



National University
of computer and emerging sciences

Lab 06

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

Submitted to: Sir Ubaid Ullah

Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

Q1 . Describe the process that you used to add and verify the forensic image?

Ans :

First add the image file in FTK imager. Then go to file and there is an option that is Verify image/Drives. Click this, and it computes Hashes and verifies them.

MD5 Hash	
Computed hash	16556ca8ee3e89dfcf332756bda1320a
Stored verification hash	16556ca8ee3e89dfcf332756bda1320a
Verify result	Match
SHA1 Hash	
Computed hash	3d3dc49eae6ca3a70a50ac9b215a32f4e727422b
Stored verification hash	3d3dc49eae6ca3a70a50ac9b215a32f4e727422b
Verify result	Match

```
Sector count: 254720
[Computed Hashes]
MD5 checksum: 16556ca8ee3e89dfcf332756bda1320a
SHA1 checksum: 3d3dc49eae6ca3a70a50ac9b215a32f4e727422b

Image Information:
Acquisition started: Thu Mar 05 11:41:11 2015
```

So the hashes calculated are the same as the info file given, which proves that the integrity of the file is preserved.

Q2 . List the MD5 and SHA1 hash values associated with the verification?

MD5 : 16556ca8ee3e89dfcf332756bda1320a

SHA1 : 3d3dc49eae6ca3a70a50ac9b215a32f4e727422b

Q3 . What is the volume serial number of this device and explain how you located it?

First you click the Swissbit[NTFS] then you go to properties tab, and there it is written.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- GE2 E01
 - Swissbit [NTFS]
 - [orphan]
 - [root]
 - [unallocated space]

File List

Name	Size	Type	Date Modified
[orphan]	0	Folder (Plac...	
[root]	1	Directory	3/5/2015 11:32:03 ...
[unallocated space]	0	Unallocate...	
backup boot sector	1	Filesystem ...	
file system slack	4	Filesystem ...	

Properties

File System Information

Cluster Size	4,096
Cluster Count	31,839
Free Cluster Count	28,729
Dirty Flag	False
Volume Label	Swissbit
Volume Serial Number	06A9-A40C
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

Volume Serial Number

Hex Value Interpreter Properties

Cursor pos = 0; clus = 0; log sec = 0



Volume Serial Number : 06A9-A40C.

Identify and examine all the picture files that are present at the root level of the device. Explain your findings from this examination?

Filename : Directions.jpg




File name Date Created:	3/4/2015 2:39:31 PM
File name Date Modified:	3/4/2015 11:01:14 AM
File name Date Accessed:	3/4/2015 2:39:31 PM

File name Date Changed:	3/4/2015 2:39:31 PM
MD5	a549f97ad490d71376f1426e66e00feb
SHA1	e60af66c7c2358edb7c377e730c0c5352b40c9a9

 	
Date Changed (MFT)	3/4/2015 2:40:22 PM
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-731122842-1092214498-5375
Group SID	S-1-5-21-731122842-1092214498-5375
Filename Date Created (MFT)	3/4/2015 2:39:31 PM
Filename Date Modified (MFT)	3/4/2015 11:01:14 AM
Filename Date Accessed (MFT)	3/4/2015 2:39:31 PM
Filename Date Changed (MFT)	3/4/2015 2:39:31 PM
Filename File Size (MFT)	118,089
Filename Physical Size (MFT)	118,784
8.3 Filename File Size (MFT)	118,089
8.3 Filename Physical Size (MFT)	118,784

Filename : marijuana-nootropic.jpg

File name Date Created:	3/4/2015 2:39:33 PM
File name Date Modified:	3/4/2015 2:39:33 PM
File name Date Accessed:	3/4/2015 2:39:33 PM
File name Date Changed:	3/4/2015 2:39:33 PM
MD5	146fb88238bd9fcf7de028d63563cffd
SHA1	b387e87b1c3ecaf53744404046f0b99508db71b7

Properties	
  	
Date Changed (MFT)	3/4/2015 2:39:33 PM
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-731122842-1092214498-5375
Group SID	S-1-5-21-731122842-1092214498-5375
Filename Date Created (MFT)	3/4/2015 2:39:33 PM
Filename Date Modified (MFT)	3/4/2015 2:39:33 PM
Filename Date Accessed (MFT)	3/4/2015 2:39:33 PM
Filename Date Changed (MFT)	3/4/2015 2:39:33 PM
Filename File Size (MFT)	0
Filename Physical Size (MFT)	172,032
8.3 Filename File Size (MFT)	0
8.3 Filename Physical Size (MFT)	172,032

Filename : marijuana-weed-drugs.jpg

File name Date Created:	3/4/2015 2:39:36 PM
File name Date Modified:	3/4/2015 2:39:36 PM
File name Date Accessed:	3/4/2015 2:39:36 PM
File name Date Changed:	3/4/2015 2:39:36 PM
MD5	9657de2dd227fdc453c834f10af1b34a
SHA1	fbff085de1958a48d8478c572206fcb3d75dee1a

Date Changed (MFT)	3/4/2015 2:39:36 PM
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-731122842-1092214498-5375
Group SID	S-1-5-21-731122842-1092214498-5375
Filename Date Created (MFT)	3/4/2015 2:39:36 PM
Filename Date Modified (MFT)	3/4/2015 2:39:36 PM
Filename Date Accessed (MFT)	3/4/2015 2:39:36 PM
Filename Date Changed (MFT)	3/4/2015 2:39:36 PM
Filename File Size (MFT)	0
Filename Physical Size (MFT)	147,456
8.3 Filename File Size (MFT)	0
8.3 Filename Physical Size (MFT)	147,456

There are a total of 3 image files, in which one has some directions, and the other 2 are pictures of Drugs.

Q5 . The device is presented with a nominal size of 4 GB. By examining the device and its geometry, explain what the actual size of the physical device is. You should show all calculations that are required to determine this?

Physical Size : $254720 * 512 = 130416640$ Bytes.

$130416640 / 1024 = 127360$ KB.

$127360 / 1024 = 124.375$ MB.

Logical Size : $15 * 255 * 63 * 512 = 123379200$ Bytes.

$123379200 / 1024 = 120487.5$ KB.

120487.5 / 1024 = 117.664 MB.

Q6 . Identify the text file that is present at the root level of the device, explain your findings in relation to it. Validate these findings from the MFT, include any HEX values and calculations that you used?

```
9890 00 00 00 00 00 00 00 00 00-30 00 00 00 70 00 00 00 | -
98a0 00 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 | -
98b0 05 00 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 | -
98c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 | H
98d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 | H
98e0 00 00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00 | -
98f0 0B 03 43 00 6F 00 6E 00-74 00 61 00 63 00 74 00 | -
9900 2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00 | .
```

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	130,700,287,234,594,632
unsigned inte...	1-8	130,700,287,234,594,632
FILETIME (U...	8	3/5/2015 11:32:03 AM
FILETIME (lo...	8	3/5/2015 4:32:03 PM
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	-
time_t (local)	4	-

```
09850 48 D7 A8 00 38 57 D0 01-8D 89 FB FB 37 57 D0 01 | H*
09860 E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01 | 3
09870 23 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | #
09880 00 00 00 00 05 01 00 00-00 00 00 00 00 00 00 00 | .
09890 00 00 00 00 00 00 00 00-30 00 00 00 70 00 00 00 | .
098a0 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 | .
098b0 05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 | .
098c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 | H*
098d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 | H*
098e0 00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00 | .
098f0 0B 03 43 00 6F 00 6E 00-74 00 61 00 63 00 74 00 | .C
09900 2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00 | .t
09910 00 00 18 00 00 00 01 00-17 00 00 00 18 00 00 00 | .
09920 73 74 65 66 61 6E 20 2D-20 30 31 36 31 2D 32 33 | stef
09930 34 38 39 36 32 31 39 00-FF FF FF FF 82 79 47 11 | 4896
09940 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | .
09950 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | .
```

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	130,700,287,234,594,632
unsigned inte...	1-8	130,700,287,234,594,632
FILETIME (U...	8	3/5/2015 11:32:03 AM
FILETIME (lo...	8	3/5/2015 4:32:03 PM
DOS date	2	-



```
09860 E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01 | 3
09870 23 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | #
09880 00 00 00 00 05 01 00 00-00 00 00 00 00 00 00 00 | .
09890 00 00 00 00 00 00 00 00-30 00 00 00 70 00 00 00 | .
098a0 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 | .
098b0 05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 | .
098c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 | H
098d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 | H
098e0 00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00 | .
098f0 0B 03 43 00 6F 00 6E 00-74 00 61 00 63 00 74 00 | .C
```

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	130,700,287,234,594,632
unsigned inte...	1-8	130,700,287,234,594,632
FILETIME (U...	8	3/5/2015 11:32:03 AM
FILETIME (lo...	8	3/5/2015 4:32:03 PM
DOS date	2	-
DOS time	2	-

```
09860 E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01 | 3
09870 23 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | #
09880 00 00 00 00 05 01 00 00-00 00 00 00 00 00 00 00 | .
09890 00 00 00 00 00 00 00 00-30 00 00 00 70 00 00 00 | .
098a0 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 | .
098b0 05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 | .
098c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 | H*
098d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 | H*
098e0 00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00 | .
098f0 0B 03 43 00 6F 00 6E 00-74 00 61 00 63 00 74 00 | .C
09900 2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00 | .t
```

Hex Value Interpreter			09850	48 D7 A8 00 38 57 D0 01-8D 89 FB FB 37 57 D0 01	H
Type	Size	Value	09860	E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01	ä
signed integer	1-8	130,700,287,234,594,632	09870	23 00 00 00 00 00 00 00-00 00 00 00 00 00 00	#
unsigned inte...	1-8	130,700,287,234,594,632	09880	00 00 00 00 05 01 00 00-00 00 00 00 00 00 00	.
FILETIME (U...	8	3/5/2015 11:32:03 AM	09890	00 00 00 00 00 00 00 00-30 00 00 00 70 00 00 00	.
FILETIME (lo...	8	3/5/2015 4:32:03 PM	098a0	00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00	.
DOS date	2	-	098b0	05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01	.
DOS time	2	-	098c0	48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01	H
			098d0	48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00	H
			098e0	00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00	.
			098f0	0B 03 43 00 6F 00 6E 00-74 00 61 00 63 00 74 00	.
			09900	2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00	.

Properties	
 	
File Class	Regular File
File Size	23
Physical Size	24
Date Accessed	3/5/2015 11:32:03 AM
Date Created	3/5/2015 11:32:03 AM
Date Modified	3/5/2015 11:31:55 AM
Encrypted	False
Compressed	False
Actual File	True

So the File Modified in the MFT header is changed because the Data modified is 1 min earlier than File Created.

Q7 . Identify the MFT entry for the file named *marijuana-nootropic.jpg*. On what date and time was the file created and on what date and time was the entry modified? Give you an answer in Universal Time Coordinated (UTC) and show the 64 bit HEX values for each.

Hex Value Interpreter		
Type	Size	Value
signed integer	1-8	130,699,535,739,094,138
unsigned integer	1-8	130,699,535,739,094,138
FILETIME (UTC)	8	3/4/2015 2:39:33 PM
FILETIME (local)	8	3/4/2015 7:39:33 PM
DOS date	2	-

FILE CREATED: 3/4/2015 2:39:33 PM

FILE MODIFIED: 3/4/2015 12:13:22 PM

FILE ACCESSED: 3/4/2015 2:39:33 PM

FILE RECORD: 3/4/2015 2:39:33 PM