Abdul Sami Qasim
22i-1725
CY-D

# Lab 06

**Scenario:**

*The investigation relates to suspect who is alleged to be importing Cannabis from Germany since 2013. A message was found on a mobile phone in Germany belonging to a drug supplier named Stefan Schmidt, it is believed that sometime in March 2015 Stefan sent messages containing pictures of drugs to our suspect. The SHA256 hash values for the pictures have been forwarded by the German police and are listed below:*

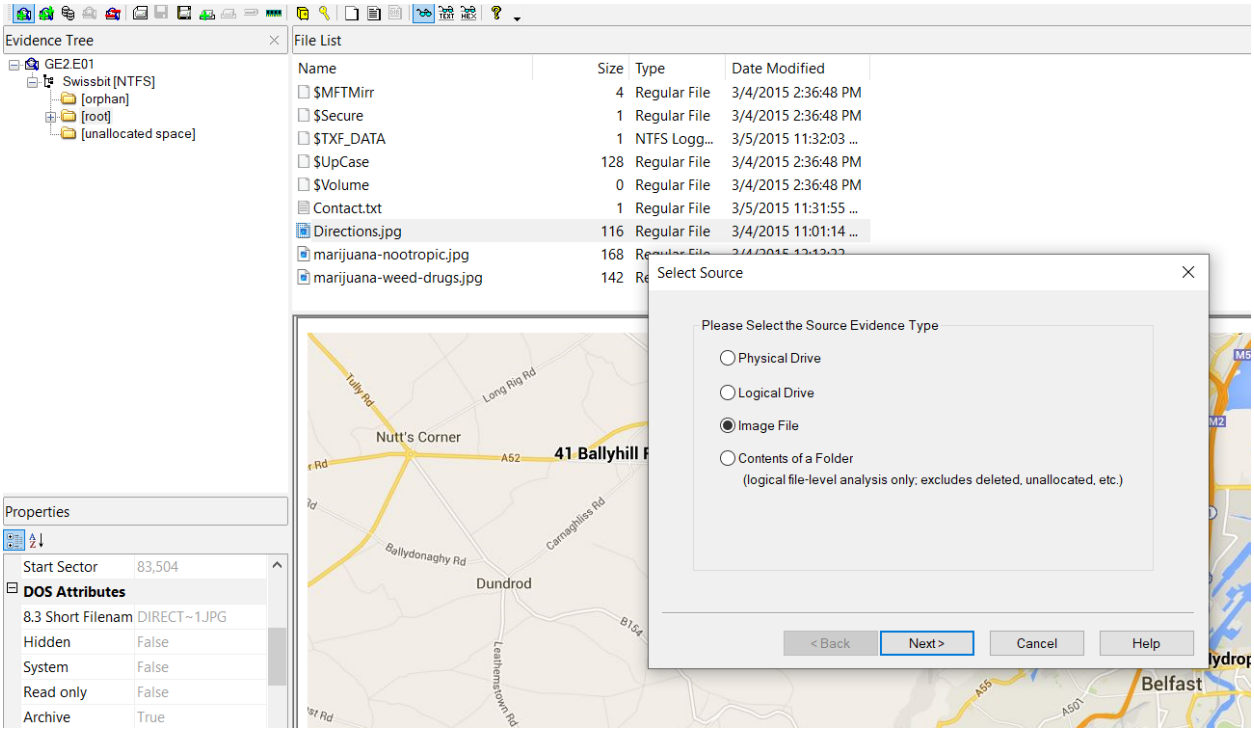
*SHA256: 6d4abf5c93e9e49459becafb0d1b319e98a466a3be7993616e228e1075cf4a77*

*SHA256: 41def7c073019b7c54721d200298a2e4d1926096ac1f4d89d8dc6c9747977ac0*

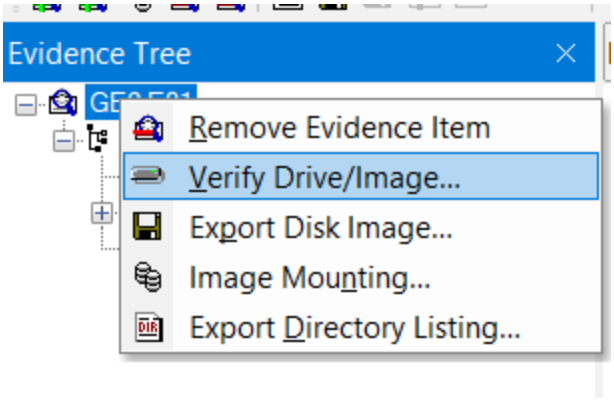
*A USB device, which was found in the possession of our suspect, has been seized by police and marked **GE2**. For the purposes of this practical you can accept that the device has been presented in a sealed evidence bag and that all chain of custody records has been completed. You are instructed to make a forensic image of the physical device and answer the questions below by examining it in a forensic manner.*

**Q1) Describe the process that you used to add and verify the forensic image?** Hint: Use the hashes from the GE2 Case Info.E01.txt to verify the forensic image.

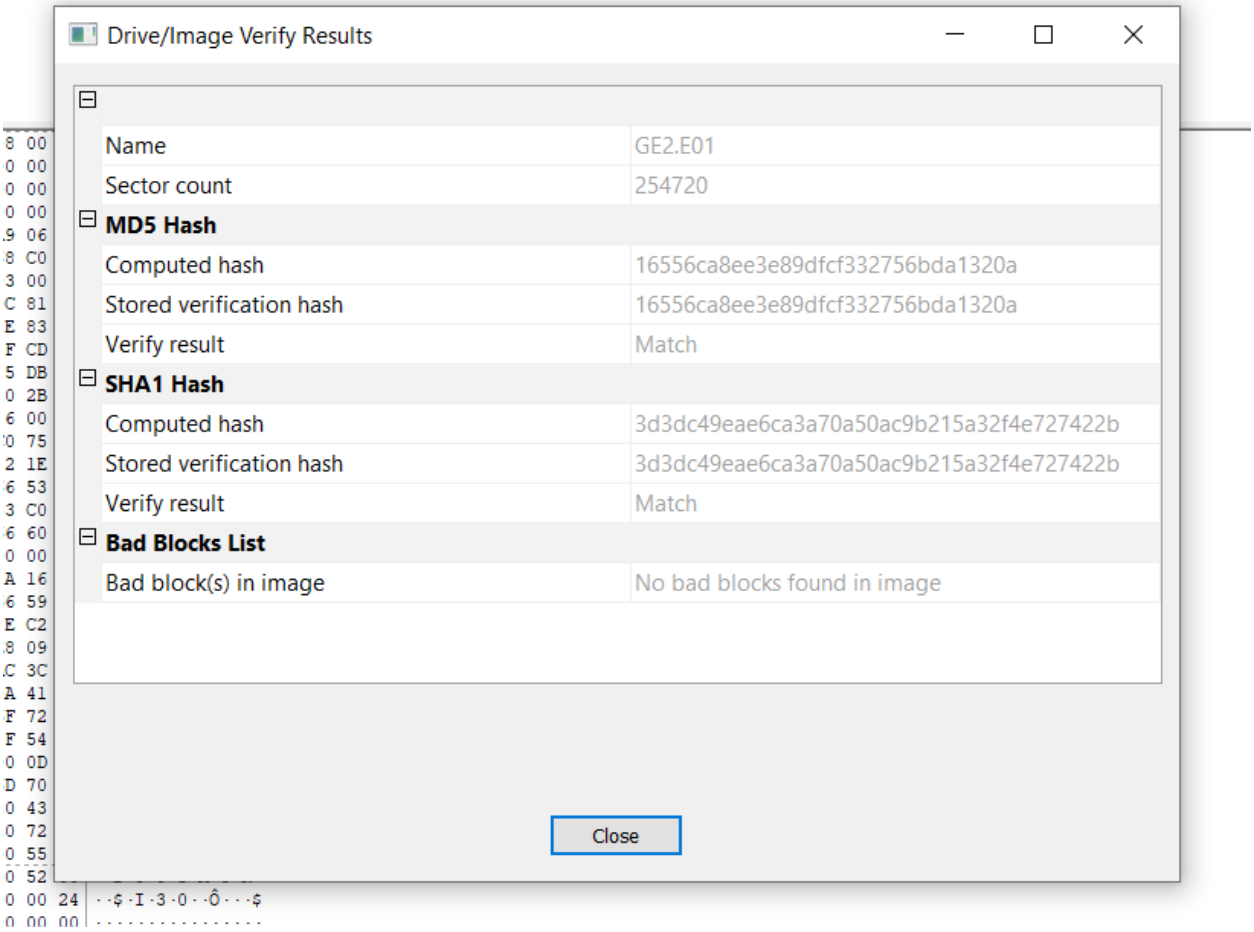
Ans: To add the image, first we go to the FTKImager and select the following option:




Afterwards, we select the file from the file explorer and it loads it in. Now, to verify the image, we do the following thing:



This shows up afterwards:




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

Ans:

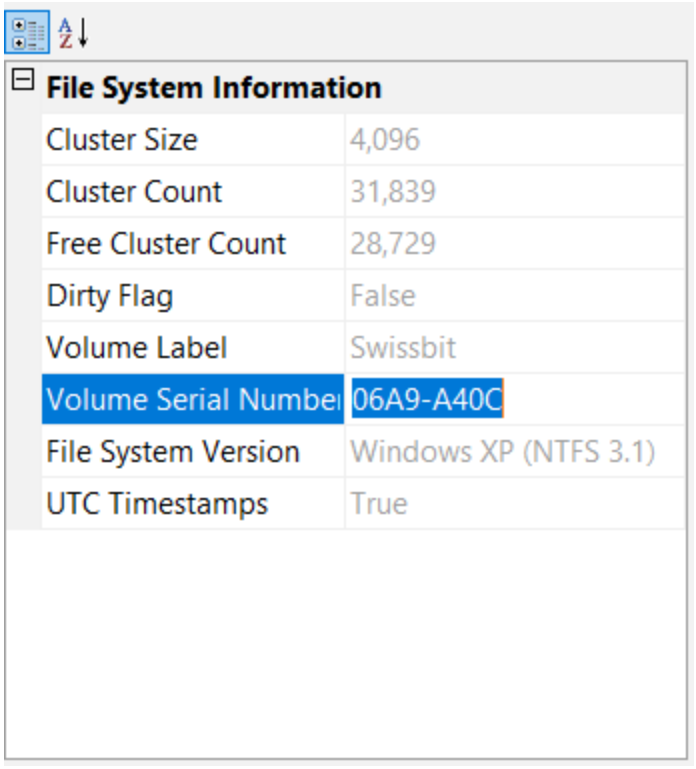
MD5: 16556ca8ee3e89dfcf332756bda1320a

SHA1: 3d3dc49eae6ca3a70a50ac9b215a32f4e727422b

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

Ans:

The serial number of the device shows up in the bottom left panel in the properties tab as follows:




The Volume Serial Number is: 06A9-A40C

**Q4) Identify and examine the picture files that are present at the root level of the device. Explain your findings from this examination?**

Format: jpg

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 11:01:14 AM |
| File name Date Changed: | 3/4/2015 11:01:14 AM |
| MD5 | a549f97ad490d71376f1426e66e00feb |
| SHA1 | e60af66c7c2358edb7c377e730c0c5352b40c9a9 |
| SHA256 | c4949ee7d1dd7d0f2672e1644af90e8d3dd16776e021aa80f2db86eac9a5e117 |

| | |
|---|---|
| Brief File Descritpion: | It shows a map with directions highlighted. This is a route most probably. |

Format: jpg

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 |
| SHA256 | 41def7c073019b7c54721d200298a2e4d1926096ac1f4d89d8dc6c9747977ac0 |
| Brief File Descritpion: | This file contains some plant based product being showed off in a person's hands. |

Format: jpg

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 |
| SHA256 | 6d4abf5c93e9e49459becafb0d1b319e98a466a3be7993616e228e1075cf4a77 |
| Brief File Descritpion: | This picture contains some green plant based product stored in a piece of paper. |

**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?** Hint: Drive Geometry in GE2 Case Info.E01.txt can be used to calculate Physical and Logical sizes.

Ans:

Total size = Sectors x 512

= 254720 x 512

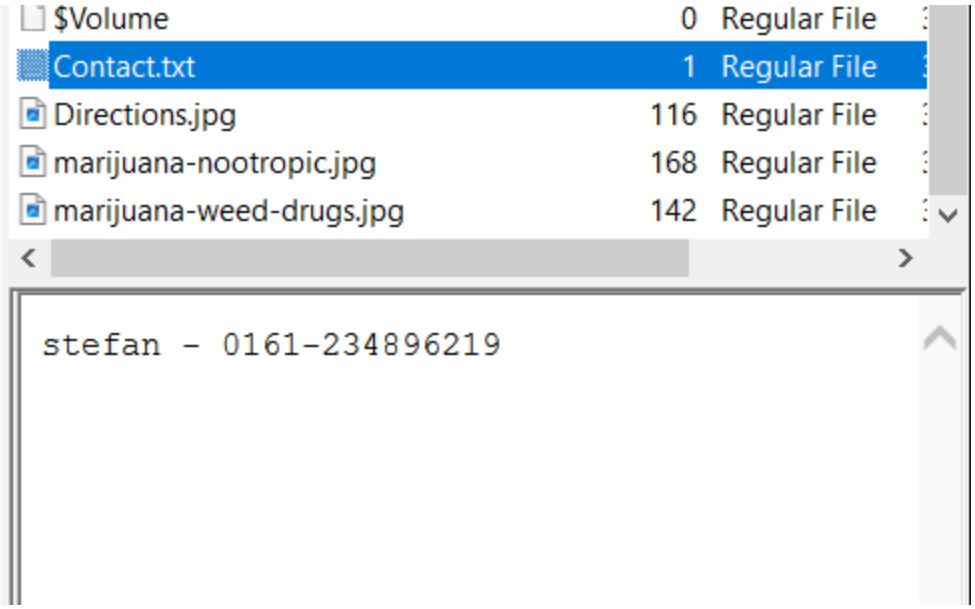
= 130,416,640 Bytes

= 124.375 MB

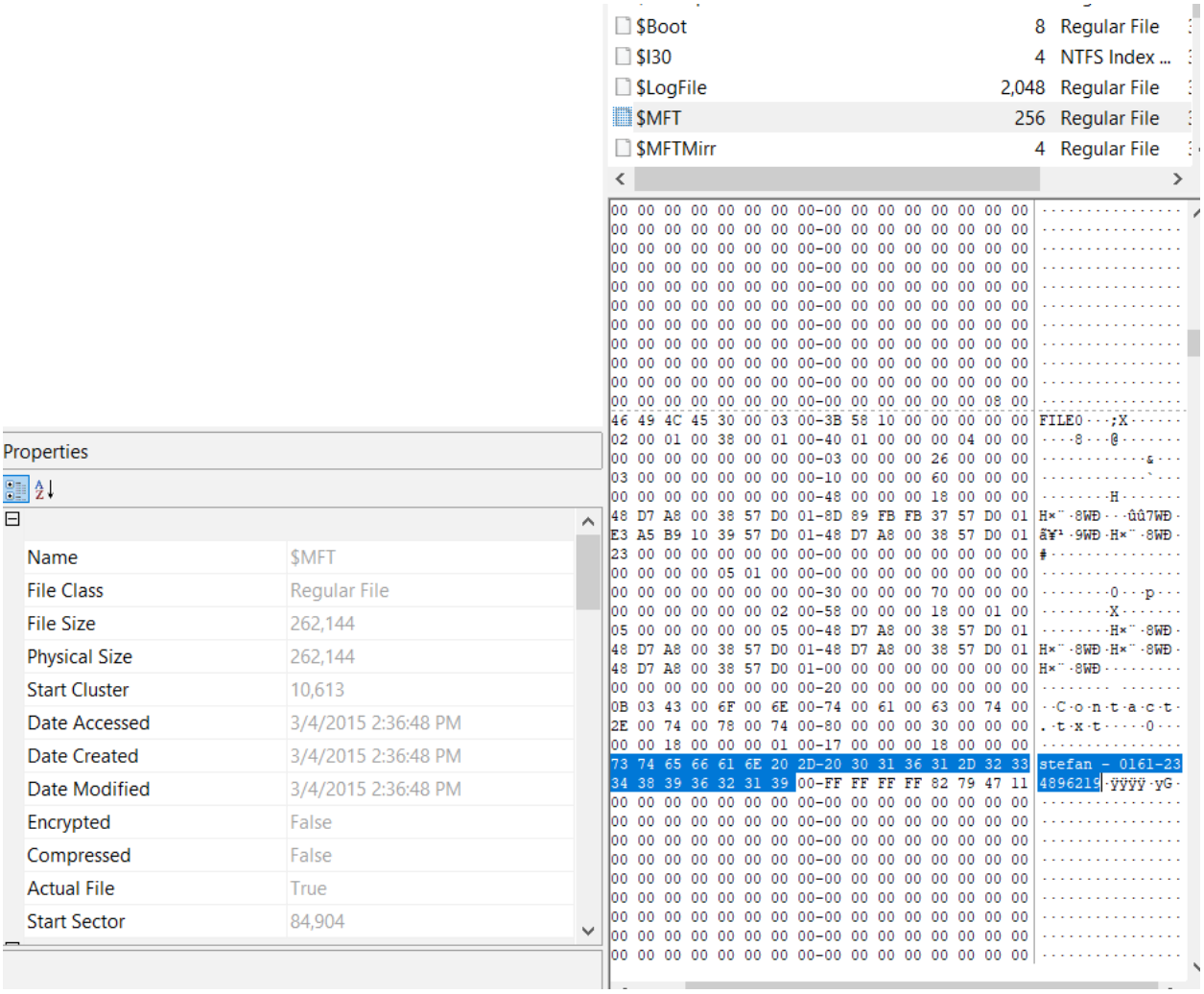
= 0.12 GB

**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?**

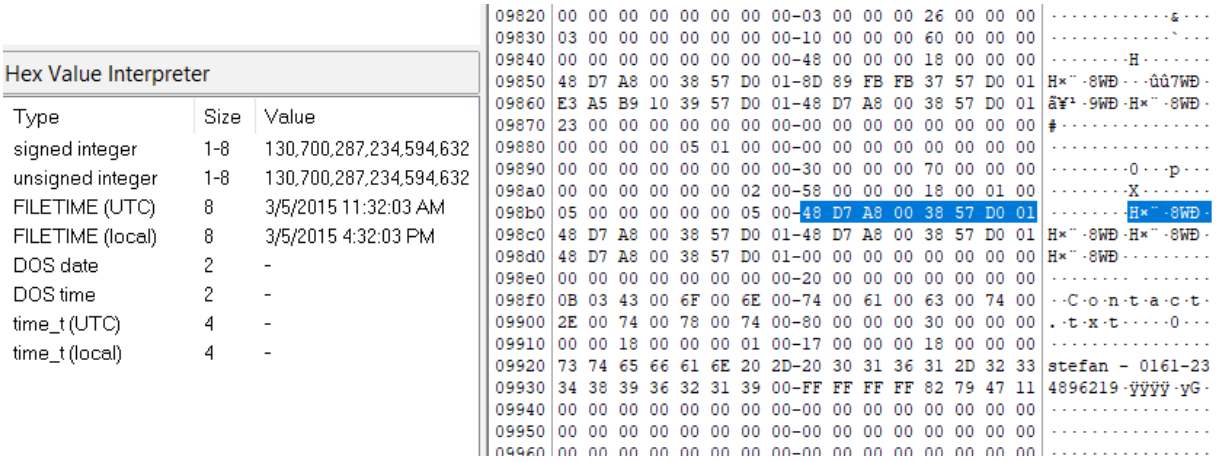
Ans: This is the contact.txt file in the image:



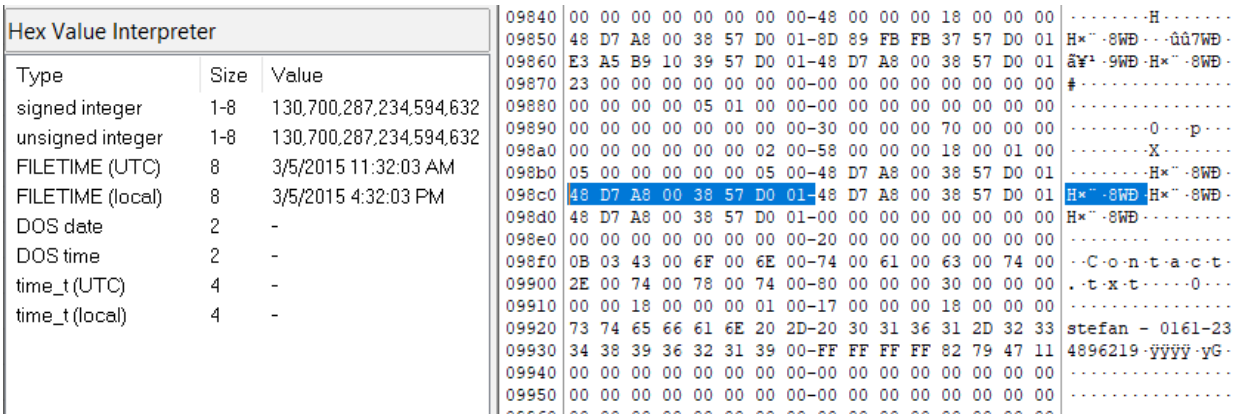

Verifying it’s data in MFT table:


$Boot 8 Regular File
$I30 4 NTFS Index ...
$LogFile 2,048 Regular File
$MFT 256 Regular File
$MFTMirr 4 Regular File
Properties
Name $MFT
File Class Regular File
File Size 262,144
Physical Size 262,144
Start Cluster 10,613
Date Accessed 3/4/2015 2:36:48 PM
Date Created 3/4/2015 2:36:48 PM
Date Modified 3/4/2015 2:36:48 PM
Encrypted False
Compressed False
Actual File True
Start Sector 84,904

Create Time:


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

Altered Time:

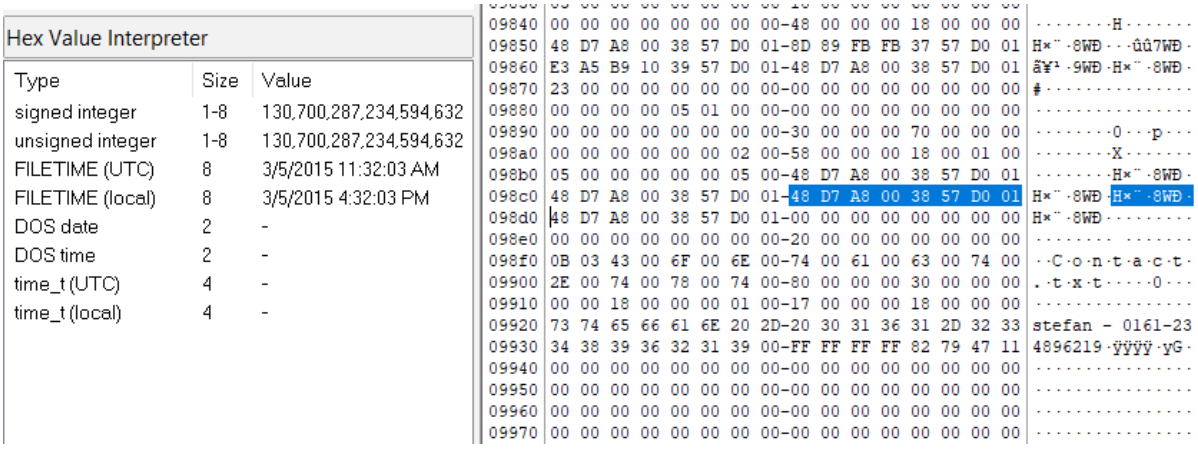


Hex Value Interpreter

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

```
09840 00 00 00 00 00 00 00 00-48 00 00 00 18 00 00 00 ........H.......
09850 48 D7 A8 00 38 57 D0 01-8D 89 FB FB 37 57 D0 01 H×¨.8WÐ...ûû7WÐ.
09860 E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01 ã¥¹.9WÐ.H×¨.8WÐ.
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 ........0...p...
098a0 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 ........X.......
098b0 05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 ........H×¨.8WÐ.
098c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 H×¨.8WÐ.H×¨.8WÐ.
098d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 H×¨.8WÐ.........
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.o.n.t.a.c.t.
09900 2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00 .t.x.t.....0...
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 stefan - 0161-23
09930 34 38 39 36 32 31 39 00-FF FF FF FF 82 79 47 11 4896219.ÿÿÿÿ.yG.
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 ................
```

Accessed Time:

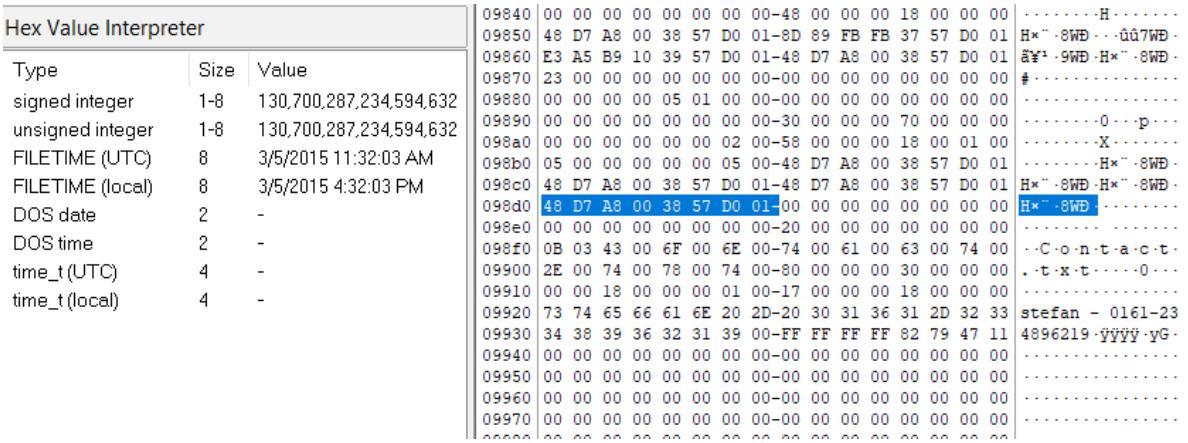


Hex Value Interpreter

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

```
09840 00 00 00 00 00 00 00 00-48 00 00 00 18 00 00 00 ........H.......
09850 48 D7 A8 00 38 57 D0 01-8D 89 FB FB 37 57 D0 01 H×¨.8WÐ...ûû7WÐ.
09860 E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01 ã¥¹.9WÐ.H×¨.8WÐ.
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 ........0...p...
098a0 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 ........X.......
098b0 05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 ........H×¨.8WÐ.
098c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 H×¨.8WÐ.H×¨.8WÐ.
098d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 H×¨.8WÐ.........
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.o.n.t.a.c.t.
09900 2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00 .t.x.t.....0...
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 stefan - 0161-23
09930 34 38 39 36 32 31 39 00-FF FF FF FF 82 79 47 11 4896219.ÿÿÿÿ.yG.
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 ................
09960 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
09970 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

MFT Change time:

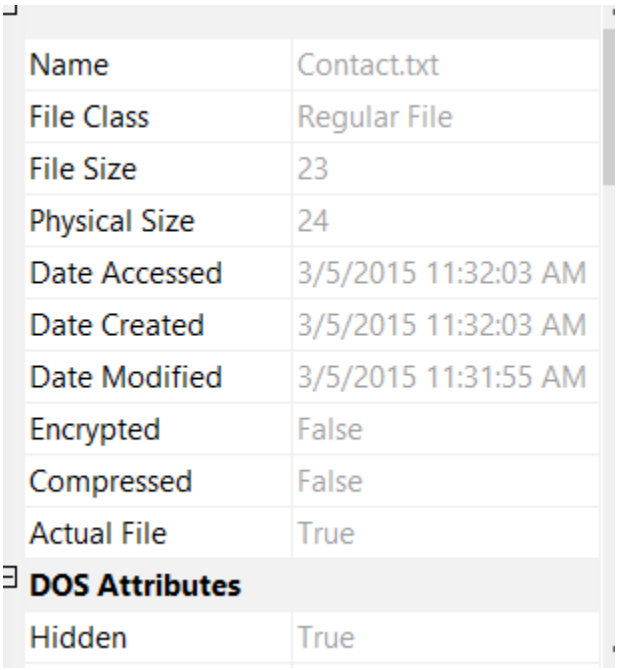


Hex Value Interpreter

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

```
09840 00 00 00 00 00 00 00 00-48 00 00 00 18 00 00 00 ........H.......
09850 48 D7 A8 00 38 57 D0 01-8D 89 FB FB 37 57 D0 01 H×¨.8WÐ...ûû7WÐ.
09860 E3 A5 B9 10 39 57 D0 01-48 D7 A8 00 38 57 D0 01 ã¥¹.9WÐ.H×¨.8WÐ.
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 ........0...p...
098a0 00 00 00 00 00 00 02 00-58 00 00 00 18 00 01 00 ........X.......
098b0 05 00 00 00 00 00 05 00-48 D7 A8 00 38 57 D0 01 ........H×¨.8WÐ.
098c0 48 D7 A8 00 38 57 D0 01-48 D7 A8 00 38 57 D0 01 H×¨.8WÐ.H×¨.8WÐ.
098d0 48 D7 A8 00 38 57 D0 01-00 00 00 00 00 00 00 00 H×¨.8WÐ.........
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.o.n.t.a.c.t.
09900 2E 00 74 00 78 00 74 00-80 00 00 00 30 00 00 00 .t.x.t.....0...
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 stefan - 0161-23
09930 34 38 39 36 32 31 39 00-FF FF FF FF 82 79 47 11 4896219.ÿÿÿÿ.yG.
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 ................
09960 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
09970 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Time in Properties:



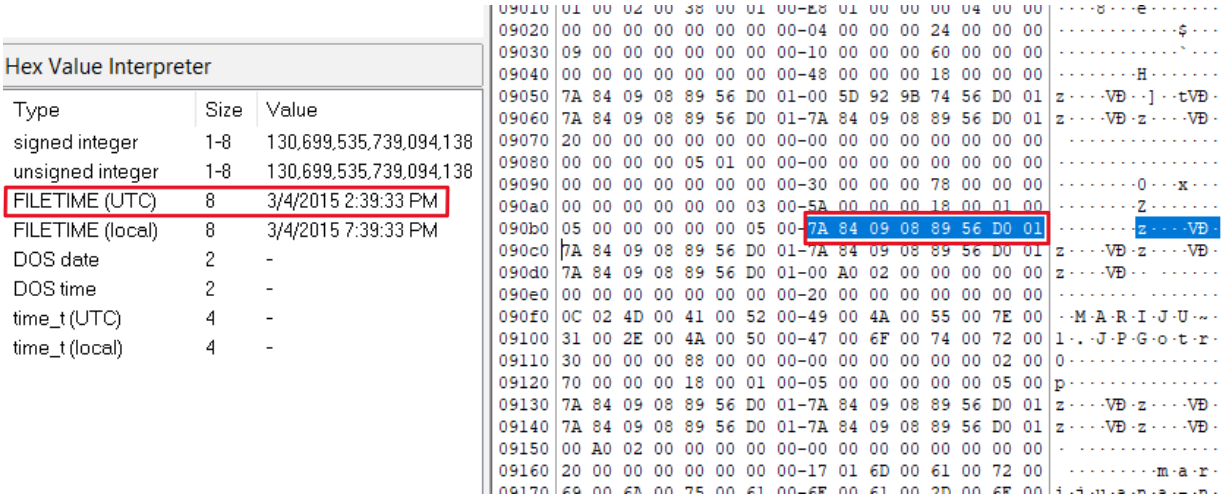
| | |
|---|---|
| Name | Contact.txt |
| File Class | Regular File |
| File Size | 23 |
| Physical Size | 24 |
| Date Accessed | 3/5/2015 11:32:03 AM |
| Date Created | 3/5/2015 11:32:03 AM |
| Date Modified | 3/5/2015 11:31:55 AM |
| Encrypted | False |
| Compressed | False |
| Actual File | True |
| **DOS Attributes** | |
| Hidden | True |

As the file in question has small size, it's data is stored in the MFT table in it's entry. (the data is highlighted).

**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 answer in Universal Time Coordinated (UTC) and show the 64 bit HEX values for each.**

Ans:

File creation entry in MFT:



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 | - |
| DOS time | 2 | - |
| time_t (UTC) | 4 | - |
| time_t (local) | 4 | - |

```
09020  00 00 00 00 00 00 00 00-04 00 00 00 24 00 00 00  ............$...
09030  09 00 00 00 00 00 00 00-10 00 00 00 60 00 00 00  ............`...
09040  00 00 00 00 00 00 00 00-48 00 00 00 18 00 00 00  ........H.......
09050  7A 84 09 08 89 56 D0 01-00 5D 92 9B 74 56 D0 01  z....VÐ..]..tVÐ.
09060  7A 84 09 08 89 56 D0 01-7A 84 09 08 89 56 D0 01  z....VÐ.z....VÐ.
09070  20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00                  
09080  00 00 00 00 05 01 00 00-00 00 00 00 00 00 00 00  ................
09090  00 00 00 00 00 00 00 00-30 00 00 00 78 00 00 00  ........0...x...
090a0  00 00 00 00 00 00 03 00-5A 00 00 00 18 00 01 00  ........Z.......
090b0  05 00 00 00 00 00 05 00-7A 84 09 08 89 56 D0 01  ........z....VÐ.
090c0  7A 84 09 08 89 56 D0 01-7A 84 09 08 89 56 D0 01  z....VÐ.z....VÐ.
090d0  7A 84 09 08 89 56 D0 01-00 A0 02 00 00 00 00 00  z....VÐ.. ......
090e0  00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00  ........ .......
090f0  0C 02 4D 00 41 00 52 00-49 00 4A 00 55 00 7E 00  ..M.A.R.I.J.U.~.
09100  31 00 2E 00 4A 00 50 00-47 00 6F 00 74 00 72 00  1...J.P.G.o.t.r.
09110  30 00 00 00 88 00 00 00-00 00 00 00 00 00 02 00  0...............
09120  70 00 00 00 18 00 01 00-05 00 00 00 00 00 05 00  p...............
09130  7A 84 09 08 89 56 D0 01-7A 84 09 08 89 56 D0 01  z....VÐ.z....VÐ.
09140  7A 84 09 08 89 56 D0 01-7A 84 09 08 89 56 D0 01  z....VÐ.z....VÐ.
09150  00 A0 02 00 00 00 00 00-00 00 00 00 00 00 00 00  . ..............
09160  20 00 00 00 00 00 00 00-17 01 6D 00 61 00 72 00  .........m.a.r.
```

File Modified time entry in MFT:

| 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 | - |
| DOS time | 2 | - |
| time_t (UTC) | 4 | - |
| time_t (local) | 4 | - |