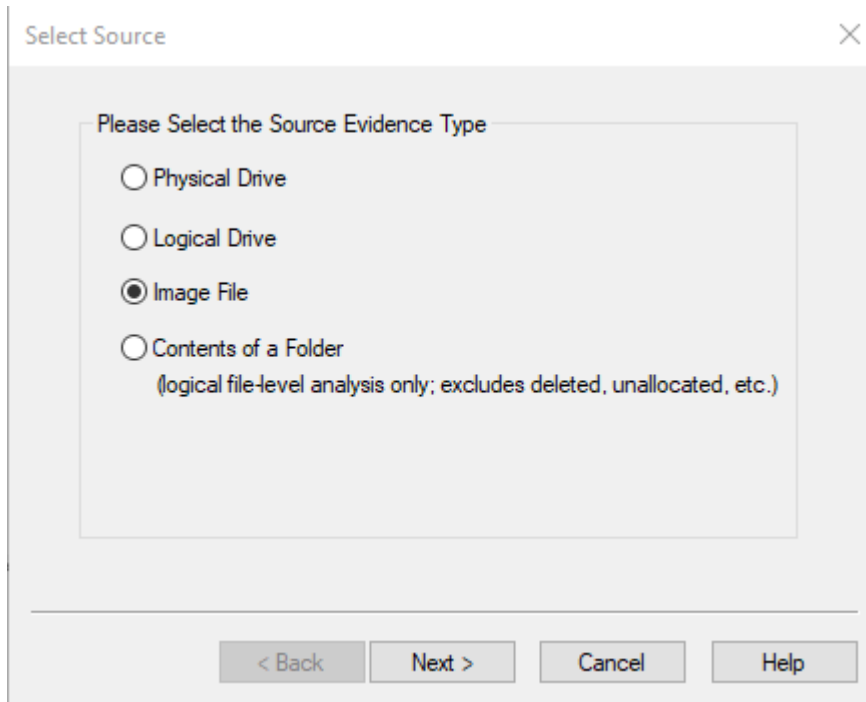


Digital Forensics-Lab06

Ahmad Abdullah i22-1609

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



Select Source

Please Select the Source Evidence Type

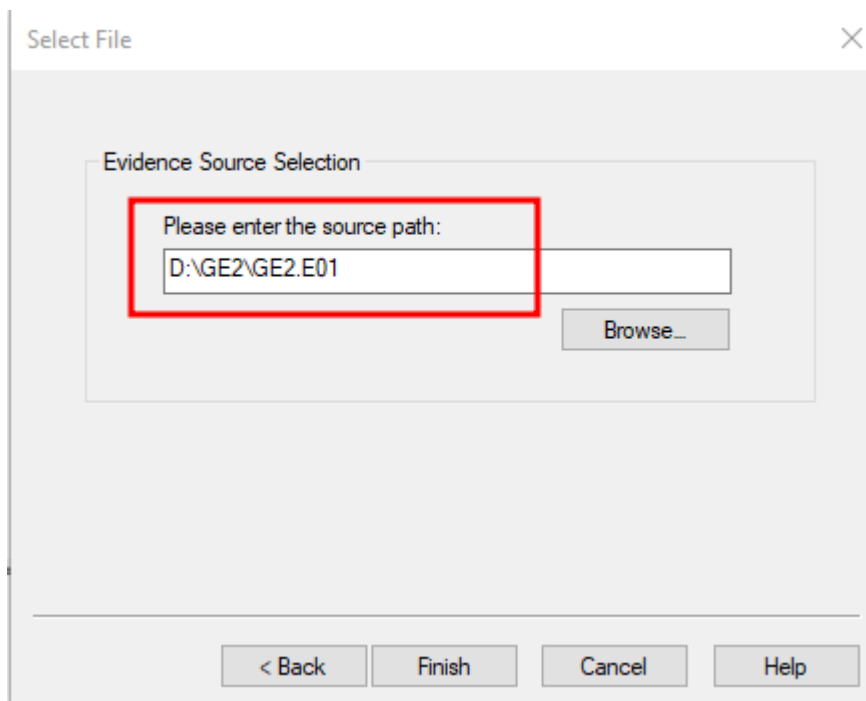
☐ Physical Drive

☐ Logical Drive

☒ Image File

☐ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

< Back Next > Cancel Help



Select File

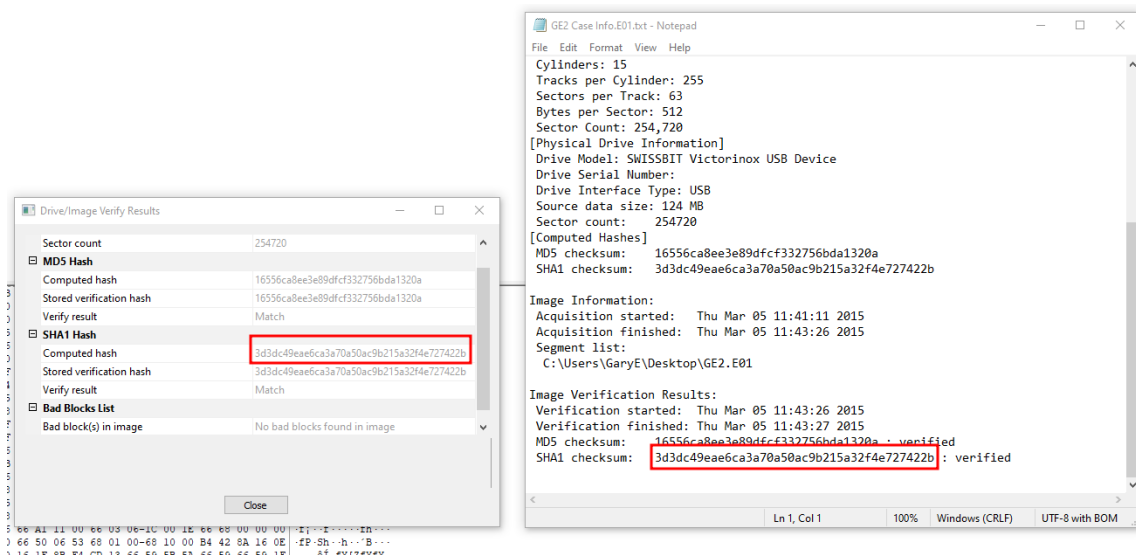
Evidence Source Selection

Please enter the source path:

D:\GE2\GE2.E01

Browse...

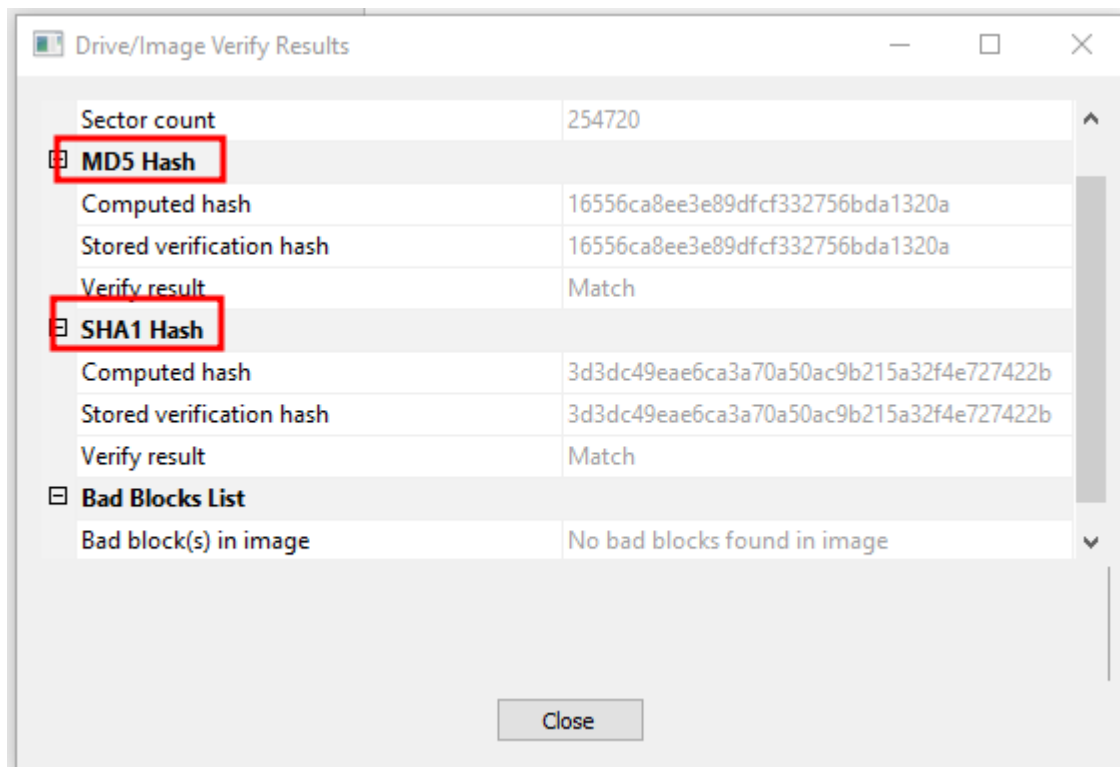
< Back Finish Cancel Help



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

MD5 checksum: 16556ca8ee3e89dfcf332756bda1320a

SHA1 checksum: 3d3dc49eae6ca3a70a50ac9b215a32f4e727422b



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

Evidence Tree

- GE2 E01
 - Swissbit [NTFS]** 1
 - [orphan]
 - [root]
 - [unallocated space]

File List

Name	Size	Type	Date Modified
[orphan]	0	Folder (Placeh...	
[root]	1	Directory	05/03/2015 11:32:03 ;
[unallocated space]	0	Unallocated Sp...	
backup boot sector	1	Filesystem Met...	
file system slack	4	Filesystem Slack	

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 3
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

Properties Hex Value Inter... Custom Conte...

Cursor pos = 0; dus = 0; log sec = 0

00000000	EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00	èR·NTFS ····
00000010	00 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 00 00 00	·····ø·?·ÿ····
00000020	00 00 00 00 80 00 00 00-FF E2 03 00 00 00 00 00	······ÿÀ····
00000030	75 29 00 00 00 00 00 00-02 00 00 00 00 00 00 00	u) ······
00000040	F6 00 00 00 01 00 00 00-0C A4 A9 06 C8 A9 06 5C	ö·····wø·Èø·\
00000050	00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07	···ú3À·Ð¼· ùhÀ·
00000060	1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E	·hf·È····f·>·N
00000070	54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB	TFSu·'A»·UI·r·û
00000080	55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC	U²u·+À·u·éÝ··i
00000090	18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13	·h·'H·····ö·í·
000000a0	9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3	··À··X·rá;··uÜ&
000000b0	0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8	··À····Z3Ü¹· +È
000000c0	66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8	fÿ·····Äÿ···è
000000d0	4B 00 2B C8 77 EF B9 00-BB CD 1A 66 23 C0 75 2D	K·+Èwi, »í·f#Àu-
000000e0	66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16	f·ûTCPAu\$·ù·r·
000000f0	68 07 BB 16 68 70 0E 16-68 09 00 66 53 66 53 66	h·»·hp·h·fSfSf
00000100	55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF	U···h·fa·í·3À;
00000110	28 10 B9 D8 0F FC F3 AA-E9 5F 01 90 90 66 60 1E	{·²ø·üóªé···f·
00000120	06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00	·f;··f····fh··
00000130	00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E	·fP·Sh·h···B··
00000140	00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F	····öí·fY[ZfYfY·
00000150	0F 82 16 00 66 FF 06 11-00 03 16 0F 00 8E C2 FF	····fÿ·····Äÿ·
00000160	0E 16 00 75 BC 07 1F 66-61 C3 A0 F8 01 E8 09 00	···uª·faÀ ø·è·
00000170	A0 FB 01 E8 03 00 F4 EB-FD B4 01 8B F0 AC 3C 00	û·è···ôéÿ···ö-<·
00000180	74 09 B4 0E BB 07 00 CD-10 EB F2 C3 0D 0A 41 20	t·'·»··í·èöÀ··A

Q5) Identify and examine the picture files present at the device's root level. Explain your findings from this examination.

Format:	JPG
Filename:	Directions.jpg
File name Date Created:	04/03/2015 2:39:31 pm
File name Date Modified:	04/03/2015 11:01:14 am
File name Date Accessed:	04/03/2015 2:39:31 pm
File name Date Changed:	04/03/2015 2:39:31 pm
MD5:	a549f97ad490d71376f1426e66e00feb
SHA1:	e60af66c7c2358edb7c377e730c0c5352b40c9a9
SHA256:	c4949ee7d1dd7d0f2672e1644af90e8d3dd16776e021aa80f2db86eac9a5e117
Brief File Description:	Direction.jpg is the image of directions from one point to another in Germany.

Format:	JPG
Filename:	marijuana-nootropic.jpg
File name Date Created:	04/03/2015 2:39:33 pm
File name Date Modified:	04/03/2015 2:39:33 pm
File name Date Accessed:	04/03/2015 2:39:33 pm
File name Date Changed:	04/03/2015 2:39:33 pm
MD5:	146fb88238bd9fcf7de028d63563cffd
SHA1:	b387e87b1c3ecaf53744404046f0b99508db71b7
SHA256:	c67200a38a5ed4a847fd1bee71fb722d8b170ab53c5a0b6a29dfe27b9ee71498
Brief File Description:	Some hands are holding marijuana like a baby.

Format:	JPG
Filename:	marijuana-weed-drugs.jpg
File name Date Created:	04/03/2015 2:39:36 pm
File name Date Modified:	04/03/2015 2:39:36 pm
File name Date Accessed:	04/03/2015 2:39:36 pm
File name Date Changed:	04/03/2015 2:39:36 pm
MD5:	9657de2dd227fdc453c834f10af1b34a

SHA1: fbff085de1958a48d8478c572206fcb3d75dee1a

SHA256:

897ed1ca1e4952b6bd863d83bef83d875f61898ed33ba50bdd959216b8fa7926

Brief File Description: Some marijuana rolled up in a paper blunt.

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.

Answer:

General Sector Size = 512 bytes

Number of Sectors in the volume = 254,720

Total Size of the volume = 512 x 254720

Physical Size = 124.375 MB

Q6) Identify the text file present at the device's root level and explain your findings concerning it. Validate these findings from the MFT, including any HEX values and calculations that you used.

Answer:

SVolume	0	Regular File	04/03/2015 2:36:48 pm
Contact.txt	1	Regular File	05/03/2015 11:31:55 am
Directions.jpg	116	Regular File	04/03/2015 11:01:14 am
marijuana-nootropic.jpg	168	Regular File	04/03/2015 12:13:22 pm
marijuana-weed-drugs.jpg	142	Regular File	04/03/2015 12:14:04 pm

stefan - 0161-234896219

STAT_DATA	1	R
SupCase	128	R
Volume	0	R
Contact.txt	1	R
Directions.jpg	116	R
marijuana-nootropic.jpg	168	R
marijuana-weed-drugs.jpg	142	R

stefan - 0161-234896219

Properties	
Archive True	
NTFS Information	
MFT Record Number	38 (38912)
Date Changed (MFT)	05/03/2015 11:39:39 am
Resident	True
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-731122842-1092214498-537562773-1106
Group SID	S-1-5-21-731122842-1092214498-537562773-513
Filename Date Created (MFT)	05/03/2015 11:32:03 am
Filename Date Modified (MFT)	05/03/2015 11:32:03 am

0x30 Data

Creation 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	05/03/2015 11:32:03 am
FILETIME (local)	8	05/03/2015 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	05/03/2015 11:32:03 am
FILETIME (local)	8	05/03/2015 4:32:03 pm
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	-
time_t (local)	4	-

MFT Change:

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	05/03/2015 11:32:03 am
FILETIME (local)	8	05/03/2015 4:32:03 pm
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	-
time_t (local)	4	-

Read Time:

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	05/03/2015 11:32:03 am	
FILETIME (local)	8	05/03/2015 4:32:03 pm	
DOS date	2	-	
DOS time	2	-	
time_t (UTC)	4	-	
time_t (local)	4	-	

Meta Data of Contact.txt

Name	Contact.txt
File Class	Regular File
File Size	23
Physical Size	24
Date Accessed	05/03/2015 11:32:03 am
Date Created	05/03/2015 11:32:03 am
Date Modified	05/03/2015 11:31:55 am
Encrypted	False
Compressed	False
Actual File	True

The Data in the MFT file and meta data of the file is the same.

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.

Answer:

Creation time: FILETIME (UTC): 04/03/2015 2:39:33 pm

unsigned integer	1-8	130,689,535,739,094,138	
FILETIME (UTC)	8	04/03/2015 2:39:33 pm	
FILETIME (local)	8	04/03/2015 7:39:33 pm	
DOS date	2	-	
DOS time	2	-	
time_t (UTC)	4	-	
time_t (local)	4	-	

Modified Time: FILETIME (UTC): 04/03/2015 2:39:33 pm

signed integer	1-8	130,699,535,739,094,138
unsigned integer	1-8	130,699,535,739,094,138
FILETIME (UTC)	8	04/03/2015 2:39:33 pm
FILETIME (local)	8	04/03/2015 7:39:33 pm
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	-
time_t (local)	4	-

09050	7A 84 09 08 89 56 D0 01-00 5D 92 9B 74 56 D0 01	z---VB-]--tVB-
09060	7A 84 09 08 89 56 D0 01-7A 84 09 08 89 56 D0 01	z---VB-z---VB-
09070	20 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	-----
09090	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---VB-
090c0	7A 84 09 08 89 56 D0 01-7A 84 09 08 89 56 D0 01	z---VB-z---VB-
090d0	7A 84 09 08 89 56 D0 01-00 A0 02 00 00 00 00 00	z---VB-----
090e0	00 00 00 00 00 00 00-20 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 02 00	0-----