

### 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:

☐ MD5 Hash

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.

Computed hash	16556ca8ee3e89dfcf332756bda1320a	
Stored verification hash	16556ca8ee3e89dfcf332756bda1320a	
Verify result	Match	
☐ SHA1 Hash		
Computed hash	3d3dc49eae6ca3a70a50ac9b215a32f4e727422b	
Stored verification hash	3d3dc49eae6ca3a70a50ac9b215a32f4e727422b	
Verify result	Match	
Sector count:	254/20	
[Computed Hashes]		
[compaced mastics]		
MD5 checksum:	16556ca8ee3e89dfcf332756bda1320a	
TIDD CHECKSuiii.	105500000000000000000000000000000000000	
SHA1 checksum:	3d3dc49eae6ca3a70a50ac9b215a32f4e727422b	
SHAI CHECKSUM:	3030C49EdE0Cd3d/0d30dC9DZ13d3Z14E/Z/4ZZD	
T T (		
Image Information		
3		
Acquicition stan	tod: Thu Man OF 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.

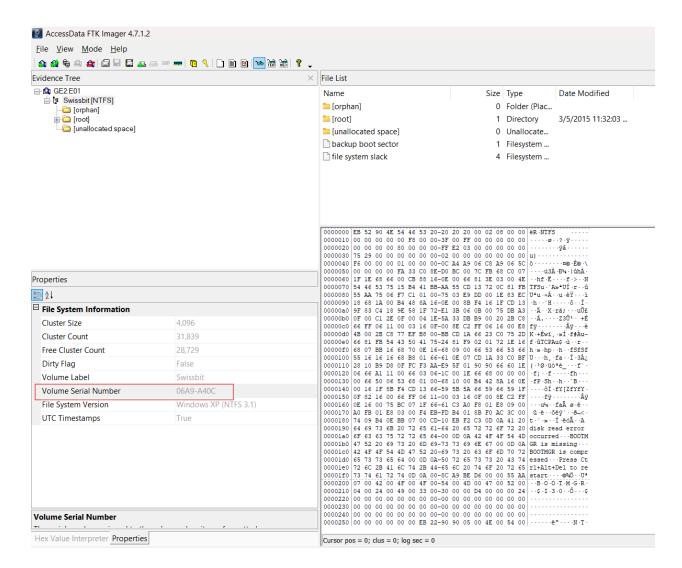
## Q2. List the MD5 and SHA1 hash values associated with the verification?

MD5: 16556ca8ee3e89dfcf332756bda1320a

SHA1: 3d3dc49eae6ca3a70a50ac9b215a32f4e727422b

# $\mathbf{Q3}$ . 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.



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

A ↓	
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

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

A ↓	
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.

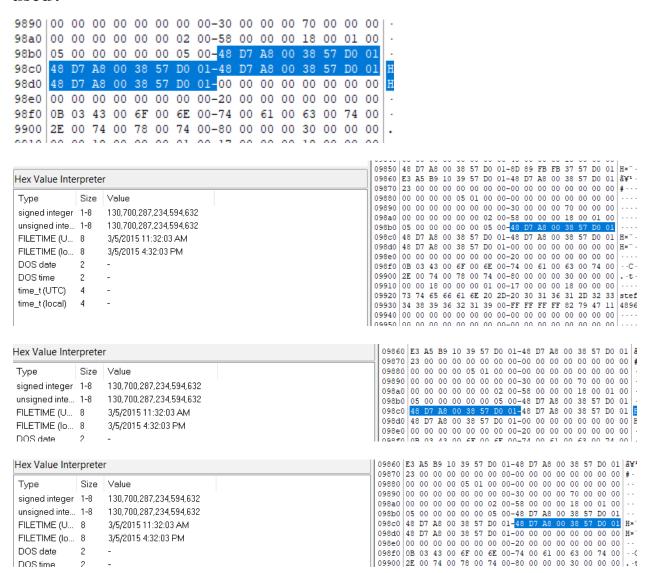
130416640 / 1024 = 127360 KB.

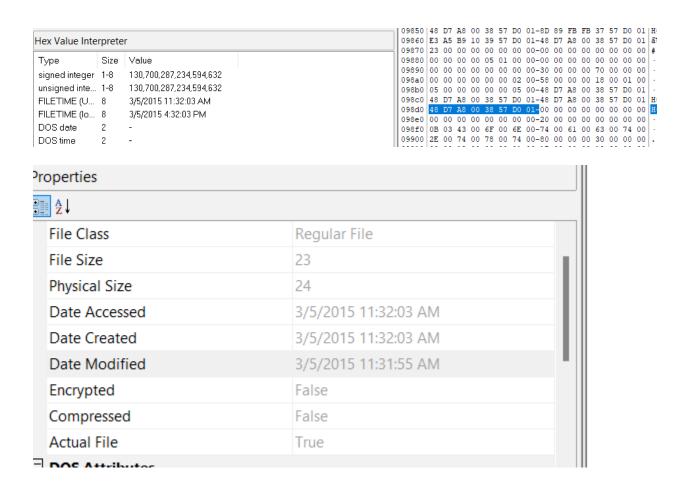
127360/1024 = 124.375 MB.

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

123379200 / 1024 =120487.5 KB.

# 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?

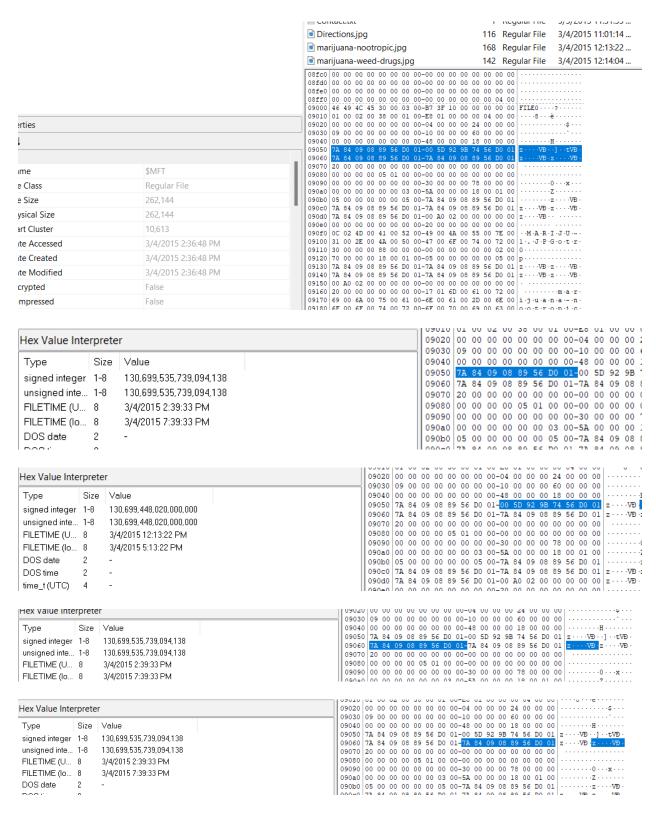




So the File Modified in the MFT header is changed because the Data modified is 1 min earlier than File Created.

### 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.



So the findings are

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