



Using a Hex Editor to Carve a
file

Outline

- What you need
- Context – What is Hex Workshop?
- Hex Workshop User Interface
- Carve .jpeg files from alienimage.dd
- Convert alienimage.dd to alienimage.E01 using FTK Imager and view in Hex Workshop
- View the filesystem structure in Hex Workshop

What you need

- A Windows machine
- Hex Workshop & Sample image files
 - Download Lab from Moodle.
 - Unzip the contents of the zipped file. You should have:
 - Hex Workshop setup file
 - AlienImage folder
 - alienimage.dd
 - alienimageMD5.txt
- Install Hex Workshop on your windows machine

Context

- What is Hex Workshop?
- The Hex Workshop Hex Editor by BreakPoint Software is a complete set of hexadecimal development tools for Microsoft Windows. Hex Workshop integrates advanced binary editing and data interpretation and visualization with the ease and flexibility of a modern word processor.
- With the Hex Workshop, you can edit, cut, copy, paste, insert, fill and delete binary data. You can also work with data in its native structure and data types using our integrated structure viewer and smart bookmarks.

- What is Hex Workshop?

- Data editing is quick and easy. Hex Workshop allows you to: jump to file or sector location, find or replace data, perform arithmetic, bitwise, and logical operations, binary compare files, generate checksums and digests, view character distributions and export data to RTF or HTML for publishing.
- <http://www.hexworkshop.com/overview.html>

Carve .jpeg files from
alienimage.dd



This is same image we used in
our FTK Imager Lab

Carving files with Hex Workshop

- File carving is a recovery technique that merely considers the contents and structures of files instead of file system structures or other meta-data which is used to organize data on storage media.
- File carving can be done automatically or manually. In this lab, we learn how to carve the files manually using Hex Workshop. This is a skillset a professional investigator should have

Download the folder from Moodle and run the application

Choose Typical Install

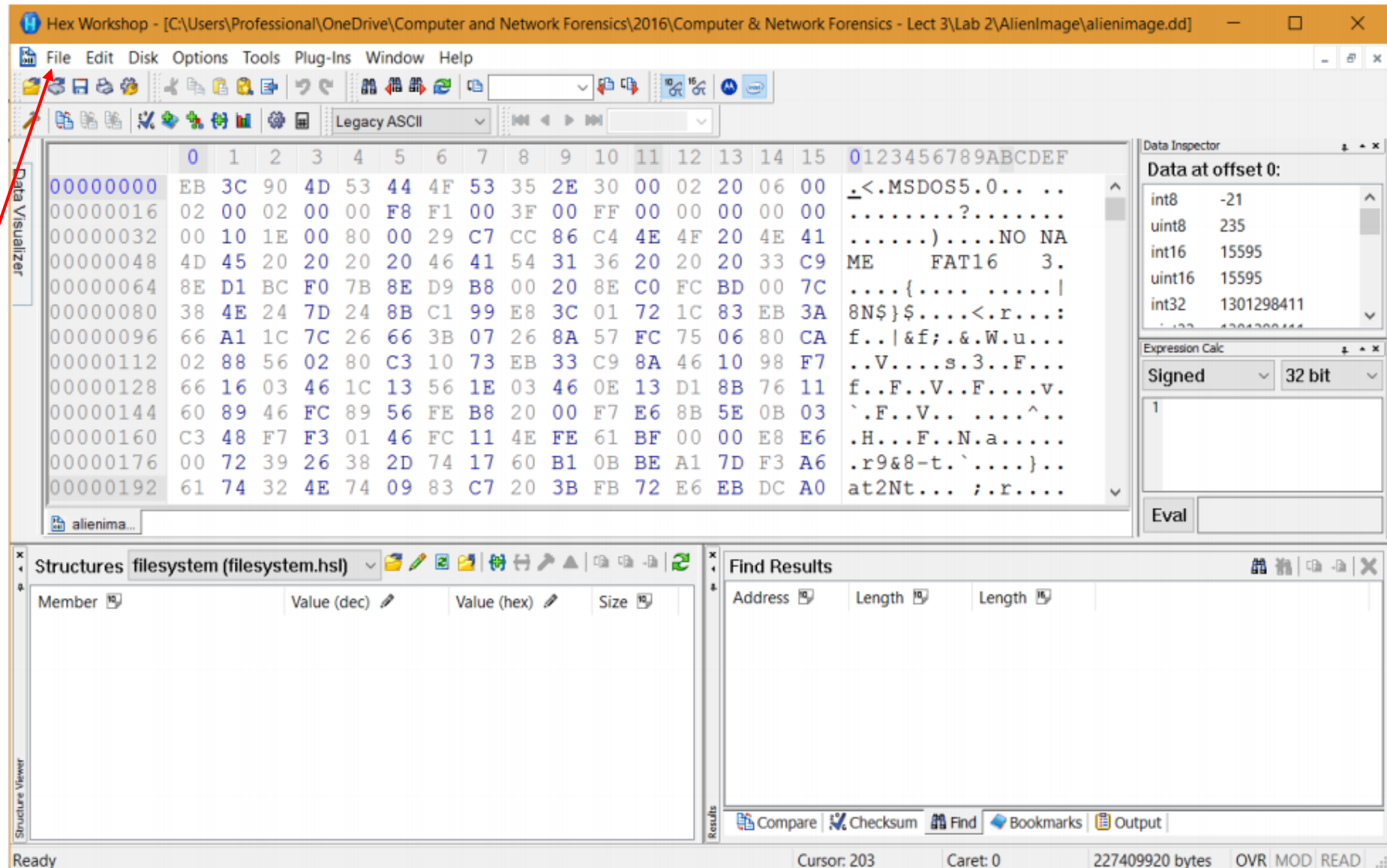
Name	Type	Compressed size	Passv
 AlienImage	File folder		
 hw_v680	Application	18,194 KB	No

Carve .jpeg files from alienimage.dd

1. Open Hex Workshop Editor on your windows machine.

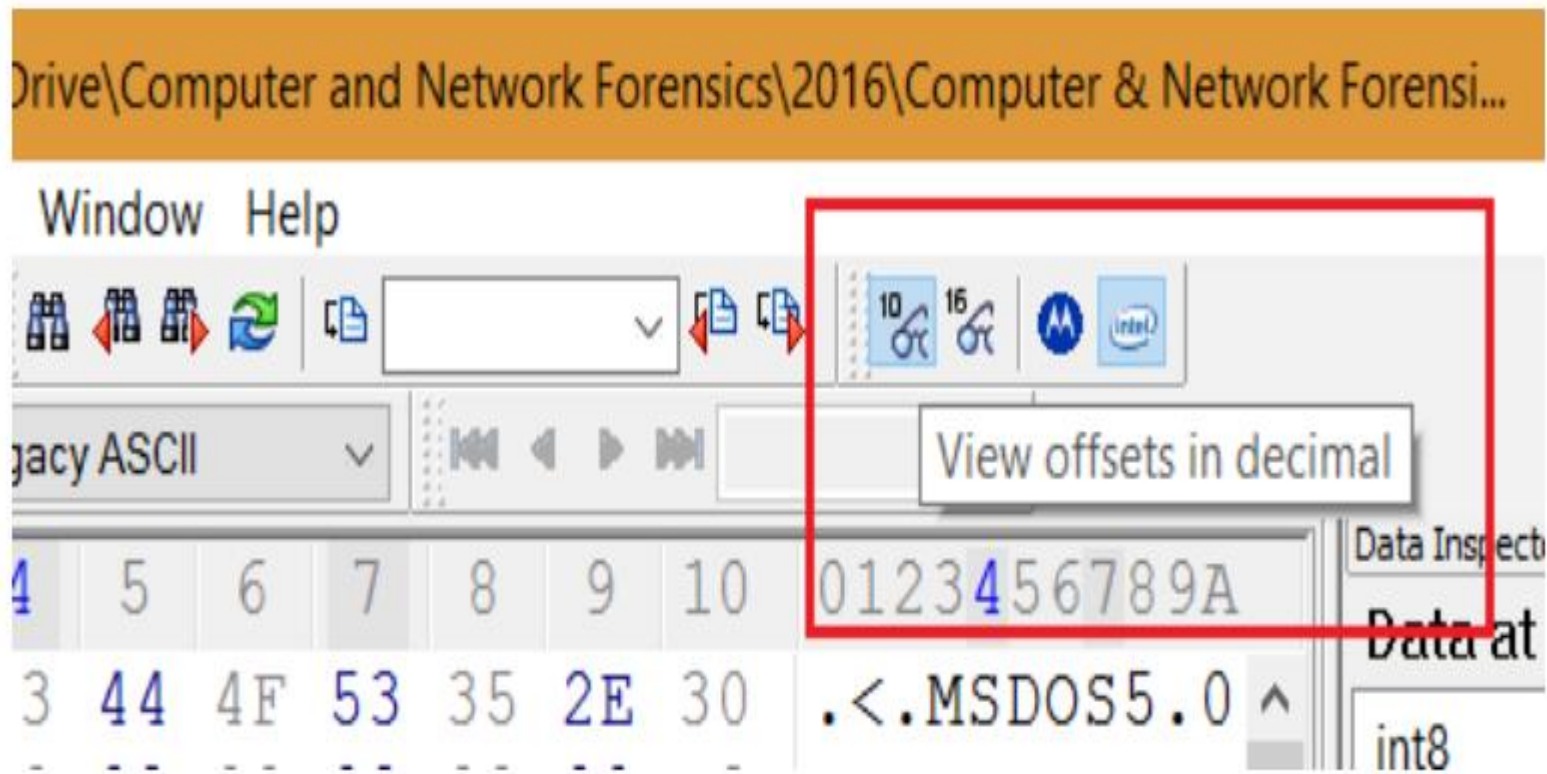
2. Open the alienimage.dd

- **File -> Open**
- Browse to path where you downloaded alienimage.dd
- Select **Open**



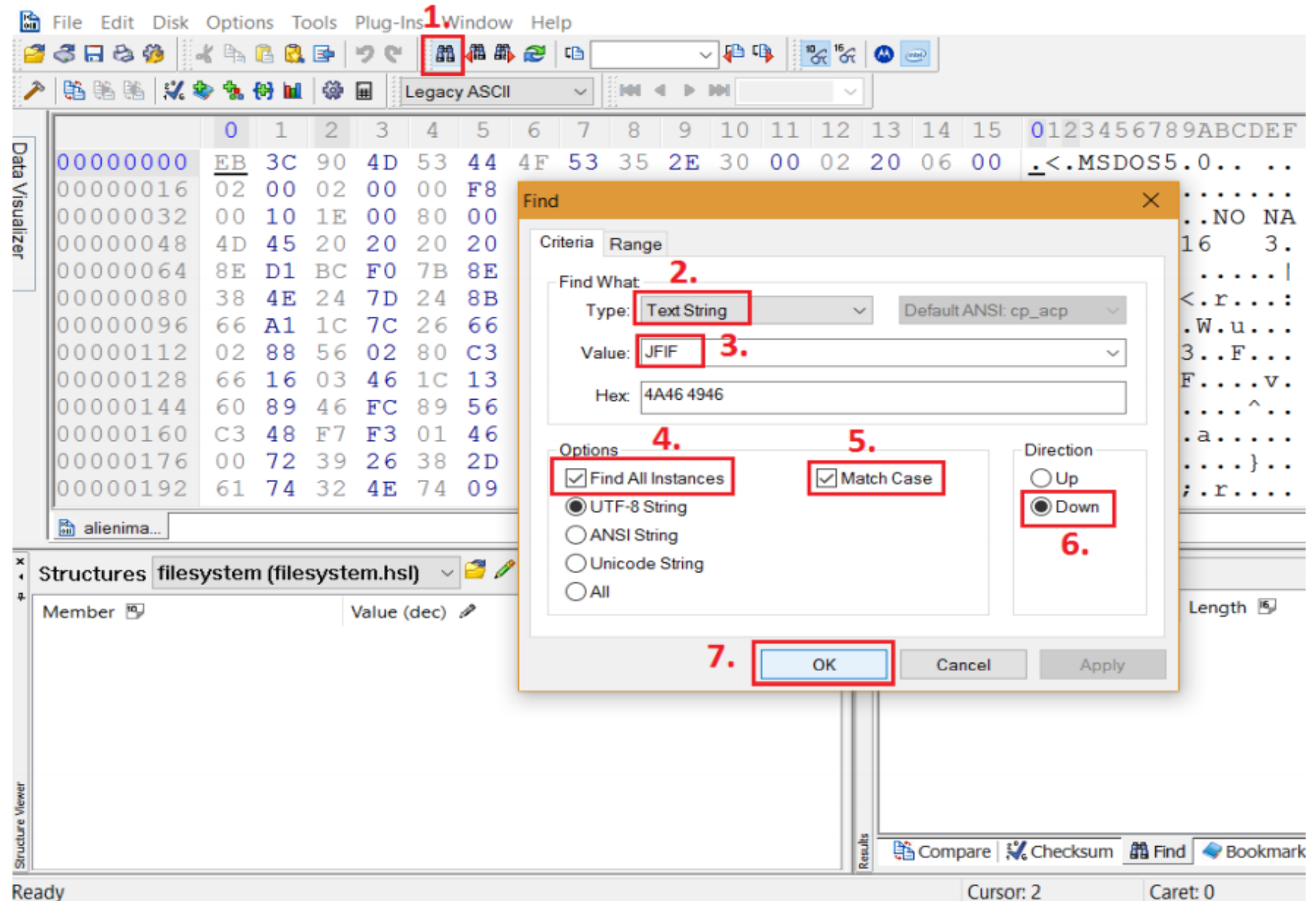
Carve .jpeg files from
alienimage.dd

Make sure
'View offsets in
Decimal' is
selected



Carve .jpeg files from alienimage.dd

1. Click on Find
2. Enter the type as 'Text String'
3. Enter the value as 'JFIF'
4. Make sure you check 'Find all Instances',
5. 'Match Case'
6. 'Down'.
7. Click 'OK'



Carve .jpeg files from alienimage.dd

8. You will see 4 instances of JFIF found.

Note the Hex Signature of the JFIF file is **FF D8 FF E0 xx xx 4A 46 49 46 00**

9. Next we need to find the end (or trail **FF D9**) of the first jpeg file

Hex Workshop - [C:\Users\Professional\OneDrive\Computer and Network Forensics\2016\Computer & Network Forensi...

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

0 1 2 3 4 5 6 7 8 9 10 0123456789A

00266222 00 00 00 00 00 00 00 00 00 00 00 00
00266233 00 00 00 00 00 00 00 00 FF D8 FF E0
00266244 00 10 4A 46 49 46 00 01 01 01 00 ..JFIF..
00266255 48 00 48 00 00 FF E1 01 22 45 78 H.H...."Ex
00266266 69 66 00 00 4D 4D 00 2A 00 00 00 if..MM.*...
00266277 08 00 07 01 12 00 03 00 00 00 01
00266288 00 01 00 00 01 1A 00 05 00 00 00
00266299 01 00 00 00 BC 01 1B 00 05 00 00
00266310 00 01 00 00 00 C4 01 28 00 03 00 (
00266321 00 00 01 00 02 00 00 01 31 00 021..
00266332 00 00 00 1C 00 00 00 CC 01 32 002..
00266343 02 00 00 00 14 00 00 00 E8 87 69i
00266354 00 04 00 00 00 01 00 00 00 62 00b..

Data Inspector

Data at offset 266342:

int8 0
uint8 0
int16 512
uint16 512
int32 512

Expression Calc

Signed 32 bit

1

Eval

Structures filesystem

Member Value (dec) Value (hex) Size

4 instances of 'JFIF' found in C:\Users\Professional\OneDrive

Address	Length	Length
00266246	4	04
00643078	4	04
01003526	4	04
01331206	4	04

Results

Compare Checksum Find Bookmarks Output

Finding all instances... Cursor: 266318 Caret: 266342 227409920 bytes OVR MOD READ

Carve .jpeg files from alienimage.dd

1. Note the data offset of the starting position of the .jpeg file for future reference.

2. Click on Find

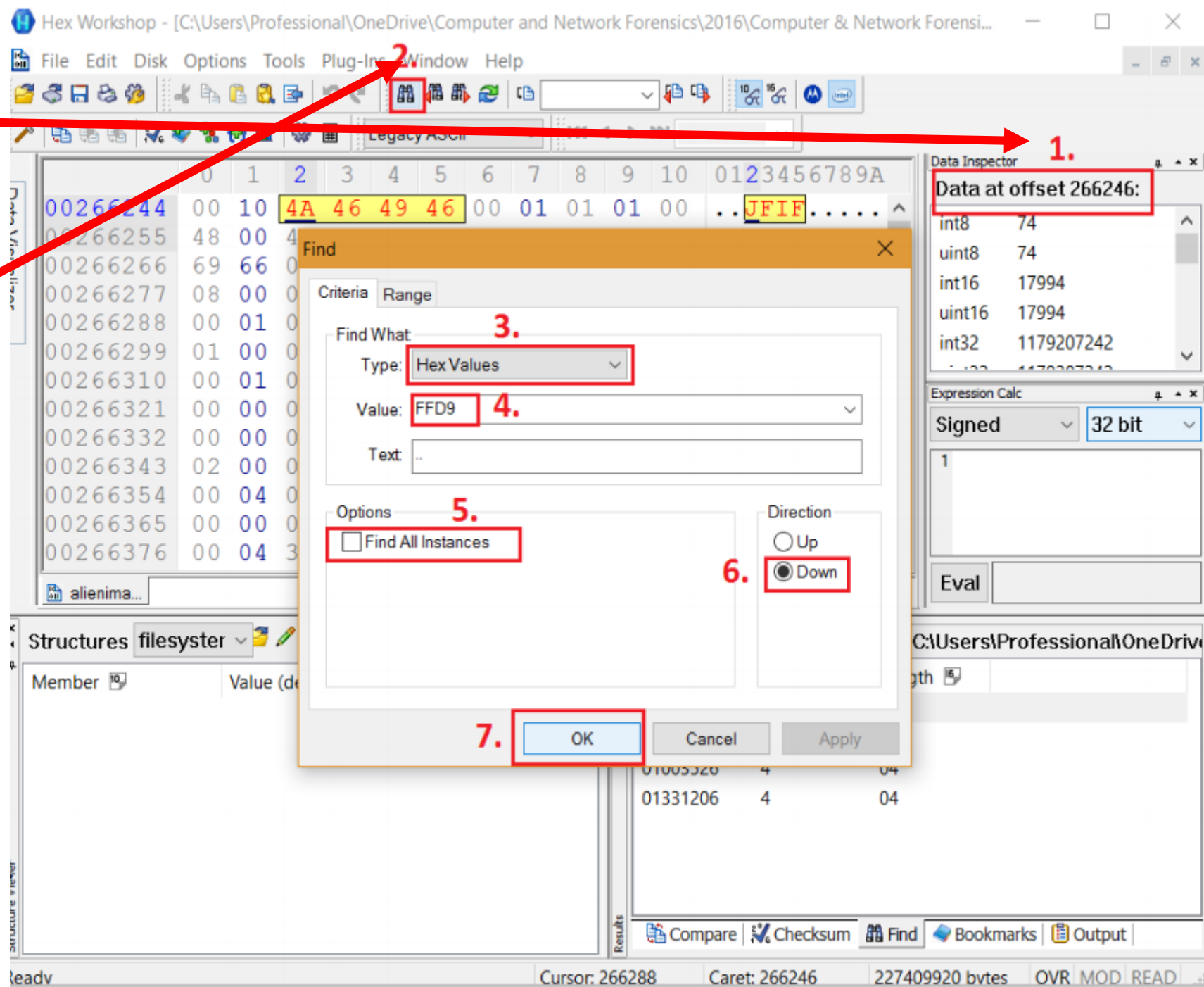
3. Enter the type as 'Hex Values'

4. Enter the value as 'FFD9'

5. Make sure you uncheck 'Find all Instances' and select

6. 'Down'.

7. Click 'OK'



Carve .jpeg files from alienimage.dd

Note the offset
of the end of the
.jpeg file.
Highlighted in
Red

Your search for
JFIF is still shown in
the right hand
corner find
window.

Hex Workshop - [C:\Users\Professional\OneDrive\Computer and Network Forensics\2016\Computer & Network Forensi...

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

	0	1	2	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8	9	A
00630432	FF	D9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630443	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630454	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630465	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630476	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630487	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630498	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630509	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630531	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630542	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630553	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00630564	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

alienima...

Data Inspector

Data at offset 630432:

int8	-1
uint8	255
int16	-9729
uint16	55807
int32	

Expression Calc

Signed 32 bit

1

Eval

Structures filesystem

Member	Value (dec)	Value (hex)	Size
--------	-------------	-------------	------

4 instances of 'JFIF' found in C:\Users\Professional\OneDrive

Address	Length	Length
00266246	4	04
00643078	4	04
01003526	4	04
01331206	4	04

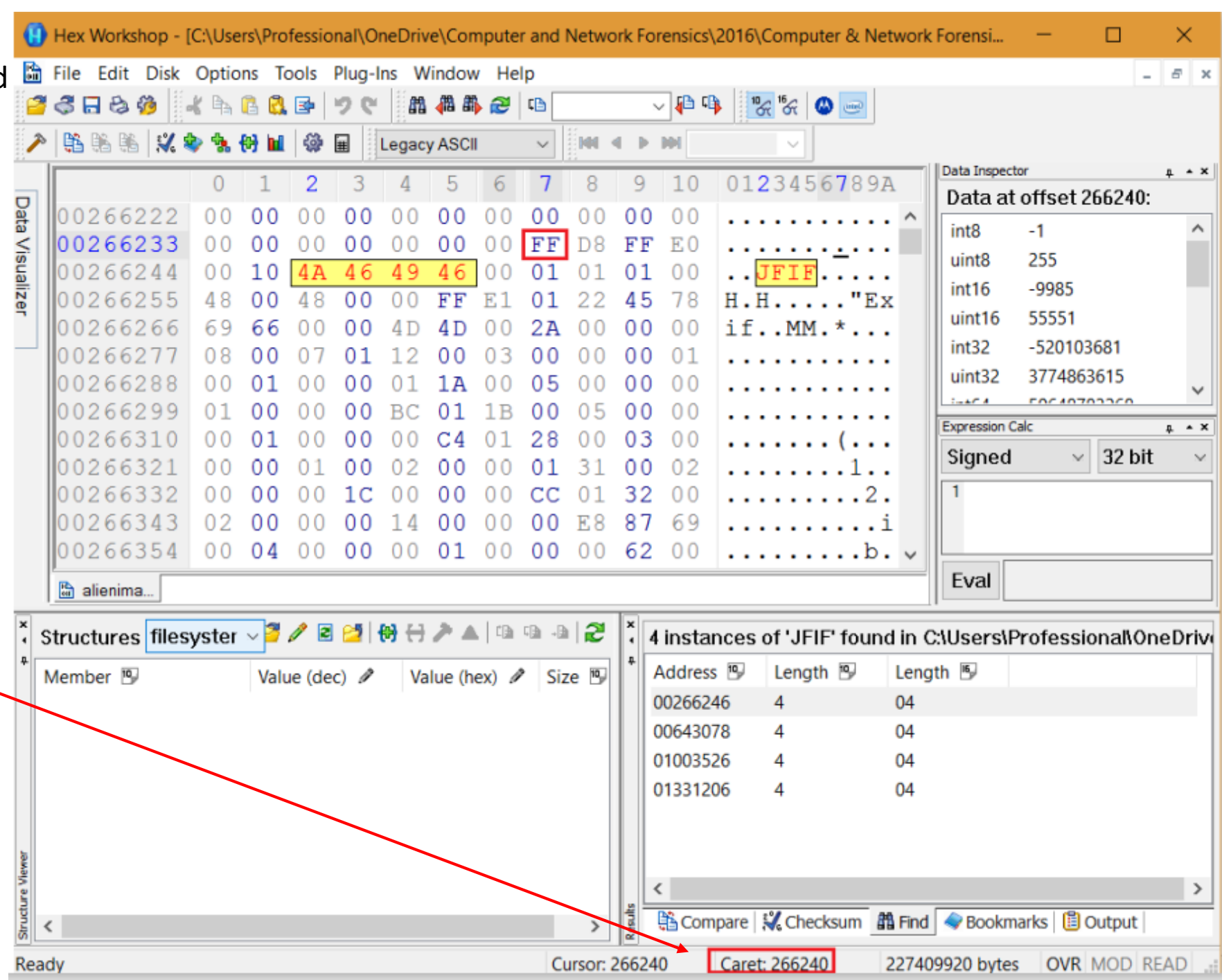
Compare Checksum Find Bookmarks Output

Found at position 0x00099EA0 (630432). Cursor: 266288 Caret: 630432 Sel: 2 OVR MOD READ

Place your
cursor at the
beginning of the
file hex signature

FF D8 FF E0 xx xx
4A 46 49 46 00

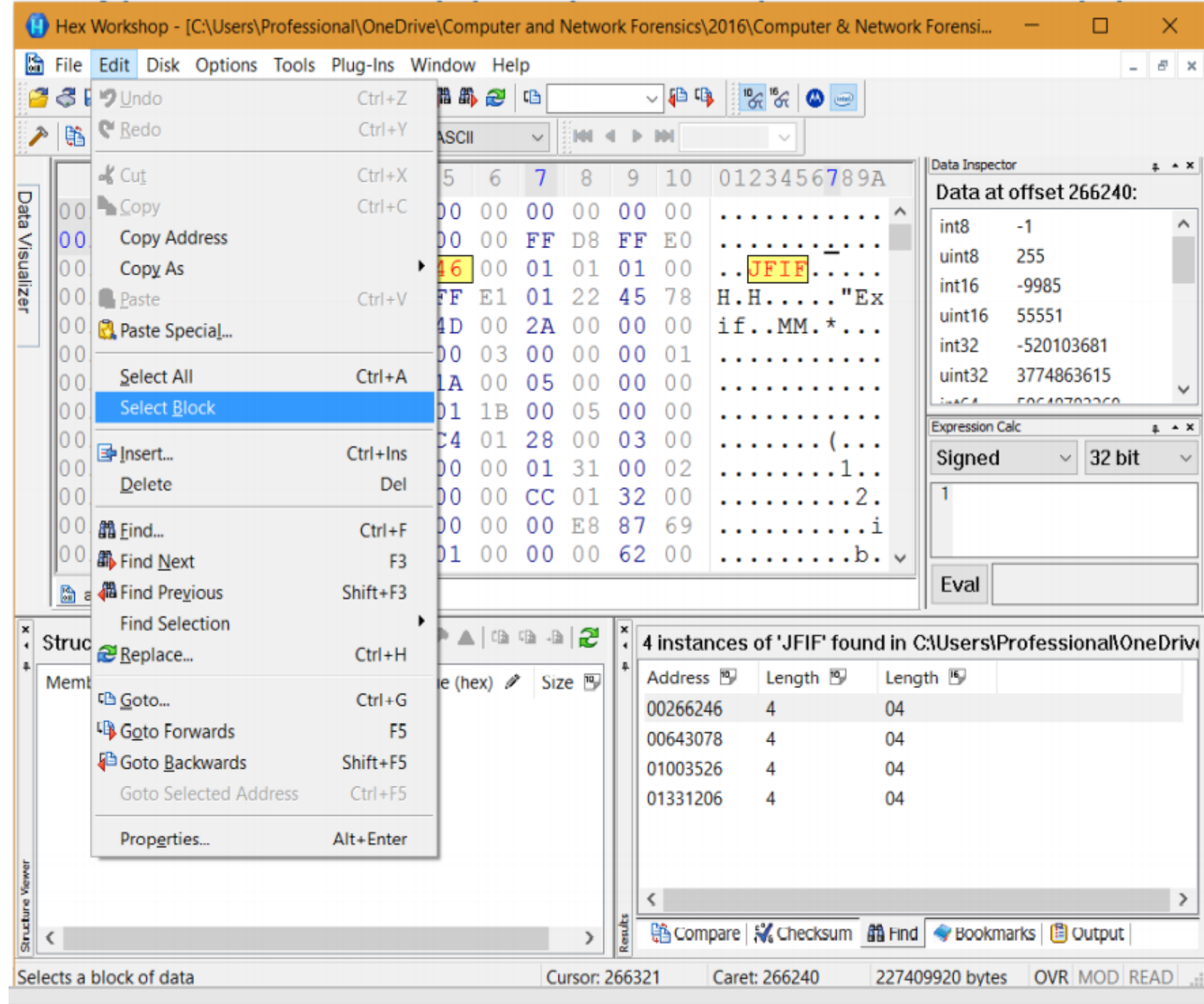
IMPORTANT: Make sure the Caret value is same as the one shown at the bottom of the screenshot here.



Carve .jpeg files from alienimage.dd

Double click on
the first search
item to go back to
the starting of the
file.

Click on **Edit** ->
Select Block

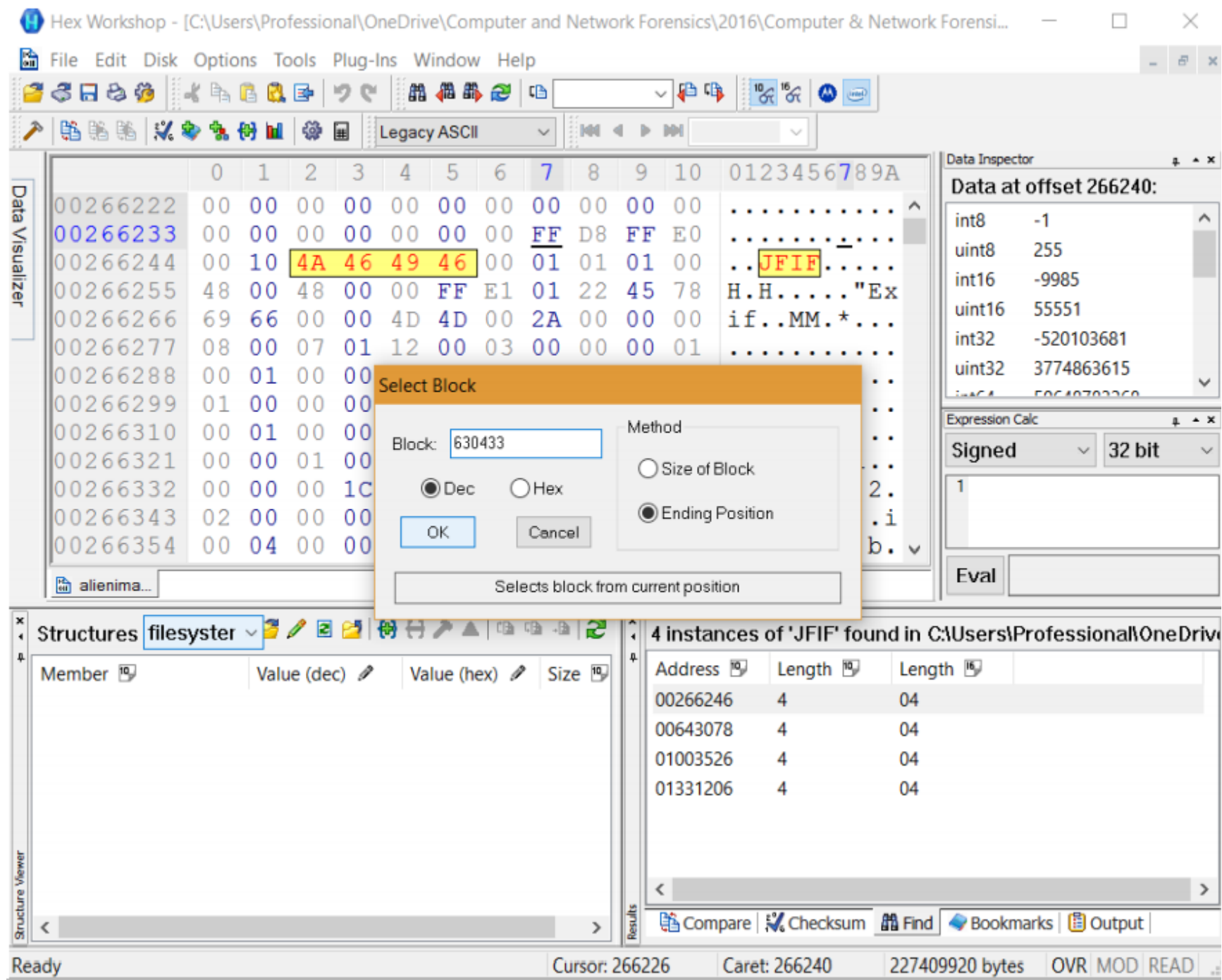


Enter the Block
with the offset
value of the end of
file

Make sure to
select 'Dec' and
'Ending Position'.

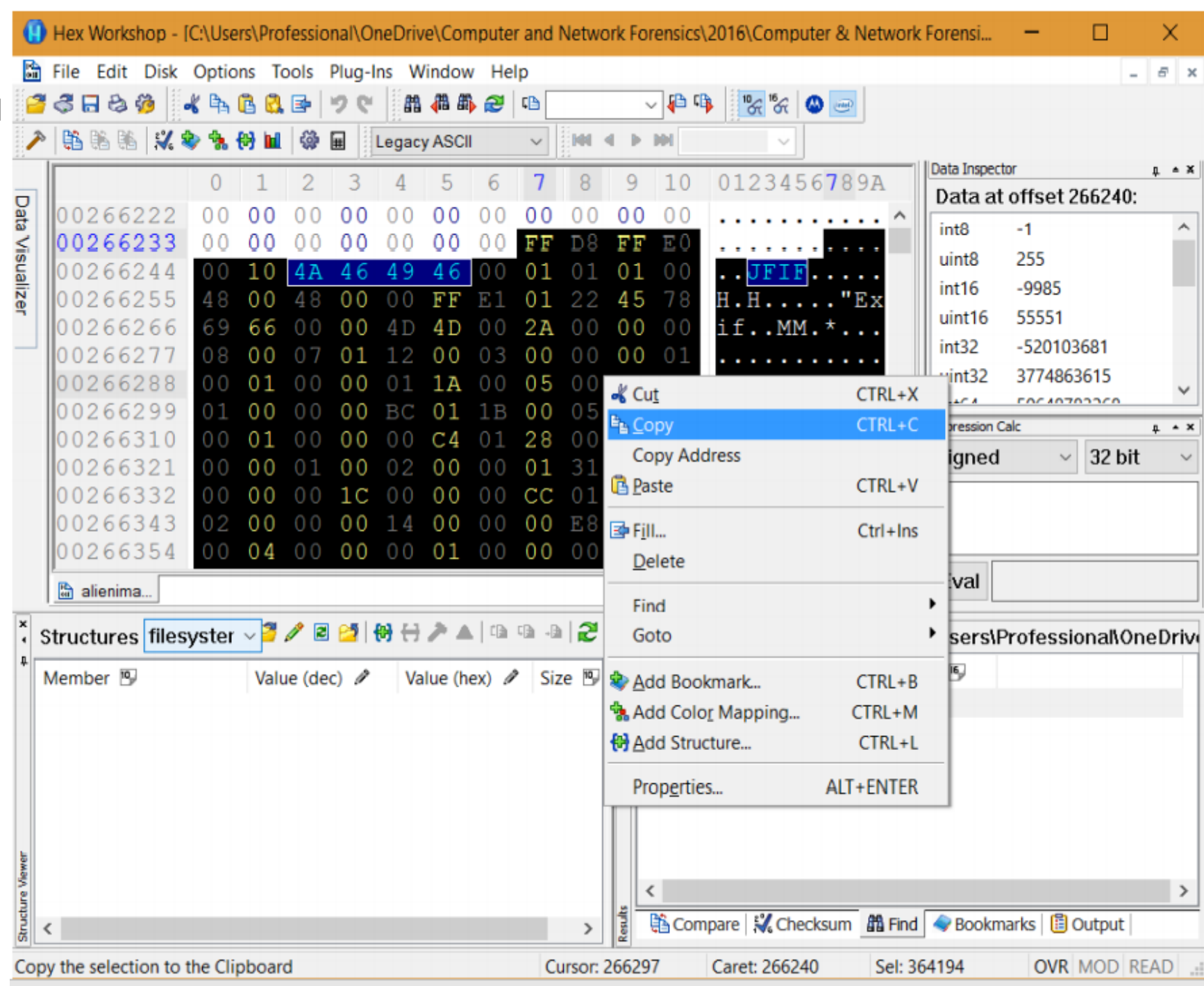
Click 'OK'

Right click the
select area and
click Copy



Carve .jpeg files from alienimage.dd

Right click the
select area and
click Copy



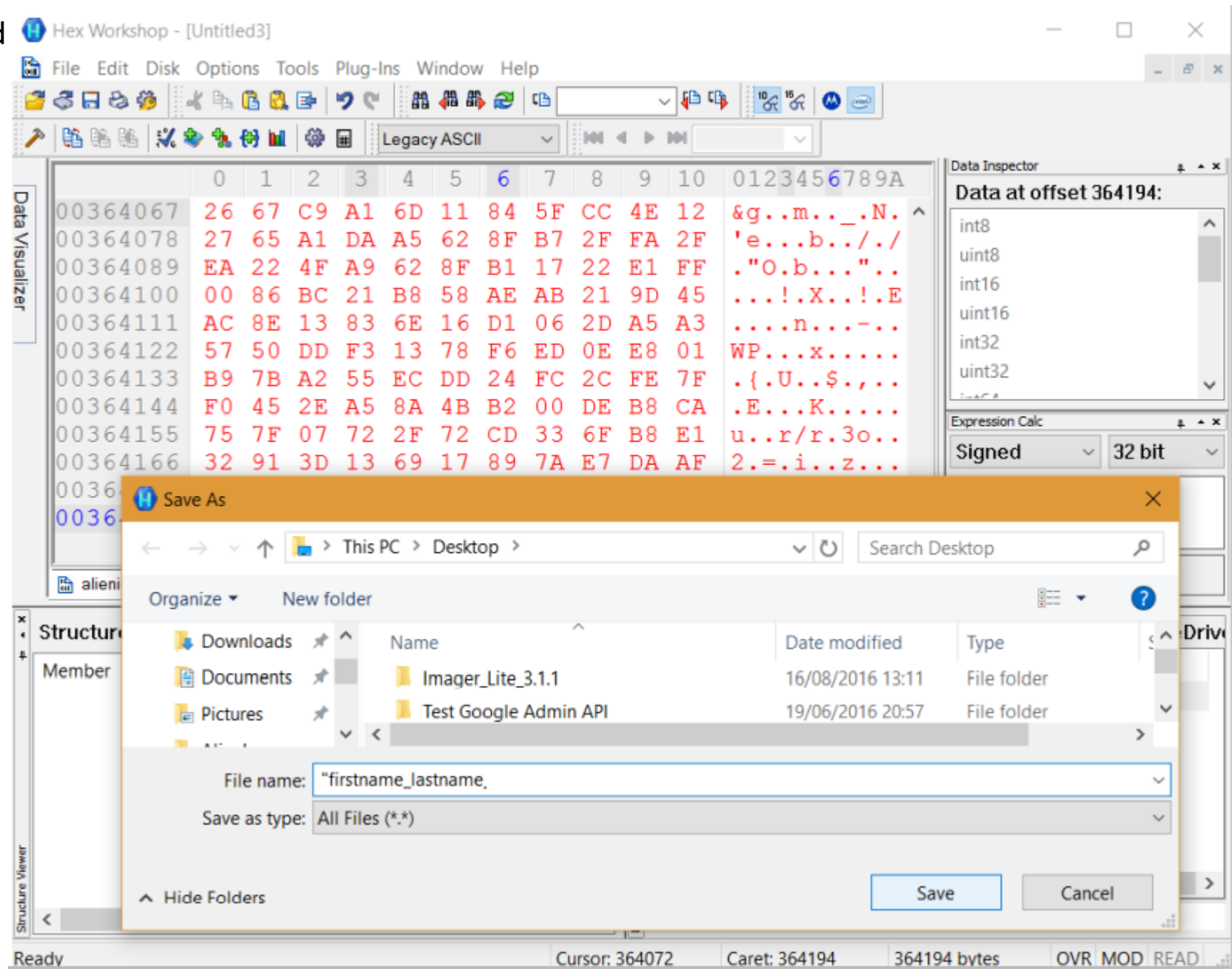
Carve .jpeg files from alienimage.dd

Create a new file
by clicking on File ->
New

Paste the copied
contents

Click 'Yes' in the
prompt window

Enter the name
of the file and take a
screenshot for
submission



Take a Screenshot

- Make sure your screenshot is similar to the one shown in the previous slide.
- Save the screenshot as 'firstname_lastname LAB HEX'.
Save as .jpeg or .png

Carve .jpeg files from alienimage.dd

Click Save

Now browse to the location of the saved file and view it. You should see the image shown here.

You have successfully carved a .jpeg file using Hex Viewer!

Carve other jpeg files for practice.



Questions

1. Write a definition of data carving
2. Convert alienimage.dd to alienimage.E01 using FTK **Imager** and view in Hex Workshop. What is different about the data this time?
3. Try carving a .jpeg file from the alienimage.**E01** image. Were you able to carve the file? Please provide a reason for your answer.

Questions

- To view the filesystem structure of alienimage.dd, find FAT16 in the file. Place your cursor at the beginning of FAT16.

On the left hand corner below, click on Select Structure Library -> filesystem.hsl -> Add Structure -> FAT 32

4. What is the OEM Name and Drive Number displayed for alienimage.dd?

Hex Workshop - [C:\Users\Professional\OneDrive\Computer and Network Forensics\2016\Computer & Network Forensics - Lect 3...

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	.	<	.	M	S	D	O	S	5	.	0
00000012	02	20	06	00	02	00	02	00	00	F8	F1	00	
00000024	3F	00	FF	00	00	00	00	00	00	10	1E	00	?	
00000036	80	00	29	C7	CC	86	C4	4E	4F	20	4E	41	..)	
00000048	4D	45	20	20	20	20	46	41	54	31	36	20	M	E	
00000060	20	20	33	C9	8E	D1	BC	F0	7B	8E	D9	B8	
00000072	00	20	8E	C0	FC	BD	00	7C	38	4E	24	7D	
00000084	24	8B	C1	99	E8	3C	01	72	1C	83	EB	3A	\$	
00000096	66	A1	1C	7C	26	66	3B	07	26	8A	57	FC	f	
00000108	75	06	80	CA	02	88	56	02	80	C3	10	73	u	
00000120	EB	33	C9	8A	46	10	98	F7	66	16	03	46	
00000132	1C	13	56	1E	03	46	0E	13	D1	8B	76	11	
00000144	60	89	46	FC	89	56	FE	B8	20	00	F7	E6	

Data Inspector

Data at offset 54:

int8	70
uint8	70
int16	16710
uint16	16710
int32	827605318
uint32	827605318

Expression Calc

Signed 32 bit

1

Eval

Structures filesystem (f)

4 instances of 'JFIF' found in C:\Users\Professional\OneDrive\Co

Select Structure Library

Submit

- Submit your answers to the questions and relevant screenshots as one **MS WORD** document to moodle

Additional Task:

It would be good practice for you to run the alien image through Autopsy and view your findings versus your findings for Lab 2 when you used FTK Imager