

# Computer & Network Forensics

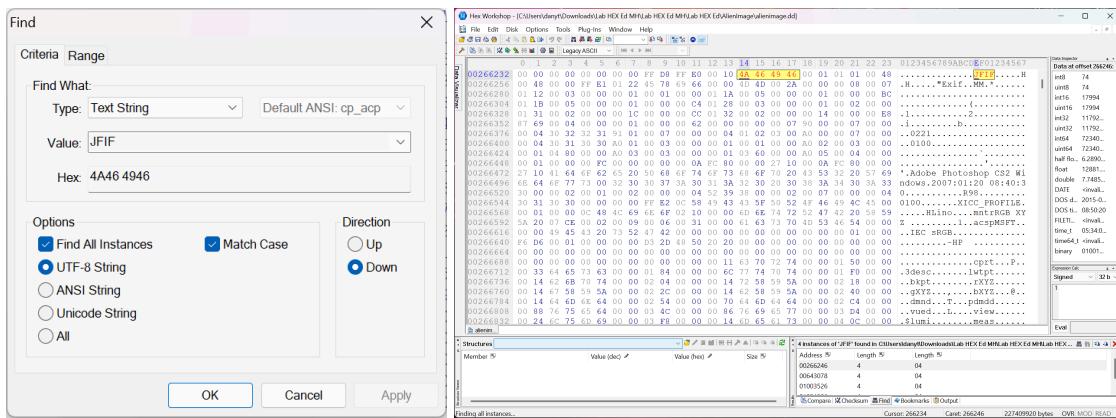
## Week 9 (Lab6)

### Using a Hex Editor to Carve a file

Carve .jpeg files from alienimage.dd

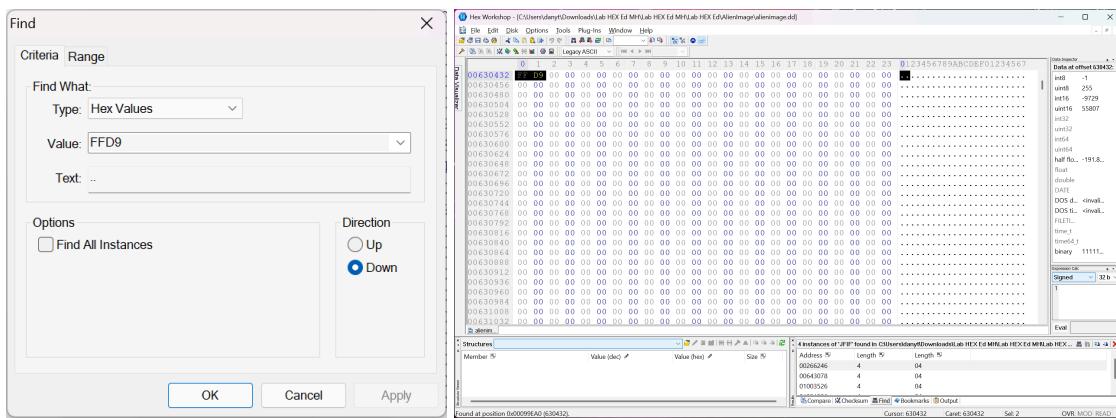
#### 1. Find the start of the file

##### Searching for 'JFIF' (Text String) – jpeg HEX Signature



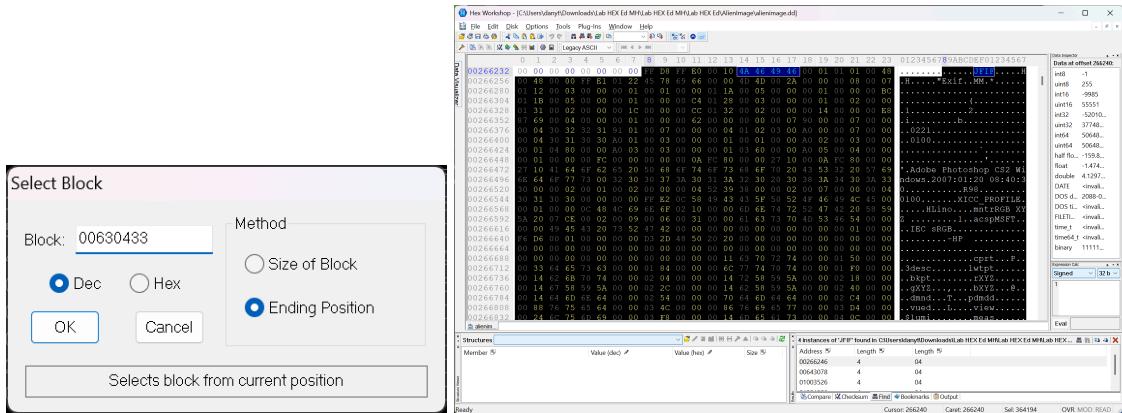
#### 2. Find the end of the file

##### Searching for 'FFD9' (HEX Value) – the tail of jpeg



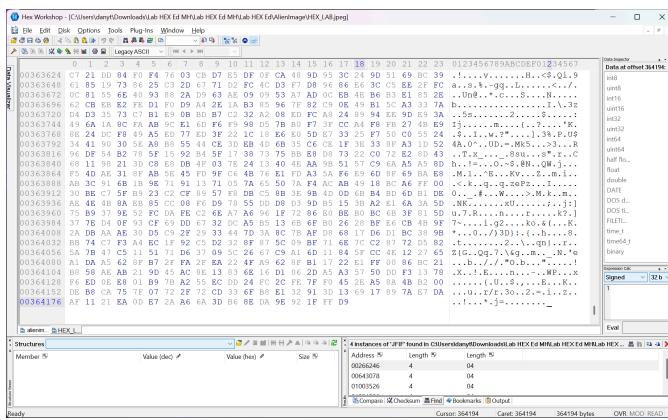
### 3. Click on Edit → Select Block

**At the start of the file ('JFIF') – Select Block**



### 4. Create a file from this HEX selection

**Copy this selected HEX into a new file and save (as `HEX_LAB.jpeg`)**



### 5. `HEX_LAB.jpeg`

**Open carved image file**



## Questions

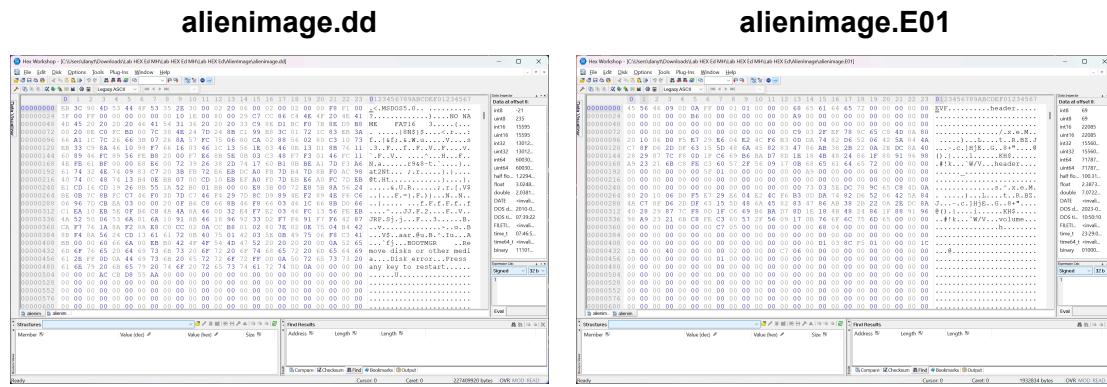
1. Write a definition of data carving

Data carving is a forensic technique used to recover files or fragments of files from raw disk data when file system structures (like file tables or directories) are missing or corrupted.

2. Convert alienimage.dd to alienimage.E01 using **FTK Imager** and view in **Hex Workshop**. What is different about the data this time?

The data in alienimage.E01 appears different because the E01 format includes additional metadata and uses compression, whereas alienimage.dd is a raw bit-by-bit copy of the disk. As a result, alienimage.E01 cannot be directly carved in the same way as alienimage.dd.

- The E01 format (EnCase evidence file) is a compressed and structured forensic image, not a raw disk copy.
- It contains metadata, checksums, and case information that FTK Imager adds to ensure integrity.
- The file content is encoded, so it no longer represents the direct sector-by-sector data of the original disk.

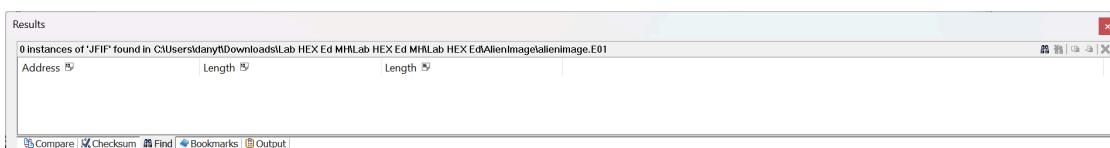


3. Try carving a .jpeg file from the alienimage.E01 image. Were you able to carve the file? Please provide a reason for your answer.

I was not able to carve a .jpeg file from the alienimage.E01 image because the E01 format does not store raw data directly. It compresses and structures data using EnCase's proprietary format, which hides file signatures like JFIF and FFD9 that are needed for manual carving.

- The E01 file is not raw binary data – it's a container for forensic information.
- JPEG signatures are buried inside the E01 encoding, not directly visible as in a .dd file.

### Zero findined results:



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

**OEM Name:** 00000057 char OemName[8] 16 3ÉŽ 8  
**Drive Number:** 00000118 int8 DriveNumber 16 10 1

The screenshot shows the Hex Workshop interface with the file alienimage.dd open. The left pane displays the hex dump of the file, and the right pane shows the data inspector. The OEM Name (00000057) and Drive Number (00000118) are highlighted with red boxes in the hex dump area.

Member	Type	Value (dec)	Value (hex)	Size
00000054 struct BOOTSECTOR_FAT32	...	512	512	
00000054 int8 jmp[3]	...	3	3	
00000057 char OemName[8]	char	16 3ÉŽ	8	
00000065 struct BPB_FAT32	...	53	53	

#### OEM Name

#### Drive Number

The screenshot shows the Hex Workshop interface with the file filesystem(filesystem.hsl) open. The left pane displays the hex dump of the file, and the right pane shows the data inspector. The OEM Name and Drive Number members are highlighted with red boxes in the hex dump area.

Member	Type	Value (dec)	Value (hex)	Size
00000054 struct BOOTSECTOR_FAT32	...	512	512	
00000054 int8 jmp[3]	...	3	3	
00000057 char OemName[8]	char	16 3ÉŽ	8	
00000065 struct BPB_FAT32	...	53	53	