NAME: N. Raghavendra Reddy

REG NO:192125031

CSA5207-CYBER FORENSICS

EXPERIMENT-01

The Count of Deleted Files using Forensic Tools

Aim of the Experiment:

Identify the count of deleted files using forensic tools

Procedure:

Step 1: Download Recover myfile tool
URL: Data recovery software download: Get Recover My Files here

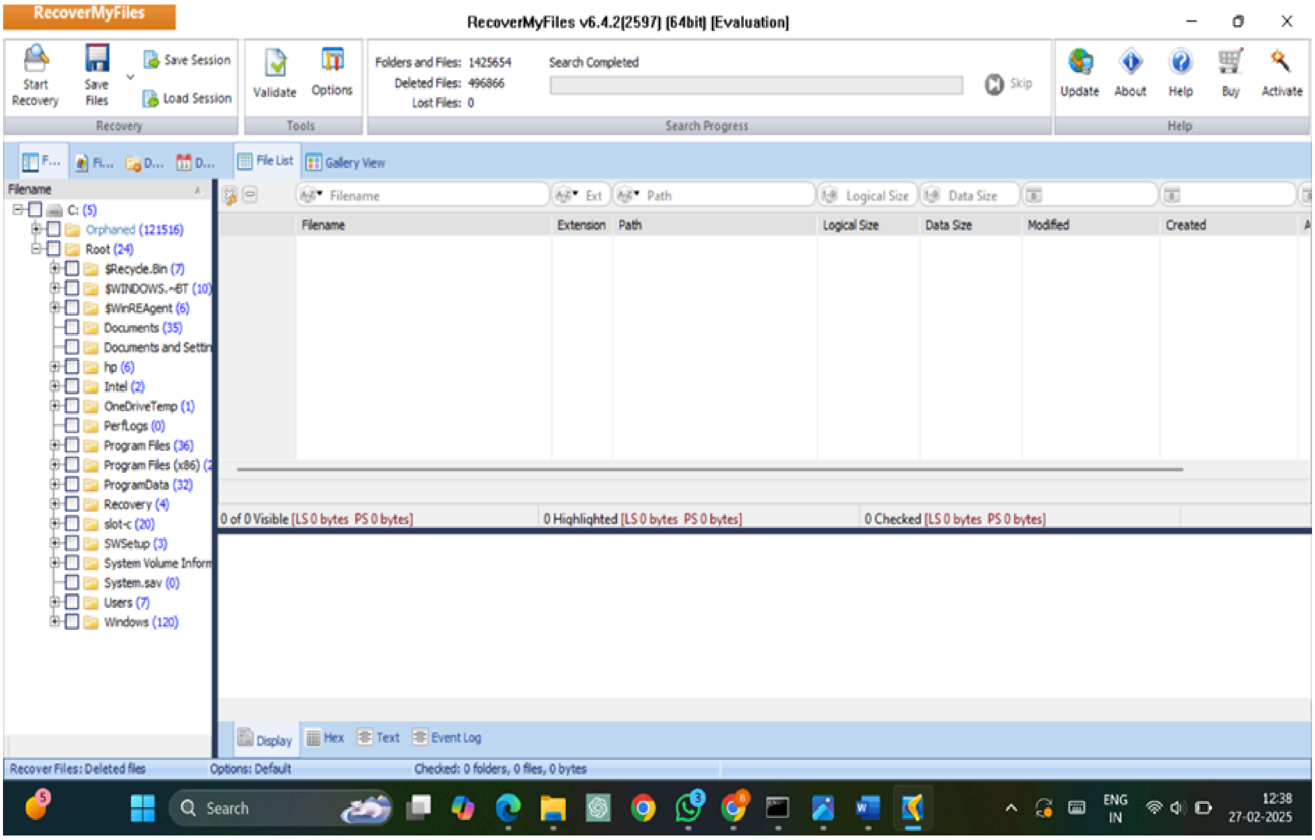
Step 2: Setup from the exe file downloaded

Step 3: Select the drive to recover the count of the deleted files

Step 4: Start the recover process

Step 5: Wait for the scanning process to complete

Step 6: After the completion of the scanning process, the count of the deleted files can be found and analysed. (Fig 1)



RecoverMyFiles v6.4.2[2597] [64bit] [Evaluation]

Folders and Files: 1425654
Deleted Files: 496866
Lost Files: 0

Search Completed

Filename
- C: (5)
  - Orphaned (121516)
  - Root (24)
    - $Recycle.Bin (7)
    - $WINDOWS.~BT (10)
    - $WinREAgent (6)
    - Documents (35)
    - Documents and Settin
    - hp (6)
    - Intel (2)
    - OneDriveTemp (1)
    - PerfLogs (0)
    - Program Files (36)
    - Program Files (x86) (2
    - ProgramData (32)
    - Recovery (4)
    - slot-c (20)
    - SWSetup (3)
    - System Volume Inform
    - System.sav (0)
    - Users (7)
    - Windows (120)

Filename	Extension	Path	Logical Size	Data Size	Modified	Created

0 of 0 Visible [LS 0 bytes PS 0 bytes] 0 Highlighted [LS 0 bytes PS 0 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

Recover Files: Deleted files Options: Default Checked: 0 folders, 0 files, 0 bytes

12:38
27-02-2025

Result:

The experiment of Identifying the count of deleted files using forensic tools successfully executed.

EXPERIMENT-02

Hiding and extracting a text file behind an image file.

Aim of the Experiment:

To study the steps for hiding and extract any text file behind an image file using Command Prompt.

Any file like .rar .jpg .txt or any file can be merged inside another file. In a simple way, we shall learn how to hide a text file inside an image file using the Command Prompt.

How to Hide the FILE?

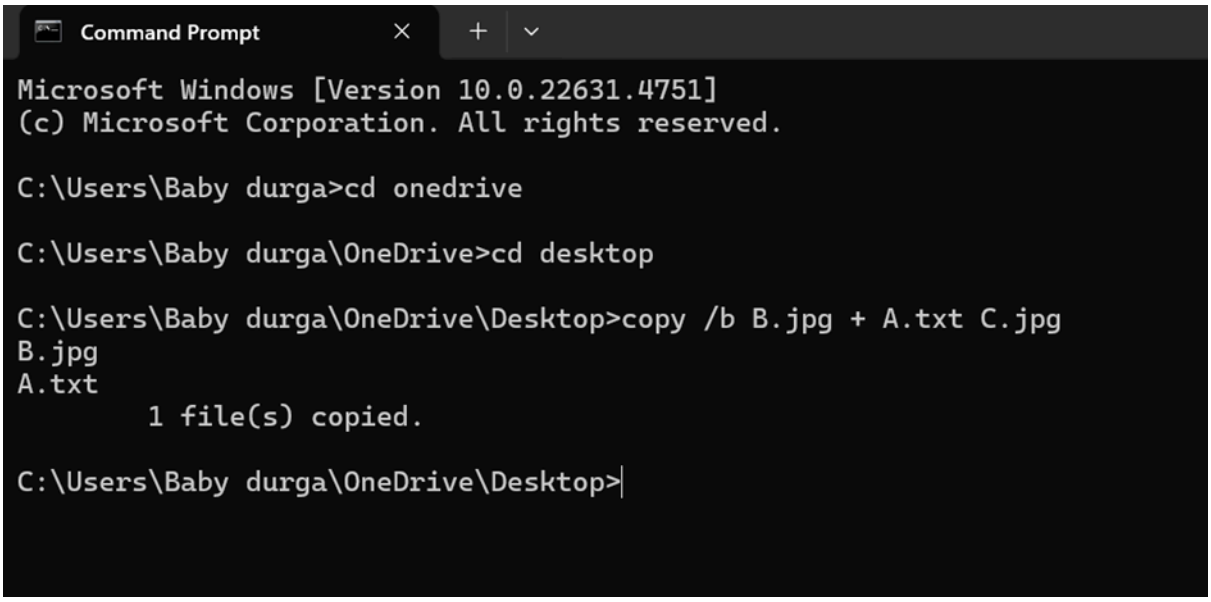
Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”. Where “C.jpg” is our output file which contains the text hidden in the image file.

Follow the steps:

1. copy the file need to hide, to desktop (for our tutorial let us assume the file to be "A.txt")
2. copy the image, within which you need to hide the file, to desktop (let it be "B.jpg")
3. now open the cmd: >ctrl+r >type: cmd and hit enter
4. in cmd first type the code as follows: >cd desktop NOTE: this code is for assigning the location on cmd to desktop
5. Now type the following code:

```
copy /b B.jpg + A.txt C.jpg
```

Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial- image.jpg Resulting-image-name.jpg*

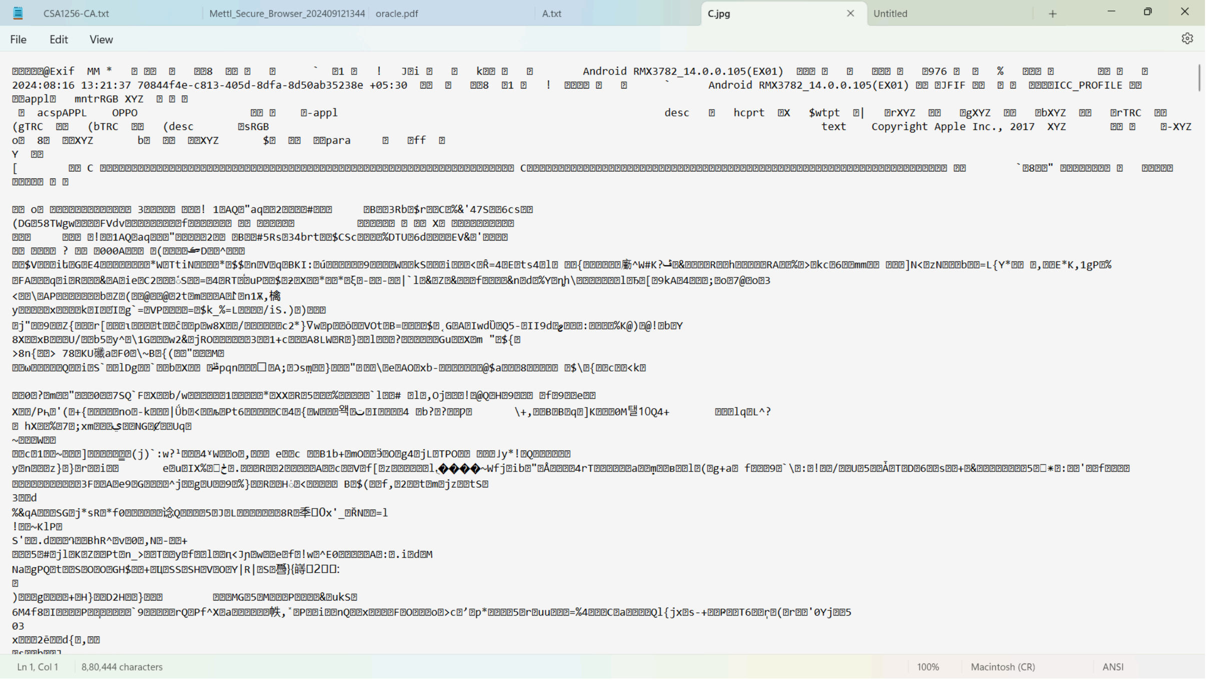


```
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Baby durga>cd onedrive

C:\Users\Baby durga\OneDrive>cd desktop

C:\Users\Baby durga\OneDrive\Desktop>copy /b B.jpg + A.txt C.jpg
B.jpg
A.txt
        1 file(s) copied.

C:\Users\Baby durga\OneDrive\Desktop>
```

"C.jpg" is the output image inside this out image our file is hidden

How to retrieve the file?

1. locate C.jpg file from where you want to retrieve text data
2. Right-click and open with notepad



```
�����@Exif  MM *   � ��  �   ��8  �� �   �      `  �1 �   !   J�i �   �   k�� �   �       Android RMX3782_14.0.0.105(EX01)  ��� �   �   ��� �   �976 �  �   %   ��� �       �� �   �
2024:08:16 13:21:37 70844f4e-c813-405d-8dfa-8d50ab35238e +05:30  ��  �   ��8  �1 �   !  ���� �   �      `      Android RMX3782_14.0.0.105(EX01) �� �JFIF ��  � �  ����ICC_PROFILE ��
��appl�   mntrRGB XYZ  � � �
 �  acspAPPL    OPPO                  �� �    �-appl                                                     desc   �   hcprt  �X   $wtpt  �|   �rXYZ  ��   �gXYZ  ��   �bXYZ  ��   �rTRC  ��
(gTRC  ��   (bTRC  ��   (desc       �sRGB                                                                     text    Copyright Apple Inc., 2017  XYZ       �� �    �-XYZ
o�  8�  ��XYZ       b�  ��  ��XYZ       $�  ��  ��para     �   �ff  �
Y  ��
```

Ln 1, Col 1 | 8,80,444 characters | 100% | Macintosh (CR) | ANSI

Done! Successfully opened! In the last of the notepad, you'll find the content of the text file.

Hide A Message into Image:

1. Open Run command window by pressing win + r.
2. Open command prompt by typing cmd and press OK
3. Enter the directory where you have your files.
4. Then type the command: echo "Your Message">>"image.jpg"
5. Now the message is successfully hidden in the image file.
6. To view the message: Open with Notepad, at last, you’ll find the Your Message

Result:

The experiment has been successfully executed.

EXPERIMENT-03

Hiding and extracting a text file behind an audio file.

Aim of the Experiment:

To study the steps for hiding and extract any text file behind an Audio file using Command Prompt.

Any file like .rar .jpg .txt or any file can be merged inside another file. In a simple way, we shall learn how to hide a text file inside an image file using the Command Prompt.

How to Hide the FILE?

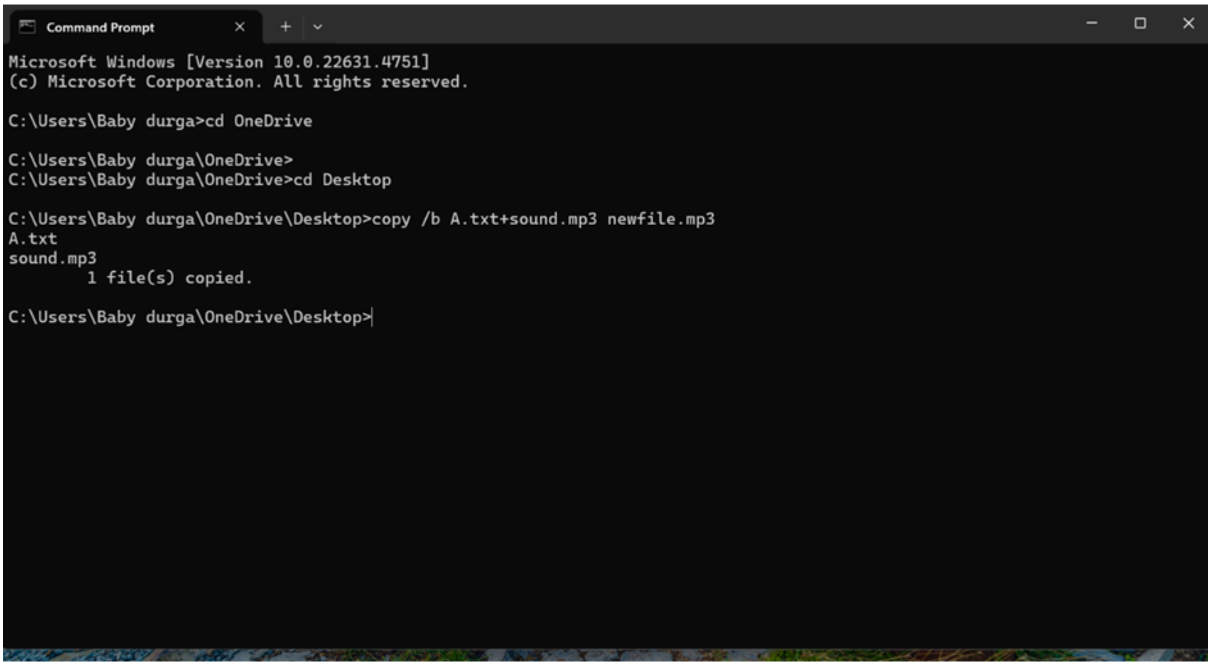
Suppose you have to hide a text file “A.txt” with the image file “sound.mp3” and combine them in a new file as “newfile.mp3”. Where “newfile.mp3” is our output file which contains the text hidden in the image file.

Follow the steps:

6. copy the file need to hide, to desktop (for our tutorial let us assume the file to be "A.txt")
7. copy the audio, within which you need to hide the file, to desktop (let it be "sound.mp3")
8. now open the cmd: >ctrl+r >type: cmd and hit enter
9. in cmd first type the code as follows: >cd desktop NOTE: this code is for assigning the location on cmd to desktop
10. Now type the following code:

```
copy /b A.txt + sound.mp3 newfile.mp3
```

Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial- audio.mp3 Resulting-audio-name.mp3*

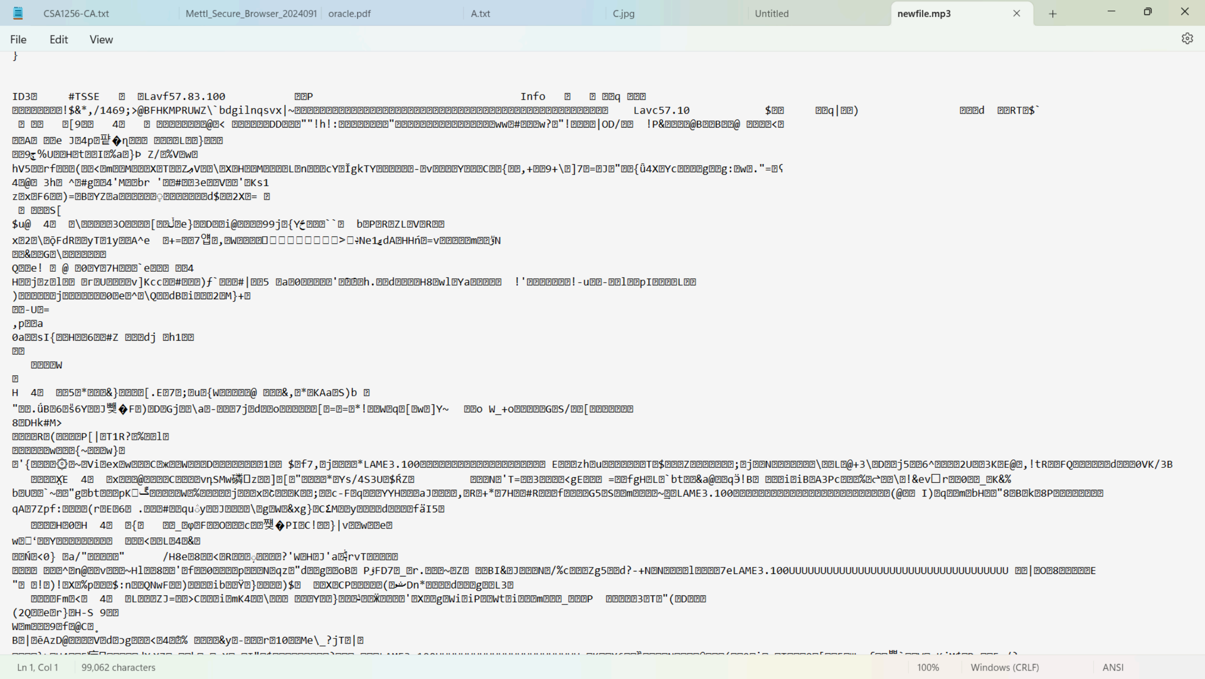


```
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Baby durga>cd OneDrive

C:\Users\Baby durga\OneDrive>
C:\Users\Baby durga\OneDrive>cd Desktop

C:\Users\Baby durga\OneDrive\Desktop>copy /b A.txt+sound.mp3 newfile.mp3
A.txt
sound.mp3
        1 file(s) copied.

C:\Users\Baby durga\OneDrive\Desktop>
```

"newfile.mp3" is the output audio inside this out audio our file is hidden

How to retrieve the file?

3. locate newfile.mp3 file from where you want to retrieve text data
4. Right-click and open with notepad



```
}


ID3▯     #TSSE   ▯  ▯Lavf57.83.100           ▯▯P                              Info   ▯   ▯ ▯▯q ▯▯▯
▯▯▯▯▯▯▯▯!$&*,/1469;>@BFHKMPRUWZ\`bdgilnqsvx|~▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯   Lavc57.10          $▯▯     ▯▯q|▯▯)              ▯▯▯d  ▯▯RT▯$`
 ▯ ▯▯   ▯[9▯▯   4▯   ▯ ▯▯▯▯▯▯▯▯@▯< ▯▯▯▯▯▯DD▯▯▯""!h!:▯▯▯▯▯▯▯▯"▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯ww▯#▯▯▯w?▯"!▯▯▯▯|OD/▯▯  !P&▯▯▯▯@B▯▯B▯▯@ ▯▯▯▯<▯
▯▯A▯ ▯▯e J▯4p▯팔�η▯▯▯ ▯▯▯▯L▯▯}▯▯▯
▯▯9ჳ%U▯▯H▯t▯▯I▯%a▯}Þ Z/▯%V▯w▯
hV5▯▯rf▯▯▯(▯▯<▯m▯▯M▯▯▯X▯T▯▯Z̷V▯▯\▯X▯H▯▯M▯▯▯▯L▯n▯▯▯cY▯ĬgkTY▯▯▯▯▯▯-▯v▯▯▯▯Y▯▯▯C▯▯{▯▯,+▯▯9+\▯]7▯=▯J▯"▯▯{ũ4X▯Yc▯▯▯▯g▯▯g:▯w▯."=▯ʕ
4▯@▯ 3h▯ ^▯#g▯▯4'M▯▯br '▯▯#▯▯3e▯▯V▯▯'▯Ks1
z▯x▯F6▯▯)=▯B▯YZ▯a▯▯▯▯▯▯▯▯▯▯▯▯▯▯d$▯▯2X▯= ▯
 ▯ ▯▯▯S[
$u@  4▯  ▯\▯▯▯▯▯3O▯▯▯▯[▯▯ܱ▯e}▯▯D▯▯i@▯▯▯▯99j▯{Yځ▯▯▯``▯  b▯P▯R▯ZL▯V▯R▯▯
x▯2▯\▯ǭFdR▯▯yT▯1y▯▯A^e  ▯+=▯▯7앱▯,▯W▯▯▯▯□□□□□□□□□>□꜠Ne1ɇdA▯HHń▯=v▯▯▯▯▯m▯▯ʒN
▯▯&▯▯G▯\▯▯▯▯▯▯▯
Q▯▯e! ▯ @ ▯0▯Y▯7H▯▯▯`e▯▯▯ ▯▯4
H▯▯j▯z▯l▯▯ ▯r▯U▯▯▯▯v]Kcc▯▯#▯▯▯)ƒ`▯▯▯#|▯▯5 ▯a▯0▯▯▯▯▯▯'▯▯▯▯h.▯▯d▯▯▯▯H8▯wl▯Ya▯▯▯▯▯  !'▯▯▯▯▯▯▯!-u▯▯-▯▯l▯▯pI▯▯▯▯L▯▯
)▯▯▯▯▯▯j▯▯▯▯▯▯▯▯0▯e▯^▯\Q▯▯dB▯i▯▯▯2▯M}+▯
▯▯-U▯=
,p▯▯a
0a▯▯sI{▯▯H▯▯6▯▯#Z ▯▯▯dj ▯h1▯▯
▯▯
   ▯▯▯▯W
▯
H  4▯  ▯▯5▯*▯▯▯&}▯▯▯▯[.E▯7▯;▯u▯{W▯▯▯▯▯@ ▯▯▯&,▯*▯KAa▯S)b ▯
"▯▯.űB▯6▯š6Y▯▯J빻�F▯)▯D▯Gj▯▯\a▯-▯▯▯7j▯d▯▯o▯▯▯▯▯▯[▯=▯=▯*!▯▯W▯q▯[▯w▯]Y~  ▯▯o W_+o▯▯▯▯▯G▯S/▯▯[▯▯▯▯▯▯▯
8▯DHk#M>
▯▯▯▯R▯(▯▯▯▯P[|▯T1R?▯%▯▯l▯
▯▯▯▯▯▯w▯▯▯{~▯▯▯w}▯
▯'{▯▯▯▯۞▯~▯Vi▯ex▯w▯▯▯C▯ж▯▯W▯▯▯D▯▯▯▯▯▯▯▯1▯▯ $▯f7,▯j▯▯▯▯*LAME3.100▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯ E▯▯▯zh▯u▯▯▯▯▯▯▯T▯$▯▯▯Z▯▯▯▯▯▯▯;▯j▯▯N▯▯▯▯▯▯▯\▯▯L▯@+3\▯D▯▯j5▯▯6^▯▯▯▯2U▯▯3K▯E@▯,!tR▯▯FQ▯▯▯▯▯▯d▯▯▯0VK/3B
   ▯▯▯▯X̧E  4▯  ▯x▯▯▯@▯▯▯▯C▯▯▯▯vηSMw磷□z▯▯]▯[▯"▯▯▯▯*▯Ys/4S3U▯$ŔZ▯        ▯▯▯N▯'T=▯▯3▯▯▯▯<gE▯▯▯ =▯▯fgH▯L▯`bt▯▯&a@▯▯qӛ!B▯ ▯▯▯i▯iB▯A3Pc▯▯▯%▯ॆ▯▯\▯!&ev□r▯▯0▯▯_▯K&%
b▯U▯▯`~▯▯"g▯bt▯▯▯pK□ࢯ▯▯▯▯▯W▯%▯▯▯▯▯j▯▯▯x▯ĉ▯▯▯K▯▯;▯▯c-F▯q▯▯▯YYH▯▯▯aJ▯▯▯▯,▯R▯+*▯7H▯▯#R▯▯▯f▯▯▯▯G5▯S▯▯m▯▯▯▯~▯▯LAME3.100▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯(@▯▯ I)▯q▯▯m▯bH▯▯"8▯B▯k▯8P▯▯▯▯▯▯▯▯
qA▯7Zpf:▯▯▯▯(r▯E▯6▯ .▯▯▯#▯▯qu꙰y▯▯J▯▯▯▯\▯g▯W▯&xg}▯CƩM▯▯y▯▯▯▯d▯▯▯▯fäI5▯
   ▯▯▯▯H▯0▯H  4▯  ▯{▯   ▯▯_▯φ▯F▯▯O▯▯▯c▯▯쨋�PI▯C!▯▯}|v▯▯w▯▯e▯
w▯□'▯▯Y▯▯▯▯▯▯▯▯▯  ▯▯▯<▯▯L▯4▯&▯
▯▯Ń▯<0} ▯a/"▯▯▯▯▯"      /H8e▯8▯▯<▯R▯▯▯꙰▯▯▯▯?'W▯H▯J'a▯ꞎrvT▯▯▯▯▯
▯▯▯▯ ▯▯▯^▯n@▯▯v▯▯▯~Hl▯▯8▯▯'▯f▯▯0▯▯▯▯p▯▯▯N▯qz▯"d▯▯g▯▯oB▯ Pɟ̄FD7▯_▯r.▯▯▯~▯Z▯ ▯▯BI&▯J▯▯▯N▯/%c▯▯▯Zg5▯▯d?-+N▯N▯▯▯▯l▯▯▯▯7eLAME3.100UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU ▯▯|▯O▯8▯▯▯▯▯E
"▯ ▯!▯)!▯X▯%p▯▯▯$:n▯▯QNwF▯▯)▯▯▯▯ib▯▯Ÿ▯}▯▯▯▯)$▯  ▯▯X▯CP▯▯▯▯▯(▯ݸDn*▯▯▯▯d▯▯▯g▯▯L3▯
   ▯▯▯▯Fm▯<▯  4▯  ▯L▯▯▯ZJ=▯▯>C▯▯▯i▯mK4▯▯\▯▯▯ ▯▯▯Y▯▯}▯▯▯ܢ▯▯Ӂ▯▯▯▯'▯X▯▯g▯Wi▯iP▯▯Wt▯i▯▯▯m▯▯▯_▯▯▯P  ▯▯▯▯▯3▯T▯"(▯D▯▯▯
(2Q▯▯e▯r}▯H-S 9▯▯
W▯m▯▯▯9▯f▯@C▯¸
B▯|▯ēAzD@▯▯▯▯V▯d▯ↄg▯▯▯<▯4▯▯% ▯▯▯▯&y▯-▯▯▯r▯10▯▯Me\_?jT▯|▯
```

Done! Successfully opened! In the last of the notepad, you'll find the content of the text file.

Hide A Message into Audio:

7. Open the Run command window by pressing win + r.
8. Open command prompt by typing cmd and press OK
9. Enter the directory where you have your files.
10. Then type the command: echo "Your Message">>"audio.mp3"
11. Now the message is successfully hidden in the audio file.
12. To view the message: Open with Notepad, at last, you'll find the Your Message

Result:

The experiment has been successfully executed.

EXPERIMENT-04

Extract Exchangeable image file format (EXIF) Data

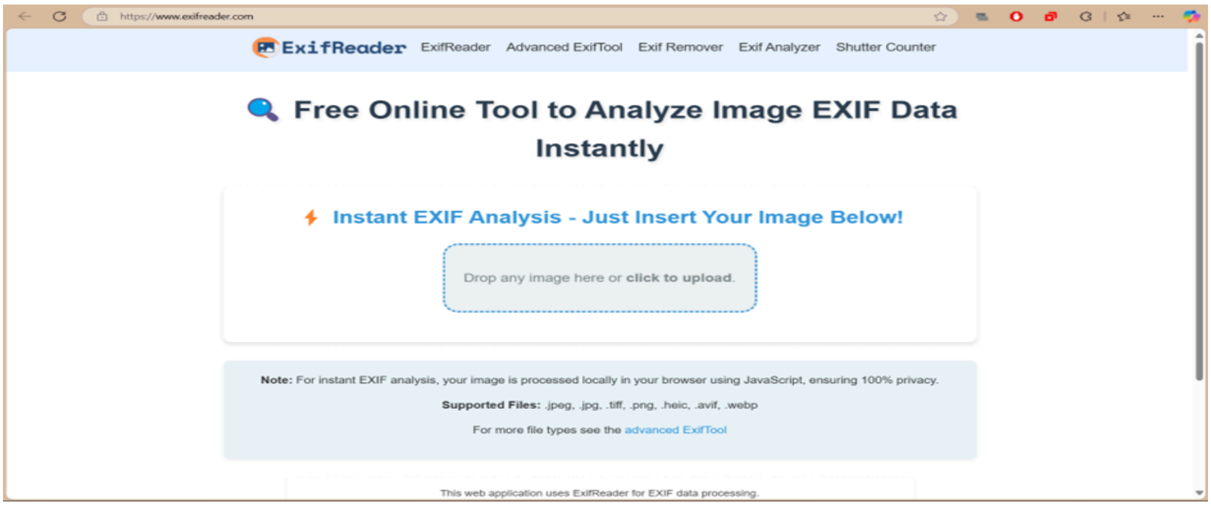
Aim of the Experiment:

How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exif reader Software.

Procedure:

Step 1: Visit The given URL belowURL: exifreader.com

Step 2: Find an Appropriate image



Free Online Tool to Analyze Image EXIF Data Instantly

Instant EXIF Analysis - Just Insert Your Image Below!

Note: For instant EXIF analysis, your image is processed locally in your browser using JavaScript, ensuring 100% privacy.

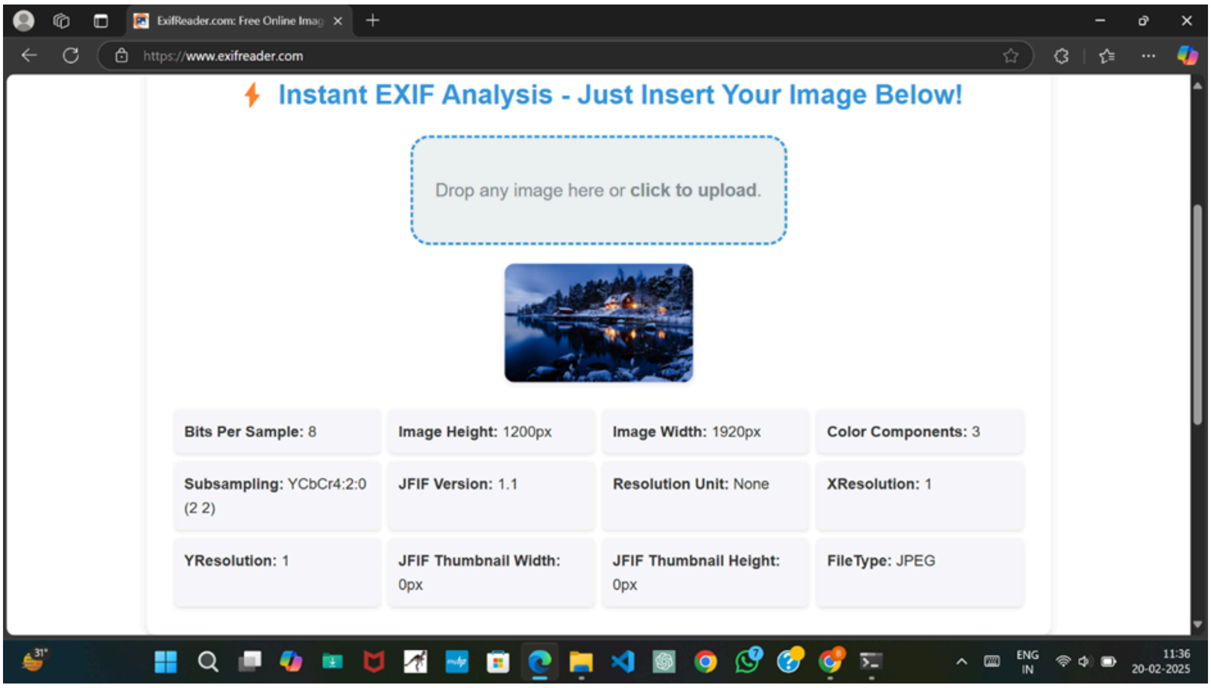
Supported Files: .jpeg, .jpg, .tiff, .png, .heic, .avif, .webp

For more file types see the advanced ExifTool

This web application uses ExifReader for EXIF data processing.

Step 3: Select the image file and upload the image file

Step 4: Analyse the exif features of the image


ExifReader.com: Free Online Imag
https://www.exifreader.com
Instant EXIF Analysis - Just Insert Your Image Below!
Drop any image here or click to upload.

Bits Per Sample: 8	**Image Height:** 1200px	**Image Width:** 1920px	**Color Components:** 3
Subsampling: YCbCr4:2:0 (2 2)	**JFIF Version:** 1.1	**Resolution Unit:** None	**XResolution:** 1
YResolution: 1	**JFIF Thumbnail Width:** 0px	**JFIF Thumbnail Height:** 0px	**FileType:** JPEG

31°
ENG
IN
11:36
20-02-2025

Step 5: After the completion of the analysing the image, you can find the result as the above image.

Result:

The experiment has been successfully executed.

EXPERIMENT-05

Extract Chrome History using forensic tools

Aim of the Experiment:

To Extract Chrome history using forensic tools and analyse them.

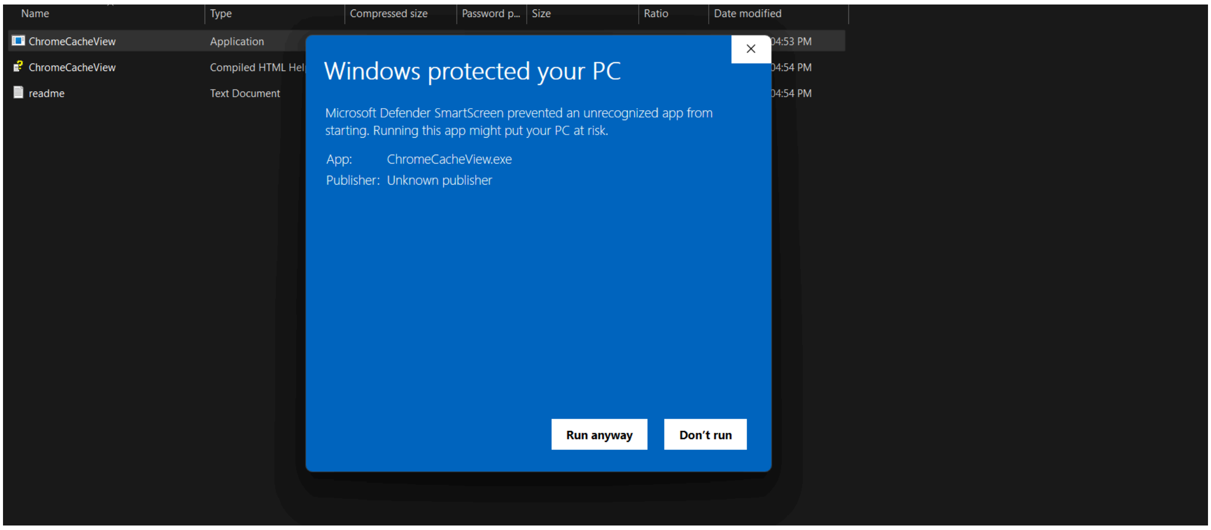
Procedure:

Step 1: Download Browsing History View tool
URL:

https://sourceforge.net/projects/browsinghistoryview/

Step 2: Setup from the exe file downloaded

Step 3: Click run anyway when the below dialog box appears



Windows protected your PC

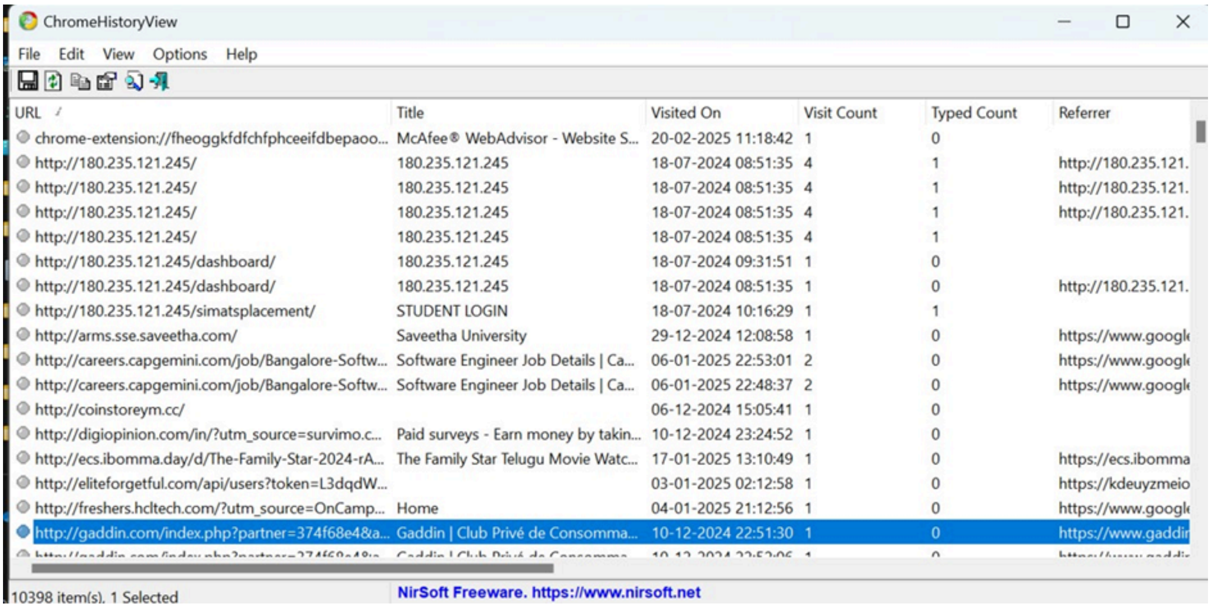
Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: ChromeCacheView.exe
Publisher: Unknown publisher

Step 4: Start the Browsing History View Tool

Step 5: Wait for the scanning process to complete

Step 6: After the completion of the scanning process, the chrome history view can be found and analysed.



URL	Title	Visited On	Visit Count	Typed Count	Referrer
chrome-extension://fheoggkfdfchfphceeifdbepaoo...	McAfee® WebAdvisor - Website S...	20-02-2025 11:18:42	1	0	
http://180.235.121.245/	180.235.121.245	18-07-2024 08:51:35	4	1	http://180.235.121.
http://180.235.121.245/	180.235.121.245	18-07-2024 08:51:35	4	1	http://180.235.121.
http://180.235.121.245/	180.235.121.245	18-07-2024 08:51:35	4	1	http://180.235.121.
http://180.235.121.245/	180.235.121.245	18-07-2024 08:51:35	4	1	
http://180.235.121.245/dashboard/	180.235.121.245	18-07-2024 09:31:51	1	0	
http://180.235.121.245/dashboard/	180.235.121.245	18-07-2024 08:51:35	1	0	http://180.235.121.
http://180.235.121.245/simatsplacement/	STUDENT LOGIN	18-07-2024 10:16:29	1	1	
http://arms.sse.saveetha.com/	Saveetha University	29-12-2024 12:08:58	1	0	https://www.googl
http://careers.capgemini.com/job/Bangalore-Softw...	Software Engineer Job Details | Ca...	06-01-2025 22:53:01	2	0	https://www.googl
http://careers.capgemini.com/job/Bangalore-Softw...	Software Engineer Job Details | Ca...	06-01-2025 22:48:37	2	0	https://www.googl
http://coinstoreym.cc/		06-12-2024 15:05:41	1	0	
http://digiopinion.com/in/?utm_source=survimo.c...	Paid surveys - Earn money by takin...	10-12-2024 23:24:52	1	0	
http://ecs.ibomma.day/d/The-Family-Star-2024-rA...	The Family Star Telugu Movie Watc...	17-01-2025 13:10:49	1	0	https://ecs.ibomma
http://eliteforgetful.com/api/users?token=L3dqdW...		03-01-2025 02:12:58	1	0	https://kdeuyzmeio
http://freshers.hcltech.com/?utm_source=OnCamp...	Home	04-01-2025 21:12:56	1	0	https://www.googl
http://gaddin.com/index.php?partner=374f68e4&a...	Gaddin | Club Privé de Consomma...	10-12-2024 22:51:30	1	0	https://www.gaddir
http://gaddin.com/index.php?partner=374f68e4&a...	Gaddin | Club Privé de Consomma...	10-12-2024 22:52:06	1	0	https://www.gaddir

10398 item(s), 1 Selected

NirSoft Freeware. https://www.nirsoft.net

Result:

The experiment has been successfully executed

EXPERIMENT-06

Extract Chrome cache using forensic tools

Aim of the Experiment:

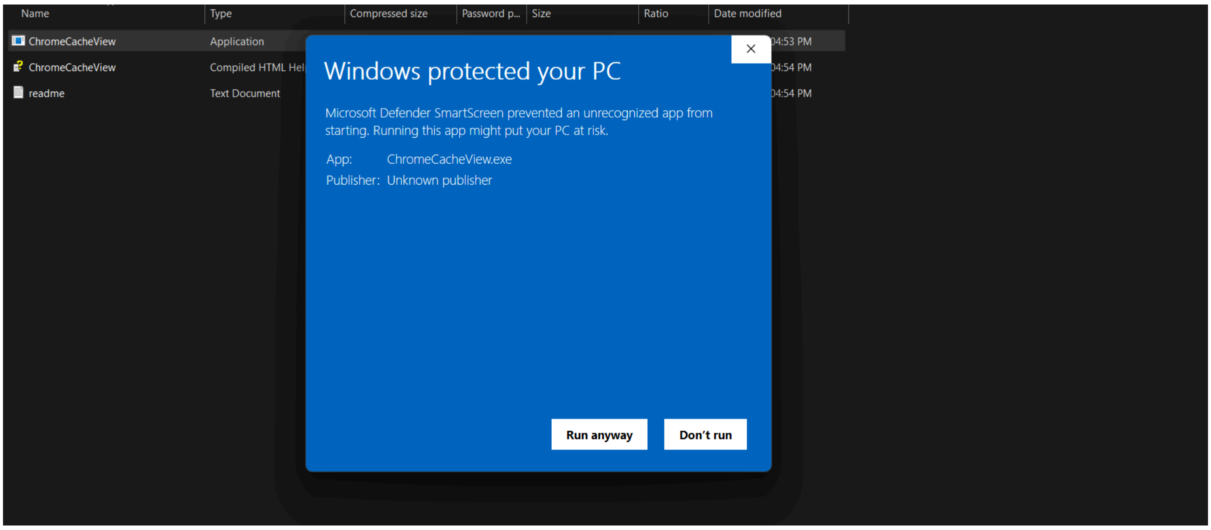
To Extract Chrome cache using forensic tools and analyse them.

Procedure:

Step 1: Download Chrome cache View tool
URL: https://sourceforge.net/projects/chromecacheview/

Step 2: Setup from the exe file downloaded

Step 3: Click run anyway when the below dialog box appears



Windows protected your PC

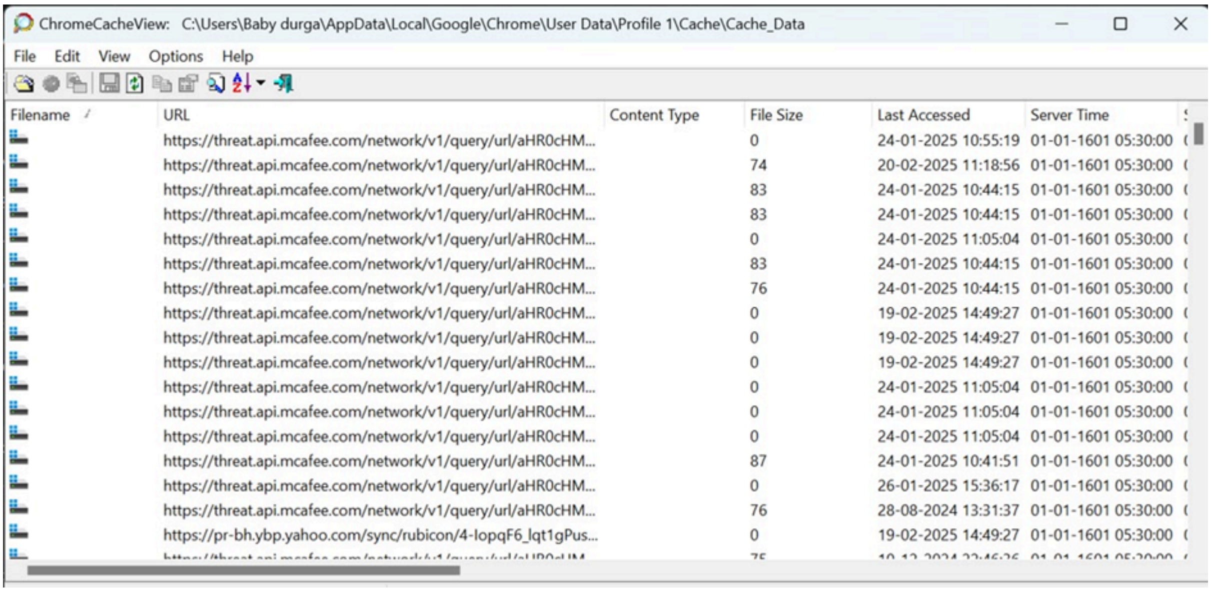
Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: ChromeCacheView.exe
Publisher: Unknown publisher

Step 4: Start the Chrome Cache View Tool

Step 5: Wait for the scanning process to complete

Step 6: After the completion of the scanning process, the chrome cache view can be found and analysed.


ChromeCacheView: C:\Users\Baby durga\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data
File
Edit
View
Options
Help

Filename	URL	Content Type	File Size	Last Accessed	Server Time
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	24-01-2025 10:55:19	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		74	20-02-2025 11:18:56	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		83	24-01-2025 10:44:15	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		83	24-01-2025 10:44:15	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	24-01-2025 11:05:04	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		83	24-01-2025 10:44:15	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		76	24-01-2025 10:44:15	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	19-02-2025 14:49:27	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	19-02-2025 14:49:27	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	19-02-2025 14:49:27	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	24-01-2025 11:05:04	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	24-01-2025 11:05:04	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	24-01-2025 11:05:04	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		87	24-01-2025 10:41:51	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		0	26-01-2025 15:36:17	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		76	28-08-2024 13:31:37	01-01-1601 05:30:00
	https://pr-bh.ybp.yahoo.com/sync/rubicon/4-IopqF6_lqt1gPus...		0	19-02-2025 14:49:27	01-01-1601 05:30:00
	https://threat.api.mcafee.com/network/v1/query/url/aHR0cHM...		75	10-12-2024 22:46:26	01-01-1601 05:30:00

Result:

The experiment has been successfully executed

EXPERIMENT-07

Extract last activity using forensic tools

Aim of the Experiment:

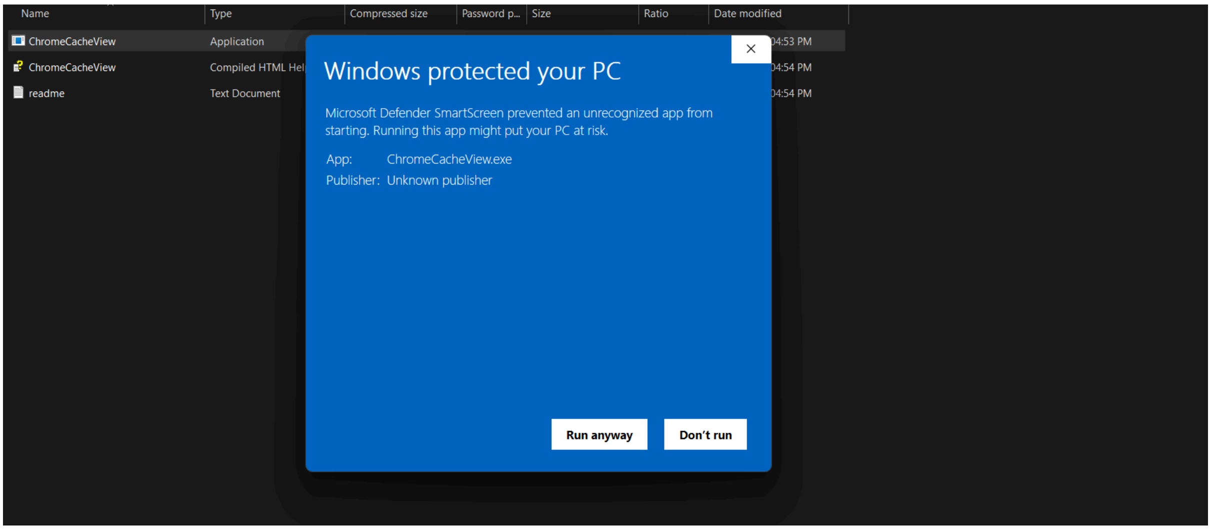
To Extract the last activity view using forensic tools and analyse them.

Procedure:

Step 1: Download last activity view View tool
URL: https://www.softportal.com/en/lastactivityview/windows/software

Step 2: Setup from the exe file downloaded

Step 3: Click run anyway when the below dialog box appears



Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
ChromeCacheView	Application					04:53 PM
ChromeCacheView	Compiled HTML Hel					04:54 PM
readme	Text Document					04:54 PM

Windows protected your PC

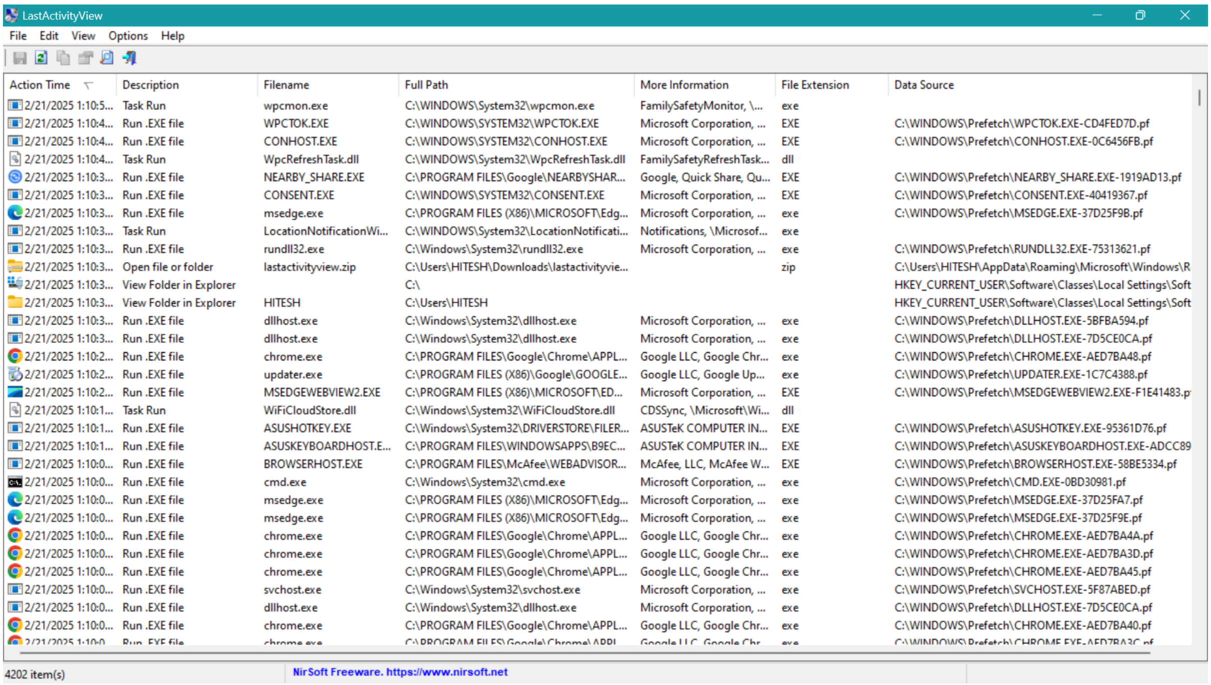
Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: ChromeCacheView.exe
Publisher: Unknown publisher

Step 4: Start the last activity view View Tool

Step 5: Wait for the scanning process to complete

Step 6: After the completion of the scanning process, the last activity view can be found and analysed.



Action Time	Description	Filename	Full Path	More Information	File Extension	Data Source
2/21/2025 1:10:5...	Task Run	wpcmon.exe	C:\WINDOWS\System32\wpcmon.exe	FamilySafetyMonitor, \...	exe	
2/21/2025 1:10:4...	Run .EXE file	WPCTOK.EXE	C:\WINDOWS\SYSTEM32\WPCTOK.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\WPCTOK.EXE-CD4FED7D.pf
2/21/2025 1:10:4...	Run .EXE file	CONHOST.EXE	C:\WINDOWS\SYSTEM32\CONHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\CONHOST.EXE-0C6456FB.pf
2/21/2025 1:10:4...	Task Run	WpcRefreshTask.dll	C:\WINDOWS\System32\WpcRefreshTask.dll	FamilySafetyRefreshTask...	dll	
2/21/2025 1:10:3...	Run .EXE file	NEARBY_SHARE.EXE	C:\PROGRAM FILES\Google\NEARBYSHAR...	Google, Quick Share, Qu...	EXE	C:\WINDOWS\Prefetch\NEARBY_SHARE.EXE-1919AD13.pf
2/21/2025 1:10:3...	Run .EXE file	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\CONSENT.EXE-40419367.pf
2/21/2025 1:10:3...	Run .EXE file	msedge.exe	C:\PROGRAM FILES (X86)\MICROSOFT\Edg...	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\MSEDGE.EXE-37D25F9B.pf
2/21/2025 1:10:3...	Task Run	LocationNotificationWi...	C:\WINDOWS\System32\LocationNotificati...	Notifications, \Microsof...	exe	
2/21/2025 1:10:3...	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\RUNDLL32.EXE-75313621.pf
2/21/2025 1:10:3...	Open file or folder	lastactivityview.zip	C:\Users\HITESH\Downloads\lastactivityvie...		zip	C:\Users\HITESH\AppData\Roaming\Microsoft\Windows\R
2/21/2025 1:10:3...	View Folder in Explorer		C:\			HKEY_CURRENT_USER\Software\Classes\Local Settings\Soft
2/21/2025 1:10:3...	View Folder in Explorer	HITESH	C:\Users\HITESH			HKEY_CURRENT_USER\Software\Classes\Local Settings\Soft
2/21/2025 1:10:3...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-5BFBA594.pf
2/21/2025 1:10:3...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CE0CA.pf
2/21/2025 1:10:2...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA48.pf
2/21/2025 1:10:2...	Run .EXE file	updater.exe	C:\PROGRAM FILES (X86)\Google\GOOGLE...	Google LLC, Google Up...	exe	C:\WINDOWS\Prefetch\UPDATER.EXE-1C7C4388.pf
2/21/2025 1:10:2...	Run .EXE file	MSEDGEWEBVIEW2.EXE	C:\PROGRAM FILES (X86)\MICROSOFT\ED...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\MSEDGEWEBVIEW2.EXE-F1E41483.p
2/21/2025 1:10:1...	Task Run	WiFiCloudStore.dll	C:\Windows\System32\WiFiCloudStore.dll	CDSSync, \Microsoft\Wi...	dll	
2/21/2025 1:10:1...	Run .EXE file	ASUSHOTKEY.EXE	C:\Windows\System32\DRIVERSTORE\FILER...	ASUSTeK COMPUTER IN...	EXE	C:\WINDOWS\Prefetch\ASUSHOTKEY.EXE-95361D76.pf
2/21/2025 1:10:1...	Run .EXE file	ASUSKEYBOARDHOST.E...	C:\PROGRAM FILES\WINDOWSAPPS\B9EC...	ASUSTeK COMPUTER IN...	EXE	C:\WINDOWS\Prefetch\ASUSKEYBOARDHOST.EXE-ADCC89
2/21/2025 1:10:0...	Run .EXE file	BROWSERHOST.EXE	C:\PROGRAM FILES\McAfee\WEBADVISOR...	McAfee, LLC, McAfee W...	EXE	C:\WINDOWS\Prefetch\BROWSERHOST.EXE-58BE5334.pf
2/21/2025 1:10:0...	Run .EXE file	cmd.exe	C:\Windows\System32\cmd.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\CMD.EXE-0BD30981.pf
2/21/2025 1:10:0...	Run .EXE file	msedge.exe	C:\PROGRAM FILES (X86)\MICROSOFT\Edg...	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\MSEDGE.EXE-37D25FA7.pf
2/21/2025 1:10:0...	Run .EXE file	msedge.exe	C:\PROGRAM FILES (X86)\MICROSOFT\Edg...	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\MSEDGE.EXE-37D25F9E.pf
2/21/2025 1:10:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
2/21/2025 1:10:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
2/21/2025 1:10:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
2/21/2025 1:10:0...	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-5F87ABED.pf
2/21/2025 1:10:0...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CE0CA.pf
2/21/2025 1:10:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA40.pf
2/21/2025 1:10:0	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL	Google LLC, Google Chr	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3C.pf

4202 item(s)

NirSoft Freeware. https://www.nirsoft.net

Result:

The experiment has been successfully executed

EXPERIMENT-08

Extract USB devices using forensic tools

Aim of the Experiment:

To Extract the connected external devices using forensic tools and analyse them.

Procedure:

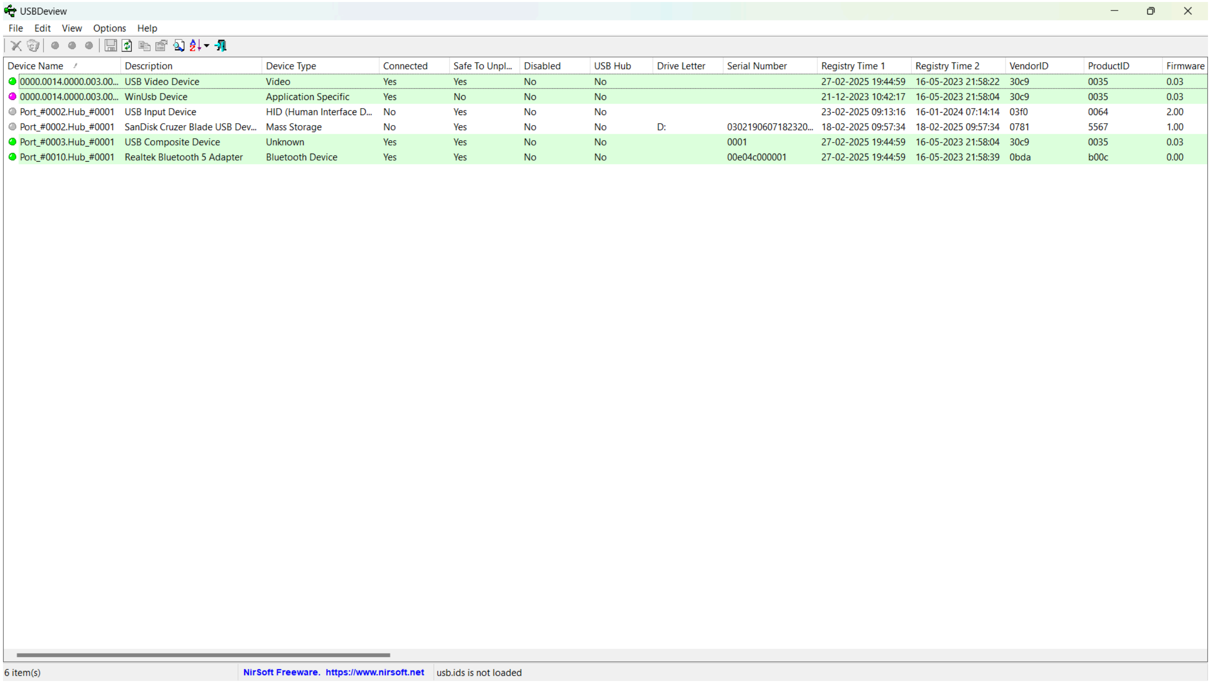
Step 1: Download previous USB devices view tool
URL: USBDeview download | SourceForge.net

Step 2: Setup from the exe file downloaded

Step 4: Start the USB devices view Tool

Step 5: Wait for the scanning process to complete

Step 6: After the completion of the scanning process, the USB devices view can be found and analysed.



Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1	Registry Time 2	VendorID	ProductID	Firmware
● 0000.0014.0000.003.00...	USB Video Device	Video	Yes	Yes	No	No			27-02-2025 19:44:59	16-05-2023 21:58:22	30c9	0035	0.03
● 0000.0014.0000.003.00...	WinUsb Device	Application Specific	Yes	No	No	No			21-12-2023 10:42:17	16-05-2023 21:58:04	30c9	0035	0.03
● Port_#0002.Hub_#0001	USB Input Device	HID (Human Interface D...	No	Yes	No	No			23-02-2025 09:13:16	16-01-2024 07:14:14	03f0	0064	2.00
● Port_#0002.Hub_#0001	SanDisk Cruzer Blade USB Dev...	Mass Storage	No	Yes	No	No	D:	0302190607182320...	18-02-2025 09:57:34	18-02-2025 09:57:34	0781	5567	1.00
● Port_#0003.Hub_#0001	USB Composite Device	Unknown	Yes	Yes	No	No		0001	27-02-2025 19:44:59	16-05-2023 21:58:04	30c9	0035	0.03
● Port_#0010.Hub_#0001	Realtek Bluetooth 5 Adapter	Bluetooth Device	Yes	Yes	No	No		00e04c000001	27-02-2025 19:44:59	16-05-2023 21:58:39	0bda	b00c	0.00

6 item(s) NirSoft Freeware. https://www.nirsoft.net usb.ids is not loaded

Result:

The experiment has been successfully executed

EXPERIMENT 9

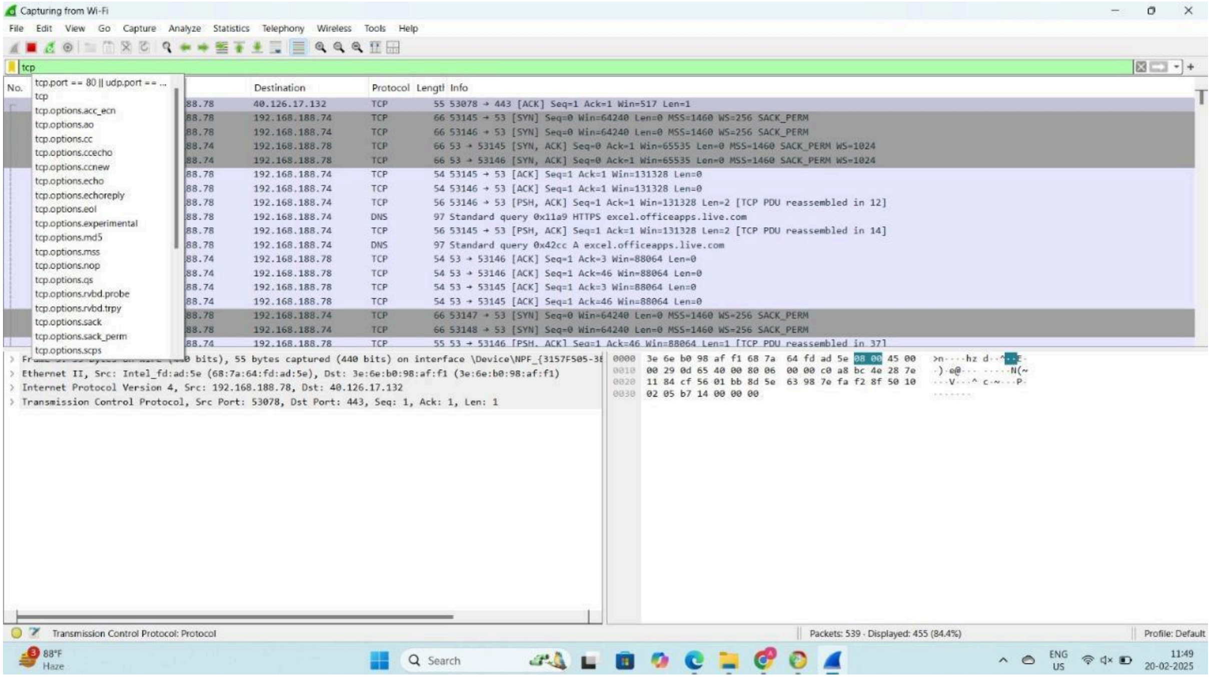
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-TCP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- TCP.

SOFTWARE USED: Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the wifi interface.
4. Click on the start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 →IP address source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on the apply button.
10. All the packets will be filtered using the source address.



tcp

```
No.          Destination      Protocol Lengtl Info
   88.78     40.126.17.132    TCP      55 53078 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1
   88.78     192.168.188.74   TCP      66 53145 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   88.78     192.168.188.74   TCP      66 53146 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   88.74     192.168.188.78   TCP      66 53 → 53145 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=1024
   88.74     192.168.188.78   TCP      66 53 → 53146 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=1024
   88.78     192.168.188.74   TCP      54 53145 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   88.78     192.168.188.74   TCP      54 53146 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   88.78     192.168.188.74   TCP      56 53146 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP PDU reassembled in 12]
   88.78     192.168.188.74   DNS      97 Standard query 0x11a9 HTTPS excel.officeapps.live.com
   88.78     192.168.188.74   TCP      56 53145 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP PDU reassembled in 14]
   88.78     192.168.188.74   DNS      97 Standard query 0x42cc A excel.officeapps.live.com
   88.74     192.168.188.78   TCP      54 53 → 53146 [ACK] Seq=1 Ack=3 Win=88064 Len=0
   88.74     192.168.188.78   TCP      54 53 → 53146 [ACK] Seq=1 Ack=46 Win=88064 Len=0
   88.74     192.168.188.78   TCP      54 53 → 53145 [ACK] Seq=1 Ack=3 Win=88064 Len=0
   88.74     192.168.188.78   TCP      54 53 → 53145 [ACK] Seq=1 Ack=46 Win=88064 Len=0
   88.78     192.168.188.74   TCP      66 53147 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   88.78     192.168.188.74   TCP      66 53148 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   88.74     192.168.188.78   TCP      55 53 → 53146 [PSH, ACK] Seq=1 Ack=46 Win=88064 Len=1 [TCP PDU reassembled in 37]
```

```
> Fr... bits), 55 bytes captured (440 bits) on interface \Device\NPF_{3157F505-3E
> Ethernet II, Src: Intel_fd:ad:5e (68:7a:64:fd:ad:5e), Dst: 3e:6e:b0:98:af:f1 (3e:6e:b0:98:af:f1)
> Internet Protocol Version 4, Src: 192.168.188.78, Dst: 40.126.17.132
> Transmission Control Protocol, Src Port: 53078, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  3e 6e b0 98 af f1 68 7a  64 fd ad 5e 08 00 45 00   >n····hz d··^··E·
0010  00 29 0d 65 40 00 80 06  00 00 c0 a8 bc 4e 28 7e   ·)·e@··· ·····N(~
0020  11 84 cf 56 01 bb 8d 5e  63 98 7e fa f2 8f 50 10   ···V···^ c·~···P·
0030  02 05 b7 14 00 00 00                               ·······
```

Transmission Control Protocol: Protocol

Packets: 539 · Displayed: 455 (84.4%)

Profile: Default

Result:

Hence, the capturing of packets using wire shark network analyzer was analyzed for TCP.

EXPERIMENT 10

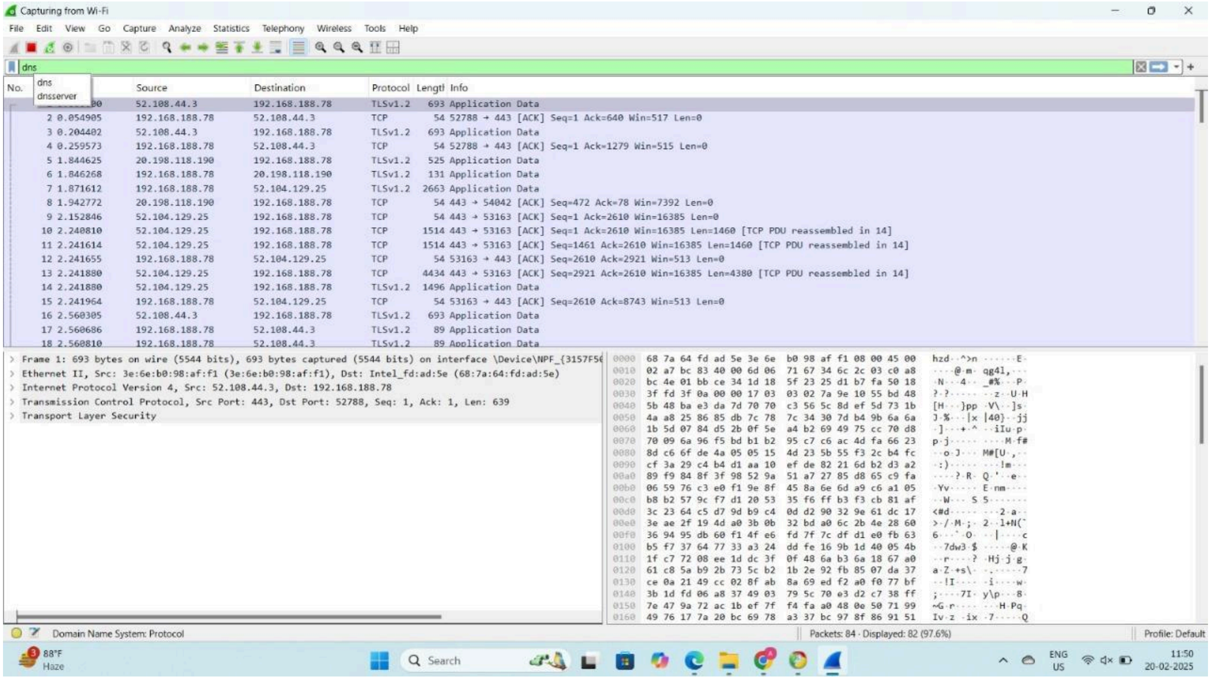
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-DNS

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- DNS.

SOFTWARE USED: Wire shark network analyzer

Procedure:

11. Open wire shark.
12. Click on list the available capture interface.
13. Choose the wifi interface.
14. Click on the start button.
15. Active packets will be displayed.
16. Capture the packets & select any IP address from the source.
17. Click on the expression and select IPV4 →IP address source address in the field name.
18. Select the double equals (==) from the selection and enter the selected IP source address.
19. Click on the apply button.
20. All the packets will be filtered using the source address.



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver

```
No.  Time      Source           Destination      Protocol Length Info
         80    52.108.44.3      192.168.188.78   TLSv1.2   693 Application Data
   2 0.054905  192.168.188.78   52.108.44.3      TCP        54 52788 → 443 [ACK] Seq=1 Ack=640 Win=517 Len=0
   3 0.204402  52.108.44.3      192.168.188.78   TLSv1.2   693 Application Data
   4 0.259573  192.168.188.78   52.108.44.3      TCP        54 52788 → 443 [ACK] Seq=1 Ack=1279 Win=515 Len=0
   5 1.844625  20.198.118.190   192.168.188.78   TLSv1.2   525 Application Data
   6 1.846268  192.168.188.78   20.198.118.190   TLSv1.2   131 Application Data
   7 1.871612  192.168.188.78   52.104.129.25    TLSv1.2  2663 Application Data
   8 1.942772  20.198.118.190   192.168.188.78   TCP        54 443 → 54042 [ACK] Seq=472 Ack=78 Win=7392 Len=0
   9 2.152846  52.104.129.25    192.168.188.78   TCP        54 443 → 53163 [ACK] Seq=1 Ack=2610 Win=16385 Len=0
  10 2.240810  52.104.129.25    192.168.188.78   TCP      1514 443 → 53163 [ACK] Seq=1 Ack=2610 Win=16385 Len=1460 [TCP PDU reassembled in 14]
  11 2.241614  52.104.129.25    192.168.188.78   TCP      1514 443 → 53163 [ACK] Seq=1461 Ack=2610 Win=16385 Len=1460 [TCP PDU reassembled in 14]
  12 2.241655  192.168.188.78   52.104.129.25    TCP        54 53163 → 443 [ACK] Seq=2610 Ack=2921 Win=513 Len=0
  13 2.241880  52.104.129.25    192.168.188.78   TCP      4434 443 → 53163 [ACK] Seq=2921 Ack=2610 Win=16385 Len=4380 [TCP PDU reassembled in 14]
  14 2.241880  52.104.129.25    192.168.188.78   TLSv1.2  1496 Application Data
  15 2.241964  192.168.188.78   52.104.129.25    TCP        54 53163 → 443 [ACK] Seq=2610 Ack=8743 Win=513 Len=0
  16 2.560305  52.108.44.3      192.168.188.78   TLSv1.2   693 Application Data
  17 2.560686  192.168.188.78   52.108.44.3      TLSv1.2    89 Application Data
  18 2.560810  192.168.188.78   52.108.44.3      TLSv1.2    89 Application Data
```

```
> Frame 1: 693 bytes on wire (5544 bits), 693 bytes captured (5544 bits) on interface \Device\NPF_{3157F5(
> Ethernet II, Src: 3e:6e:b0:98:af:f1 (3e:6e:b0:98:af:f1), Dst: Intel_fd:ad:5e (68:7a:64:fd:ad:5e)
> Internet Protocol Version 4, Src: 52.108.44.3, Dst: 192.168.188.78
> Transmission Control Protocol, Src Port: 443, Dst Port: 52788, Seq: 1, Ack: 1, Len: 639
> Transport Layer Security
```

```
0000  68 7a 64 fd ad 5e 3e 6e  b0 98 af f1 08 00 45 00   hzd··^>n ······E·
0010  02 a7 bc 83 40 00 6d 06  71 67 34 6c 2c 03 c0 a8   ····@·m· qg4l,···
0020  bc 4e 01 bb ce 34 1d 18  5f 23 25 d1 b7 fa 50 18   ·N···4·· _#%···P·
0030  3f fd 3f 0a 00 00 17 03  03 02 7a 9e 10 55 bd 48   ?·?····· ··z··U·H
0040  5b 48 ba e3 da 7d 70 70  c3 56 5c 8d ef 5d 73 1b   [H···}pp ·V\··]s·
0050  4a a8 25 86 85 db 7c 78  7c 34 30 7d b4 9b 6a 6a   J·%···|x |40}··jj
0060  1b 5d 07 84 d5 2b 0f 5e  a4 b2 69 49 75 cc 70 d8   ·]···+·^ ··iIu·p·
0070  70 09 6a 96 f5 bd b1 b2  95 c7 c6 ac 4d fa 66 23   p·j····· ····M·f#
0080  8d c6 6f de 4a 05 05 15  4d 23 5b 55 f3 2c b4 fc   ··o·J··· M#[U·,··
0090  cf 3a 29 c4 b4 d1 aa 10  ef de 82 21 6d b2 d3 a2   ·:)····· ···!m···
00a0  89 f9 84 8f 3f 98 52 9a  51 a7 27 85 d8 65 c9 fa   ····?·R· Q·'··e··
00b0  06 59 76 c3 e0 f1 9e 8f  45 8a 6e 6d a9 c6 a1 05   ·Yv····· E·nm····
00c0  b8 b2 57 9c f7 d1 20 53  35 f6 ff b3 f3 cb 81 af   ··W··· S 5·······
00d0  3c 23 64 c5 d7 9d b9 c4  0d d2 90 32 9e 61 dc 17   <#d····· ···2·a··
00e0  3e ae 2f 19 4d a0 3b 0b  32 bd a0 6c 2b 4e 28 60   >·/·M·;· 2··l+N(`
00f0  36 94 95 db 60 f1 4f e6  fd 7f 7c df d1 e0 fb 63   6···`·O· ··|····c
0100  b5 f7 37 64 77 33 a3 24  dd fe 16 9b 1d 40 05 4b   ··7dw3·$ ·····@·K
0110  1f c7 72 08 ee 1d dc 3f  0f 48 6a b3 6a 18 67 a0   ··r····? ·Hj·j·g·
0120  61 c8 5a b9 2b 73 5c b2  1b 2e 92 fb 85 07 da 37   a·Z·+s\· ·.·····7
0130  ce 0a 21 49 cc 02 8f ab  8a 69 ed f2 a0 f0 77 bf   ··!I···· ·i····w·
0140  3b 1d fd 06 a8 37 49 03  79 5c 70 e3 d2 c7 38 ff   ;····7I· y\p···8·
0150  7e 47 9a 72 ac 1b ef 7f  f4 fa a0 48 0e 50 71 99   ~G·r···· ···H·Pq·
0160  49 76 17 7a 20 bc 69 78  a3 37 bc 97 8f 86 91 51   Iv·z ·ix ·7·····Q
```

Domain Name System: Protocol | Packets: 84 · Displayed: 82 (97.6%) | Profile: Default

Result:

Hence, the capturing of packets using wire shark network analyzer was analyzed for DNS.

EXPERIMENT 11

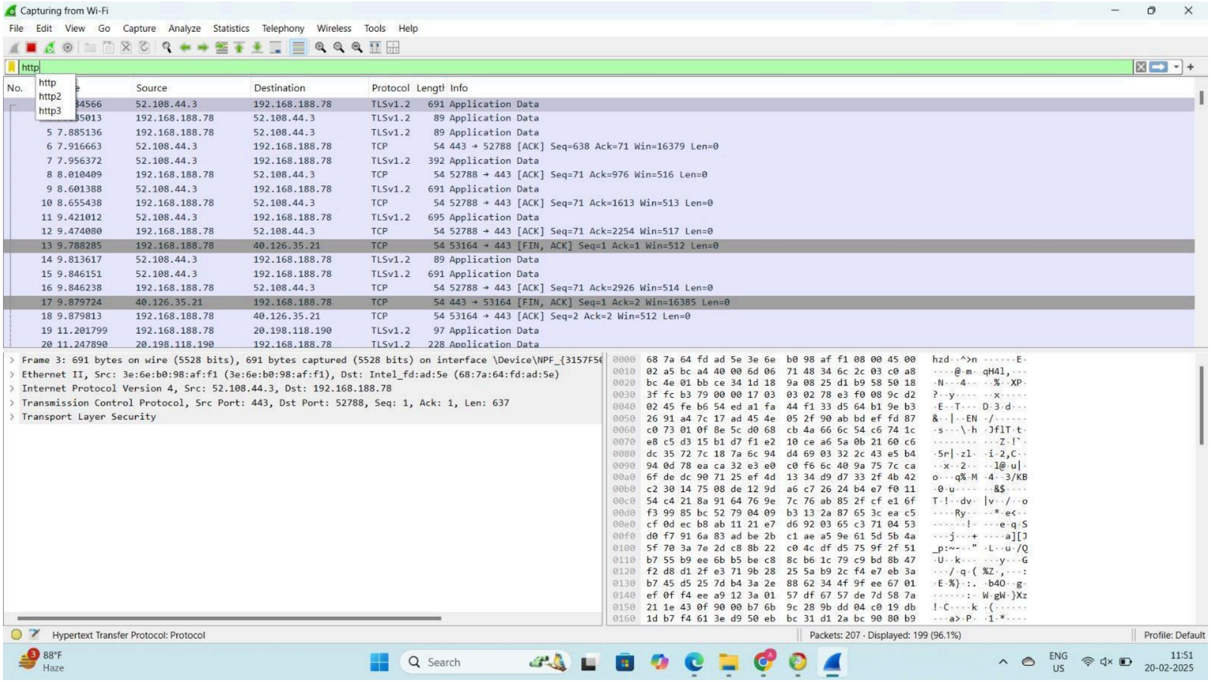
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-HTTP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- HTTP.

SOFTWARE USED: Wire shark network analyzer

Procedure:

21. Open wire shark.
22. Click on list the available capture interface.
23. Choose the wifi interface.
24. Click on the start button.
25. Active packets will be displayed.
26. Capture the packets & select any IP address from the source.
27. Click on the expression and select IPV4 →IP address source address in the field name.
28. Select the double equals (==) from the selection and enter the selected IP source address.
29. Click on the apply button.
30. All the packets will be filtered using the source address.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3
Hypertext Transfer Protocol: Protocol
Profile: Default
88°F
Haze
Search
ENG
US
11:51
20-02-2025

```
No.    Time       Source           Destination      Protocol Length Info
    …34566     52.108.44.3      192.168.188.78   TLSv1.2   691 Application Data
    …35013     192.168.188.78   52.108.44.3      TLSv1.2    89 Application Data
  5 7.885136   192.168.188.78   52.108.44.3      TLSv1.2    89 Application Data
  6 7.916663   52.108.44.3      192.168.188.78   TCP        54 443 → 52788 [ACK] Seq=638 Ack=71 Win=16379 Len=0
  7 7.956372   52.108.44.3      192.168.188.78   TLSv1.2   392 Application Data
  8 8.010409   192.168.188.78   52.108.44.3      TCP        54 52788 → 443 [ACK] Seq=71 Ack=976 Win=516 Len=0
  9 8.601388   52.108.44.3      192.168.188.78   TLSv1.2   691 Application Data
 10 8.655438   192.168.188.78   52.108.44.3      TCP        54 52788 → 443 [ACK] Seq=71 Ack=1613 Win=513 Len=0
 11 9.421012   52.108.44.3      192.168.188.78   TLSv1.2   695 Application Data
 12 9.474080   192.168.188.78   52.108.44.3      TCP        54 52788 → 443 [ACK] Seq=71 Ack=2254 Win=517 Len=0
 13 9.788285   192.168.188.78   40.126.35.21     TCP        54 53164 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
 14 9.813617   52.108.44.3      192.168.188.78   TLSv1.2    89 Application Data
 15 9.846151   52.108.44.3      192.168.188.78   TLSv1.2   691 Application Data
 16 9.846238   192.168.188.78   52.108.44.3      TCP        54 52788 → 443 [ACK] Seq=71 Ack=2926 Win=514 Len=0
 17 9.879724   40.126.35.21     192.168.188.78   TCP        54 443 → 53164 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
 18 9.879813   192.168.188.78   40.126.35.21     TCP        54 53164 → 443 [ACK] Seq=2 Ack=2 Win=512 Len=0
 19 11.201799  192.168.188.78   20.198.118.190   TLSv1.2    97 Application Data
 20 11.247890  20.198.118.190   192.168.188.78   TLSv1.2   228 Application Data
```

```
> Frame 3: 691 bytes on wire (5528 bits), 691 bytes captured (5528 bits) on interface \Device\NPF_{3157F5…
> Ethernet II, Src: 3e:6e:b0:98:af:f1 (3e:6e:b0:98:af:f1), Dst: Intel_fd:ad:5e (68:7a:64:fd:ad:5e)
> Internet Protocol Version 4, Src: 52.108.44.3, Dst: 192.168.188.78
> Transmission Control Protocol, Src Port: 443, Dst Port: 52788, Seq: 1, Ack: 1, Len: 637
> Transport Layer Security
```

```
0000  68 7a 64 fd ad 5e 3e 6e  b0 98 af f1 08 00 45 00   hzd··^>n ······E·
0010  02 a5 bc a4 40 00 6d 06  71 48 34 6c 2c 03 c0 a8   ····@·m· qH4l,···
0020  bc 4e 01 bb ce 34 1d 18  9a 08 25 d1 b9 58 50 18   ·N···4·· ··%··XP·
0030  3f fc b3 79 00 00 17 03  03 02 78 e3 f0 08 9c d2   ?··y···· ··x·····
0040  02 45 fe b6 54 ed a1 fa  44 f1 33 d5 64 b1 9e b3   ·E··T··· D·3·d···
0050  26 91 a4 7c 17 ad 45 4e  05 2f 90 ab bd ef fd 87   &··|··EN ·/······
0060  c0 73 01 0f 8e 5c d0 68  cb 4a 66 6c 54 c6 74 1c   ·s···\·h ·JflT·t·
0070  e8 c5 d3 15 b1 d7 f1 e2  10 ce a6 5a 0b 21 60 c6   ········ ···Z·!`·
0080  dc 35 72 7c 18 7a 6c 94  d4 69 03 32 2c 43 e5 b4   ·5r|·zl· ·i·2,C··
0090  94 0d 78 ea ca 32 e3 e0  c0 f6 6c 40 9a 75 7c ca   ··x··2·· ··l@·u|·
00a0  6f de dc 90 71 25 ef 4d  13 34 d9 d7 33 2f 4b 42   o···q%·M ·4··3/KB
00b0  c2 30 14 75 08 de 12 9d  a6 c7 26 24 b4 e7 f0 11   ·0·u···· ··&$····
00c0  54 c4 21 8a 91 64 76 9e  7c 76 ab 85 2f cf e1 6f   T·!··dv· |v··/··o
00d0  f3 99 85 bc 52 79 04 09  b3 13 2a 87 65 3c ea c5   ····Ry·· ··*·e<··
00e0  cf 0d ec b8 ab 11 21 e7  d6 92 03 65 c3 71 04 53   ······!· ···e·q·S
00f0  d0 f7 91 6a 83 ad be 2b  c1 ae a5 9e 61 5d 5b 4a   ···j···+ ····a][J
0100  5f 70 3a 7e 2d c8 8b 22  c0 4c df d5 75 9f 2f 51   _p:~-··" ·L··u·/Q
0110  b7 55 b9 ee 6b b5 be c8  8c b6 1c 79 c9 bd 8b 47   ·U··k··· ···y···G
0120  f2 d8 d1 2f e3 71 9b 28  25 5a b9 2c f4 e7 eb 3a   ···/·q·( %Z·,···:
0130  b7 45 d5 25 7d b4 3a 2e  88 62 34 4f 9f ee 67 01   ·E·%}·:. ·b4O··g·
0140  ef 0f f4 ee a9 12 3a 01  57 df 67 57 de 7d 58 7a   ······:· W·gW·}Xz
0150  21 1e 43 0f 90 00 b7 6b  9c 28 9b dd 04 c0 19 db   !·C····k ·(······
0160  1d b7 f4 61 3e d9 50 eb  bc 31 d1 2a bc 90 80 b9   ···a>·P· ·1·*····
```

Packets: 207 · Displayed: 199 (96.1%)

Result:

Hence, the capturing of packets using wire shark network analyzer was analyzed for HTTP.

EXPERIMENT 12

Identifying Hidden Processes and terminate processes

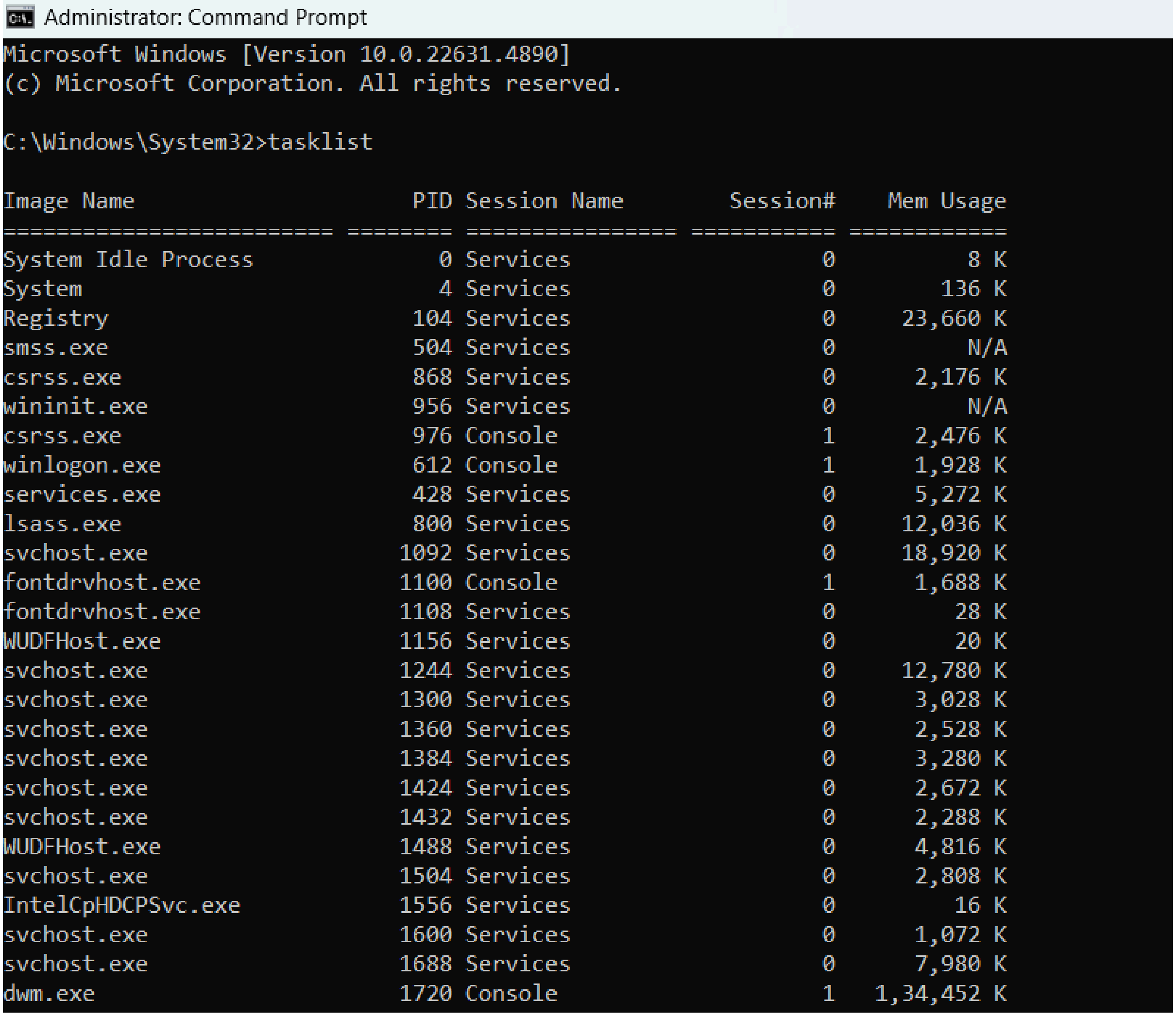
Aim: To Identify Hidden Processes and terminate processes.

SOFTWARE USED: CMD prompt.

Procedure:

1. Open cmd with run as administrator.
2. List all running processes:

```
tasklist
```

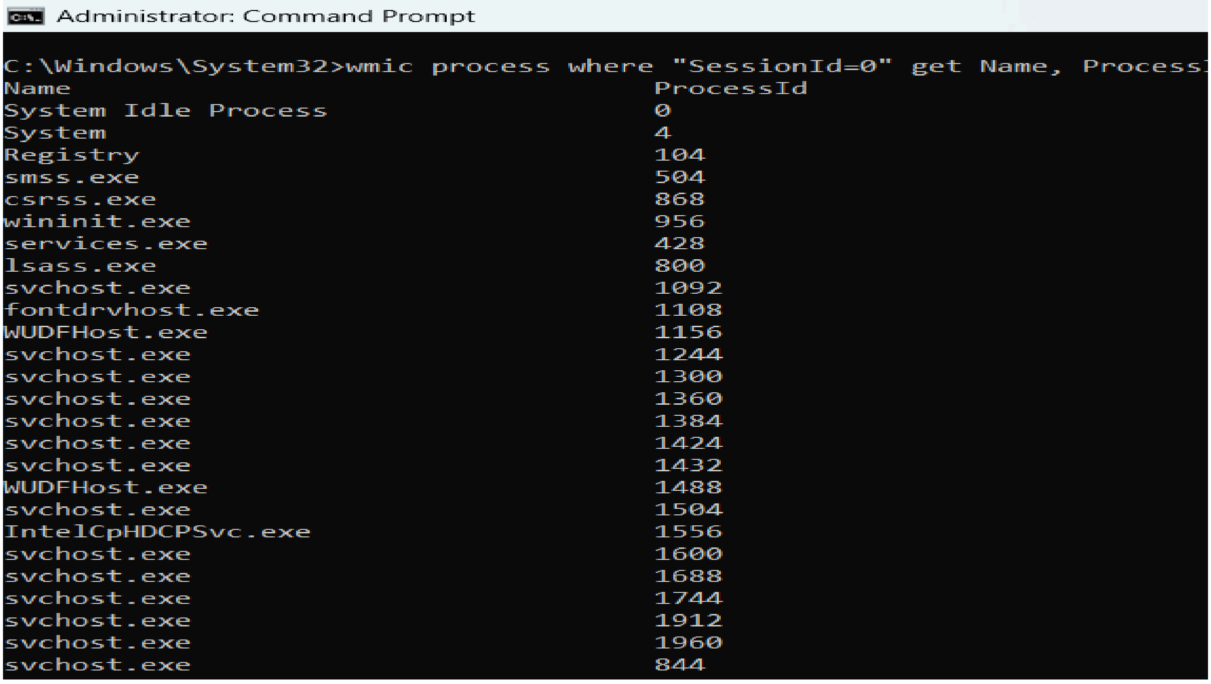


```
Microsoft Windows [Version 10.0.22631.4890]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        136 K
Registry                       104 Services                   0     23,660 K
smss.exe                       504 Services                   0          N/A
csrss.exe                      868 Services                   0      2,176 K
wininit.exe                    956 Services                   0          N/A
csrss.exe                      976 Console                    1      2,476 K
winlogon.exe                   612 Console                    1      1,928 K
services.exe                   428 Services                   0      5,272 K
lsass.exe                      800 Services                   0     12,036 K
svchost.exe                   1092 Services                   0     18,920 K
fontdrvhost.exe               1100 Console                    1      1,688 K
fontdrvhost.exe               1108 Services                   0         28 K
WUDFHost.exe                  1156 Services                   0         20 K
svchost.exe                   1244 Services                   0     12,780 K
svchost.exe                   1300 Services                   0      3,028 K
svchost.exe                   1360 Services                   0      2,528 K
svchost.exe                   1384 Services                   0      3,280 K
svchost.exe                   1424 Services                   0      2,672 K
svchost.exe                   1432 Services                   0      2,288 K
WUDFHost.exe                  1488 Services                   0      4,816 K
svchost.exe                   1504 Services                   0      2,808 K
IntelCpHDCPSvc.exe            1556 Services                   0         16 K
svchost.exe                   1600 Services                   0      1,072 K
svchost.exe                   1688 Services                   0      7,980 K
dwm.exe                       1720 Console                    1   1,34,452 K
```

3. The above command will list all running tasks.

4. now run the below command to list all the hidden tasks

   wmic proess where "SessionId=0" get Name, ProcessId

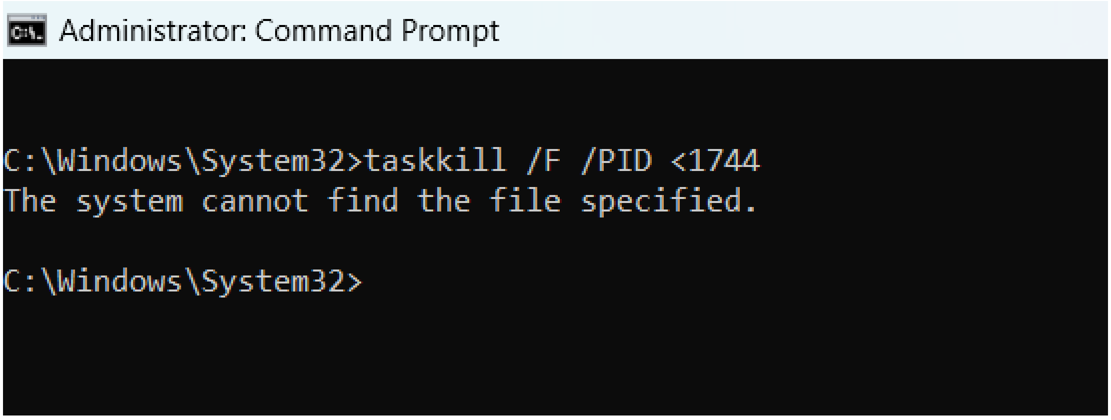


```
C:\Windows\System32>wmic process where "SessionId=0" get Name, Process
Name                                      ProcessId
System Idle Process                       0
System                                    4
Registry                                  104
smss.exe                                  504
csrss.exe                                 868
wininit.exe                               956
services.exe                              428
lsass.exe                                 800
svchost.exe                               1092
fontdrvhost.exe                           1108
WUDFHost.exe                              1156
svchost.exe                               1244
svchost.exe                               1300
svchost.exe                               1360
svchost.exe                               1384
svchost.exe                               1424
svchost.exe                               1432
WUDFHost.exe                              1488
svchost.exe                               1504
IntelCpHDCPSvc.exe                        1556
svchost.exe                               1600
svchost.exe                               1688
svchost.exe                               1744
svchost.exe                               1912
svchost.exe                               1960
svchost.exe                               844
```

5. The above command will list all running hidden tasks.
6. to terminate any running task run the below command

   taskkill /F /PID <PID_NUMBER>

7. The Pid_number should be the ID of the process.



```
C:\Windows\System32>taskkill /F /PID <1744
The system cannot find the file specified.

C:\Windows\System32>
```

Result:

Hence, the termination of the running process can be executed successfully.

EXPERIMENT 13

Hiding a ZIP File Inside an Image

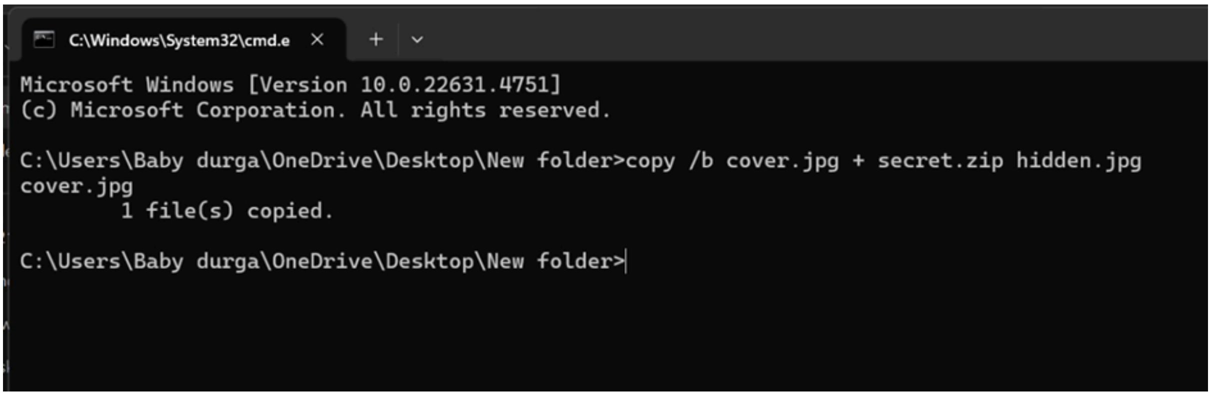
Aim: To Hide a ZIP File Inside an Image.

SOFTWARE USED: CMD prompt.

Procedure:

1. Place the image file (cover.jpg) and ZIP file (secret.zip) in the same folder.
2. Open cmd inside the folder.
3. Run the following cmd

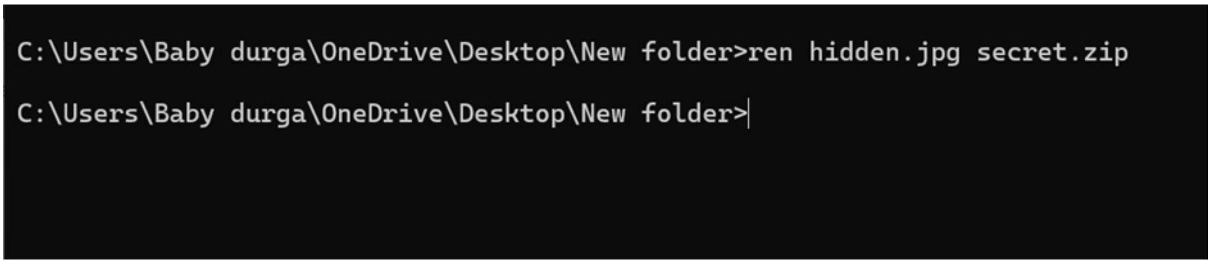
```
copy /b cover.jpg + secret.zip hidden.jpg
```



```
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Baby durga\OneDrive\Desktop\New folder>copy /b cover.jpg + secret.zip hidden.jpg
cover.jpg
        1 file(s) copied.

C:\Users\Baby durga\OneDrive\Desktop\New folder>
```

8. hidden.jpg will look like a normal image but contains the hidden ZIP file.
9. To view the hidden file run the below cmd

ren hidden.jpg secret.zip



```
C:\Users\Baby durga\OneDrive\Desktop\New folder>ren hidden.jpg secret.zip

C:\Users\Baby durga\OneDrive\Desktop\New folder>
```

10. After the above cmd the hidden file will be restored.

Result:

Hence, hiding the file command executed successfully.

EXPERIMENT 14

View All Wi-Fi Passwords Saved on the Computer

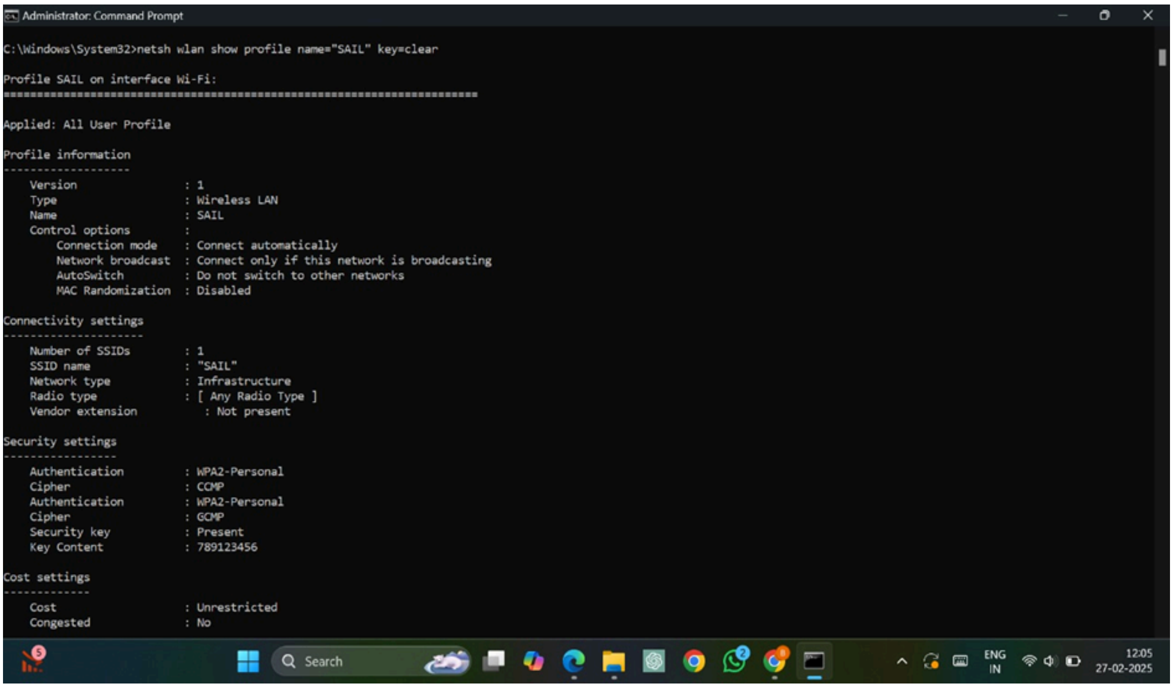
Aim: To View All Wi-Fi Passwords Saved on the Computer.

SOFTWARE USED: CMD prompt.

Procedure:

1. Open Command prompt as administrator
2. Run below command to see all saved Wi-Fi networks

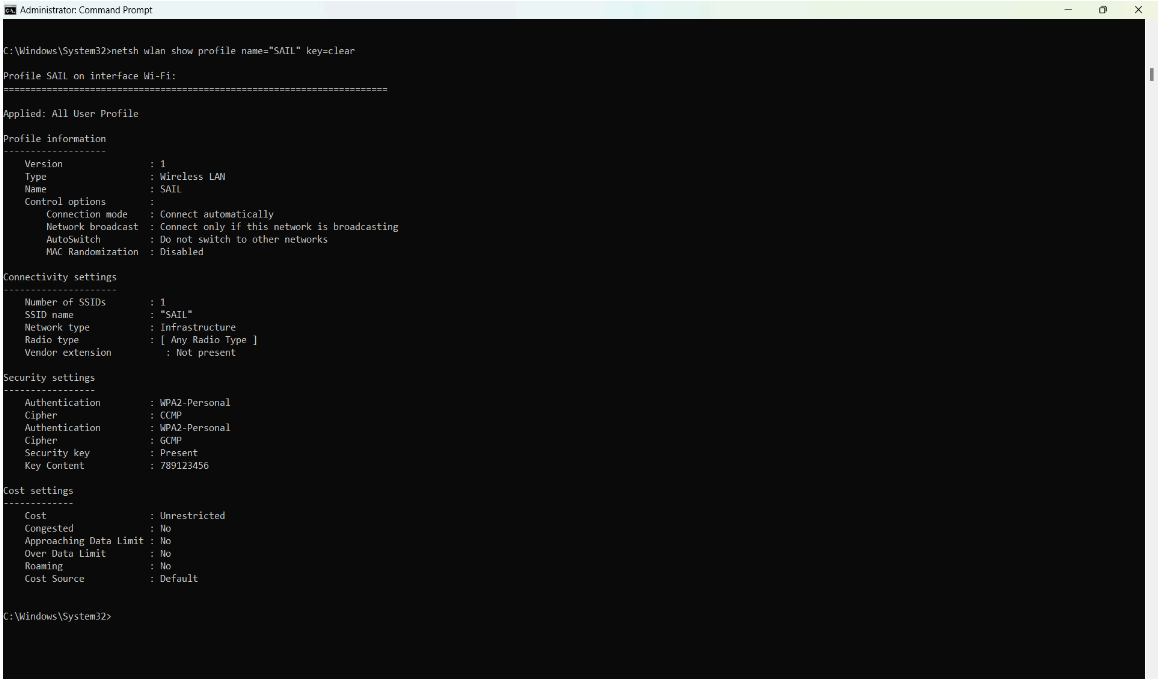
```
netsh wlan show profiles
```



```
C:\Windows\System32>netsh wlan show profile name="SAIL" key=clear

Profile SAIL on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : SAIL
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "SAIL"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : 789123456

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
```

3. To see the password for a specific Wi-Fi network, use below cmd

```
netsh wlan show profile name="WiFi-Network-Name"
key=clear
```



```
C:\Windows\System32>netsh wlan show profile name="SAIL" key=clear

Profile SAIL on interface Wi-Fi:
========================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : SAIL
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "SAIL"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : 789123456

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default


C:\Windows\System32>
```

4. Now the password of the desired password is found.

Result:

Hence, the password of the desired wifi is executed successfully.

EXPERIMENT 15

To extract the recent login and logout

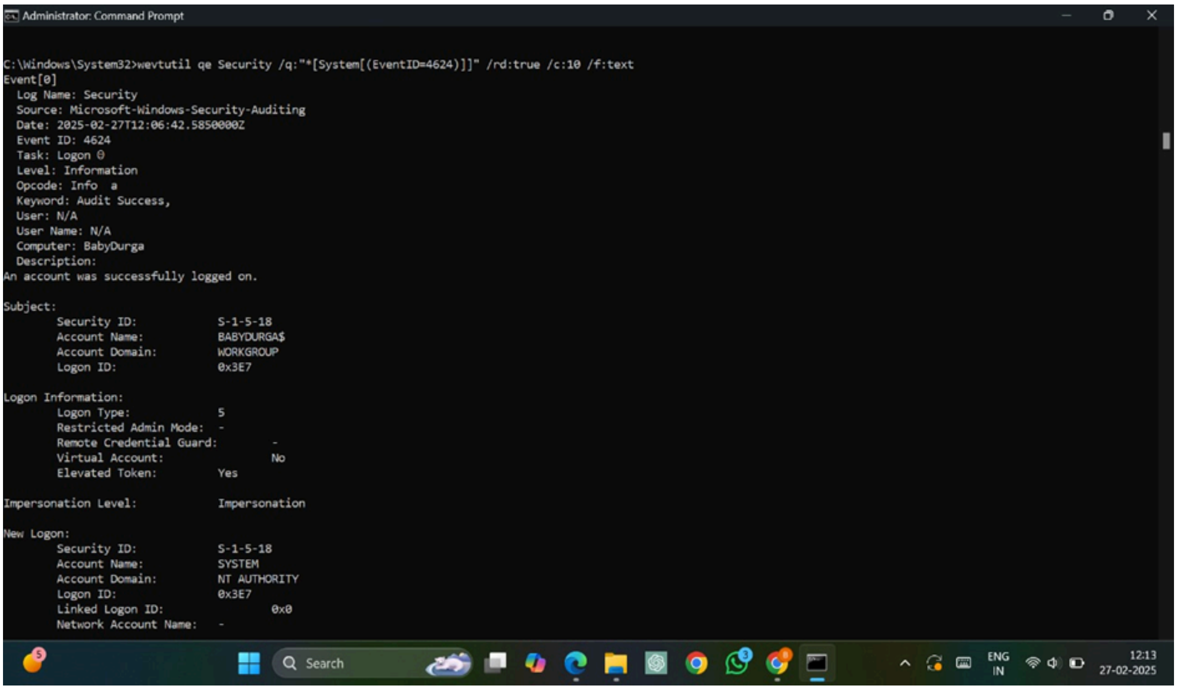
Aim: To extract the recent login and logout

SOFTWARE USED: CMD prompt.

Procedure:

5. Open Command prompt as administrator
6. Run below command to see to recent logins

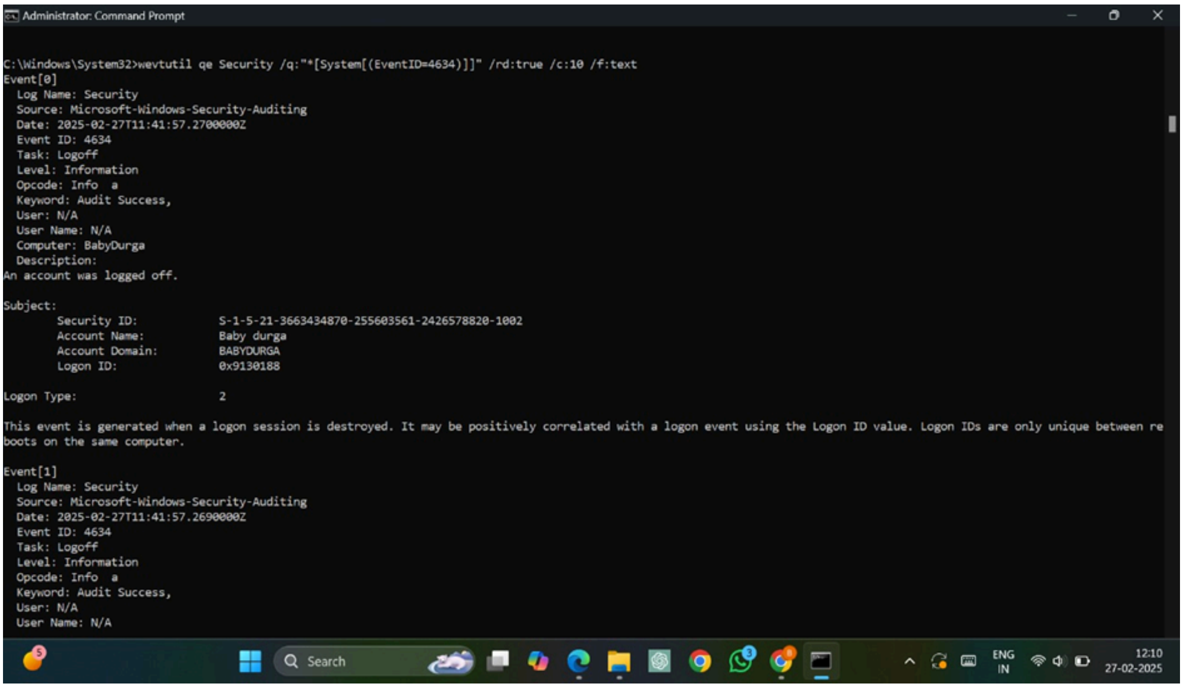
```
wevtutil qe Security /q:"*[System[(EventID=4624)]]"
/rd:true /c:10 /f:text
```



```
C:\Windows\System32>wevtutil qe Security /q:"*[System[(EventID=4624)]]" /rd:true /c:10 /f:text
Event[0]
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2025-02-27T12:06:42.5850000Z
  Event ID: 4624
  Task: Logon 0
  Level: Information
  Opcode: Info  a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
  Computer: BabyDurga
  Description:
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           BABYDURGA$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Remote Credential Guard:        -
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7
        Linked Logon ID:                0x0
        Network Account Name:   -
```

7. Run below command to see to recent logout

```
wevtutil qe Security /q:"*[System[(EventID=4634)]]"
/rd:true /c:10 /f:text
```



```
C:\Windows\System32>wevtutil qe Security /q:"*[System[(EventID=4634)]]" /rd:true /c:10 /f:text
Event[0]
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2025-02-27T11:41:57.2700000Z
  Event ID: 4634
  Task: Logoff
  Level: Information
  Opcode: Info  a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
  Computer: BabyDurga
  Description:
An account was logged off.

Subject:
        Security ID:            S-1-5-21-3663434870-255603561-2426578820-1002
        Account Name:           Baby durga
        Account Domain:         BABYDURGA
        Logon ID:               0x9130188

Logon Type:                     2

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between re
boots on the same computer.

Event[1]
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2025-02-27T11:41:57.2690000Z
  Event ID: 4634
  Task: Logoff
  Level: Information
  Opcode: Info  a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
```

8. Now the last 10 logins and logouts can be found.

Result:

Hence, recent 10 login and logout can be extracted successfully .