

# 1 LAB 3 GUIDE

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

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

The screenshot displays the WinHex application window with the file 'mystery1.doc' open. The main editing area is split into two panes: a hexadecimal view on the left and an ASCII view on the right. In the ASCII view, the characters 'JFIF' are highlighted with a red rectangular box, which is the standard signature for a JPEG image file. The right-hand sidebar provides detailed file information, including the file size (5.2 KB / 5,316 bytes), creation and last write times (both 10/27/2018 at 12:14:24), and various system attributes. The status bar at the bottom indicates the current offset is 147 and the block size is 55 bytes.

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](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 ( <a href="#">#!</a> ) <sup>[1]</sup>
00 00 02 00 06 04 06 00 08 00 00 00 00 00	NULNULSTXNULACKEOTACKNULACKNULNULNULNUL	0	wk1	Lotus 1-2-3 spreadsheet (v1) file
00 00 1A 00 00 10 04 00 00 00 00 00	NULNULSUBNULNUL LF EOTNULNULNULNUL	0	wk3	Lotus 1-2-3 spreadsheet (v3) file
00 00 1A 00 02 10 04 00 00 00 00 00	NULNULSUBNULSTX LF EOTNULNULNULNUL	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"

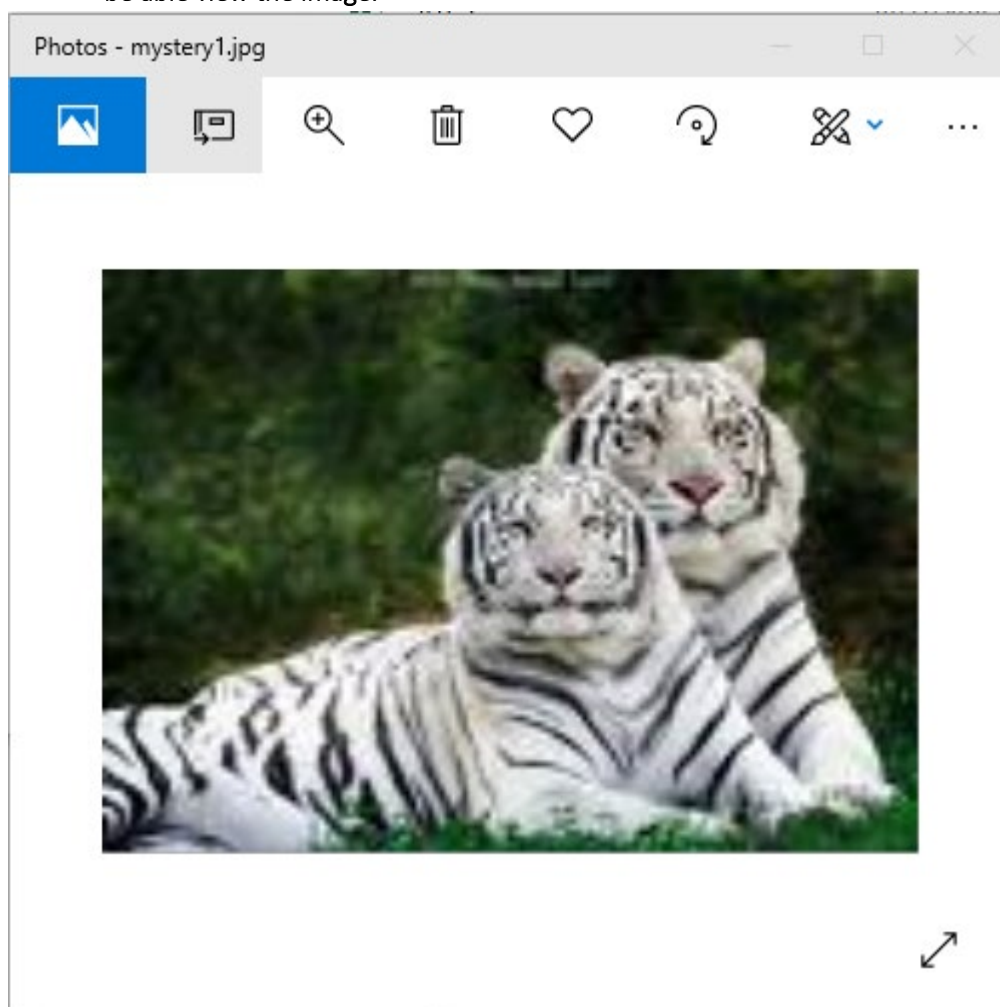
mystery1.doc																	ANSI ASCII	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
00000000	F0	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	øÿà	JFIF
00000016	00	01	00	00	FF	DB	00	43	00	09	06	07	08	07	06	09	ÿÛ	C
00000032	08	07	08	0A	0A	09	0B	0D	16	0F	0D	0C	0C	0D	1B	14		

Original Hexadecimal value

mystery1.doc																	ANSI ASCII	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿøà	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	i/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	1	¢	(

1.2.2 Refer to [https://www.garykessler.net/library/file\\_sigs.html](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.

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	i/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	1	¢	(

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	i/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	1	¢	(

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.


mystery2.docx - Word

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW Sign in

Clipboard Font Paragraph Styles Editing

## Send Passwords Securely Through Your Body Instead of Wi-Fi

By Kacey Deamer, Staff Writer | September 29, 2016 05:11pm ET



**INNOVATIONS**

A smartphone can be used to send a secure password through the human body and open a door with an electronic smart lock.

*Credit: Mark Stone/University of Washington*

Rather than rely on easy-to-hack Wi-Fi or Bluetooth signals, researchers have developed a system that uses the human body to securely transmit passwords.

Computer scientists and electrical engineers have devised a way to relay the signal from a fingerprint scanner or touchpad through the body to a receiving device that is also in contact with the user. These "on-body" transmissions offer a [secure option for authentication](#) that does not require a password, the researchers said.

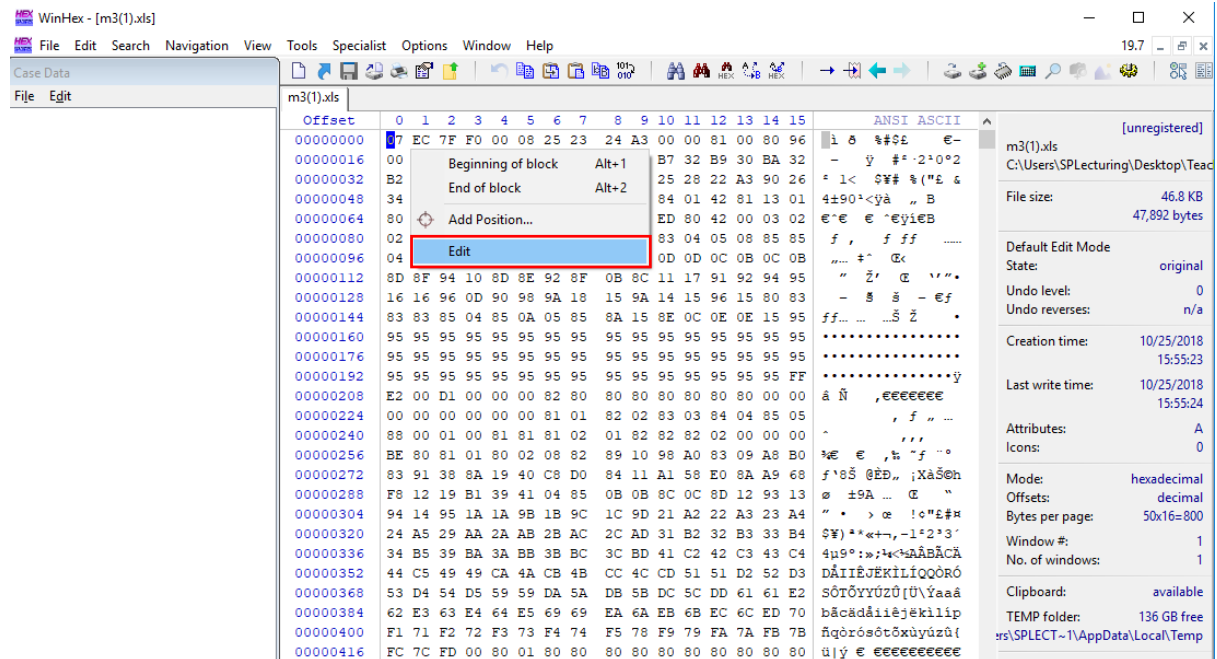
"Let's say I want to open a door using an electronic smart lock," said study co-lead author Merhdad Hessar, an electrical engineering doctoral student at the University of

PAGE 1 OF 2 537 WORDS ENGLISH (SINGAPORE) 100%

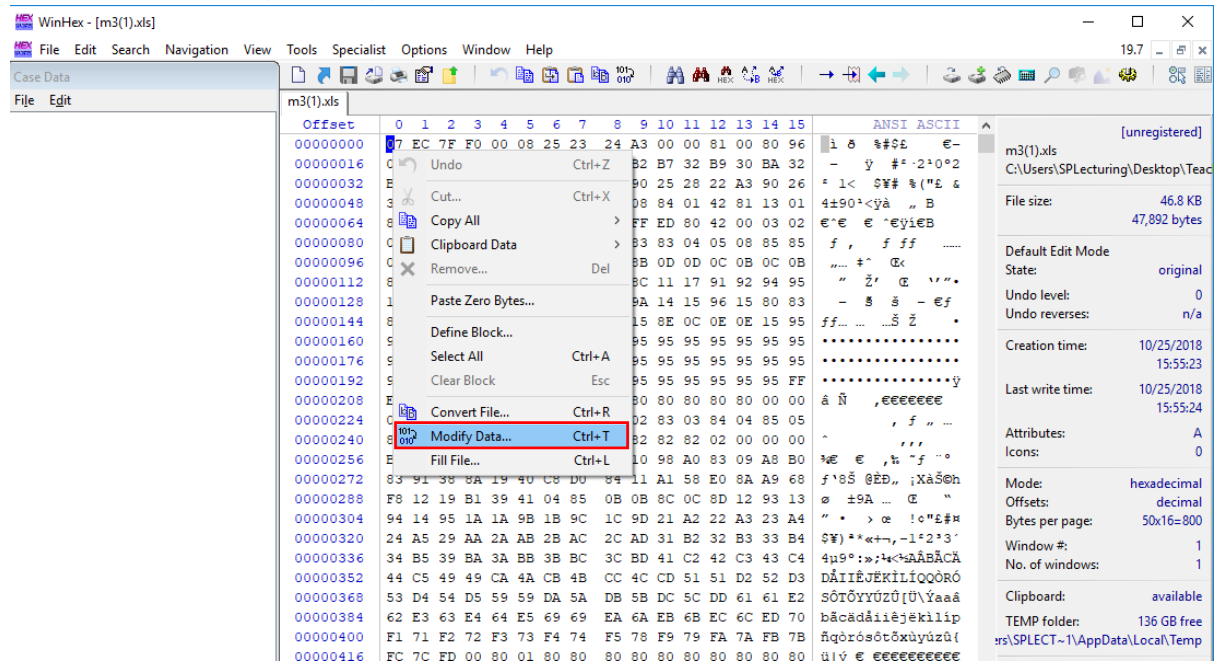
IT2514



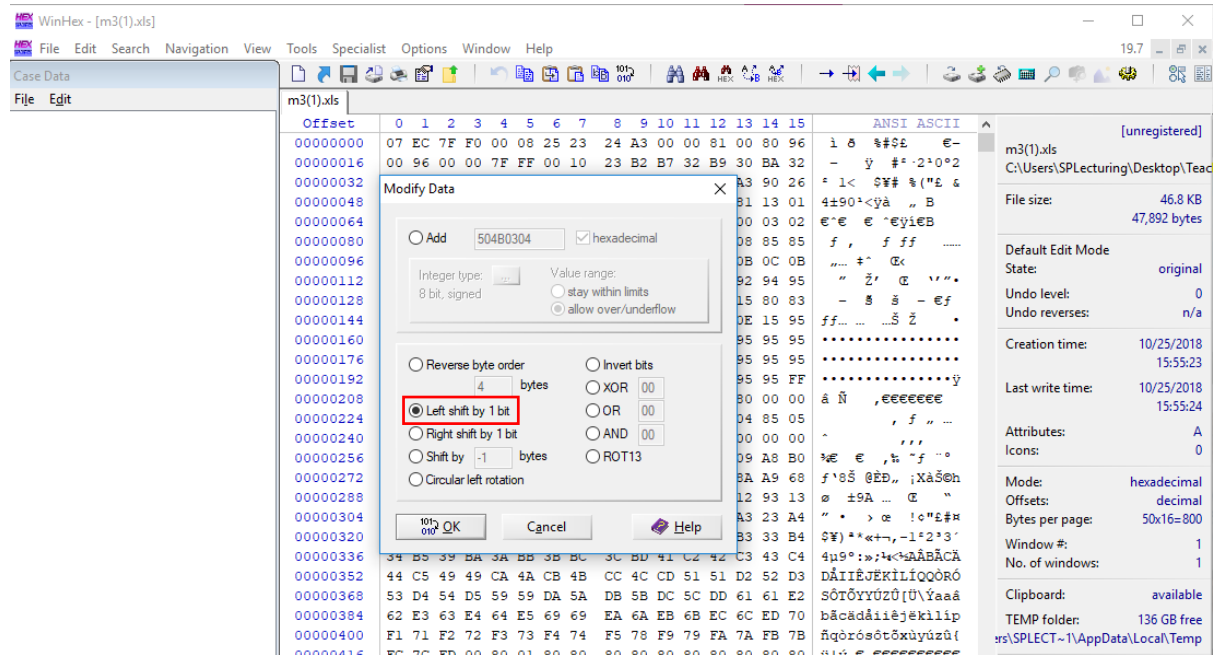
### 1.3.2 Right click on the Hexadecimal data and select “Edit” option.



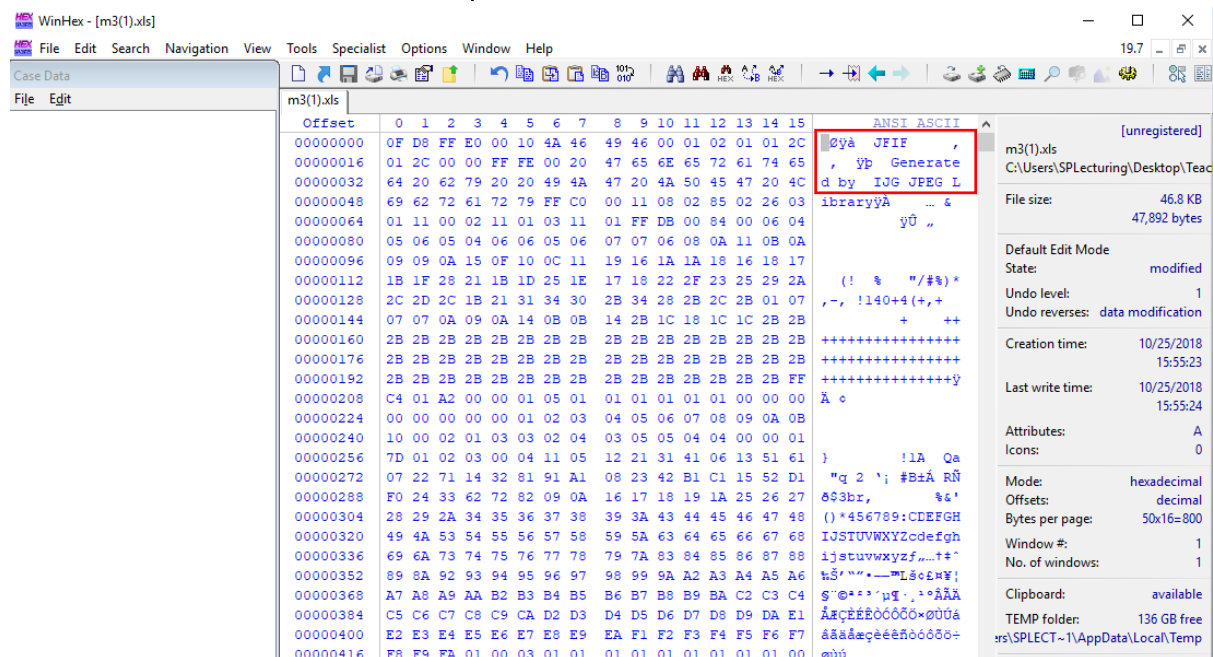
### 1.3.3 Select “Modify Data” option.



### 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"

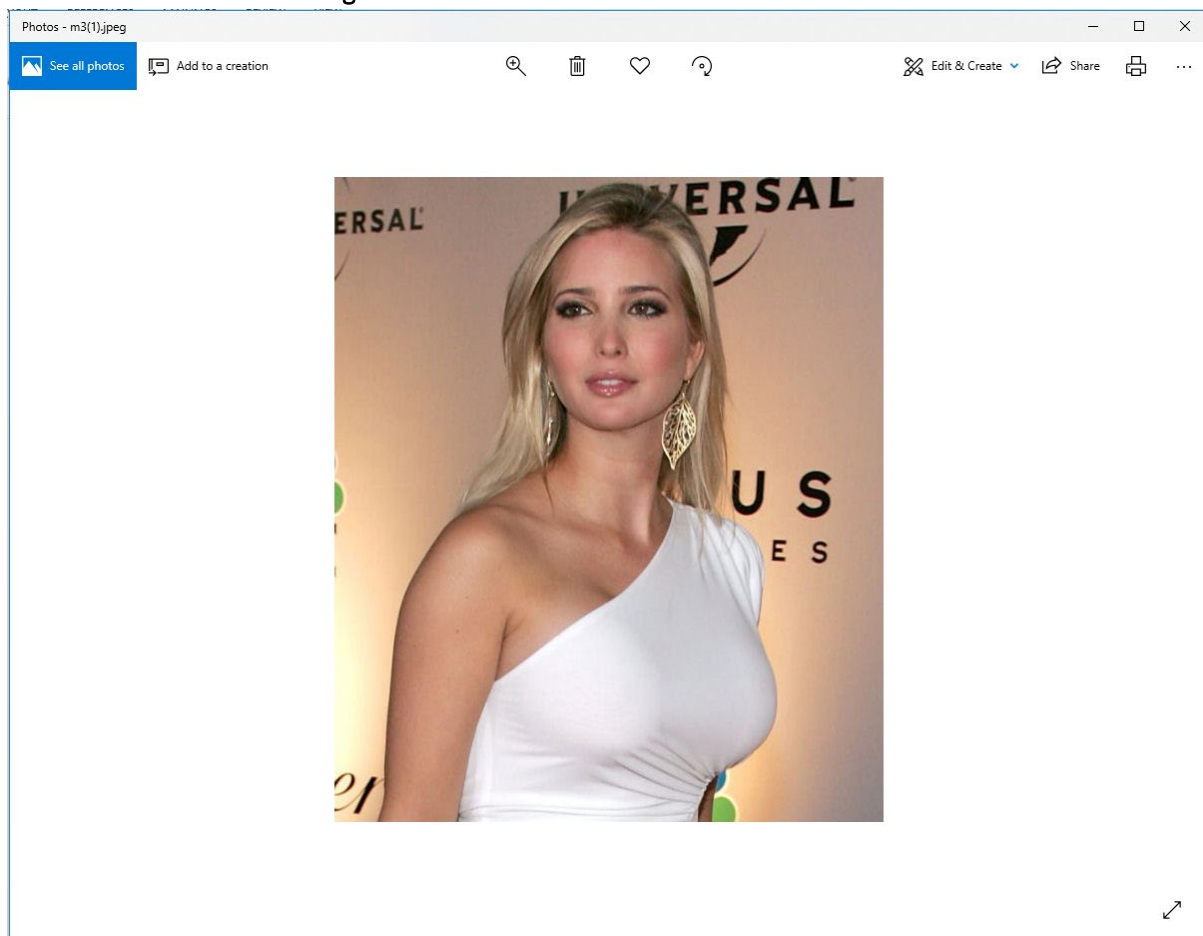
m3(1).jpeg																		
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	0F	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	01	2C	ÿà	JFIF ,
00000016	01	2C	00	00	FF	FE	00	20	47	65	6E	65	72	61	74	65	, ÿþ	Generate
00000032	64	20	62	79	20	20	49	4A	47	20	4A	50	45	47	20	4C	d by	IJG JPEG L
00000048	69	62	72	61	72	79	FF	C0	00	11	08	02	85	02	26	03	ibraryÿÀ	... &

Original Hexadecimal value

m3(1).jpeg																	ANSI ASCII	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
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	libraryÿÀ	... &

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.

WinHex - [test1-carve.doc]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

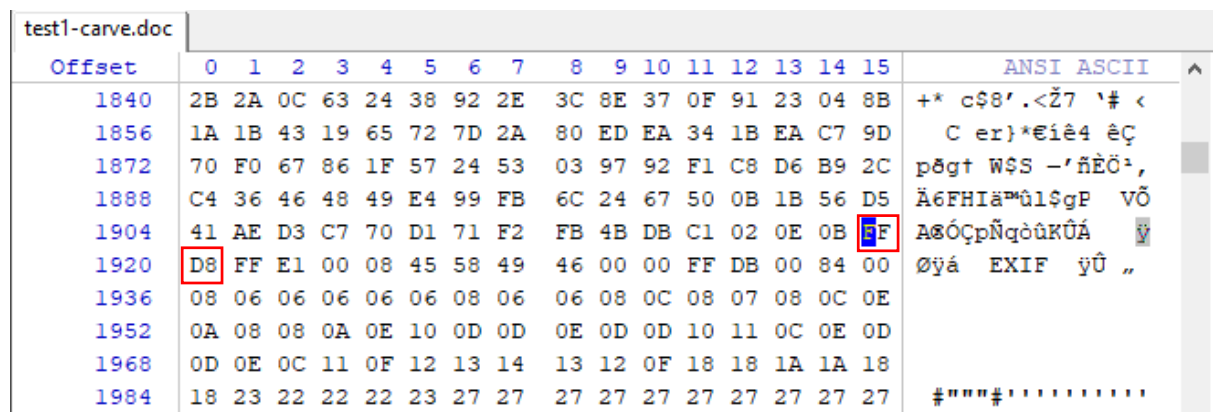
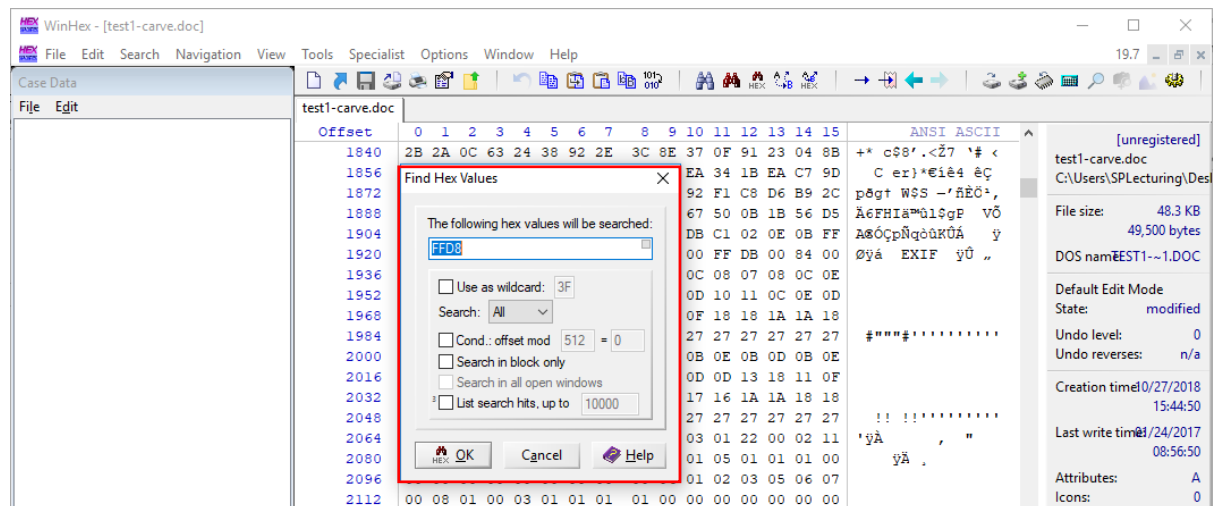
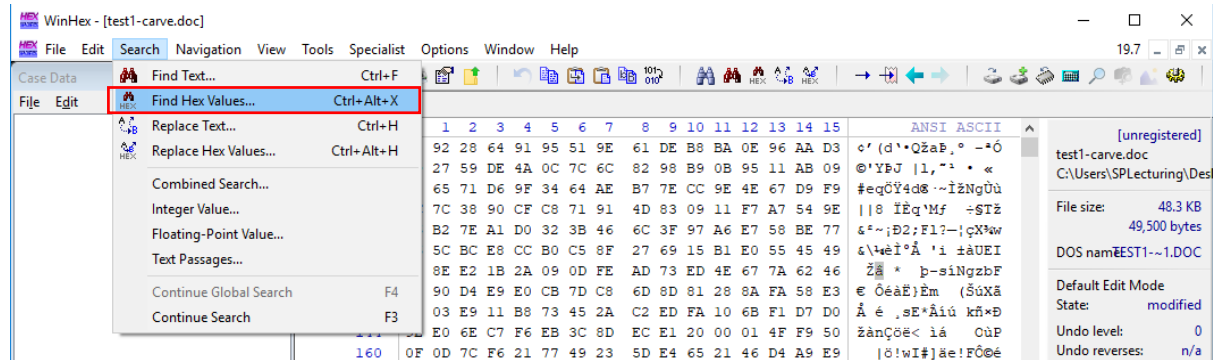
File Edit

test1-carve.doc

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0	A2	92	28	64	91	95	51	9E	61	DE	B8	BA	0E	96	AA	D3	c' (d' Qzaf, o -o
16	A9	27	59	DE	4A	0C	7C	6C	82	98	B9	0B	95	11	AB	09	@'YBj 1, " " «
32	23	65	71	D6	9F	34	64	AE	B7	7E	CC	9E	4E	67	D9	F9	#eq0Y4d8 ~i2NgUù
48	7C	7C	38	90	CF	C8	71	91	4D	83	09	11	F7	A7	54	9E	8 IÈq'Mf ÷STž
64	26	B2	7E	A1	D0	32	38	46	6C	3F	97	A6	E7	58	BE	77	¿~;D2:F1?~ çXw
80	26	5C	BC	E8	CC	B0	C5	8F	27	69	15	B1	E0	55	45	49	¿\wèI°Á 'i ±àUEI
96	02	8E	2	1B	2A	09	0D	FE	AD	73	ED	4E	67	7A	62	46	ž * p-siNgzbF
112	80	90	D4	E9	E0	CB	7D	C8	6D	8D	81	28	8A	FA	58	E3	€ ÓéáE)Èm (ŠúXā
128	C5	03	E9	11	B8	73	45	2A	C2	ED	FA	10	6B	F1	D7	D0	Ā é ,sE*Āiū kh×D
144	9E	E0	6E	C7	F6	EB	3C	8D	EC	E1	20	00	01	4F	F9	50	žānÇöè< iā OūP
160	0F	0D	7C	F6	21	77	49	23	5D	E4	65	21	46	D4	A9	E9	ō!wI#jāe!FÖé
176	F6	6B	E8	3F	7B	57	1F	D8	1C	AA	38	A3	27	1F	8B	09	öke?{W ö *8E' <
192	1F	E2	2D	8F	19	1F	8E	BA	45	D7	29	50	F0	90	BC	3E	ā- ž°E×)P8 i<
208	DC	E1	15	23	BD	BB	08	C7	C4	12	14	7A	BC	2A	05	75	Ūā #» ČĀ z4* u
224	63	24	2B	20	2B	32	06	DC	15	60	36	23	62	18	01	E1	c\$+ +2 Ū °6#b ā
240	5D	45	C4	28	FE	85	C1	A0	00	AA	61	40	0B	32	1A	16	]EĀ(p..Ā *a@ 2
256	B1	6A	D5	EA	2B	75	2B	E7	A9	E5	86	8E	8E	C1	55	07	±jÖè+u+çöā+žžĀU
272	E6	40	2F	3B	7A	EF	61	4A	86	1A	F3	DA	A7	17	35	EA	æ@;/ziāJ† óŮš 5ē
288	BA	45	87	25	1F	6C	2C	AA	63	4B	55	AB	DE	23	70	DF	°E+% 1,*cRūeP#pB
304	6A	F8	9D	19	6C	75	ED	F6	7D	36	FF	00	97	B5	69	5A	jō luio)6Y -μiZ
320	75	AD	29	E1	A1	D0	5B	42	40	56	23	F5	29	B5	01	E8	u-)ā;D(B@V#8)μ ē
336	3C	7A	6A	6F	55	7B	77	8A	56	9D	37	AD	69	D6	BF	C3	<zjōU{wšV 7-iŌzĀ
352	55	F5	76	49	7C	F3	26	52	B6	2D	8A	A6	42	4B	D9	41	UšvI ō&Rq-š;BRŪA
368	5D	D1	DA	9F	F9	75	6D	92	0B	65	4C	69	40	5D	9B	F1	]NŪYūm' eLi@] >ñ
384	35	D6	E3	DC	1F	D9	2E	24	7B	4E	43	8D	91	91	2F	3D	ŠŌāŮ Ů.š{NC ')/=
400	C7	E2	C9	3A	4C	1F	F4	67	99	07	75	E2	10	30	F4	2B	ČāĒ:L ōg™ uā Ō6+
416	80	55	68	C0	F4	2D	5D	F5	CD	7D	BB	96	D9	FC	5C	6D	€UhĀō-jŌí)»-Ůū\m
432	23	97	9F	15	8C	12	96	DC	D8	05	D0	B1	FF	00	86	AB	#-Y Ą -ŮŮ D±y †«
448	44	42	4C	4B	00	00	10	00	FF	00	0E	B4	DD	DA	D3	17	DBLK ŷ °YŮŮ
464	19	D7	AA	F7	3F	B7	FF	00	71	FC	DB	D2	DB	97	EC	1A	*±÷? ŷ quŮŮŮ-i
480	4E	7A	2E	AC	4A	EF	50	2B	E5	A5	B4	9D	4A	15	48	05	Nz..JiP+ĀY' J H
496	48	62	C2	E0	41	04	10	7A	53	4E	0B	E7	B9	AE	E3	58	HbĀĀā zSN ç'šĀX
512	32	F6	44	81	43	15	DC	57	E3	BE	AB	F2	90	1C	5E	59	žŌD C ŪWāš«Ō ^Y
528	7A	32	B7	AB	EC	31	C4	53	F7	6A	E4	A5	69	F1	35	A0	z2 «llĀS÷jāYiñ5
544	D5	6E	44	40	CF	9F	11	04	F7	9F	00	1A	57	A1	21	4D	ŌnD@iY ÷Y W;!M
560	7F	EE	D3	57	B7	F7	72	6F	F7	05	CB	EE	CF	FC	6D	FB	iŌW ÷ro÷ ÈiŮmū
576	B5	C7	FF	00	4E	E1	F3	09	25	86	84	D0	1D	A8	2B	E5	μÇY Náo †,D °+ā
592	4D	B5	01	84	EE	48	A9	EB	AB	69	61	B9	99	BC	B6	D3	Mu „iHŌè«ia™kŌ
608	51	18	47	80	F0	F8	EA	56	D2	88	24	B2	A3	92	36	24	Q ĞŌšŌVŮ°š'ē'6š
624	82	29	BF	86	A2	92	3D	A8	DE	3A	B8	6C	6A	B7	4F	C2	,)ž†c°="B:,lj ŌĀ
640	BA	8A	5C	62	3A	8E	BF	89	D5	C6	4B	8F	73	64	B1	2B	°š\b:žžhŌĒK sdi+
656	3F	34	43	BC	69	B5	51	41	1F	0A	B6	98	CA	D1	90	E8	?4C+μQA q"ĒN ē
672	4A	3A	9B	95	97	62	08	3B	15	23	C4	1D	58	64	42	56	J:»-b ; #Ā XdBV
688	55	3F	CC	95	00	6F	B0	24	6A	19	50	01	4A	6F	E4	37	U?i• °°šj P Joā7
704	3A	D9	EC	BC	B9	6D	87	9F	32	AB	6F	78	24	49	61	25	:Ůi4+m+Y2«oxšIa%
720	26	89	C4	91	BD	77	0E	86	E5	6F	0A	74	D6	FD	39	2C	šhĀ'w †āc tŌY9,
736	61	8C	99	D8	97	A2	4F	17	73	D3	46	60	58	01	73	29	aŌ™Ō-ŌO šŌF'X s)
752	36	96	8D	B6	3A	C0	E4	AB	AE	F5	11	8F	32	2A	DF	B3	6- q:Āā«Ōš 2*β)
768	A6	AD	38	4C	E5	8B	11	56	56	24	23	BC	68	D4	A0	55	;-8Lā< VVš#4hŌ U
784	DA	4A	11	F1	66	3A	9D	D8	6A	02	59	2E	49	96	93	28	ŮŮ Ĥf: Ōj Y.I-“(

Page 1 of 62 Offset: 98 = 226 Block: n/a Size: n/a

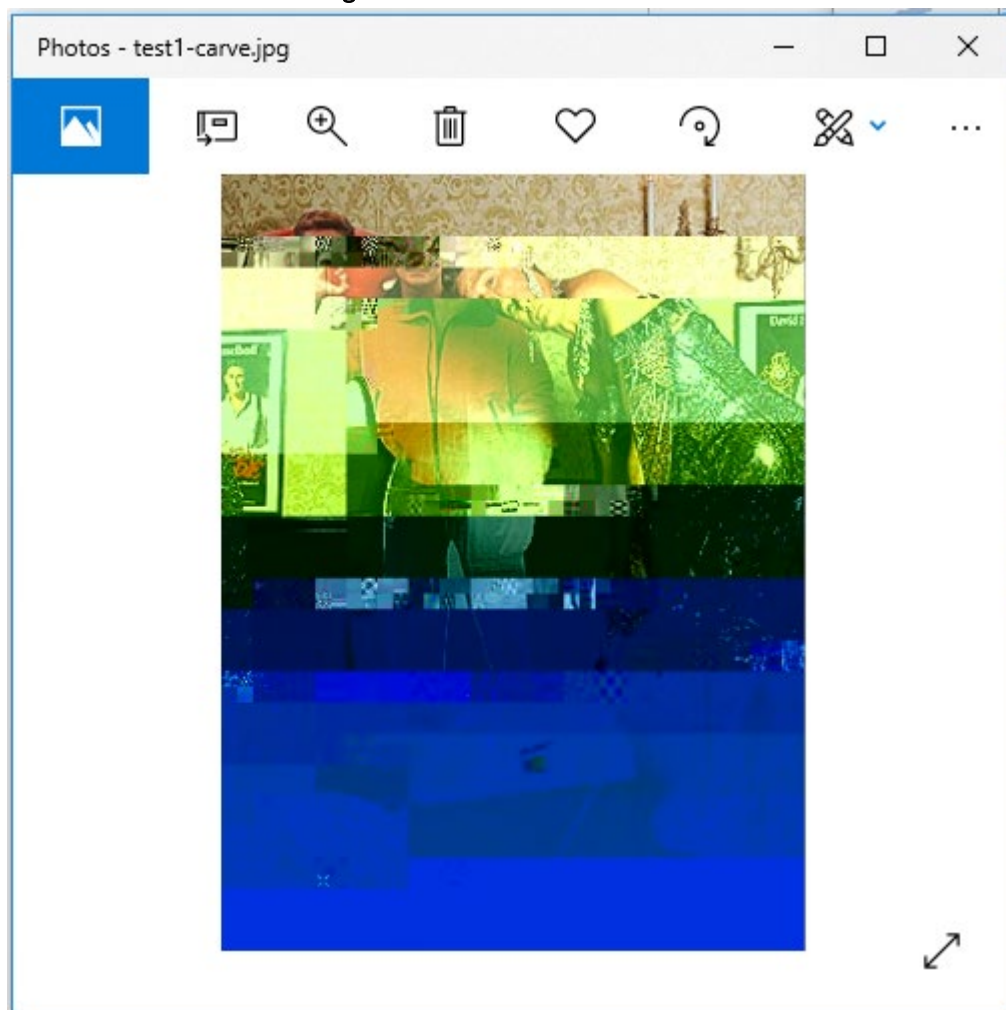
### 1.4.2 Perform a search for the Hexadecimal value of "FF D8".



- 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																	ANSI	ASCII	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15			
0	FF	D8	FF	E1	00	08	45	58	49	46	00	00	FF	DB	00	84	yøÿá	EXIF	yÛ „
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	'yÀ	,	"
144	27	27	FF	C0	00	11	08	01	90	01	2C	03	01	22	00	02	yÄ	.	
160	11	01	03	11	01	FF	C4	00	B8	00	00	01	05	01	01	01			
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			

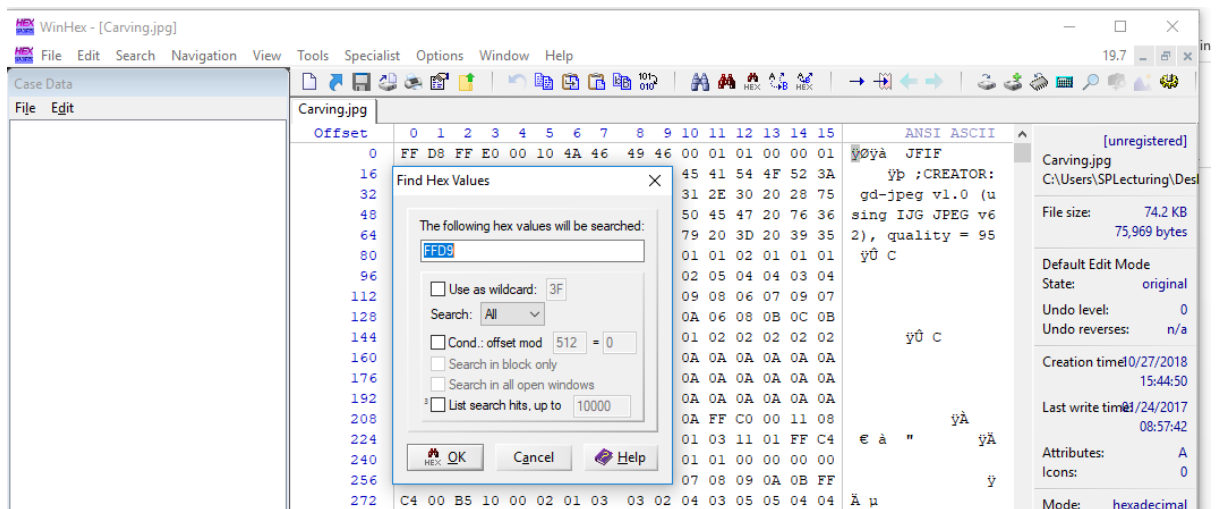
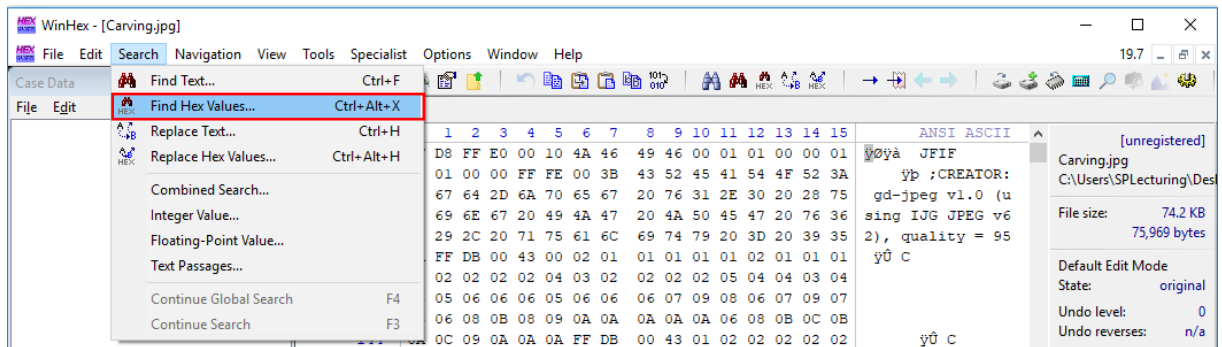
- 1.4.4 Save the changes in WinHex, change the extension of the file from “.doc” to “.jpg” and you will be able view the image.



IT2514



### 1.5.2 Perform a search for the Hexadecimal value of "FF D9".



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
75472	0F	4F	AD	62	FE	CE	9E	0F	4F	08	7C	1B	D0	AD	AD	6C	O-bpfz O   Ð--l
75488	0C	1F	69	B3	49	E6	08	B8	CB	30	07	3C	7B	54	B7	3A	i' Ia ,E0 <{T :
75504	CD	A6	9D	77	AE	78	EB	5A	BE	4B	51	63	7A	20	5B	C9	í; w0xZ3KQcz [É
75520	41	2B	04	2A	14	B6	54	7A	E4	FE	75	85	0C	3C	F0	DC	A+ * qTzäpu... <8Ü
75536	3B	4E	93	97	2D	D6	AF	AA	5F	13	EF	B4	6C	92	3D	4A	;N"--Ö' a _ i' l' =J
75552	FC	F3	84	BD	AC	9C	5B	D5	B5	BF	76	EE	6E	78	6E	5F	üó„%æ[Öu2vinxn_
75568	1D	5E	78	51	25	F8	A1	E2	79	35	3D	7A	EA	06	93	52	^xQ%0;ây5=zè "R
75584	BA	63	BB	74	8D	93	81	F4	AC	2F	85	D7	AC	7E	1F	D9	°c>t " ö-/...x~ Ü
75600	59	EF	56	11	79	B0	8D	C3	9F	92	52	B8	3F	95	75	3A	YiV y° ÄY'R,?·u:
75616	07	8D	BC	29	E2	0B	5F	ED	6F	0F	6A	90	5E	59	C9	80	4) ä _io j ^YEE
75632	B7	30	2E	54	FB	D6	07	C3	79	B4	66	F0	ED	DD	8C	C1	-O.TüÖ Äy'föiYGA
75648	73	06	BD	75	1A	63	03	FE	5A	67	FA	D7	D0	61	9E	1D	s 'su c pZgú×Daž
75664	D2	A4	E8	CA	F1	6B	47	BD	D3	46	77	E7	94	25	19	5D	ÖmEñkG%ÓFwç"% ]
75680	59	EB	DF	6D	4B	EC	CB	29	22	50	02	F6	55	35	1C	AB	YëBmKiE)"P öU5 «
75696	6A	13	74	78	24	7A	9A	D3	B9	87	44	27	6A	C8	63	3F	j tx\$zšÖ'<D'jÈc?
75712	51	54	65	86	08	99	A1	B7	9B	2C	A7	18	65	AE	D4	6E	QTet " ; -> , \$ eöÖn
75728	D2	5B	9F	5F	D9	50	4B	03	04	14	00	02	00	08	00	8F	Ö(YÖPK
75744	69	0C	3F	55	09	9F	44	42	00	00	00	43	00	00	00	0A	i ?U YDB C
75760	00	1C	00	61	6E	73	77	65	72	2E	74	78	74	55	54	09	answer.txtUT
75776	00	03	0E	6D	45	4E	0C	6D	45	4E	75	78	0B	00	01	04	mEN mENux
75792	88	13	00	00	04	88	13	00	00	0D	C8	BB	0D	C0	20	0C	- È» À
75808	05	C0	9E	29	9E	18	80	25	B2	42	16	70	E1	80	25	64	Äž)ž €%<B páE&d
75824	23	7F	94	F5	93	2B	EF	32	9D	4E	59	9B	52	4C	63	00	# "ö"+i2 NY>RLc
75840	F7	62	90	C6	CB	8E	C7	1C	B9	24	90	95	E6	42	1B	87	-b EÈžÇ 'ç ·æB +
75856	26	E3	8F	9E	E5	2A	27	FA	68	ED	03	50	4B	01	02	1E	šä žä*'úhi PK
75872	03	14	00	02	00	08	00	8F	69	0C	3F	55	09	9F	44	42	i ?U YDB
75888	00	00	00	43	00	00	00	0A	00	18	00	00	00	00	00	01	C
75904	00	00	00	A4	81	00	00	00	00	61	6E	73	77	65	72	2E	m answer.
75920	74	78	74	55	54	05	00	03	0E	6D	45	4E	75	78	0B	00	txtUT mENux
75936	01	04	88	13	00	00	04	88	13	00	00	50	4B	05	06	00	- ^ ^ PK
75952	00	00	00	01	00	01	00	50	00	00	00	86	00	00	00	00	P +
75968	00																



### 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”.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
0	50	4B	03	04	14	00	02	00	08	00	8F	69	0C	3F	55	09	PK	i ?U
16	9F	44	42	00	00	00	43	00	00	00	0A	00	1C	00	61	6E	YDB	C an
32	73	77	65	72	2E	74	78	74	55	54	09	00	03	0E	6D	45	swer.txt	UT mE
48	4E	0C	6D	45	4E	75	78	0B	00	01	04	88	13	00	00	04	N mENux	^
64	88	13	00	00	0D	C8	BB	0D	C0	20	0C	05	C0	9E	29	9E	^	E» À Àž)ž
80	18	80	25	B2	42	16	70	E1	80	25	64	23	7F	94	F5	93	€%*B pã€%d# "õ"	
96	2B	EF	32	9D	4E	59	9B	52	4C	63	00	F7	62	90	C6	CB	+i2 NY>RLc ÷b EE	
112	8E	C7	1C	B9	24	90	95	E6	42	1B	87	26	E3	8F	9E	E5	žÇ 'š *æB +&ã žã	
128	2A	27	FA	68	ED	03	50	4B	01	02	1E	03	14	00	02	00	*'úhi PK	
144	08	00	8F	69	0C	3F	55	09	9F	44	42	00	00	00	43	00	i ?U YDB	C
160	00	00	0A	00	18	00	00	00	00	00	01	00	00	00	A4	81		¤
176	00	00	00	00	61	6E	73	77	65	72	2E	74	78	74	55	54	answer.txt	UT
192	05	00	03	0E	6D	45	4E	75	78	0B	00	01	04	88	13	00	mENux	^
208	00	04	88	13	00	00	50	4B	05	06	00	00	00	00	01	00	^	PK
224	01	00	50	00	00	00	86	00	00	00	00	00	00	00	00	00	P	†

[unregistered]

Carving.jpg  
C:\Users\SP\lecturing\Des

File size: 236 B  
236 bytes

Default Edit Mode  
State: modified

Undo level: 1  
Undo reverts: check removal

Creation time: 10/27/2018  
15:44:50

Last write time: 10/24/2017  
08:57:42

Attributes: A  
Icons: 0

Mode: hexadecimal  
Offsets: decimal  
Bytes per page: 60x16=800

Window #: 1  
No. of windows: 1

Clipboard: available  
TEMP folder: 136 GB free  
f~1\AppData\Local\Temp

### 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](https://www.garykessler.net/library/file_sigs.html)) we suspect it can be a zip file.

50 49 43 54 00 08 PICT...  
IMG ADEX Corp. ChromaGraph

50 4B 03 04 PK...  
ZIP PKZIP archive file (Ref. 1 | Ref. 2)

**Trailer:** filename 50 4B 17 characters 00 00 00  
**Trailer:** (filename PK 17 characters ...)

**Note:** PK are the initials of Phil Katz, co-creator of the ZIP file format and author of PKZIP.

ZIP Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forums theme, SubEthaEdit Mode, Trillian zipped skin, Virtual Skipper skin

JAR Java archive; compressed file package for classes and data

KMZ Google Earth saved working session file

KWD KWord document

ODT, ODP, OTT OpenDocument text document, presentation, and text document template, respectively.

OXPS Microsoft Open XML paper specification file

SXC, SXD, SXI, SXW OpenOffice spreadsheet (Calc), drawing (Draw), presentation (Impress), and word processing (Writer) files, respectively.

SXC StarOffice spreadsheet

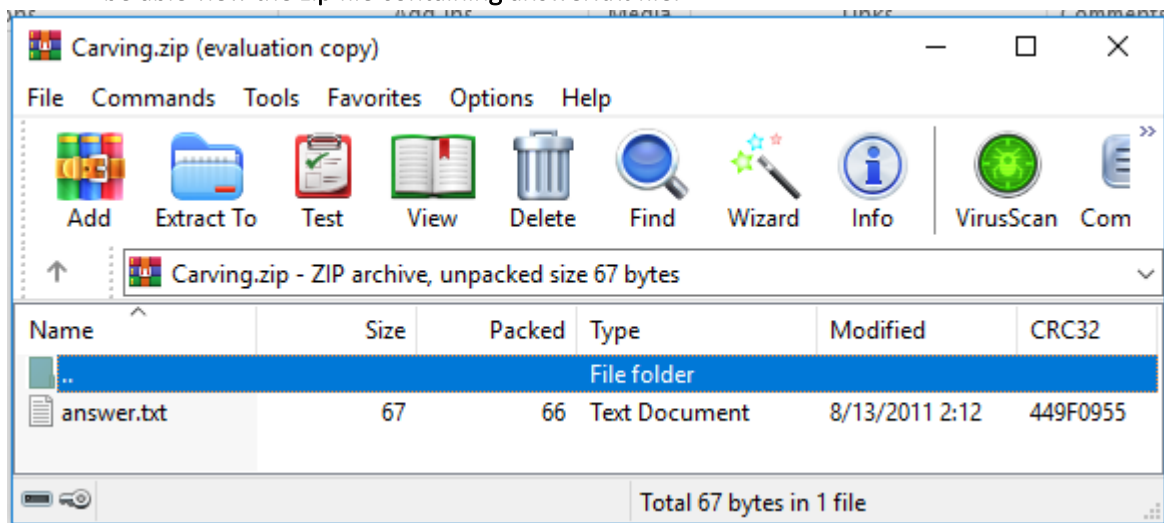
WMZ Windows Media compressed skin file

XPI Mozilla Browser Archive

XPS XML paper specification file

XPT eXact Packager Models

- 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”.”

