1 LAB 3 GUIDE

Objective: Users sometimes hide files from plying eyes in shared computers by changing the file extension, file signature and also shifting the bits in file.

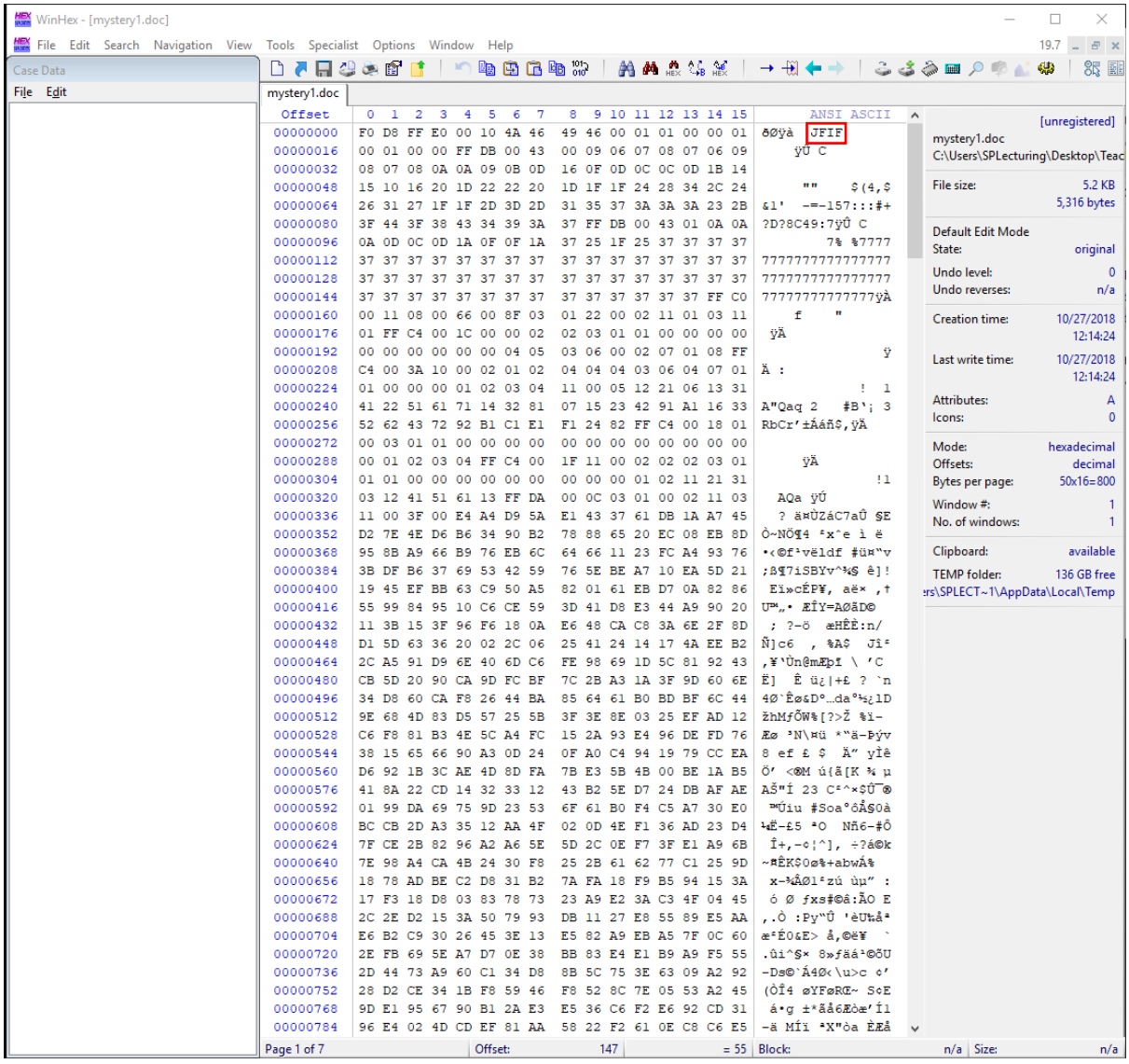
a. Download “DFI Practical 3v2” from the blackboard.

b. Read the ”Intro to WinHex.pptx “ article to familiarize yourself with this hex editor. Read the online manual of WinHex to learn more about its capabilities.

c. Follow steps in this guide to work on your Lab 3

1.1 MYSTERY1.DOC GUIDE (SUSPECTED FILE SIGNATURE ISSUE)

1.1.1 Open up file “Mystery1.doc” in WinHex.



1.1.2 Now we know that this is a jpg file as JFIF represent jpg. Navigate to https://en.wikipedia.org/wiki/List_of_file_signatures and look for jpg file signature.

Hex signature	ISO 8859-1	Offset	Extension	Description
23 21	#!	0		Script or data to be passed to the program following the shebang (#!)[1]
00 00 02 00 06 04 06 00 08 00 00 00 00 00	NULNULSTXNULACKEOTACKNULACKNULNULNULNULNUL	0	wk1	Lotus 1-2-3 spreadsheet (v1) file
00 00 1A 00 00 10 04 00 00 00 00 00	NULNULSUBNULNUL LF EOTNULNULNULNULNUL	0	wk3	Lotus 1-2-3 spreadsheet (v3) file
00 00 1A 00 02 10 04 00 00 00 00 00	NULNULSUBNULSTX LF EOTNULNULNULNULNUL	0	wk4 wk5	Lotus 1-2-3 spreadsheet (v4, v5) file
00 00 1A 00 05 10 04	NULNULSUBNULENQ LF EOT	0	123	Lotus 1-2-3 spreadsheet (v9) file

1.1.3 Change the file signature of Mystery1.doc from “F0 D8 FF E0” to “FF D8 FF E0”

mystery1.doc

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	F0	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ðØÿà JFIF
00000016	00	01	00	00	FF	DB	00	43	00	09	06	07	08	07	06	09	ÿÛ C
00000032	08	07	08	0A	0A	09	0B	0D	16	0F	0D	0C	0C	0D	1B	14	

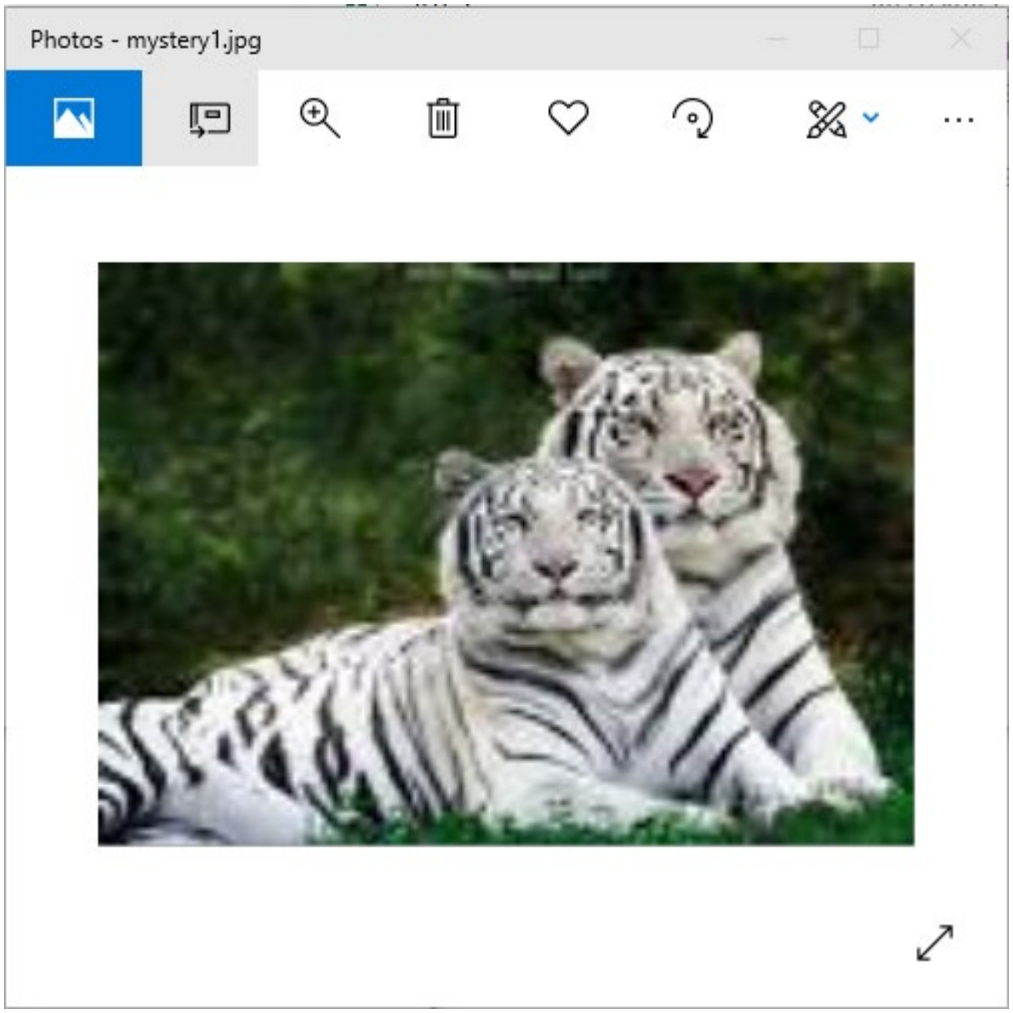
Original Hexadecimal value

mystery1.doc

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà JFIF
00000016	00	01	00	00	FF	DB	00	43	00	09	06	07	08	07	06	09	ÿÛ C
00000032	08	07	08	0A	0A	09	0B	0D	16	0F	0D	0C	0C	0D	1B	14	

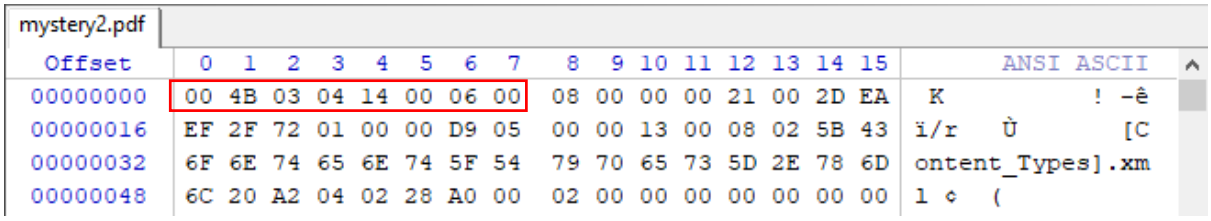
Modified Hexadecimal value

1.1.4 Save the changes in WinHex, change the extension of the file from “.doc” to “.jpg” and you will be able view the image.



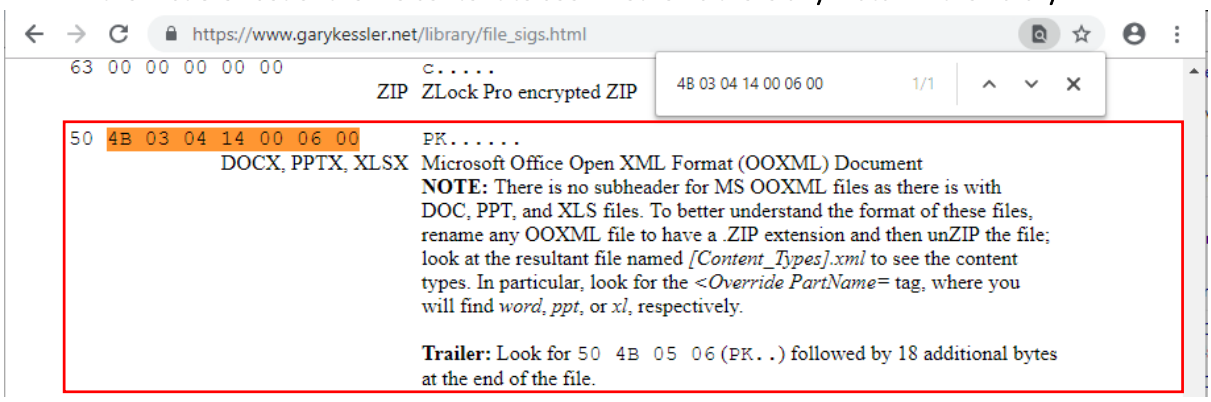
1.2 MYSTERY2.PDF (SUSPECTED FILE SIGNATURE)

1.2.1 Open Mystery2.PDF using WinHex. And take note of the file signature. Note that the signature might be corrupted.



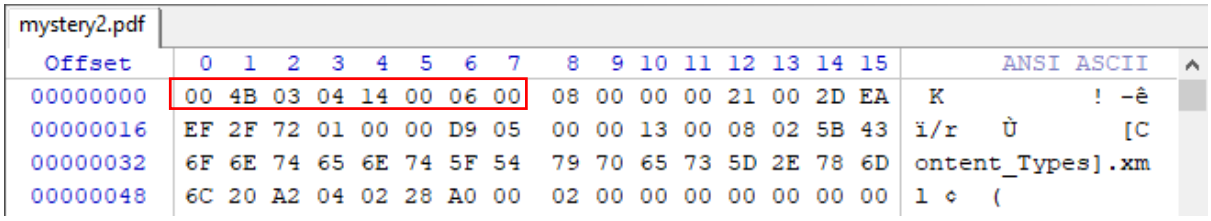
```
mystery2.pdf
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15    ANSI ASCII
00000000  00 4B 03 04 14 00 06 00  08 00 00 00 21 00 2D EA    K          ! -ê
00000016  EF 2F 72 01 00 00 D9 05  00 00 13 00 08 02 5B 43   ï/r   Ù       [C
00000032  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D   ontent_Types].xm
00000048  6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00   l ¢  (
```

1.2.2 Refer to https://www.garykessler.net/library/file_sigs.html and check for file signature. Check the first 8 Offset of the file content to see whether is there any match in the library.



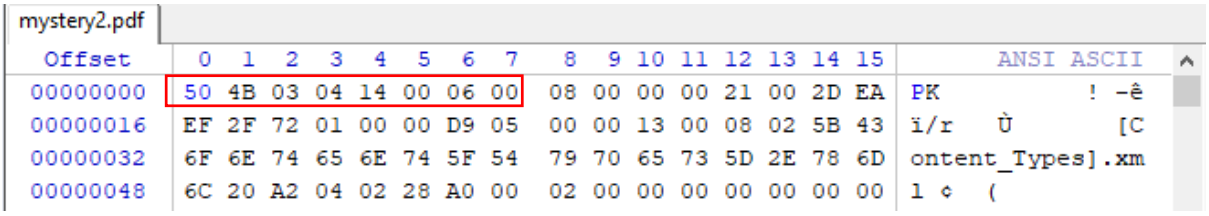
```
https://www.garykessler.net/library/file_sigs.html
63 00 00 00 00 00          c.....
                     ZIP   ZLock Pro encrypted ZIP
                                                    4B 03 04 14 00 06 00   1/1

50 4B 03 04 14 00 06 00    PK......
                 DOCX, PPTX, XLSX  Microsoft Office Open XML Format (OOXML) Document
                 NOTE: There is no subheader for MS OOXML files as there is with
                 DOC, PPT, and XLS files. To better understand the format of these files,
                 rename any OOXML file to have a .ZIP extension and then unZIP the file;
                 look at the resultant file named [Content_Types].xml to see the content
                 types. In particular, look for the <Override PartName= tag, where you
                 will find word, ppt, or xl, respectively.

                 Trailer: Look for 50 4B 05 06 (PK..) followed by 18 additional bytes
                 at the end of the file.
```

1.2.3 Change the file signature of Mystery2.PDF from "00 4B 03 04 14 00 60 00" to "50 4B 03 04 14 00 60 00"



```
mystery2.pdf
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15    ANSI ASCII
00000000  00 4B 03 04 14 00 06 00  08 00 00 00 21 00 2D EA    K          ! -ê
00000016  EF 2F 72 01 00 00 D9 05  00 00 13 00 08 02 5B 43   ï/r   Ù       [C
00000032  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D   ontent_Types].xm
00000048  6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00   l ¢  (
```

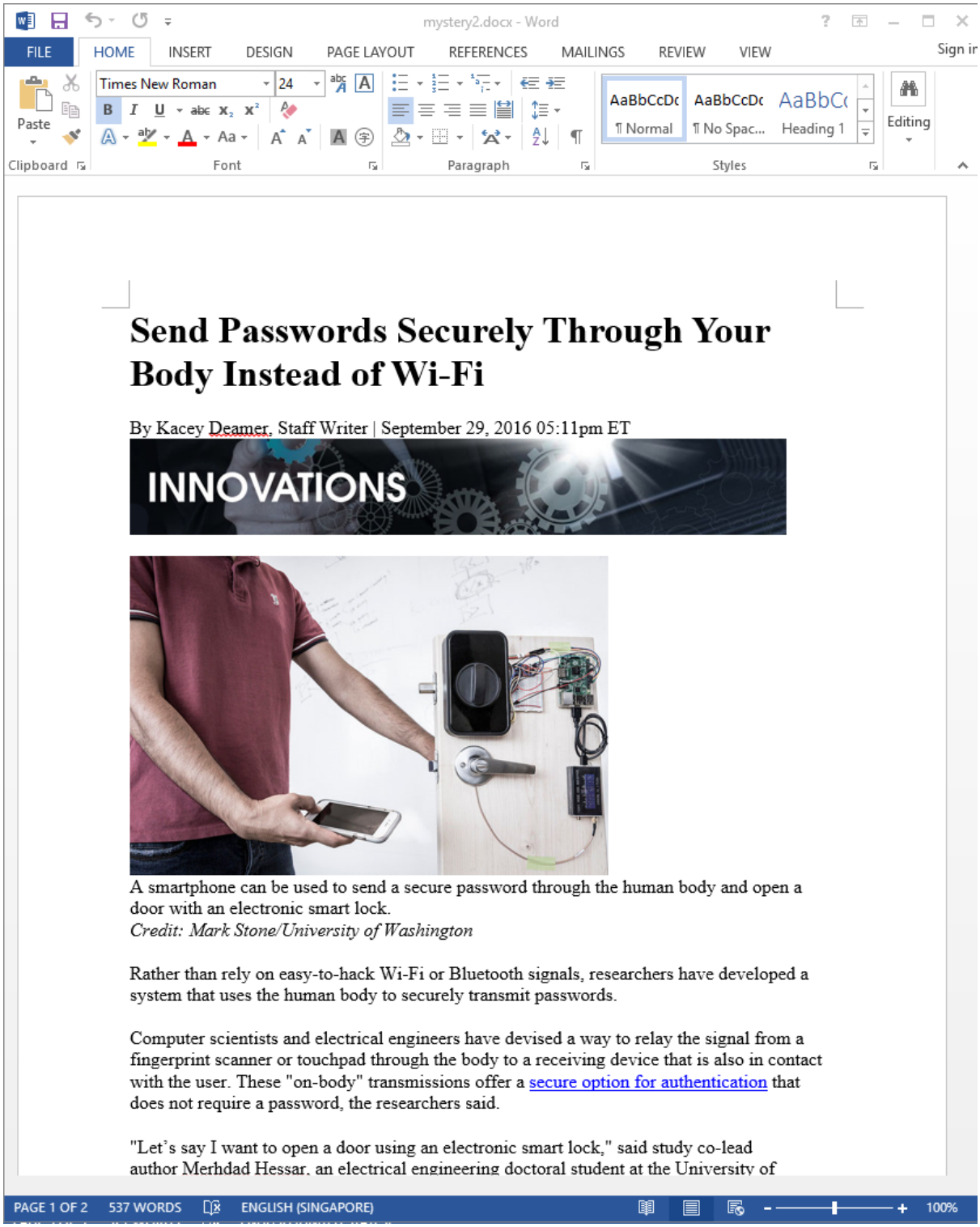
Original Hexadecimal value



```
mystery2.pdf
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15    ANSI ASCII
00000000  50 4B 03 04 14 00 06 00  08 00 00 00 21 00 2D EA   PK          ! -ê
00000016  EF 2F 72 01 00 00 D9 05  00 00 13 00 08 02 5B 43   ï/r   Ù       [C
00000032  6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D   ontent_Types].xm
00000048  6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00   l ¢  (
```

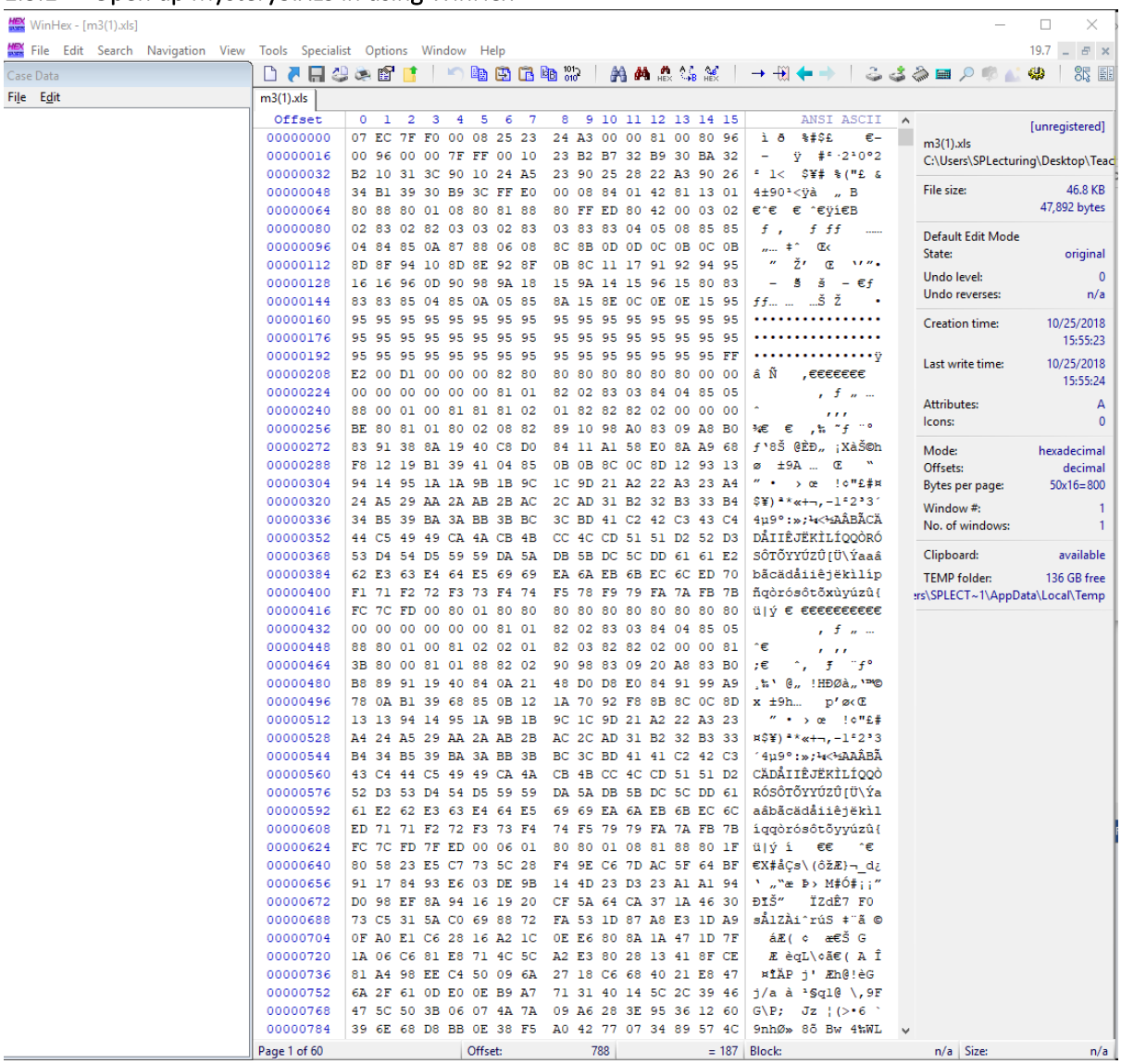
Modified Hexadecimal value

1.2.4 Save the changes in WinHex, change the extension of the file from ".PDF" to ".docx" and you will be able view the image.

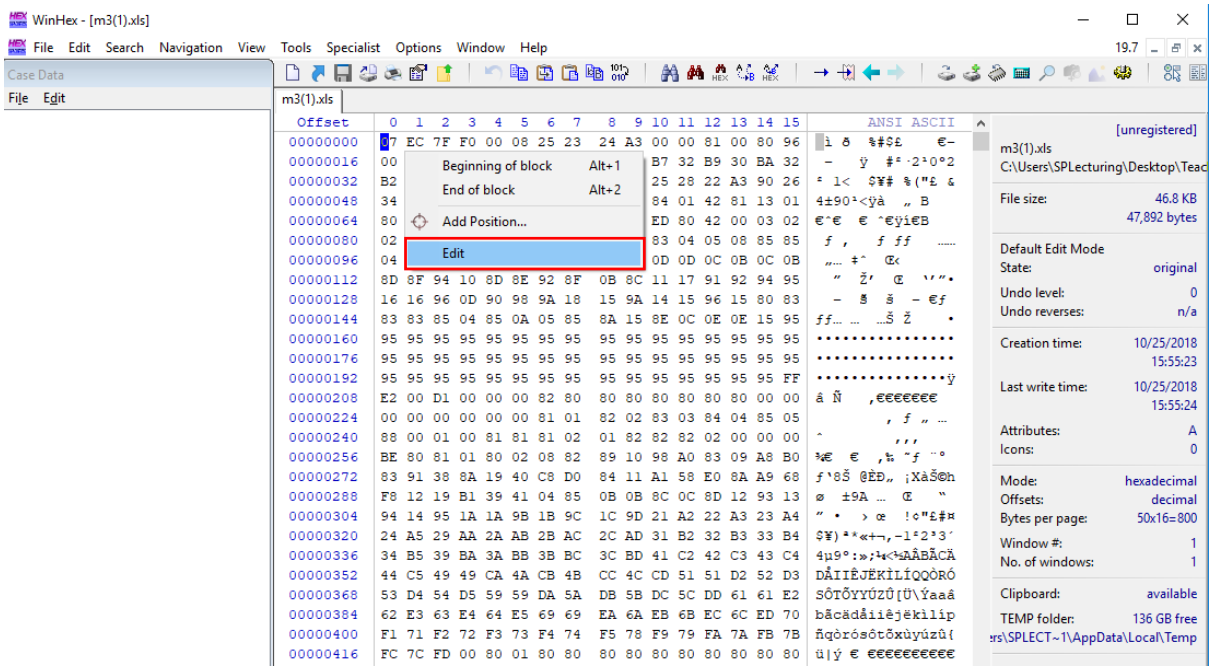


1.3 MYSTERY3.XLS (BIT SHIFTING)

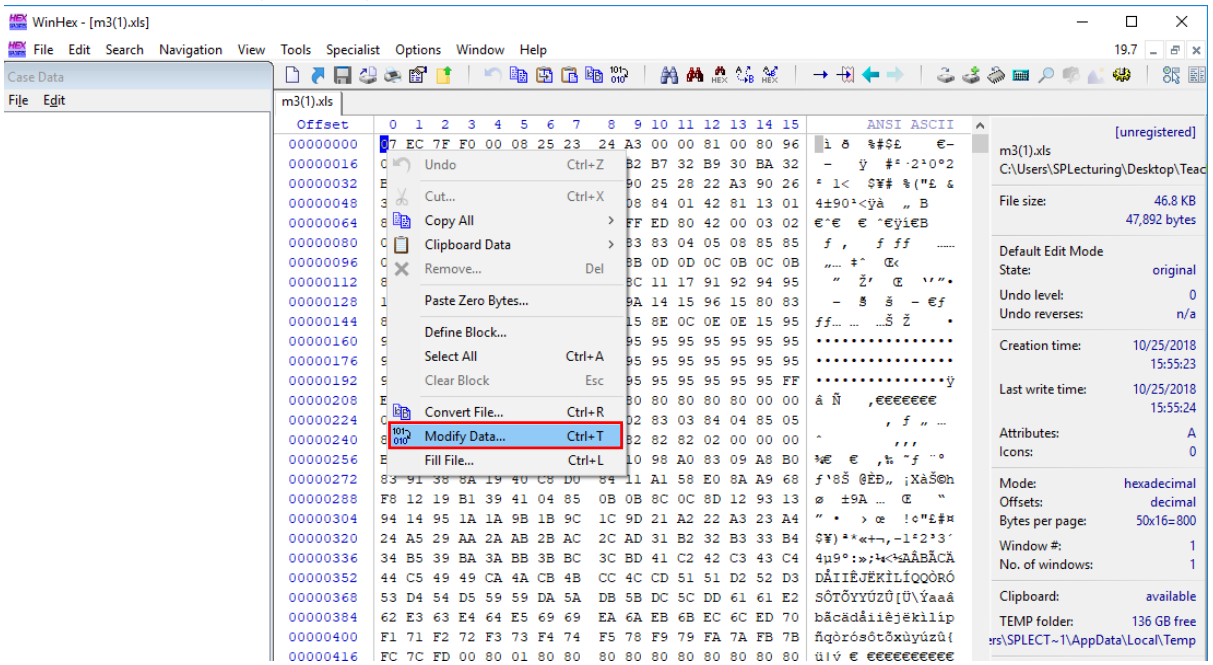
1.3.1 Open up Mystery3.XLS in using WinHex



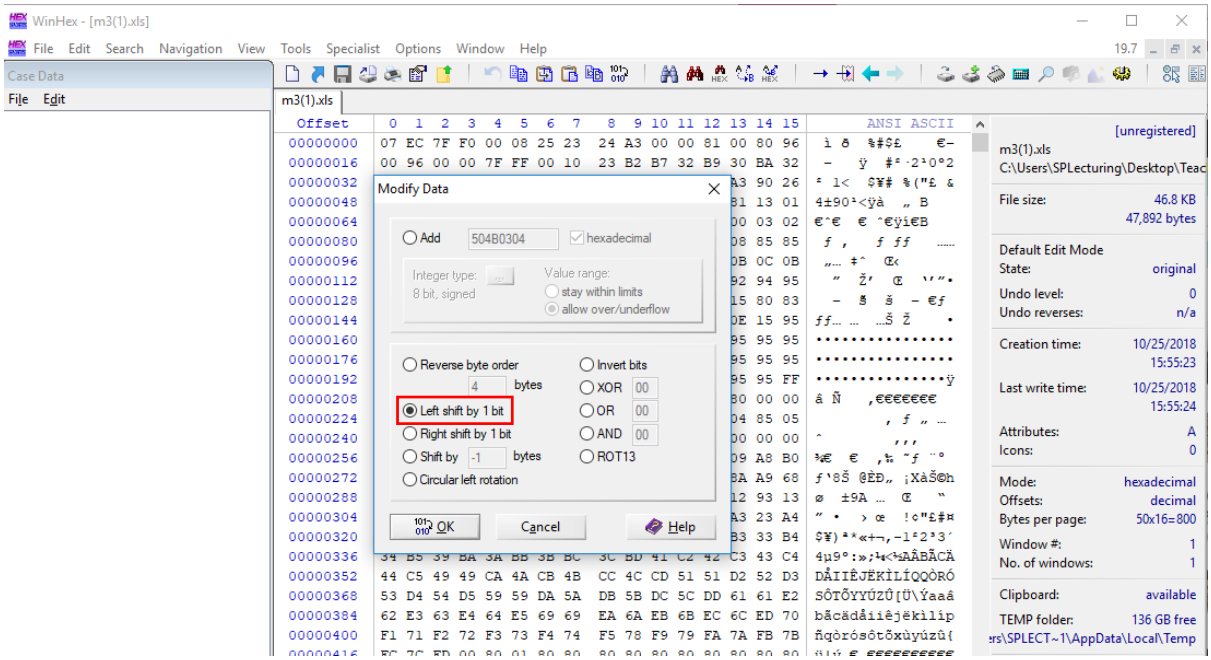
1.3.2 Right click on the Hexadecimal data and select “Edit” option.



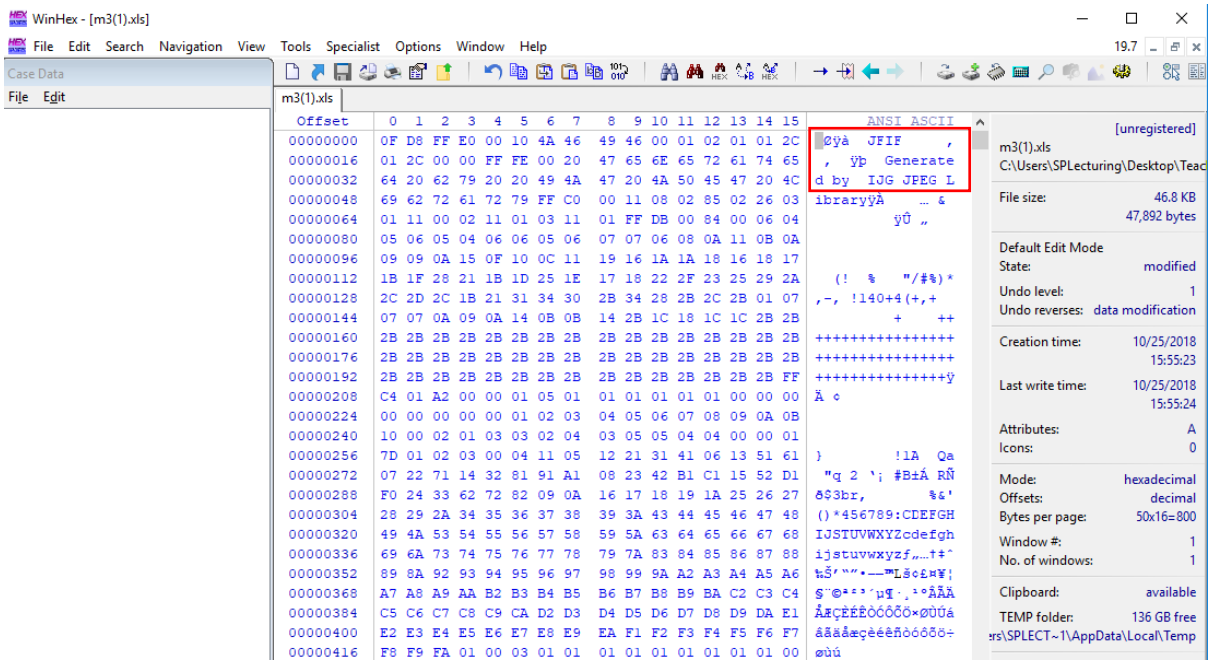
1.3.3 Select “Modify Data” option.



1.3.4 Check the “Left shift by 1 bit” radio button and press ok



1.3.5 The file will be should to 1 bit by the left. Notice the new Hexadecimal value of the file



1.3.6 The file signature for JPEG is Hexadecimal value of “FF D8 FF E8”. Change the file signature (first 4 offset) to the Hexadecimal value “FF D8 FF E8”

m3(1).jpeg

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	0F	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	01	2C	Øÿà JFIF ,
00000016	01	2C	00	00	FF	FE	00	20	47	65	6E	65	72	61	74	65	, ÿþ Generate
00000032	64	20	62	79	20	20	49	4A	47	20	4A	50	45	47	20	4C	d by IJG JPEG L
00000048	69	62	72	61	72	79	FF	C0	00	11	08	02	85	02	26	03	ibraryÿÀ … &

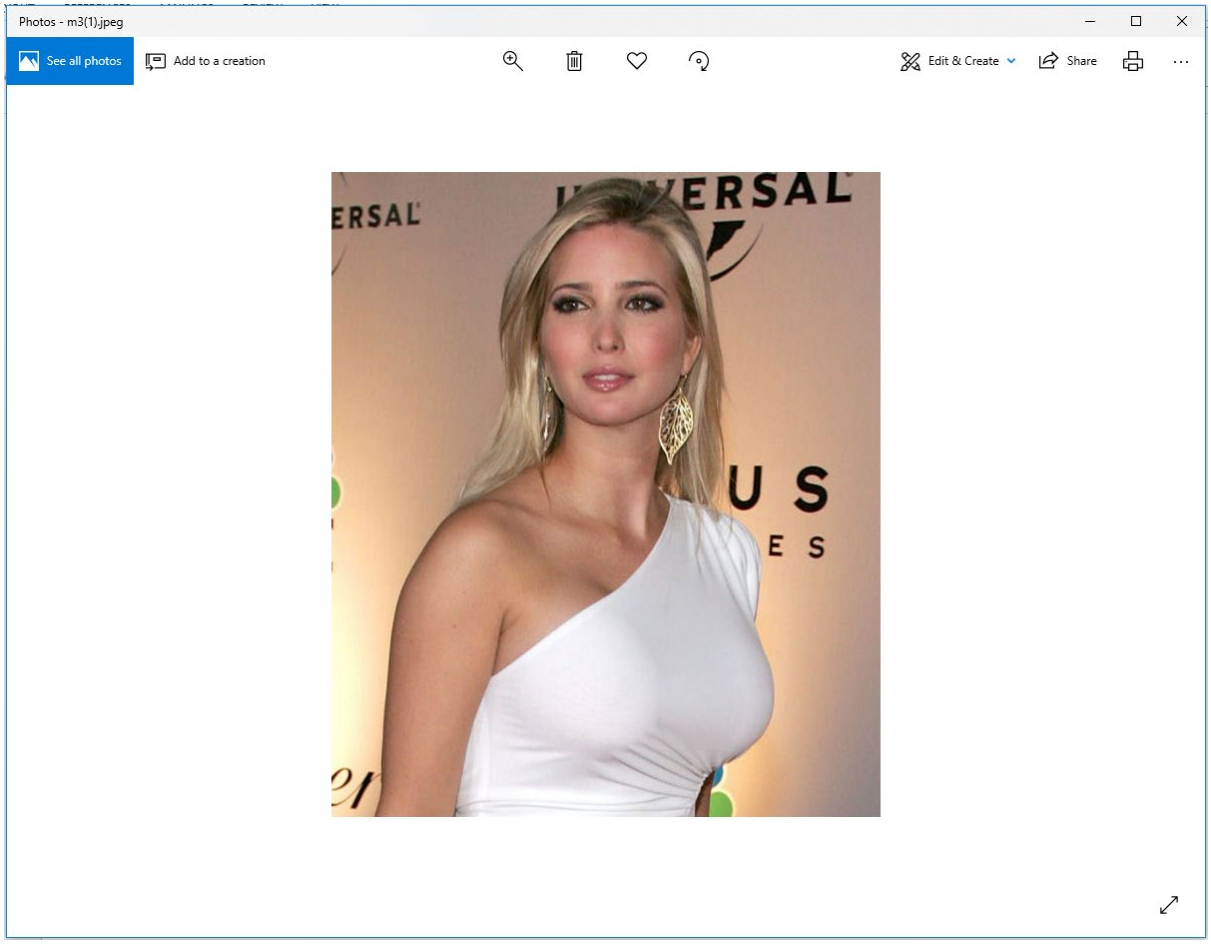
Original Hexadecimal value

m3(1).jpeg

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	01	2C	ÿØÿà JFIF ,
00000016	01	2C	00	00	FF	FE	00	20	47	65	6E	65	72	61	74	65	, ÿþ Generate
00000032	64	20	62	79	20	20	49	4A	47	20	4A	50	45	47	20	4C	d by IJG JPEG L
00000048	69	62	72	61	72	79	FF	C0	00	11	08	02	85	02	26	03	ibraryÿÀ … &

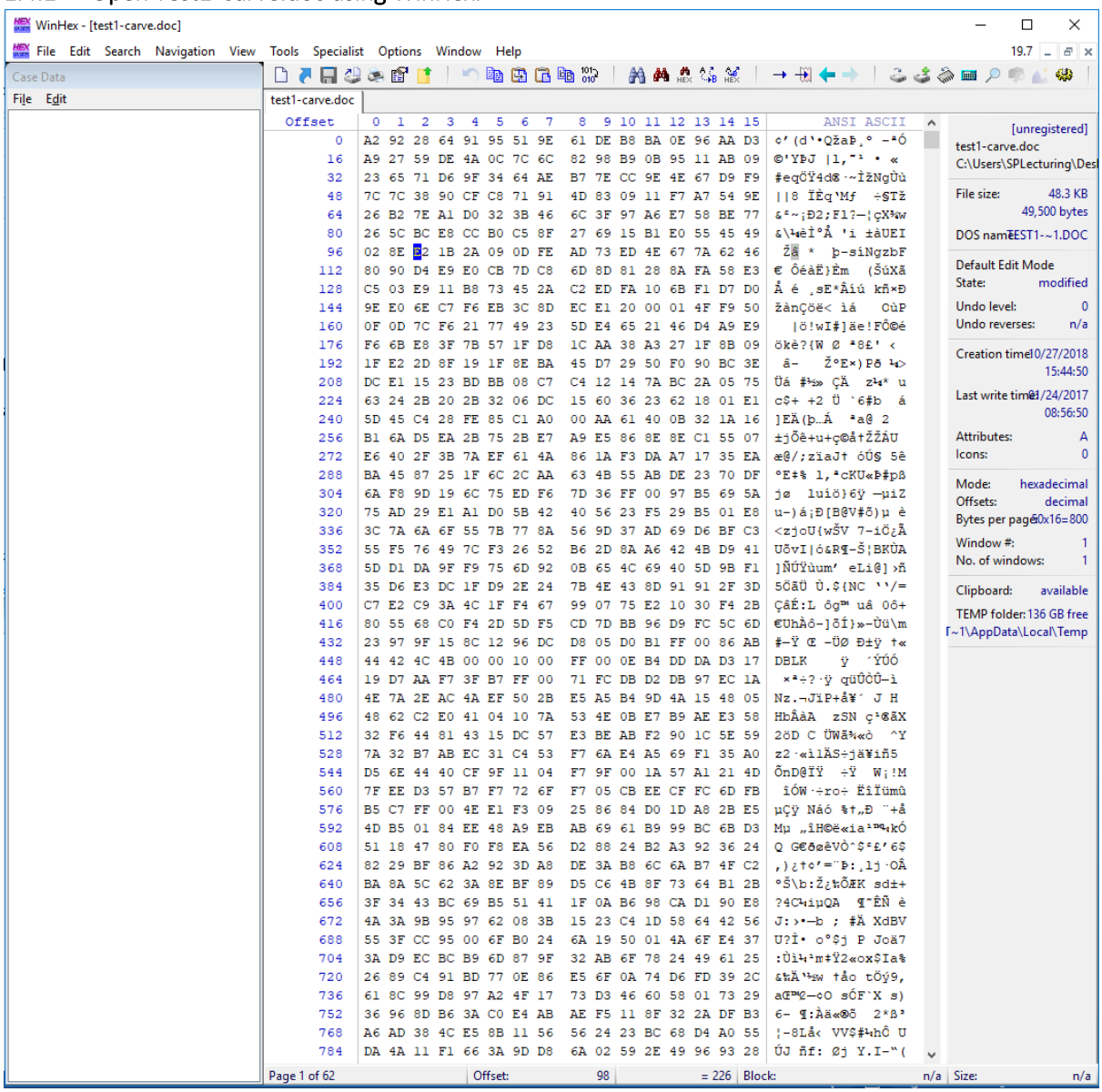
Modified Hexadecimal value

1.3.7 Save the changes in WinHex, change the extension of the file from “.xls” to “.jpg” and you will be able view the image.

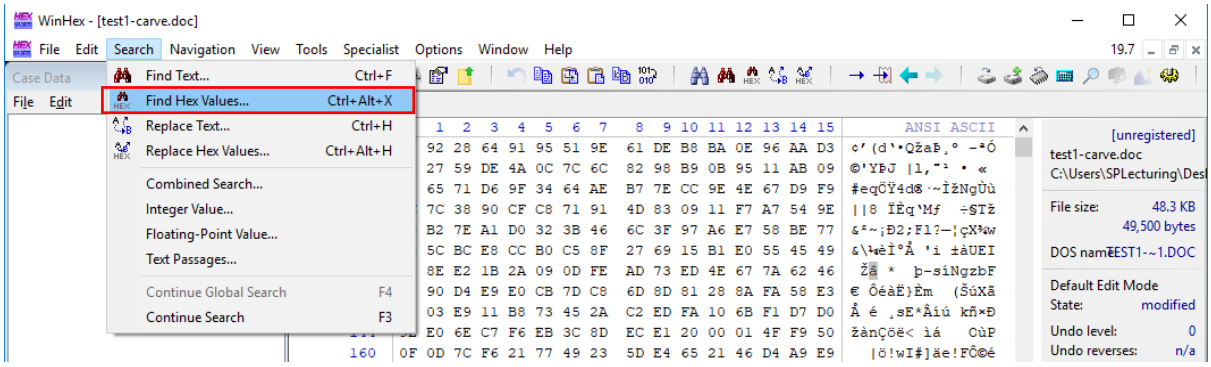


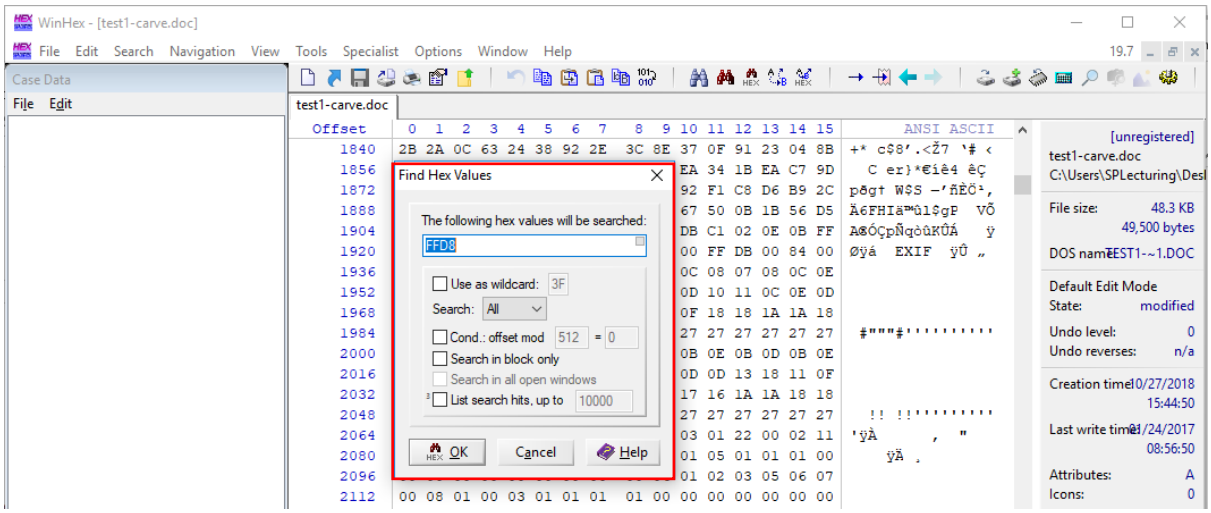
1.4 TEST1-CARVE.DOC

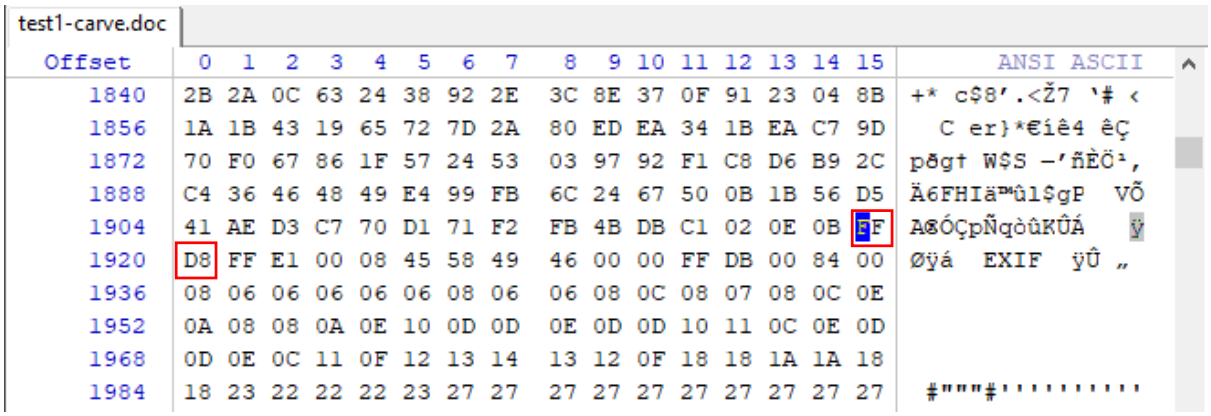
1.4.1 Open Test1-Carve.doc using WinHex.



1.4.2 Perform a search for the Hexadecimal value of “FF D8”.





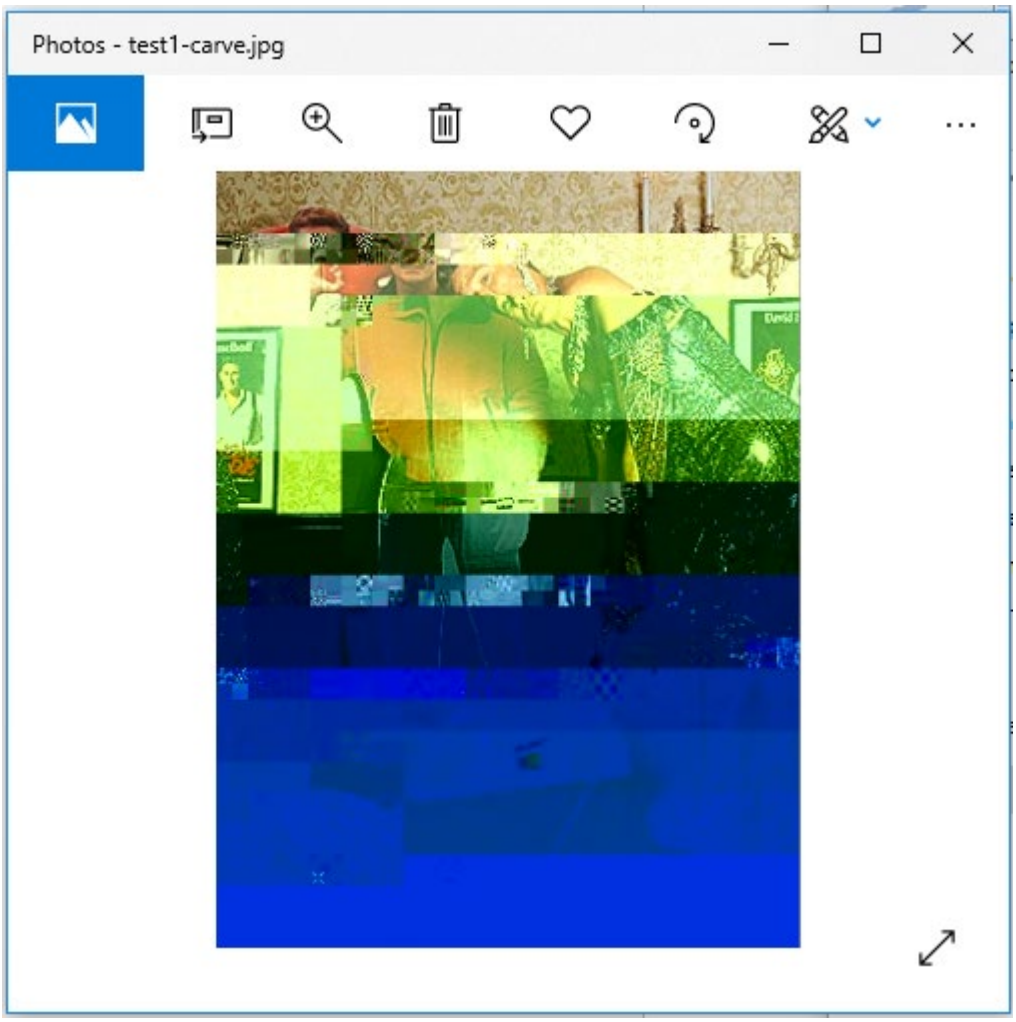


1.4.3 Upon location of the Hexadecimal value “FF D8”, remove all unwanted data before the Hexadecimal value of “FF D8” and search for the Hexadecimal value “FF D9” and remove all unwanted data after the Hexadecimal value of “FF D9”

test1-carve.doc

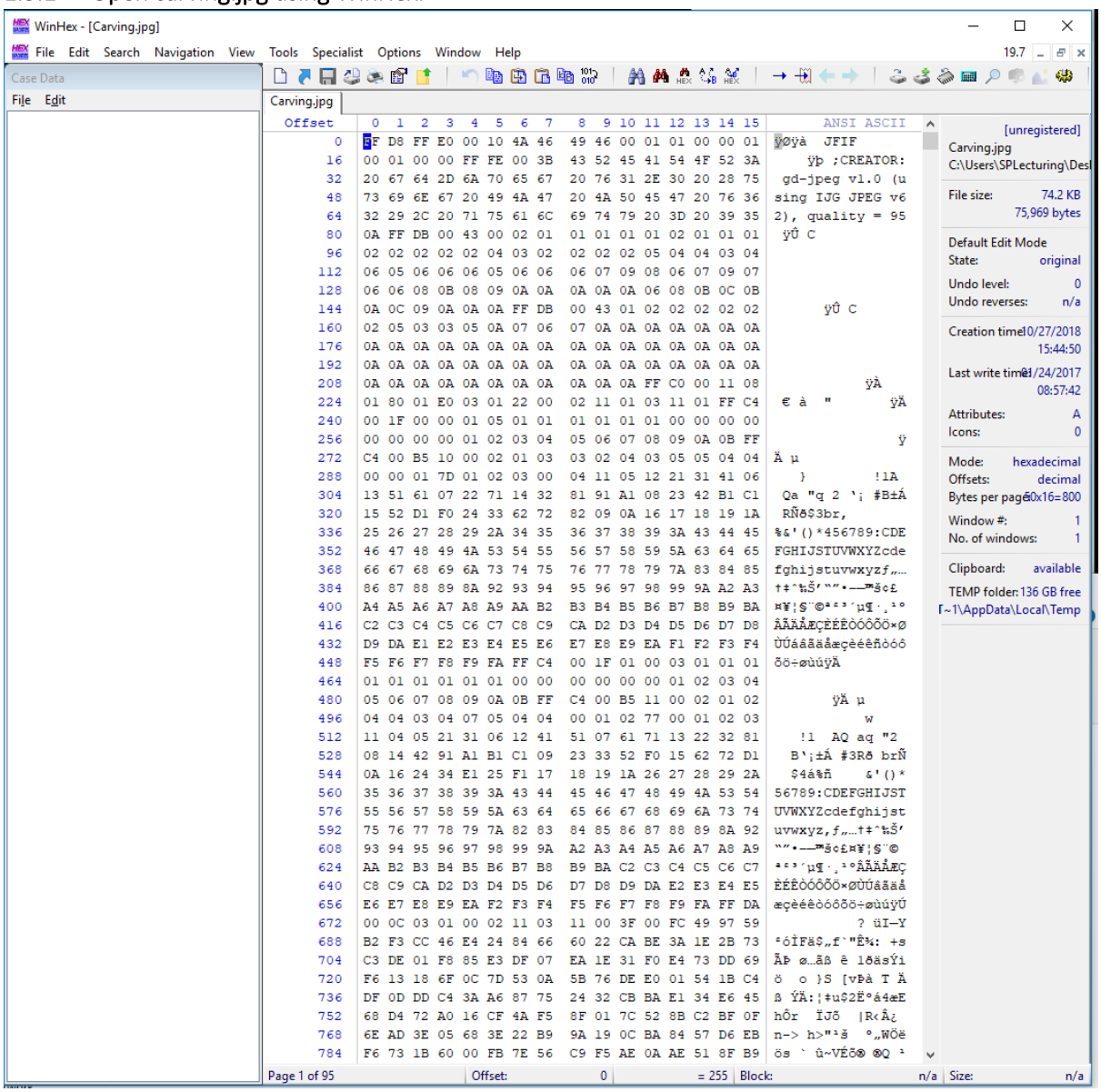
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0	FF	D8	FF	E1	00	08	45	58	49	46	00	00	FF	DB	00	84	ÿØÿá EXIF ÿÛ „
16	00	08	06	06	06	06	06	08	06	06	08	0C	08	07	08	0C	
32	0E	0A	08	08	0A	0E	10	0D	0D	0E	0D	0D	10	11	0C	0E	
48	0D	0D	0E	0C	11	0F	12	13	14	13	12	0F	18	18	1A	1A	
64	18	18	23	22	22	22	23	27	27	27	27	27	27	27	27	27	#"""#''''''''''
80	27	01	09	08	08	09	0A	09	0B	09	09	0B	0E	0B	0D	0B	'
96	0E	11	0E	0E	0E	0E	11	13	0D	0D	0E	0D	0D	13	18	11	
112	0F	0F	0F	0F	11	18	16	17	14	14	14	17	16	1A	1A	18	
128	18	1A	1A	21	21	20	21	21	27	27	27	27	27	27	27	27	!! !!''''''''''
144	27	27	FF	C0	00	11	08	01	90	01	2C	03	01	22	00	02	''ÿÀ , "
160	11	01	03	11	01	FF	C4	00	B8	00	00	01	05	01	01	01	ÿÄ ¸
176	00	00	00	00	00	00	00	00	00	00	04	01	02	03	05	06	
192	07	00	08	01	00	03	01	01	01	01	00	00	00	00	00	00	

1.4.4 Save the changes in WinHex, change the extension of the file from “.doc” to “.jpg” and you will be able view the image.

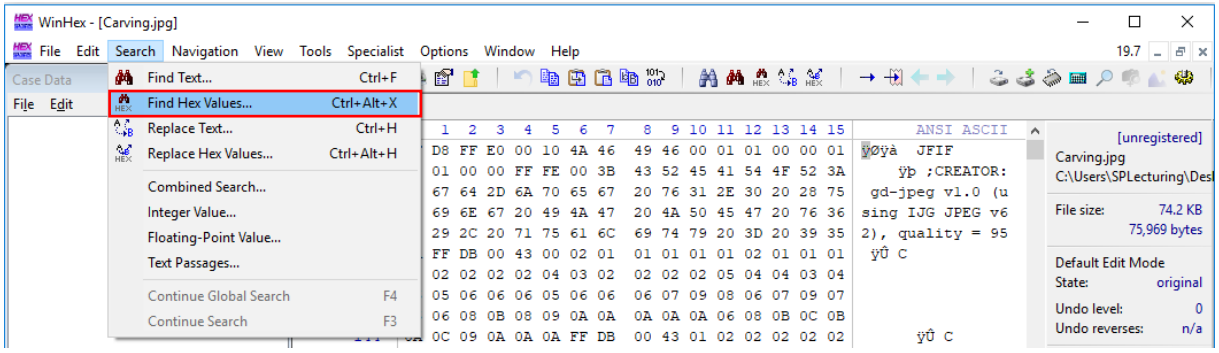


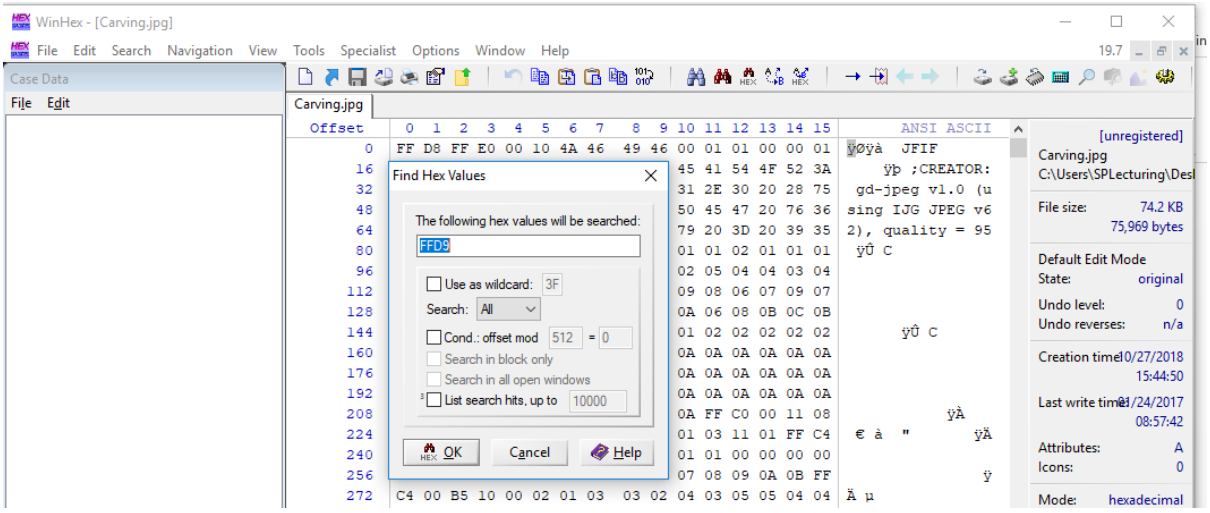
1.5 CARVING.JPG

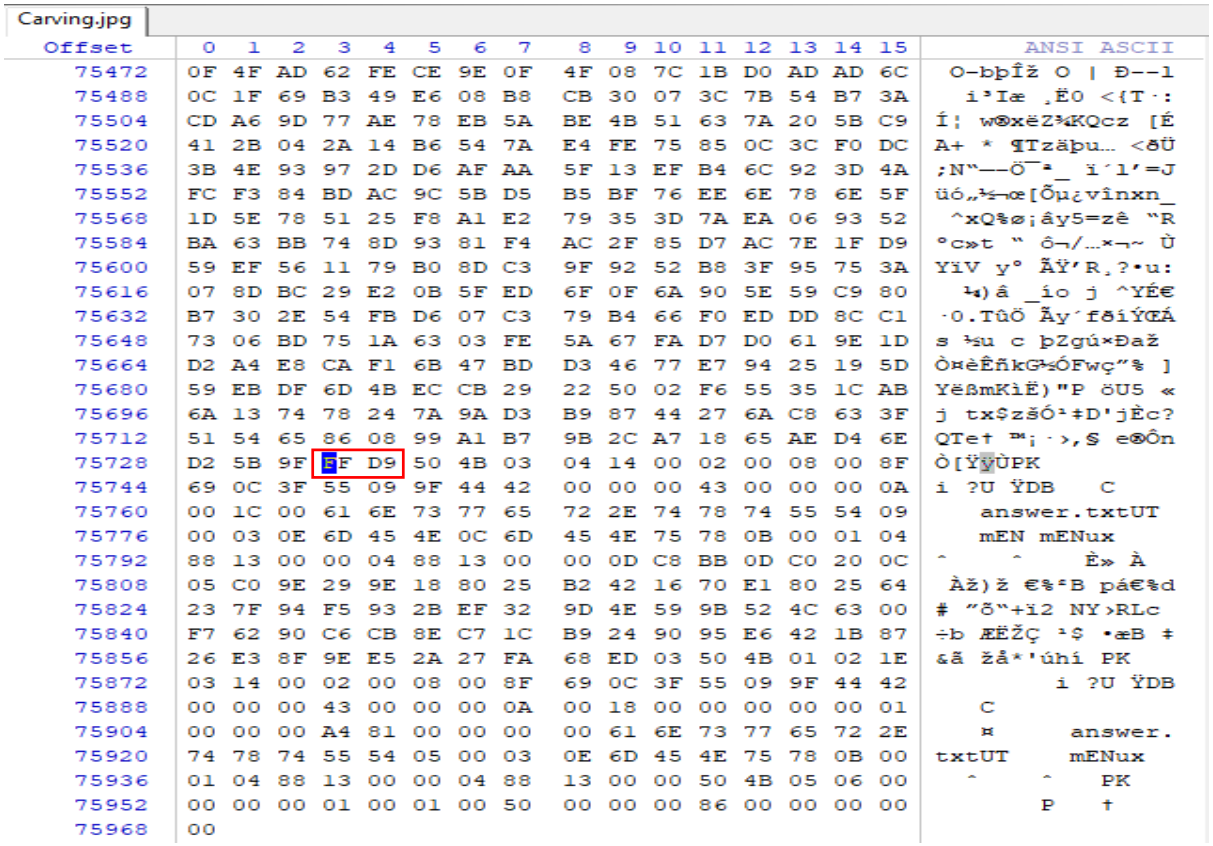
1.5.1 Open carving.jpg using WinHex.



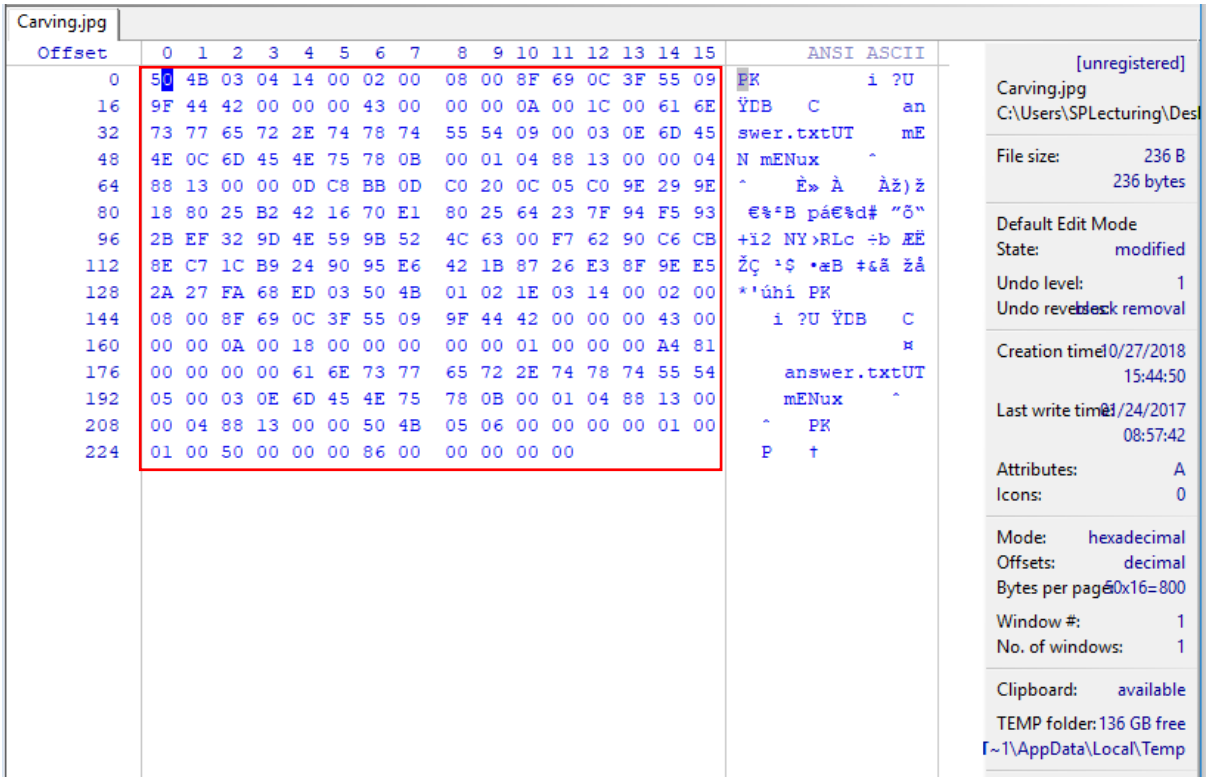
1.5.2 Perform a search for the Hexadecimal value of “FF D9”.



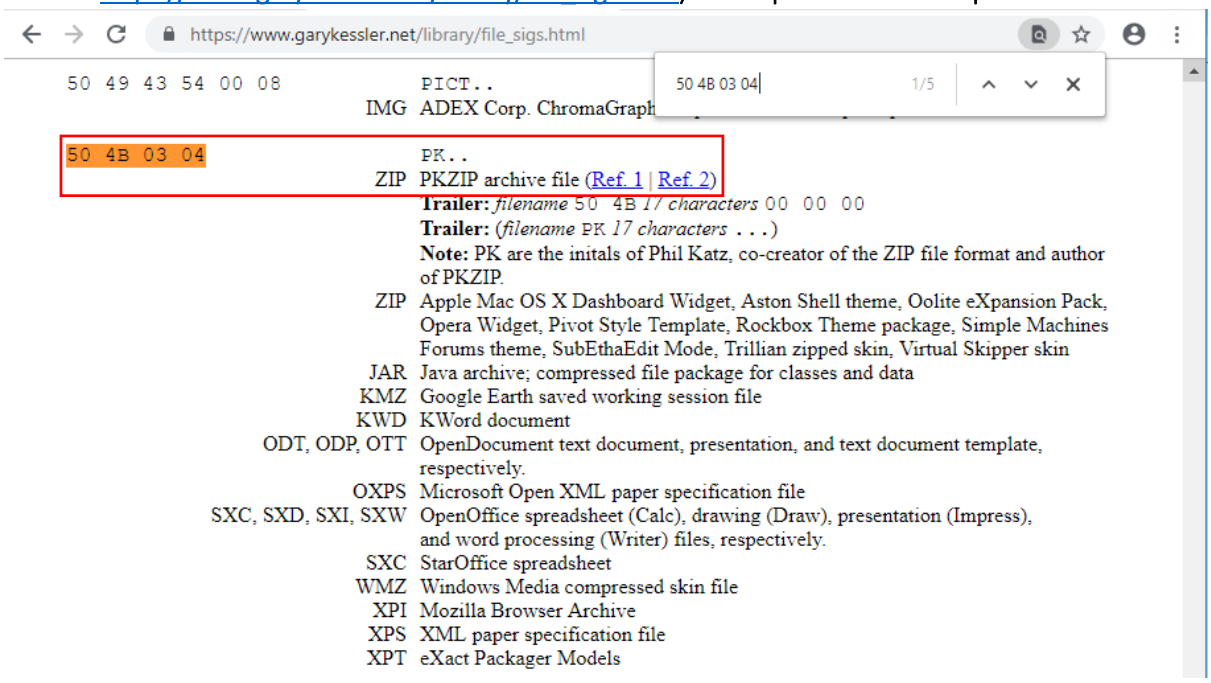




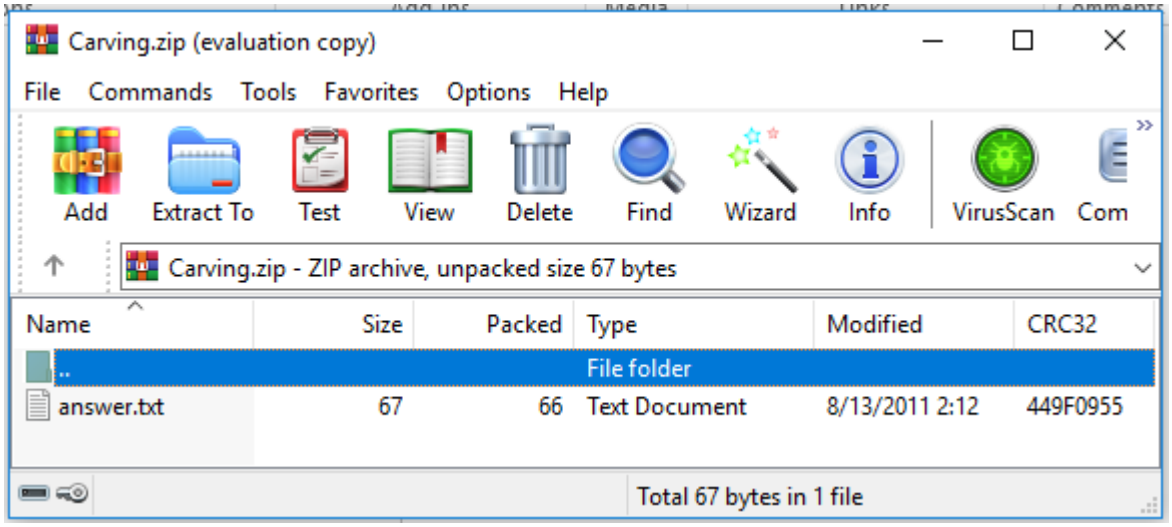
1.5.3 Upon location of the Hexadecimal value “FF D9”, remove all unwanted data before the Hexadecimal value of “FF D9” as well as “FF D9”.



1.5.4 Based on the file signature’s Hexadecimal value of “50 4B 03 04 14 00 20 00” (from https://www.garykessler.net/library/file_sigs.html) we suspect it can be a zip file.



1.5.5 Save the changes in WinHex, change the extension of the file from “.jpg” to “.zip” and you will be able view the zip file containing answer.txt file.



1.5.6 The text in answer.txt is “Congratulations. The answer for this tutorial page is "turnips".”