Experiment No. 3

Date of Performance (DOP): 30/07/2025
Date of Submission (DOS): 04/08/2025

3.1 Aim:

To understand and perform operations related to data storage including:

- Magic Numbers
- Extension Obfuscation
- Bit and Block Shifting
- Recovering a Deleted File
- File Carving

3.2 Lab Outcome:

By the end of this lab, students will be able to:

- Identify file types using magic numbers
- Demonstrate extension obfuscation and its detection
- Apply bit and block shifting techniques on file data
- Perform basic file recovery methods
- Conduct file carving to extract embedded files

3.3 Learning Objectives:

- Understand the concept of file signatures (magic numbers)
- Learn how file extensions can be manipulated and hidden

- Apply data manipulation techniques like bit and block shifting
- Practice recovering deleted files using forensic tools
- Learn the basics of file carving and apply them on disk images

3.4 Requirements:

- Operating System: Kali Linux / Windows with forensic tools
- Software Tools:
    - Hex Editor (e.g., Bless, HxD)
    - Foremost / Scalpel (for file carving)
    - PhotoRec / Recuva (for file recovery)
    - Command-line utilities (e.g., `xxd`, `file`)
- Sample files with known formats (JPEG, PDF, PNG, etc.)

3.5 Related Theory:

A) Magic Numbers:

A magic number is a constant numerical or text value used to identify a file format. It resides in the file header. For example:

- JPEG: `FF D8 FF E0`
- PDF: %PDF
- PNG: `89 50 4E 47`

Tools like `file` command in Linux use magic numbers to determine file types regardless of file extensions.

B) Extension Obfuscation:

Changing a file extension (e.g., `.exe` to `.jpg`) to disguise its true format. This technique is often used in malware to bypass detection. Magic numbers can help reveal the actual file type.

C) Bit and Block Shifting:

Bit shifting involves shifting bits of data to the left or right, altering the binary content of a file. Block shifting involves moving chunks of data within a file. These can be used for obfuscation or simple encryption.

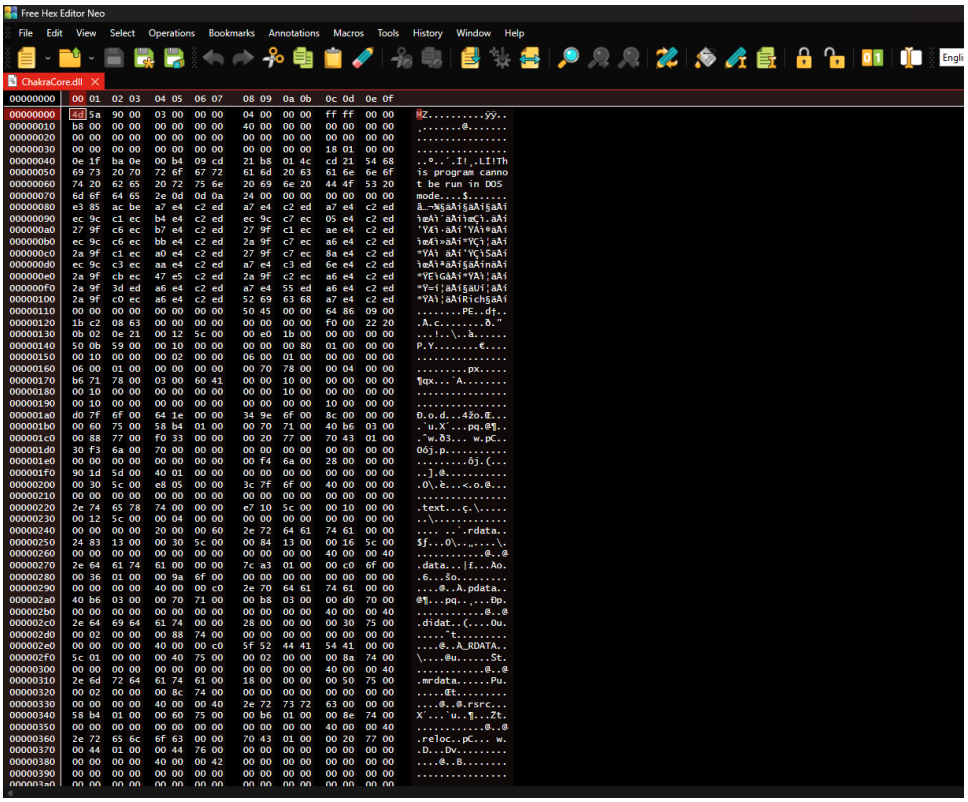
D) Recovering a Deleted File:

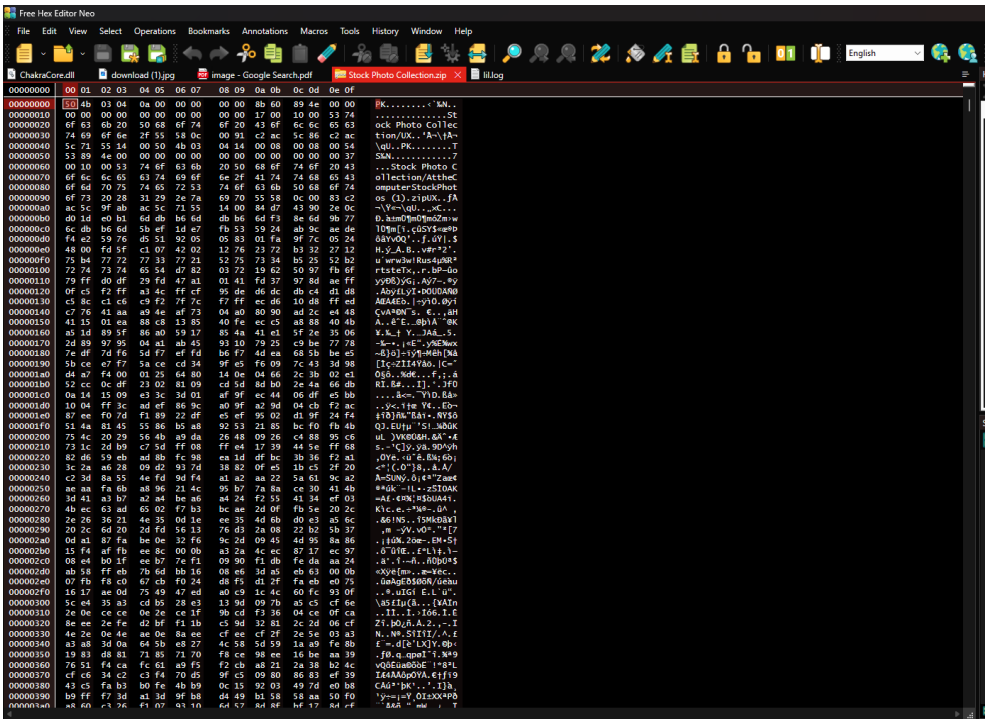
Files deleted from a filesystem are often recoverable unless overwritten. Tools like `PhotoRec` or `Recuva` scan raw disk space to recover such files based on known file signatures.

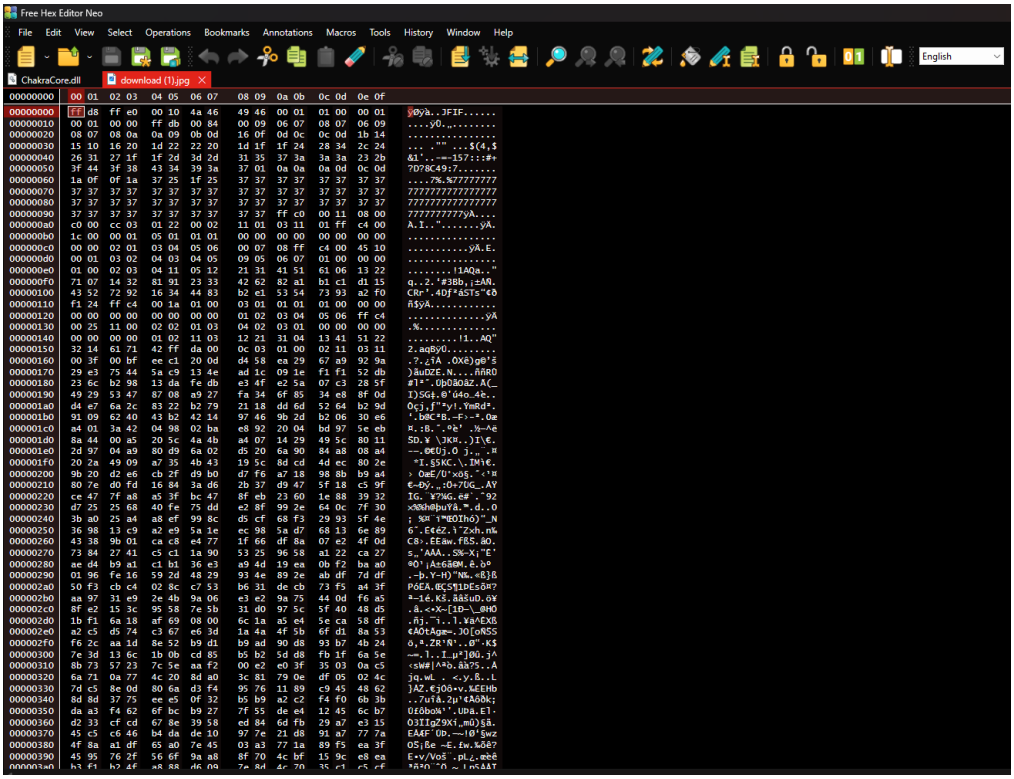
E) File Carving:

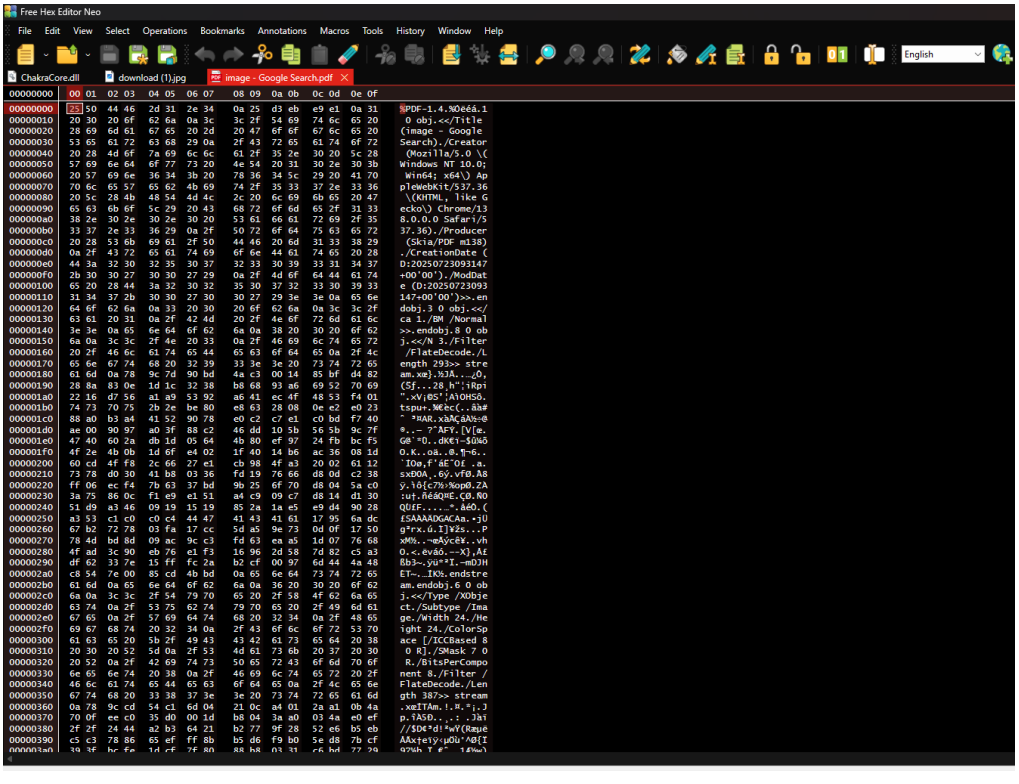
File carving is the process of extracting files from raw disk images without relying on file system metadata. Tools like `foremost` or `scalpel` can scan a binary image and extract files using header/footer patterns.

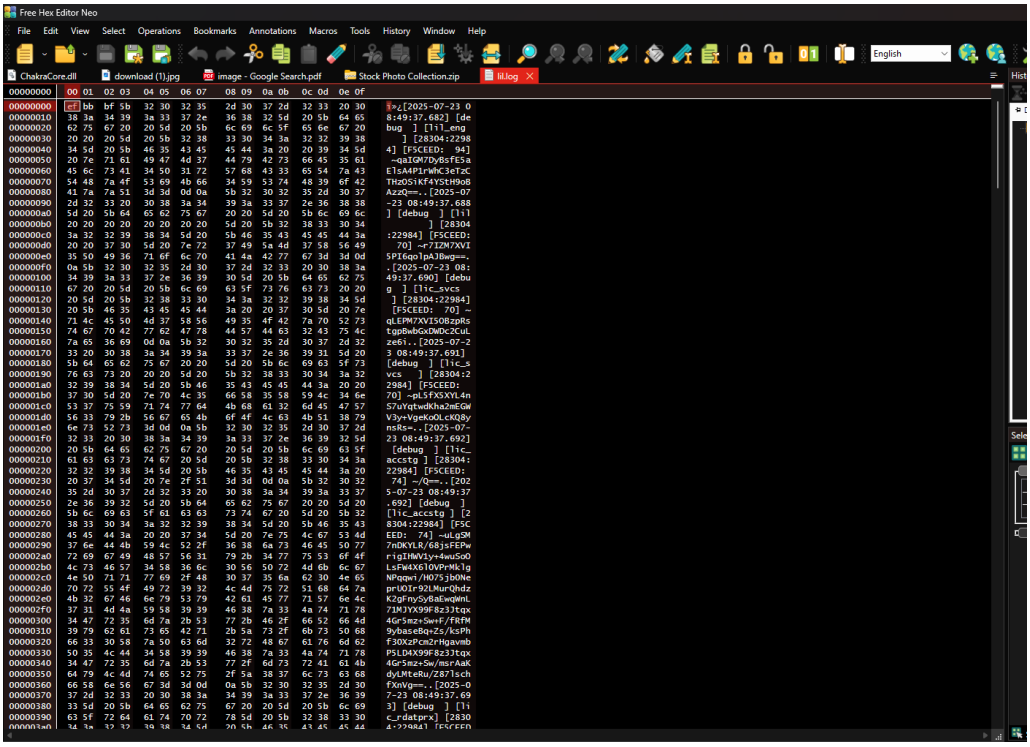
3.6 Output:


Free Hex Editor Neo
File Edit View Select Operations Bookmarks Annotations Macros Tools History Window Help
ChakraCore.dll

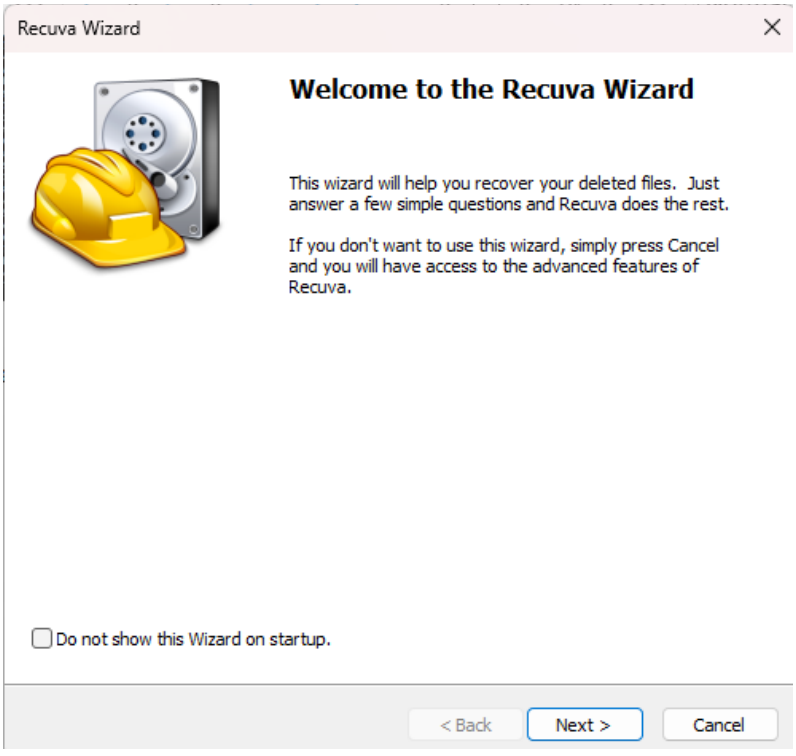

Free Hex Editor Neo
File Edit View Select Operations Bookmarks Annotations Macros Tools History Window Help
ChakraCore.dll
download (1).jpg
image - Google Search.pdf
Stock Photo Collection.zip
lil.log

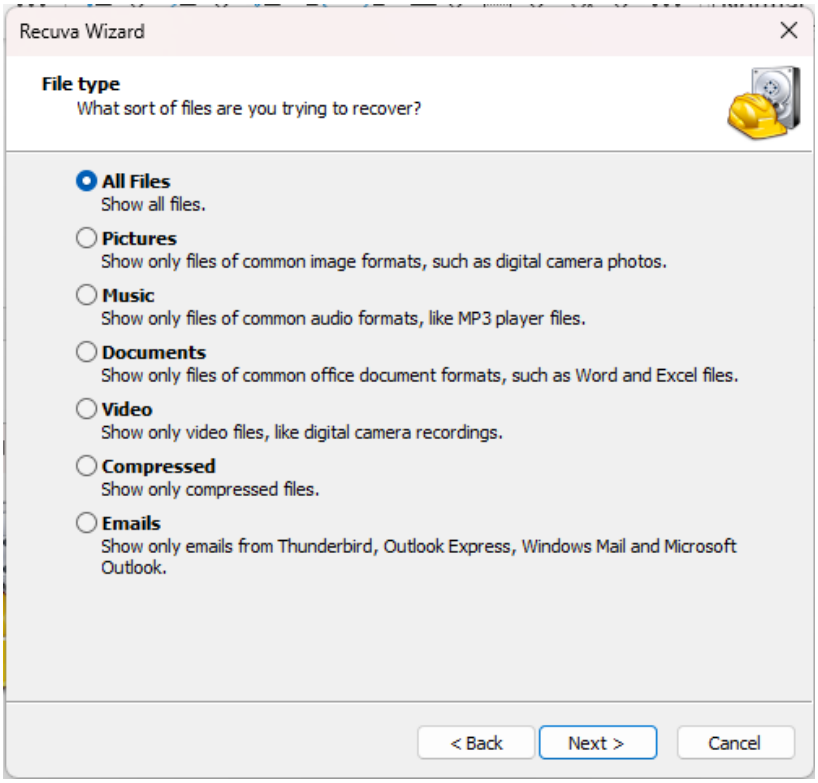

Free Hex Editor Neo
File Edit View Select Operations Bookmarks Annotations Macros Tools History Window Help
English
ChakraCore.dll
download (1).jpg
00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01
00000010 00 01 00 00 ff db 00 84 00 09 06 07 08 07 06 09
00000020 08 07 08 0a 0a 09 0b 0d 16 0f 0d 0c 0c 0d 1b 14
00000030 15 10 16 20 1d 22 22 20 1d 1f 1f 24 28 34 2c 24
00000040 26 31 27 1f 1f 2d 3d 2d 31 35 37 3a 3a 3a 23 2b
00000050 3f 44 3f 38 43 34 39 3a 37 01 0a 0a 0a 0d 0c 0d
00000060 1a 0f 0f 1a 37 25 1f 25 37 37 37 37 37 37 37 37
00000070 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37
00000080 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37
00000090 37 37 37 37 37 37 37 37 37 ff c0 00 11 08 00
000000a0 c0 00 cc 03 01 22 00 02 11 01 03 11 01 ff c4 00
000000b0 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00
000000c0 00 00 02 01 03 04 05 06 00 07 08 ff c4 00 45 10
000000d0 00 01 03 02 04 03 04 05 09 05 06 07 01 00 00 00
000000e0 01 00 02 03 04 11 05 12 21 31 41 51 61 06 13 22
000000f0 71 07 14 32 81 91 23 33 42 62 82 a1 b1 c1 d1 15
00000100 43 52 72 92 16 34 44 83 b2 e1 53 54 73 93 a2 f0
00000110 f1 24 ff c4 00 1a 01 00 03 01 01 01 01 00 00 00
00000120 00 00 00 00 00 00 01 02 03 04 05 06 ff c4
00000130 00 25 11 00 02 02 01 03 04 02 03 01 00 00 00 00
00000140 00 00 00 00 01 02 11 03 12 21 31 04 13 41 51 22
00000150 32 14 61 71 42 ff da 00 0c 03 01 00 02 11 03 11
00000160 00 3f 00 bf ee c1 20 0d d4 58 ea 29 67 a9 92 9a
00000170 29 e3 75 4e c9 13 4e ad 1c 09 1e f1 f1 52 db
00000180 23 6c b2 98 13 da fe db e3 4f e2 5a 07 c3 28 5f
00000190 49 29 53 47 87 08 a9 27 fa 34 6f 85 34 e8 8f 0d
000001a0 d4 e7 6a 2c 83 22 b2 79 21 18 dd 6d 52 64 b2 9d
000001b0 91 09 62 40 43 b2 42 14 97 46 9b 2d b2 06 30 e6
000001c0 a4 01 3a 42 04 98 02 ba e8 92 20 04 bd 97 5e eb
000001d0 8a 44 00 a5 20 5c 4a 4b a4 07 14 29 49 5c 80 11
000001e0 2d 97 04 a9 80 d9 6a 02 d5 20 6a 90 84 a8 08 a4
000001f0 20 2a 49 09 a7 35 4b 43 19 5c 8d cd 4d ec 80 2e
00000200 9b 20 d2 e6 cb 2f d9 b0 d7 f6 a7 18 98 8b b9 a4
00000210 80 7e d0 fd 16 84 3a d6 2b 37 d9 47 5f 18 c5 9f
00000220 ce 47 7f a8 a5 3f bc 47 8f eb 23 60 1e 88 39 32
00000230 d7 25 25 68 40 fe 75 dd e2 8f 99 2e 64 0c 7f 30
00000240 3b a0 25 a4 a8 ef 99 8c d5 cf 68 f3 29 93 5f 4e
00000250 36 98 13 c9 a2 e9 5a 1e ec 98 5a d7 68 13 6e 89
00000260 43 38 9b 01 ca c8 e4 77 1f 66 df 8a 07 e2 4f 0d
00000270 73 84 27 41 c3 c1 1a 90 53 25 96 58 a1 22 ca 27
00000280 ae d4 b9 a1 c1 b1 36 e3 a9 4d 19 ea 0b f2 ba a0
00000290 01 96 fe 16 59 2d 48 29 93 4e 89 2e ab df 7d df
000002a0 50 f3 cb c4 02 8c c7 53 b6 31 de cb 73 f5 a4 3f
000002b0 aa 97 31 e9 2e 4b 9a 06 e3 e2 9a 75 44 0d f6 a5
000002c0 8f e2 15 3c 95 58 7e 5b 31 d0 97 5c 5f 40 48 d5
000002d0 1b f1 6a 18 af 69 08 00 6c 1a a5 e4 5e ca 58 df
000002e0 a2 c5 d5 74 c3 67 e6 3d 1a 4a 4f 5b 6f d1 8a 53
000002f0 f6 2c aa 1d 8e 52 b9 d1 b9 ad 90 d8 93 b7 4b 24
00000300 7e 3d 13 6c 1b 0b cd 85 b5 b2 5d d8 fb 1f 6a 5e
00000310 8b 73 57 23 7c 5e aa f2 00 e2 ed 3f 35 03 0a c3
00000320 6a 71 0a 77 4c 20 8d a0 3c 81 79 0e df 05 02 4c
00000330 7d c5 8e 0d 80 6a d3 f4 95 76 11 89 c9 45 48 62
00000340 8d 8d 37 75 ee e5 0f 32 b5 b9 a2 c2 f4 f0 6b 3b
00000350 da a3 f4 62 6f bc b9 27 7f 55 de e4 12 45 6c b7
00000360 d2 33 cf cd 67 8e 39 58 ed 84 6d fb 29 a7 e3 15
00000370 45 c5 c6 46 b4 da de 10 97 7e 21 d8 91 a7 77 7a
00000380 4f 8a a1 df 65 a0 7e 45 03 a3 77 1a 89 f5 ea 3f
00000390 45 95 76 2f 56 6f 9a a8 8f 70 4c bf 15 9c e8 ea
000003a0 b3 f1 b2 4f a8 88 d6 09 7e 8d 4c 70 35 c1 c5 cf

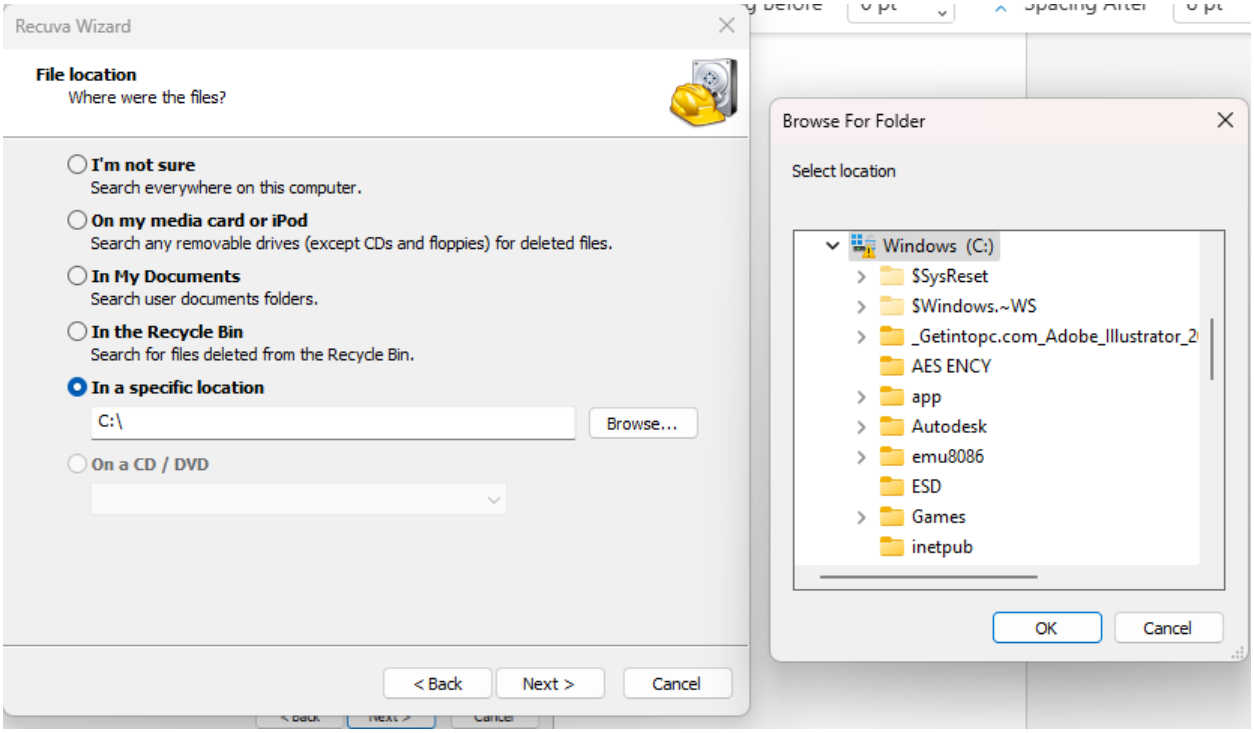

Free Hex Editor Neo
File Edit View Select Operations Bookmarks Annotations Macros Tools History Window Help
English
ChakraCore.dll
download (1).jpg
image - Google Search.pdf
00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 25 50 44 46 2d 31 2e 34 0a 25 d3 eb e9 e1 0a 31
00000010 20 30 20 6f 62 6a 0a 3c 3c 2f 54 69 74 6c 65 20
00000020 28 69 6d 61 67 65 20 2d 20 47 6f 6f 67 6c 65 20
00000030 53 65 61 72 63 68 29 0a 2f 43 72 65 61 74 6f 72
00000040 20 28 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 5c 28
00000050 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b
00000060 20 57 69 6e 36 34 3b 20 78 36 34 5c 29 20 41 70
00000070 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36
00000080 20 5c 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47
00000090 65 63 6b 6f 5c 29 20 43 68 72 6f 6d 65 2f 31 33
000000a0 38 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 35
000000b0 33 37 2e 33 36 29 0a 2f 50 72 6f 64 75 63 65 72
000000c0 20 28 53 6b 69 61 2f 50 44 46 20 6d 31 33 38 29
000000d0 0a 2f 43 72 65 61 74 69 6f 6e 44 61 74 65 20 28
000000e0 44 3a 32 30 32 35 30 37 32 33 30 39 33 31 34 37
000000f0 2b 30 30 27 30 30 27 29 0a 2f 4d 6f 64 44 61 74
00000100 65 20 28 44 3a 32 30 32 35 30 37 32 33 30 39 33
00000110 31 34 37 2b 30 30 27 30 30 27 29 3e 3e 0a 65 6e
00000120 64 6f 62 6a 0a 33 20 30 20 6f 62 6a 0a 3c 3c 2f
00000130 63 61 20 31 0a 2f 42 4d 20 2f 4e 6f 72 6d 61 6c
00000140 3e 3e 0a 65 6e 64 6f 62 6a 0a 38 20 30 20 6f 62
00000150 6a 0a 3c 3c 2f 4e 20 33 0a 2f 46 69 6c 74 65 72
00000160 20 2f 46 6c 61 74 65 44 65 63 6f 64 65 0a 2f 4c
00000170 65 6e 67 74 68 20 32 39 33 3e 3e 20 73 74 72 65
00000180 61 6d 0a 78 9c 7d 90 bd 4a c3 00 14 85 bf d4 82
00000190 28 8a 83 0e 1d 1c 32 38 b8 68 93 a6 69 52 70 69
000001a0 22 16 d7 56 a1 a9 53 92 a6 41 ec 4f 48 53 f4 01
000001b0 74 73 70 75 2b 2e be 80 e8 63 28 08 0e e2 e0 23
000001c0 88 a0 b3 a4 41 52 90 78 e0 c2 c7 e1 c0 bd f7 40
000001d0 ae 00 90 97 a0 3f 88 c2 46 dd 10 5b 56 5b 9c 7f
000001e0 47 40 60 2a db 1d 1c 64 4b 80 ef 97 24 fb bc f5
000001f0 4f 2e 4b 0b 1d 6f e4 02 1f 40 14 b6 ac 36 08 1d
00000200 60 cd 4f f8 2c 66 27 e1 cb 98 4f a3 20 02 61 12
00000210 73 78 d0 30 41 b8 03 36 fd 19 76 66 d8 0d c2 38
00000220 ff 06 ec f4 7b 63 37 bd 9b 25 6f 70 d8 04 5a c0
00000230 3a 75 86 0c f1 e9 e1 51 a4 c0 09 c7 d8 14 d1 30
00000240 51 d9 a3 46 09 19 15 19 85 2a 1a e5 e9 d4 90 28
00000250 a3 53 c1 c0 c0 c4 44 47 41 43 41 61 17 95 6a dc
00000260 67 b2 72 78 03 fa 17 cc 5d a5 9e 73 0d 0f 17 50
00000270 78 4d bd 8d 09 ac 9c c3 fd 63 ea a5 1d 07 76 68
00000280 4f ad 3c 90 eb 76 e1 f3 16 96 2d 58 7d 82 c5 a3
00000290 df 62 33 7e 15 ff fc 2a b2 cf 00 97 6d 44 4a 48
000002a0 c8 54 7e 00 85 cd 4b bd 0a 65 6e 64 73 74 72 65
000002b0 61 6d 0a 65 6e 64 6f 62 6a 0a 36 20 30 20 6f 62
000002c0 6a 0a 3c 3c 2f 54 79 70 65 20 2f 58 4f 62 6a 65
000002d0 63 74 0a 2f 53 75 62 74 79 70 65 20 2f 49 6d 61
000002e0 67 65 0a 2f 57 69 64 74 68 20 32 34 0a 2f 48 65
000002f0 69 67 68 74 20 32 34 0a 2f 43 6f 6c 6f 72 53 70
00000300 61 63 65 20 5b 2f 49 43 43 42 61 73 65 64 20 38
00000310 20 30 20 52 5d 0a 2f 53 4d 61 73 6b 20 37 20 30
00000320 20 52 0a 2f 42 69 74 73 50 65 72 43 6f 6d 70 6f
00000330 6e 65 6e 74 20 38 0a 2f 46 69 6c 74 65 72 20 2f
00000340 46 6c 61 74 65 44 65 63 6f 64 65 0a 2f 4c 65 6e
00000350 67 74 68 20 33 38 37 3e 3e 20 73 74 72 65 61 6d
00000360 0a 78 9c cd 54 c1 6d 04 21 0c a4 01 2a a1 0b 4a
00000370 70 0f ee c0 35 d0 00 1d b8 04 3a a0 03 4a e0 ef
00000380 2f 2f 24 44 a2 b3 64 21 b2 77 9f 28 52 e6 b5 eb
00000390 c5 c3 78 86 65 ef ff 8b b5 d6 f9 b0 5e d8 7b cf

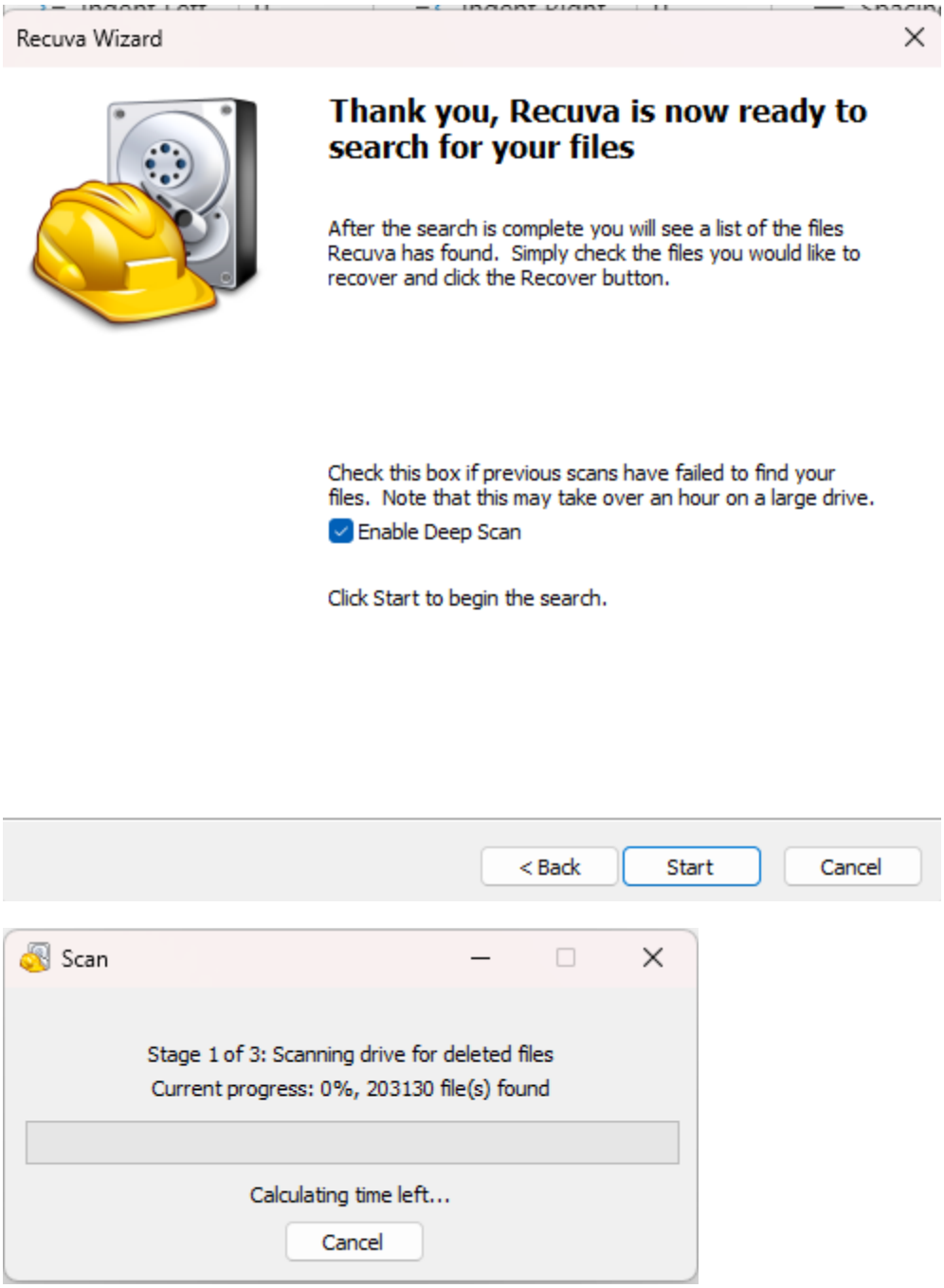


File Carving and recovery

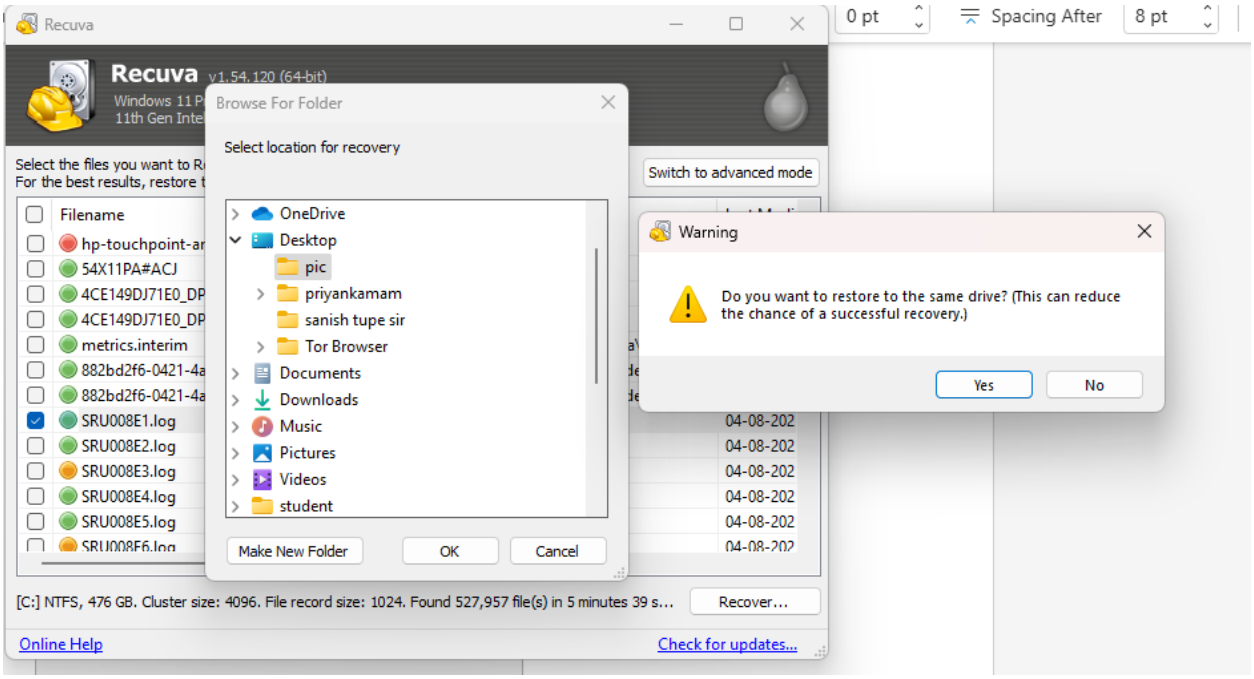


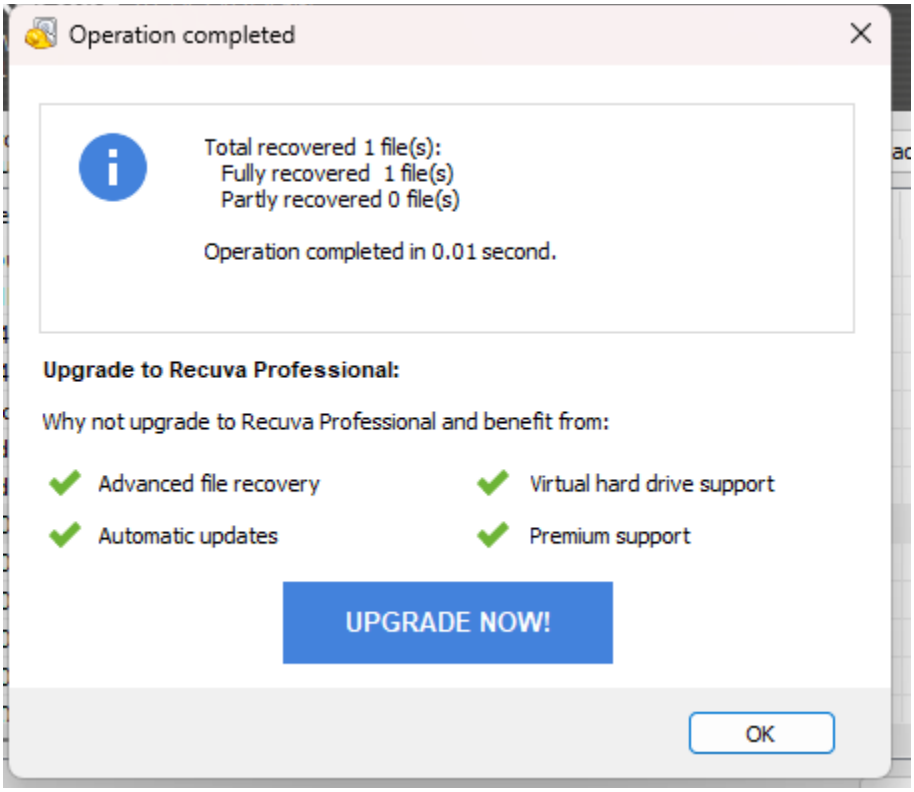

Recuva Wizard
File type
What sort of files are you trying to recover?
All Files
Show all files.
Pictures
Show only files of common image formats, such as digital camera photos.
Music
Show only files of common audio formats, like MP3 player files.
Documents
Show only files of common office document formats, such as Word and Excel files.
Video
Show only video files, like digital camera recordings.
Compressed
Show only compressed files.
Emails
Show only emails from Thunderbird, Outlook Express, Windows Mail and Microsoft Outlook.
< Back
Next >
Cancel

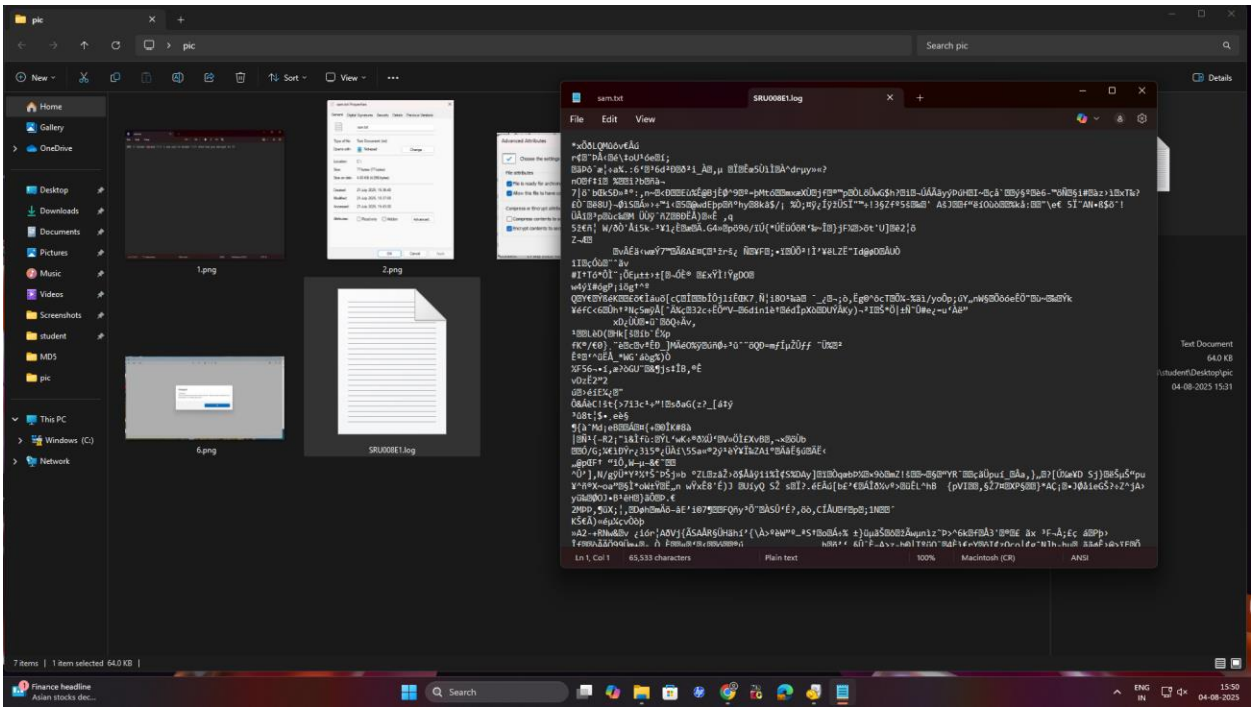

Recuva Wizard
File location
Where were the files?
I'm not sure
Search everywhere on this computer.
On my media card or iPod
Search any removable drives (except CDs and floppies) for deleted files.
In My Documents
Search user documents folders.
In the Recycle Bin
Search for files deleted from the Recycle Bin.
In a specific location
C:\
Browse...
On a CD / DVD
< Back
Next >
Cancel
Browse For Folder
Select location
Windows (C:)
$SysReset
$Windows.~WS
_Getintopc.com_Adobe_Illustrator_2
AES ENCY
app
Autodesk
emu8086
ESD
Games
inetpub
OK
Cancel


Recuva Wizard
Thank you, Recuva is now ready to search for your files
After the search is complete you will see a list of the files Recuva has found. Simply check the files you would like to recover and click the Recover button.
Check this box if previous scans have failed to find your files. Note that this may take over an hour on a large drive.
Enable Deep Scan
Click Start to begin the search.
< Back
Start
Cancel

Scan
Stage 1 of 3: Scanning drive for deleted files
Current progress: 0%, 203130 file(s) found
Calculating time left...
Cancel


Recuva
Recuva v1.54.120 (64-bit)
Browse For Folder
Select location for recovery
OneDrive
Desktop
pic
priyankamam
sanish tupe sir
Tor Browser
Documents
Downloads
Music
Pictures
Videos
student
Make New Folder
OK
Cancel
Switch to advanced mode
Filename
Warning
Do you want to restore to the same drive? (This can reduce the chance of a successful recovery.)
Yes
No
[C:] NTFS, 476 GB. Cluster size: 4096. File record size: 1024. Found 527,957 file(s) in 5 minutes 39 s...
Recover...
Online Help
Check for updates...
0 pt
Spacing After
8 pt


Operation completed
Total recovered 1 file(s):
Fully recovered 1 file(s)
Partly recovered 0 file(s)
Operation completed in 0.01 second.
Upgrade to Recuva Professional:
Why not upgrade to Recuva Professional and benefit from:
Advanced file recovery
Virtual hard drive support
Automatic updates
Premium support
UPGRADE NOW!
OK



3.7 Conclusion:

This experiment demonstrated how file types can be identified through their headers, regardless of extensions. It explored how malicious actors may use obfuscation techniques and how forensic tools can recover or carve deleted/hidden data. Understanding these core forensic methods is essential in digital investigations and cybersecurity.