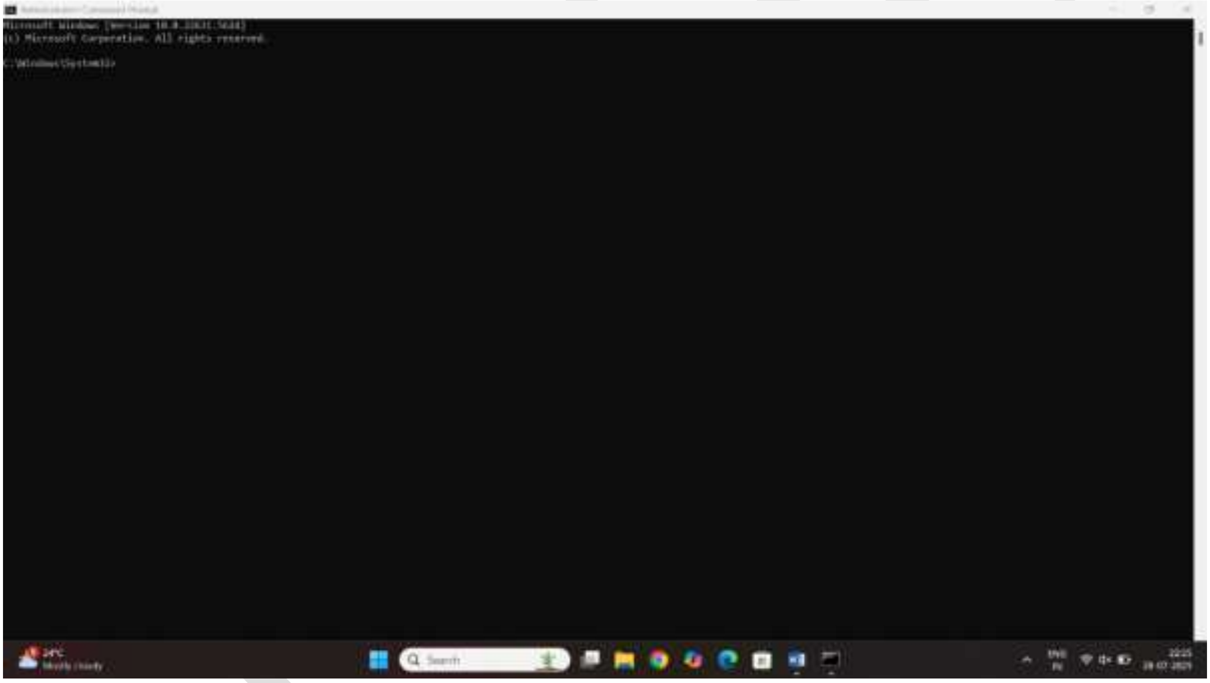
Module 6 windows forensics

Lab 1 Acquire volatile information windows machine

There was tool called PS tool

Step1 download the ps tool

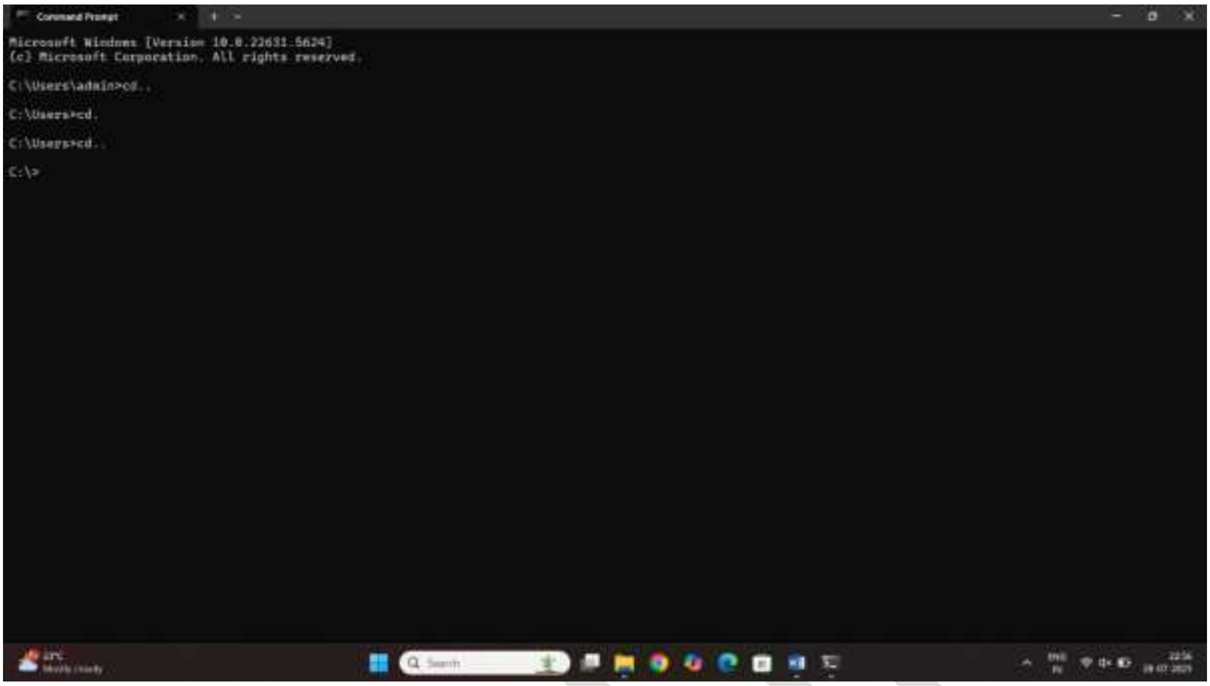
Step2 open the ps cmd run as administrative



```
Microsoft Windows [Version 10.0.22631.5624]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

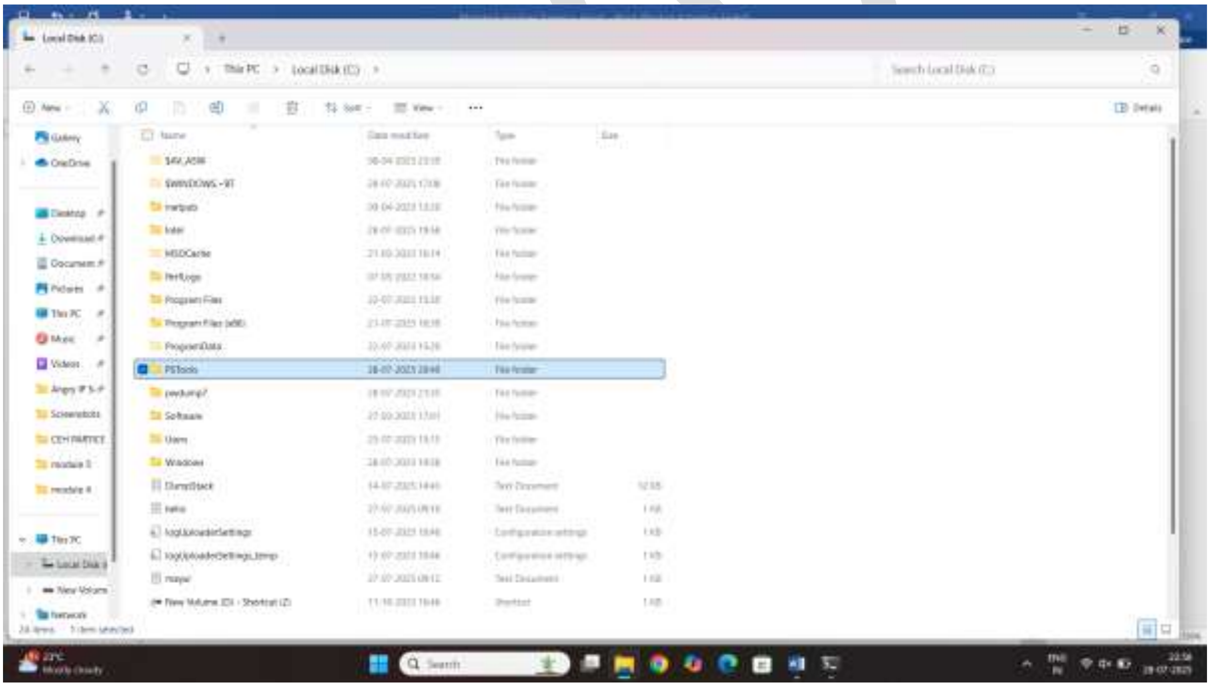
Step3 go to c drive

Command: cd..



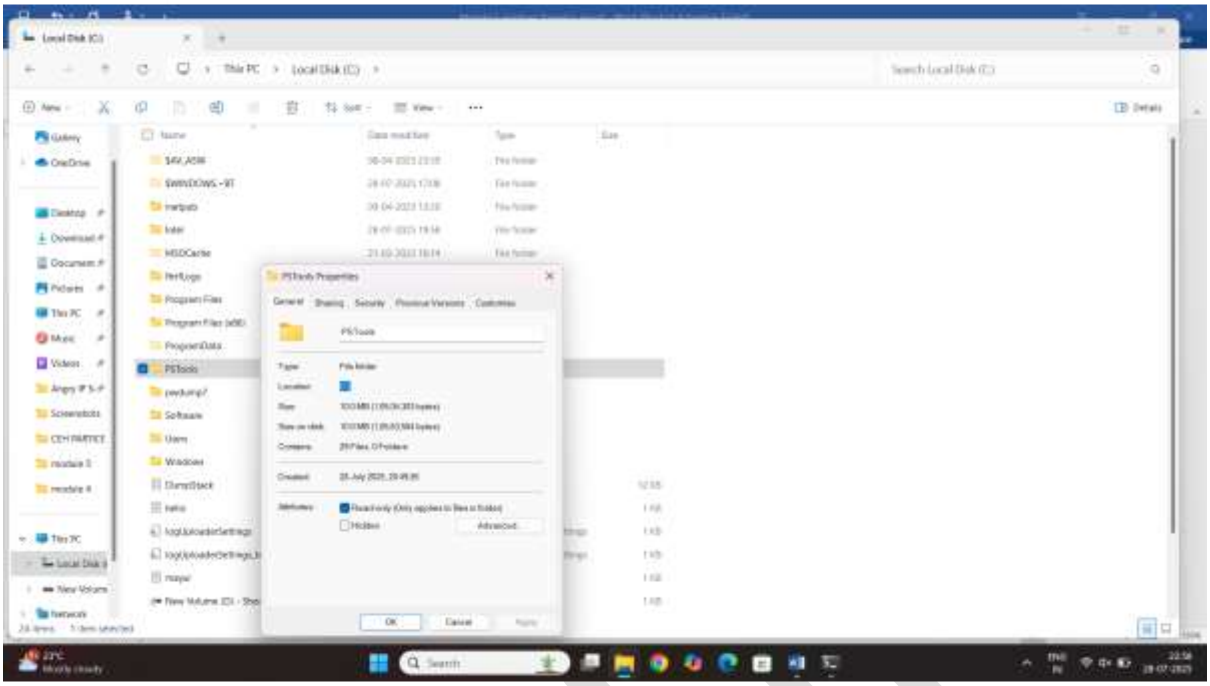
```
Microsoft Windows [Version 10.0.22631.5624]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd..

C:\Users>cd.

C:\Users>cd..

C:\>
```

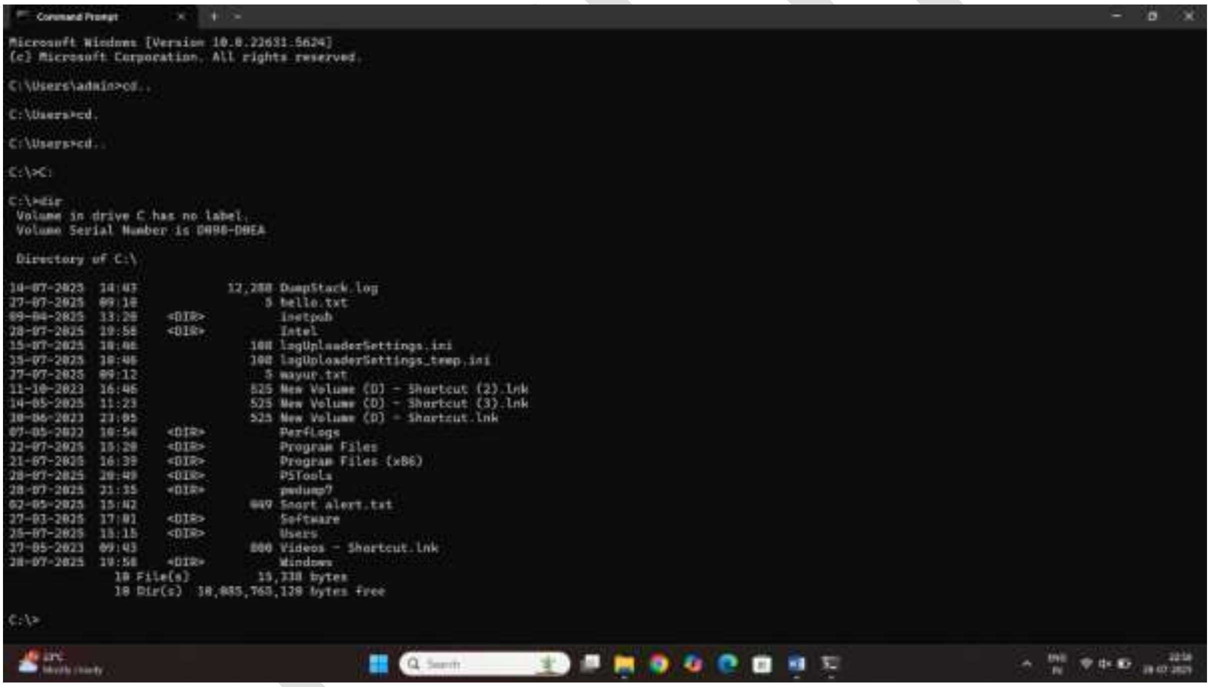
Step4 go to ps tool path open them cmd



This PC > Local Disk (C:)

Name	Date modified	Type	Size
$AV_ASW	[illegible]	File folder	
$WINDOWS.~BT	[illegible]	File folder	
inetpub	[illegible]	File folder	
Intel	[illegible]	File folder	
MSOCache	[illegible]	File folder	
PerfLogs	[illegible]	File folder	
Program Files	[illegible]	File folder	
Program Files (x86)	[illegible]	File folder	
ProgramData	[illegible]	File folder	
PSTools	28-07-2025 20:48	File folder	
pwdump7	[illegible]	File folder	
Software	[illegible]	File folder	
Users	[illegible]	File folder	
Windows	[illegible]	File folder	
DumpStack	[illegible]	Text Document	12 KB
hello	[illegible]	Text Document	1 KB
logUploaderSettings	[illegible]	Configuration settings	1 KB
logUploaderSettings_temp	[illegible]	Configuration settings	1 KB
mayur	[illegible]	Text Document	1 KB
New Volume (D) - Shortcut (Z)	[illegible]	Shortcut	1 KB

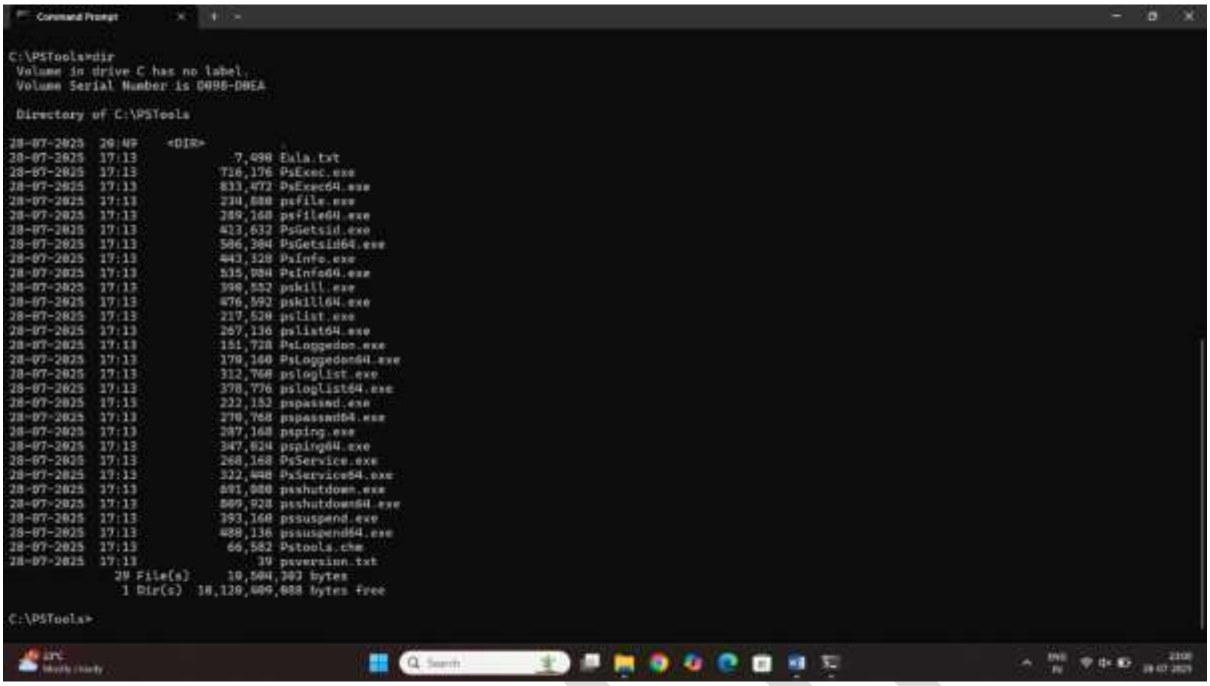




```
Microsoft Windows [Version 10.0.22631.5624]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd..

C:\Users>cd.

C:\Users>cd..

C:\>C:

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is D898-D0EA

 Directory of C:\

10-07-2025  10:03            12,288 DumpStack.log
27-07-2025  09:10                 5 hello.txt
09-04-2025  13:20    <DIR>          inetpub
28-07-2025  19:58    <DIR>          Intel
15-07-2025  10:46               100 logUploaderSettings.ini
15-07-2025  10:46               100 logUploaderSettings_temp.ini
27-07-2025  09:12                 5 mayur.txt
11-10-2023  16:46               525 New Volume (D) - Shortcut (2).lnk
14-05-2025  11:23               525 New Volume (D) - Shortcut (3).lnk
30-06-2023  23:05               525 New Volume (D) - Shortcut.lnk
07-05-2022  10:54    <DIR>          PerfLogs
22-07-2025  15:20    <DIR>          Program Files
21-07-2025  16:39    <DIR>          Program Files (x86)
28-07-2025  20:49    <DIR>          PSTools
28-07-2025  21:35    <DIR>          pmdump7
02-05-2025  15:42               089 Snort alert.txt
27-03-2025  17:01    <DIR>          Software
25-07-2025  15:15    <DIR>          Users
17-05-2023  09:43               800 Videos - Shortcut.lnk
28-07-2025  19:58    <DIR>          Windows
              10 File(s)         15,338 bytes
              10 Dir(s)  10,085,760,128 bytes free

C:\>
```

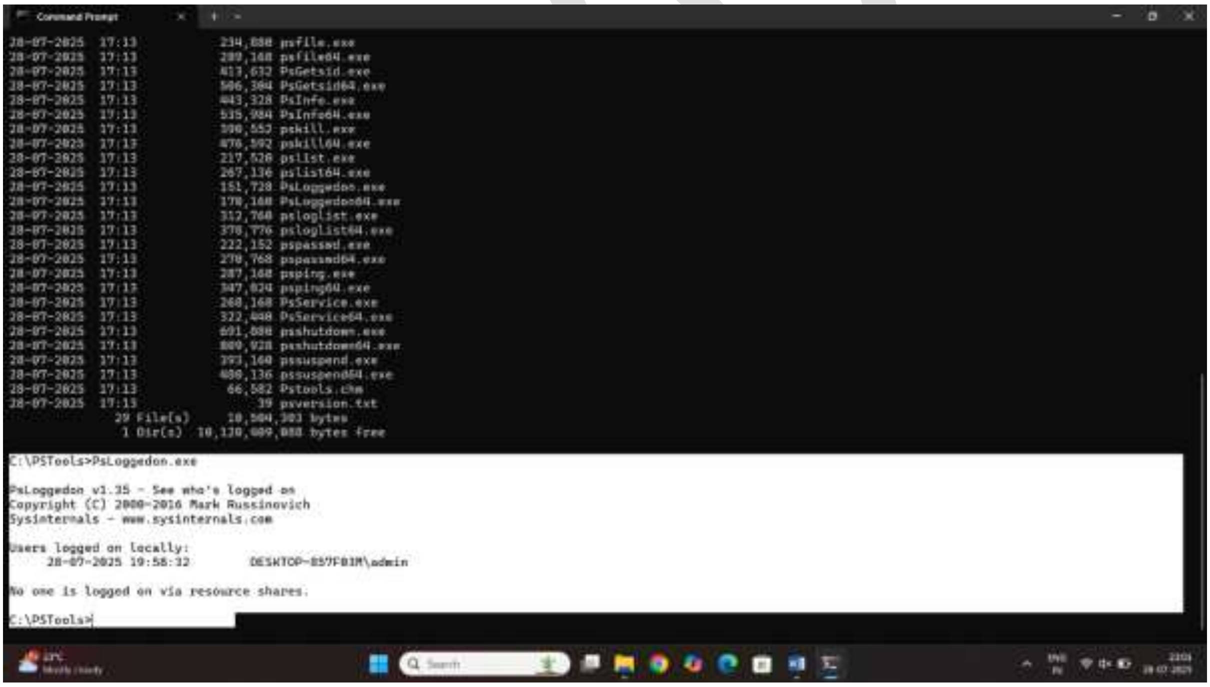
Step5 go to ps tool directory

Command: cd pstool



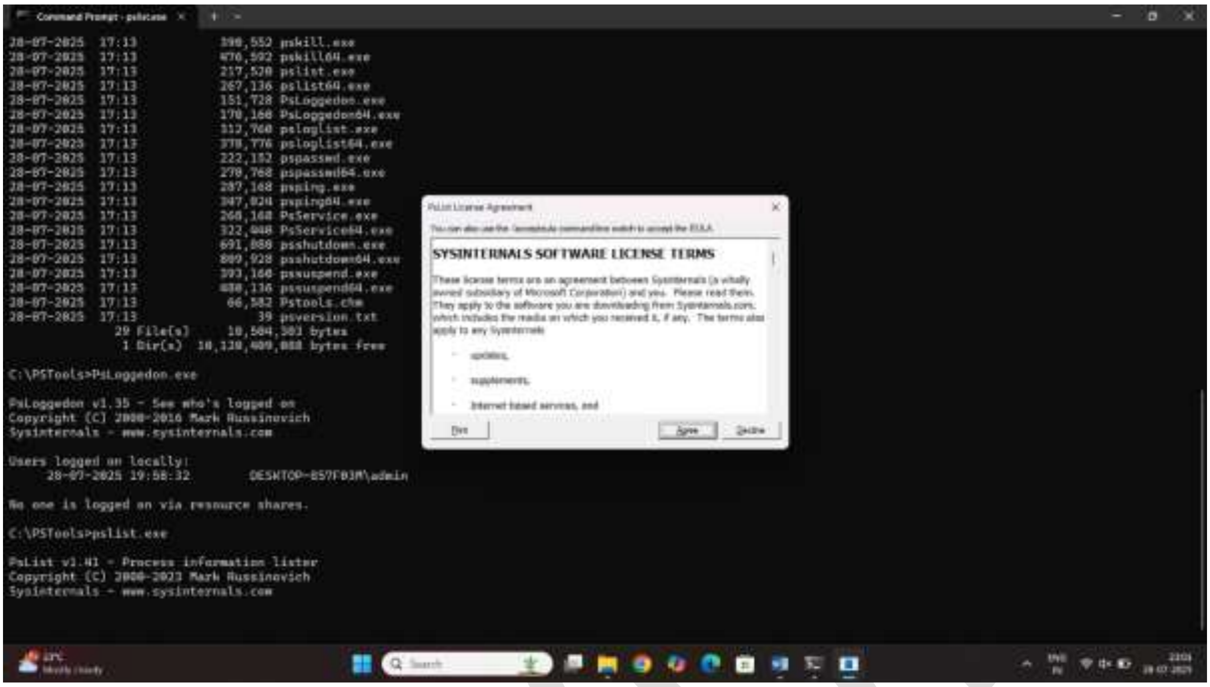
```
C:\PSTools>dir
 Volume in drive C has no label.
 Volume Serial Number is 0098-D0EA

 Directory of C:\PSTools

28-07-2025  20:49    <DIR>
28-07-2025  17:13             7,490 Eula.txt
28-07-2025  17:13           716,176 PsExec.exe
28-07-2025  17:13           833,472 PsExec64.exe
28-07-2025  17:13           234,888 psfile.exe
28-07-2025  17:13           289,160 psfile64.exe
28-07-2025  17:13           413,632 PsGetsid.exe
28-07-2025  17:13           506,384 PsGetsid64.exe
28-07-2025  17:13           443,328 PsInfo.exe
28-07-2025  17:13           535,984 PsInfo64.exe
28-07-2025  17:13           398,552 pskill.exe
28-07-2025  17:13           476,592 pskill64.exe
28-07-2025  17:13           217,528 pslist.exe
28-07-2025  17:13           267,136 pslist64.exe
28-07-2025  17:13           151,728 PsLoggedon.exe
28-07-2025  17:13           170,160 PsLoggedon64.exe
28-07-2025  17:13           312,760 psloglist.exe
28-07-2025  17:13           378,776 psloglist64.exe
28-07-2025  17:13           222,152 pspasswd.exe
28-07-2025  17:13           270,768 pspasswd64.exe
28-07-2025  17:13           287,168 psping.exe
28-07-2025  17:13           347,824 psping64.exe
28-07-2025  17:13           268,168 PsService.exe
28-07-2025  17:13           322,448 PsService64.exe
28-07-2025  17:13           691,088 psshutdown.exe
28-07-2025  17:13           809,928 psshutdown64.exe
28-07-2025  17:13           393,160 pssuspend.exe
28-07-2025  17:13           488,136 pssuspend64.exe
28-07-2025  17:13            66,582 Pstools.chm
28-07-2025  17:13                39 psversion.txt
              29 File(s)     10,504,303 bytes
               1 Dir(s)  10,120,409,088 bytes free

C:\PSTools>
```

Step6 type the command psLoggdon.exe



```
28-07-2025  17:13           234,888 psfile.exe
28-07-2025  17:13           289,160 psfile64.exe
28-07-2025  17:13           413,632 PsGetsid.exe
28-07-2025  17:13           506,384 PsGetsid64.exe
28-07-2025  17:13           443,328 PsInfo.exe
28-07-2025  17:13           535,984 PsInfo64.exe
28-07-2025  17:13           398,552 pskill.exe
28-07-2025  17:13           476,592 pskill64.exe
28-07-2025  17:13           217,528 pslist.exe
28-07-2025  17:13           267,136 pslist64.exe
28-07-2025  17:13           151,728 PsLoggedon.exe
28-07-2025  17:13           170,160 PsLoggedon64.exe
28-07-2025  17:13           312,760 psloglist.exe
28-07-2025  17:13           378,776 psloglist64.exe
28-07-2025  17:13           222,152 pspasswd.exe
28-07-2025  17:13           270,768 pspasswd64.exe
28-07-2025  17:13           287,168 psping.exe
28-07-2025  17:13           347,824 psping64.exe
28-07-2025  17:13           268,168 PsService.exe
28-07-2025  17:13           322,448 PsService64.exe
28-07-2025  17:13           691,088 psshutdown.exe
28-07-2025  17:13           809,928 psshutdown64.exe
28-07-2025  17:13           393,160 pssuspend.exe
28-07-2025  17:13           488,136 pssuspend64.exe
28-07-2025  17:13            66,582 Pstools.chm
28-07-2025  17:13                39 psversion.txt
              29 File(s)     10,504,303 bytes
               1 Dir(s)  10,120,409,088 bytes free

C:\PSTools>PsLoggedon.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     28-07-2025 19:58:32        DESKTOP-857F83M\admin

No one is logged on via resource shares.

C:\PSTools>
```

Step7 command psloglist.exe



```
28-07-2025  17:13           390,552 pskill.exe
28-07-2025  17:13           476,592 pskill64.exe
28-07-2025  17:13           217,520 pslist.exe
28-07-2025  17:13           267,136 pslist64.exe
28-07-2025  17:13           151,728 PsLoggedon.exe
28-07-2025  17:13           170,160 PsLoggedon64.exe
28-07-2025  17:13           312,760 psloglist.exe
28-07-2025  17:13           370,776 psloglist64.exe
28-07-2025  17:13           222,152 pspasswd.exe
28-07-2025  17:13           270,768 pspasswd64.exe
28-07-2025  17:13           287,168 psping.exe
28-07-2025  17:13           307,024 psping64.exe
28-07-2025  17:13           260,160 PsService.exe
28-07-2025  17:13           322,000 PsService64.exe
28-07-2025  17:13           691,000 psshutdown.exe
28-07-2025  17:13           809,928 psshutdown64.exe
28-07-2025  17:13           393,160 pssuspend.exe
28-07-2025  17:13           400,136 pssuspend64.exe
28-07-2025  17:13            66,582 Pstools.chm
28-07-2025  17:13                39 psversion.txt
              29 File(s)     10,504,301 bytes
               1 Dir(s)  10,120,409,088 bytes free

C:\PSTools>PsLoggedon.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     28-07-2025 19:58:32         DESKTOP-857F03M\admin

No one is logged on via resource shares.

C:\PSTools>pslist.exe

PsList v1.41 - Process information lister
Copyright (C) 2000-2023 Mark Russinovich
Sysinternals - www.sysinternals.com
```

PsList License Agreement

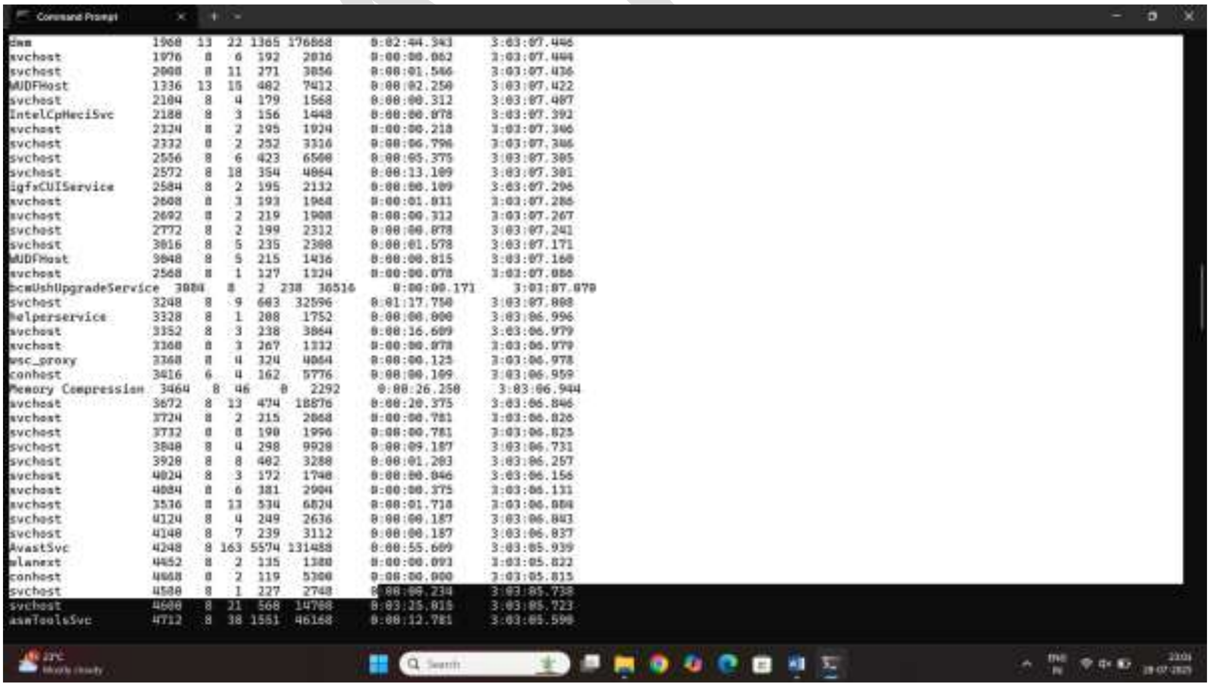
You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

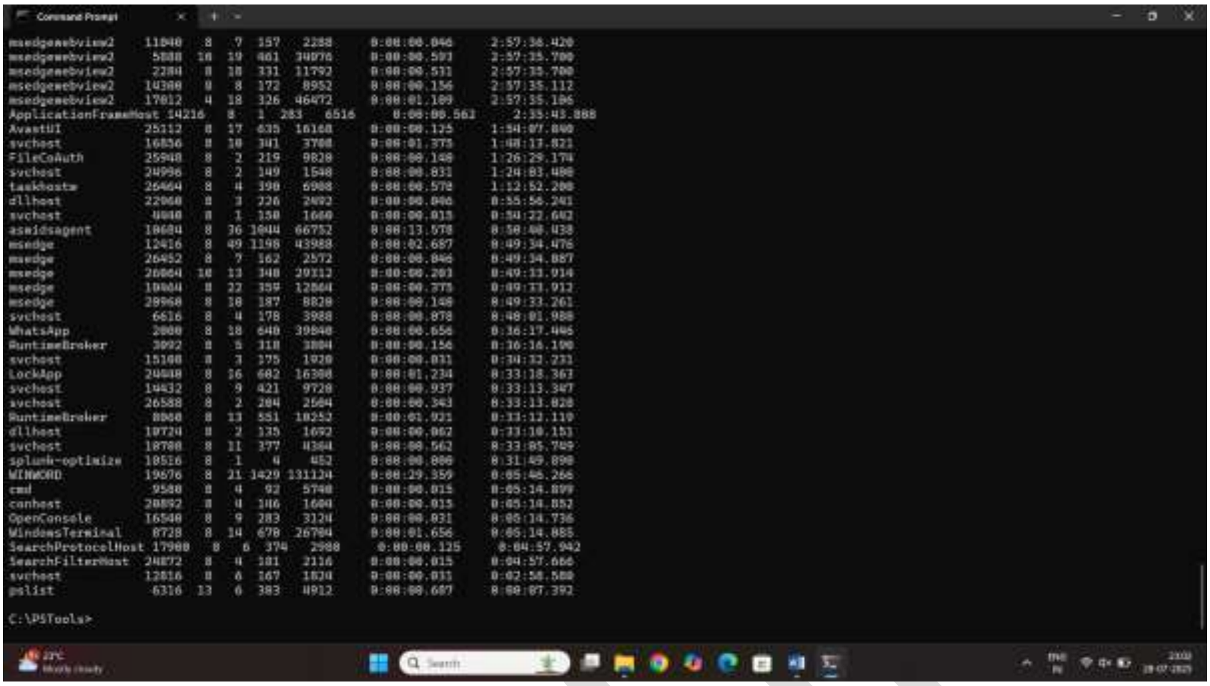
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet based services, and

Result:



```
dwm                 1960  13  22 1365 176868     0:02:44.343     3:03:07.446
svchost             1976   8   6  192   2036     0:00:00.062     3:03:07.444
svchost             2000   8  11  271   3056     0:00:01.546     3:03:07.436
WUDFHost            1336  13  15  482   7412     0:00:02.250     3:03:07.422
svchost             2104   8   4  179   1568     0:00:00.312     3:03:07.407
IntelCpHeciSvc      2188   8   3  156   1448     0:00:00.078     3:03:07.392
svchost             2324   8   2  195   1924     0:00:00.218     3:03:07.346
svchost             2332   8   2  252   3316     0:00:06.796     3:03:07.346
svchost             2556   8   6  423   6500     0:00:05.375     3:03:07.305
svchost             2572   8  18  354   4064     0:00:13.109     3:03:07.301
igfxCUIService      2584   8   2  195   2132     0:00:00.109     3:03:07.296
svchost             2608   8   3  193   1960     0:00:01.031     3:03:07.286
svchost             2692   8   2  219   1900     0:00:00.312     3:03:07.267
svchost             2772   8   2  199   2312     0:00:00.078     3:03:07.241
svchost             3016   8   5  235   2300     0:00:01.578     3:03:07.171
WUDFHost            3048   8   5  215   1436     0:00:00.015     3:03:07.160
svchost             2568   8   1  127   1324     0:00:00.078     3:03:07.086
bcmUshUpgradeService  3084   8   2  238  36516     0:00:00.171     3:03:07.070
svchost             3248   8   9  603  32596     0:01:17.750     3:03:07.008
helperservice       3328   8   1  208   1752     0:00:00.000     3:03:06.996
svchost             3352   8   3  238   3064     0:00:16.609     3:03:06.979
svchost             3360   8   3  267   1332     0:00:00.078     3:03:06.979
wsc_proxy           3368   8   4  324   4064     0:00:00.125     3:03:06.978
conhost             3416   6   4  162   5776     0:00:00.109     3:03:06.959
Memory Compression  3464   8  46    0   2292     0:00:26.250     3:03:06.944
svchost             3672   8  13  474  18876     0:00:20.375     3:03:06.846
svchost             3724   8   2  215   2068     0:00:00.781     3:03:06.826
svchost             3732   8   8  190   1996     0:00:00.781     3:03:06.825
svchost             3840   8   4  298   9928     0:00:09.187     3:03:06.731
svchost             3928   8   8  402   3288     0:00:01.203     3:03:06.257
svchost             4024   8   3  172   1740     0:00:00.046     3:03:06.156
svchost             4084   8   6  381   2904     0:00:00.375     3:03:06.131
svchost             3536   8  13  534   6824     0:00:01.718     3:03:06.084
svchost             4124   8   4  249   2636     0:00:00.187     3:03:06.043
svchost             4148   8   7  239   3112     0:00:00.187     3:03:06.037
AvastSvc            4248   8 163 5574 131488     0:00:55.609     3:03:05.939
wlanext             4452   8   2  135   1380     0:00:00.093     3:03:05.822
conhost             4460   8   2  119   5300     0:00:00.000     3:03:05.815
svchost             4580   8   1  227   2748     0:00:00.234     3:03:05.738
svchost             4600   8  21  568  14708     0:03:25.015     3:03:05.723
aswToolsSvc         4712   8  38 1551  46168     0:00:12.781     3:03:05.590
```

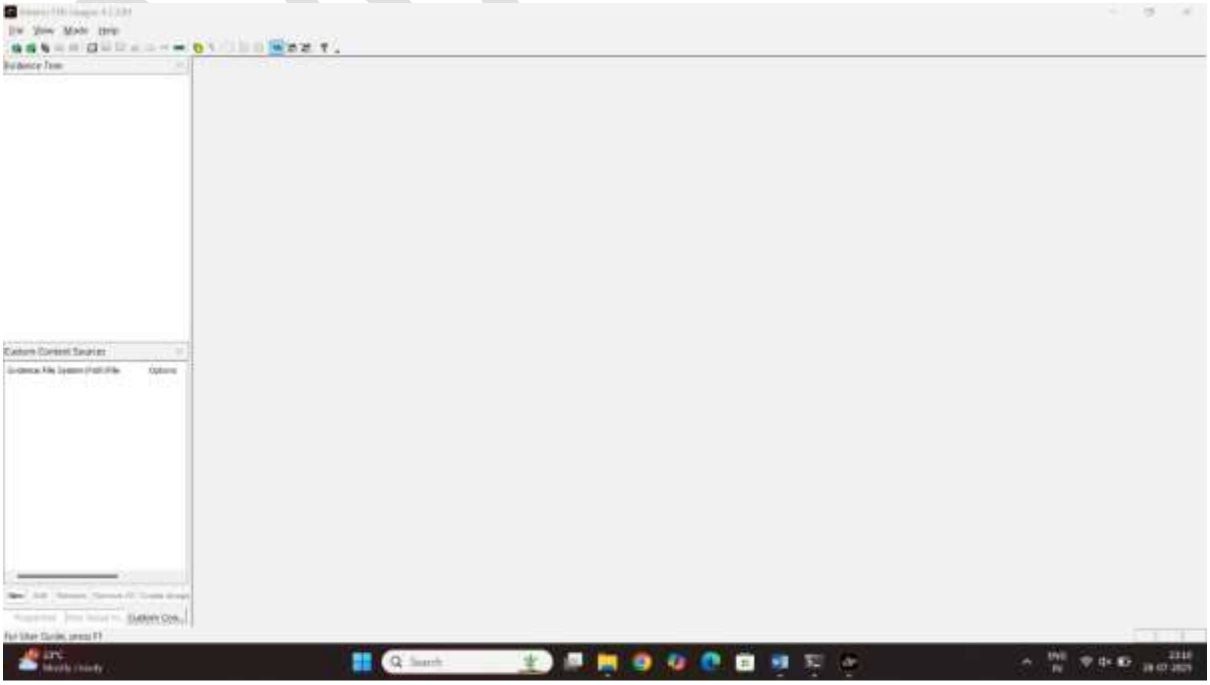


```
msedgewebview2     11040   8   7  157   2288     0:00:00.046    2:57:36.420
msedgewebview2      5888  10  19  461  34076     0:00:00.593    2:57:35.700
msedgewebview2      2284   8  18  331  11792     0:00:00.531    2:57:35.700
msedgewebview2     14300   8   8  172   8952     0:00:00.156    2:57:35.112
msedgewebview2     17012   4  18  326  46472     0:00:01.109    2:57:35.106
ApplicationFrameHost 14216   8   1  283   6516     0:00:00.562    2:35:43.888
AvastUI            25112   8  17  635  16168     0:00:00.125    1:54:07.840
svchost            16856   8  10  341   3700     0:00:01.375    1:48:13.821
FileCoAuth         25940   8   2  219   9828     0:00:00.140    1:26:29.174
svchost            24996   8   2  149   1548     0:00:00.031    1:24:03.400
taskhostw          26464   8   4  390   6908     0:00:00.578    1:12:52.208
dllhost            22068   8   3  226   2492     0:00:00.046    0:55:56.241
svchost             4040   8   1  158   1660     0:00:00.015    0:54:22.642
aswidsagent        10604   8  36 1044  66752     0:00:13.578    0:50:40.438
msedge             12416   8  49 1198  43988     0:00:02.687    0:49:34.476
msedge             26452   8   7  162   2572     0:00:00.046    0:49:34.887
msedge             26064  10  13  348  29312     0:00:00.203    0:49:13.914
msedge             10484   8  22  359  12864     0:00:00.375    0:49:13.912
msedge             28968   8  18  187   8828     0:00:00.140    0:49:33.261
svchost             6616   8   4  178   3988     0:00:00.078    0:48:01.988
WhatsApp            2080   8  18  640  39840     0:00:00.656    0:36:17.446
RuntimeBroker       3092   8   5  318   3804     0:00:00.156    0:36:16.190
svchost            15108   8   3  175   1920     0:00:00.031    0:34:32.231
LockApp            24440   8  16  602  16308     0:00:01.234    0:33:18.363
svchost            14432   8   9  421   9720     0:00:00.937    0:33:13.347
svchost            26588   8   2  204   2504     0:00:00.343    0:33:13.028
RuntimeBroker       8060   8  13  551  10252     0:00:01.921    0:33:12.119
dllhost            10724   8   2  135   1692     0:00:00.062    0:33:10.151
svchost            18700   8  11  377   4304     0:00:00.562    0:33:05.749
splunk-optimize    10516   8   1    4    452     0:00:00.000    0:31:49.890
WINWORD            19676   8  21 1429 131124     0:00:29.359    0:05:46.266
cmd                 9588   8   4   92   5740     0:00:00.015    0:05:14.899
conhost            20892   8   4  146   1604     0:00:00.015    0:05:14.852
OpenConsole        16540   8   9  283   3124     0:00:00.031    0:05:14.736
WindowsTerminal     8728   8  14  678  26704     0:00:01.656    0:05:14.885
SearchProtocolHost 17980   8   6  374   2988     0:00:00.125    0:04:57.942
SearchFilterHost   24872   8   4  181   2116     0:00:00.015    0:04:57.666
svchost            12816   8   6  167   1824     0:00:00.031    0:02:58.580
pslist              6316  13   6  383   4912     0:00:00.687    0:00:07.392

C:\PSTools>
```

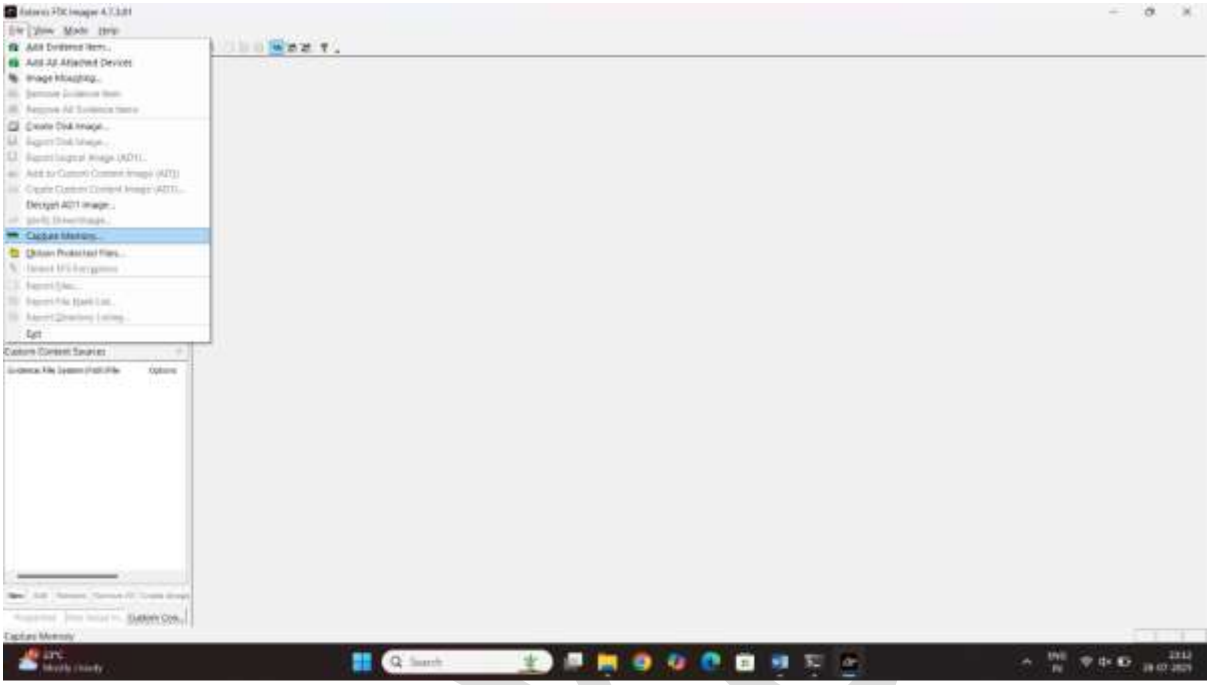
Lab2 investigate forensic image of windows RAM capture

Using ftk imager

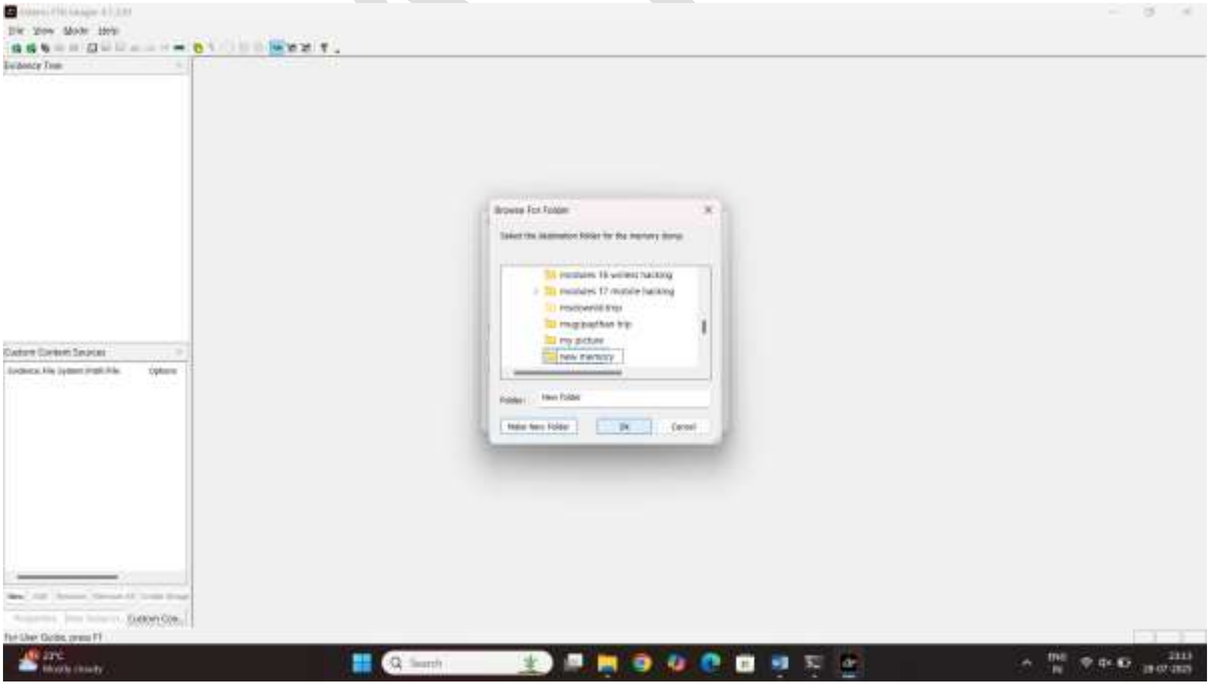
Step1 start the ftk imager

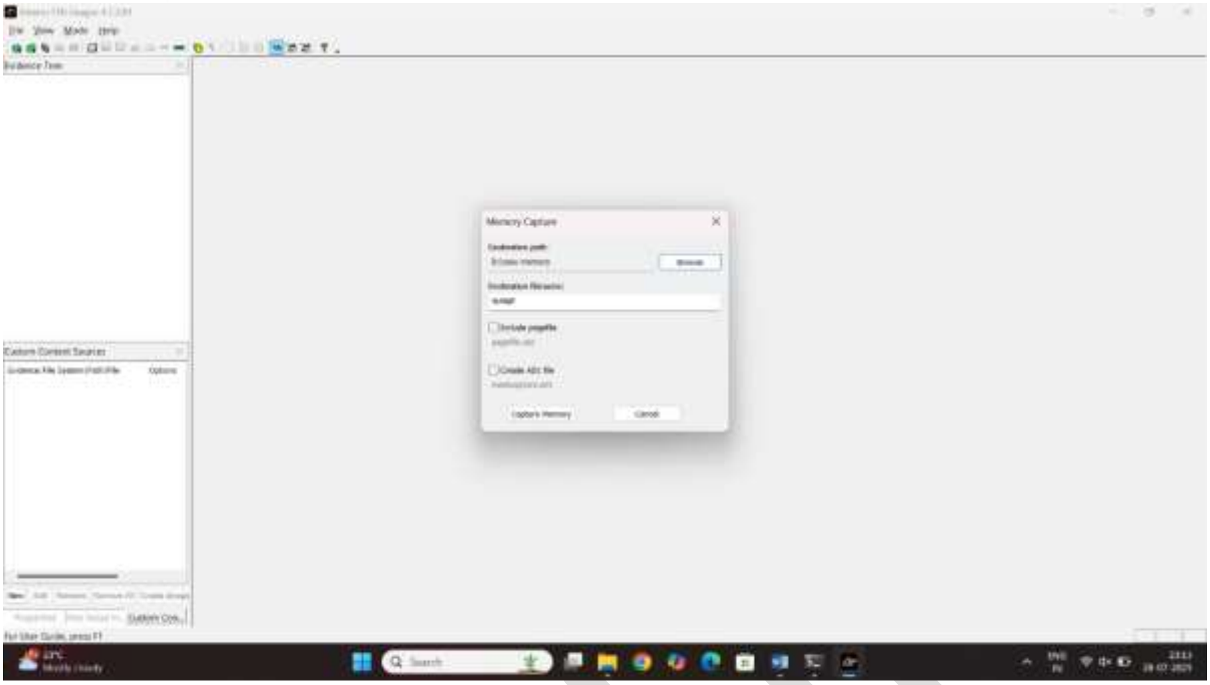


Step2 click on the file and select the option capture memory

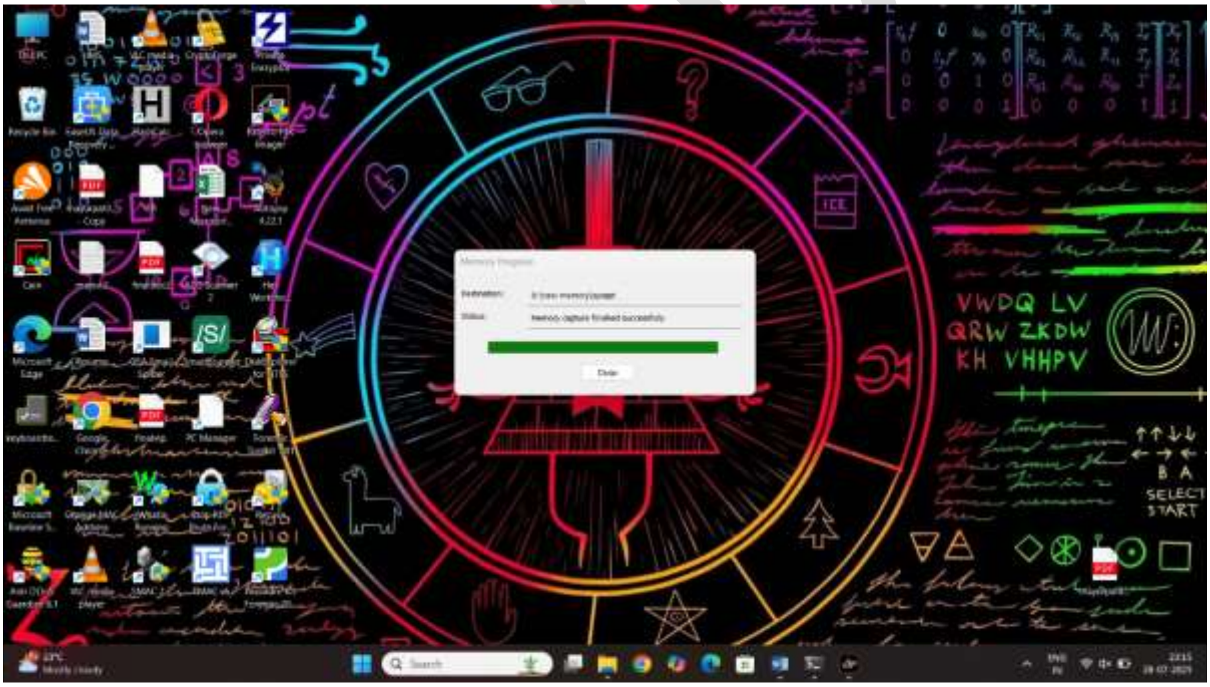


Step3 select the destination folder and file name



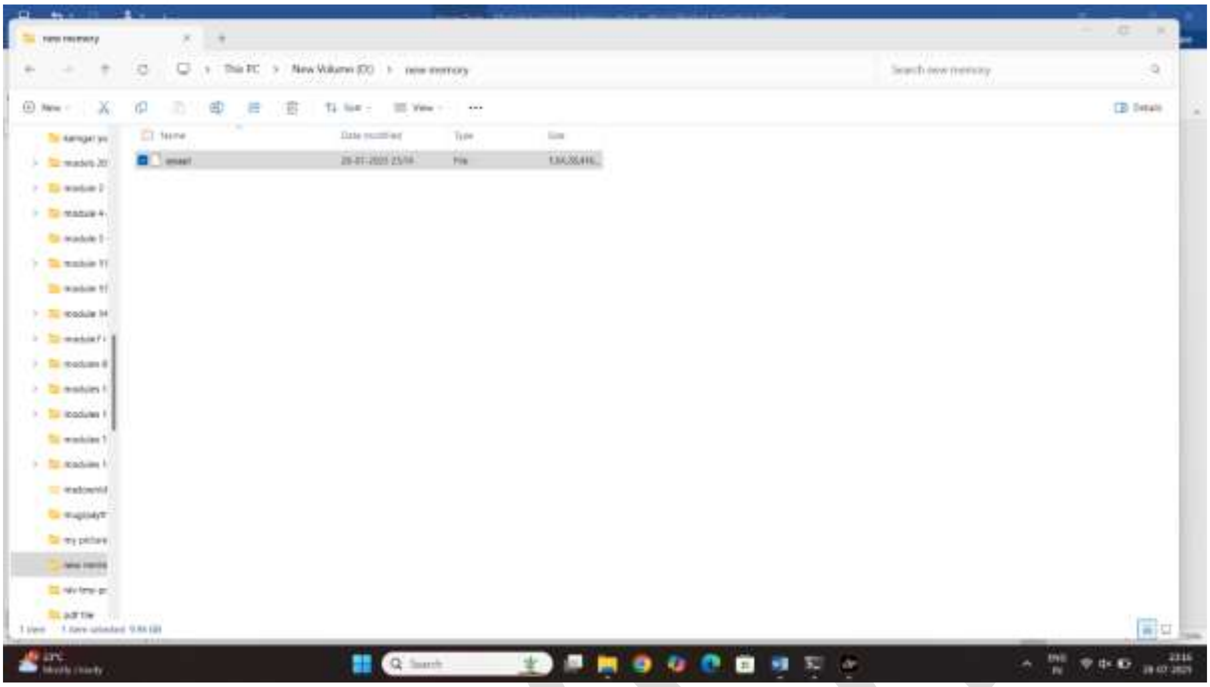


Step4 click on the capture memory



Memory capture finished successfully

Result:



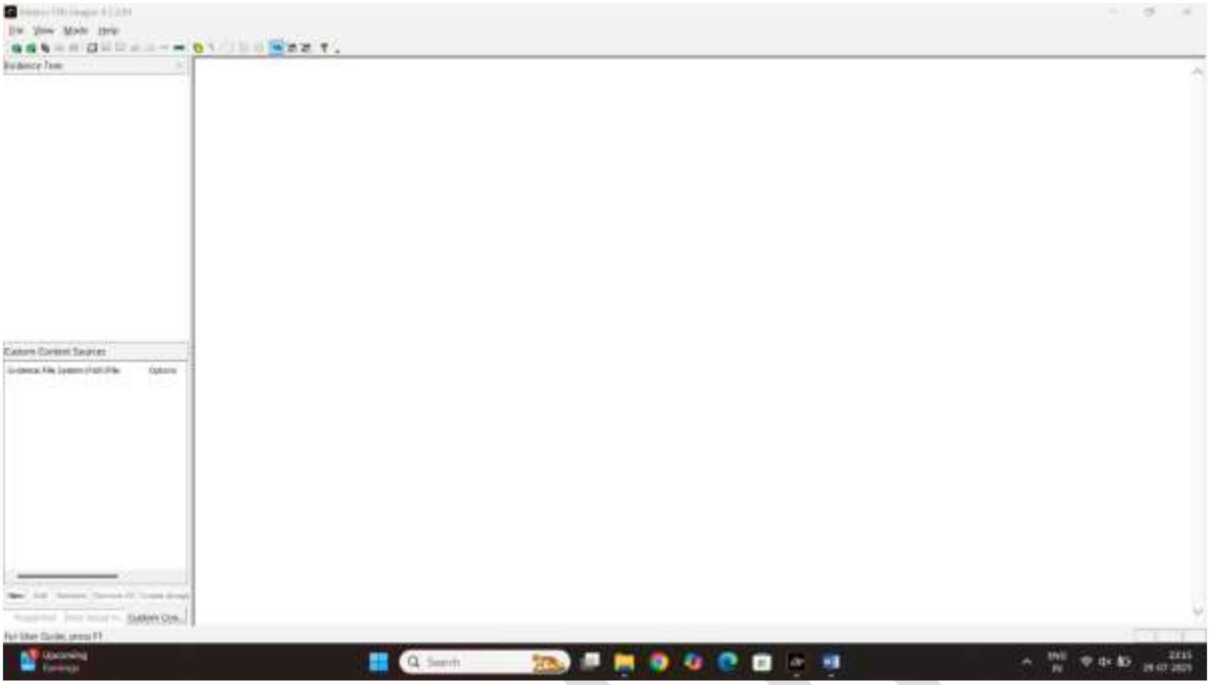
Name	Date modified	Type	Size
email	28-07-2025 23:14	File	1,04,00,416...

Lab 3 extract and

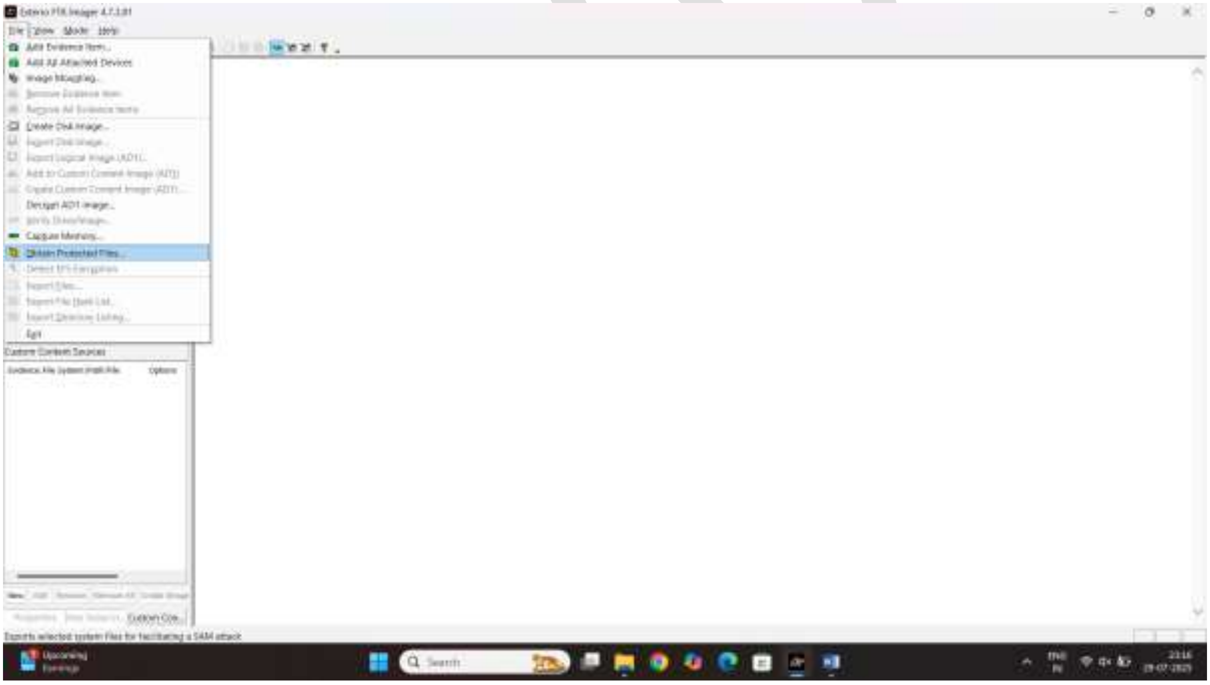
Lab 4 capture and examine windows registry files on live system

Using FTK

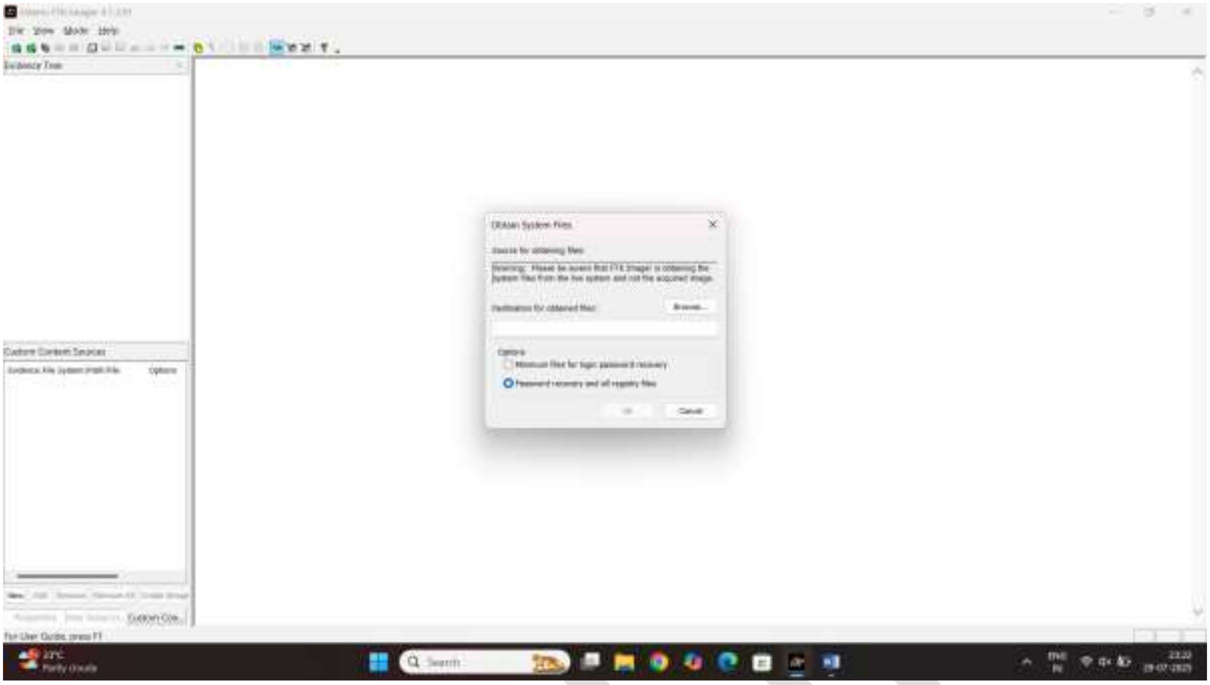
Step1 start the application


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value In... Custom Con...
For User Guide, press F1

Step2 click on file and select the protected file


Exterro FTK Imager 4.7.3.81
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
Custom Content Sources
Evidence:File System|Path|File Options
Exports selected system files for facilitating a SAM attack

Step3 select the option password recovery and registry



Obtain System Files

Source for obtaining files

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

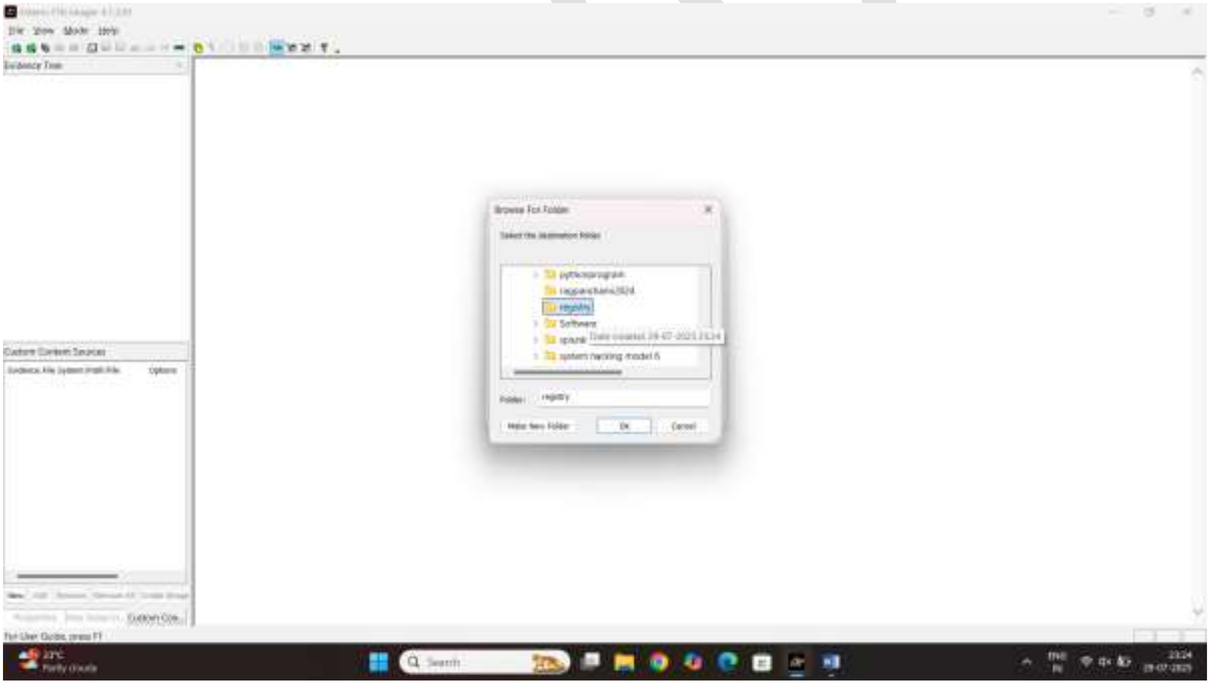
Destination for obtained files:

Options

□ Minimum files for login password recovery

● Password recovery and all registry files

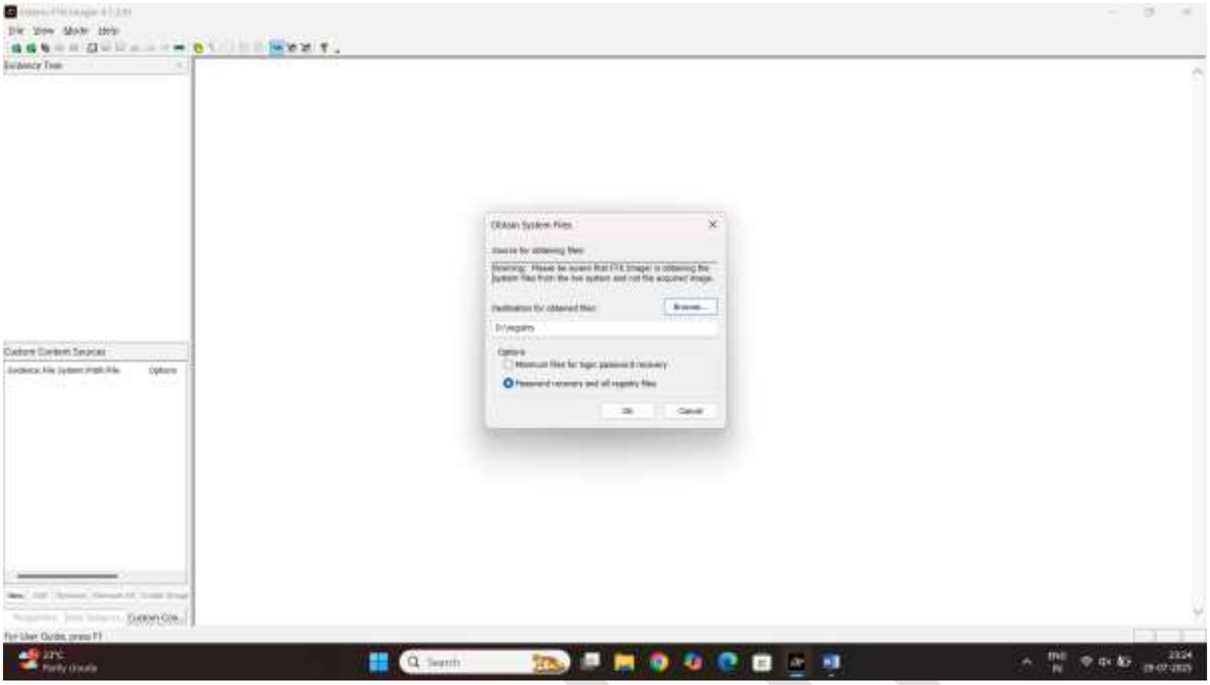
Step4 select the destination file path



Browse For Folder

Select the destination folder

Folder: registry



Obtain System Files

Source for obtaining files:

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files: Browse...

D:\registry

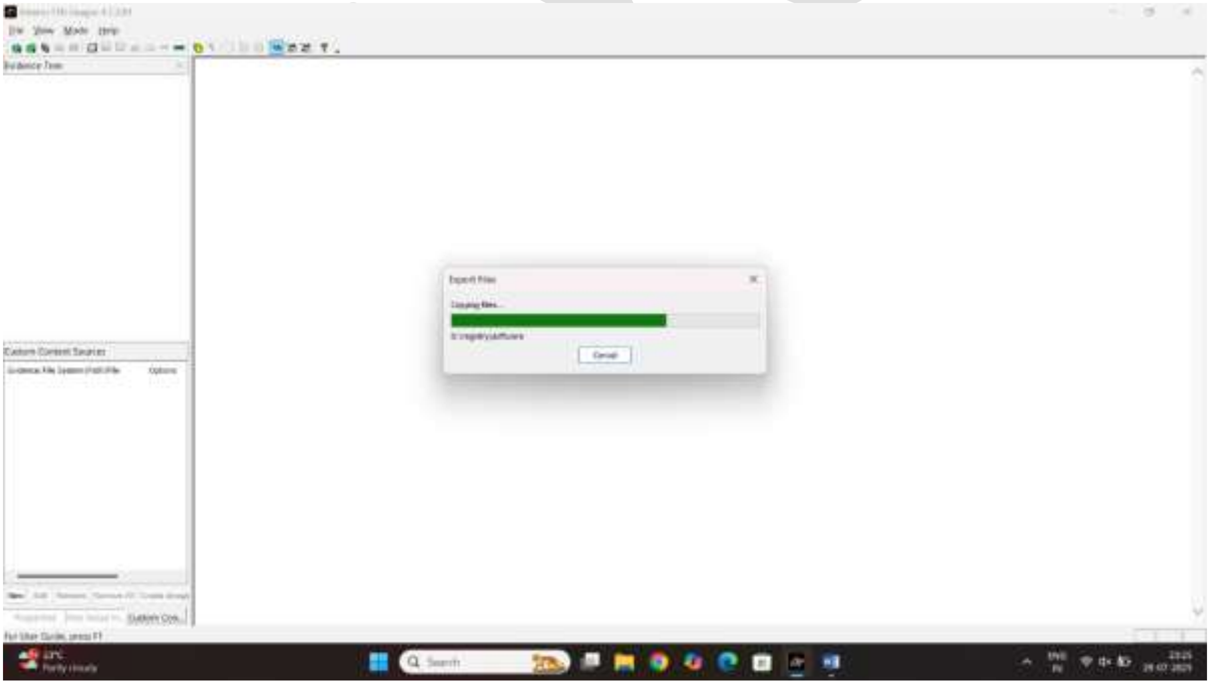
Options

○ Minimum files for login password recovery

● Password recovery and all registry files

Ok Cancel

Click on the ok

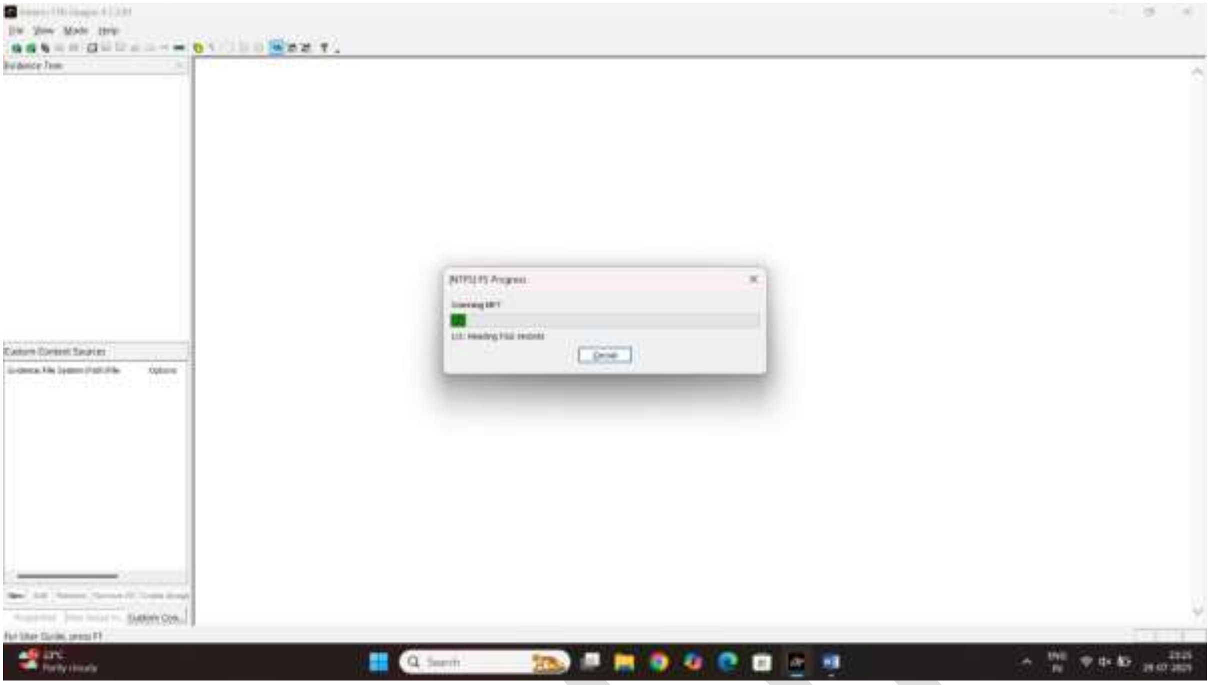


Export Files

Copying files...

D:\registry\software

Cancel

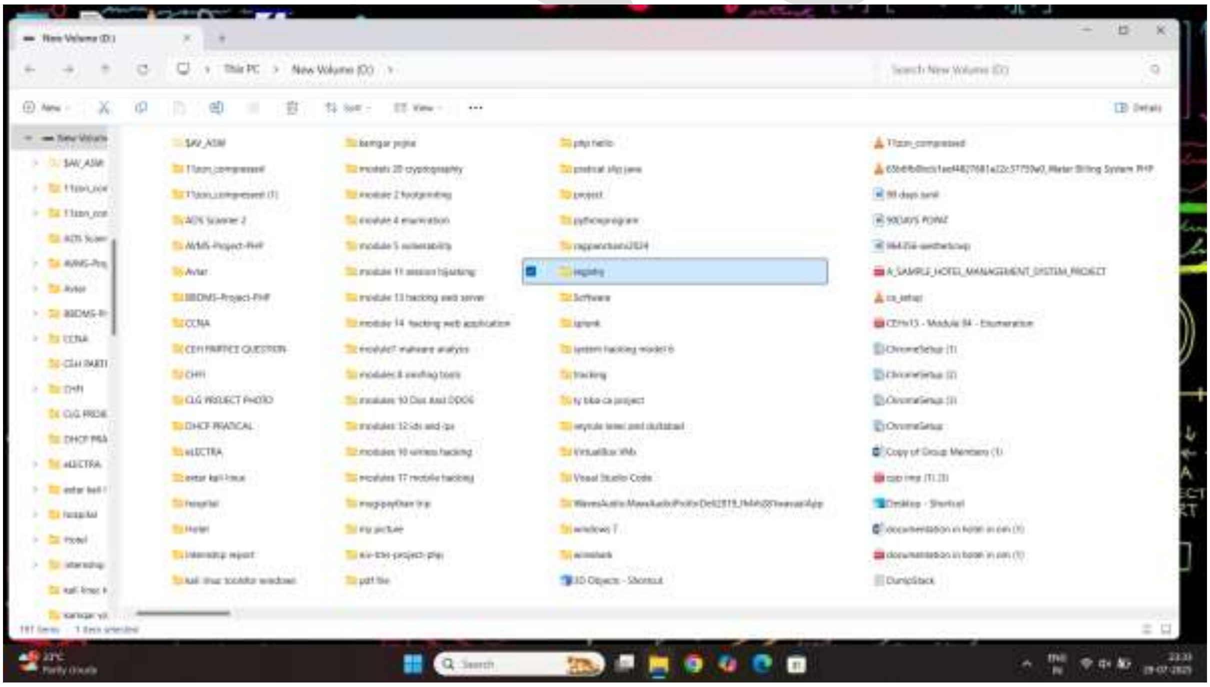


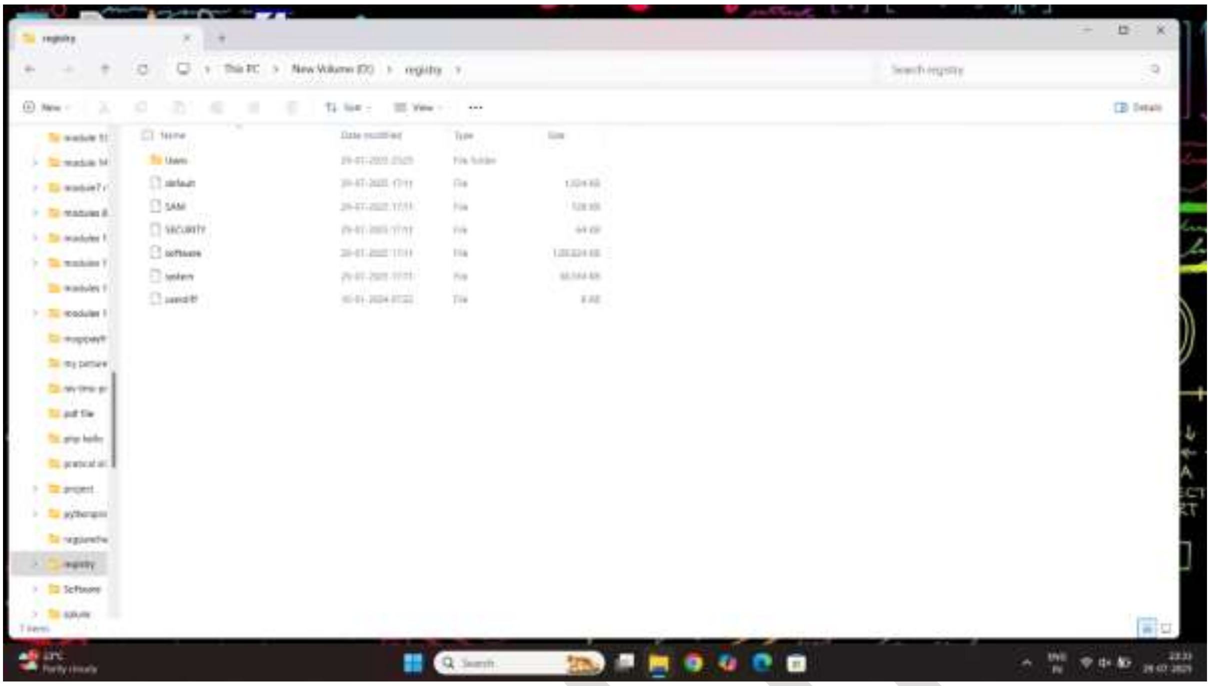
[NTFS] FS Progress

Scanning MFT

Reading FILE records

Step5 go to file registry



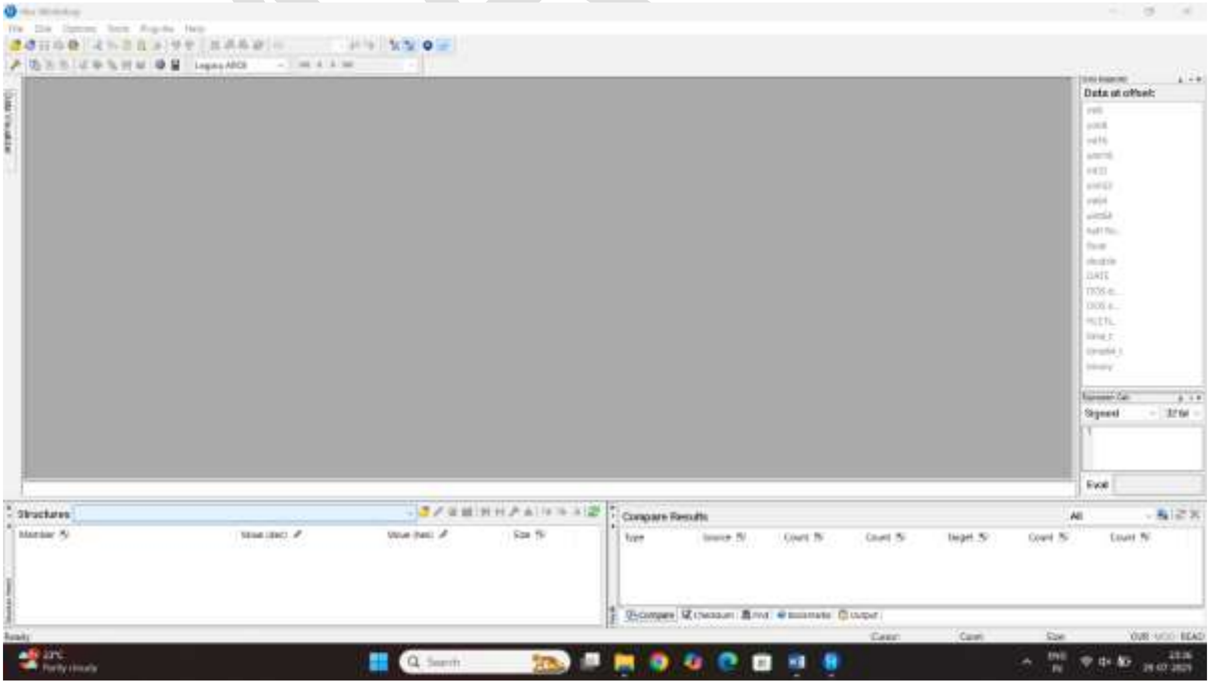


This PC > New Volume (D:) > registry

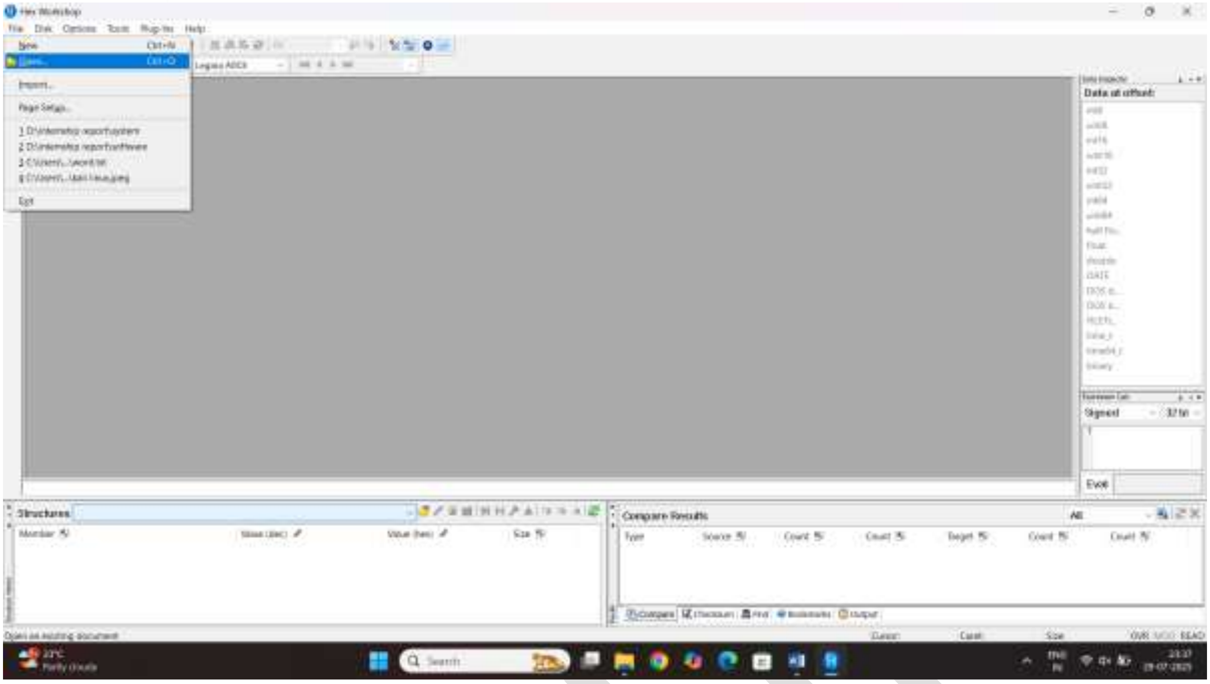
Name	Date modified	Type	Size
Users	29-07-2025 23:25	File folder	
default	29-07-2025 17:11	File	1,024 KB
SAM	29-07-2025 17:11	File	128 KB
SECURITY	29-07-2025 17:11	File	64 KB
software	29-07-2025 17:11	File	120,024 KB
system	29-07-2025 17:11	File	50,144 KB
userdiff	10-01-2024 07:22	File	8 KB

Lab 5 How to check this registry file using hex work shop

Step1 start the application

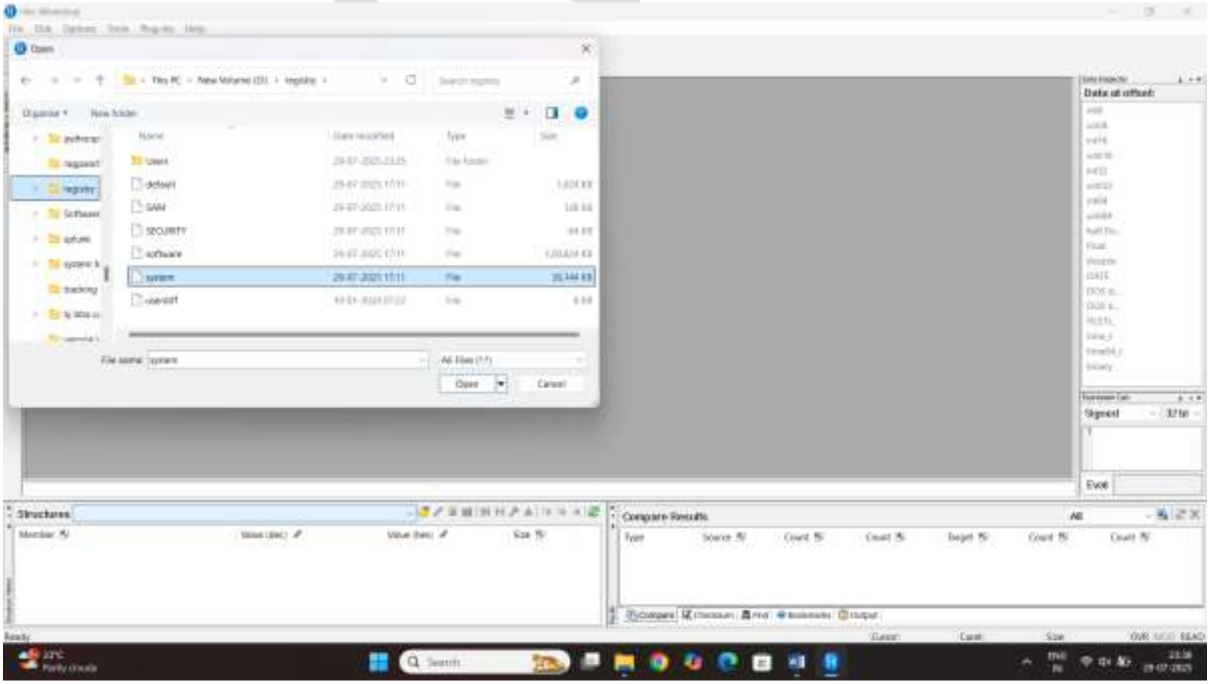


Step2 click on the open option


Hex Workshop
File Disk Options Tools Plug-Ins Help
New Ctrl+N
Open... Ctrl+O
Import...
Page Setup...
1 D:\internship report\system
2 D:\internship report\software
3 C:\Users\...\word.txt
4 C:\Users\...\train.jpeg
Exit
Data at offset:
Structures
Compare Results
Open an existing document

Step3 select the file registry option

Step4 select the registry file



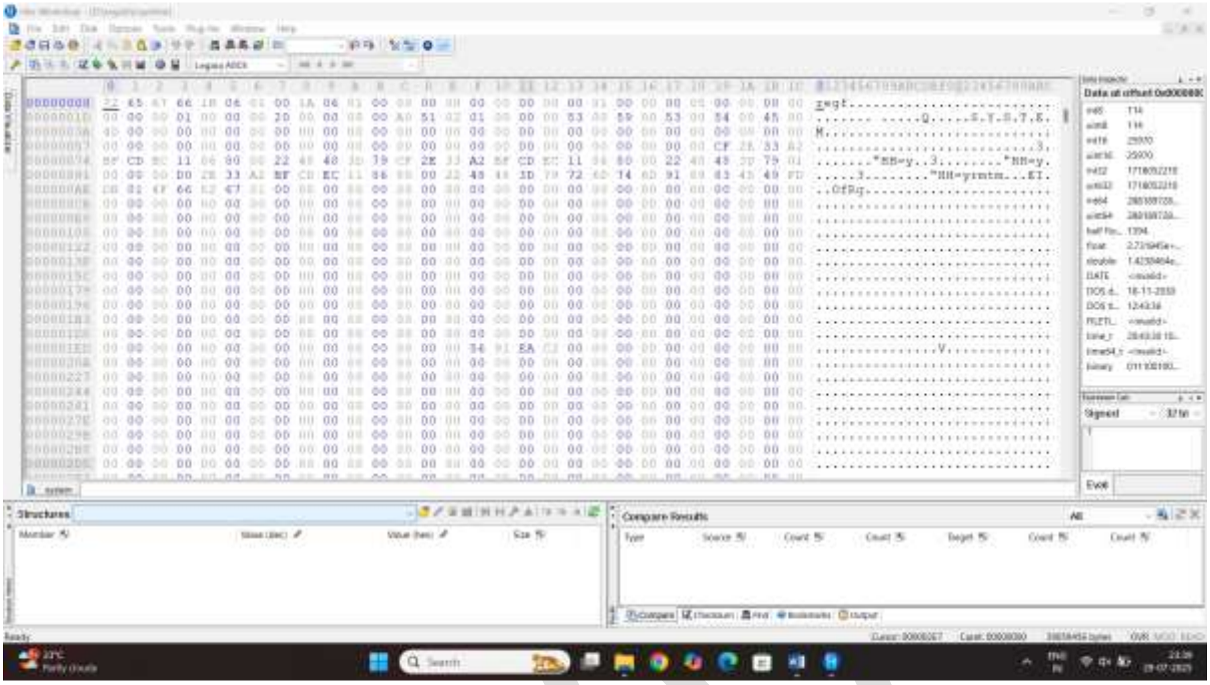
Name	Date modified	Type	Size
Users	29-07-2025 23:25	File folder	
default	29-07-2025 17:11	File	1,024 KB
SAM	29-07-2025 17:11	File	128 KB
SECURITY	29-07-2025 17:11	File	64 KB
software	29-07-2025 17:11	File	1,03,424 KB
system	29-07-2025 17:11	File	35,144 KB
userdiff	12-01-2024 07:22	File	8 KB

File name: system

All Files (*.*)

Click on the open

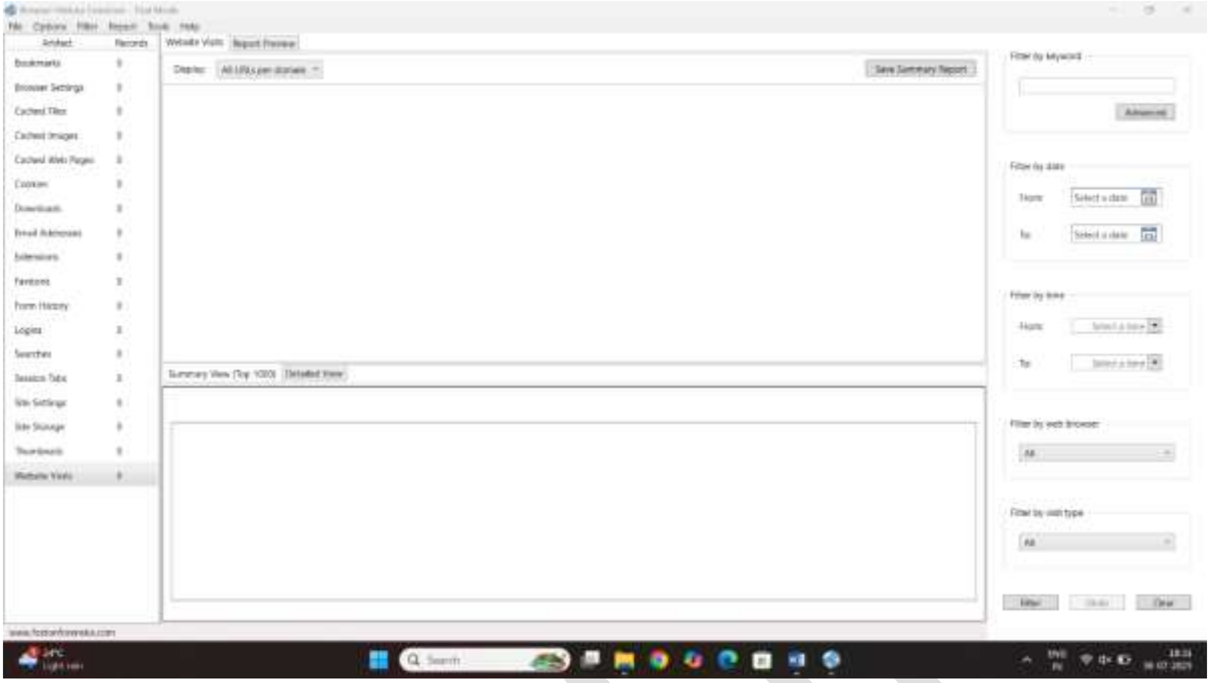
Result:



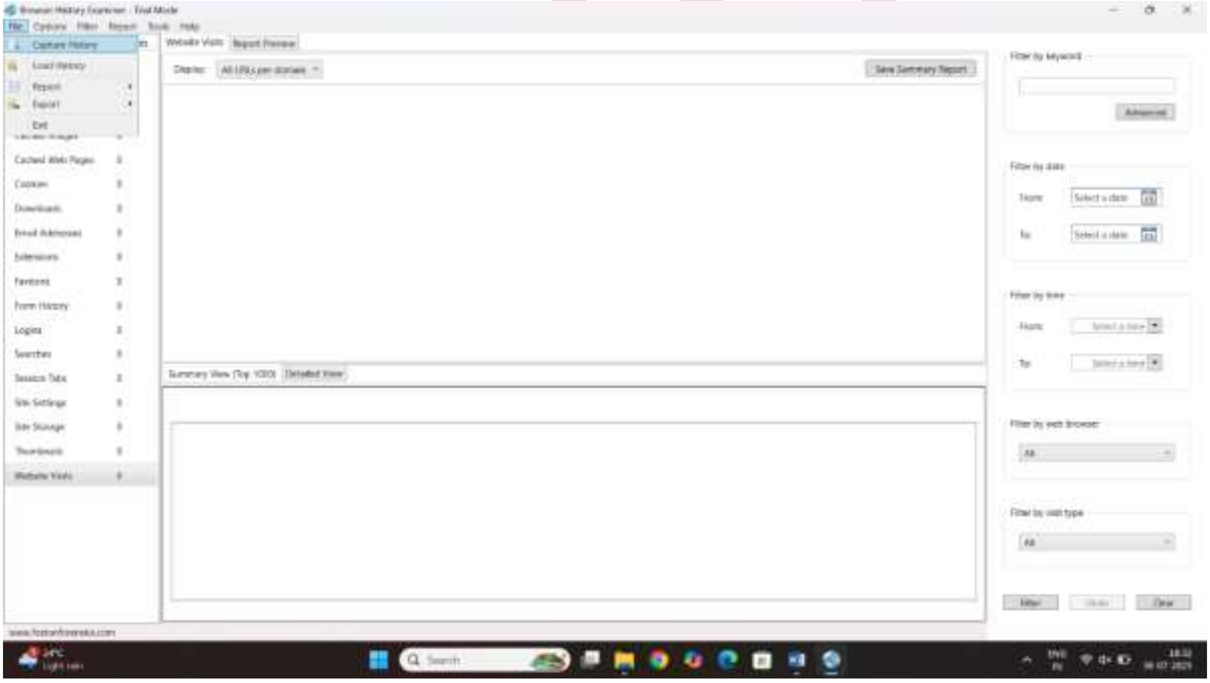
Lab6 extract and rebuild cached web page of google chrome

There was tool called browser History

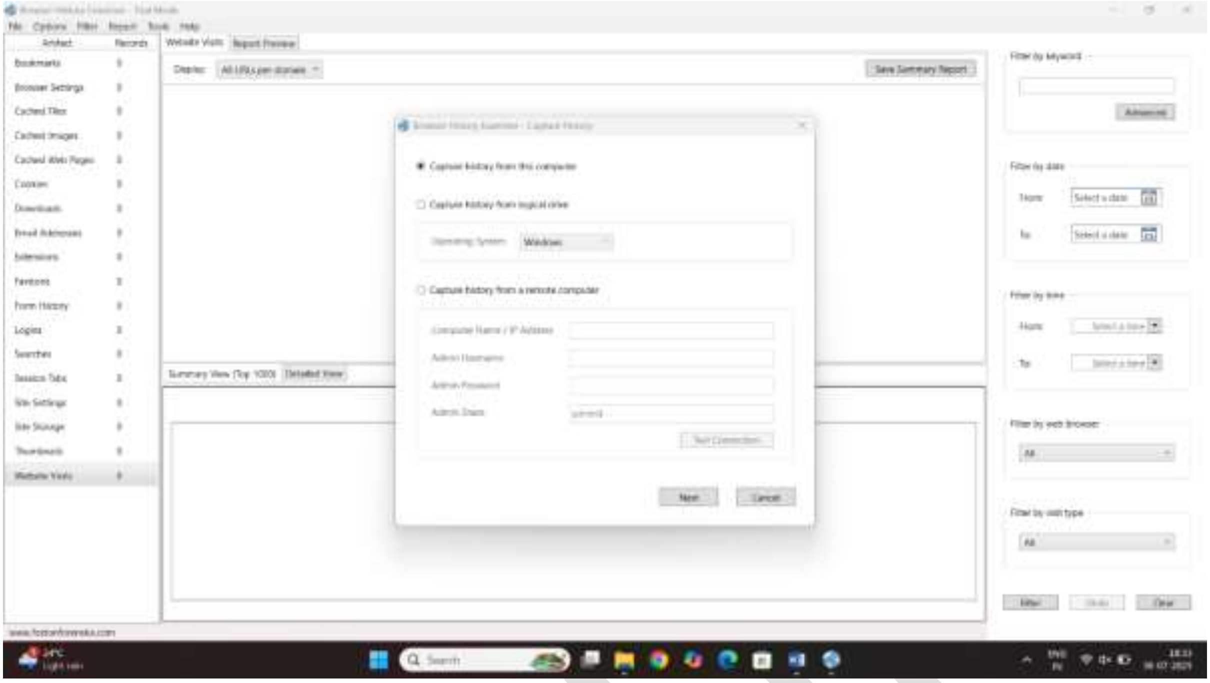
Step1 start the application



Step2 click on the capture history



Step3 click capture history from this computer



Browser History Examiner - Capture History

● Capture history from this computer

○ Capture history from logical drive

Operating System: Windows

○ Capture history from a remote computer

Computer Name / IP Address:

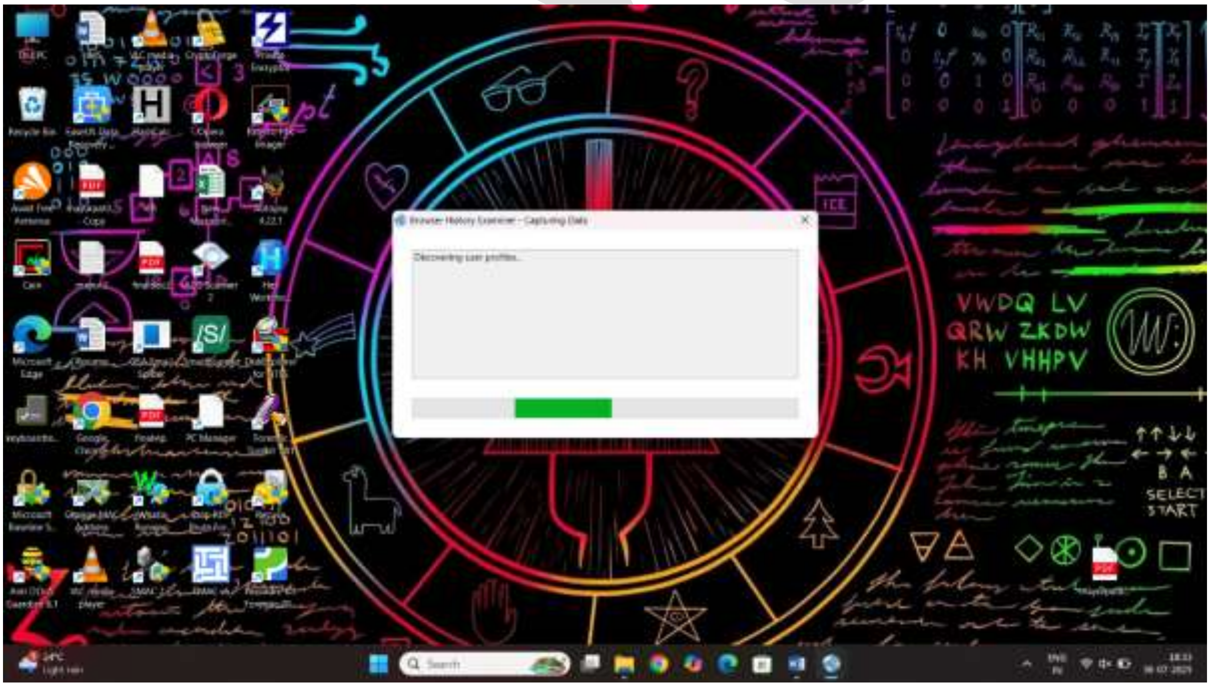
Admin Username:

Admin Password:

Admin Share: admin$

Click on the next

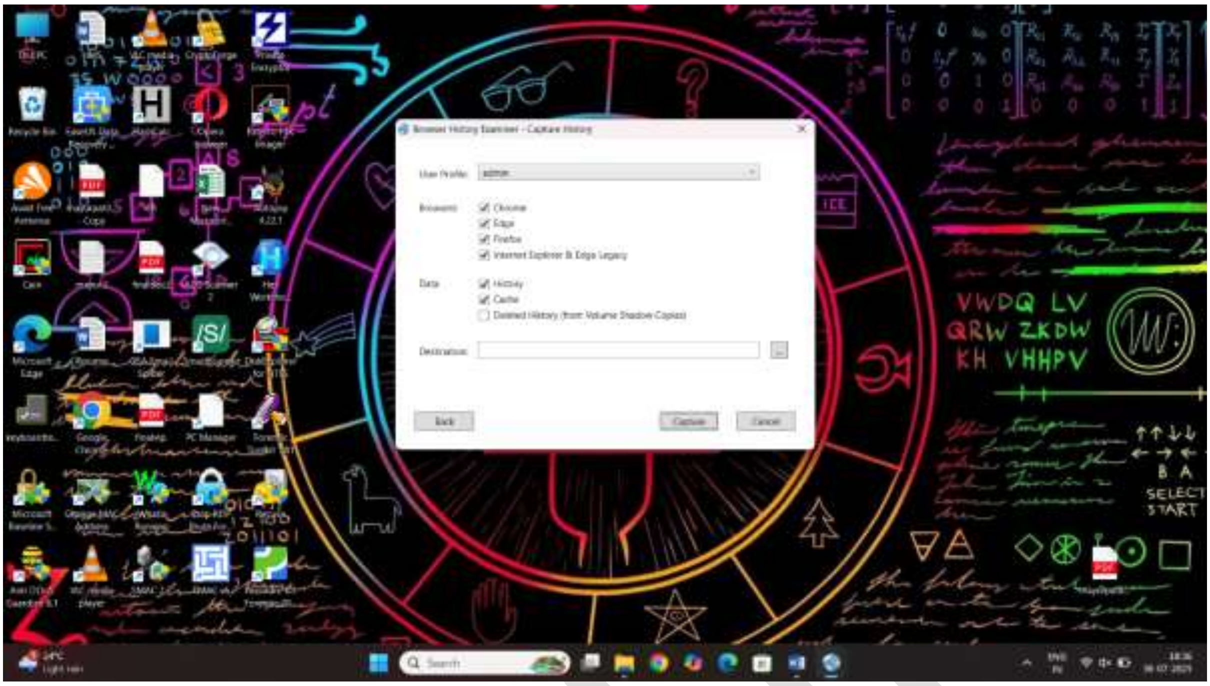
Step4 start the DB process



Browser History Examiner - Capturing Data

Discovering user profiles...

Click on the next



Browser History Examiner - Capture History

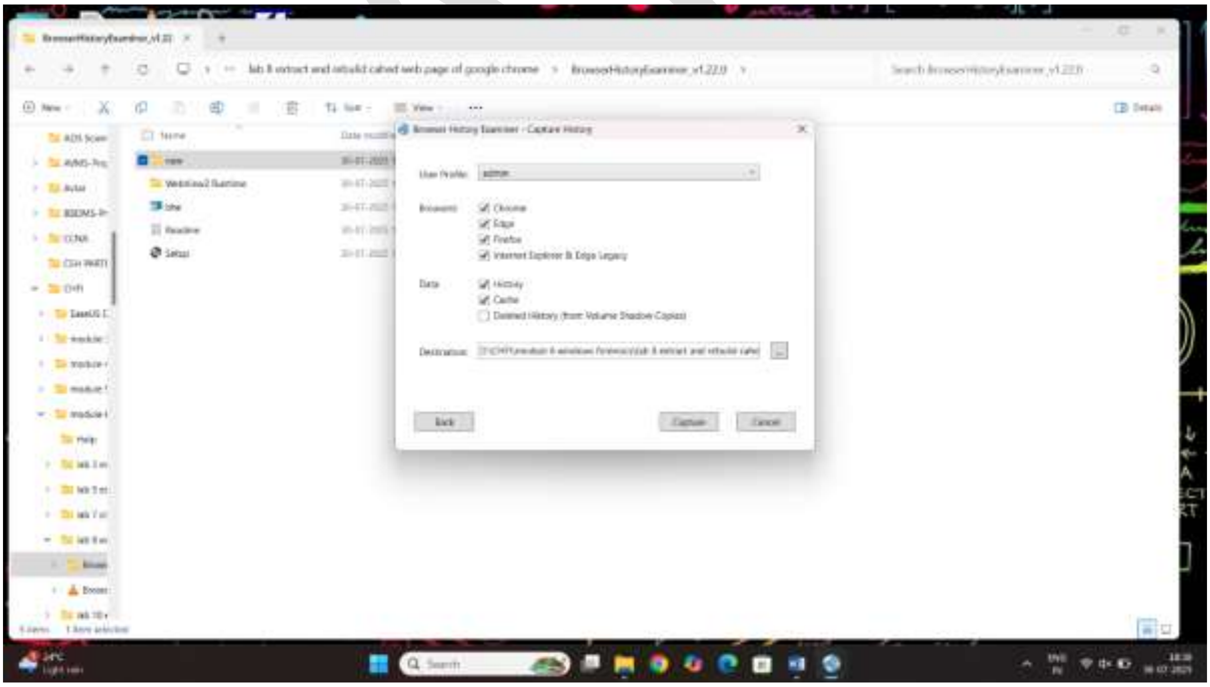
User Profile: admin

Browsers: ☑ Chrome ☑ Edge ☑ Firefox ☑ Internet Explorer & Edge Legacy

Data: ☑ History ☑ Cache ☐ Deleted History (from Volume Shadow Copies)

Destination:

Step5 select the destination file



lab 8 extract and rebuild cahed web page of google chrome > BrowserHistoryExaminer_v1.22.0

Browser History Examiner - Capture History

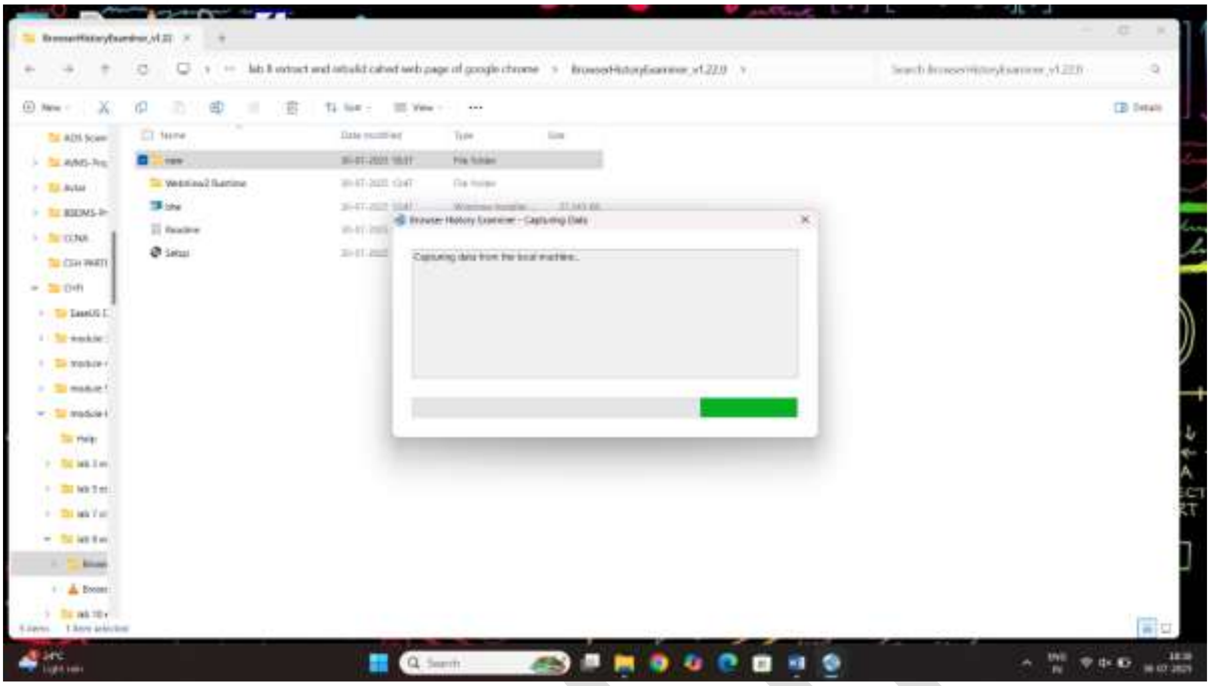
User Profile: admin

Browsers: ☑ Chrome ☑ Edge ☑ Firefox ☑ Internet Explorer & Edge Legacy

Data: ☑ History ☑ Cache ☐ Deleted History (from Volume Shadow Copies)

Destination: D:\CHFI\module 6 windows forensics\lab 8 extract and rebuild cahe

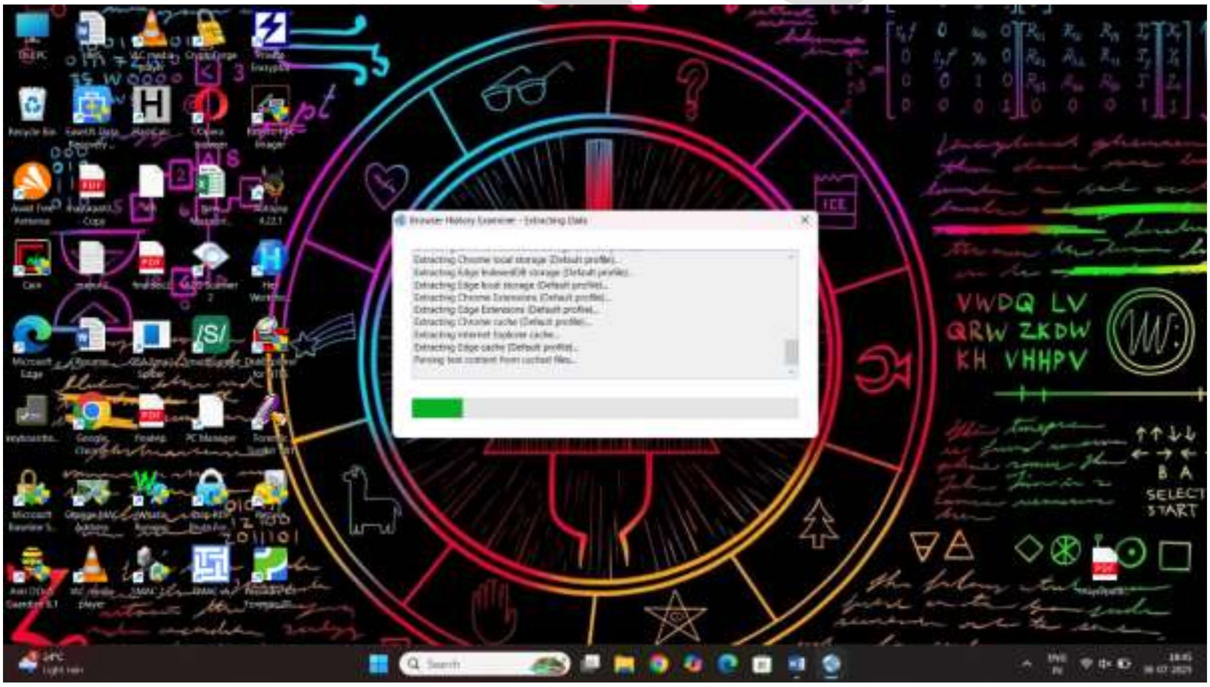
Click on the capture



Browser History Examiner - Capturing Data

```
Capturing data from the local machine...
```

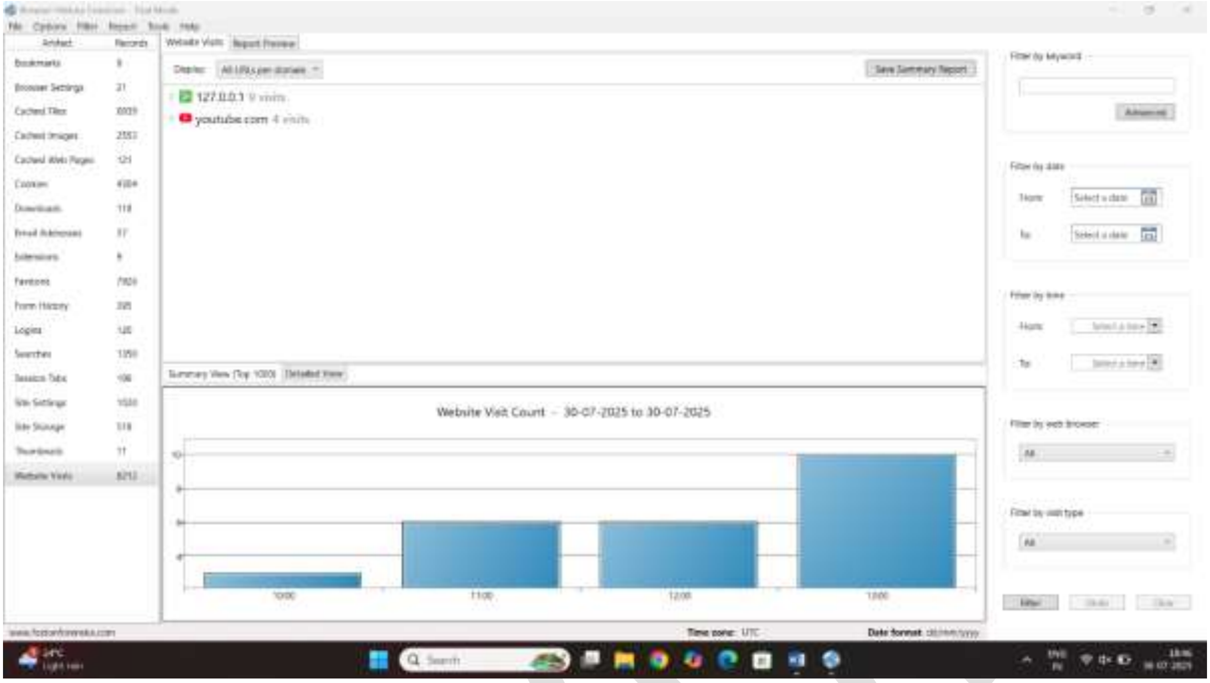
Step6 Extracting data process on



Browser History Examiner - Extracting Data

```
Extracting Chrome local storage (Default profile)...
Extracting Edge IndexedDB storage (Default profile)...
Extracting Edge local storage (Default profile)...
Extracting Chrome Extensions (Default profile)...
Extracting Edge Extensions (Default profile)...
Extracting Chrome cache (Default profile)...
Extracting Internet Explorer cache...
Extracting Edge cache (Default profile)...
Parsing text content from cached files...
```

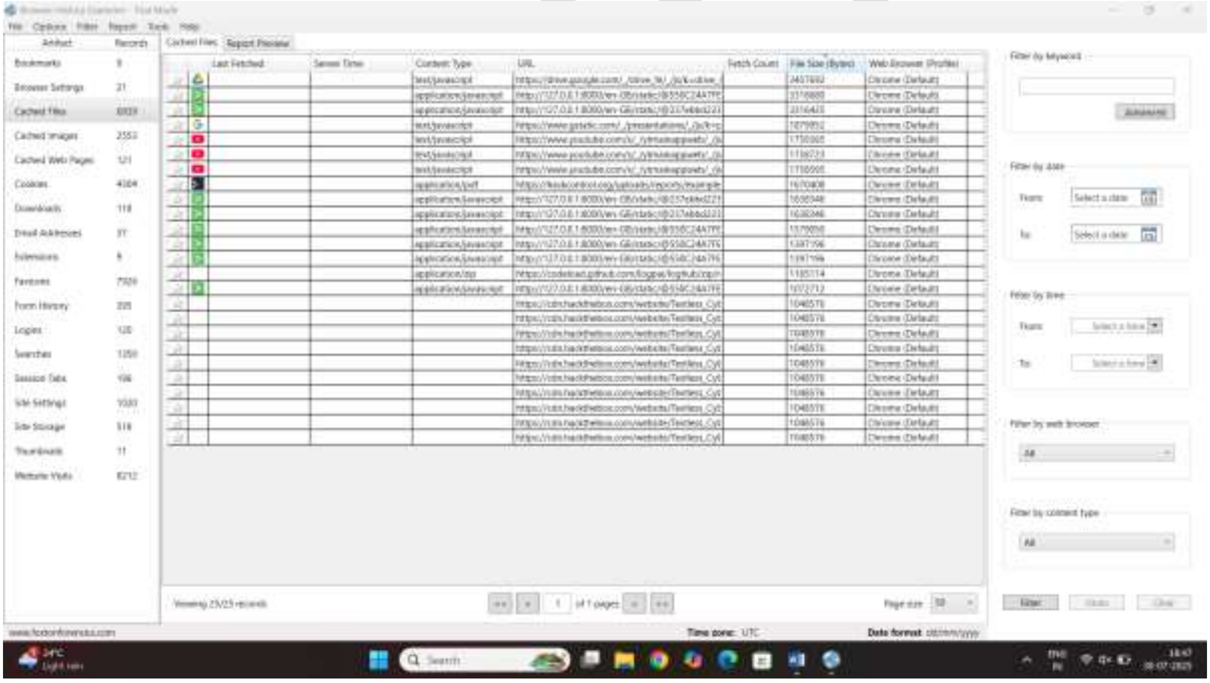
Result:



Artifact	Records
Bookmarks	9
Browser Settings	21
Cached Files	8939
Cached Images	2553
Cached Web Pages	121
Cookies	4304
Downloads	118
Email Addresses	37
Extensions	9
Favicons	7929
Form History	395
Logins	120
Searches	1350
Session Tabs	106
Site Settings	1533
Site Storage	518
Thumbnails	11
Website Visits	8212

127.0.0.1 9 visits

youtube.com 4 visits



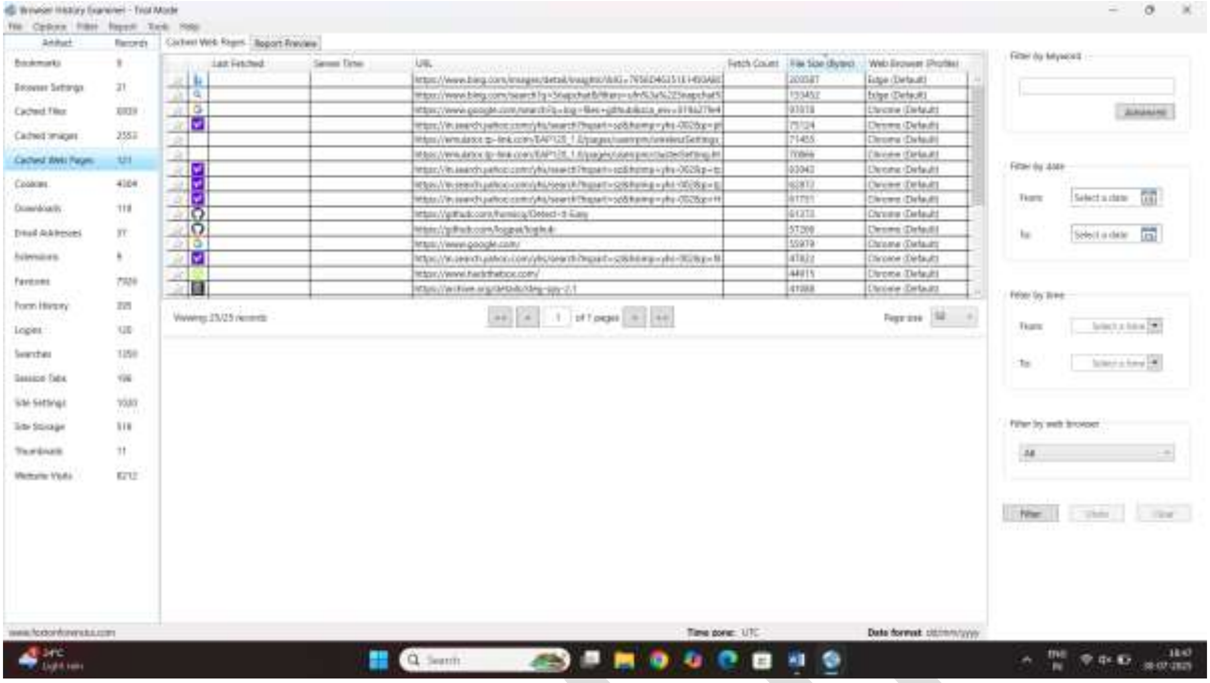
Artifact	Records
Bookmarks	9
Browser Settings	21
Cached Files	8939
Cached Images	2553
Cached Web Pages	121
Cookies	4304
Downloads	118
Email Addresses	37
Extensions	9
Favicons	7929
Form History	395
Logins	120
Searches	1350
Session Tabs	106
Site Settings	1533
Site Storage	518
Thumbnails	11
Website Visits	8212

Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
		text/javascript	https://drive.google.com/_/drive_fe/_/js/k=drive_		2457692	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@558C24A7FE		3316880	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@237ebbd221		3316420	Chrome (Default)
		text/javascript	https://www.gstatic.com/_/presentations/_/js/k=p		1079952	Chrome (Default)
		text/javascript	https://www.youtube.com/s/_/ytmainappweb/_/js		1750065	Chrome (Default)
		text/javascript	https://www.youtube.com/s/_/ytmainappweb/_/js		1738723	Chrome (Default)
		text/javascript	https://www.youtube.com/s/_/ytmainappweb/_/js		1738595	Chrome (Default)
		application/pdf	https://faculcontrol.org/uploads/reports/example		1670408	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@237ebbd221		1636348	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@237ebbd221		1636346	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@558C24A7FE		1579050	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@558C24A7FE		1397196	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@558C24A7FE		1397196	Chrome (Default)
		application/zip	https://codeload.github.com/logpai/loghub/zip/r		1185114	Chrome (Default)
		application/javascript	http://127.0.0.1:8000/en-GB/static/@558C24A7FE		1072712	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)
			https://cdn.hackthebox.com/website/Textless_Cyt		1048576	Chrome (Default)

Viewing 25/25 records

1 of 1 pages

Page size 50

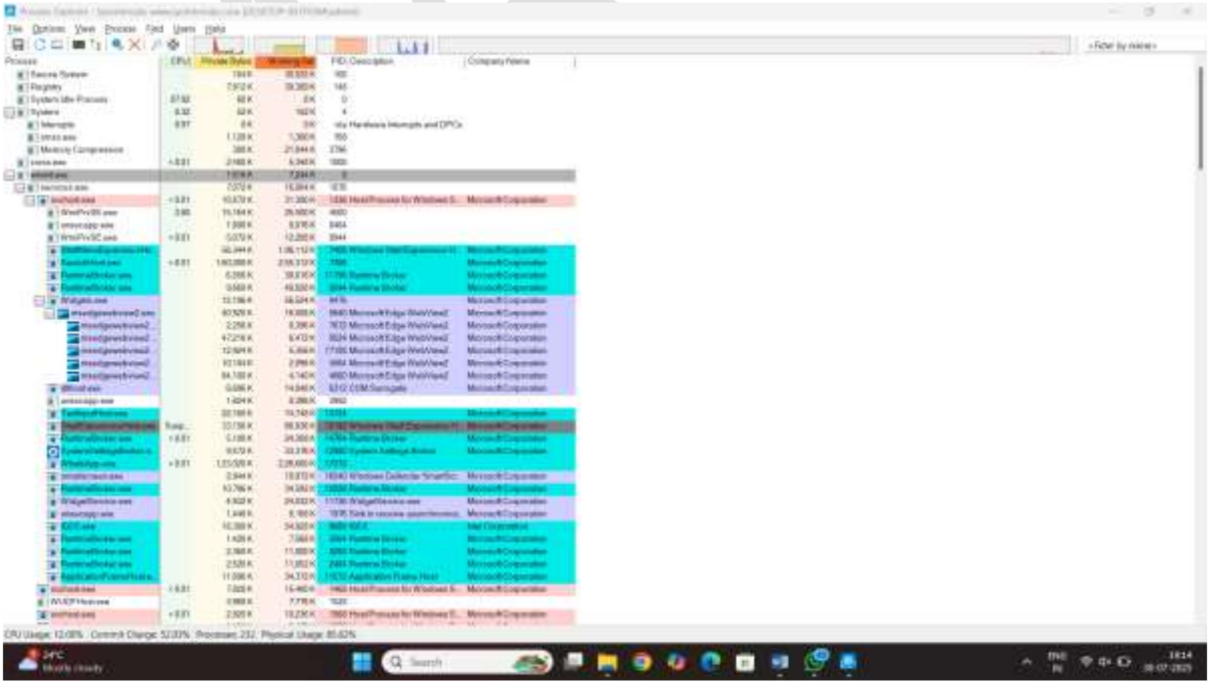


Artifact	Records
Bookmarks	8
Browser Settings	21
Cached Files	3303
Cached Images	2553
Cached Web Pages	121
Cookies	4304
Downloads	118
Email Addresses	37
Extensions	8
Favicons	7929
Form History	335
Logins	120
Searches	1359
Session Tabs	196
Site Settings	1033
Site Storage	518
Thumbnails	11
Website Visits	8212

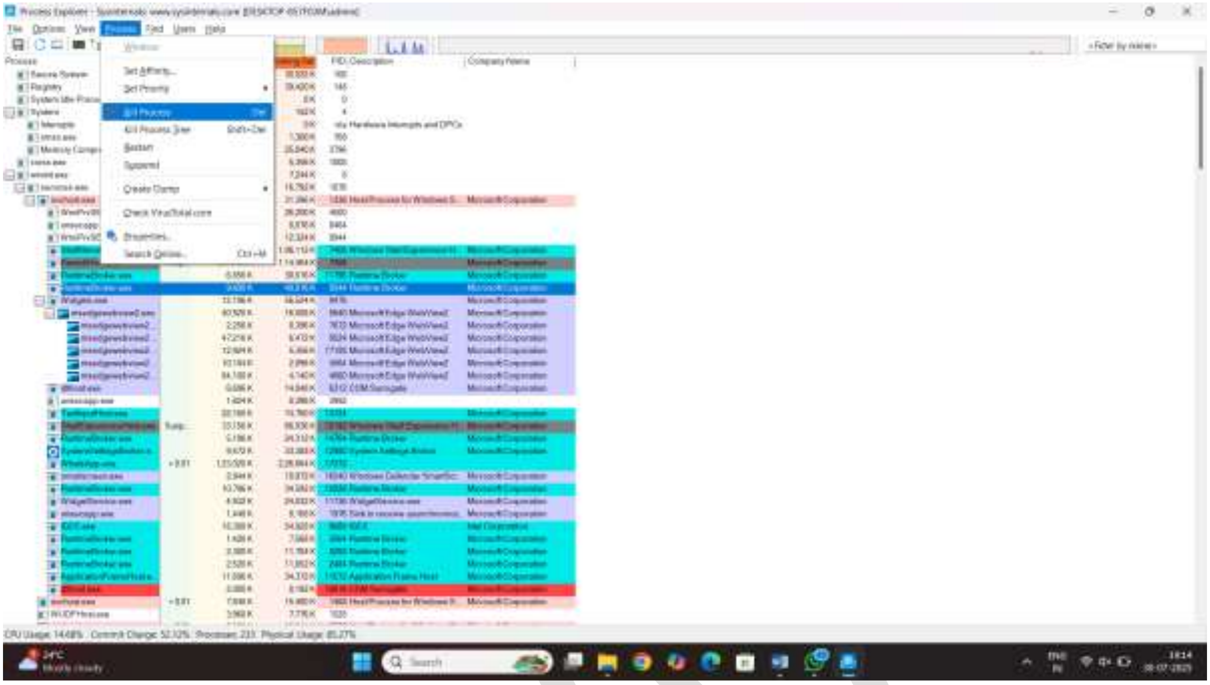
Viewing 25/25 records

Lab7 extract information about loaded process on a computer

Step1 start the application



Step2 how to kil malicious process


Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Users Help
Window
Set Affinity...
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend
Create Dump
Check VirusTotal.com
Properties...
Search Online... Ctrl+M
CPU Usage: 14.68% Commit Charge: 52.12% Processes: 233 Physical Usage: 85.27%

Click on kill process