DIGITAL FORENSIC

Assignment Report

By:

[Putri Anastasya]

[001202200131]

PRESIDENT UNIVERSITY

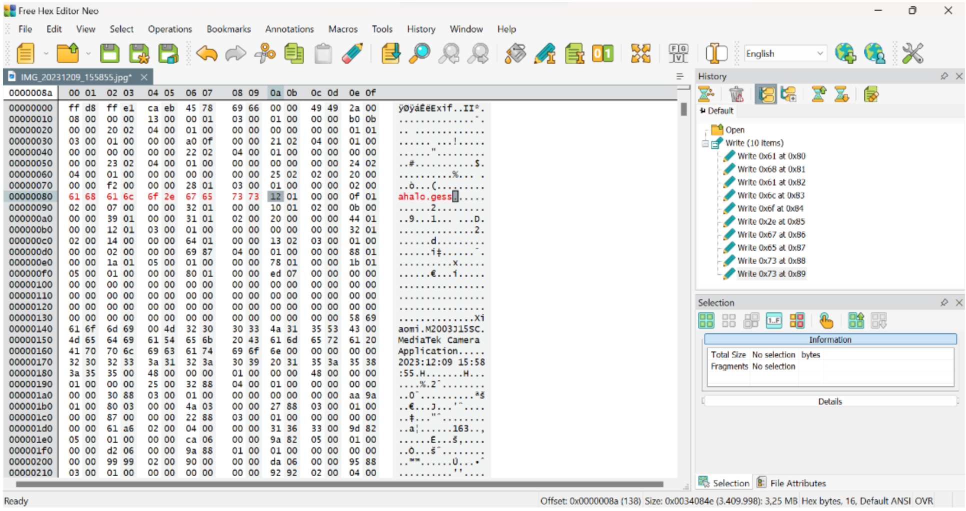
Faculty of Computing

Information Technology Study Program

2023-2

1. Hex Editor Neo

First, insert a photo in hex editor with a size between 3 to 5 MB. Select one of the columns on the right, except column one. Then insert a hidden message.


Free Hex Editor Neo
File Edit View Select Operations Bookmarks Annotations Macros Tools History Window Help
English
IMG_20231209_155855.jpg*

```
0000008a  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f
00000000  ff d8  ff e1  ca eb  45 78   69 66  00 00  49 49  2a 00   ÿØÿáÊëExif..II*.
00000010  08 00  00 00  13 00  00 01   03 00  01 00  00 00  b0 0b   ..............°.
00000020  00 00  20 02  04 00  01 00   00 00  00 00  00 00  01 01   .. .............
00000030  03 00  01 00  00 00  a0 0f   00 00  21 02  04 00  01 00   ...... ...!.....
00000040  00 00  00 00  00 00  22 02   04 00  01 00  00 00  00 00   ......".........
00000050  00 00  23 02  04 00  01 00   00 00  00 00  00 00  24 02   ..#...........$.
00000060  04 00  01 00  00 00  00 00   00 00  25 02  02 00  20 00   ..........%... .
00000070  00 00  f2 00  00 00  28 01   03 00  01 00  00 00  02 00   ..ò...(.........
00000080  61 68  61 6c  6f 2e  67 65   73 73  12 01  00 00  0f 01   ahalo.gess......
00000090  02 00  07 00  00 00  32 01   00 00  10 01  02 00  0b 00   ......2.........
000000a0  00 00  39 01  00 00  31 01   02 00  20 00  00 00  44 01   ..9...1... ...D.
000000b0  00 00  12 01  03 00  01 00   00 00  00 00  00 00  32 01   ..............2.
000000c0  02 00  14 00  00 00  64 01   00 00  13 02  03 00  01 00   ......d.........
000000d0  00 00  02 00  00 00  69 87   04 00  01 00  00 00  88 01   ......i‡......ˆ.
000000e0  00 00  1a 01  05 00  01 00   00 00  78 01  00 00  1b 01   ..........x.....
000000f0  05 00  01 00  00 00  80 01   00 00  ed 07  00 00  00 00   ......€...í.....
00000100  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000110  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000120  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000130  00 00  00 00  00 00  00 00   00 00  00 00  00 00  58 69   ..............Xi
00000140  61 6f  6d 69  00 4d  32 30   30 33  4a 31  35 53  43 00   aomi.M2003J15SC.
00000150  4d 65  64 69  61 54  65 6b   20 43  61 6d  65 72  61 20   MediaTek Camera 
00000160  41 70  70 6c  69 63  61 74   69 6f  6e 00  00 00  00 00   Application.....
00000170  32 30  32 33  3a 31  32 3a   30 39  20 31  35 3a  35 38   2023:12:09 15:58
00000180  3a 35  35 00  48 00  00 00   01 00  00 00  48 00  00 00   :55.H.......H...
00000190  01 00  00 00  25 00  32 88   04 00  01 00  00 00  00 00   ....%.2ˆ........
000001a0  00 00  30 88  03 00  01 00   00 00  00 00  00 00  aa 9a   ..0ˆ..........ªš
000001b0  01 00  80 03  00 00  4a 03   00 00  27 88  03 00  01 00   ..€...J...'ˆ....
000001c0  00 00  87 00  00 00  22 88   03 00  01 00  00 00  00 00   ..‡..."ˆ........
000001d0  00 00  61 a6  02 00  04 00   00 00  31 36  33 00  9d 82   ..a¦......163..‚
000001e0  05 00  01 00  00 00  ca 06   00 00  9a 82  05 00  01 00   ......Ê...š‚....
000001f0  00 00  d2 06  00 00  9a 88   01 00  01 00  00 00  00 00   ..Ò...šˆ........
00000200  00 00  99 99  02 00  90 00   00 00  da 06  00 00  95 88   ..™™......Ú...•ˆ
00000210  03 00  01 00  00 00  00 00   00 00  92 92  02 00  04 00   ..........''....
```

History

- Default
- Open
- Write (10 Items)
  - Write 0x61 at 0x80
  - Write 0x68 at 0x81
  - Write 0x61 at 0x82
  - Write 0x6c at 0x83
  - Write 0x6f at 0x84
  - Write 0x2e at 0x85
  - Write 0x67 at 0x86
  - Write 0x65 at 0x87
  - Write 0x73 at 0x88
  - Write 0x73 at 0x89

Selection

Information

Total Size	No selection	bytes
Fragments	No selection	

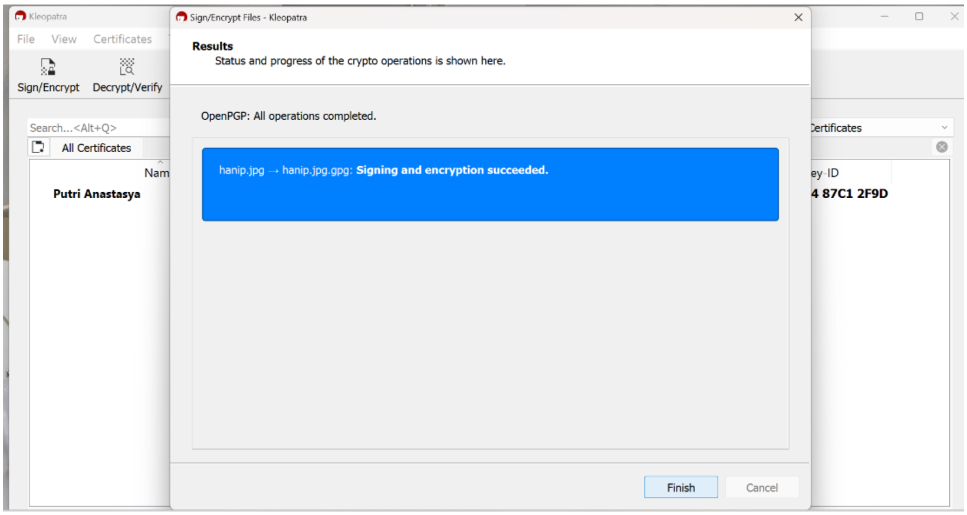
Details

Ready

Offset: 0x0000008a (138) Size: 0x0034084e (3.409.998): 3,25 MB Hex bytes, 16, Default ANSI OVR

2. Kleopatra

After that open kleopatra to encrypt a photo that already contains a hidden message from the previous tool. If it has been encrypted, the output will appear like this.



Putri Anastasya

4 87C1 2F9D

Sign/Encrypt Files - Kleopatra

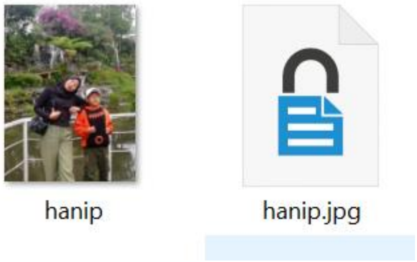
Results

Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

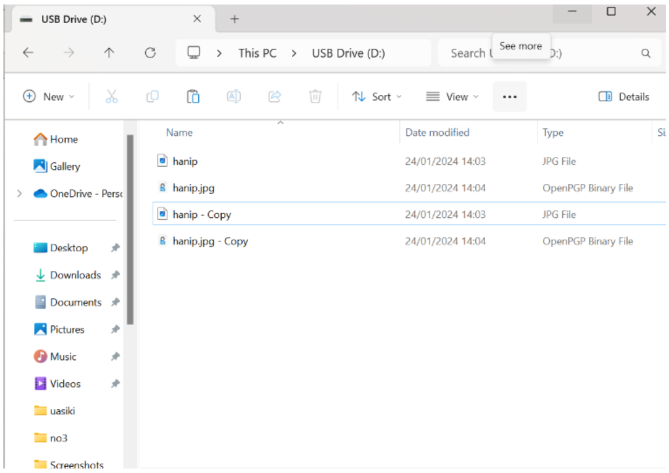
hanip.jpg → hanip.jpg.gpg: **Signing and encryption succeeded.**

If it is successful, the file will look like this. This is the encrypted file of kleopatra and the photo containing the hidden message from hex editor neo.



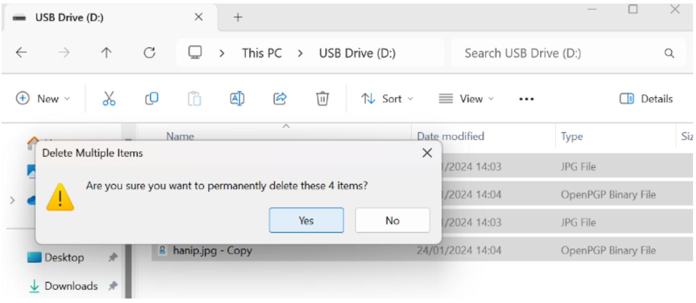
3. Copy File from Part A and Part B

After that, insert the encrypted file of kleopatra and the photo containing the hidden message into the USB.



Name	Date modified	Type
hanip	24/01/2024 14:03	JPG File
hanip.jpg	24/01/2024 14:04	OpenPGP Binary File
hanip - Copy	24/01/2024 14:03	JPG File
hanip.jpg - Copy	24/01/2024 14:04	OpenPGP Binary File

Then delete all files on the usb to make the file on the USB empty.



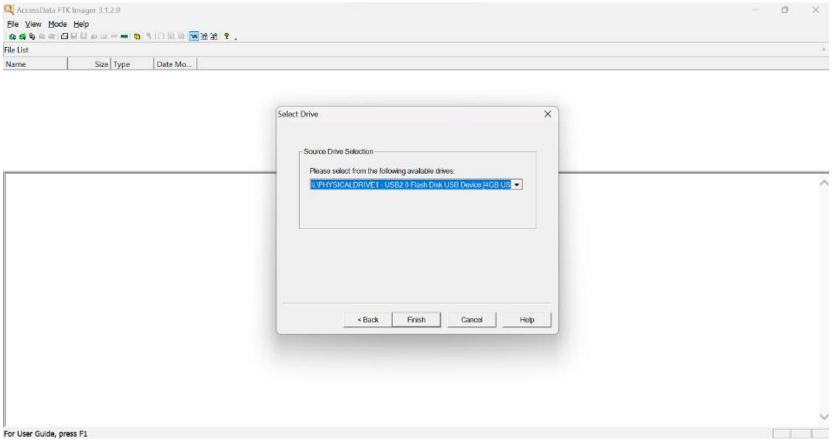
Delete Multiple Items

Are you sure you want to permanently delete these 4 items?

4. How to Recovery the Files use FTK Imager Data Tool

4.1 If file in USB was empty

Open the AccessData FTK Manager application and select the physical drive and look for the USB. And select the availabels drive.



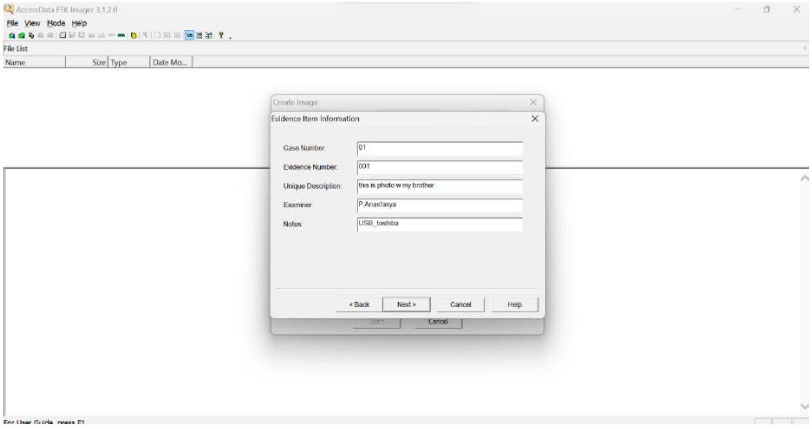
Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - USB2.0 Flash Disk USB Device [4GB US

After that, click Add and select Raw. A display will appear like this and fill in the Evidance information that appears on the screen like this.



Evidence Item Information

Case Number: 01

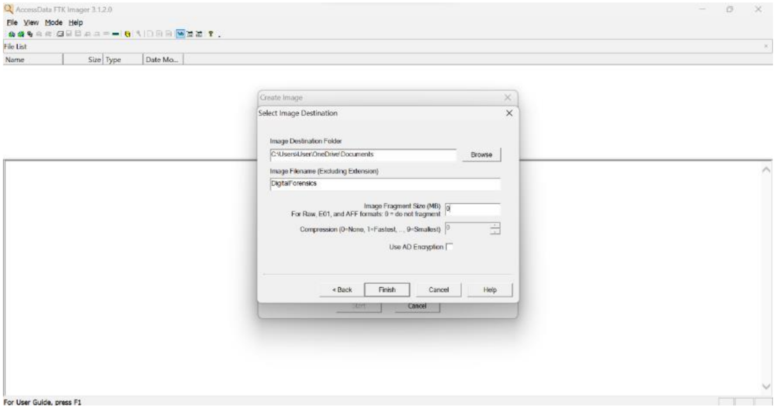
Evidence Number: 001

Unique Description: this is photo w my brother

Examiner: P.Anastasya

Notes: USB_toshiba

Select browse image destination folder, and fill in the Image filename with the desired file name. Fill in Image Fragment Size with size 0.



Select Image Destination

Image Destination Folder: C:\Users\User\OneDrive\Documents

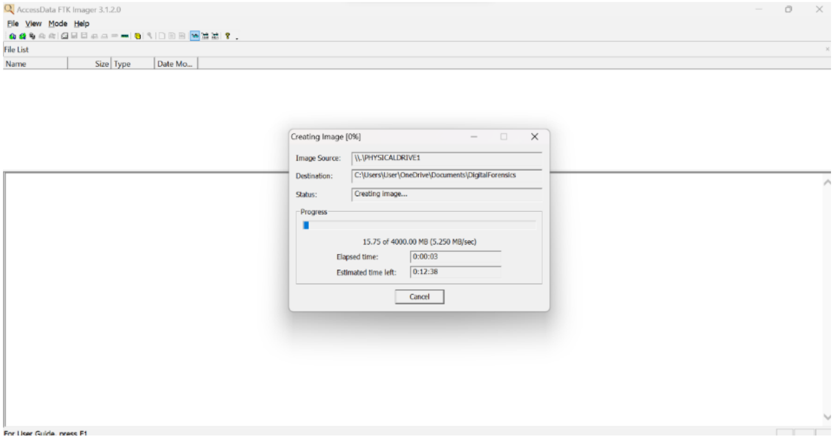
Image Filename (Excluding Extension): DigitalForensics

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Then the Creating Image and veryfing process will be run as shown below. This is the progress of data recovery.



Creating Image [0%]

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\User\OneDrive\Documents\DigitalForensics

Status: Creating image...

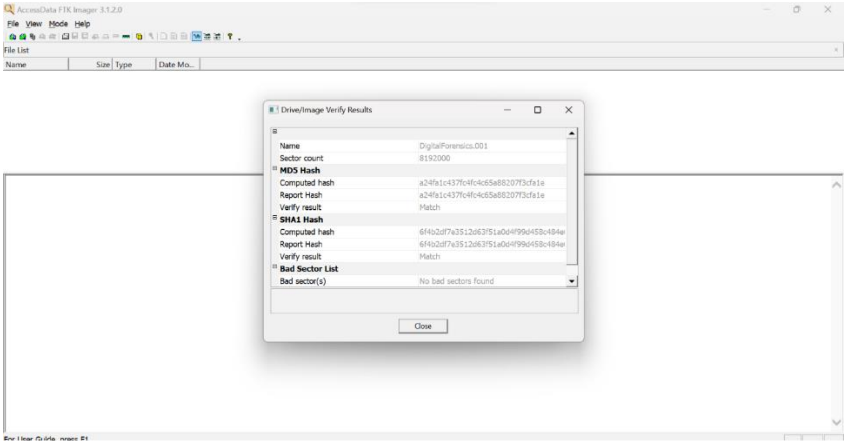
Progress

15.75 of 4000.00 MB (5.250 MB/sec)

Elapsed time: 0:00:03

Estimated time left: 0:12:38

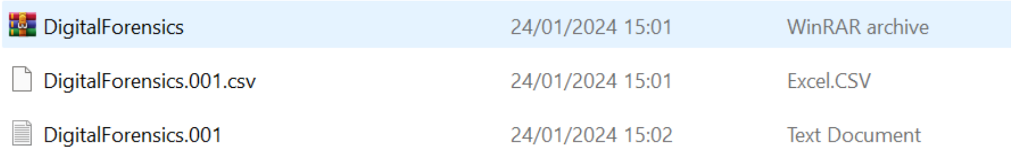
If the process is complete, the display will appear as below.



Drive/Image Verify Results

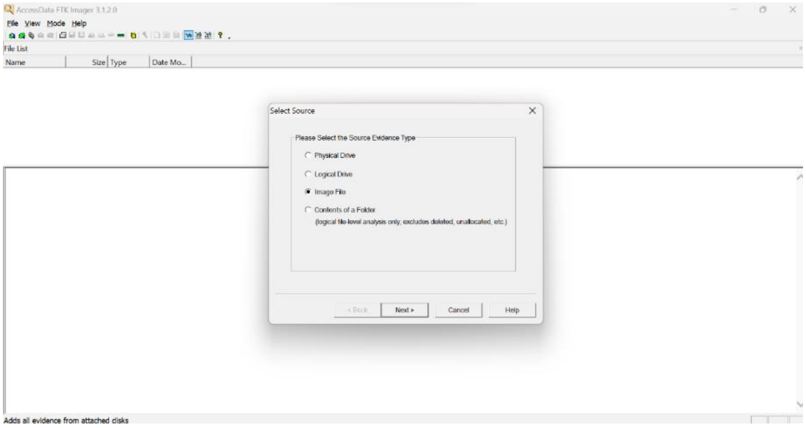
Name	DigitalForensics.001
Sector count	8192000
MD5 Hash	
Computed hash	a24fa1c437fc4fc4c65a88207f3cfa1e
Report Hash	a24fa1c437fc4fc4c65a88207f3cfa1e
Verify result	Match
SHA1 Hash	
Computed hash	6f4b2df7e3512d63f51a0d4f99d458c484e
Report Hash	6f4b2df7e3512d63f51a0d4f99d458c484e
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

The file will be saved as a rar.



DigitalForensics	24/01/2024 15:01	WinRAR archive
DigitalForensics.001.csv	24/01/2024 15:01	Excel.CSV
DigitalForensics.001	24/01/2024 15:02	Text Document

After that, click File and Add Evidance Item and select Image File and then Enter the Source Path by clicking Browse and selecting where the file is located.



Select Source

Please Select the Source Evidence Type

○ Physical Drive

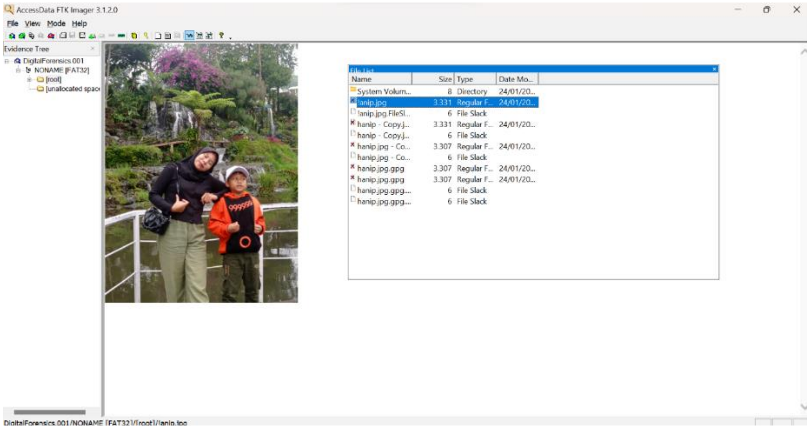
○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Adds all evidence from attached disks

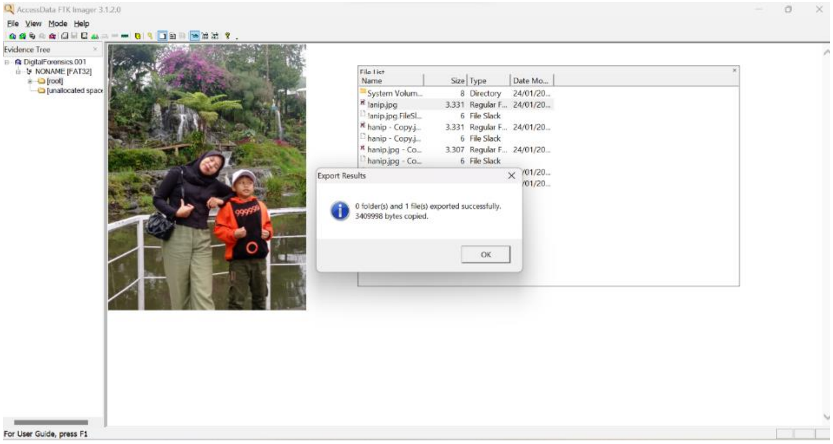
The result of recovery from files that have been deleted from USB. A display will appear like this.



Name	Size	Type	Date Mo...
System Volum...	8	Directory	24/01/20...
!anip.jpg	3.331	Regular F...	24/01/20...
!anip.jpg.FileSl...	6	File Slack	
hanip - Copy.j...	3.331	Regular F...	24/01/20...
hanip - Copy.j...	6	File Slack	
hanip.jpg - Co...	3.307	Regular F...	24/01/20...
hanip.jpg - Co...	6	File Slack	
hanip.jpg.gpg	3.307	Regular F...	24/01/20...
hanip.jpg.gpg	3.307	Regular F...	24/01/20...
hanip.jpg.gpg....	6	File Slack	
hanip.jpg.gpg....	6	File Slack	

DigitalForensics.001/NONAME [FAT32]/[root]/!anip.jpg

To restore the files that have been deleted, we export the files that we recovered.



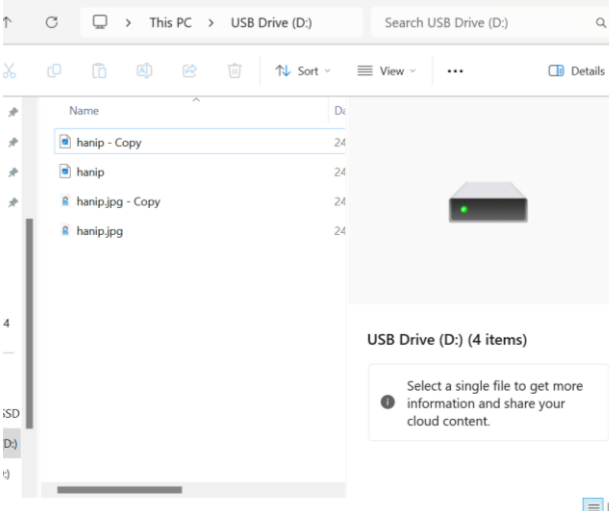
Name	Size	Type	Date Mo...
System Volum...	8	Directory	24/01/20...
!anip.jpg	3.331	Regular F...	24/01/20...
!anip.jpg.FileSl...	6	File Slack	
hanip - Copy.j...	3.331	Regular F...	24/01/20...
hanip - Copy.j...	6	File Slack	
hanip.jpg - Co...	3.307	Regular F...	24/01/20...
hanip.jpg - Co...	6	File Slack	

Export Results

0 folder(s) and 1 file(s) exported successfully.
3409998 bytes copied.

For User Guide, press F1

4.2 If There is a File on USB

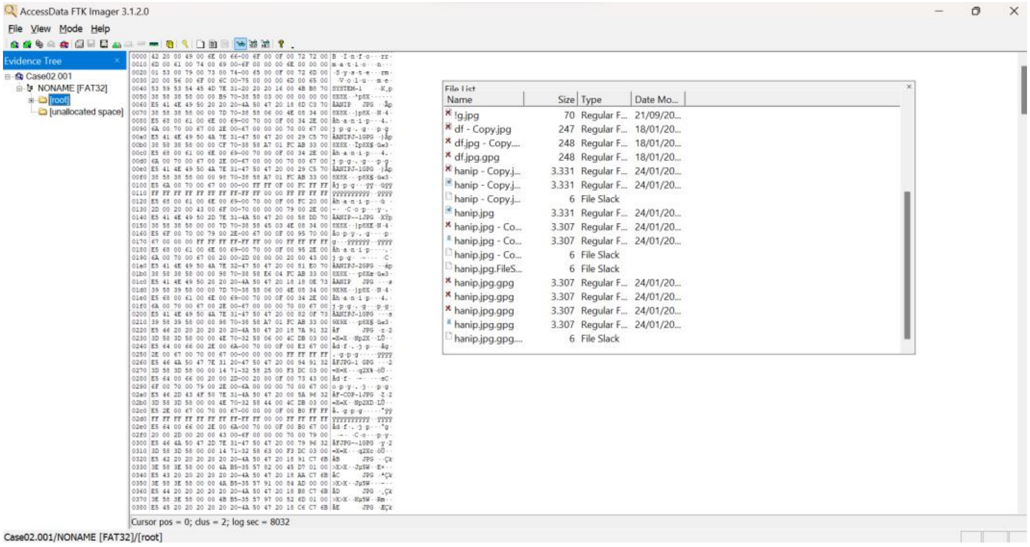


Name
hanip - Copy
hanip
hanip.jpg - Copy
hanip.jpg

USB Drive (D:) (4 items)

Select a single file to get more information and share your cloud content.

We use the same steps as when the USB is empty, the result will be like this.

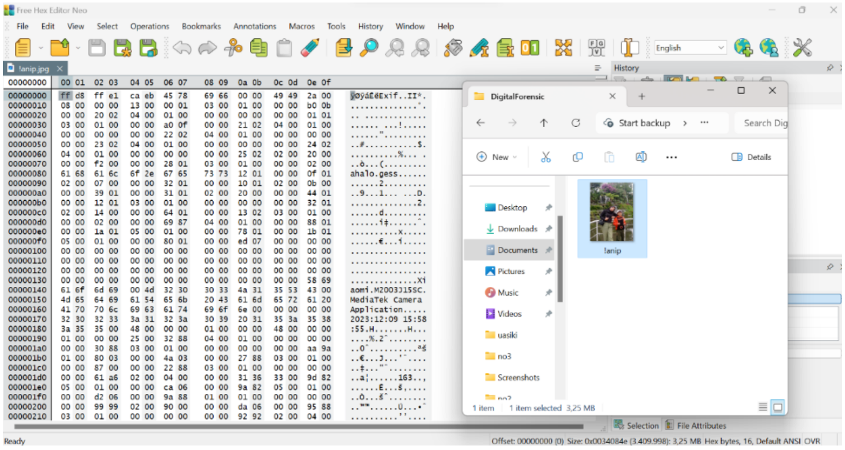


Name	Size	Type	Date Mo...
!g.jpg	70	Regular F...	21/09/20...
df - Copy.jpg	247	Regular F...	18/01/20...
df.jpg - Copy....	248	Regular F...	18/01/20...
df.jpg.gpg	248	Regular F...	18/01/20...
hanip - Copy.j...	3.331	Regular F...	24/01/20...
hanip - Copy.j...	3.331	Regular F...	24/01/20...
hanip - Copy.j...	6	File Slack	
hanip.jpg	3.331	Regular F...	24/01/20...
hanip.jpg - Co...	3.307	Regular F...	24/01/20...
hanip.jpg - Co...	3.307	Regular F...	24/01/20...
hanip.jpg - Co...	6	File Slack	
hanip.jpg.FileS...	6	File Slack	
hanip.jpg.gpg	3.307	Regular F...	24/01/20...
hanip.jpg.gpg	3.307	Regular F...	24/01/20...
hanip.jpg.gpg	3.307	Regular F...	24/01/20...
hanip.jpg.gpg	3.307	Regular F...	24/01/20...
hanip.jpg.gpg....	6	File Slack	

Cursor pos = 0; clus = 2; log sec = 8032

Case02.001/NONAME [FAT32]/[root]

After that decrypt in kleopatra and we open the file again with jpg format in hex editor neo to see the hidden message in the recovered file ,whether the file is the same as before recovery.



```
00000000  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000  ff d8 ff e1 ca eb 45 78 69 66 00 00 49 49 2a 00  ÿØÿáÊëExif..II*.
00000010  08 00 00 00 13 00 00 01 03 00 01 00 00 00 b0 0b  ..............°.
00000020  00 00 20 02 04 00 01 00 00 00 00 00 00 00 01 01  .. .............
00000030  03 00 01 00 00 00 a0 0f 00 00 21 02 04 00 01 00  ...... ...!.....
00000040  00 00 00 00 00 00 22 02 04 00 01 00 00 00 00 00  ......".........
00000050  00 00 23 02 04 00 01 00 00 00 00 00 00 00 24 02  ..#...........$.
00000060  04 00 01 00 00 00 00 00 00 00 25 02 02 00 20 00  ..........%... .
00000070  00 00 f2 00 00 00 28 01 03 00 01 00 00 00 02 00  ..ò...(.........
00000080  61 68 61 6c 6f 2e 67 65 73 73 12 01 00 00 0f 01  ahalo.gess......
00000090  02 00 07 00 00 00 32 01 00 00 10 01 02 00 0b 00  ......2.........
000000a0  00 00 39 01 00 00 31 01 02 00 20 00 00 00 44 01  ..9...1... ...D.
000000b0  00 00 12 01 03 00 01 00 00 00 00 00 00 00 32 01  ..............2.
000000c0  02 00 14 00 00 00 64 01 00 00 13 02 03 00 01 00  ......d.........
000000d0  00 00 02 00 00 00 69 87 04 00 01 00 00 00 88 01  ......i‡......ˆ.
000000e0  00 00 1a 01 05 00 01 00 00 00 78 01 00 00 1b 01  ..........x.....
000000f0  05 00 01 00 00 00 80 01 00 00 ed 07 00 00 00 00  ......€...í.....
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 69  ..............Xi
00000140  61 6f 6d 69 00 4d 32 30 30 33 4a 31 35 53 43 00  aomi.M2003J15SC.
00000150  4d 65 64 69 61 54 65 6b 20 43 61 6d 65 72 61 20  MediaTek Camera 
00000160  41 70 70 6c 69 63 61 74 69 6f 6e 00 00 00 00 00  Application.....
00000170  32 30 32 33 3a 31 32 3a 30 39 20 31 35 3a 35 38  2023:12:09 15:58
00000180  3a 35 35 00 48 00 00 00 01 00 00 00 48 00 00 00  :55.H.......H...
00000190  01 00 00 00 25 00 32 88 04 00 01 00 00 00 00 00  ....%.2ˆ........
000001a0  00 00 30 88 03 00 01 00 00 00 00 00 00 00 aa 9a  ..0ˆ..........ªš
000001b0  01 00 80 03 00 00 4a 03 00 00 27 88 03 00 01 00  ..€...J...'ˆ....
000001c0  00 00 87 00 00 00 22 88 03 00 01 00 00 00 00 00  ..‡..."ˆ........
000001d0  00 00 61 a6 02 00 04 00 00 00 31 36 33 00 9d 82  ..a¦......163..‚
000001e0  05 00 01 00 00 00 ca 06 00 00 9a 82 05 00 01 00  ......Ê...š‚....
000001f0  00 00 d2 06 00 00 9a 88 01 00 01 00 00 00 00 00  ..Ò...šˆ........
00000200  00 00 99 99 02 00 90 00 00 00 da 06 00 00 95 88  ..™™......Ú...•ˆ
00000210  03 00 01 00 00 00 00 00 00 00 92 92 02 00 04 00  ..........’’....
```

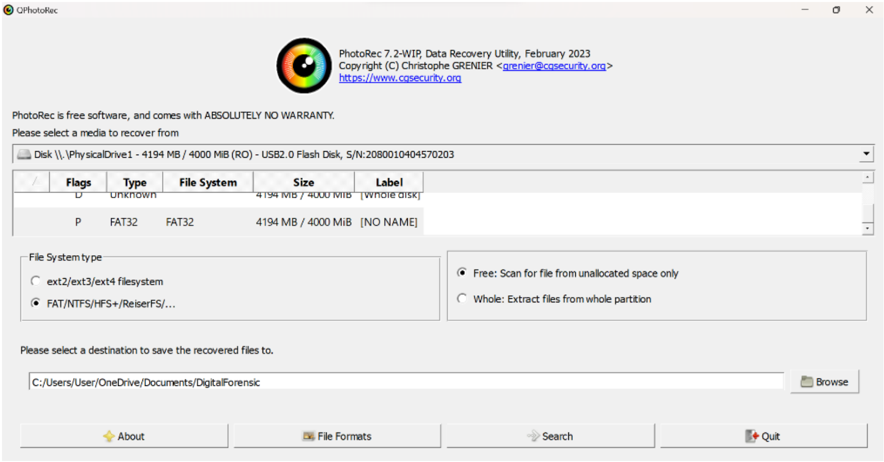
1 item 1 item selected 3,25 MB

Ready

Offset: 00000000 (0) Size: 0x0034084e (3.409.998): 3,25 MB Hex bytes, 16, Default ANSI OVR

5. How to Recovery the Files use PhotoRec

Select USB to media to recover and then select browse so that the final destination file is there.



PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.

Please select a media to recover from

Disk \\.\PhysicalDrive1 - 4194 MB / 4000 MiB (RO) - USB2.0 Flash Disk, S/N:2080010404570203

Flags	Type	File System	Size	Label
D	Unknown		4194 MB / 4000 MiB	[Whole disk]
P	FAT32	FAT32	4194 MB / 4000 MiB	[NO NAME]

File System type

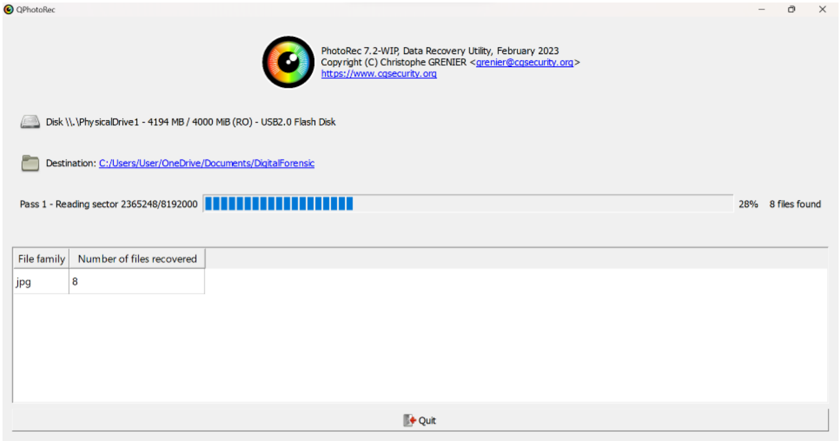
○ ext2/ext3/ext4 filesystem
● FAT/NTFS/HFS+/ReiserFS/...

● Free: Scan for file from unallocated space only
○ Whole: Extract files from whole partition

Please select a destination to save the recovered files to.

C:/Users/User/OneDrive/Documents/DigitalForensic

This is process recovery file in USB



PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

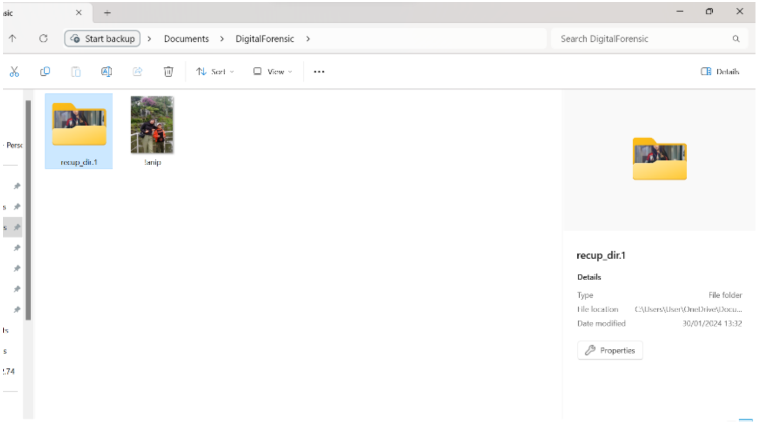
Disk \\.\PhysicalDrive1 - 4194 MB / 4000 MiB (RO) - USB2.0 Flash Disk

Destination: C:/Users/User/OneDrive/Documents/DigitalForensic

Pass 1 - Reading sector 2365248/8192000 28% 8 files found

File family	Number of files recovered
jpg	8

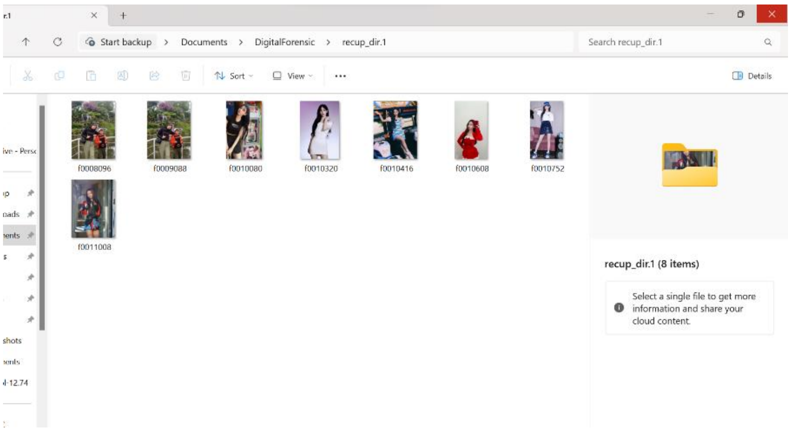
This is the result recovery files use PhotoRec



recup_dir.1

Details

Type File folder
File location C:\Users\User\OneDrive\Docu...
Date modified 30/01/2024 13:32

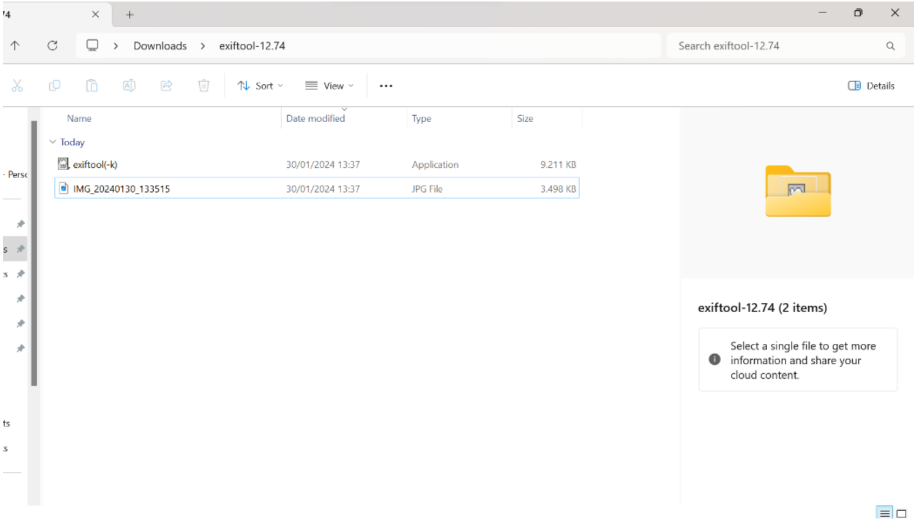


recup_dir.1 (8 items)

Select a single file to get more information and share your cloud content.

6. Exif Tool

This tool serves to view the location information of the photo. Just drag and drop the photo you want to find the location.

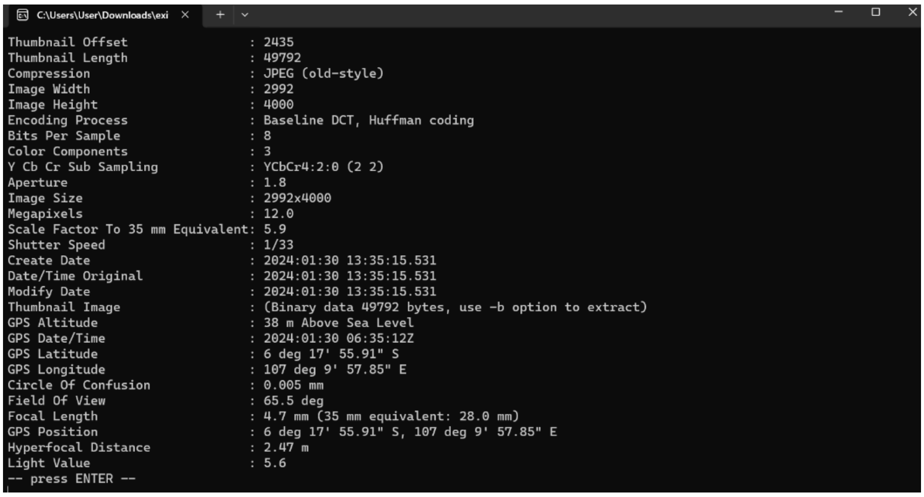


Name	Date modified	Type	Size
exiftool(-k)	30/01/2024 13:37	Application	9.211 KB
IMG_20240130_133515	30/01/2024 13:37	JPG File	3.498 KB

exiftool-12.74 (2 items)

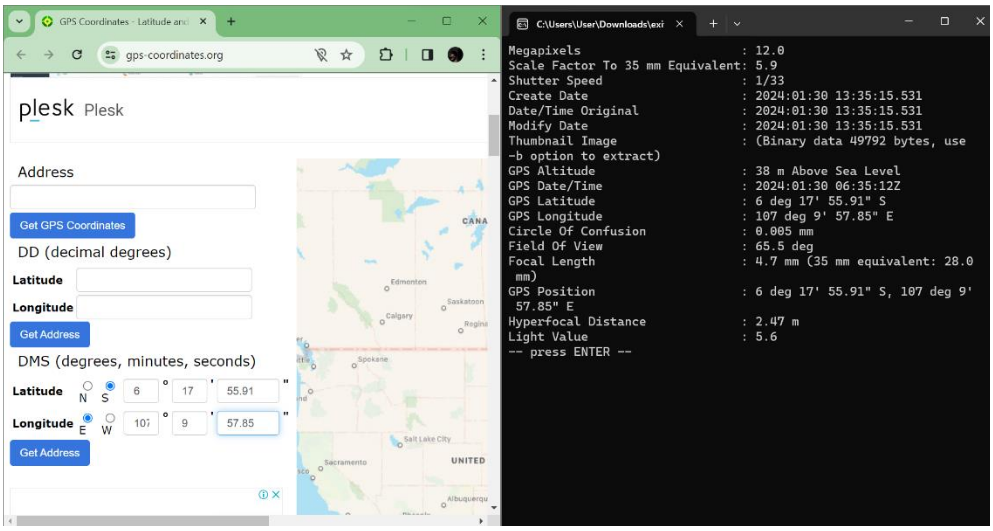
Select a single file to get more information and share your cloud content.

The result will provide photo information in the form of a command prompt.



```
Thumbnail Offset                : 2435
Thumbnail Length                : 49792
Compression                     : JPEG (old-style)
Image Width                     : 2992
Image Height                    : 4000
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 1.8
Image Size                      : 2992x4000
Megapixels                      : 12.0
Scale Factor To 35 mm Equivalent: 5.9
Shutter Speed                   : 1/33
Create Date                     : 2024:01:30 13:35:15.531
Date/Time Original              : 2024:01:30 13:35:15.531
Modify Date                     : 2024:01:30 13:35:15.531
Thumbnail Image                 : (Binary data 49792 bytes, use -b option to extract)
GPS Altitude                    : 38 m Above Sea Level
GPS Date/Time                   : 2024:01:30 06:35:12Z
GPS Latitude                    : 6 deg 17' 55.91" S
GPS Longitude                   : 107 deg 9' 57.85" E
Circle Of Confusion             : 0.005 mm
Field Of View                   : 65.5 deg
Focal Length                    : 4.7 mm (35 mm equivalent: 28.0 mm)
GPS Position                    : 6 deg 17' 55.91" S, 107 deg 9' 57.85" E
Hyperfocal Distance             : 2.47 m
Light Value                     : 5.6
-- press ENTER --
```

After we get all of location information, we use [GPS Coordinates - Latitude and Longitude Finder (gps-coordinates.org)] to see the location of where the photo as taken.



Address

DD (decimal degrees)

Latitude

Longitude

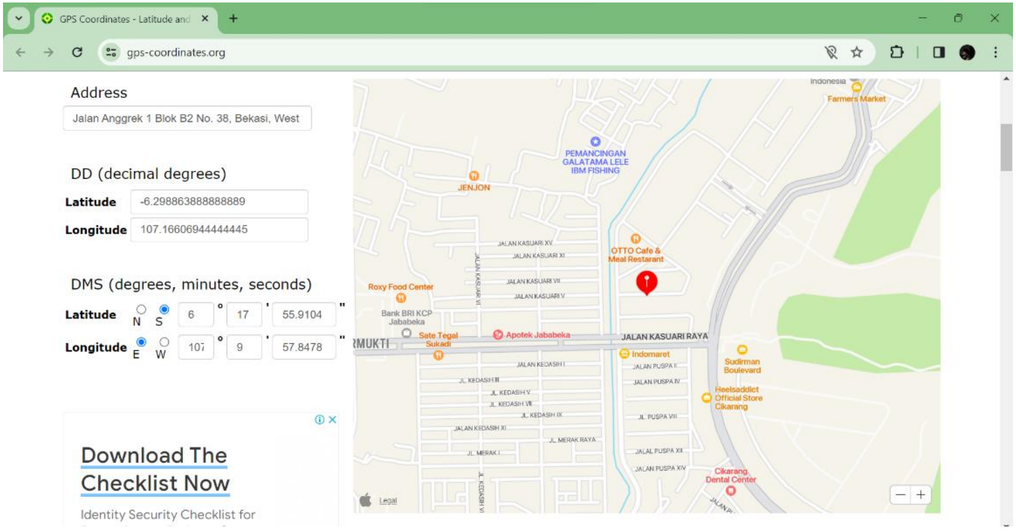
DMS (degrees, minutes, seconds)

Latitude ○ N ● S 6 ° 17 ' 55.91 "

Longitude ● E ○ W 107 ° 9 ' 57.85 "

```
Megapixels                      : 12.0
Scale Factor To 35 mm Equivalent: 5.9
Shutter Speed                   : 1/33
Create Date                     : 2024:01:30 13:35:15.531
Date/Time Original              : 2024:01:30 13:35:15.531
Modify Date                     : 2024:01:30 13:35:15.531
Thumbnail Image                 : (Binary data 49792 bytes, use
-b option to extract)
GPS Altitude                    : 38 m Above Sea Level
GPS Date/Time                   : 2024:01:30 06:35:12Z
GPS Latitude                    : 6 deg 17' 55.91" S
GPS Longitude                   : 107 deg 9' 57.85" E
Circle Of Confusion             : 0.005 mm
Field Of View                   : 65.5 deg
Focal Length                    : 4.7 mm (35 mm equivalent: 28.0
 mm)
GPS Position                    : 6 deg 17' 55.91" S, 107 deg 9'
 57.85" E
Hyperfocal Distance             : 2.47 m
Light Value                     : 5.6
-- press ENTER --
```

And this is the result, location is absolutely correct. Disclaimer we only can get information of latitude and longitude user taken photo with turned on GPS



Address

Jalan Anggrek 1 Blok B2 No. 38, Bekasi, West

DD (decimal degrees)

Latitude -6.298863888888889

Longitude 107.16606944444445

DMS (degrees, minutes, seconds)

Latitude ○ N ● S 6 ° 17 ' 55.9104 "

Longitude ● E ○ W 107 ° 9 ' 57.8478 "