



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

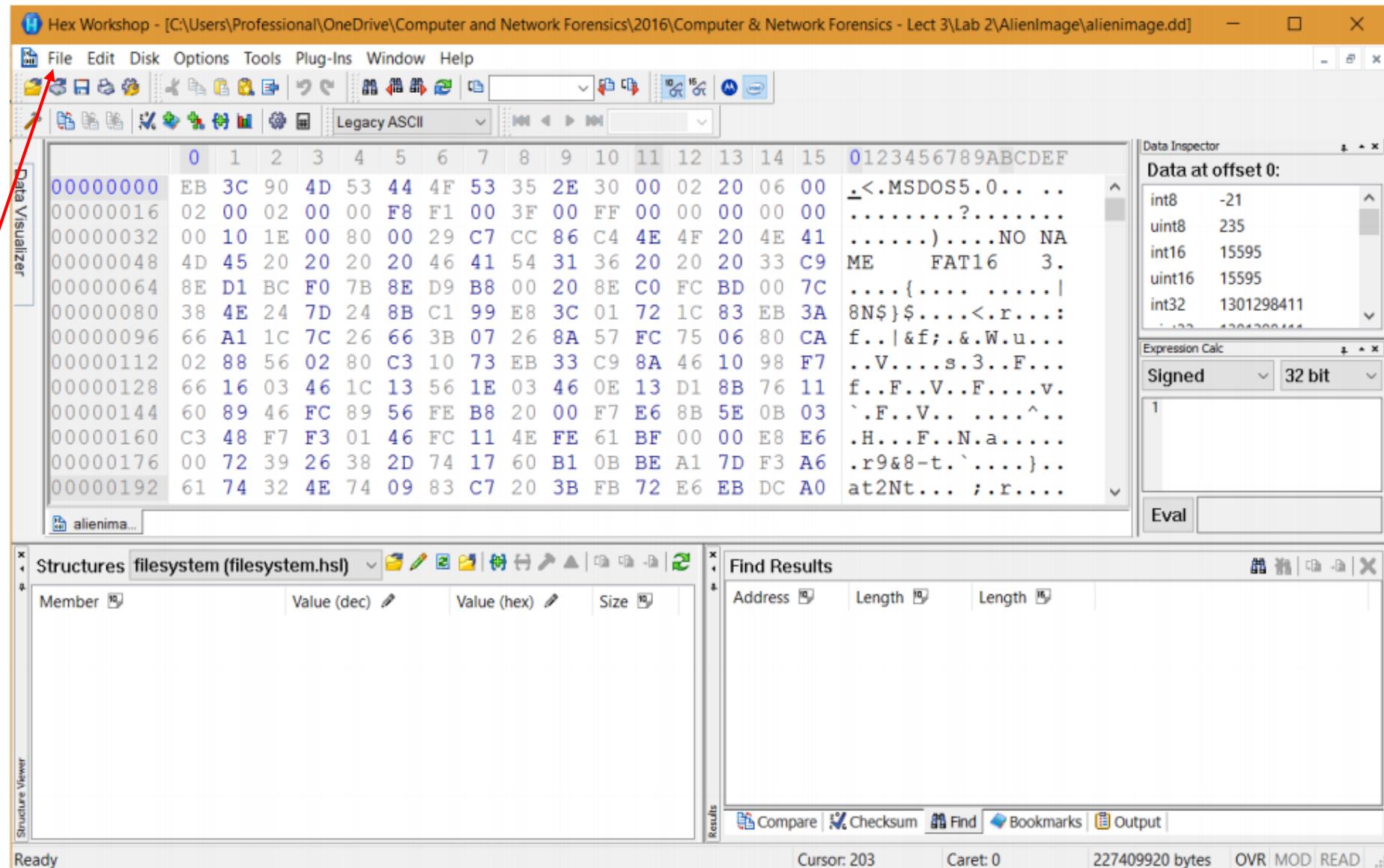
Name	Type	Compressed size	Passv
AlienImage	File folder		
hw_v680	Application	18,194 KB	No

Carve .jpeg files from alienimage.dd

1. Open Hex Workshop Editor on your windows machine.

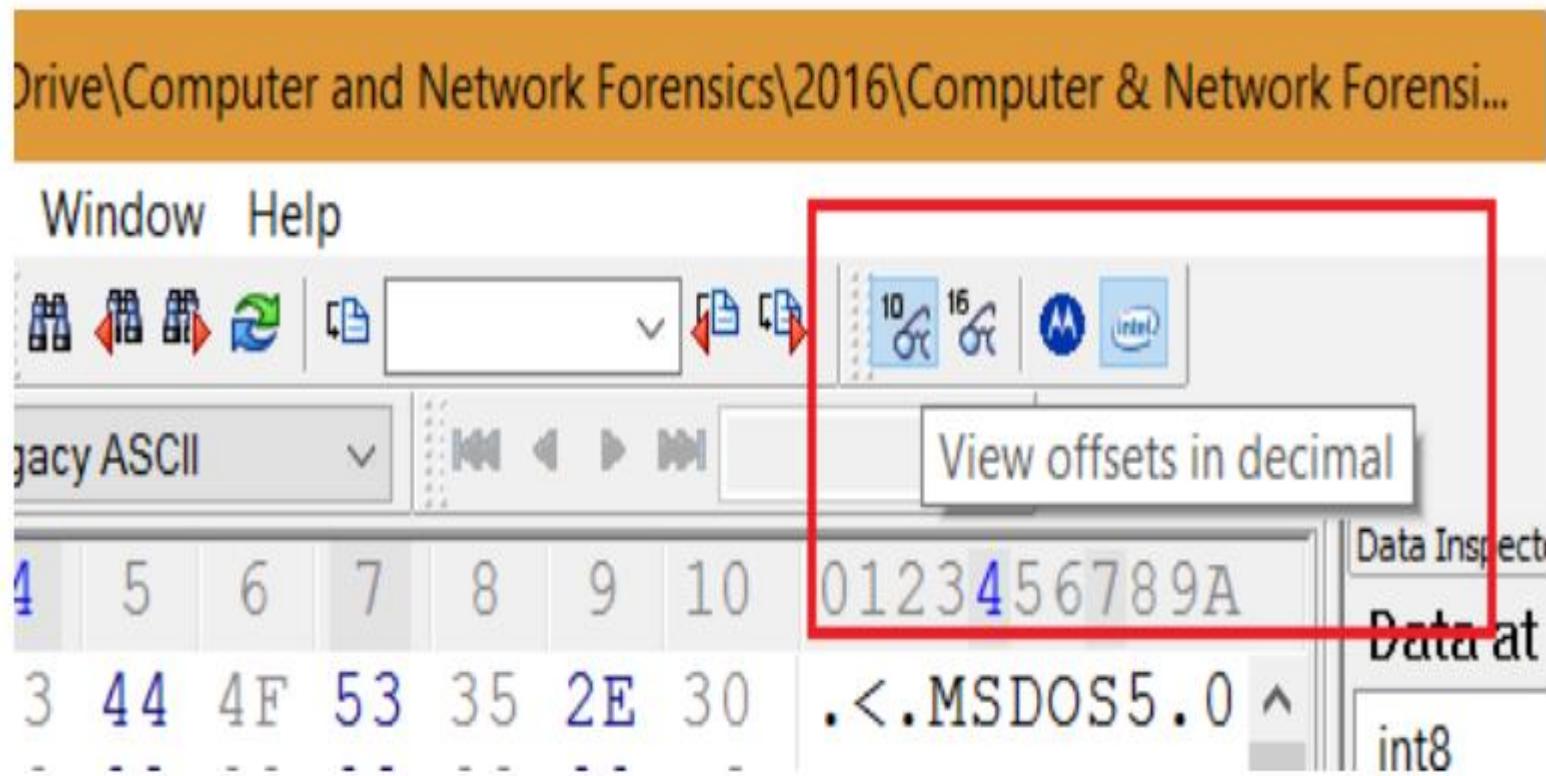
2. Open the alienimage.dd

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



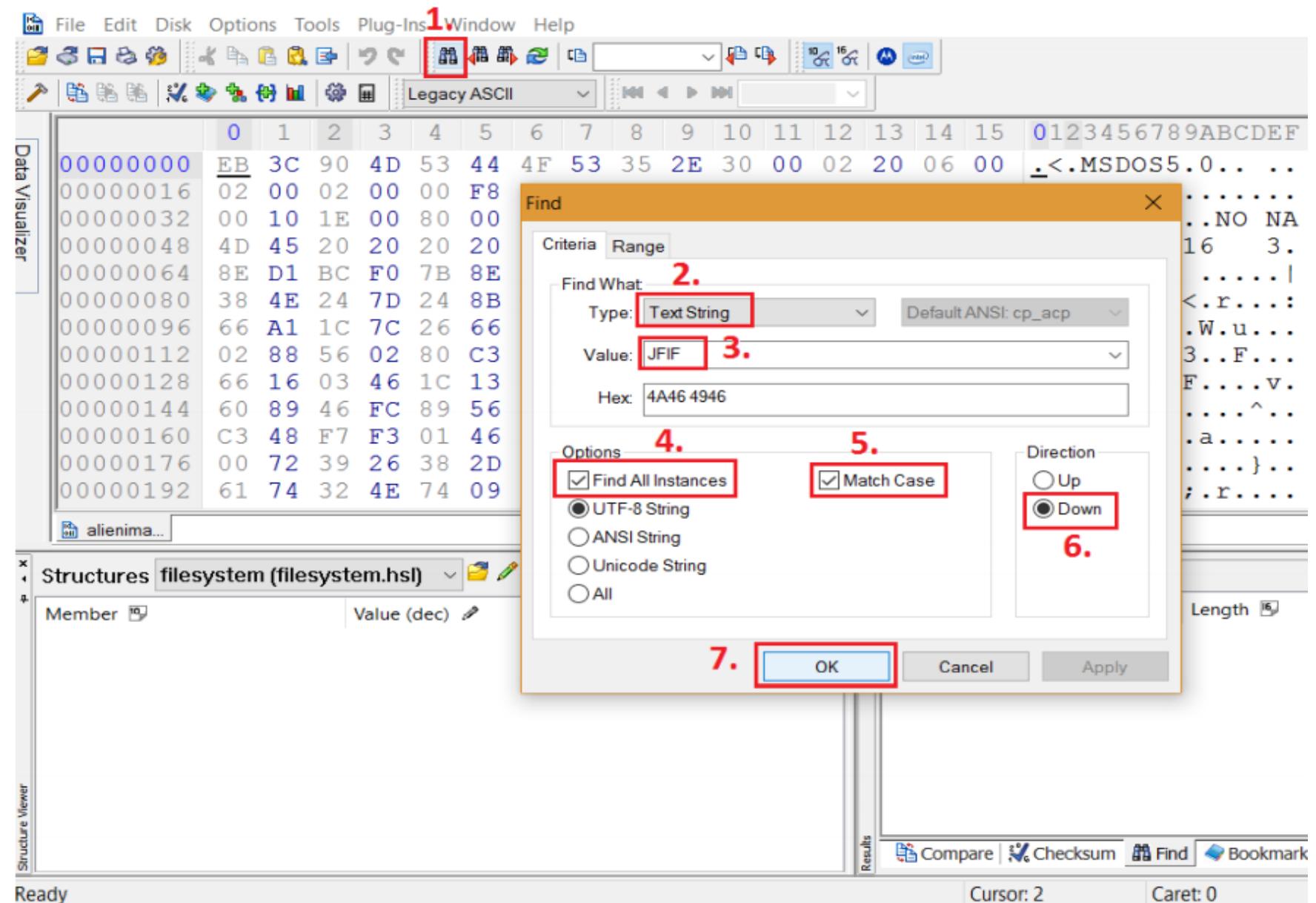
Carve .jpeg files from
alienimage.dd

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

The screenshot shows the Hex Workshop interface with the following details:

- Hex View:** The main pane displays memory starting at address 00266222. A red box highlights the sequence **FF D8 FF E0**, which is the JFIF header signature. Below it, another red box highlights the sequence **4A 46 49 46**, which is part of the JPEG file data.
- Data Inspector:** Shows data at offset 266342, including fields like int8, uint8, int16, uint16, and int32, all set to 512.
- Structure Viewer:** Shows a table for "Structures filesyster".
- Results:** A table titled "4 instances of 'JFIF' found in C:\Users\Professional\OneDrive" lists the following addresses and lengths:

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

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

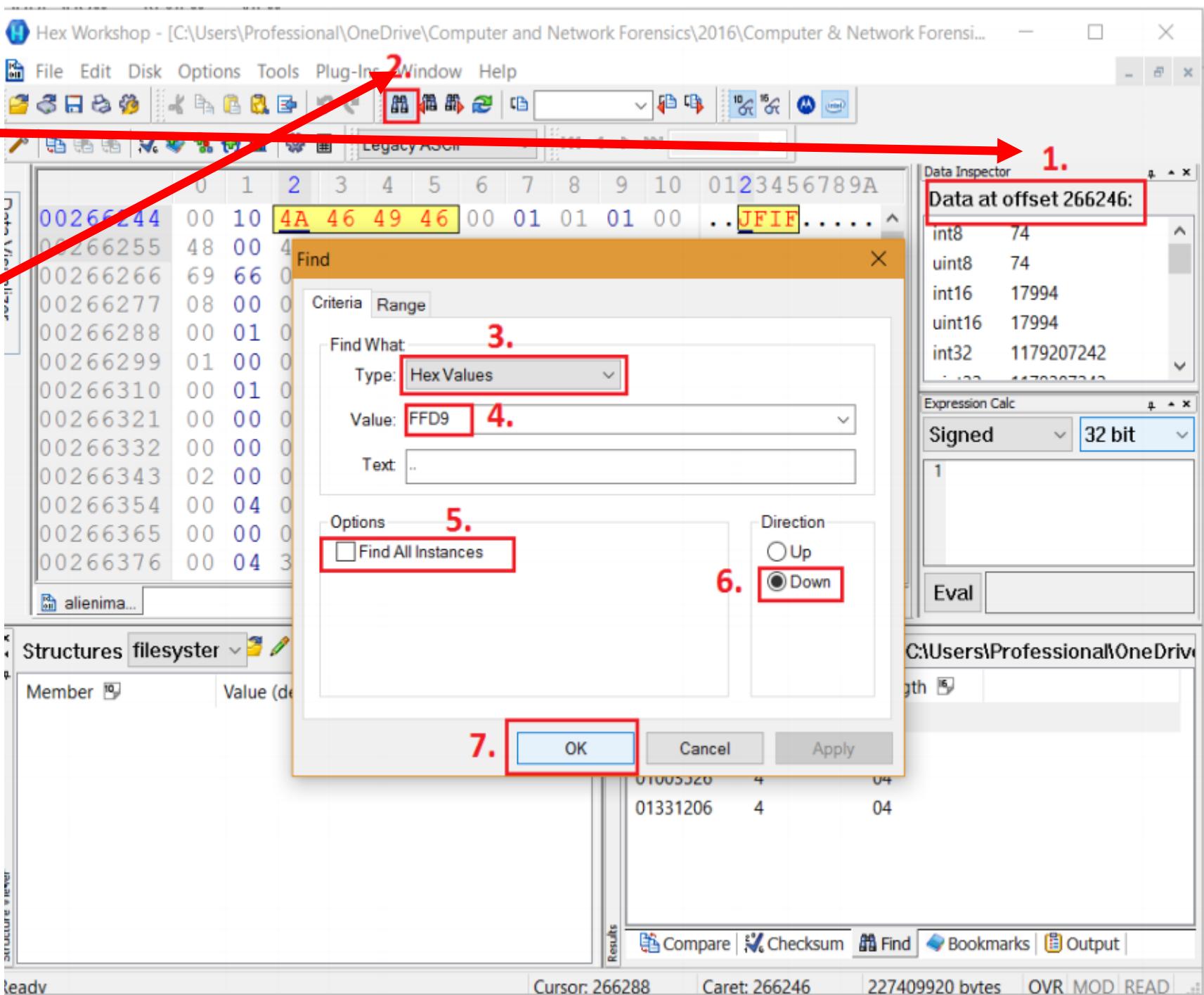
3. Enter the type as 'Hex Values'

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.

The screenshot shows the Hex Workshop interface with the following details:

- Title Bar:** Hex Workshop - [C:\Users\Professional\OneDrive\Computer and Network Forensics\2016\Computer & Network Forensi...]
- Menu Bar:** File, Edit, Disk, Options, Tools, Plug-Ins, Window, Help
- Toolbar:** Includes icons for Open, Save, Find, Replace, Cut, Copy, Paste, and various analysis tools.
- Data Visualizer:** A large grid showing memory dump data. The cursor is at address 0x00099FA0 (630432). The value at this address is FF D9, which is the start of a JPEG file (marker 0xFF D9).
- Data Inspector:** Shows the data at offset 630432:
 - int8 -1
 - uint8 255
 - int16 -9729
 - uint16 55807
 - int32 -127
- Expression Calc:** Shows a signed 32-bit value of 1.
- Structure Viewer:** Shows a 'filesyster' structure with a member table.
- Results:** Shows 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
- Status Bar:** Found at position 0x00099FA0 (630432), Cursor: 266288, Caret: 630432, Sel: 2, OVR MOD READ

Carve .jpeg files from alienimage.dd

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.

The screenshot shows the Hex Workshop application interface. The main window displays a hex dump of a file, with the cursor positioned at offset 266240. The JFIF signature (FF D8 FF E0 xx xx) is highlighted in red. The caret value (266240) is also highlighted in red at the bottom of the interface. The application includes various toolbars, a Data Inspector panel, and a Structures viewer panel.

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

File Edit Disk Options Tools Plug-Ins Window Help

Data Visualizer

Legacy ASCII

Data at offset 266240:

int8	-1
uint8	255
int16	-9985
uint16	55551
int32	-520103681
uint32	3774863615

Expression Calc

Signed 32 bit

Eval

Structures filester

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

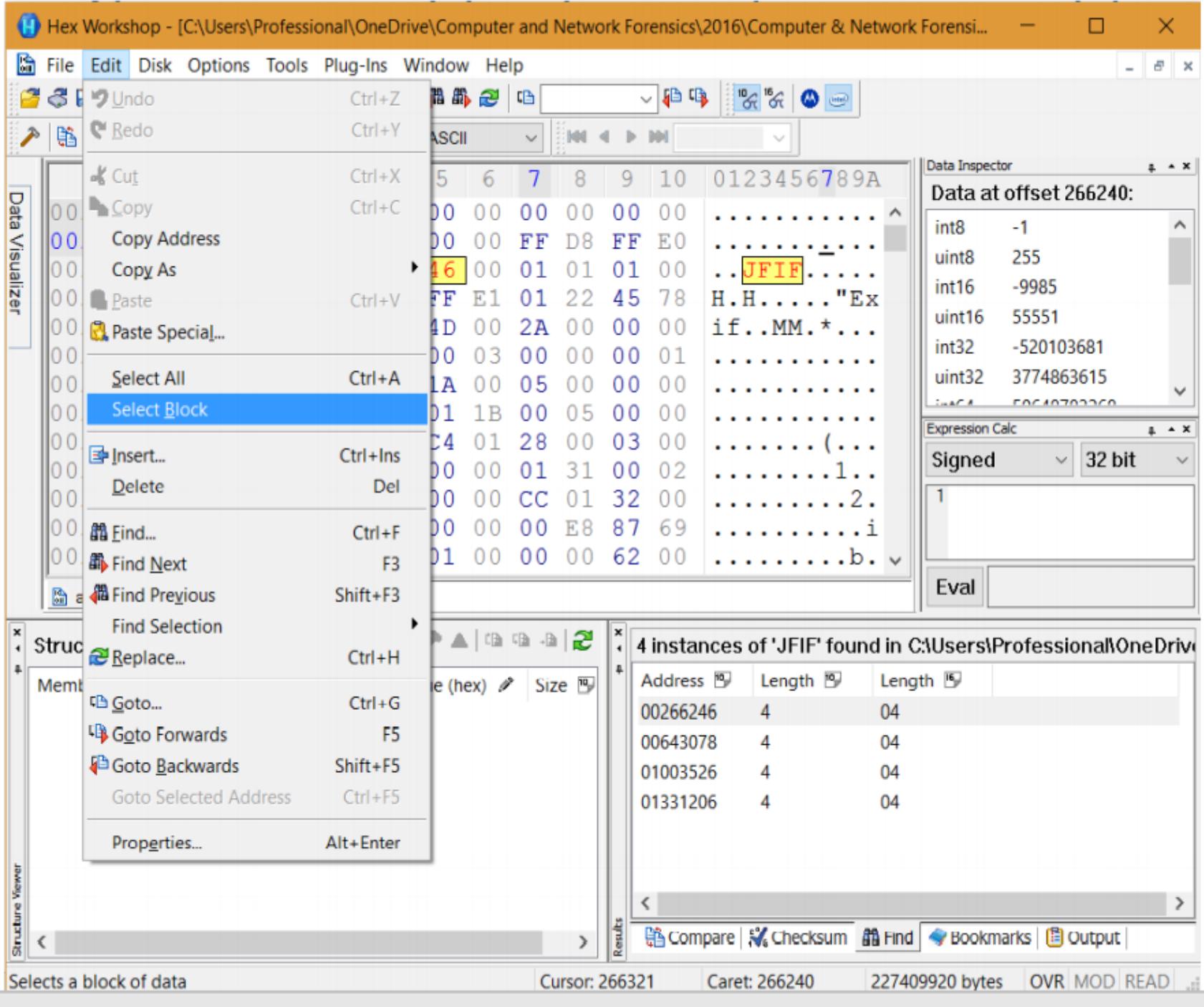
Compare Checksum Find Bookmarks Output

Ready Cursor: 266240 Caret: 266240 227409920 bytes OVR MOD READ

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



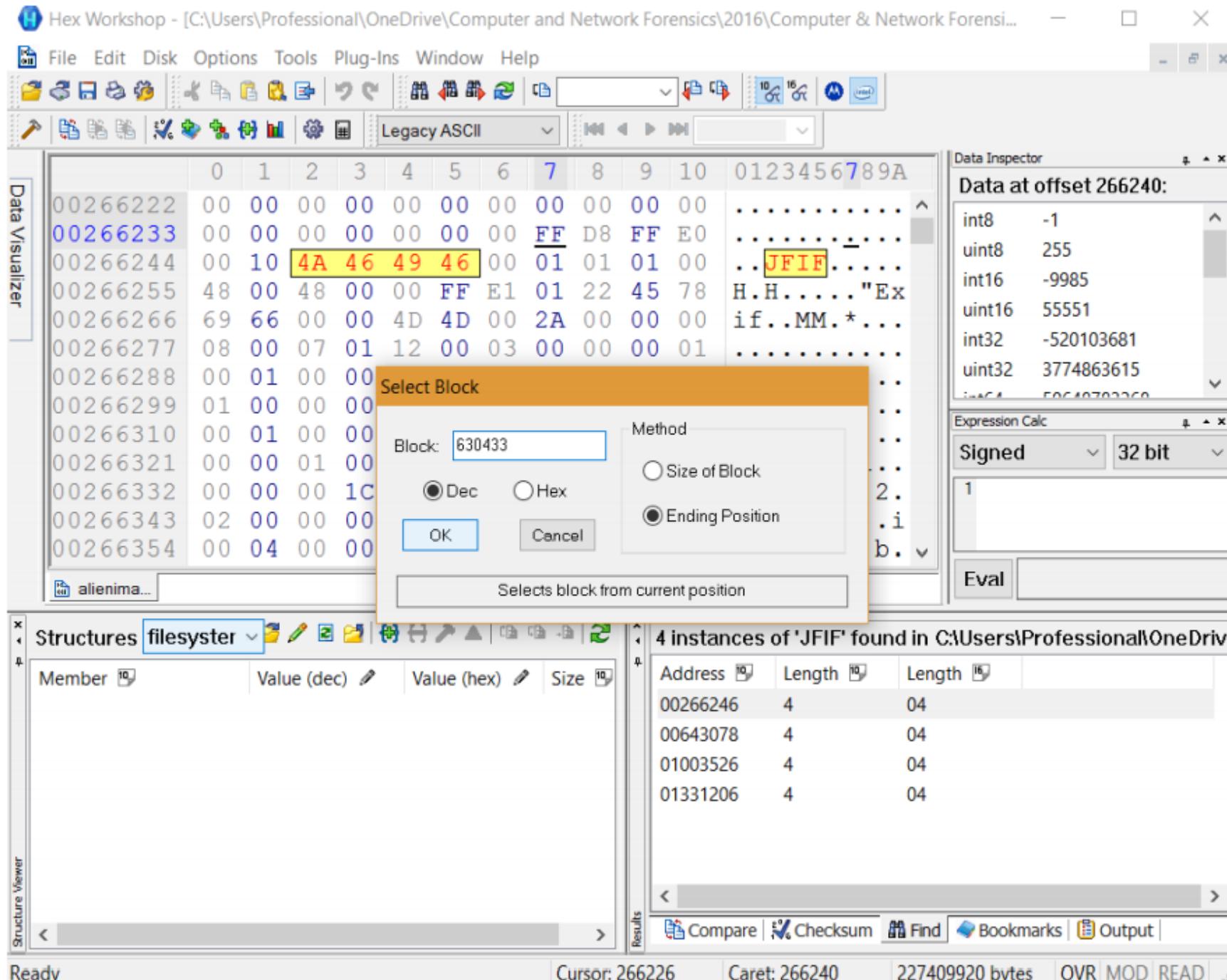
Carve .jpeg files from alienimage.dd

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

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

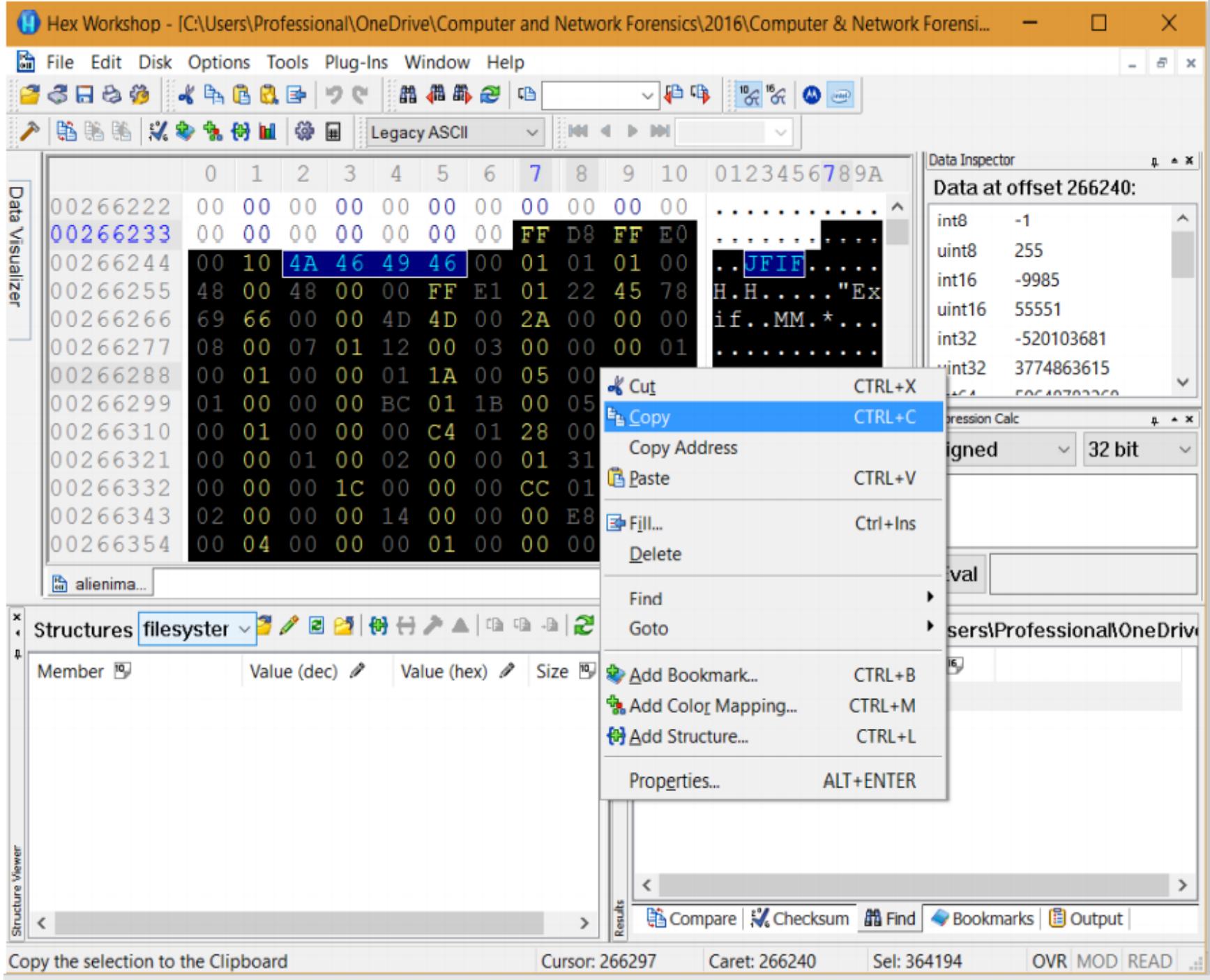
Click 'OK'

Right click the
select area and
click Copy

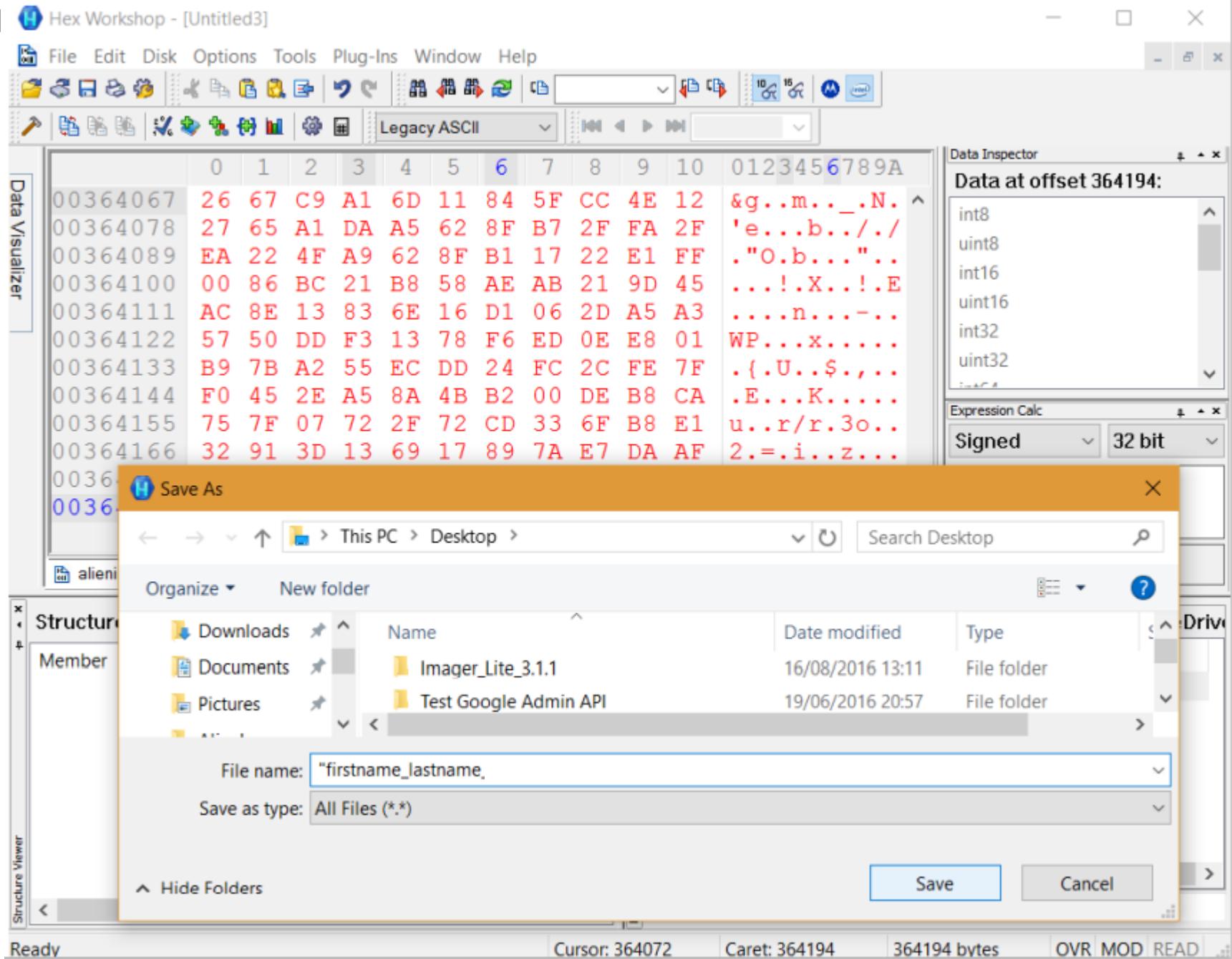


Carve .jpeg files from alienimage.dd

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

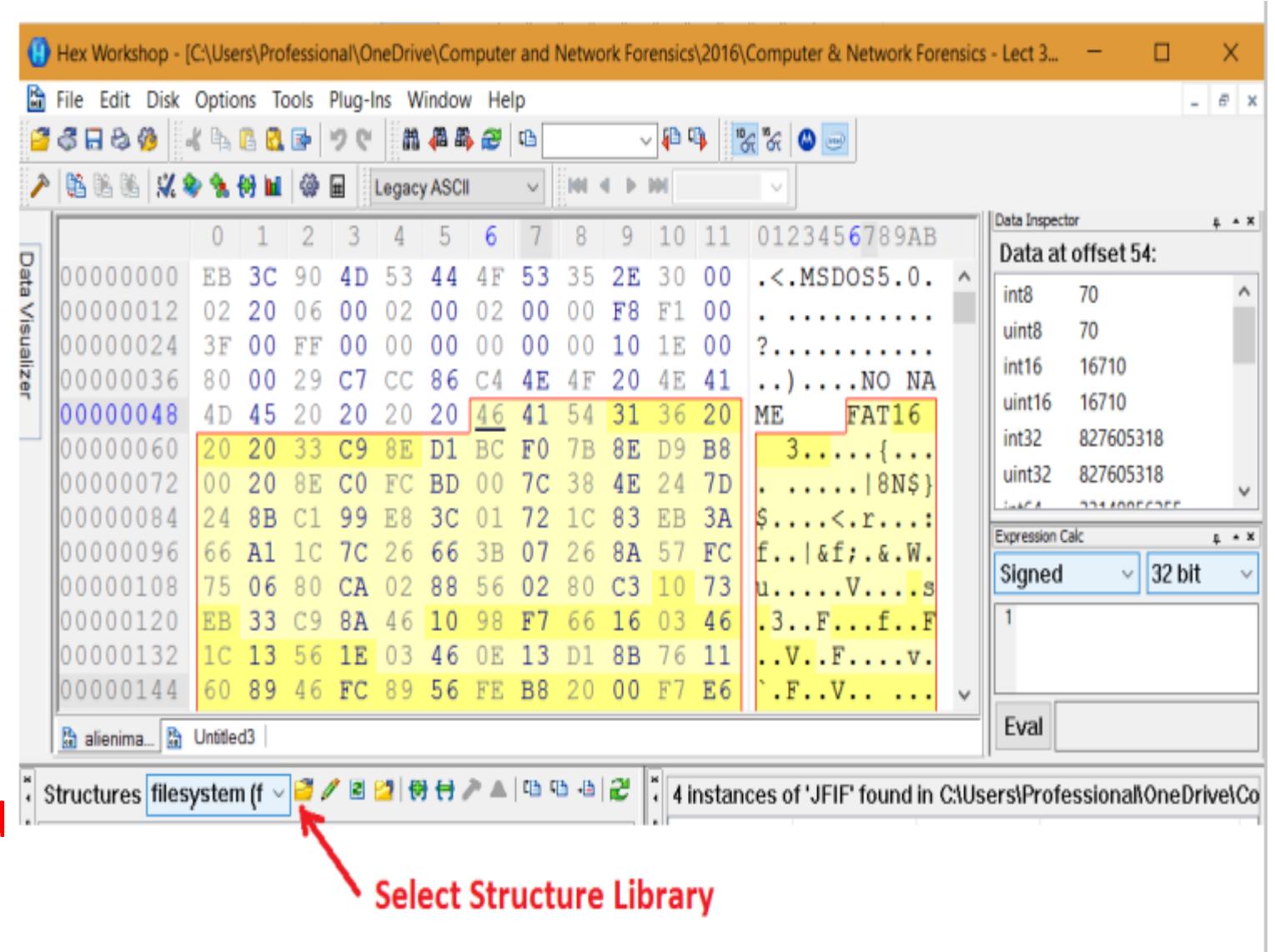
1. Write a definition of data carving
2. Convert alienimage.dd to alienimage.E01 using FTK **Imager** and view in Hex Workshop. What is different about the data this time?
3. Try carving a .jpeg file from the alienimage.**E01** image. Were you able to carve the file? Please provide a reason for your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



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