

Computer & Network Forensics

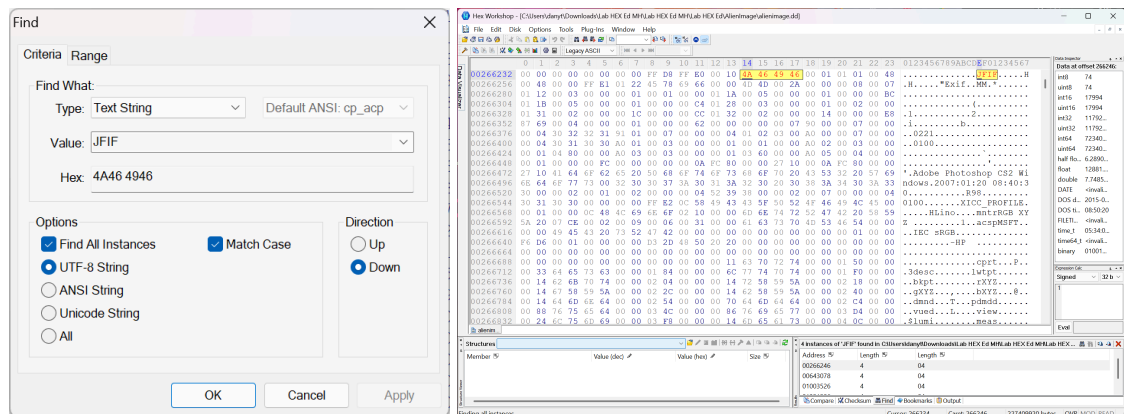
Week 9 (Lab6)

Using a Hex Editor to Carve a file

Carve .jpeg files from alienimage.dd

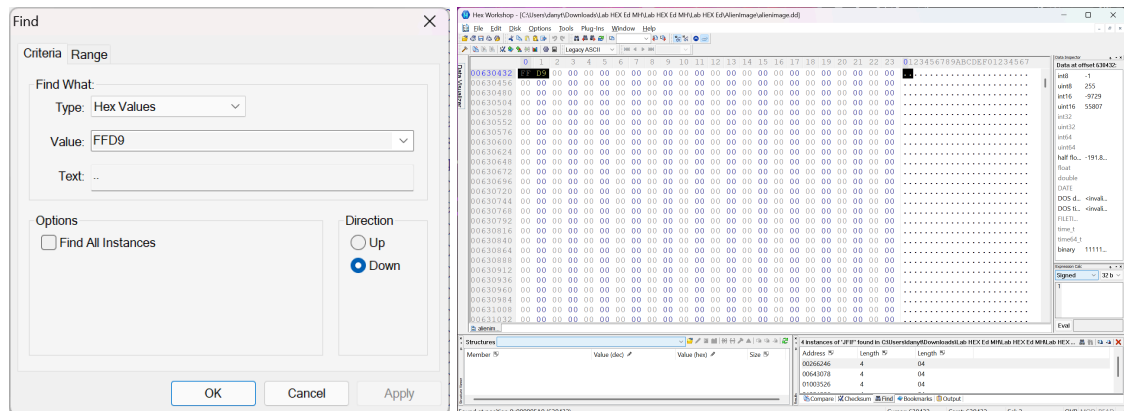
1. Find the start of the file

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



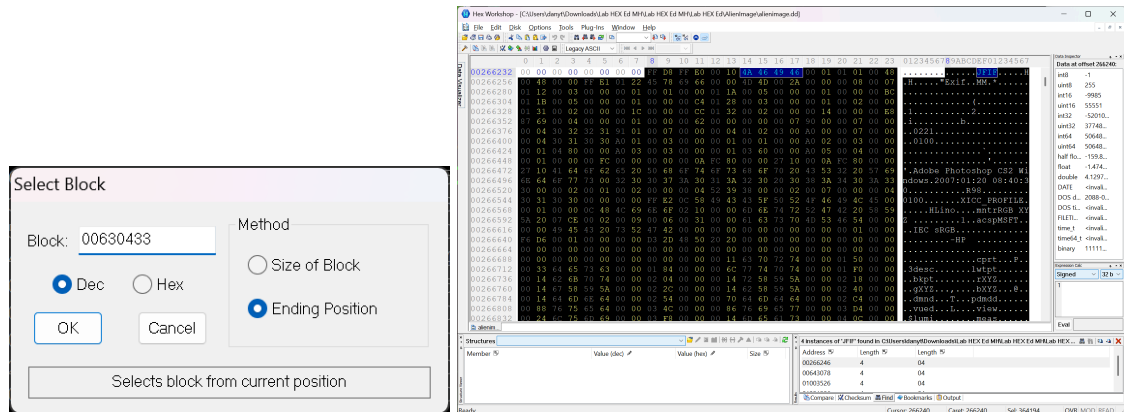
2. Find the end of the file

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



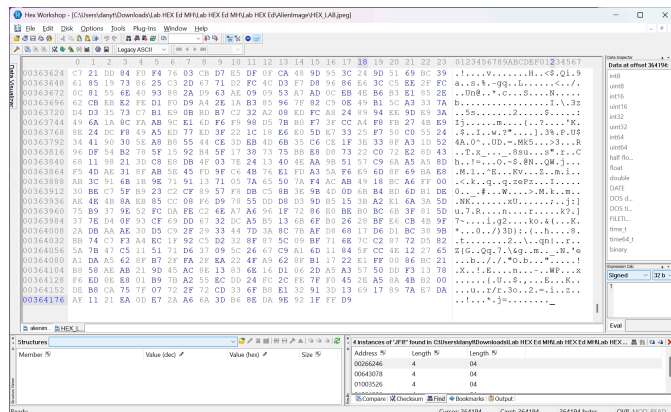
3. Click on Edit → Select Block

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

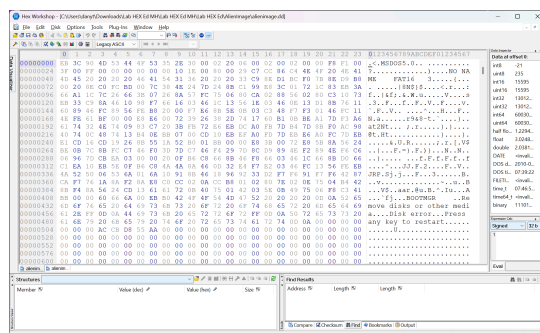
Data carving is a forensic technique used to recover files or fragments of files from raw disk data when file system structures (like file tables or directories) are missing or corrupted.

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

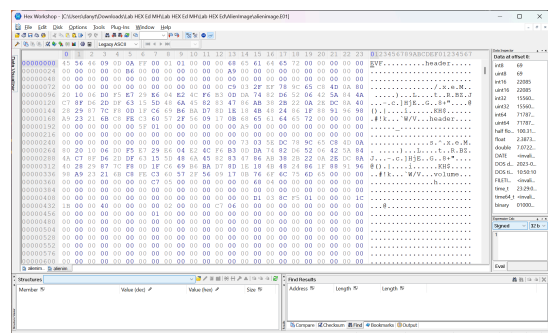
The data in `alienimage.E01` appears different because the E01 format includes additional metadata and uses compression, whereas `alienimage.dd` is a raw bit-by-bit copy of the disk. As a result, `alienimage.E01` cannot be directly carved in the same way as `alienimage.dd`.

- 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.

alienimage.dd



alienimage.E01

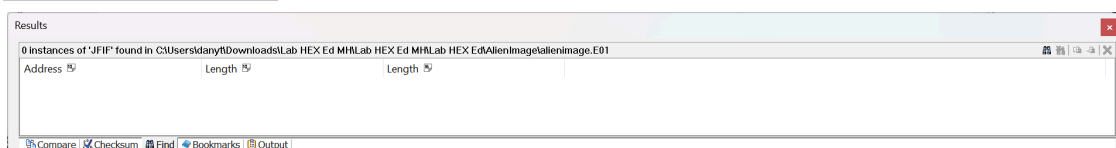


3. Try carving a `.jpeg` file from the `alienimage.E01` image. Were you able to carve the file? Please provide a reason for your answer.

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 findind 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

Hex Workshop - [C:\Users\danyt\Downloads\Lab HEX Ed MH\Lab HEX Ed MH\alienimage\alienimage.dd]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

0123456789ABCDEF01234567

00000000 EB 3C 90 4D 53 44 F5 53 35 2E 30 0D 02 06 00 02 00 00 00 F8 F1 00 .<.MSDOS5.0.....
00000024 3F 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ?.....2.....NO NA
00000048 4D 45 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ME FAT16 3.....
00000072 00 20 8E C0 FC BD 00 7C 39 4E 24 7D 24 8B C1 99 58 3C 01 72 1C 83 EB 3A18NS)\$.<.r...
00000096 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA 02 88 56 02 80 C3 10 73 f...l&f; &W.u...
00000120 EB 33 C9 8A 46 10 98 F7 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 .3.F...f...F...F...
00000144 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 C3 48 F7 F3 01 46 FC 11 .F.V...^...H...F...
00000168 4E FE 61 BF 00 00 E8 E6 00 72 39 FB 2E 6B DC 2D 74 17 60 B1 0B BE A1 7D F3 A6 N.a.....t968-t...
00000192 61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB D0 A0 FB 7D B4 7D 8B F0 AC 98 at2Nt...r...
00000216 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB EF A0 FD 7B EB E6 A0 FC 7D EB t.Ht...r...
00000240 E1 CD 16 CD 19 26 8B 55 1A 52 80 01 B8 00 00 E8 3B 00 72 E8 5B 8A 56 24 .&.U.R...r...[.V\$
00000264 BE 06 7C 8B FC C7 46 F0 3D 7D C7 46 F4 29 7D BC D9 49 4E F2 89 4E F6 C6 .|.F.=|.F...|.R...N...
00000288 06 96 7D CB EA 03 00 00 0F B6 C8 66 8B 46 F8 66 03 4C 6B D0 66 .|.f...f.F.f.F.f.F...
00000312 C1 EA 10 EB 5E 0F B6 C8 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB .|.J.J.F.2...F.V...
00000336 4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33 D7 F6 91 F7 F6 42 87 JRP.Sj...F...3...B...
00000360 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 02 80 7E 02 E5 75 04 B4 42 .v.....u..B...
00000384 B8 F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 .V\$.aar.@.B..Iu..A...
00000408 BB 00 00 00 66 6A 00 EB B0 42 4F 54 4D 47 52 20 20 00 0A 52 65 .fj...BOOTMGR...Re
00000432 6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 6F 72 FF 0A 72 65 73 73 20 move disks or other medi
00000456 61 2E FF 0A 64 69 73 6B 73 20 65 72 6F 72 FF 0A 72 65 73 73 20 a...Disk error...Press
00000480 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61 72 74 0A 00 00 00 00 any key to restart....
00000504 00 00 00 AC CB D8 55 AA 00 00 00 00 00 00 00 00 00 00 00 00U.....
00000528 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000552 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000576 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
alienim... alienim...

Structures (filesystem.hsl)

Member Value (dec) Value (hex) Size

00000054 struct BOOTSECTOR_FAT32 [-] 512

00000054 int8 jmp[3] 3

00000057 char OemName[8] 16 3ÉŽ

00000065 struct BPB_FAT32 [-] 8

Cursor: 54 Caret: 54 Sel: 5 OVR MOD READ

OEM Name

Drive Number

Hex Workshop - [C:\Users\danyt\Downloads\Lab HEX Ed MH\Lab HEX Ed MH\alienimage\alienimage.dd]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

0123456789ABCDEF01234567

00000000 EB 3C 90 4D 53 44 F5 53 35 2E 30 0D 02 06 00 02 00 00 00 F8 F1 00 .<.MSDOS5.0.....
00000024 3F 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ?.....2.....NO NA
00000048 4D 45 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ME FAT16 3.....
00000072 00 20 8E C0 FC BD 00 7C 39 4E 24 7D 24 8B C1 99 58 3C 01 72 1C 83 EB 3A18NS)\$.<.r...
00000096 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA 02 88 56 02 80 C3 10 73 f...l&f; &W.u...
00000120 EB 33 C9 8A 46 10 98 F7 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 .3.F...f...F...F...
00000144 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 C3 48 F7 F3 01 46 FC 11 .F.V...^...H...F...
00000168 4E FE 61 BF 00 00 E8 E6 00 72 39 FB 2E 6B DC 2D 74 17 60 B1 0B BE A1 7D F3 A6 N.a.....t968-t...
00000192 61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB D0 A0 FB 7D B4 7D 8B F0 AC 98 at2Nt...r...
00000216 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB EF A0 FD 7B EB E6 A0 FC 7D EB t.Ht...r...
00000240 E1 CD 16 CD 19 26 8B 55 1A 52 80 01 B8 00 00 E8 3B 00 72 E8 5B 8A 56 24 .&.U.R...r...[.V\$
00000264 BE 06 7C 8B FC C7 46 F0 3D 7D C7 46 F4 29 7D BC D9 49 4E F2 89 4E F6 C6 .|.F.=|.F...|.R...N...
00000288 06 96 7D CB EA 03 00 00 0F B6 C8 66 8B 46 F8 66 03 4C 6B D0 66 .|.f...f.F.f.F.f.F...
00000312 C1 EA 10 EB 5E 0F B6 C8 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB .|.J.J.F.2...F.V...
00000336 4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33 D7 F6 91 F7 F6 42 87 JRP.Sj...F...3...B...
00000360 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 02 80 7E 02 E5 75 04 B4 42 .v.....u..B...
00000384 B8 F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 .V\$.aar.@.B..Iu..A...
00000408 BB 00 00 00 66 6A 00 EB B0 42 4F 54 4D 47 52 20 20 00 0A 52 65 .fj...BOOTMGR...Re
00000432 6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 6F 72 FF 0A 72 65 73 73 20 move disks or other medi
00000456 61 2E FF 0A 64 69 73 6B 73 20 65 72 6F 72 FF 0A 72 65 73 73 20 a...Disk error...Press
00000480 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61 72 74 0A 00 00 00 00 any key to restart....
00000504 00 00 00 AC CB D8 55 AA 00 00 00 00 00 00 00 00 00 00 00 00U.....
00000528 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000552 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000576 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
alienim... alienim...

Structures (filesystem.hsl)

Member Value (dec) Value (hex) Size

00000054 struct BOOTSECTOR_FAT32 [-] 512

00000054 int8 jmp[3] 3

00000057 char OemName[8] 16 3ÉŽ

00000065 struct BPB_FAT32 [-] 8

Cursor: 54 Caret: 54 Sel: 5 OVR MOD READ

Hex Workshop - [C:\Users\danyt\Downloads\Lab HEX Ed MH\Lab HEX Ed MH\alienimage\alienimage.dd]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

0123456789ABCDEF01234567

00000000 EB 3C 90 4D 53 44 F5 53 35 2E 30 0D 02 06 00 02 00 00 00 F8 F1 00 .<.MSDOS5.0.....
00000024 3F 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ?.....2.....NO NA
00000048 4D 45 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ME FAT16 3.....
00000072 00 20 8E C0 FC BD 00 7C 39 4E 24 7D 24 8B C1 99 58 3C 01 72 1C 83 EB 3A18NS)\$.<.r...
00000096 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA 02 88 56 02 80 C3 10 73 f...l&f; &W.u...
00000120 EB 33 C9 8A 46 10 98 F7 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 .3.F...f...F...F...
00000144 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 C3 48 F7 F3 01 46 FC 11 .F.V...^...H...F...
00000168 4E FE 61 BF 00 00 E8 E6 00 72 39 FB 2E 6B DC 2D 74 17 60 B1 0B BE A1 7D F3 A6 N.a.....t968-t...
00000192 61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB D0 A0 FB 7D B4 7D 8B F0 AC 98 at2Nt...r...
00000216 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB EF A0 FD 7B EB E6 A0 FC 7D EB t.Ht...r...
00000240 E1 CD 16 CD 19 26 8B 55 1A 52 80 01 B8 00 00 E8 3B 00 72 E8 5B 8A 56 24 .&.U.R...r...[.V\$
00000264 BE 06 7C 8B FC C7 46 F0 3D 7D C7 46 F4 29 7D BC D9 49 4E F2 89 4E F6 C6 .|.F.=|.F...|.R...N...
00000288 06 96 7D CB EA 03 00 00 0F B6 C8 66 8B 46 F8 66 03 4C 6B D0 66 .|.f...f.F.f.F.f.F...
00000312 C1 EA 10 EB 5E 0F B6 C8 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB .|.J.J.F.2...F.V...
00000336 4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33 D7 F6 91 F7 F6 42 87 JRP.Sj...F...3...B...
00000360 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 02 80 7E 02 E5 75 04 B4 42 .v.....u..B...
00000384 B8 F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 .V\$.aar.@.B..Iu..A...
00000408 BB 00 00 00 66 6A 00 EB B0 42 4F 54 4D 47 52 20 20 00 0A 52 65 .fj...BOOTMGR...Re
00000432 6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 6F 72 FF 0A 72 65 73 73 20 move disks or other medi
00000456 61 2E FF 0A 64 69 73 6B 73 20 65 72 6F 72 FF 0A 72 65 73 73 20 a...Disk error...Press
00000480 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61 72 74 0A 00 00 00 00 any key to restart....
00000504 00 00 00 AC CB D8 55 AA 00 00 00 00 00 00 00 00 00 00 00 00U.....
00000528 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000552 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000576 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
alienim... alienim...

Structures (filesystem.hsl)

Member Value (dec) Value (hex) Size

00000054 struct BOOTSECTOR_FAT32 [-] 512

00000054 int8 jmp[3] 3

00000057 char OemName[8] 16 3ÉŽ

00000065 struct BPB_FAT32 [-] 8

Cursor: 54 Caret: 54 Sel: 5 OVR MOD READ