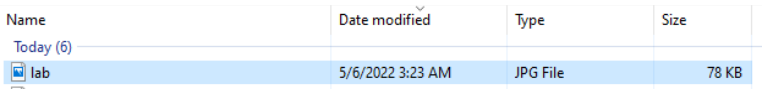
Farzad Kheirabadi
CYB 528
UNIT 4

WinHex Introduction - JPG Image Analysis

- Open the Image file

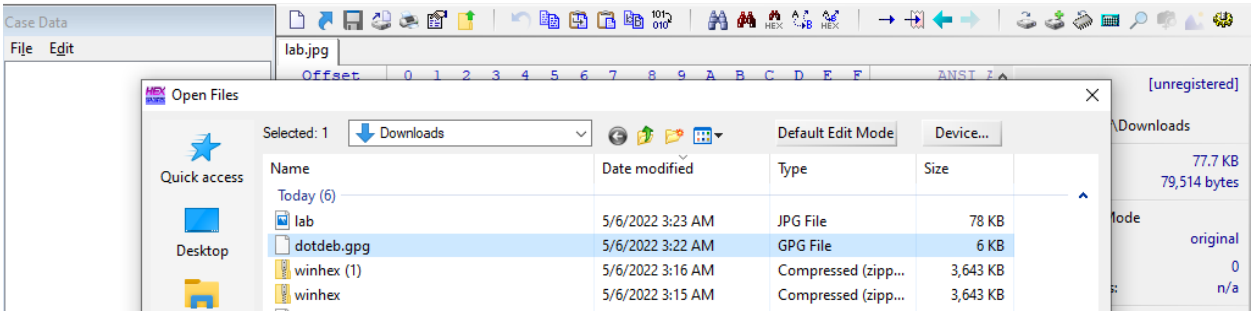


- In the below screenshot JFIF highlighted in yellow indicates it is a JPEG file.

Farzad Kheirabadi
CYB 528
UNIT 4

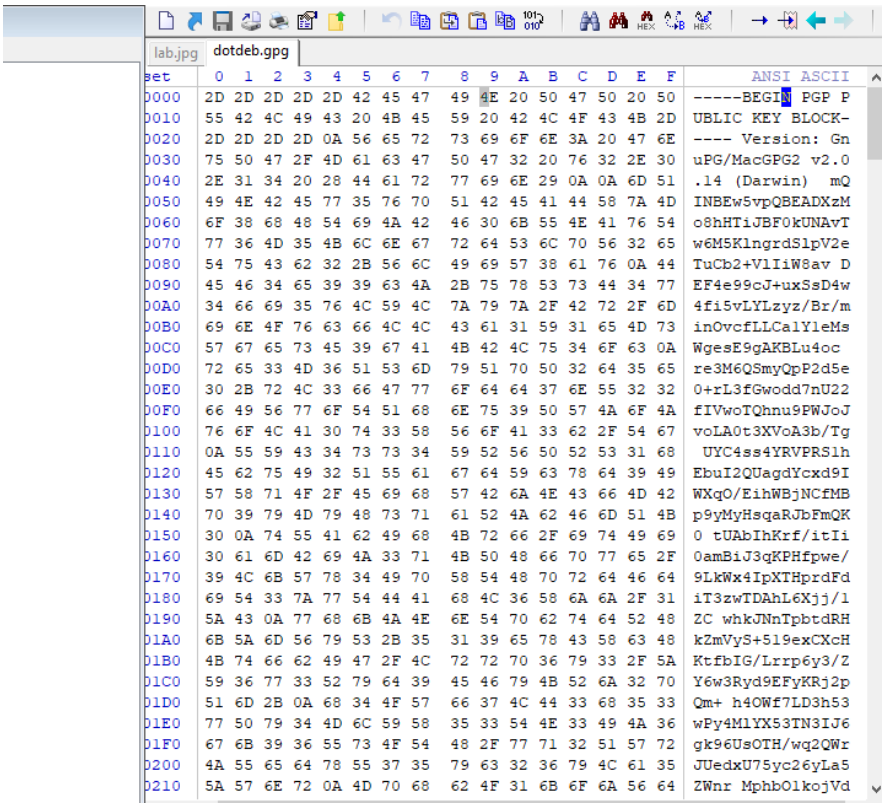
```
00000010  00 48 00 00 FF E2 0C 58  49 43 43 5F 50 52 4F 46  H  ÿâ XICC
00000020  49 4C 45 00 01 01 00 00  0C 48 4C 69 6E 6F 02 10  ILE      HL
00000030  00 00 6D 6E 74 72 52 47  42 20 58 59 5A 20 07 CE    mntrRGB X
00000040  00 02 00 09 00 06 00 31  00 00 61 63 73 70 4D 53         1  a
00000050  46 54 00 00 00 00 49 45  43 20 73 52 47 42 00 00  FT    IEC s
00000060  00 00 00 00 00 00 00 00  00 00 00 00 F6 D6 00 01
00000070  00 00 00 00 D3 2D 48 50  20 20 00 00 00 00 00 00      Ó-HP
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0  00 00 00 00 00 00 00 00  00 11 63 70 72 74 00 00            c
000000B0  01 50 00 00 00 33 64 65  73 63 00 00 01 84 00 00  P   3desc
000000C0  00 6C 77 74 70 74 00 00  01 F0 00 00 00 14 62 6B  lwtpt    ð
000000D0  70 74 00 00 02 04 00 00  00 14 72 58 59 5A 00 00  pt        r
000000E0  02 18 00 00 00 14 67 58  59 5A 00 00 02 2C 00 00        gXYZ
000000F0  00 14 62 58 59 5A 00 00  02 40 00 00 00 14 64 6D    bXYZ   @
00000100  6E 64 00 00 02 54 00 00  00 70 64 6D 64 64 00 00  nd   T   pd
00000110  02 C4 00 00 00 88 76 75  65 64 00 00 03 4C 00 00   Ä    ˆvued
00000120  00 86 76 69 65 77 00 00  03 D4 00 00 00 24 6C 75   †view   Ô
00000130  6D 69 00 00 03 F8 00 00  00 14 6D 65 61 73 00 00  mi   ø    m
00000140  04 0C 00 00 00 24 74 65  63 68 00 00 04 30 00 00       $tech
00000150  00 0C 72 54 52 43 00 00  04 3C 00 00 08 0C 67 54    rTRC   <
00000160  52 43 00 00 04 3C 00 00  08 0C 62 54 52 43 00 00  RC   <    b
00000170  04 3C 00 00 08 0C 74 65  78 74 00 00 00 00 43 6F  <    text
00000180  70 79 72 69 67 68 74 20  28 63 29 20 31 39 39 38  pyright (c)
00000190  20 48 65 77 6C 65 74 74  2D 50 61 63 6B 61 72 64   Hewlett-Pa
000001A0  20 43 6F 6D 70 61 6E 79  00 00 64 65 73 63 00 00   Company  d
000001B0  00 00 00 00 00 12 73 52  47 42 20 49 45 43 36 31        sRGB
000001C0  39 36 36 2D 32 2E 31 00  00 00 00 00 00 00 00 00  966-2.1
000001D0  00 00 12 73 52 47 42 20  49 45 43 36 31 39 36 36     sRGB IEC
000001E0  2D 32 2E 31 00 00 00 00  00 00 00 00 00 00 00 00  -2.1
000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000210  00 00 00 00 00 00 58 59  5A 20 00 00 00 00 00 00        XYZ
```

- Here in the below pic as shown we open dotdeb.gpg file.



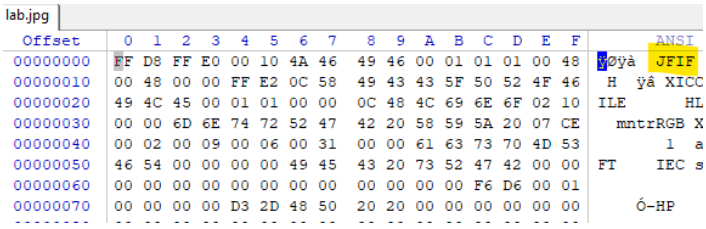
- In the picture below it can be noticed there is no relevant information about what the file is about. It is compressed with gzip then it is encrypted with gpg.

Farzad Kheirabadi
CYB 528
UNIT 4



WinHex – PLAYING WITH FILES

- Here is the file which indicates it is a JPEG file



Farzad Kheirabadi
CYB 528
UNIT 4

- In the given file below, we will change the value from 19 to 49 as highlighted below

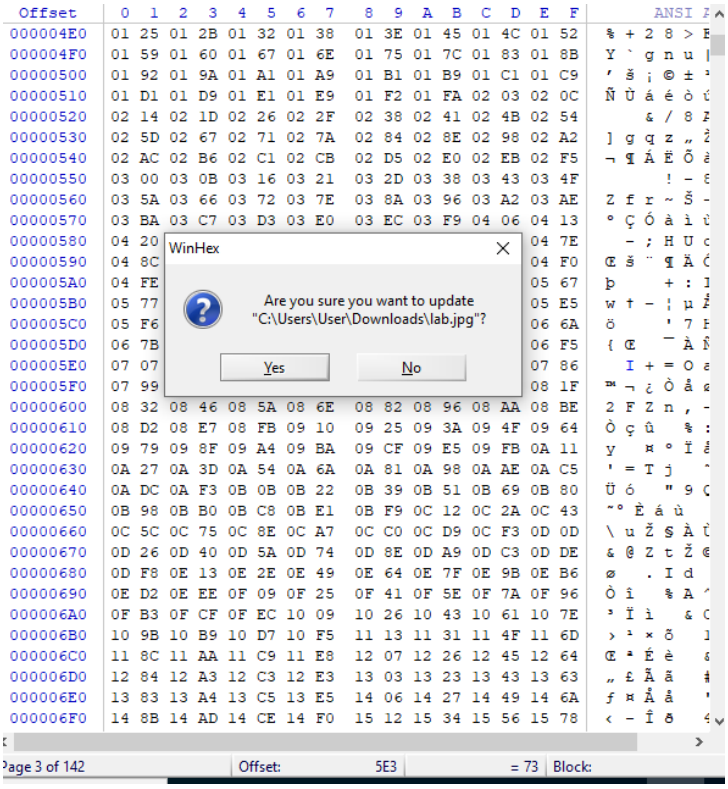
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI
01	25	01	2B	01	32	01	38	01	3E	01	45	01	4C	01	52	% + 2 8 > E
01	59	01	60	01	67	01	6E	01	75	01	7C	01	83	01	8B	Y ` g n u |
01	92	01	9A	01	A1	01	A9	01	B1	01	B9	01	C1	01	C9	' š ¡ © ± ¹
01	D1	01	D9	01	E1	01	E9	01	F2	01	FA	02	03	02	0C	Ñ Ù á é ò ú
02	14	02	1D	02	26	02	2F	02	38	02	41	02	4B	02	54	& / 8 A K
02	5D	02	67	02	71	02	7A	02	84	02	8E	02	98	02	A2	] g q z „ Ž
02	AC	02	B6	02	C1	02	CB	02	D5	02	E0	02	EB	02	F5	¬ ¶ Á Ë Õ à
03	00	03	0B	03	16	03	21	03	2D	03	38	03	43	03	4F	! - 8 C O
03	5A	03	66	03	72	03	7E	03	8A	03	96	03	A2	03	AE	Z f r ~ Š - ¢ ®
03	BA	03	C7	03	D3	03	E0	03	EC	03	F9	04	06	04	13	º Ç Ó à ì ù
04	20	04	2D	04	3B	04	48	04	55	04	63	04	71	04	7E	– ; H U c q ~
04	8C	04	9A	04	A8	04	B6	04	C4	04	D3	04	E1	04	F0	Œ š ¨ ¶ Ä Ó á ð
04	FE	05	0D	05	1C	05	2B	05	3A	05	49	05	58	05	67	þ + : I X g
05	77	05	86	05	96	05	A6	05	B5	05	C5	05	D5	05	E5	w † – ¦ µ Å Õ å
05	F6	06	06	06	16	06	27	06	37	06	48	06	59	06	6A	ö ' 7 H Y j
06	7B	06	8C	06	9D	06	AF	06	C0	06	D1	06	E3	06	F5	{ Œ ¯ À Ñ ã õ
07	07	07	49	07	2B	07	3D	07	4F	07	61	07	74	07	86	I + = O a t †
07	99	07	AC	07	BF	07	D2	07	E5	07	F8	08	0B	08	1F	™ ¬ ¿ Ò å ø
08	32	08	46	08	5A	08	6E	08	82	08	96	08	AA	08	BE	2 F Z n ‚ - ª ¾
08	D2	08	E7	08	FB	09	10	09	25	09	3A	09	4F	09	64	Ò ç û % : O d
09	79	09	8F	09	A4	09	BA	09	CF	09	E5	09	FB	0A	11	y ¤ º Ï å û
0A	27	0A	3D	0A	54	0A	6A	0A	81	0A	98	0A	AE	0A	C5	' = T j ˜ ® Å
0A	DC	0A	F3	0B	0B	0B	22	0B	39	0B	51	0B	69	0B	80	Ü ó " 9 Q i €
0B	98	0B	B0	0B	C8	0B	E1	0B	F9	0C	12	0C	2A	0C	43	˜ ° È á ù * C
0C	5C	0C	75	0C	8E	0C	A7	0C	C0	0C	D9	0C	F3	0D	0D	\ u Ž § À Ù ó
0D	26	0D	40	0D	5A	0D	74	0D	8E	0D	A9	0D	C3	0D	DE	& @ Z t Ž © Ã Þ
0D	F8	0E	13	0E	2E	0E	49	0E	64	0E	7F	0E	9B	0E	B6	ø . I d › ¶
0E	D2	0E	EE	0F	09	0F	25	0F	41	0F	5E	0F	7A	0F	96	Ò î % A ^ z –
0F	B3	0F	CF	0F	EC	10	09	10	26	10	43	10	61	10	7E	³ Ï ì & C a ~
10	9B	10	B9	10	D7	10	F5	11	13	11	31	11	4F	11	6D	› ¹ × õ 1 O m
11	8C	11	AA	11	C9	11	E8	12	07	12	26	12	45	12	64	Œ ª É è & E d
12	84	12	A3	12	C3	12	E3	13	03	13	23	13	43	13	63	„ £ Ã ã # C c
13	83	13	A4	13	C5	13	E5	14	06	14	27	14	49	14	6A	ƒ ¤ Å å ' I j
14	8B	14	AD	14	CE	14	F0	15	12	15	34	15	56	15	78	‹ - Î ð 4 V x

- Before changing the value, we can open the file it looks like this

Farzad Kheirabadi
CYB 528
UNIT 4

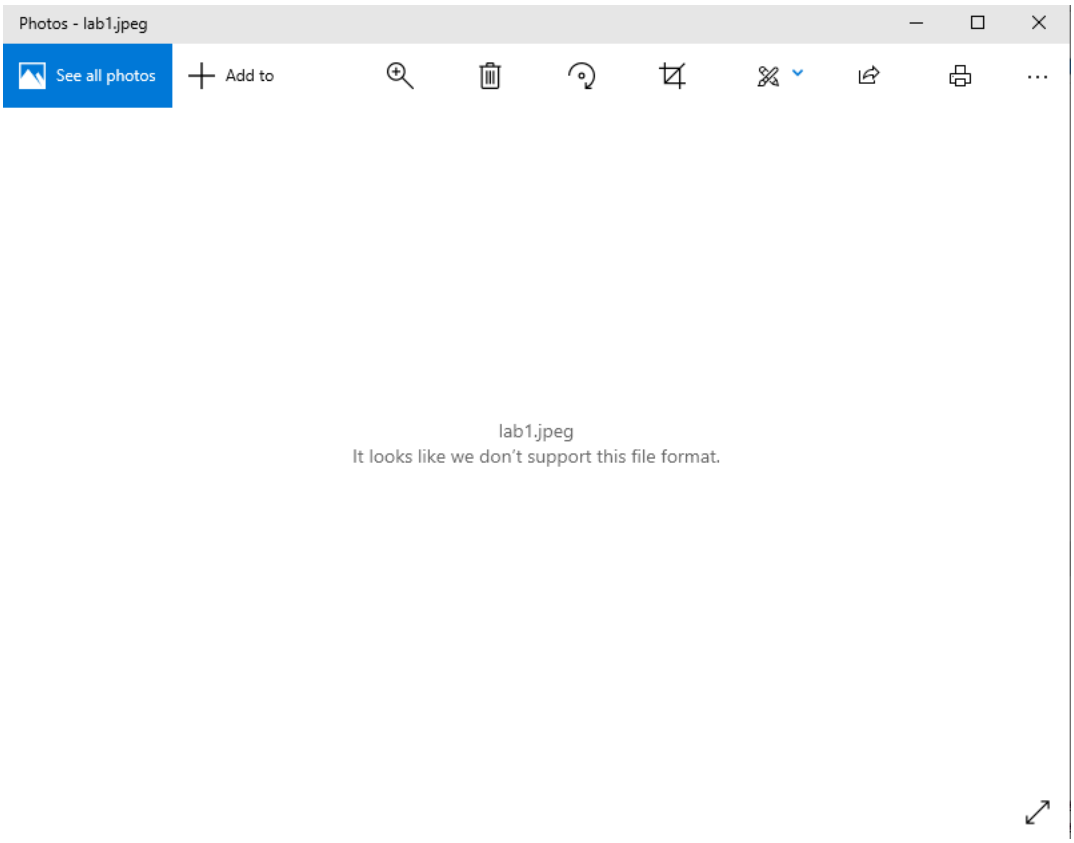
- After the value has been changed save the file with a different name > Ihave changed to

Lab1



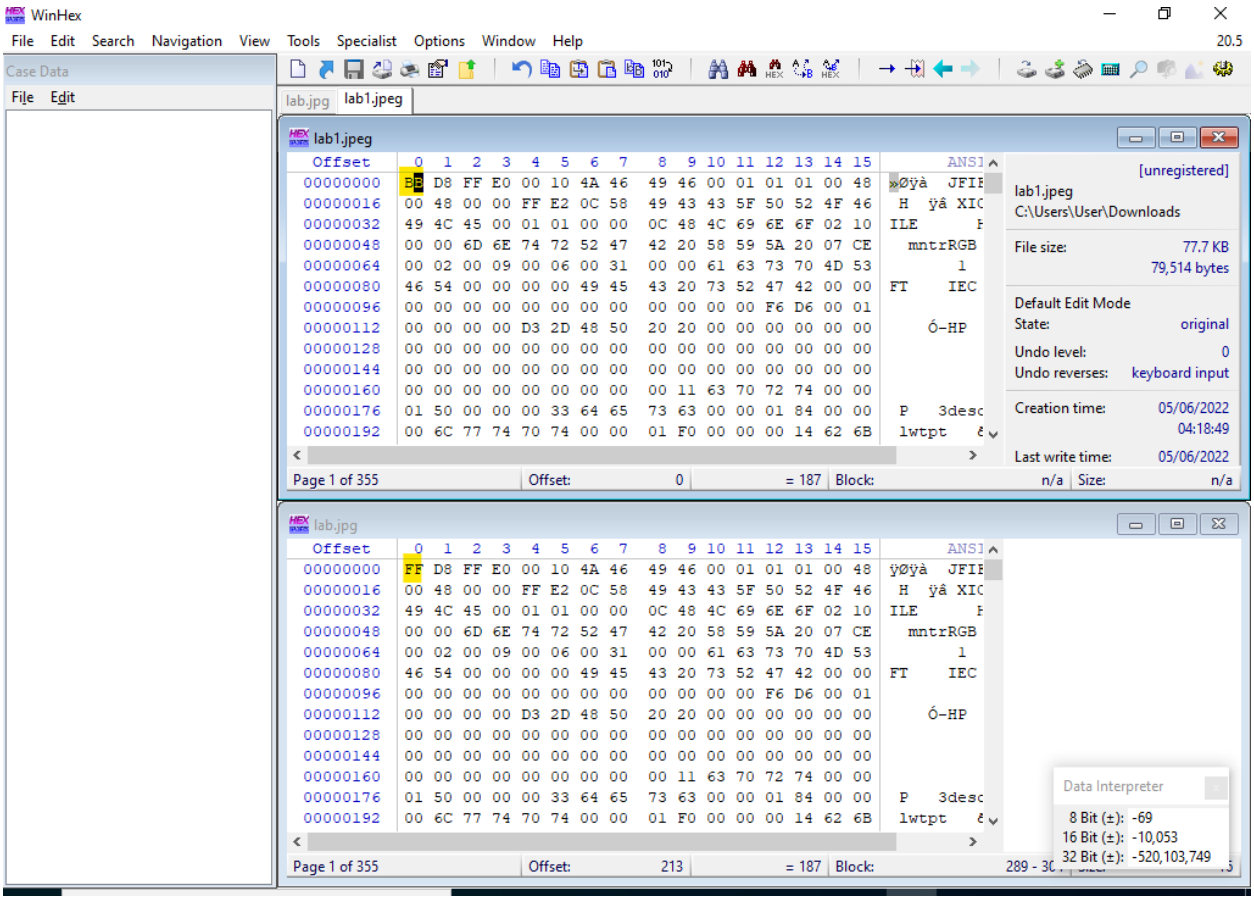
- After making the changes we are not able to open the file

Farzad Kheirabadi
CYB 528
UNIT 4



- As you can see below the changes made in the values are made.

Farzad Kheirabadi
CYB 528
UNIT 4



These values should be changed back to its original value to get image file working.

WinHex – WRITE BLOCKING

- Open the image file

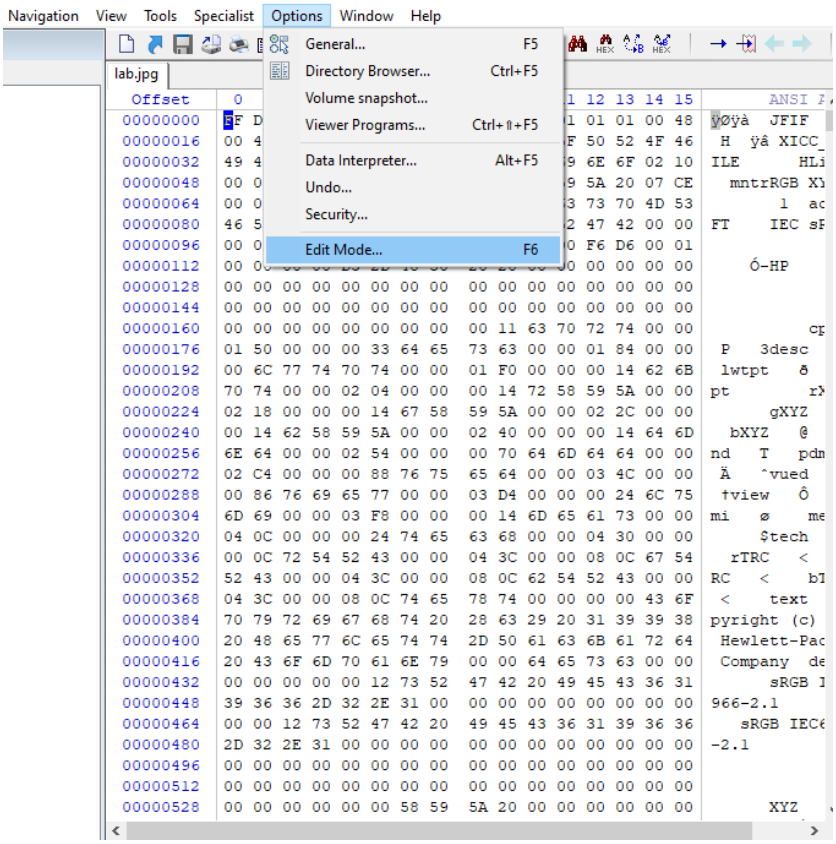
Farzad Kheirabadi
CYB 528
UNIT 4

lab.jpg

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI A
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	48	ÿØÿà JFIF H
00000016	00	48	00	00	FF	E2	0C	58	49	43	43	5F	50	52	4F	46	ÿâ XICC_PROF
00000032	49	4C	45	00	01	01	00	00	0C	48	4C	69	6E	6F	02	10	ILE HLino
00000048	00	00	6D	6E	74	72	52	47	42	20	58	59	5A	20	07	CE	mntrRGB XYZ Î
00000064	00	02	00	09	00	06	00	31	00	00	61	63	73	70	4D	53	1 acspMS
00000080	46	54	00	00	00	00	49	45	43	20	73	52	47	42	00	00	FT IEC sRGB
00000096	00	00	00	00	00	00	00	00	00	00	00	00	F6	D6	00	01	öÖ
00000112	00	00	00	00	D3	2D	48	50	20	20	00	00	00	00	00	00	Ó-HP
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	11	63	70	72	74	00	00	cprt
00000176	01	50	00	00	00	33	64	65	73	63	00	00	01	84	00	00	P 3desc
00000192	00	6C	77	74	70	74	00	00	01	F0	00	00	00	14	62	6B	lwtpt ð bk
00000208	70	74	00	00	02	04	00	00	00	14	72	58	59	5A	00	00	pt rXYZ
00000224	02	18	00	00	00	14	67	58	59	5A	00	00	02	2C	00	00	gXYZ ,
00000240	00	14	62	58	59	5A	00	00	02	40	00	00	00	14	64	6D	bXYZ @ dm
00000256	6E	64	00	00	02	54	00	00	00	70	64	6D	64	64	00	00	nd T pdmdd
00000272	02	C4	00	00	00	88	76	75	65	64	00	00	03	4C	00	00	Ä ˆvued L
00000288	00	86	76	69	65	77	00	00	03	D4	00	00	00	24	6C	75	†view Ô $lu
00000304	6D	69	00	00	03	F8	00	00	00	14	6D	65	61	73	00	00	mi ø meas
00000320	04	0C	00	00	00	24	74	65	63	68	00	00	04	30	00	00	$tech 0
00000336	00	0C	72	54	52	43	00	00	04	3C	00	00	08	0C	67	54	rTRC < gT
00000352	52	43	00	00	04	3C	00	00	08	0C	62	54	52	43	00	00	RC < bTRC
00000368	04	3C	00	00	08	0C	74	65	78	74	00	00	00	00	43	6F	< text Co
00000384	70	79	72	69	67	68	74	20	28	63	29	20	31	39	39	38	pyright (c) 1998
00000400	20	48	65	77	6C	65	74	74	2D	50	61	63	6B	61	72	64	Hewlett-Packard
00000416	20	43	6F	6D	70	61	6E	79	00	00	64	65	73	63	00	00	Company desc
00000432	00	00	00	00	00	12	73	52	47	42	20	49	45	43	36	31	sRGB IEC61
00000448	39	36	36	2D	32	2E	31	00	00	00	00	00	00	00	00	00	966-2.1
00000464	00	00	12	73	52	47	42	20	49	45	43	36	31	39	36	36	sRGB IEC6
00000480	2D	32	2E	31	00	00	00	00	00	00	00	00	00	00	00	00	-2.1
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000528	00	00	00	00	00	00	58	59	5A	20	00	00	00	00	00	00	XYZ

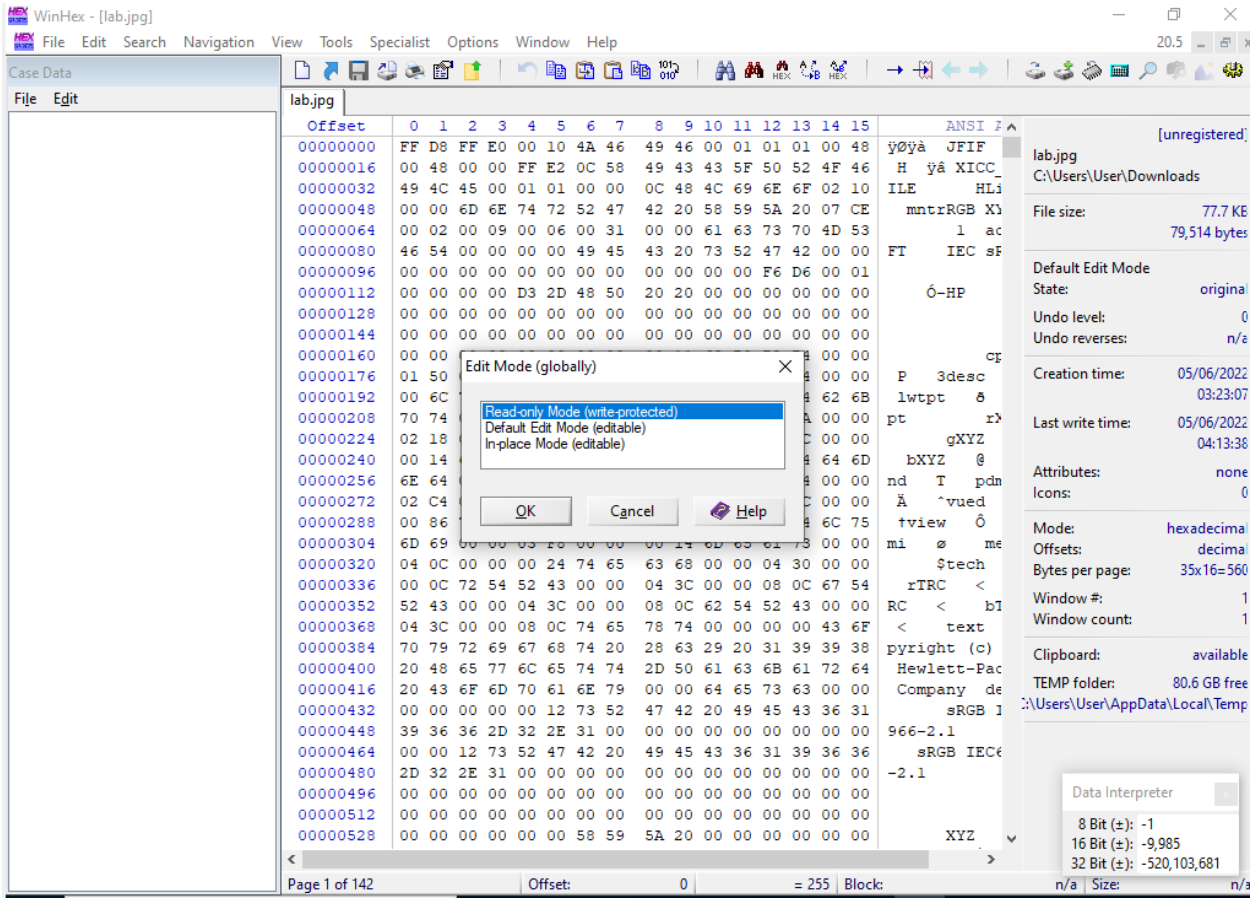
- Go to Options and then to EDIT mode.

Farzad Kheirabadi
CYB 528
UNIT 4

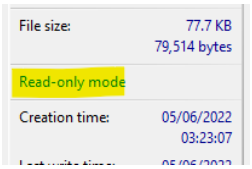


- Now select the read only mode and click OK.

Farzad Kheirabadi
CYB 528
UNIT 4

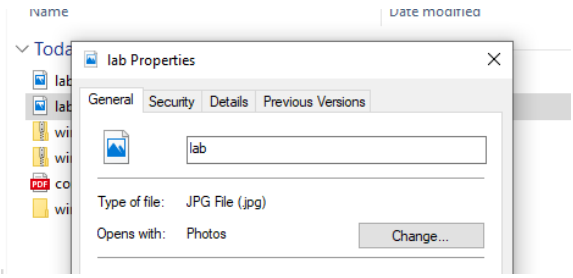


- Now below you can see the highlighted text where it shows read only mode



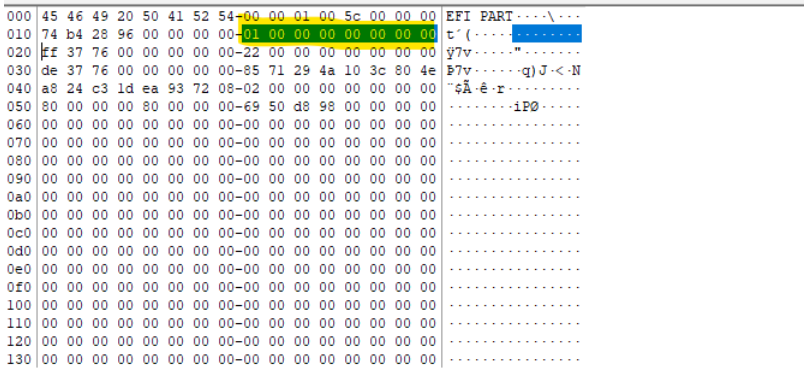
- Right click on the disk image file and go to properties and in attributes check mark the “READ ONLY” and apply

Farzad Kheirabadi
CYB 528
UNIT 4



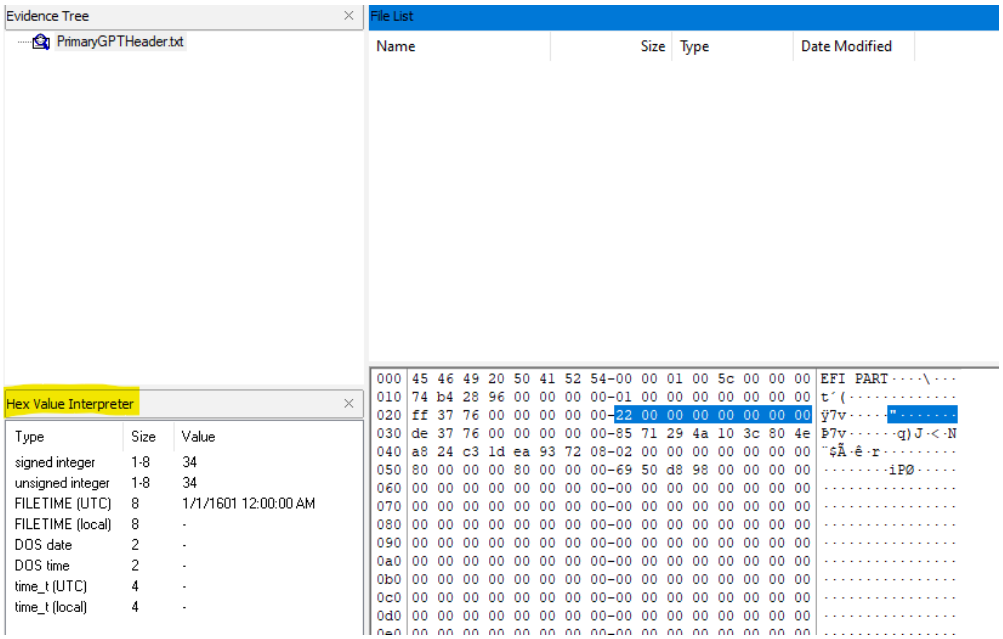
WinHex – GPT HEADER

- The LBA of the header

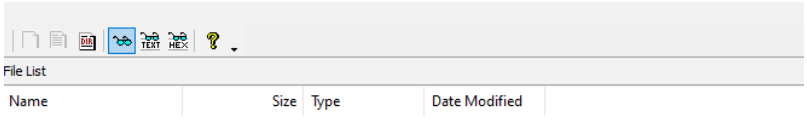


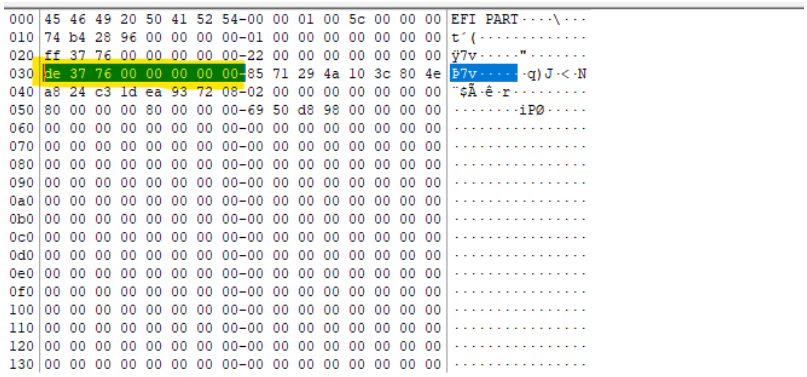
- The value of the First usable LBA

Farzad Kheirabadi
CYB 528
UNIT 4



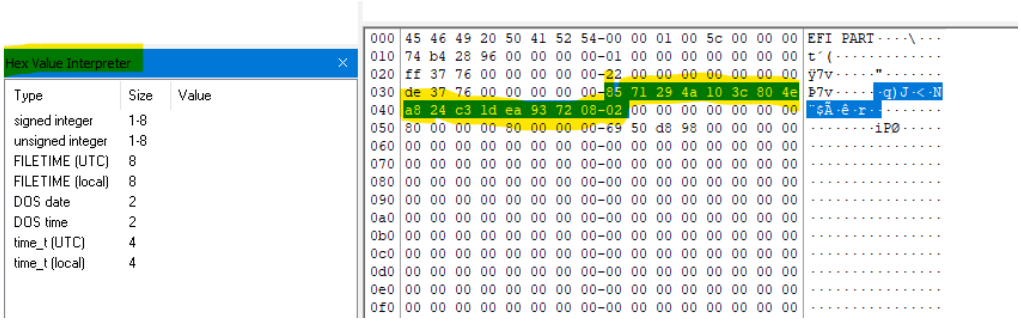
- Value of the Last Usable LBA



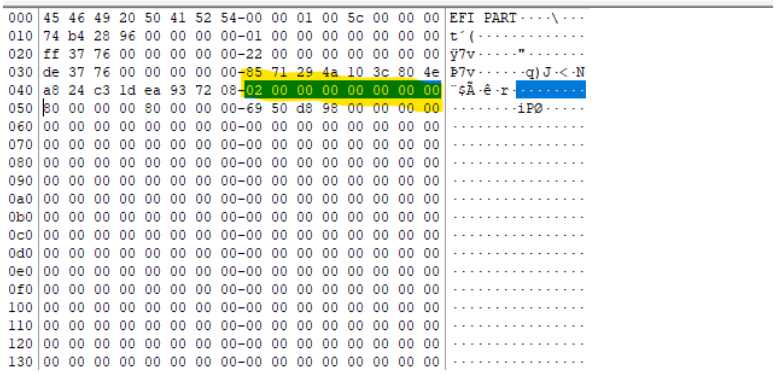


Farzad Kheirabadi
CYB 528
UNIT 4

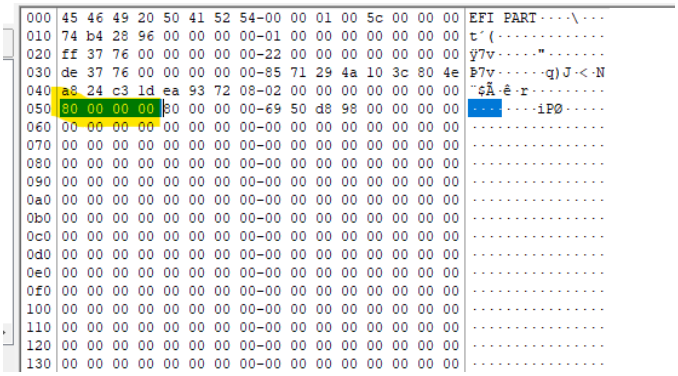
- The GUID of the disk



- Partition Entry LBA



- Number of Partitions



File System Analysis

Farzad Kheirabadi
CYB 528
UNIT 4

Creating an empty disk image, initialize it with a filesystem, mount it, execute a series of commands that create and remove files (and thus change the filesystem and disk image), unmount the disk image, and then examine the disk image to see what data remains.

Create a new disk 10 MB image

```
10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.0162677 s, 645 MB/s
```

This will create a 10M disk image, whereas ZFS requires at least 64M.
Initialize it with a file system

```
mkfs.fat 4.1 (2017-01-24)
```