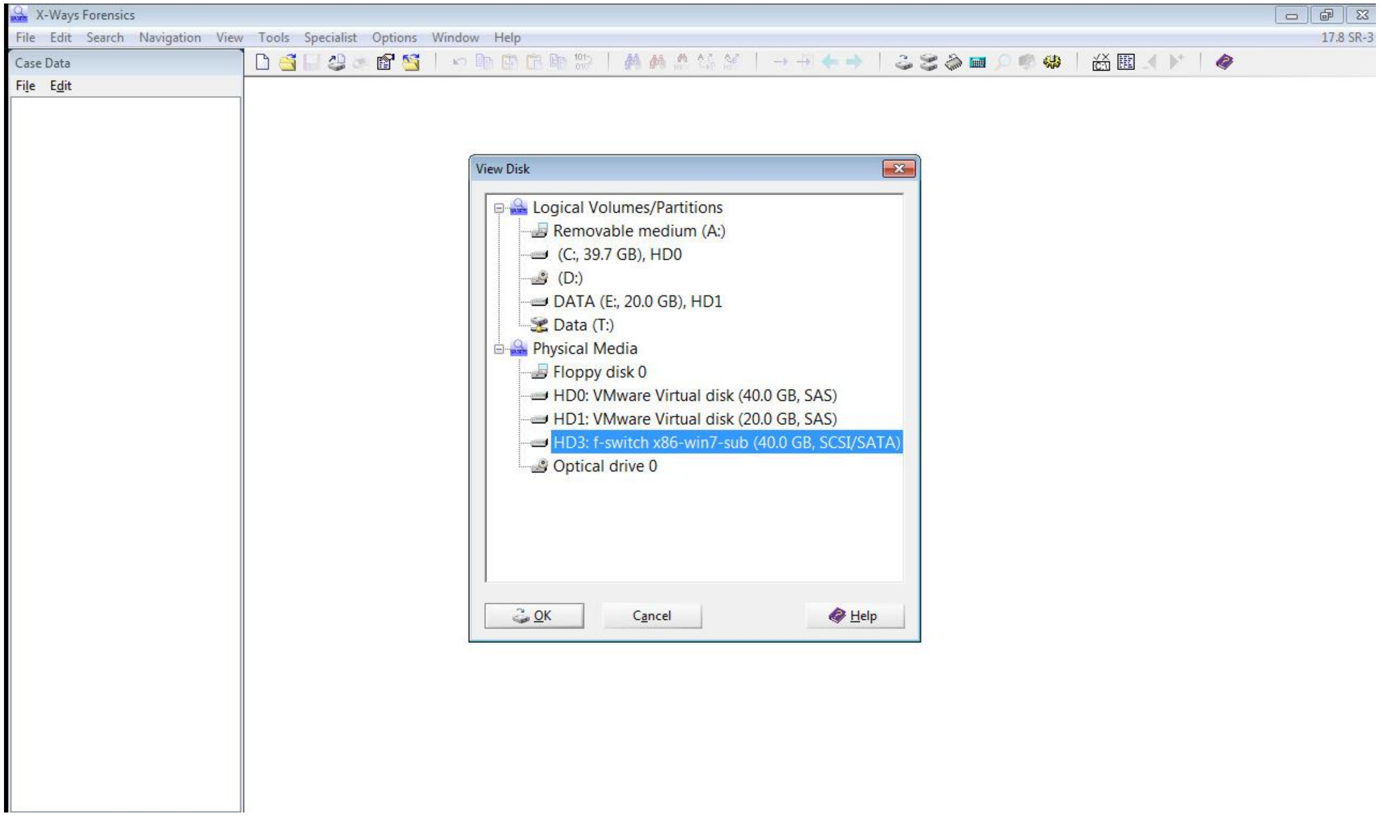
Step 2, Open a Terminal window in Apple OS X and use the following commands to obtain file and data hashes “md5 <path/to/file>” and “dd if=/dev/rdisk0 bs=1b count=1 | md5”.



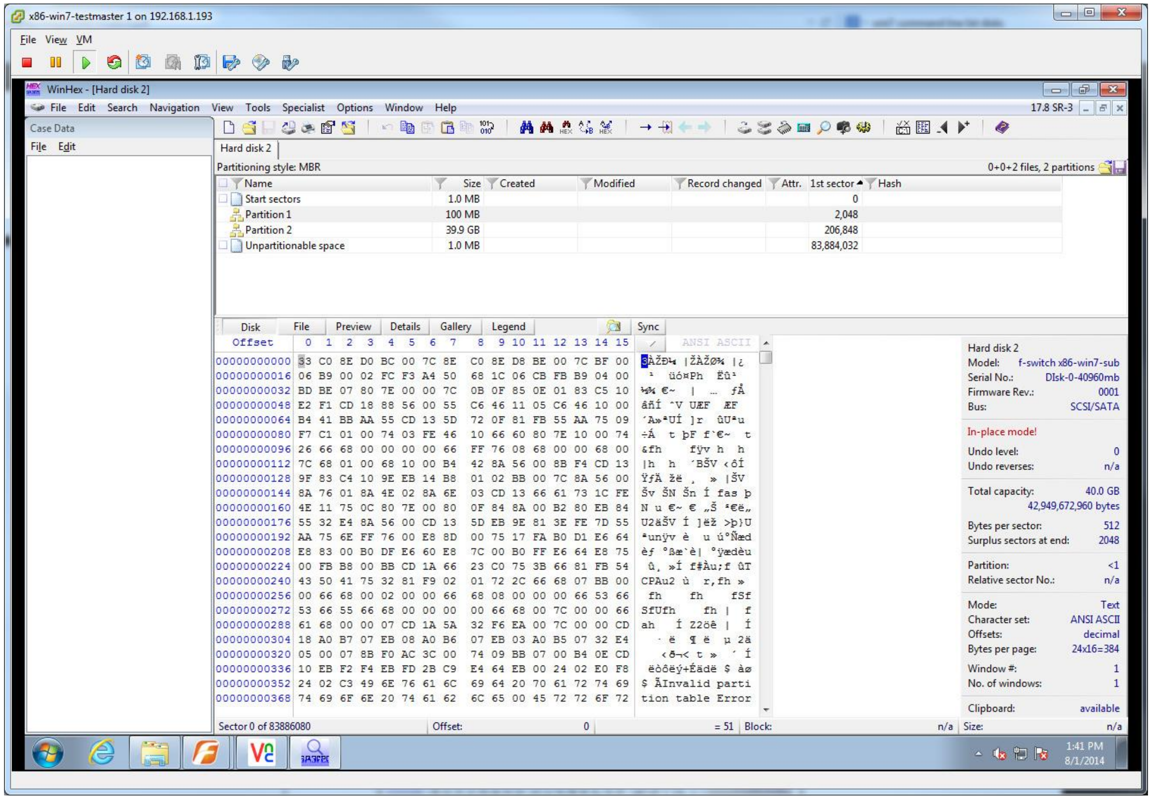
```
sh-3.2# md5 /mach_kernel >> osx-hash.txt
sh-3.2# dd if=dev/rdisk0 bs-1b count=1 | md5 >> osxhash.txt
dd: unknown operand bs-1b
sh-3.2# dd if=dev/rdisk0 bs=1b count=1 | md5 >> osxhash.txt
1+0 records in
1+0 records out
512 bytes transferred in 0.030748 secs (16652 bytes/sec)
sh-3.2#
```

DISK VALIDITY TESTING – WINHEX

Step 1: Open X-Ways Forensics go to Tools -> Open Disk and select the F-Response Now/Universal presented physical resource.


X-Ways Forensics
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
View Disk
OK
Cancel
Help

- Logical Volumes/Partitions
  - Removable medium (A:)
  - (C:, 39.7 GB), HD0
  - (D:)
  - DATA (E:, 20.0 GB), HD1
  - Data (T:)
- Physical Media
  - Floppy disk 0
  - HD0: VMware Virtual disk (40.0 GB, SAS)
  - HD1: VMware Virtual disk (20.0 GB, SAS)
  - HD3: f-switch x86-win7-sub (40.0 GB, SCSI/SATA)
  - Optical drive 0


x86-win7-testmaster 1 on 192.168.1.193
File View VM
WinHex - [Hard disk 2]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
Hard disk 2
Disk File Preview Details Gallery Legend Sync

Partitioning style: MBR

0+0+2 files, 2 partitions

Name	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
Start sectors	1.0 MB					0	
Partition 1	100 MB					2,048	
Partition 2	39.9 GB					206,848	
Unpartitionable space	1.0 MB					83,884,032	

```
Offset        0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
0000000000   33 C0 8E D0 BC 00 7C 8E  C0 8E D8 BE 00 7C BF 00   3ÀŽÐ¼ |ŽÀŽØ¾ |¿
0000000016   06 B9 00 02 FC F3 A4 50  68 1C 06 CB FB B9 04 00    ¹  üó¤Ph  Ëû¹
0000000032   BD BE 07 80 7E 00 00 7C  0B 0F 85 0E 01 83 C5 10   ½¾ €~  |  …  ƒÅ
0000000048   E2 F1 CD 18 88 56 00 55  C6 46 11 05 C6 46 10 00   âñÍ ˆV UÆF  ÆF
0000000064   B4 41 BB AA 55 CD 13 5D  72 0F 81 FB 55 AA 75 09   ´A»ªUÍ ]r  ûUªu
0000000080   F7 C1 01 00 74 03 FE 46  10 66 60 80 7E 10 00 74   ÷Á  t þF f`€~  t
0000000096   26 66 68 00 00 00 00 66  FF 76 08 68 00 00 68 00   &fh    fÿv h  h
0000000112   7C 68 01 00 68 10 00 B4  42 8A 56 00 8B F4 CD 13   |h  h  ´BŠV ‹ôÍ
0000000128   9F 83 C4 10 9E EB 14 B8  01 02 BB 00 7C 8A 56 00   ŸƒÄ žë ¸  » |ŠV
0000000144   8A 76 01 8A 4E 02 8A 6E  03 CD 13 66 61 73 1C FE   Šv ŠN Šn Í fas þ
0000000160   4E 11 75 0C 80 7E 00 80  0F 84 8A 00 B2 80 EB 84   N u €~ € „Š ²€ë„
0000000176   55 32 E4 8A 56 00 CD 13  5D EB 9E 81 3E FE 7D 55   U2äŠV Í ]ëž >þ}U
0000000192   AA 75 6E FF 76 00 E8 8D  00 75 17 FA B0 D1 E6 64   ªunÿv è  u ú°Ñæd
0000000208   E8 83 00 B0 DF E6 60 E8  7C 00 B0 FF E6 64 E8 75   èƒ °ßæ`è| °ÿædèu
0000000224   00 FB B8 00 BB CD 1A 66  23 C0 75 3B 66 81 FB 54    û¸ »Í f#Àu;f ûT
0000000240   43 50 41 75 32 81 F9 02  01 72 2C 66 68 07 BB 00   CPAu2 ù  r,fh »
0000000256   00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66    fh    fh    fSf
0000000272   53 66 55 66 68 00 00 00  00 66 68 00 7C 00 00 66   SfUfh    fh |  f
0000000288   61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD   ah   Í Z2öê |  Í
0000000304   18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4     · ë  ¶ ë  µ 2ä
0000000320   05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD     ‹ð¬< t »  ´ Í
0000000336   10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8    ëòôëý+Éädë $ àø
0000000352   24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69   $ ÃInvalid parti
0000000368   74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72   tion table Error
```

Hard disk 2
Model: f-switch x86-win7-sub
Serial No.: DIsk-0-40960mb
Firmware Rev.: 0001
Bus: SCSI/SATA

In-place mode!

Undo level: 0
Undo reverses: n/a

Total capacity: 40.0 GB
42,949,672,960 bytes

Bytes per sector: 512
Surplus sectors at end: 2048

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

Mode: Text
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 24x16=384

Window #: 1
No. of windows: 1

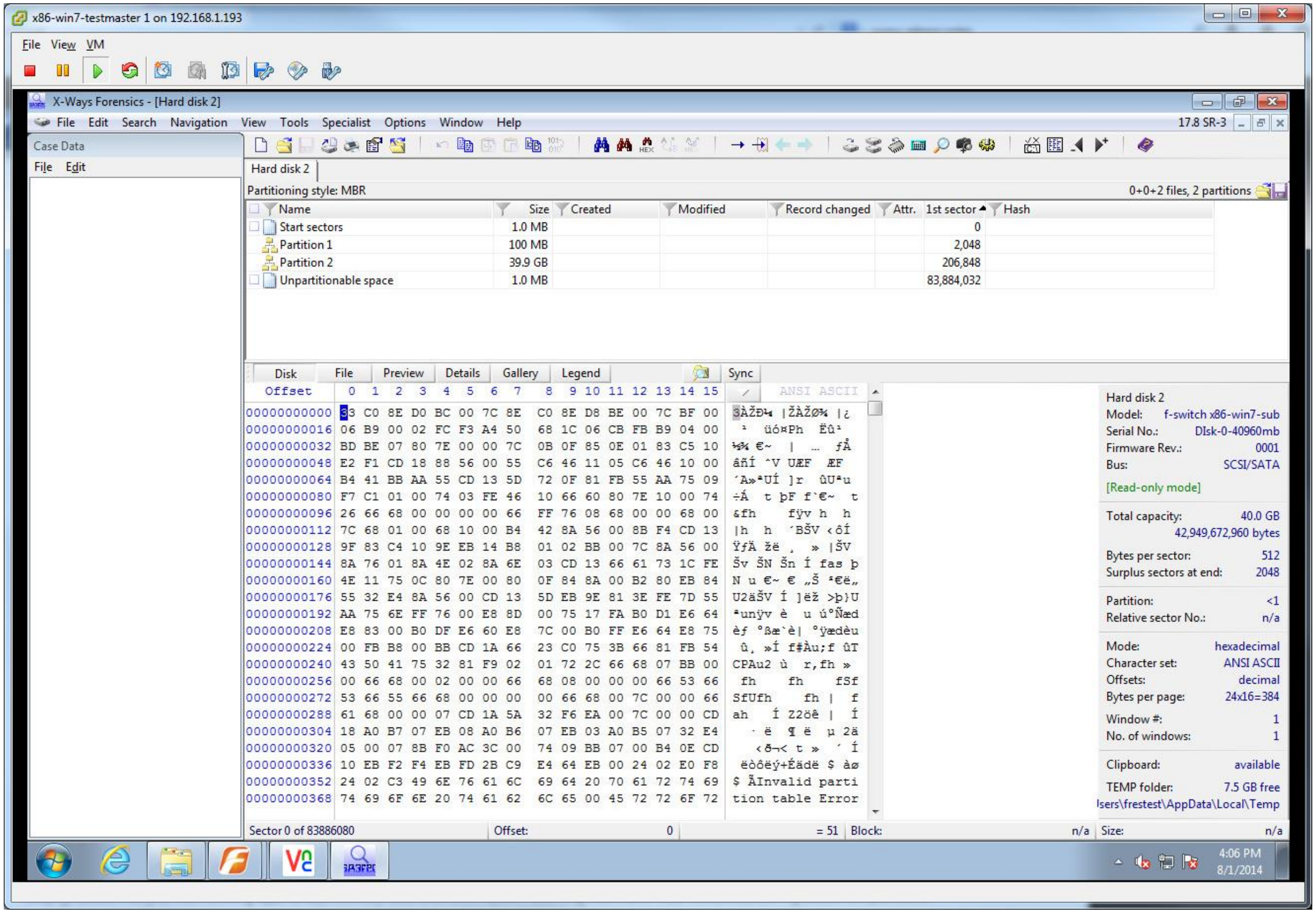
Clipboard: available

Sector 0 of 83886080 | Offset: 0 | = 51 | Block: n/a | Size: n/a

Step 2, Note Total capacity. Divide total number of bytes by number of bytes per sector to obtain total sector count

READ ACCURACY TESTING – WINHEX, X-WAYS

Step 1, Open F-Response Now/Universal presented disk/share in X-Ways. Note total number of bytes and bytes per sector and compare to baseline.


x86-win7-testmaster 1 on 192.168.1.193
File View VM
X-Ways Forensics - [Hard disk 2]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
Hard disk 2
Disk File Preview Details Gallery Legend Sync

Partitioning style: MBR

0+0+2 files, 2 partitions

Name	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
Start sectors	1.0 MB					0	
Partition 1	100 MB					2,048	
Partition 2	39.9 GB					206,848	
Unpartitionable space	1.0 MB					83,884,032	

```
     Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15    ANSI ASCII
00000000000 33 C0 8E D0 BC 00 7C 8E  C0 8E D8 BE 00 7C BF 00  3ÀŽÐ¼ |ŽÀŽØ¾ |¿
00000000016 06 B9 00 02 FC F3 A4 50  68 1C 06 CB FB B9 04 00   ¹  üó¤Ph  Ëû¹
00000000032 BD BE 07 80 7E 00 00 7C  0B 0F 85 0E 01 83 C5 10  ½¾ €~  |  …  ƒÅ
00000000048 E2 F1 CD 18 88 56 00 55  C6 46 11 05 C6 46 10 00  âñÍ ˆV UÆF  ÆF
00000000064 B4 41 BB AA 55 CD 13 5D  72 0F 81 FB 55 AA 75 09  ´A»ªUÍ ]r  ûUªu
00000000080 F7 C1 01 00 74 03 FE 46  10 66 60 80 7E 10 00 74  ÷Á  t þF f`€~  t
00000000096 26 66 68 00 00 00 00 66  FF 76 08 68 00 00 68 00  &fh    fÿv h  h
00000000112 7C 68 01 00 68 10 00 B4  42 8A 56 00 8B F4 CD 13  |h  h  ´BŠV ‹ôÍ
00000000128 9F 83 C4 10 9E EB 14 B8  01 02 BB 00 7C 8A 56 00  ŸƒÄ žë ¸  » |ŠV
00000000144 8A 76 01 8A 4E 02 8A 6E  03 CD 13 66 61 73 1C FE  Šv ŠN Šn Í fas þ
00000000160 4E 11 75 0C 80 7E 00 80  0F 84 8A 00 B2 80 EB 84  N u €~ € „Š ²€ë„
00000000176 55 32 E4 8A 56 00 CD 13  5D EB 9E 81 3E FE 7D 55  U2äŠV Í ]ëž >þ}U
00000000192 AA 75 6E FF 76 00 E8 8D  00 75 17 FA B0 D1 E6 64  ªunÿv è  u ú°Ñæd
00000000208 E8 83 00 B0 DF E6 60 E8  7C 00 B0 FF E6 64 E8 75  èƒ °ßæ`è| °ÿædèu
00000000224 00 FB B8 00 BB CD 1A 66  23 C0 75 3B 66 81 FB 54   û¸ »Í f#Àu;f ûT
00000000240 43 50 41 75 32 81 F9 02  01 72 2C 66 68 07 BB 00  CPAu2 ù  r,fh »
00000000256 00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66   fh    fh    fSf
00000000272 53 66 55 66 68 00 00 00  00 66 68 00 7C 00 00 66  SfUfh    fh |  f
00000000288 61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD  ah   Í Z2öê |  Í
00000000304 18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4    · ë  ¶ ë  µ 2ä
00000000320 05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD     ‹ð¬< t »  ´ Í
00000000336 10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8   ëòôëý+Éädë $ àø
00000000352 24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69  $ ÃInvalid parti
00000000368 74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72  tion table Error
```

Sector 0 of 83886080 | Offset: 0 | = 51 | Block: n/a | Size: n/a

Hard disk 2
Model: f-switch x86-win7-sub
Serial No.: DIsk-0-40960mb
Firmware Rev.: 0001
Bus: SCSI/SATA
[Read-only mode]

Total capacity: 40.0 GB
42,949,672,960 bytes

Bytes per sector: 512
Surplus sectors at end: 2048

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

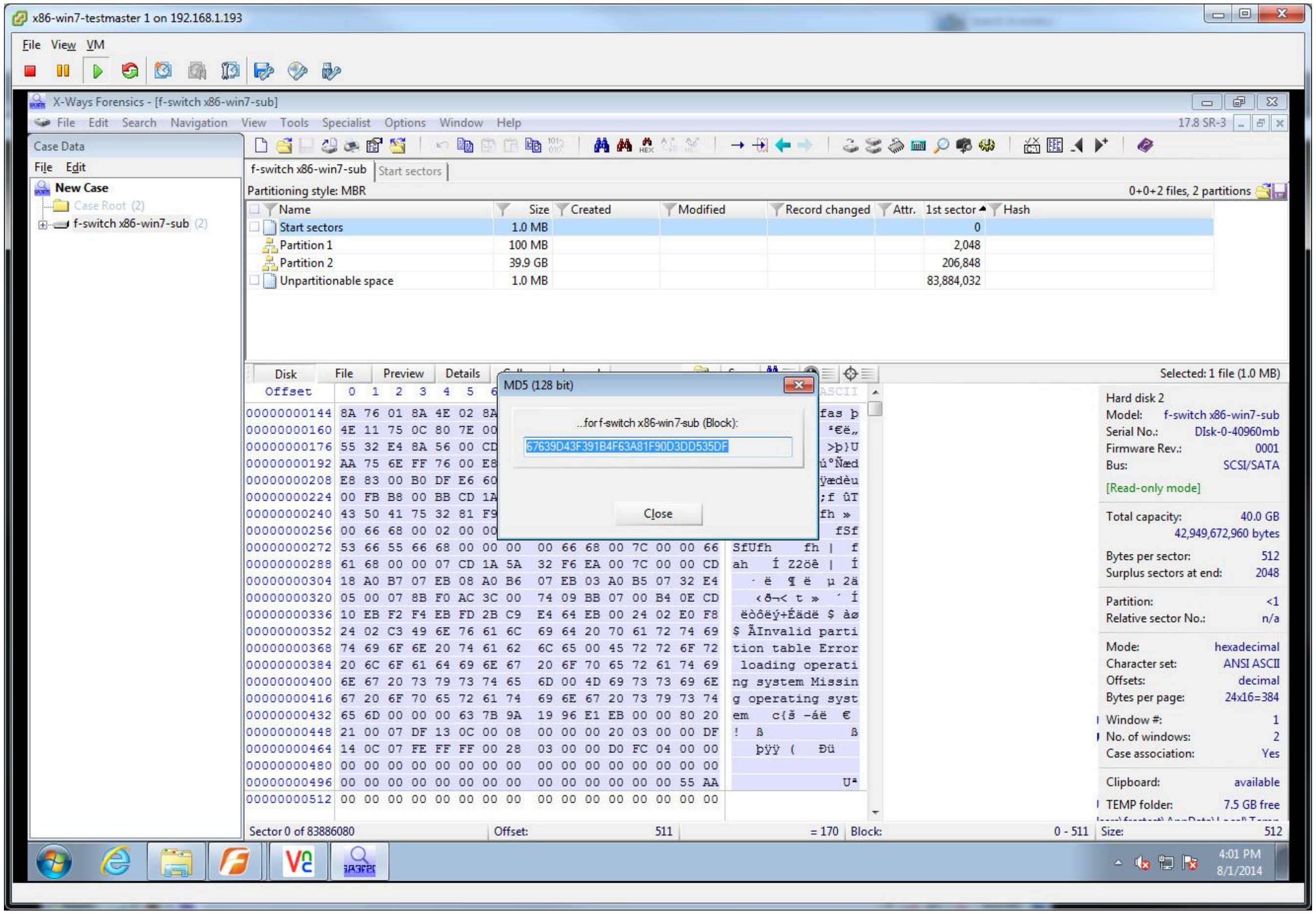
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 24x16=384

Window #: 1
No. of windows: 1

Clipboard: available

TEMP folder: 7.5 GB free
Isers\frestest\AppData\Local\Temp

Step 2,Select the sector of disk hashed previously during the baseline gathering phase. Press Ctrl-F2 to bring up the hashing dialog. Select MD5 as the hashing type and press Ok, record and compare resulting hash with hash obtained during baseline operation.



x86-win7-testmaster 1 on 192.168.1.193
File View VM
X-Ways Forensics - [f-switch x86-win7-sub]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
New Case
Case Root (2)
f-switch x86-win7-sub (2)
f-switch x86-win7-sub
Start sectors
Disk
File
Preview
Details

Partitioning style: MBR 0+0+2 files, 2 partitions

Name	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
Start sectors	1.0 MB					0	
Partition 1	100 MB					2,048	
Partition 2	39.9 GB					206,848	
Unpartitionable space	1.0 MB					83,884,032	

Selected: 1 file (1.0 MB)

MD5 (128 bit)

...for f-switch x86-win7-sub (Block):

67639D43F391B4F63A81F90D3DD535DF

Close

```
Offset       0  1  2  3  4  5  6
00000000144 8A 76 01 8A 4E 02 8A                                        fas þ
00000000160 4E 11 75 0C 80 7E 00                                         ᵃ€ë„
00000000176 55 32 E4 8A 56 00 CD                                        >þ}U
00000000192 AA 75 6E FF 76 00 E8                                        ú°Ñæd
00000000208 E8 83 00 B0 DF E6 60                                        ÿædèu
00000000224 00 FB B8 00 BB CD 1A                                        ;f ûT
00000000240 43 50 41 75 32 81 F9                                        fh »
00000000256 00 66 68 00 02 00 00                                          fSf
00000000272 53 66 55 66 68 00 00 00  00 66 68 00 7C 00 00 66  SfUfh    fh |  f
00000000288 61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD  ah   Í Z2öê |  Í
00000000304 18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4    · ë  ¶ ë  µ 2ä
00000000320 05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD    ‹ð¬< t »  ´ Í
00000000336 10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8   ëòôëý+Éädë $ àø
00000000352 24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69  $ ÃInvalid parti
00000000368 74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72  tion table Error
00000000384 20 6C 6F 61 64 69 6E 67  20 6F 70 65 72 61 74 69   loading operati
00000000400 6E 67 20 73 79 73 74 65  6D 00 4D 69 73 73 69 6E  ng system Missin
00000000416 67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74  g operating syst
00000000432 65 6D 00 00 00 63 7B 9A  19 96 E1 EB 00 00 80 20  em   c{š –áë  €
00000000448 21 00 07 DF 13 0C 00 08  00 00 00 20 03 00 00 DF  !  ß            ß
00000000464 14 0C 07 FE FF FF 00 28  03 00 00 D0 FC 04 00 00    þÿÿ (   Ðü
00000000480 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000496 00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA                Uª
00000000512 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Hard disk 2
Model: f-switch x86-win7-sub
Serial No.: DIsk-0-40960mb
Firmware Rev.: 0001
Bus: SCSI/SATA
[Read-only mode]

Total capacity: 40.0 GB
42,949,672,960 bytes

Bytes per sector: 512
Surplus sectors at end: 2048

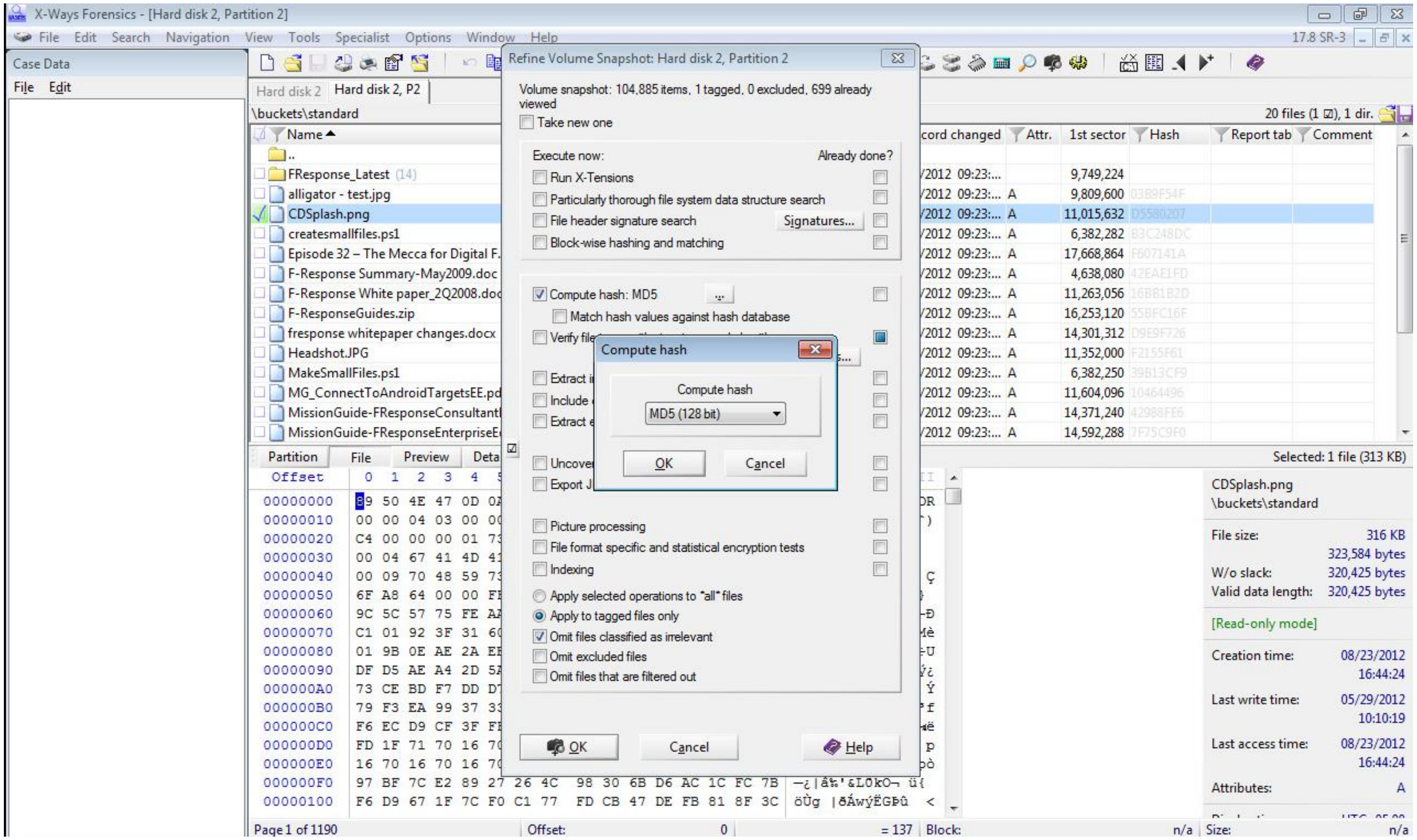
Partition: <1
Relative sector No.: n/a

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 24x16=384
Window #: 1
No. of windows: 2
Case association: Yes

Clipboard: available
TEMP folder: 7.5 GB free

Sector 0 of 83886080 | Offset: 511 | = 170 | Block: 0 - 511 | Size: 512

Step 3, Browse and select file. Choose Specialist->Refine Volume Snapshot->Compute hash_MD5(128 bit)->Option button for 'Apply to tagged files only'->OK button to calculate Hash value.


X-Ways Forensics - [Hard disk 2, Partition 2]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
Hard disk 2
Hard disk 2, P2
Partition
File
Preview
Deta

Refine Volume Snapshot: Hard disk 2, Partition 2

Volume snapshot: 104,885 items, 1 tagged, 0 excluded, 699 already viewed

□ Take new one

Execute now: / Already done?

- □ Run X-Tensions □
- □ Particularly thorough file system data structure search □
- □ File header signature search (Signatures...) □
- □ Block-wise hashing and matching □
- ☑ Compute hash: MD5 □
- □ Match hash values against hash database
- □ Verify file... ■
- □ Extract i... □
- □ Include ... □
- □ Extract e... □
- □ Uncove... □
- □ Export J... □
- □ Picture processing □
- □ File format specific and statistical encryption tests □
- □ Indexing □

○ Apply selected operations to "all" files

● Apply to tagged files only

☑ Omit files classified as irrelevant

□ Omit excluded files

□ Omit files that are filtered out

OK | Cancel | Help

Compute hash

Compute hash: MD5 (128 bit)

OK | Cancel

\buckets\standard — 20 files (1 ☑), 1 dir.

Name	...cord changed	Attr.	1st sector	Hash
..				
FResponse_Latest (14)	/2012 09:23:...		9,749,224	
alligator - test.jpg	/2012 09:23:...	A	9,809,600	03B9F54F
✓ CDSplash.png	/2012 09:23:...	A	11,015,632	D5580207
createsmallfiles.ps1	/2012 09:23:...	A	6,382,282	B3C248DC
Episode 32 – The Mecca for Digital F...	/2012 09:23:...	A	17,668,864	F607141A
F-Response Summary-May2009.doc	/2012 09:23:...	A	4,638,080	42EAE1FD
F-Response White paper_2Q2008.doc	/2012 09:23:...	A	11,263,056	16B81B2D
F-ResponseGuides.zip	/2012 09:23:...	A	16,253,120	55BFC16F
fresponse whitepaper changes.docx	/2012 09:23:...	A	14,301,312	D9E9F726
Headshot.JPG	/2012 09:23:...	A	11,352,000	F2155F61
MakeSmallFiles.ps1	/2012 09:23:...	A	6,382,250	39B13CF9
MG_ConnectToAndroidTargetsEE.pd...	/2012 09:23:...	A	11,604,096	10464496
MissionGuide-FResponseConsultant...	/2012 09:23:...	A	14,371,240	42988FE6
MissionGuide-FResponseEnterpriseE...	/2012 09:23:...	A	14,592,288	7F75C9F0

Selected: 1 file (313 KB)

```
Offset    0  1  2  3  4  5
00000000  89 50 4E 47 0D 0A
00000010  00 00 04 03 00 00
00000020  C4 00 00 00 01 73
00000030  00 04 67 41 4D 41
00000040  00 09 70 48 59 73
00000050  6F A8 64 00 00 FF
00000060  9C 5C 57 75 FE AA
00000070  C1 01 92 3F 31 60
00000080  01 9B 0E AE 2A EE
00000090  DF D5 AE A4 2D 5A
000000A0  73 CE BD F7 DD D7
000000B0  79 F3 EA 99 37 33
000000C0  F6 EC D9 CF 3F FF
000000D0  FD 1F 71 70 16 70
000000E0  16 70 16 70 16 70
000000F0  97 BF 7C E2 89 27 26 4C  98 30 6B D6 AC 1C FC 7B   —¿|â‰'&L0kÖ¬ ü{
00000100  F6 D9 67 1F 7C F0 C1 77  FD CB 47 DE FB 81 8F 3C   öÙg |ðÁwýËGÞû <
```

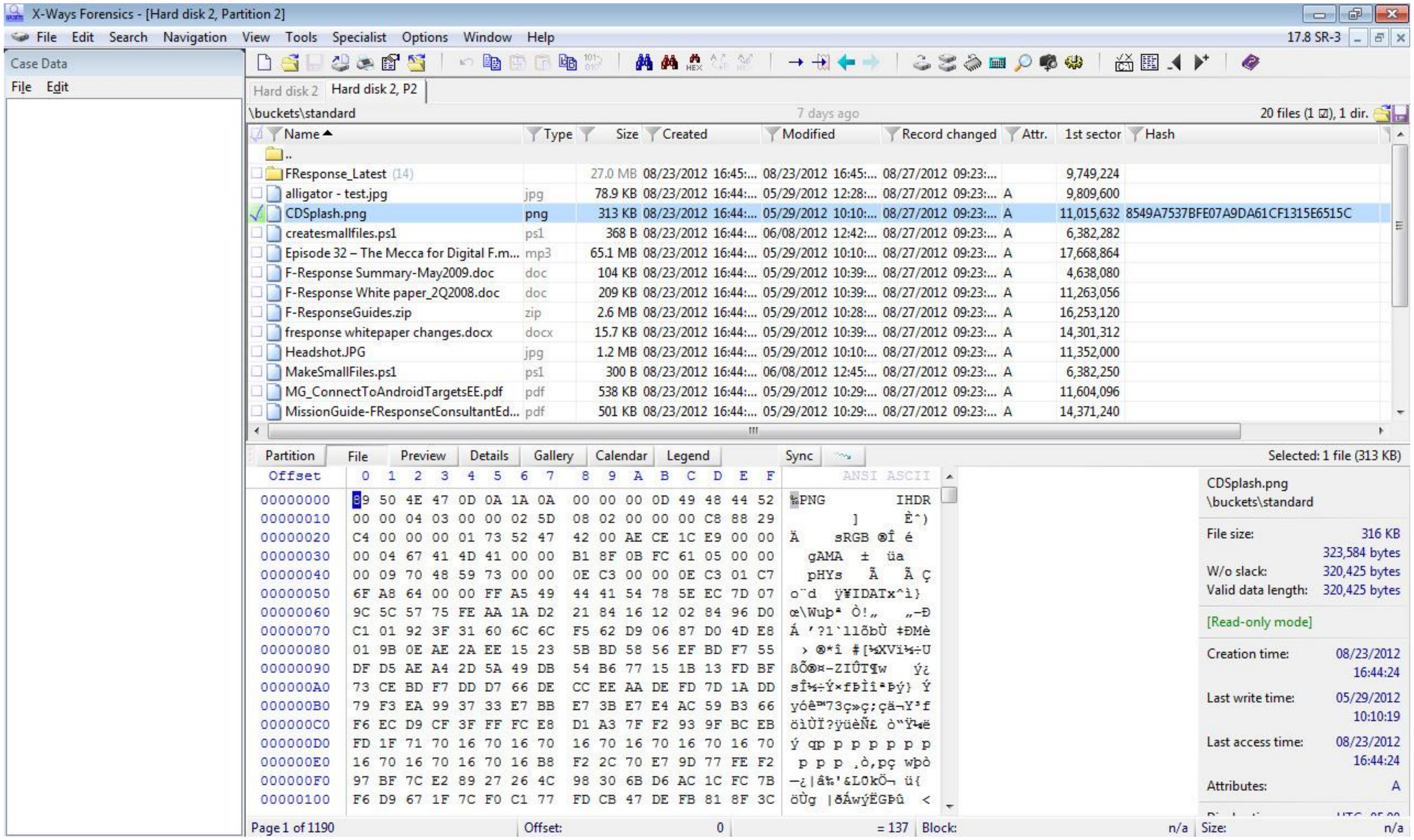
CDSplash.png
\buckets\standard

File size:	316 KB 323,584 bytes
W/o slack:	320,425 bytes
Valid data length:	320,425 bytes

[Read-only mode]

Creation time:	08/23/2012 16:44:24
Last write time:	05/29/2012 10:10:19
Last access time:	08/23/2012 16:44:24
Attributes:	A

Page 1 of 1190 | Offset: 0 | = 137 | Block: n/a | Size: n/a


X-Ways Forensics - [Hard disk 2, Partition 2]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
Hard disk 2
Hard disk 2, P2
Partition File Preview Details Gallery Calendar Legend Sync

\buckets\standard 7 days ago 20 files (1 ☑), 1 dir.

Name	Type	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
..								
FResponse_Latest (14)		27.0 MB	08/23/2012 16:45:...	08/23/2012 16:45:...	08/27/2012 09:23:...		9,749,224	
alligator - test.jpg	jpg	78.9 KB	08/23/2012 16:44:...	05/29/2012 12:28:...	08/27/2012 09:23:...	A	9,809,600	
✓ CDSplash.png	png	313 KB	08/23/2012 16:44:...	05/29/2012 10:10:...	08/27/2012 09:23:...	A	11,015,632	8549A7537BFE07A9DA61CF1315E6515C
createsmallfiles.ps1	ps1	368 B	08/23/2012 16:44:...	06/08/2012 12:42:...	08/27/2012 09:23:...	A	6,382,282	
Episode 32 – The Mecca for Digital F.m...	mp3	65.1 MB	08/23/2012 16:44:...	05/29/2012 10:10:...	08/27/2012 09:23:...	A	17,668,864	
F-Response Summary-May2009.doc	doc	104 KB	08/23/2012 16:44:...	05/29/2012 10:39:...	08/27/2012 09:23:...	A	4,638,080	
F-Response White paper_2Q2008.doc	doc	209 KB	08/23/2012 16:44:...	05/29/2012 10:39:...	08/27/2012 09:23:...	A	11,263,056	
F-ResponseGuides.zip	zip	2.6 MB	08/23/2012 16:44:...	05/29/2012 10:28:...	08/27/2012 09:23:...	A	16,253,120	
fresponse whitepaper changes.docx	docx	15.7 KB	08/23/2012 16:44:...	05/29/2012 10:39:...	08/27/2012 09:23:...	A	14,301,312	
Headshot.JPG	jpg	1.2 MB	08/23/2012 16:44:...	05/29/2012 10:10:...	08/27/2012 09:23:...	A	11,352,000	
MakeSmallFiles.ps1	ps1	300 B	08/23/2012 16:44:...	06/08/2012 12:45:...	08/27/2012 09:23:...	A	6,382,250	
MG_ConnectToAndroidTargetsEE.pdf	pdf	538 KB	08/23/2012 16:44:...	05/29/2012 10:29:...	08/27/2012 09:23:...	A	11,604,096	
MissionGuide-FResponseConsultantEd...	pdf	501 KB	08/23/2012 16:44:...	05/29/2012 10:29:...	08/27/2012 09:23:...	A	14,371,240	

Selected: 1 file (313 KB)

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52   ‰PNG        IHDR
00000010   00 00 04 03 00 00 02 5D  08 02 00 00 00 C8 88 29          ]     È^)
00000020   C4 00 00 00 01 73 52 47  42 00 AE CE 1C E9 00 00   Ä    sRGB ®Î é
00000030   00 04 67 41 4D 41 00 00  B1 8F 0B FC 61 05 00 00     gAMA  ±  üa
00000040   00 09 70 48 59 73 00 00  0E C3 00 00 0E C3 01 C7     pHYs   Ã   Ã Ç
00000050   6F A8 64 00 00 FF A5 49  44 41 54 78 5E EC 7D 07   o¨d  ÿ¥IDATx^ì}
00000060   9C 5C 57 75 FE AA 1A D2  21 84 16 12 02 84 96 D0   œ\Wuþª Ò!„   „–Ð
00000070   C1 01 92 3F 31 60 6C 6C  F5 62 D9 06 87 D0 4D E8   Á ’?1`llõbÙ ‡ÐMè
00000080   01 9B 0E AE 2A EE 15 23  5B BD 58 56 EF BD F7 55    › ®*î #[½XVï½÷U
00000090   DF D5 AE A4 2D 5A 49 DB  54 B6 77 15 1B 13 FD BF   ßÕ®¤-ZIÛT¶w    ý¿
000000A0   73 CE BD F7 DD D7 66 DE  CC EE AA DE FD 7D 1A DD   sÎ½÷Ý×fÞÌîªÞý} Ý
000000B0   79 F3 EA 99 37 33 E7 BB  E7 3B E7 E4 AC 59 B3 66   yóê™73ç»ç;çä¬Y³f
000000C0   F6 EC D9 CF 3F FF FC E8  D1 A3 7F F2 93 9F BC EB   öìÙÏ?ÿüèÑ£ ò“Ÿ¼ë
000000D0   FD 1F 71 70 16 70 16 70  16 70 16 70 16 70 16 70   ý qp p p p p p p
000000E0   16 70 16 70 16 70 16 B8  F2 2C 70 E7 9D 77 FE F2    p p p ¸ò,pç wþò
000000F0   97 BF 7C E2 89 27 26 4C  98 30 6B D6 AC 1C FC 7B   —¿|â‰'&L˜0kÖ¬ ü{
00000100   F6 D9 67 1F 7C F0 C1 77  FD CB 47 DE FB 81 8F 3C   öÙg |ðÁwýËGÞû  <
```

Page 1 of 1190 Offset: 0 = 137 Block: n/a Size: n/a

CDSplash.png
\buckets\standard

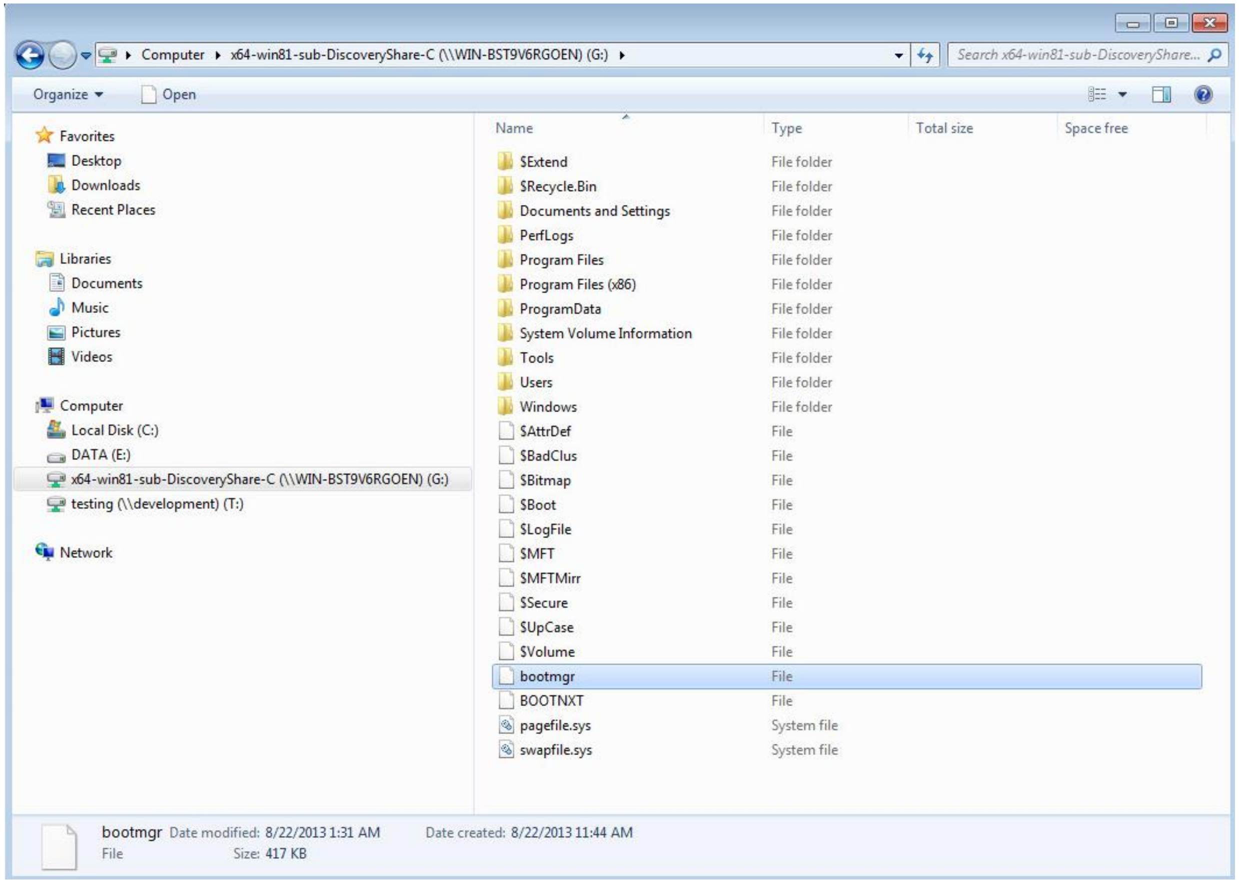
File size: 316 KB
323,584 bytes
W/o slack: 320,425 bytes
Valid data length: 320,425 bytes

[Read-only mode]

Creation time: 08/23/2012 16:44:24
Last write time: 05/29/2012 10:10:19
Last access time: 08/23/2012 16:44:24
Attributes: A

Step 4, Record and review the resulting hash value.

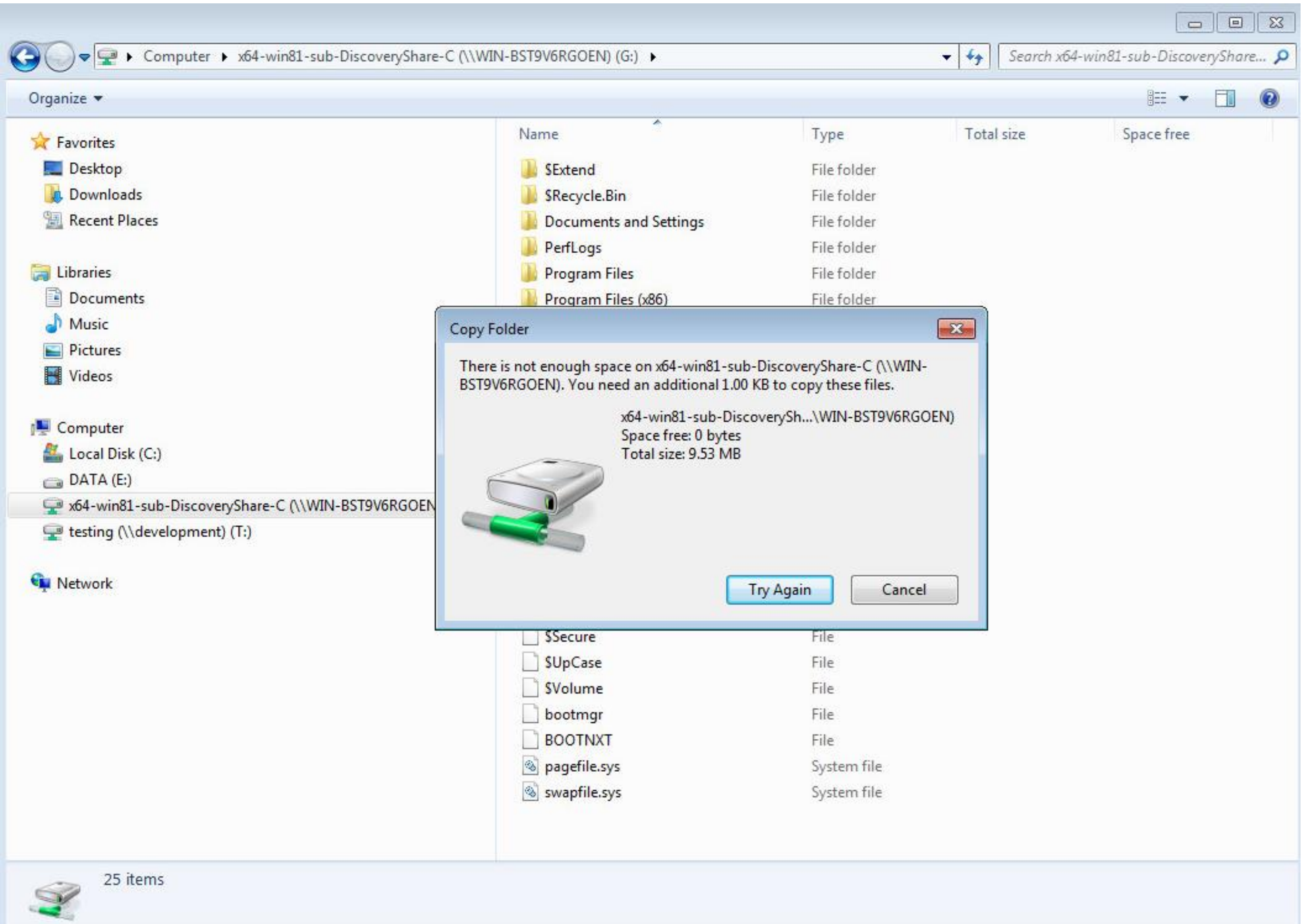
WRITE PREVENTION TESTING – WINDOWS


Computer ▸ x64-win81-sub-DiscoveryShare-C (\\WIN-BST9V6RGOEN) (G:) ▸
Search x64-win81-sub-DiscoveryShare...
Organize ▾
Open
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
DATA (E:)
x64-win81-sub-DiscoveryShare-C (\\WIN-BST9V6RGOEN) (G:)
testing (\\development) (T:)
Network

Name	Type	Total size	Space free
$Extend	File folder		
$Recycle.Bin	File folder		
Documents and Settings	File folder		
PerfLogs	File folder		
Program Files	File folder		
Program Files (x86)	File folder		
ProgramData	File folder		
System Volume Information	File folder		
Tools	File folder		
Users	File folder		
Windows	File folder		
$AttrDef	File		
$BadClus	File		
$Bitmap	File		
$Boot	File		
$LogFile	File		
$MFT	File		
$MFTMirr	File		
$Secure	File		
$UpCase	File		
$Volume	File		
bootmgr	File		
BOOTNXT	File		
pagefile.sys	System file		
swapfile.sys	System file		

bootmgr Date modified: 8/22/2013 1:31 AM Date created: 8/22/2013 11:44 AM
File Size: 417 KB

Step 1, Open newly mounted F-Response Now/Universal Discovery Share, select a file, type Delete or Shift+Delete to attempt to delete the file--Option does not exist.


Computer ▸ x64-win81-sub-DiscoveryShare-C (\\WIN-BST9V6RGOEN) (G:) ▸
Search x64-win81-sub-DiscoveryShare...
Organize
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
DATA (E:)
x64-win81-sub-DiscoveryShare-C (\\WIN-BST9V6RGOEN
testing (\\development) (T:)
Network
25 items

Name	Type	Total size	Space free
$Extend	File folder		
$Recycle.Bin	File folder		
Documents and Settings	File folder		
PerfLogs	File folder		
Program Files	File folder		
Program Files (x86)	File folder		
$Secure	File		
$UpCase	File		
$Volume	File		
bootmgr	File		
BOOTNXT	File		
pagefile.sys	System file		
swapfile.sys	System file		

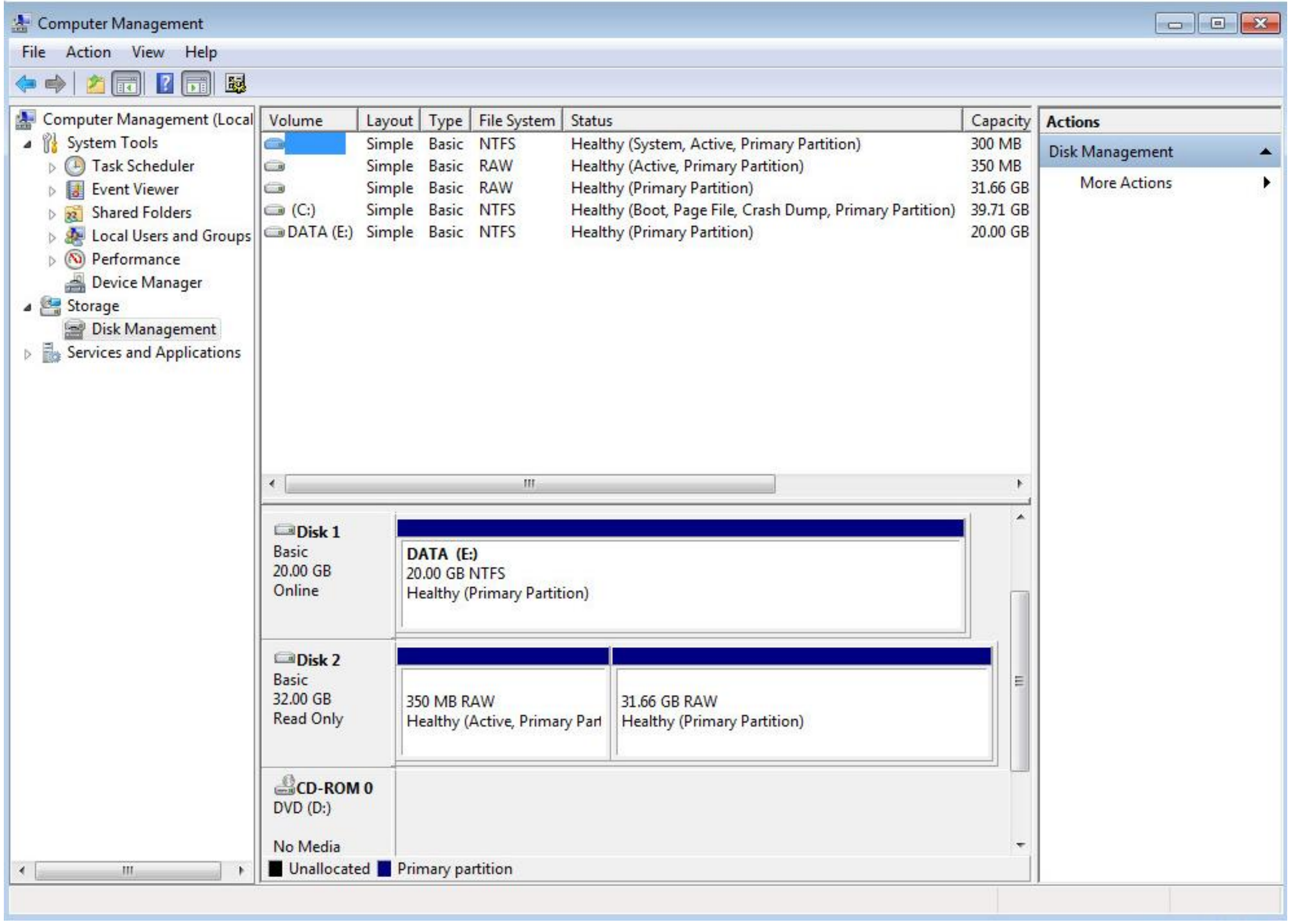
Copy Folder

There is not enough space on x64-win81-sub-DiscoveryShare-C (\\WIN-BST9V6RGOEN). You need an additional 1.00 KB to copy these files.

x64-win81-sub-DiscoverySh...\WIN-BST9V6RGOEN)
Space free: 0 bytes
Total size: 9.53 MB

Step 2, Select a file from the local disk and attempt to copy and paste it to the F-Response Now/Universal Discovery Share.

Step 3, Open Disk Manager to review the F-Response Now/Universal presented physical disk. Note the system sees the disk as Read Only.



Volume	Layout	Type	File System	Status	Capacity
	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	300 MB
	Simple	Basic	RAW	Healthy (Active, Primary Partition)	350 MB
	Simple	Basic	RAW	Healthy (Primary Partition)	31.66 GB
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	39.71 GB
DATA (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	20.00 GB

Disk 1
Basic
20.00 GB
Online

DATA (E:)
20.00 GB NTFS
Healthy (Primary Partition)

Disk 2
Basic
32.00 GB
Read Only

350 MB RAW
Healthy (Active, Primary Part

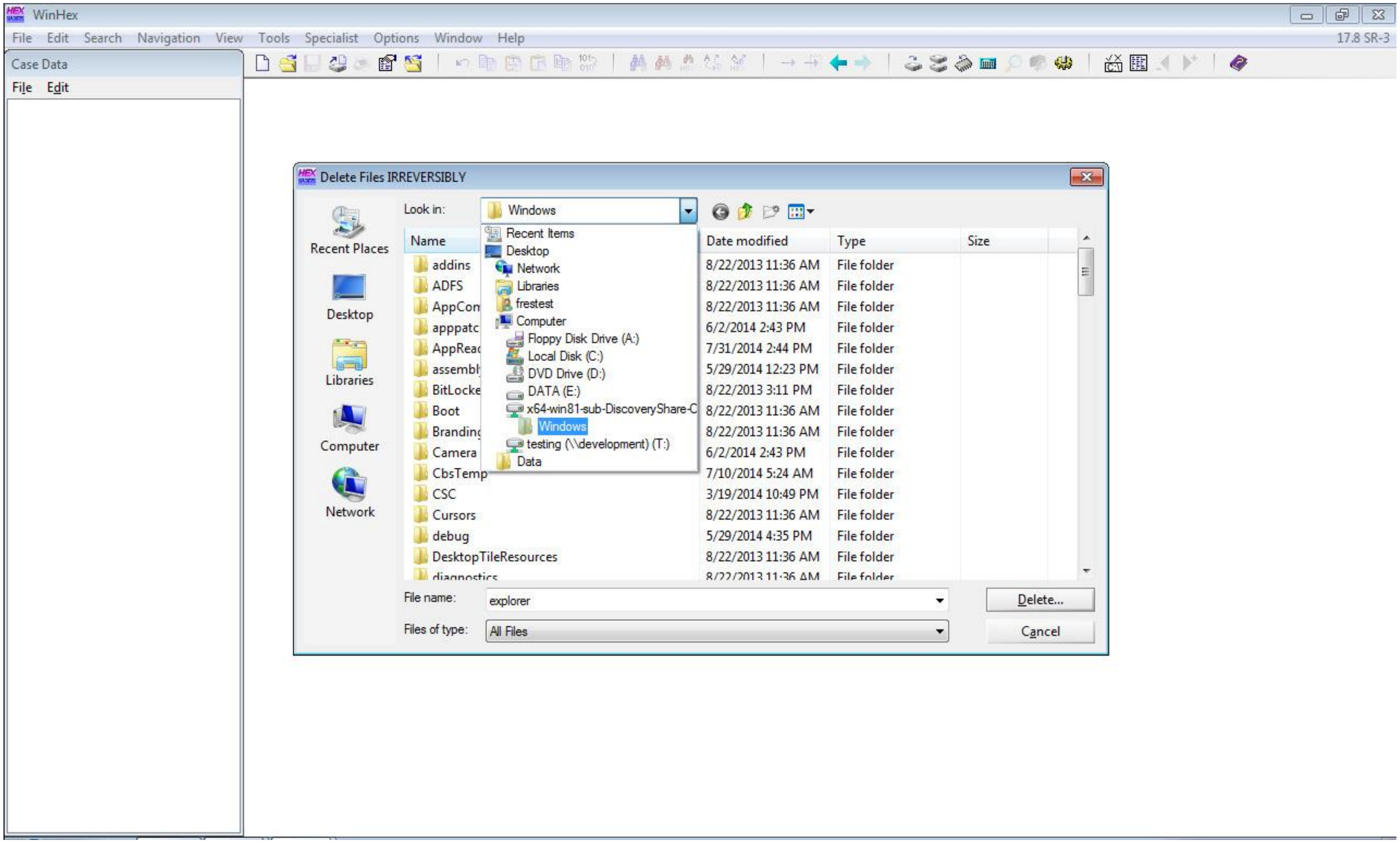
31.66 GB RAW
Healthy (Primary Partition)

CD-ROM 0
DVD (D:)

No Media

■ Unallocated ■ Primary partition

Step 4, Open WinHex and navigate to Tools ->File Tools->Wipe Securely->Choose a file from the F-Response Now/Universal presented source(s)



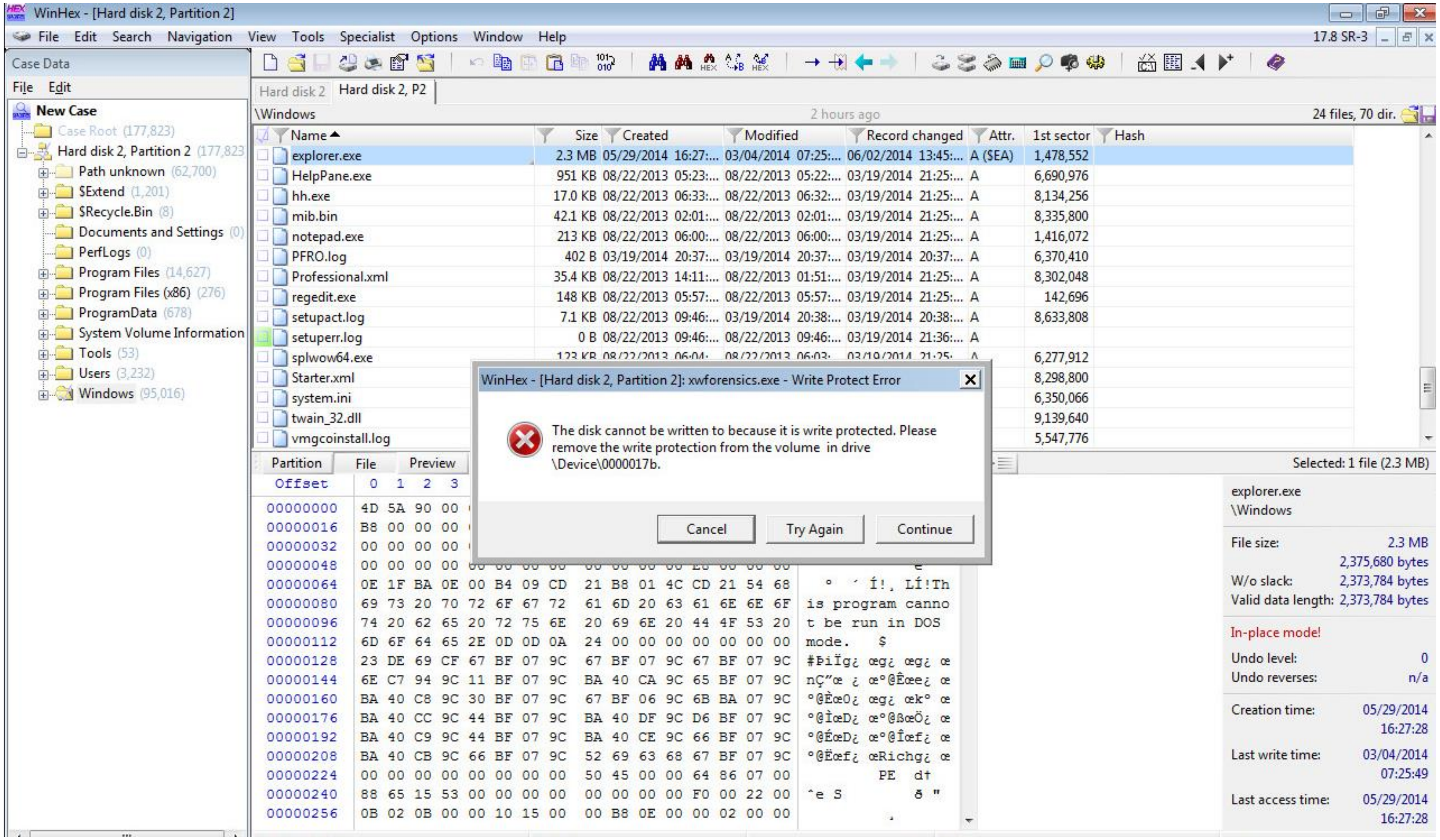
Look in: Windows

Name	Date modified	Type	Size
addins	8/22/2013 11:36 AM	File folder	
ADFS	8/22/2013 11:36 AM	File folder	
AppCon	8/22/2013 11:36 AM	File folder	
apppatc	6/2/2014 2:43 PM	File folder	
AppRead	7/31/2014 2:44 PM	File folder	
assembl	5/29/2014 12:23 PM	File folder	
BitLocke	8/22/2013 3:11 PM	File folder	
Boot	8/22/2013 11:36 AM	File folder	
Branding	8/22/2013 11:36 AM	File folder	
Camera	6/2/2014 2:43 PM	File folder	
CbsTemp	7/10/2014 5:24 AM	File folder	
CSC	3/19/2014 10:49 PM	File folder	
Cursors	8/22/2013 11:36 AM	File folder	
debug	5/29/2014 4:35 PM	File folder	
DesktopTileResources	8/22/2013 11:36 AM	File folder	
diagnostics	8/22/2013 11:36 AM	File folder	

File name: explorer

Files of type: All Files

Step 5, ->Click Delete->OK->OK



\Windows 2 hours ago 24 files, 70 dir.

Name ▲	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
explorer.exe	2.3 MB	05/29/2014 16:27:...	03/04/2014 07:25:...	06/02/2014 13:45:...	A ($EA)	1,478,552	
HelpPane.exe	951 KB	08/22/2013 05:23:...	08/22/2013 05:22:...	03/19/2014 21:25:...	A	6,690,976	
hh.exe	17.0 KB	08/22/2013 06:33:...	08/22/2013 06:32:...	03/19/2014 21:25:...	A	8,134,256	
mib.bin	42.1 KB	08/22/2013 02:01:...	08/22/2013 02:01:...	03/19/2014 21:25:...	A	8,335,800	
notepad.exe	213 KB	08/22/2013 06:00:...	08/22/2013 06:00:...	03/19/2014 21:25:...	A	1,416,072	
PFRO.log	402 B	03/19/2014 20:37:...	03/19/2014 20:37:...	03/19/2014 20:37:...	A	6,370,410	
Professional.xml	35.4 KB	08/22/2013 14:11:...	08/22/2013 01:51:...	03/19/2014 21:25:...	A	8,302,048	
regedit.exe	148 KB	08/22/2013 05:57:...	08/22/2013 05:57:...	03/19/2014 21:25:...	A	142,696	
setupact.log	7.1 KB	08/22/2013 09:46:...	03/19/2014 20:38:...	03/19/2014 20:38:...	A	8,633,808	
setuperr.log	0 B	08/22/2013 09:46:...	08/22/2013 09:46:...	03/19/2014 21:36:...	A		
splwow64.exe	123 KB	08/22/2013 06:04:...	08/22/2013 06:03:...	03/19/2014 21:25:...	A	6,277,912	
Starter.xml						8,298,800	
system.ini						6,350,066	
twain_32.dll						9,139,640	
vmgcoinstall.log						5,547,776	

Selected: 1 file (2.3 MB)

WinHex - [Hard disk 2, Partition 2]: xwforensics.exe - Write Protect Error

The disk cannot be written to because it is write protected. Please remove the write protection from the volume in drive \Device\0000017b.

Cancel | Try Again | Continue

```
Offset     0  1  2  3
00000000  4D 5A 90 00
00000016  B8 00 00 00
00000032  00 00 00 00
00000048  00 00 00 00
00000064  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68    º  ´ Í!¸ LÍ!Th
00000080  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00000096  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS
00000112  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode.   $
00000128  23 DE 69 CF 67 BF 07 9C  67 BF 07 9C 67 BF 07 9C  #ÞiÏg¿ œg¿ œg¿ œ
00000144  6E C7 94 9C 11 BF 07 9C  BA 40 CA 9C 65 BF 07 9C  nÇ"œ ¿ œº@Êœe¿ œ
00000160  BA 40 C8 9C 30 BF 07 9C  67 BF 06 9C 6B BA 07 9C  º@Èœ0¿ œg¿ œkº œ
00000176  BA 40 CC 9C 44 BF 07 9C  BA 40 DF 9C D6 BF 07 9C  º@ÌœD¿ œº@ßœÖ¿ œ
00000192  BA 40 C9 9C 44 BF 07 9C  BA 40 CE 9C 66 BF 07 9C  º@ÉœD¿ œº@Îœf¿ œ
00000208  BA 40 CB 9C 66 BF 07 9C  52 69 63 68 67 BF 07 9C  º@Ëœf¿ œRichg¿ œ
00000224  00 00 00 00 00 00 00 00  50 45 00 00 64 86 07 00          PE  d†
00000240  88 65 15 53 00 00 00 00  00 00 00 00 F0 00 22 00  ˆe S        ð "
00000256  0B 02 0B 00 00 10 15 00  00 B8 0E 00 00 02 00 00           ¸
```

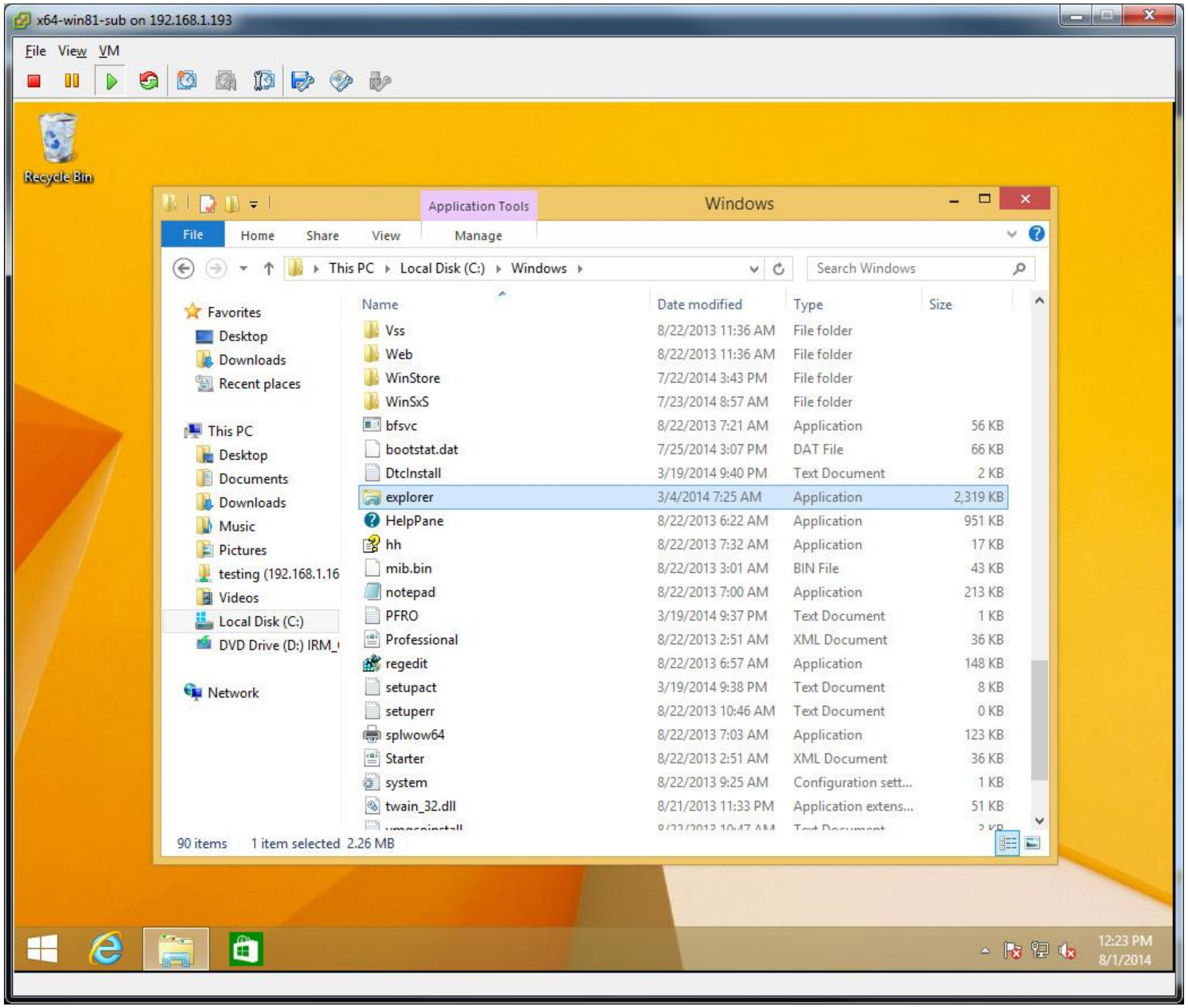
explorer.exe
\Windows

File size:	2.3 MB 2,375,680 bytes
W/o slack:	2,373,784 bytes
Valid data length:	2,373,784 bytes

In-place mode!

Undo level:	0
Undo reverses:	n/a
Creation time:	05/29/2014 16:27:28
Last write time:	03/04/2014 07:25:49
Last access time:	05/29/2014 16:27:28

Step 6, Return to F-Response Now/Universal testing computer, confirm no data changes have occurred.

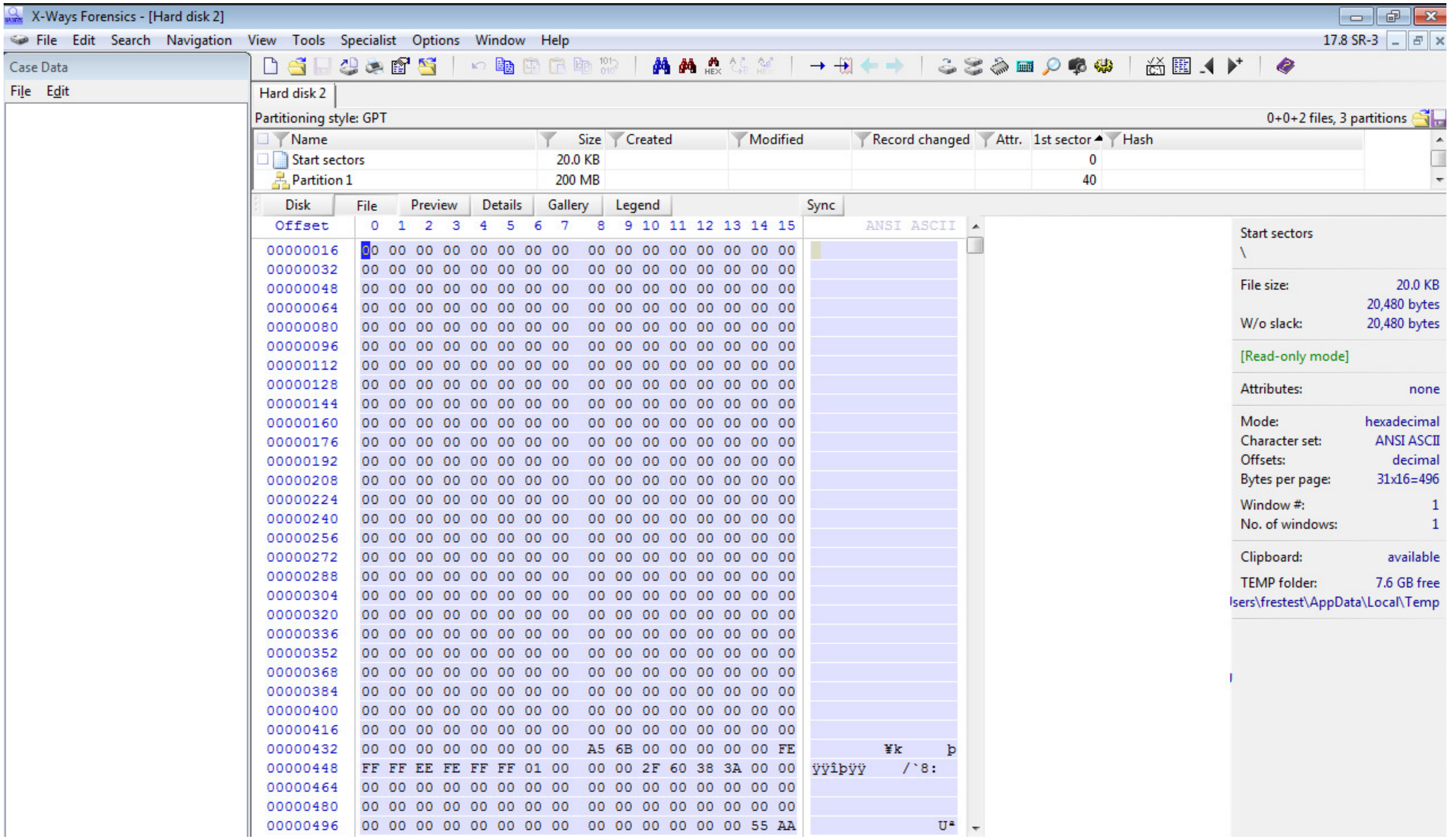


Name	Date modified	Type	Size
Vss	8/22/2013 11:36 AM	File folder	
Web	8/22/2013 11:36 AM	File folder	
WinStore	7/22/2014 3:43 PM	File folder	
WinSxS	7/23/2014 8:57 AM	File folder	
bfsvc	8/22/2013 7:21 AM	Application	56 KB
bootstat.dat	7/25/2014 3:07 PM	DAT File	66 KB
DtcInstall	3/19/2014 9:40 PM	Text Document	2 KB
explorer	3/4/2014 7:25 AM	Application	2,319 KB
HelpPane	8/22/2013 6:22 AM	Application	951 KB
hh	8/22/2013 7:32 AM	Application	17 KB
mib.bin	8/22/2013 3:01 AM	BIN File	43 KB
notepad	8/22/2013 7:00 AM	Application	213 KB
PFRO	3/19/2014 9:37 PM	Text Document	1 KB
Professional	8/22/2013 2:51 AM	XML Document	36 KB
regedit	8/22/2013 6:57 AM	Application	148 KB
setupact	3/19/2014 9:38 PM	Text Document	8 KB
setuperr	8/22/2013 10:46 AM	Text Document	0 KB
splwow64	8/22/2013 7:03 AM	Application	123 KB
Starter	8/22/2013 2:51 AM	XML Document	36 KB
system	8/22/2013 9:25 AM	Configuration sett...	1 KB
twain_32.dll	8/21/2013 11:33 PM	Application extens...	51 KB
vmgcoinstall	8/22/2013 10:47 AM	Text Document	3 KB

90 items 1 item selected 2.26 MB

WRITE PREVENTION TESTING – LINUX, APPLE OS X

Step 1, Open the attached disk using X-Ways Forensics, record the value of sector zero.


X-Ways Forensics - [Hard disk 2]
File Edit Search Navigation View Tools Specialist Options Window Help
17.8 SR-3
Case Data
File Edit
Hard disk 2
Disk File Preview Details Gallery Legend Sync

Partitioning style: GPT

0+0+2 files, 3 partitions

Name	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
Start sectors	20.0 KB					0	
Partition 1	200 MB					40	

```
  Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15    ANSI ASCII
00000016     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000032     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000048     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000064     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000096     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000112     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000128     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000144     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000176     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000192     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000208     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000224     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000240     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000256     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000272     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000288     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000304     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000320     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000336     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000352     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000368     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000384     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000400     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000416     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000432     00 00 00 00 00 00 00 00  A5 6B 00 00 00 00 00 FE            ¥k     þ
00000448     FF FF EE FE FF FF 01 00  00 00 2F 60 38 3A 00 00    ÿÿîþÿÿ   /`8:
00000464     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000480     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000496     00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA                  Uª
```

Start sectors
\

File size: 20.0 KB
20,480 bytes
W/o slack: 20,480 bytes

[Read-only mode]

Attributes: none

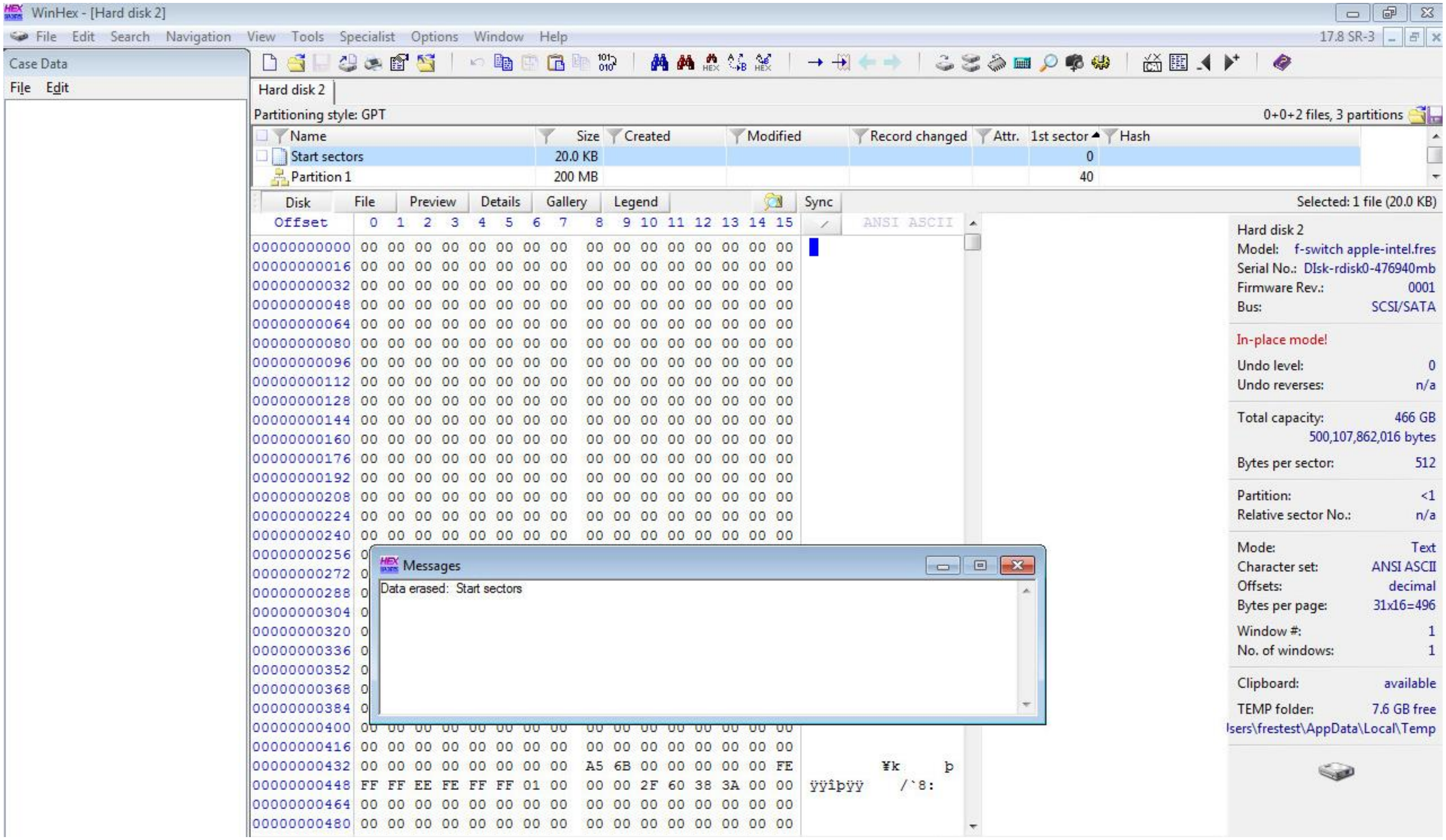
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 31x16=496

Window #: 1
No. of windows: 1

Clipboard: available

TEMP folder: 7.6 GB free
\sers\frestest\AppData\Local\Temp

Step 2, Use Winhex to Wipe Start Sectors securely.



Partitioning style: GPT

0+0+2 files, 3 partitions

Name	Size	Created	Modified	Record changed	Attr.	1st sector	Hash
Start sectors	20.0 KB					0	
Partition 1	200 MB					40	

Selected: 1 file (20.0 KB)

```
Offset        0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
0000000000   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000016   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000032   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000048   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000064   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000080   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000096   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000112   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000128   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000144   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000176   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000192   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000208   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000224   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000240   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000256   0
0000000272   0
0000000288   0
0000000304   0
0000000320   0
0000000336   0
0000000352   0
0000000368   0
0000000384   0
0000000400   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000416   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000432   00 00 00 00 00 00 00 00  A5 6B 00 00 00 00 00 FE          ¥k     þ
0000000448   FF FF EE FE FF FF 01 00  00 00 2F 60 38 3A 00 00   ÿÿîþÿÿ    /`8:
0000000464   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000480   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Messages

Data erased: Start sectors

Hard disk 2
Model: f-switch apple-intel.fres
Serial No.: DIsk-rdisk0-476940mb
Firmware Rev.: 0001
Bus: SCSI/SATA

In-place mode!

Undo level: 0
Undo reverses: n/a

Total capacity: 466 GB
500,107,862,016 bytes

Bytes per sector: 512

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

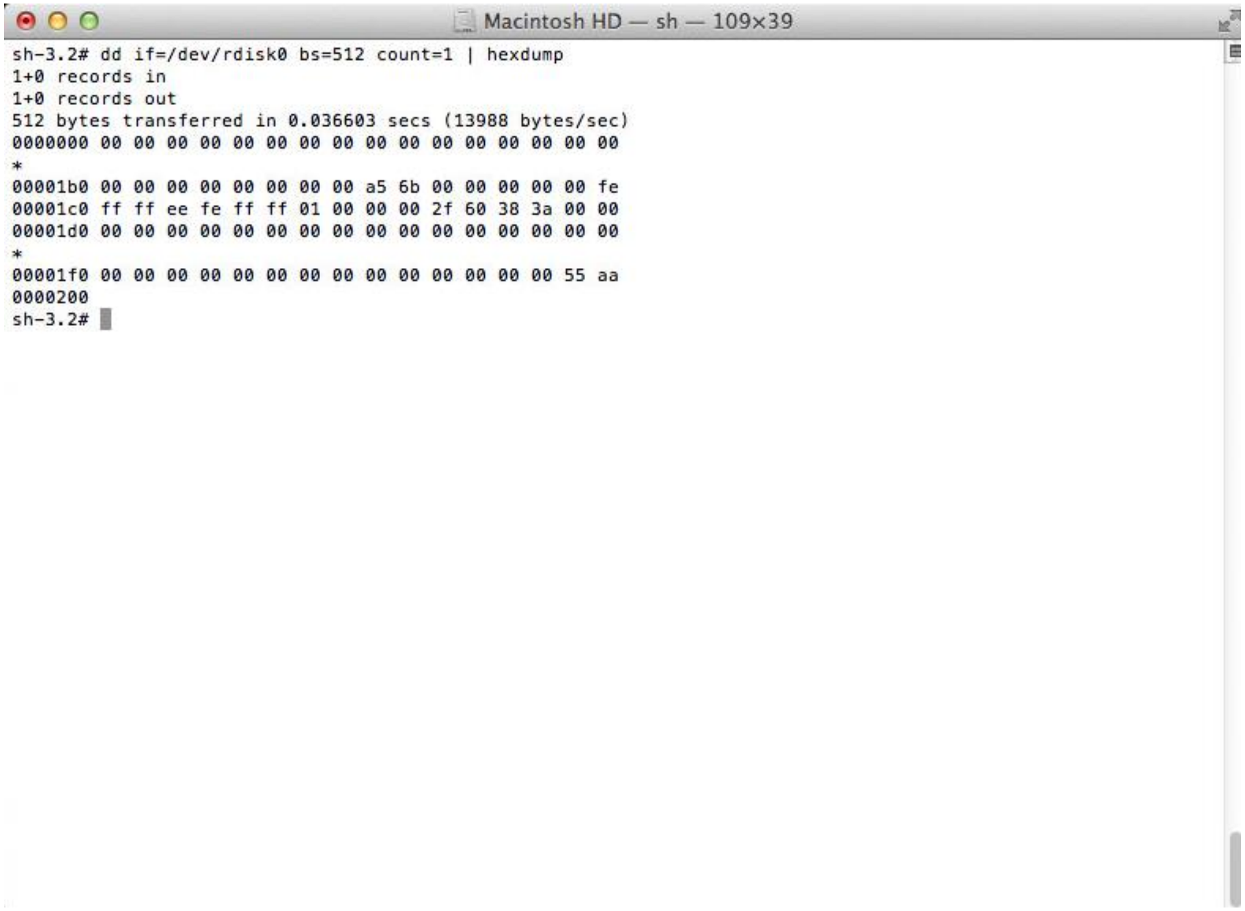
Mode: Text
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 31x16=496

Window #: 1
No. of windows: 1

Clipboard: available

TEMP folder: 7.6 GB free
Isers\frestest\AppData\Local\Temp

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.



```
sh-3.2# dd if=/dev/rdisk0 bs=512 count=1 | hexdump
1+0 records in
1+0 records out
512 bytes transferred in 0.036603 secs (13988 bytes/sec)
0000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
00001b0 00 00 00 00 00 00 00 00 a5 6b 00 00 00 00 00 fe
00001c0 ff ff ee fe ff ff 01 00 00 00 2f 60 38 3a 00 00
00001d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
00001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 aa
0000200
sh-3.2# 
```

APPENDIX A. CONTACTS

Agile Risk Management LLC DBA F-RESPONSE

3333 W Kennedy Blvd Suite 201

Tampa, FL 33609

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

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.

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.

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.