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

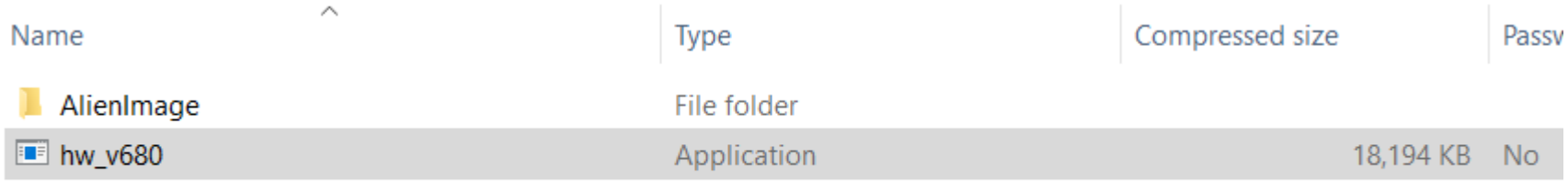
Carving files with Hex Workshop

- 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

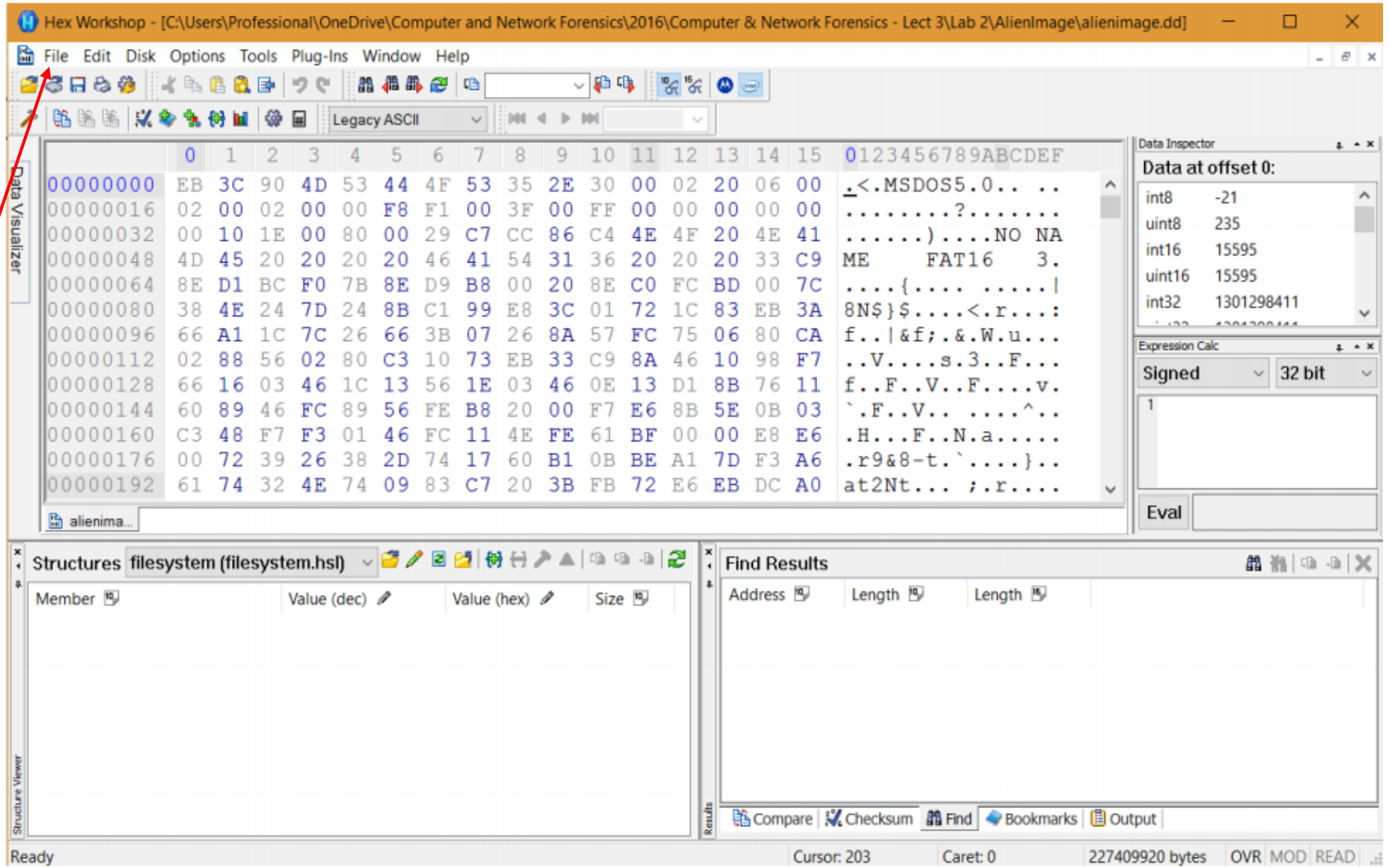
Choose Typical Install



Carve .jpeg files from alienimage.dd

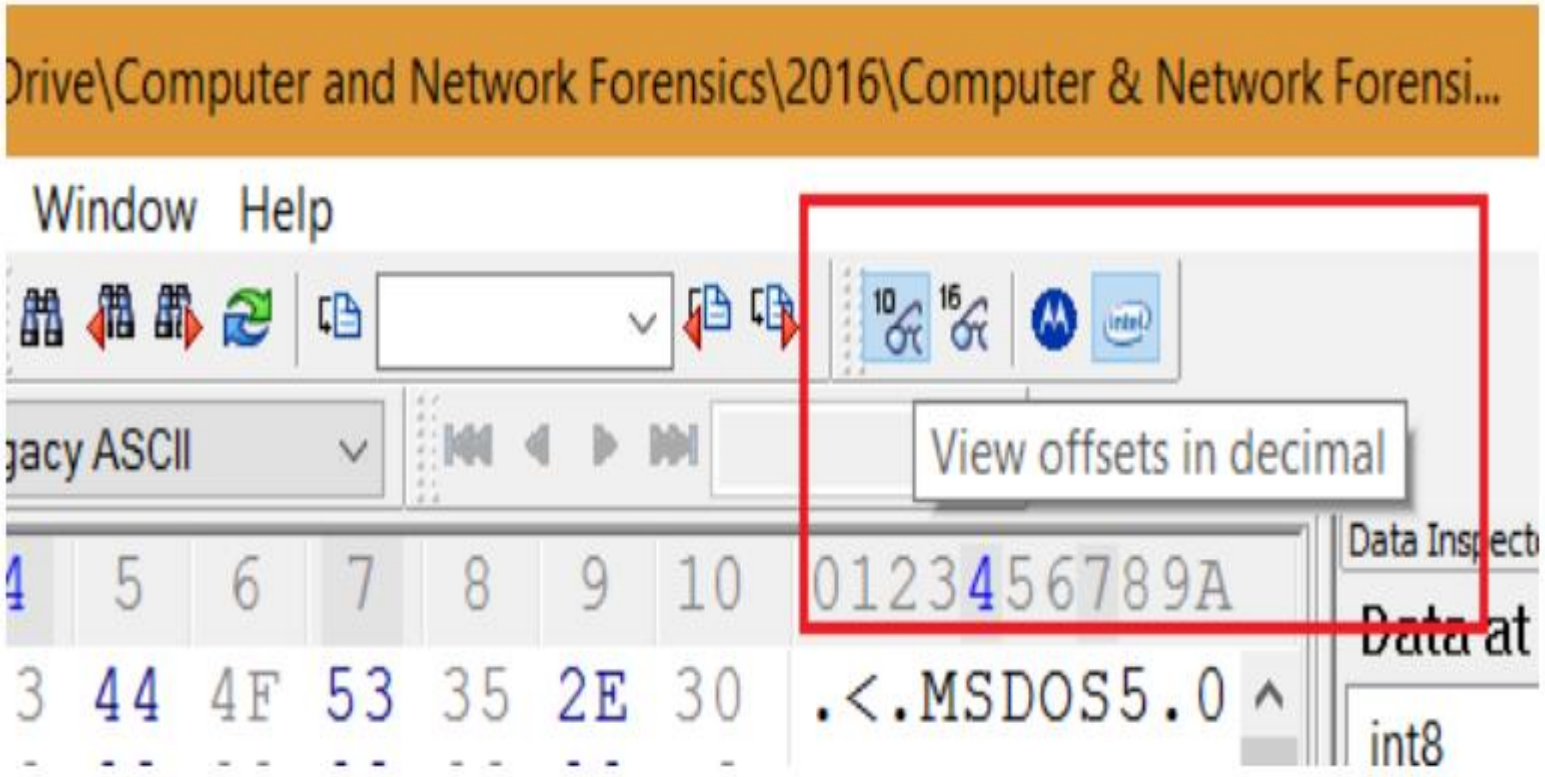
1. Open Hex Workshop Editor on your windows machine.

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



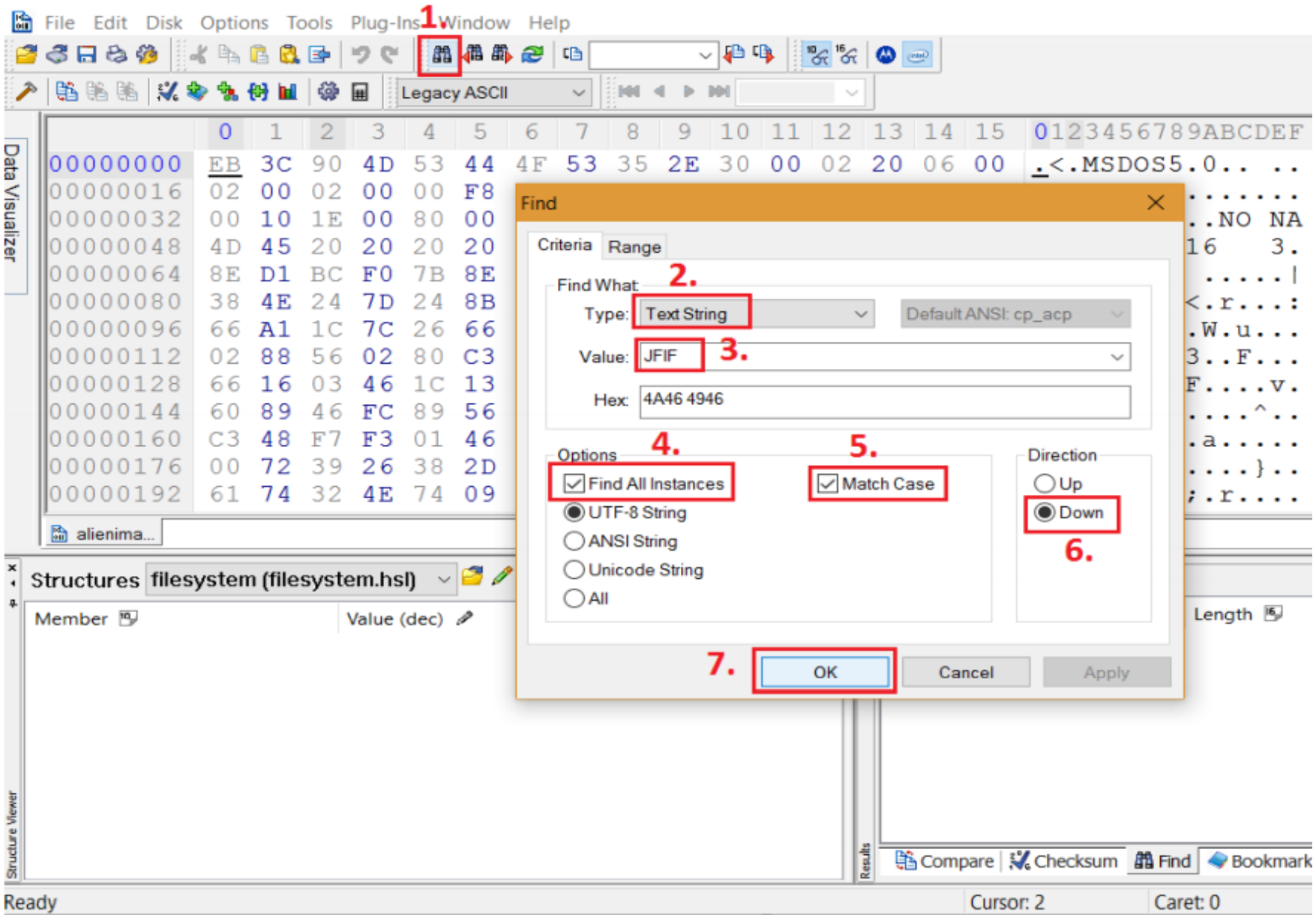
Carve .jpeg files from alienimage.dd

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’

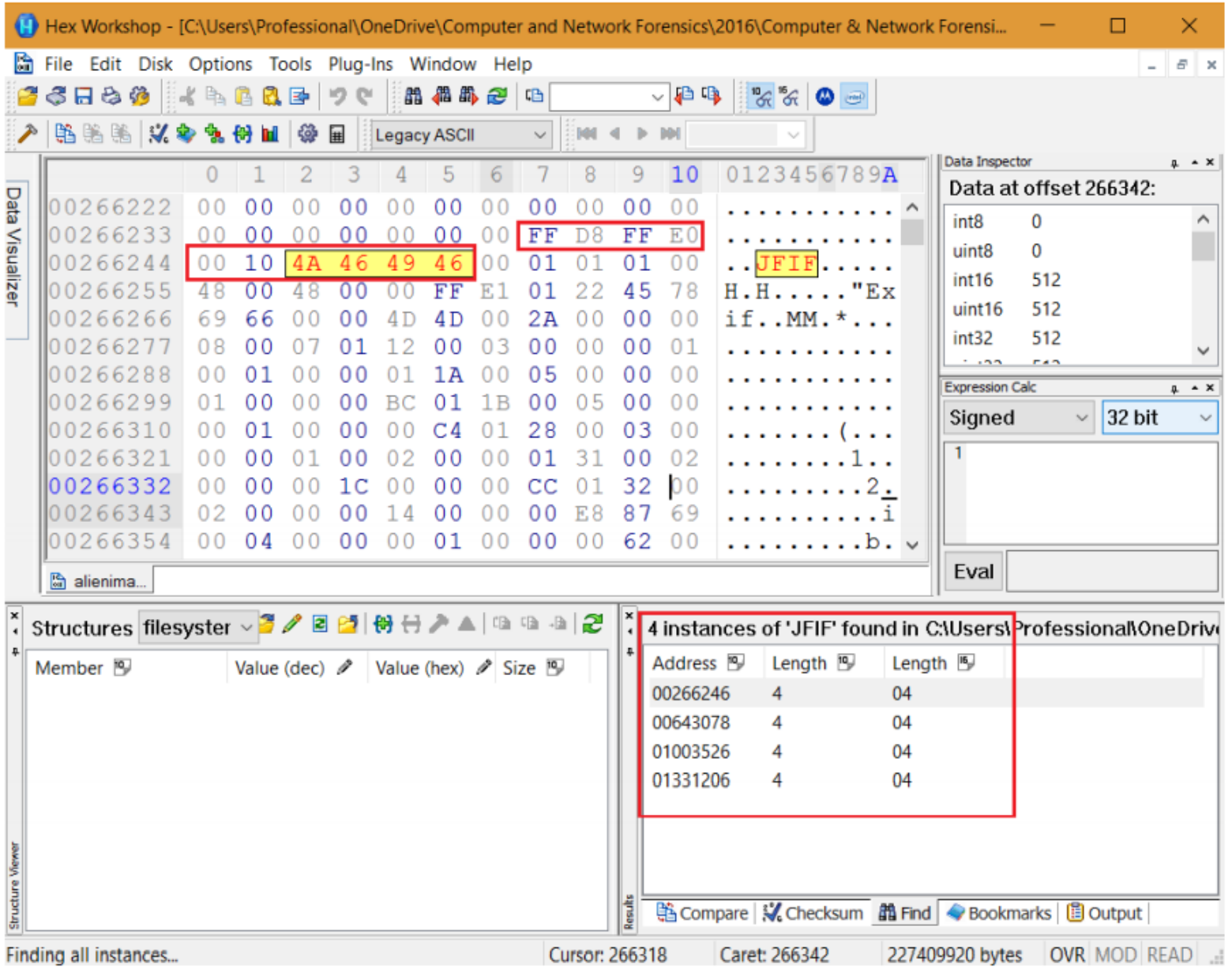


Carve .jpeg files from alienimage.dd

8. You will see 4 instances of JFIF found.

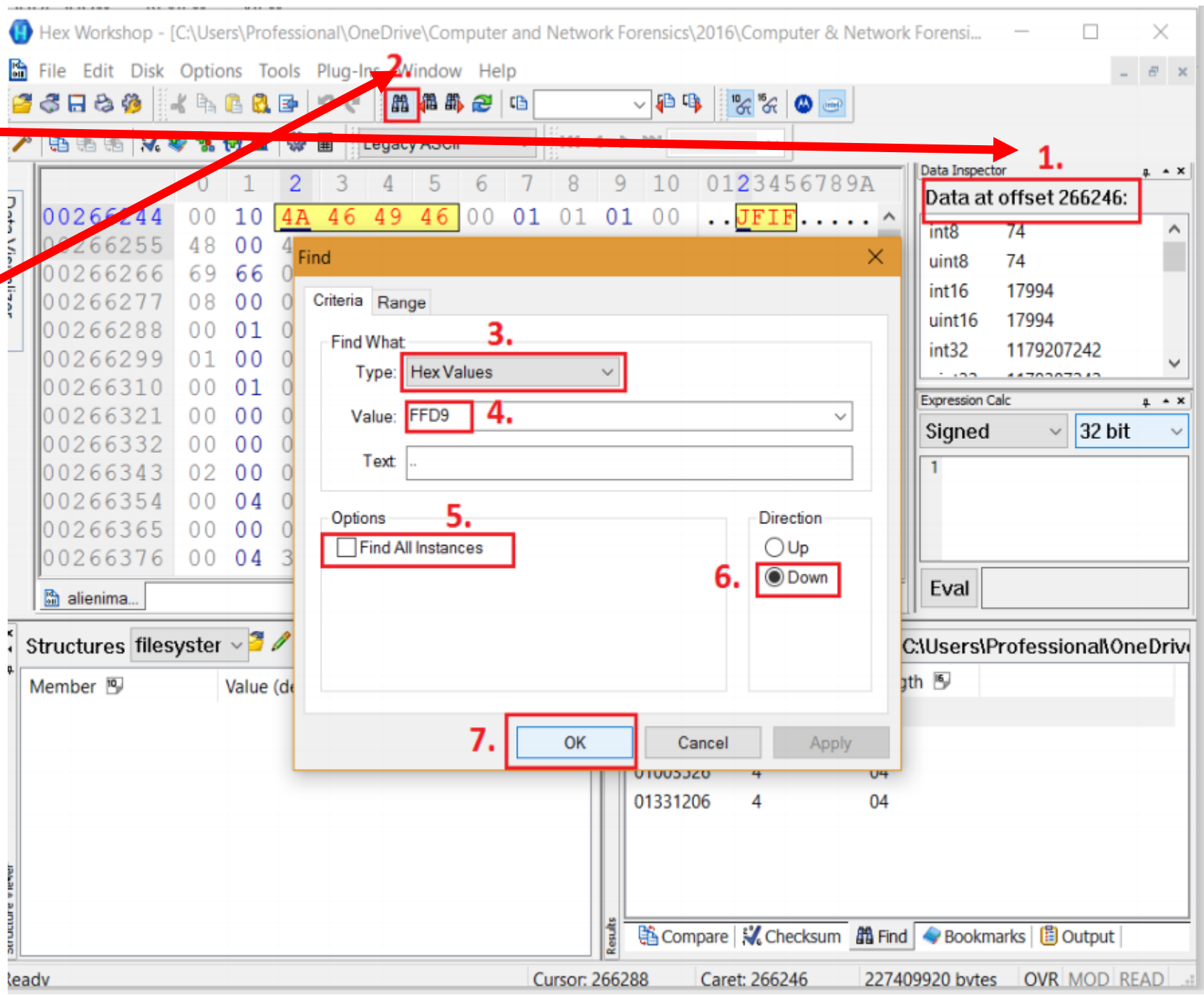
Note the Hex Signature of the JFIF file is FF D8 FF E0 xx xx 4A 46 49 46 00

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



Carve .jpeg files from alienimage.dd

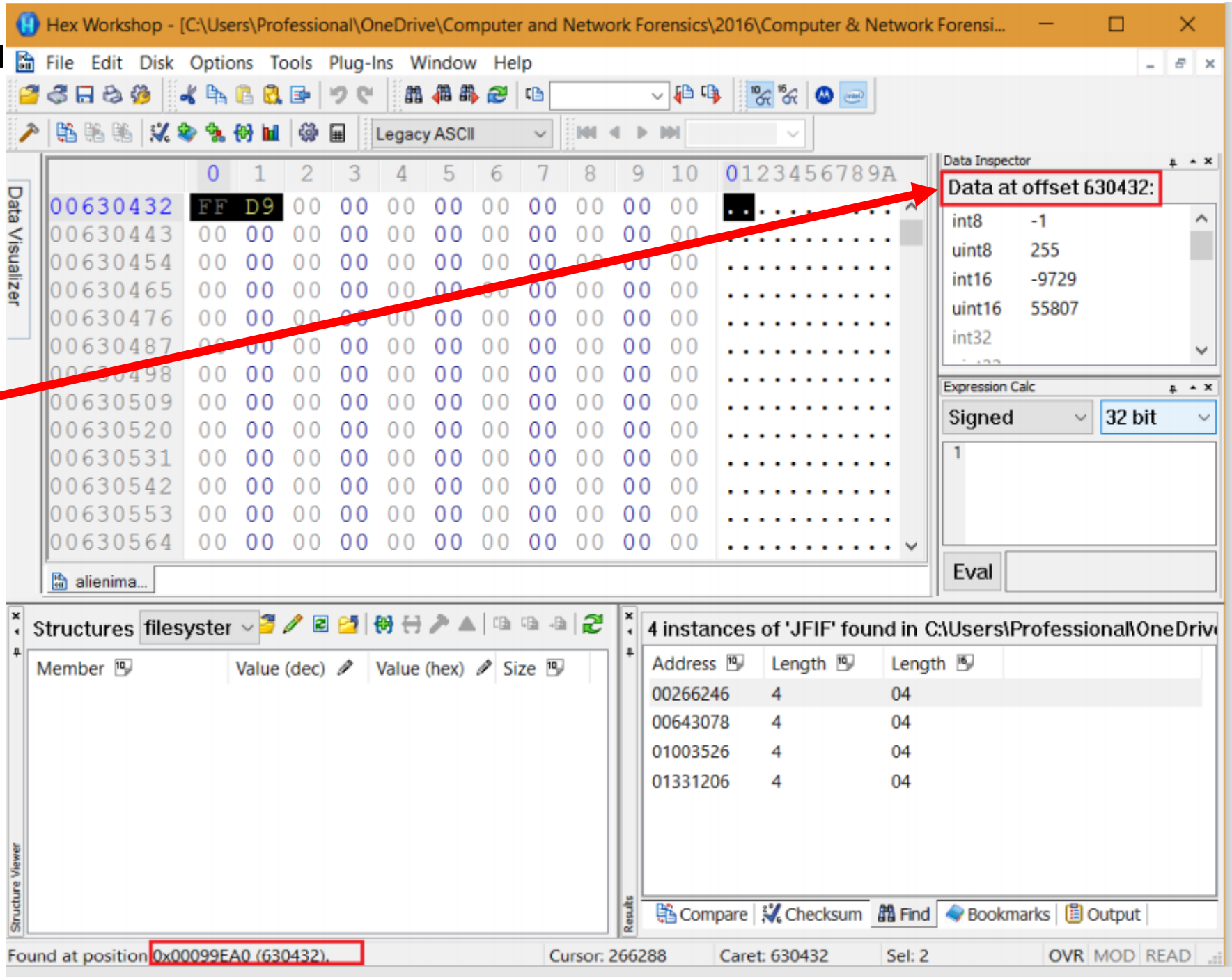
1. Note the data offset of the starting position of the .jpeg file for future reference.
2. Click on Find
3. Enter the type as ‘Hex Values’
4. Enter the value as ‘FFD9’
5. Make sure you uncheck ‘Find all Instances’ and select
6. ‘Down’.
7. Click ‘OK’



Carve .jpeg files from alienimage.dd

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

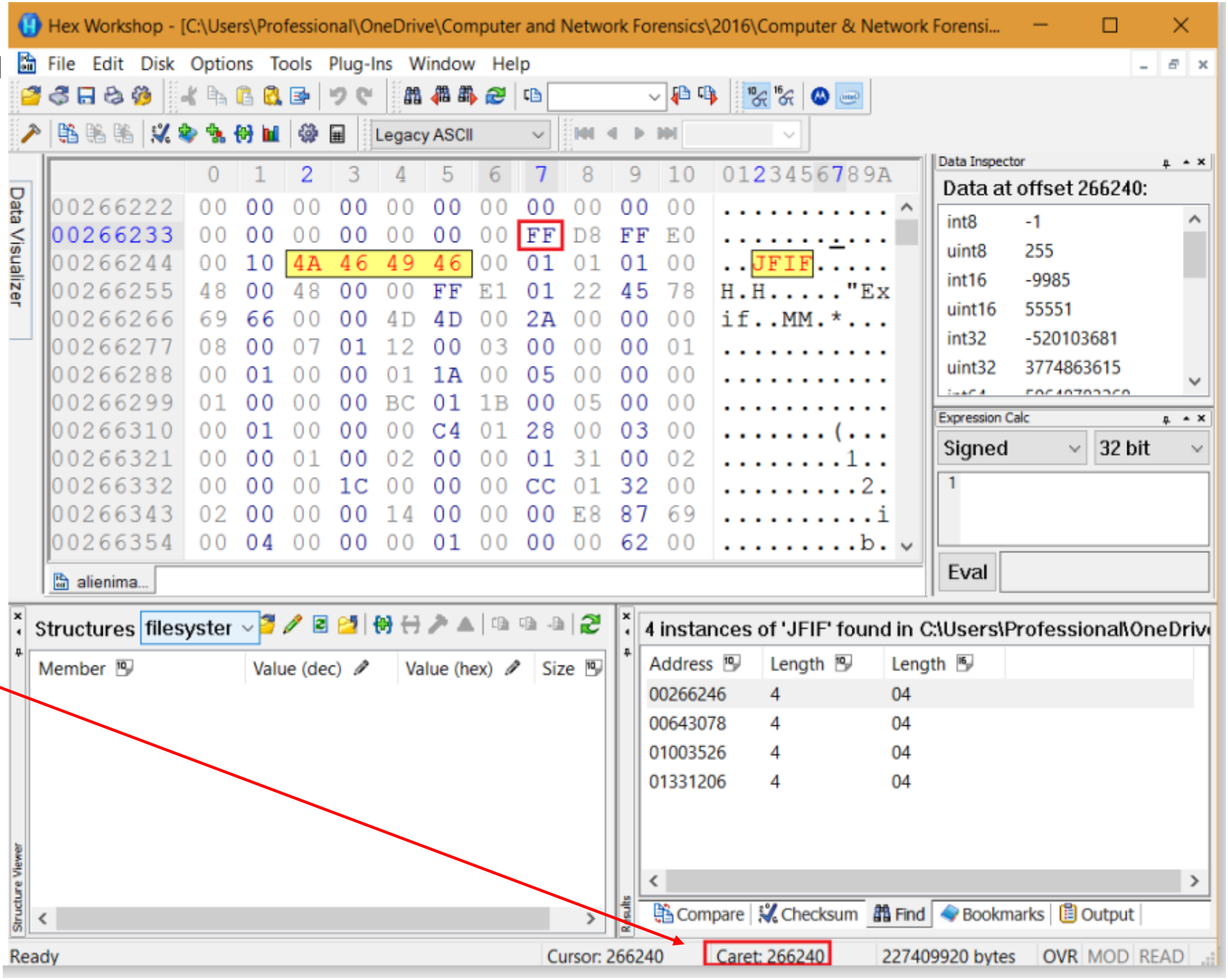
Your search for JFIF is still shown in the right hand corner find window.



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

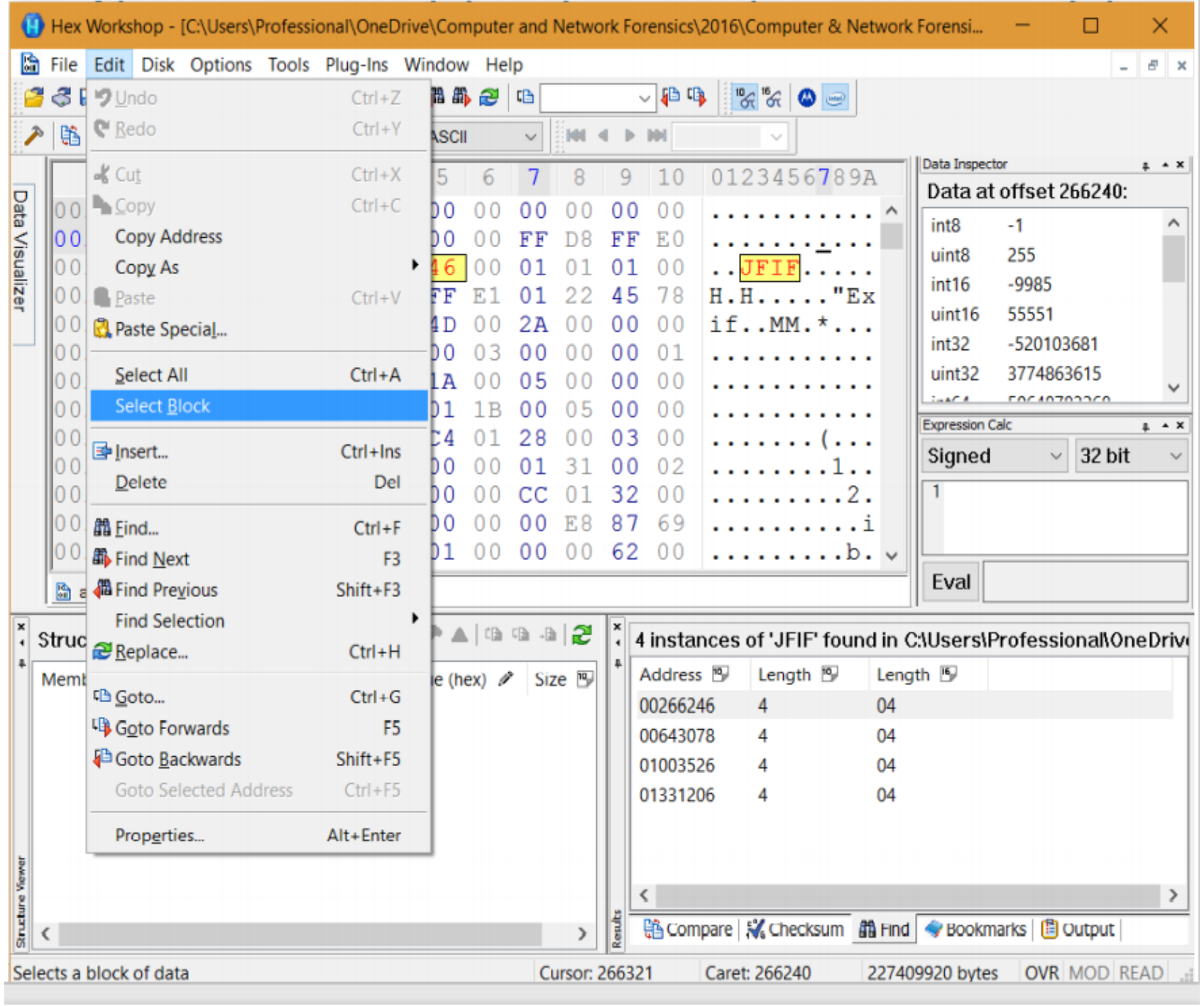
IMPORTANT: Make sure the Caret value is same as the one shown at the bottom of the screenshot here.



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**



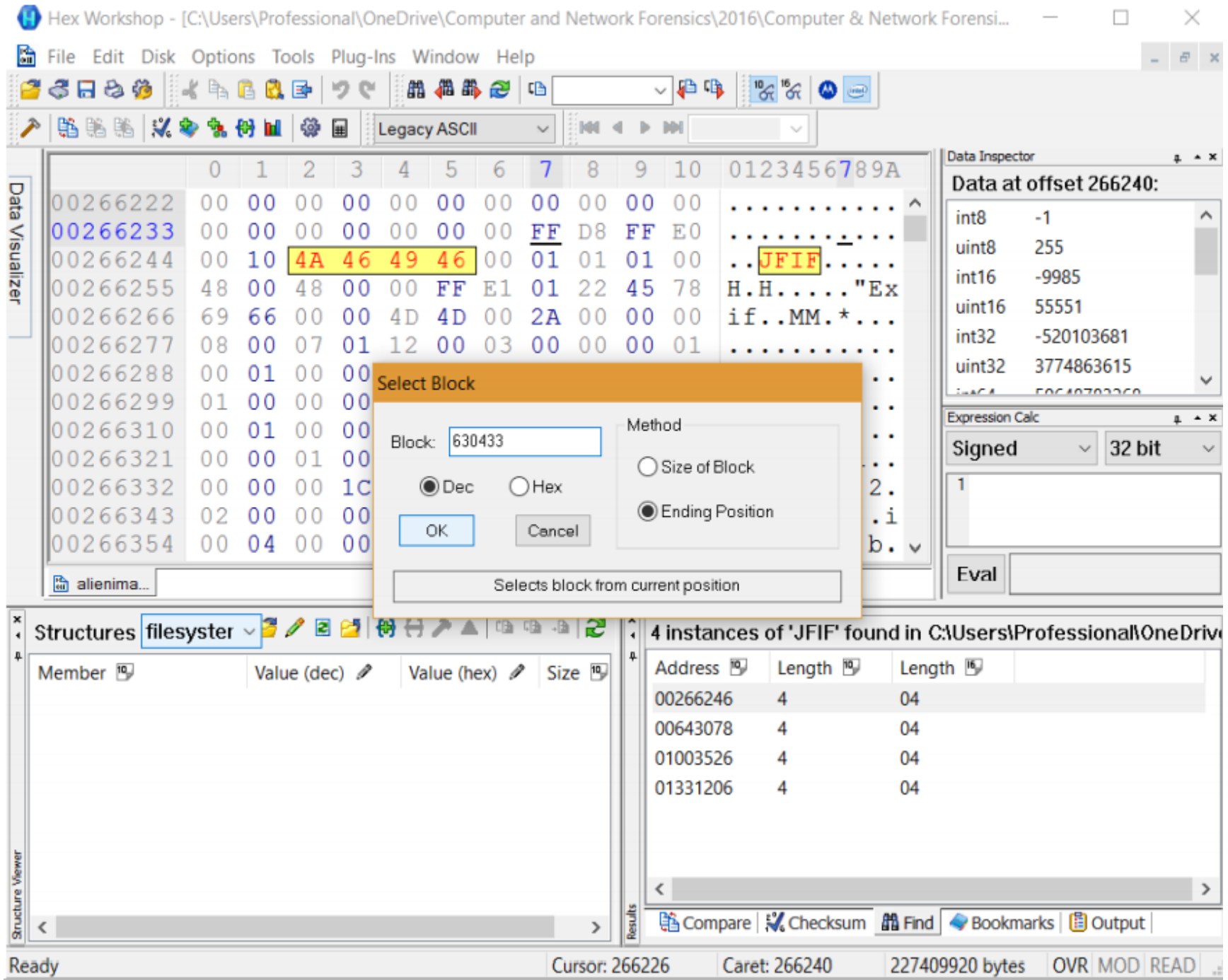
Carve .jpeg files from alienimage.dd

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

Make sure to select ‘Dec’ and ‘Ending Position’.

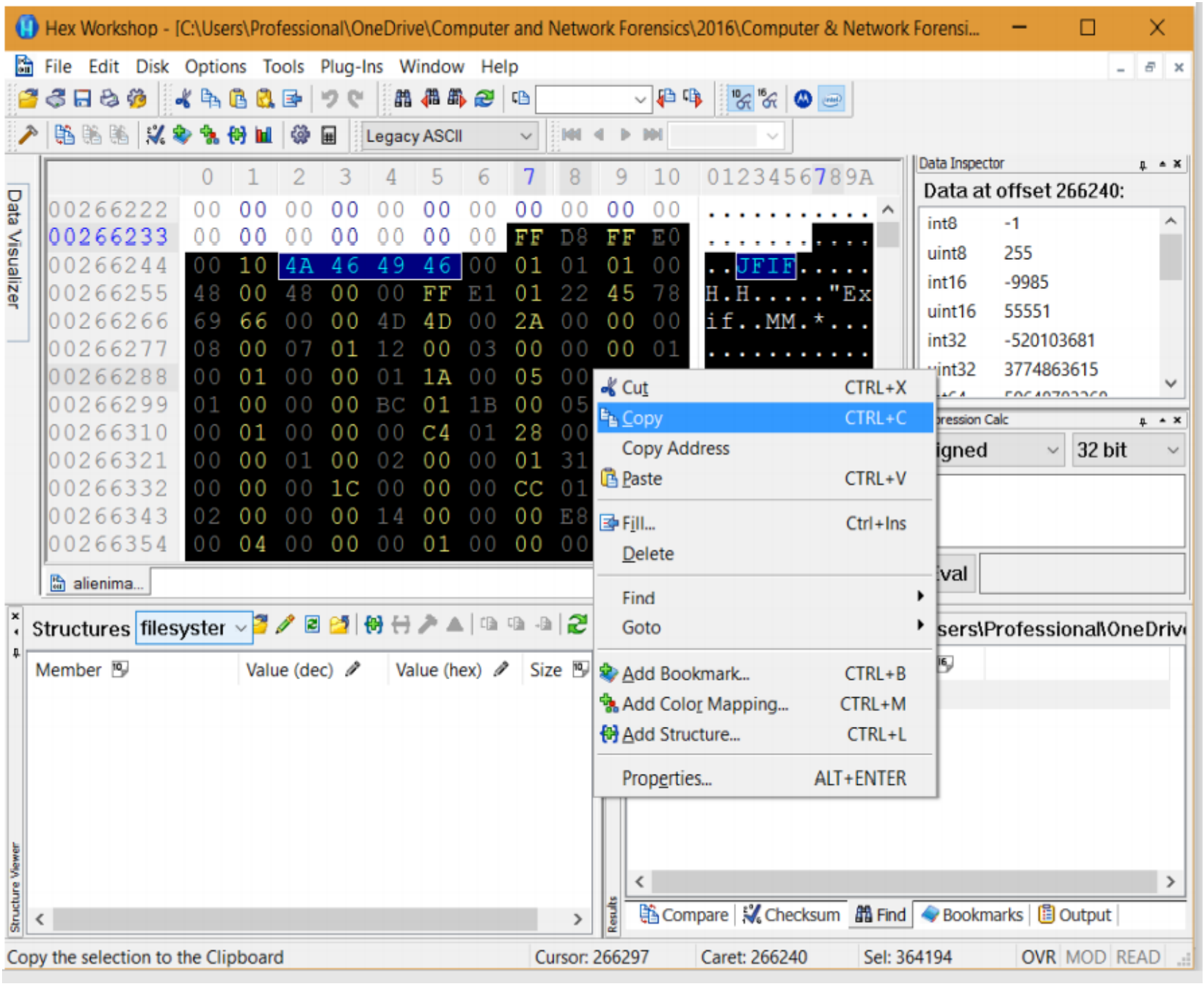
Click ‘OK’

Right click the select area and click Copy



Carve .jpeg files from alienimage.dd

Right click the select area and click Copy



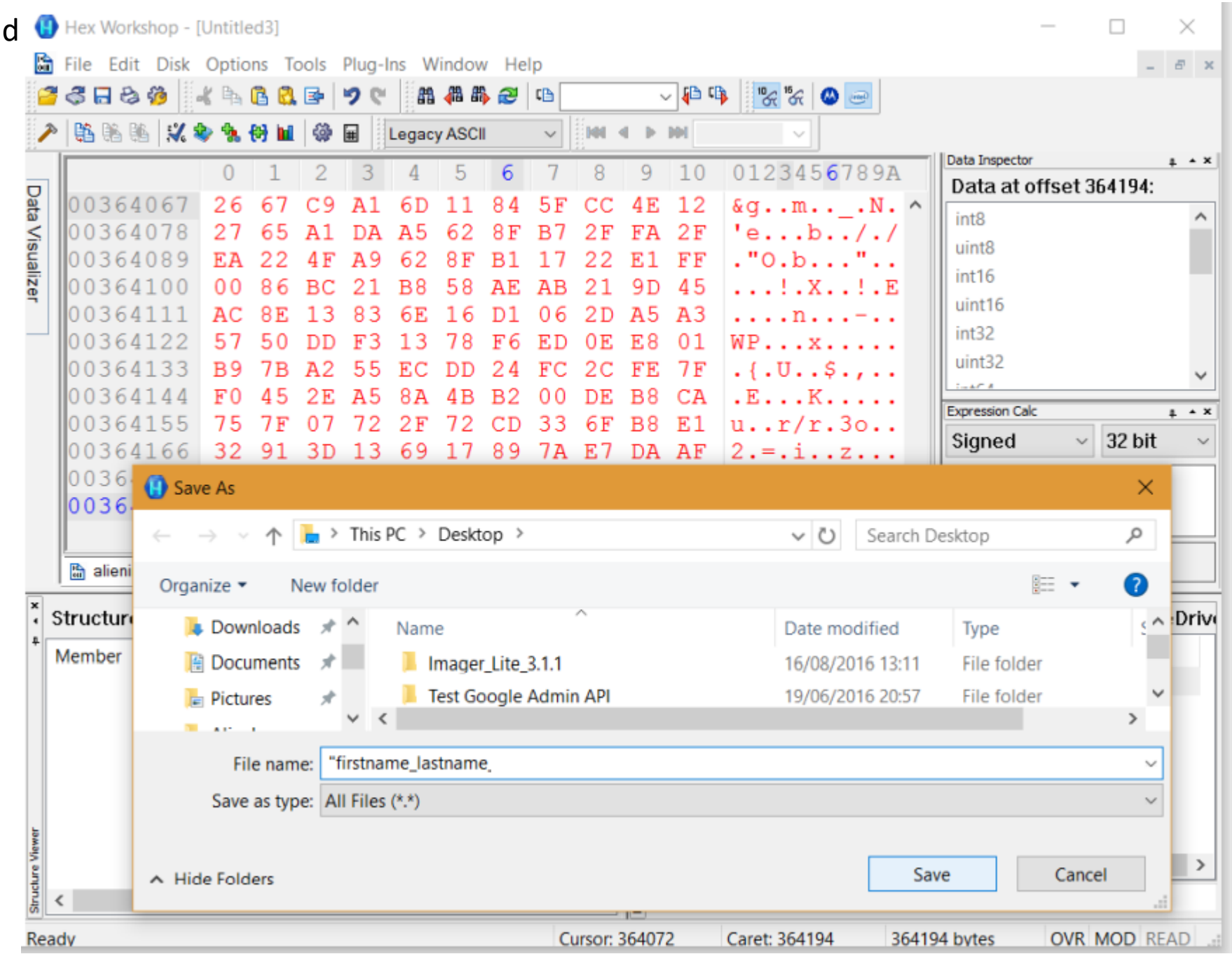
Carve .jpeg files from alienimage.dd

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

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?

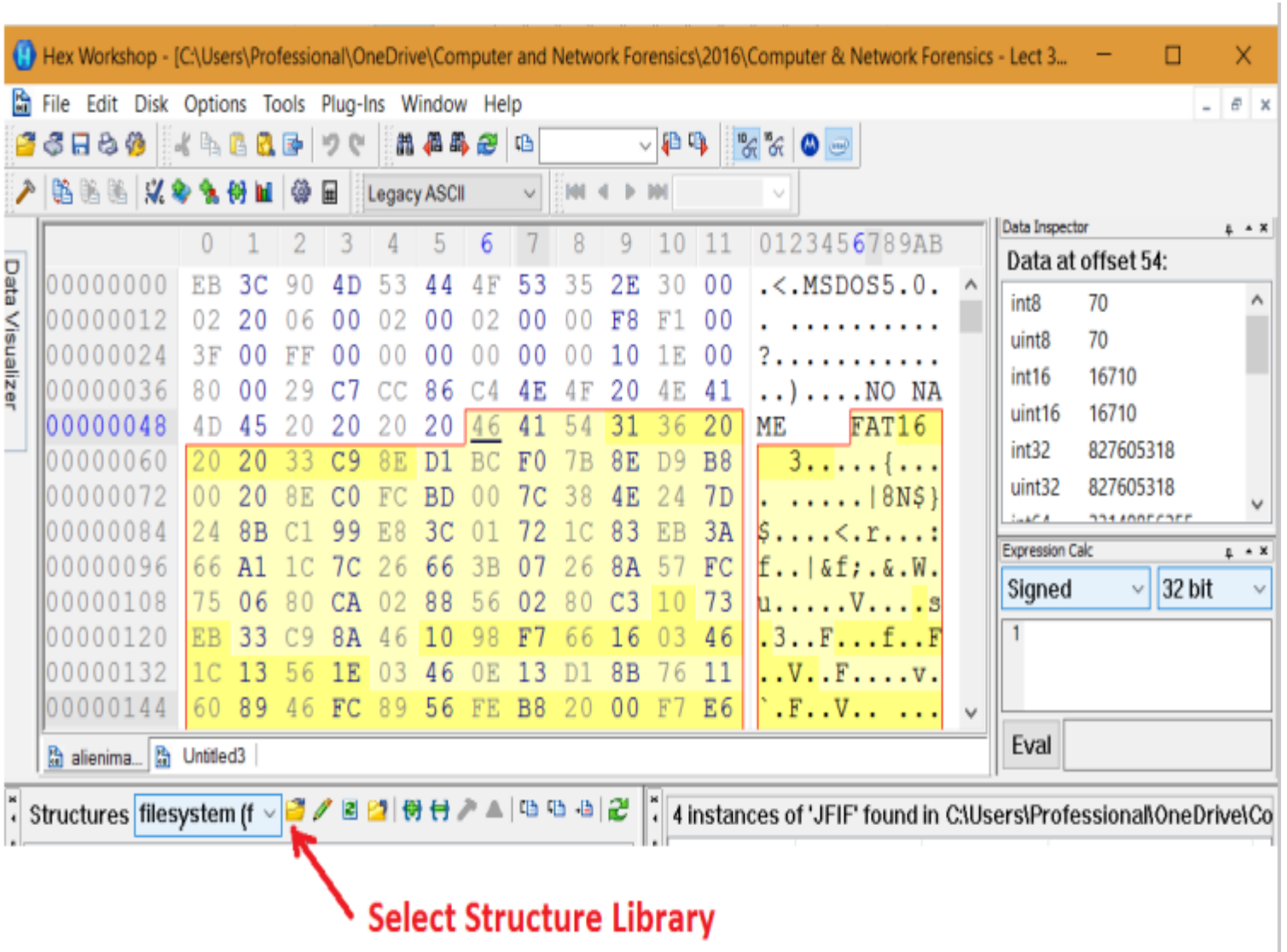
3. Try carving a .jpeg file from the alienimage.E01 image. Were you able to carve the file? Please provide a reason for your answer.

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 you 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