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 Recovermyfile tool
URL: [Data recovery software download: Get Recover My Files here]

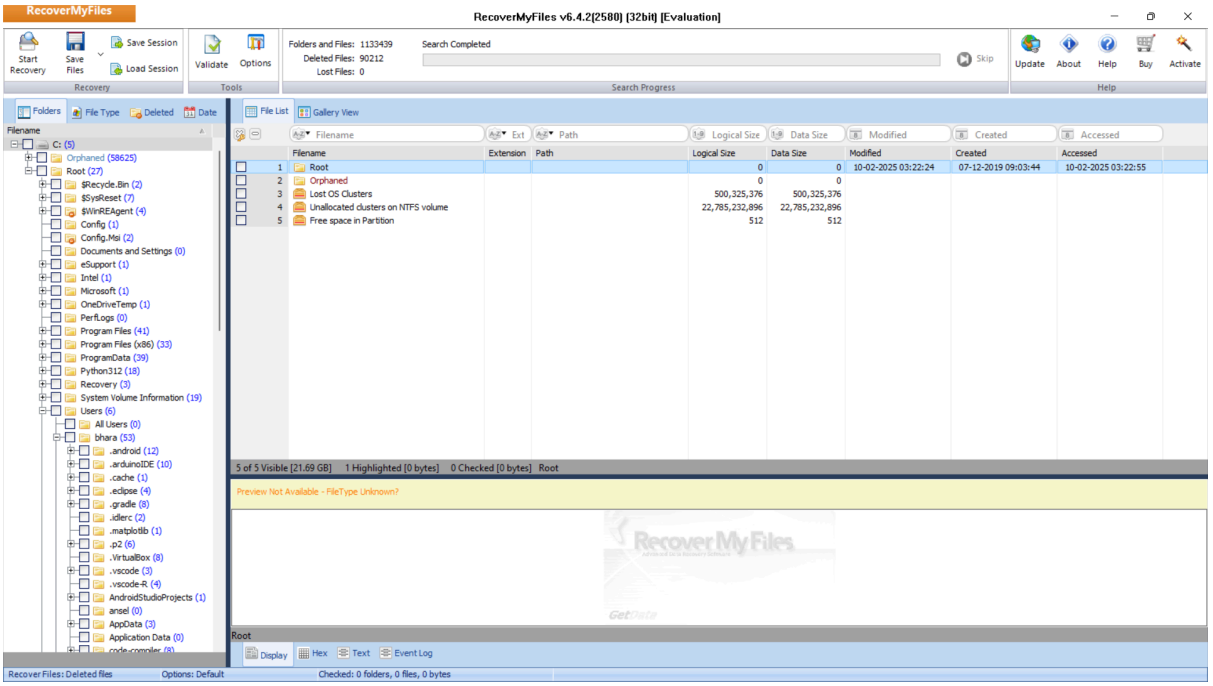
Step 2: Setup from the exe file downloaded

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)



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?

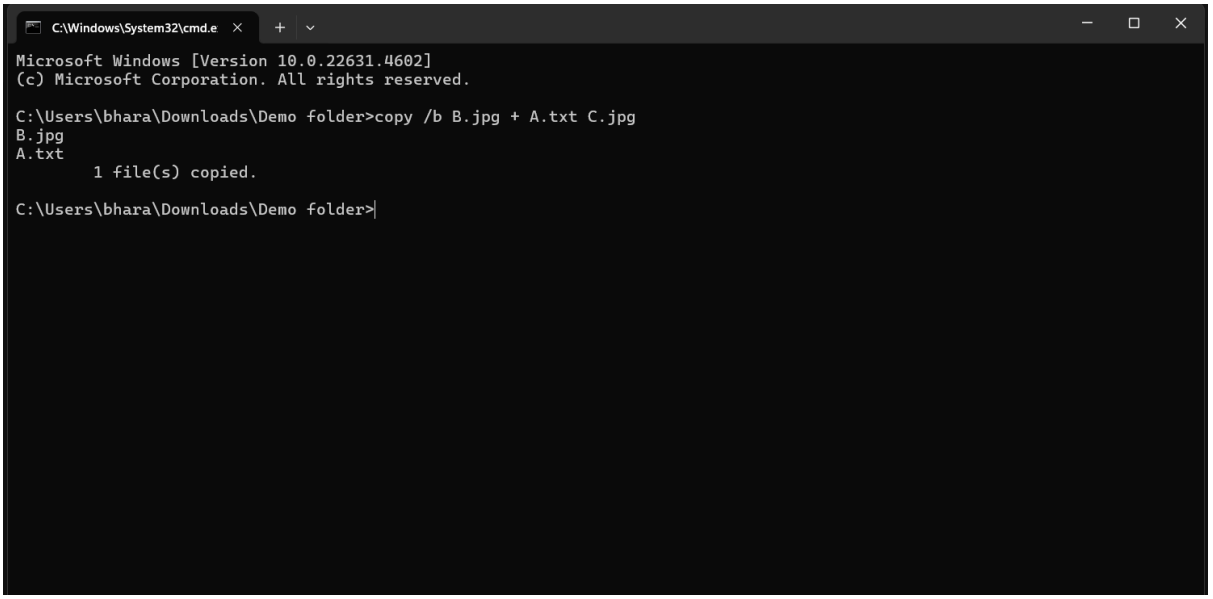
Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”. Where “C.jpg” is our output file which contains the text hidden in the image file.

Follow the steps:

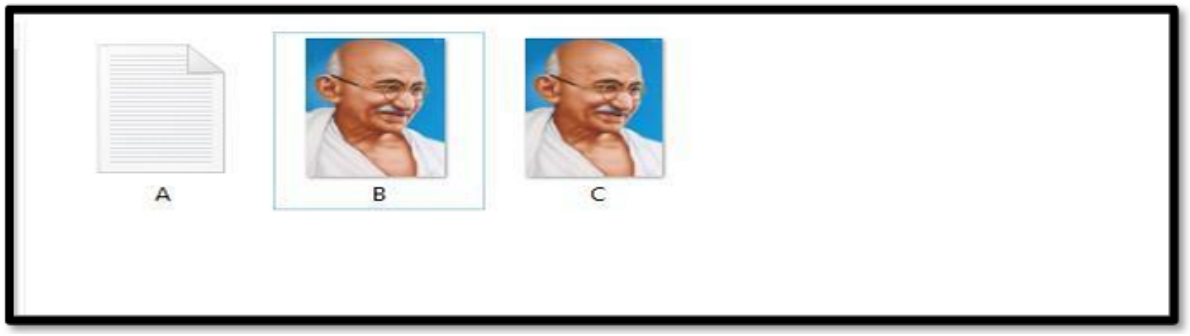
1. copy the file need to hide, to desktop (for our tutorial let us assume the file to be "A.txt")
2. copy the image, within which you need to hide the file, to desktop (let it be "B.jpg")
3. now open the cmd: >ctrl+r >type: cmd and hit enter
4. in cmd first type the code as follows: >cd desktop NOTE: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

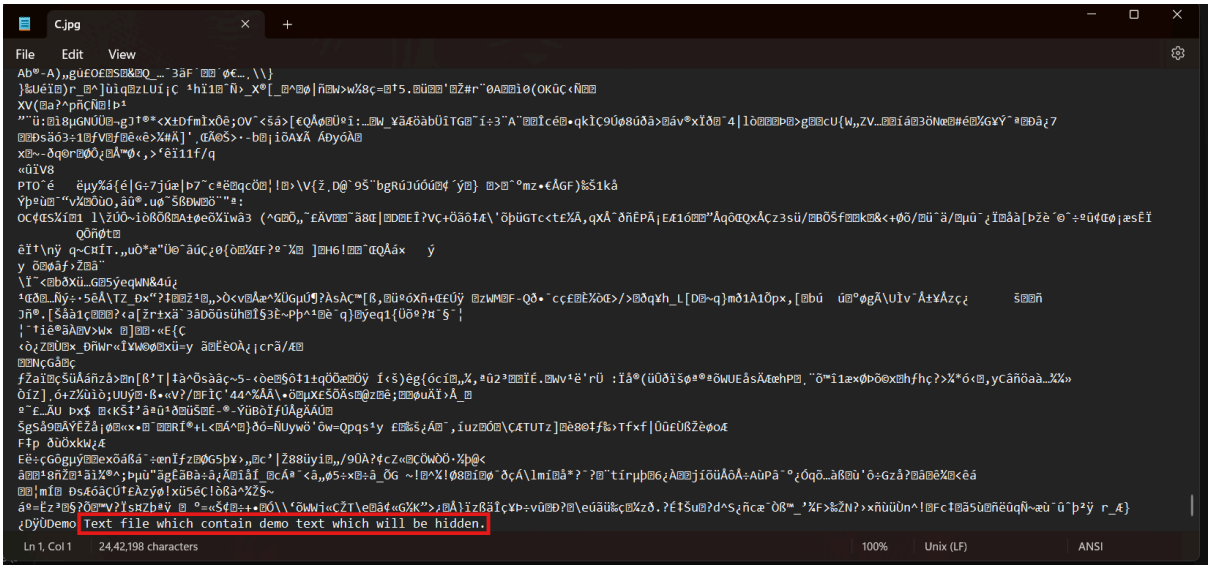


"C.jpg" is the output image inside this out image our file is hidden



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



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.

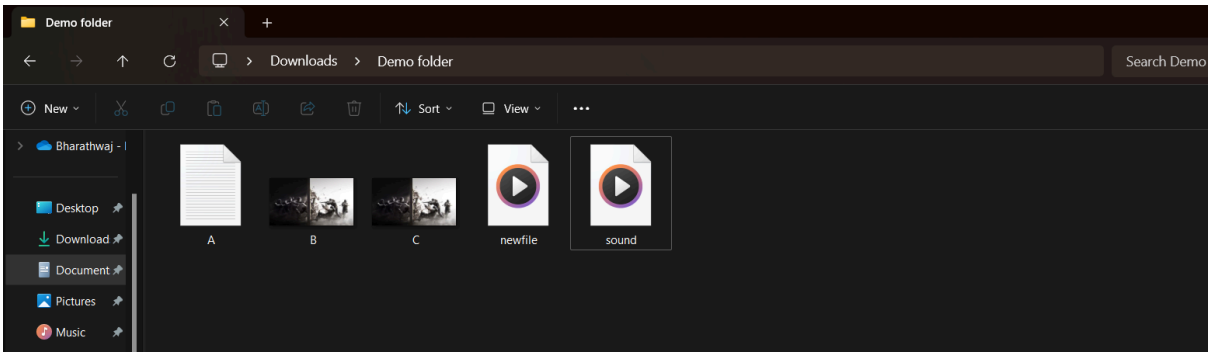
Follow the steps:

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

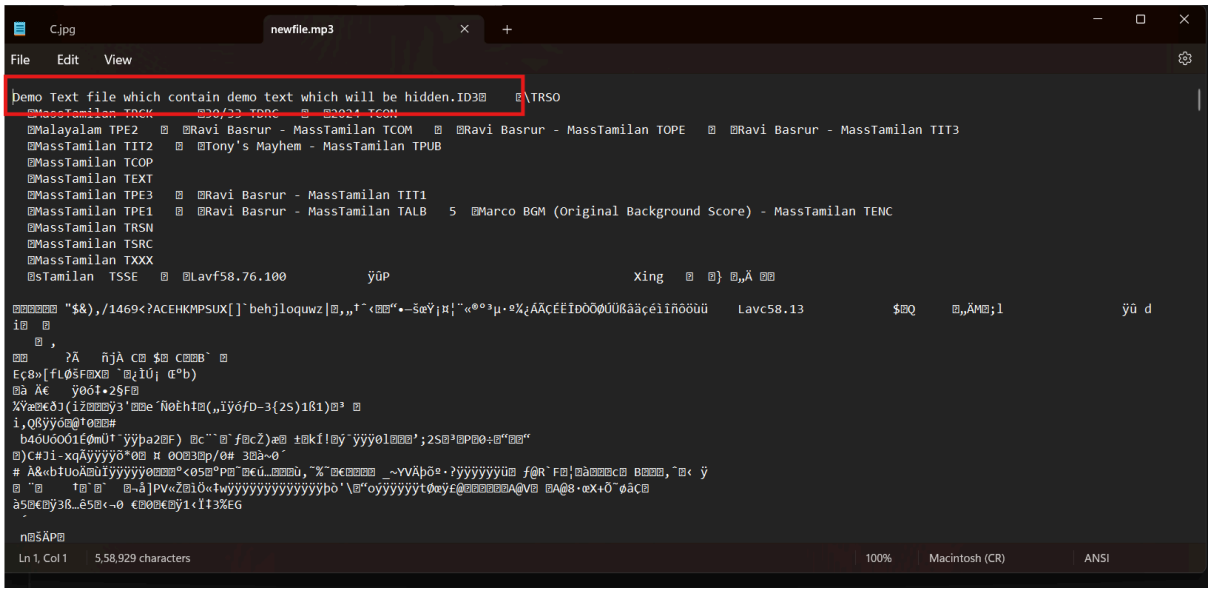
Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial- audio.mp3 Resulting-audio-name.mp3*

"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



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.

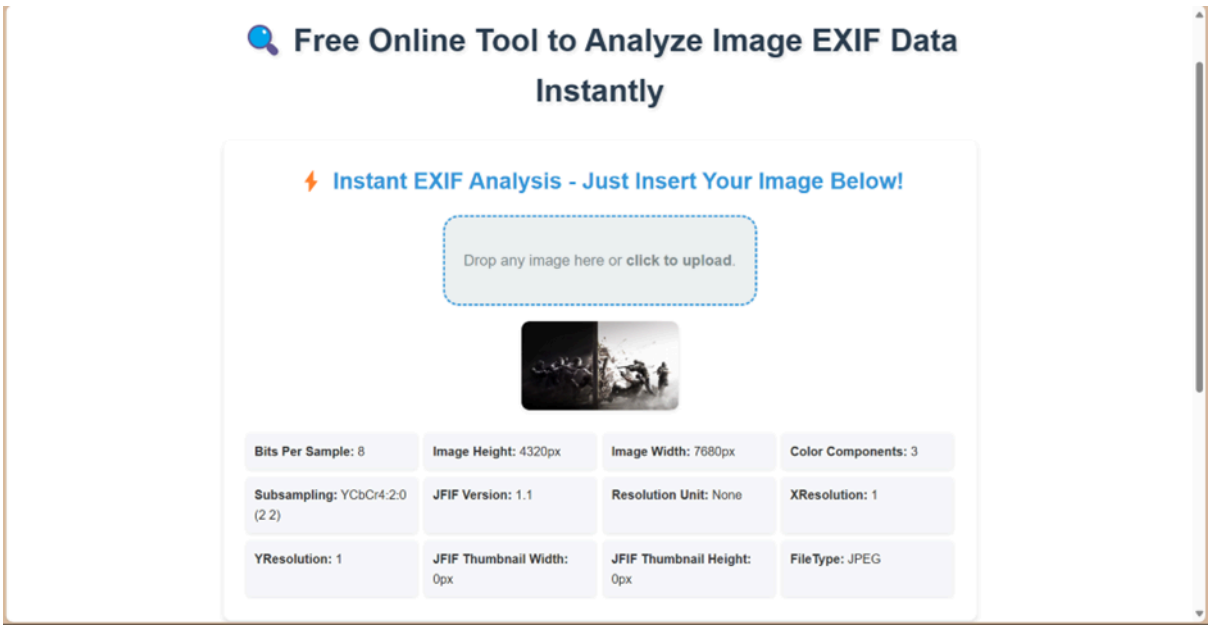
Procedure:

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

Step 2: Find an Appropriate image file

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

Step 4: Analyse the exif features of the image



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.

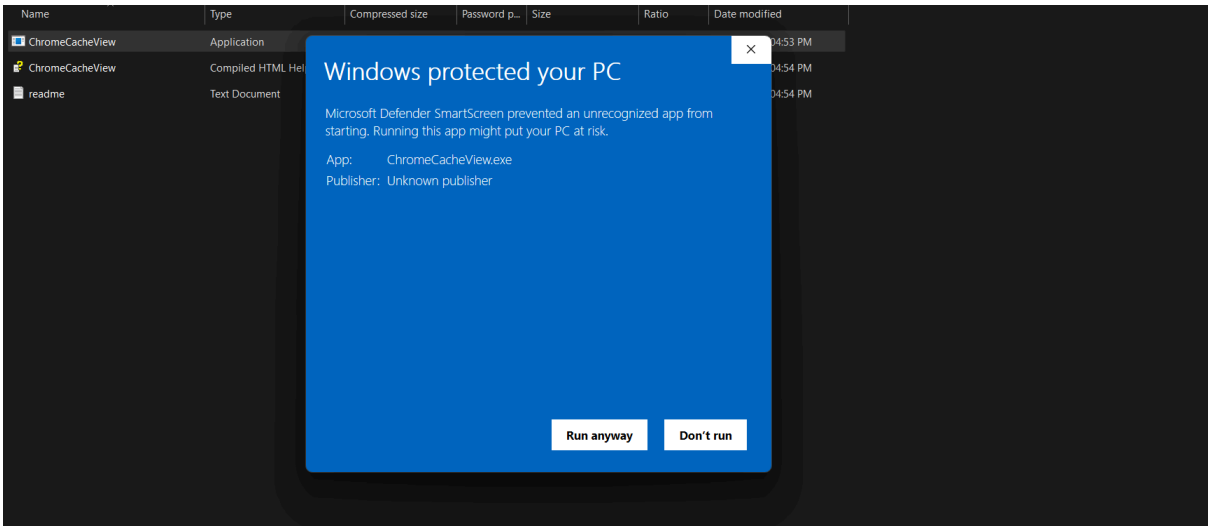
Procedure:

Step 1: Download Browsing History View tool
URL:

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

Step 2: Setup from the exe file downloaded

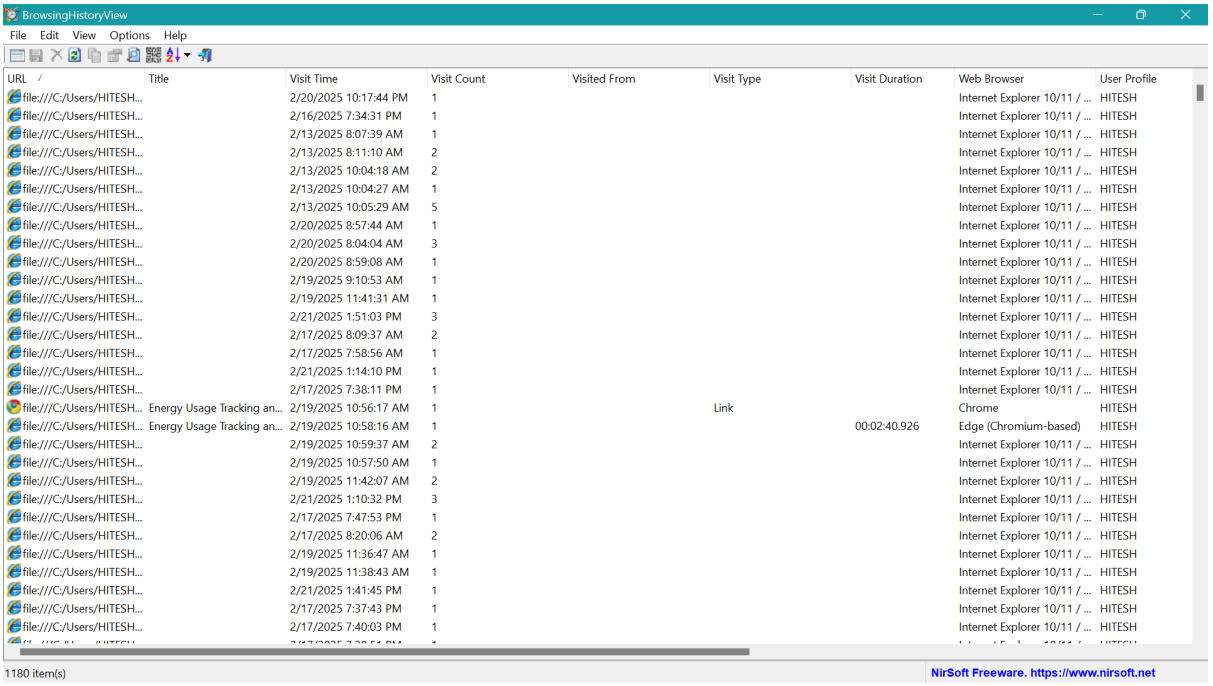
Step 3: Click run anyway when the below dialog box appears



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.



Result:

The experiment has been successfully executed

EXPERIMENT-06

Extract Chrome cache using forensic tools

Aim of the Experiment:

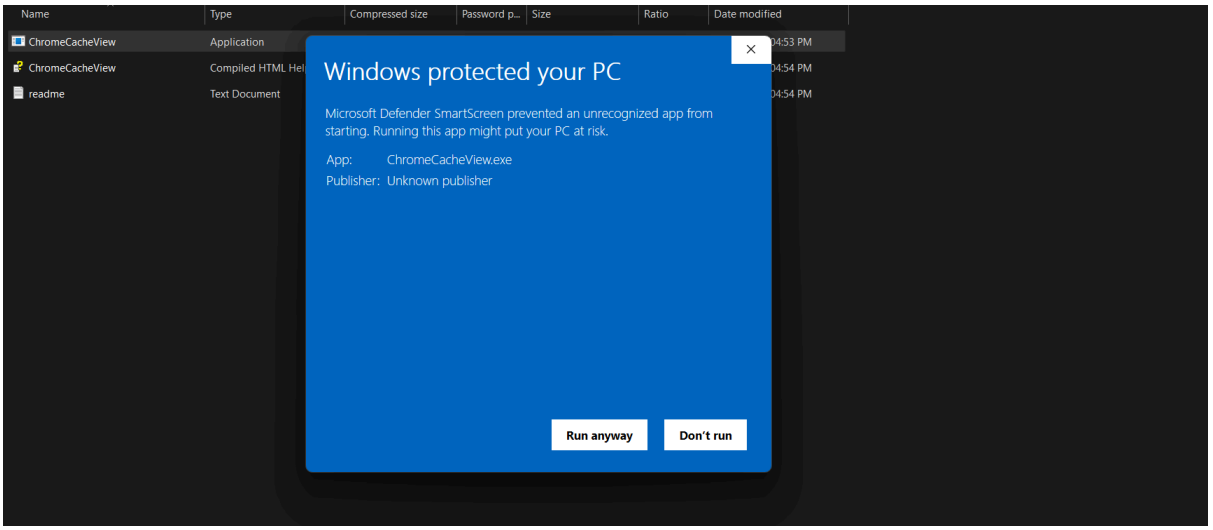
To Extract Chrome cache using forensic tools and analyse them.

Procedure:

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

Step 2: Setup from the exe file downloaded

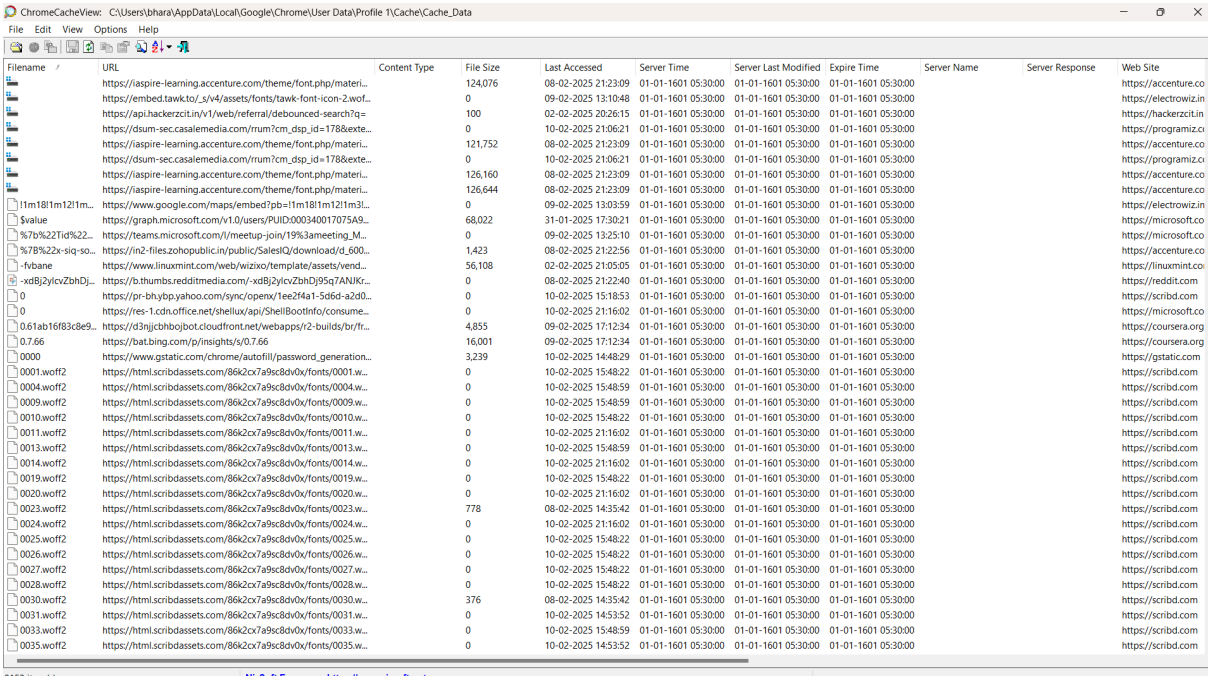
Step 3: Click run anyway when the below dialog box appears



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.



Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Web Site
	https://iaspire-learning.accenture.com/theme/font.php/materi...		124,076	08-02-2025 21:23:09	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://accenture.co
	https://embed.tawk.to/_s/v4/assets/fonts/tawk-font-icon-2.wof...		0	09-02-2025 13:10:48	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://electrowiz.in
	https://api.hackerzcit.in/v1/web/referral/debounced-search?q=		100	02-02-2025 20:26:15	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://hackerzcit.in
	https://dsum-sec.casalemedia.com/rrum?cm_dsp_id=178&exte...		0	10-02-2025 21:06:21	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://programiz.c
	https://iaspire-learning.accenture.com/theme/font.php/materi...		121,752	08-02-2025 21:23:09	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://accenture.co
	https://dsum-sec.casalemedia.com/rrum?cm_dsp_id=178&exte...		0	10-02-2025 21:06:21	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://programiz.c
	https://iaspire-learning.accenture.com/theme/font.php/materi...		126,160	08-02-2025 21:23:09	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://accenture.co
	https://iaspire-learning.accenture.com/theme/font.php/materi...		126,644	08-02-2025 21:23:09	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://accenture.co
!1m18!1m12!1m...	https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!...		0	09-02-2025 13:03:59	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://electrowiz.in
$value	https://graph.microsoft.com/v1.0/users/PUID:00034001707 5A9...		68,022	31-01-2025 17:30:21	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://microsoft.co
%7b%22Tid%22...	https://teams.microsoft.com/l/meetup-join/19%3ameeting_M...		0	09-02-2025 13:25:10	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://microsoft.co
%7B%22x-siq-so...	https://in2-files.zohopublic.in/public/SalesIQ/download/d_600...		1,423	08-02-2025 21:22:56	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://accenture.co
-fvbane	https://www.linuxmint.com/web/wizixo/template/assets/vend...		56,108	02-02-2025 21:05:05	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://linuxmint.co
-xdBj2ylcvZbhDj...	https://b.thumbs.redditmedia.com/-xdBj2ylcvZbhDj95q7ANIKr...		0	08-02-2025 21:22:40	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://reddit.com
0	https://pr-bh.ybp.yahoo.com/sync/openx/1ee2f4a1-5d6d-a2d0...		0	10-02-2025 15:18:53	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0	https://res-1.cdn.office.net/shellux/api/ShellBootInfo/consume...		0	10-02-2025 21:16:02	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://microsoft.co
0.61ab16f83c8e9...	https://d3njjcbhbojbot.cloudfront.net/webapps/r2-builds/br/fr...		4,855	09-02-2025 17:12:34	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://coursera.org
0.7.66	https://bat.bing.com/p/insights/s/0.7.66		16,001	09-02-2025 17:12:34	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://coursera.org
0000	https://www.gstatic.com/chrome/autofill/password_generation...		3,239	10-02-2025 14:48:29	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://gstatic.com
0001.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0001.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0004.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0004.w...		0	10-02-2025 15:48:59	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0009.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0009.w...		0	10-02-2025 15:48:59	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0010.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0010.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0011.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0011.w...		0	10-02-2025 21:16:02	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0013.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0013.w...		0	10-02-2025 15:48:59	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0014.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0014.w...		0	10-02-2025 21:16:02	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0019.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0019.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0020.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0020.w...		0	10-02-2025 21:16:02	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0023.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0023.w...		778	08-02-2025 14:35:42	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0024.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0024.w...		0	10-02-2025 21:16:02	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0025.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0025.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0026.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0026.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0027.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0027.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0028.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0028.w...		0	10-02-2025 15:48:22	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0030.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0030.w...		376	08-02-2025 14:35:42	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0031.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0031.w...		0	10-02-2025 14:53:52	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0033.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0033.w...		0	10-02-2025 15:48:59	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com
0035.woff2	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0035.w...		0	10-02-2025 14:53:52	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://scribd.com

Result:

The experiment has been successfully executed

EXPERIMENT-07

Extract last activity using forensic tools

Aim of the Experiment:

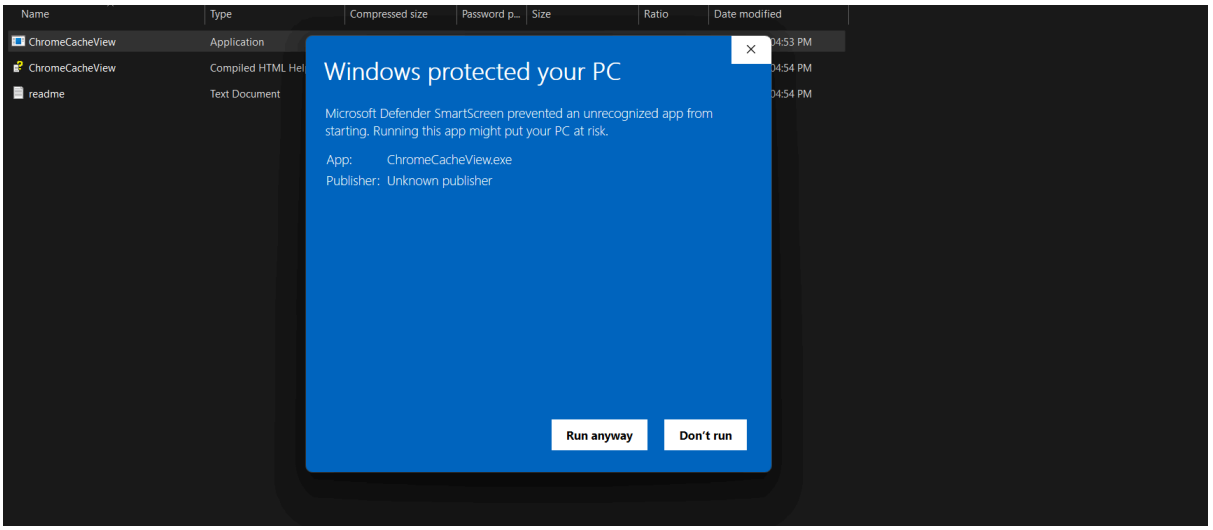
To Extract the last activity view using forensic tools and analyse them.

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

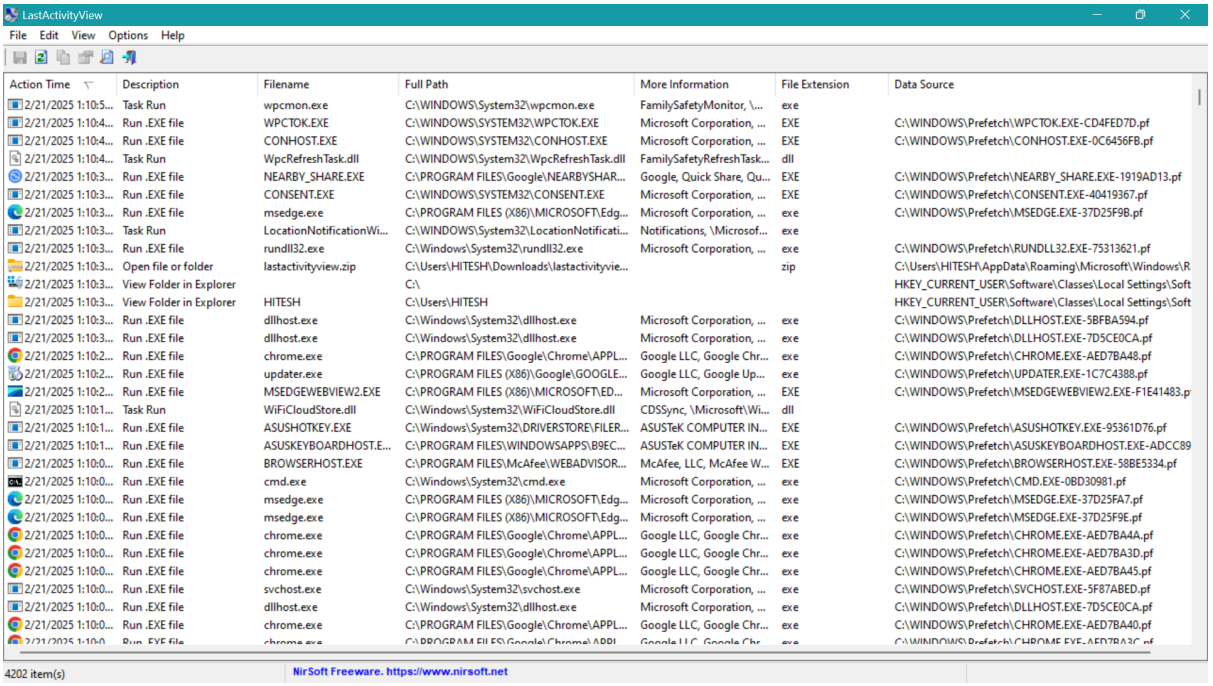
Step 3: Click run anyway when the below dialog box appears



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.



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:

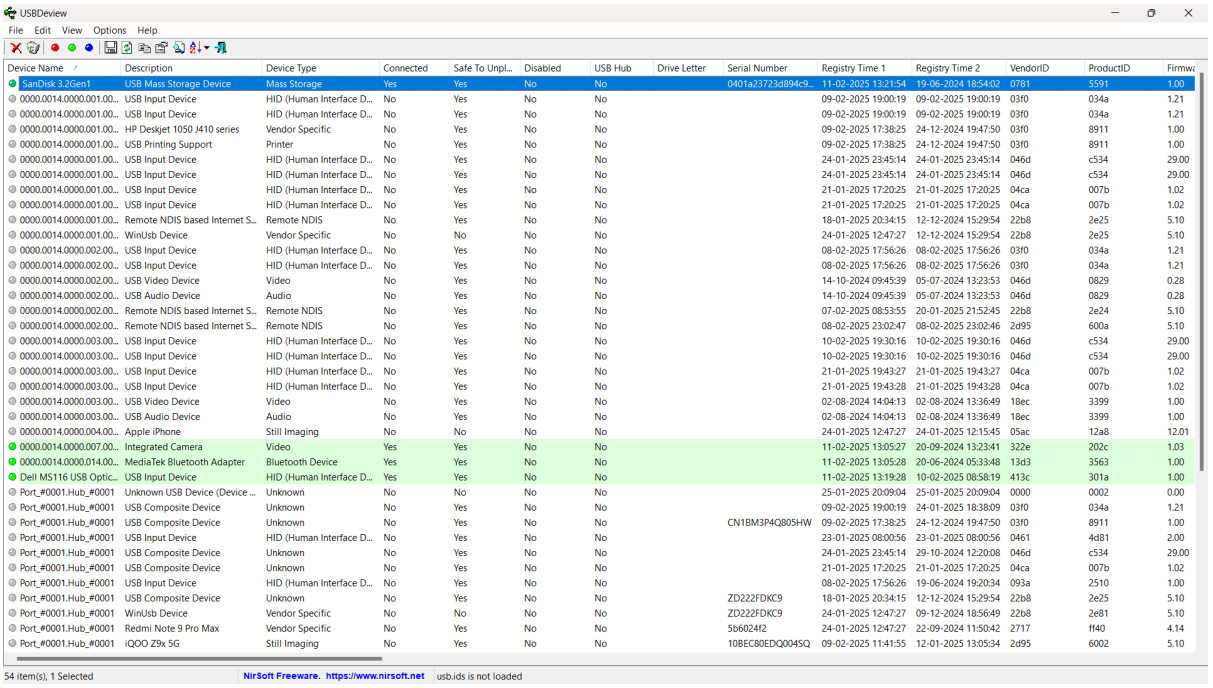
Step 1: Download previous USB devices view tool
URL: [USBDeview download | SourceForge.net]

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.



Result:

The experiment has been successfully executed

EXPERIMENT 9

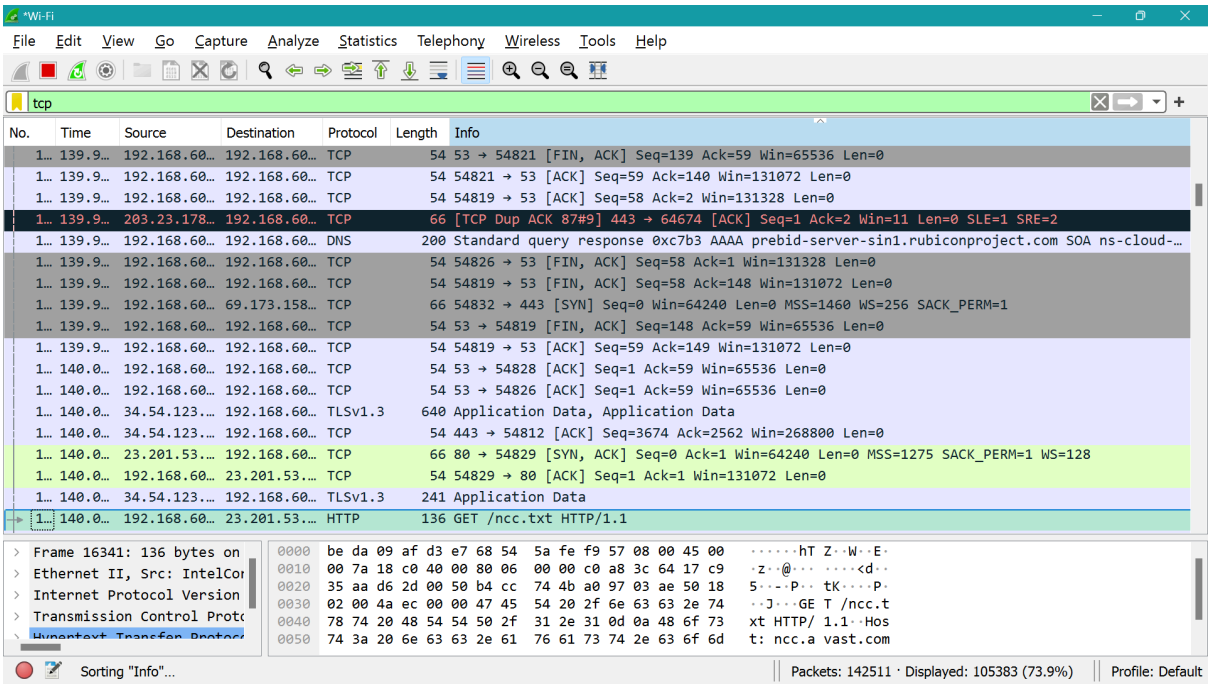
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-TCP

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.



Result:

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

EXPERIMENT 10

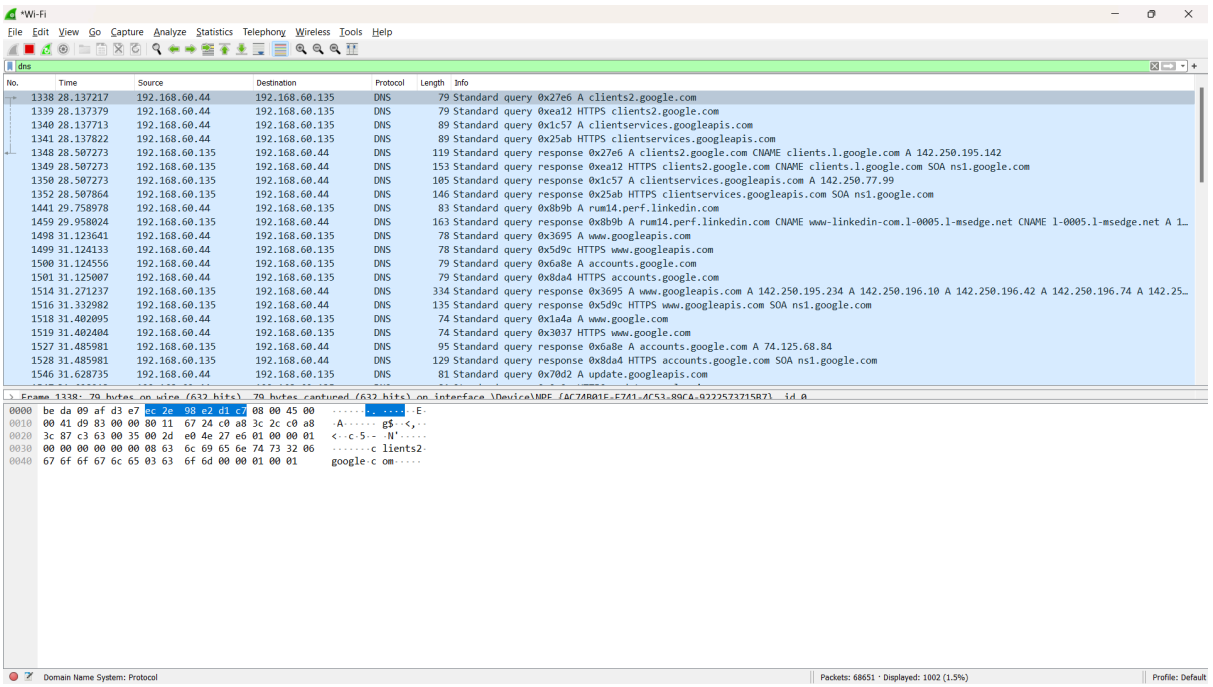
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-DNS

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.



Result:

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

EXPERIMENT 11

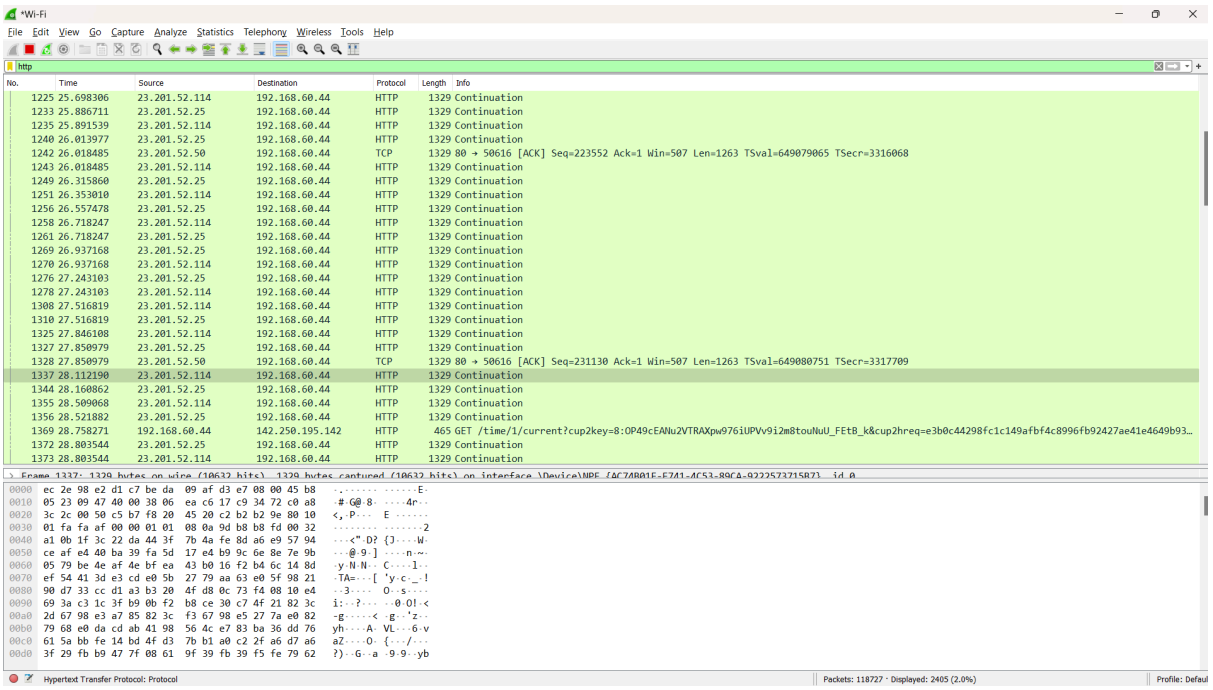
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-HTTP

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.



Result:

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

EXPERIMENT 12

Identifying Hidden Processes and terminate processes

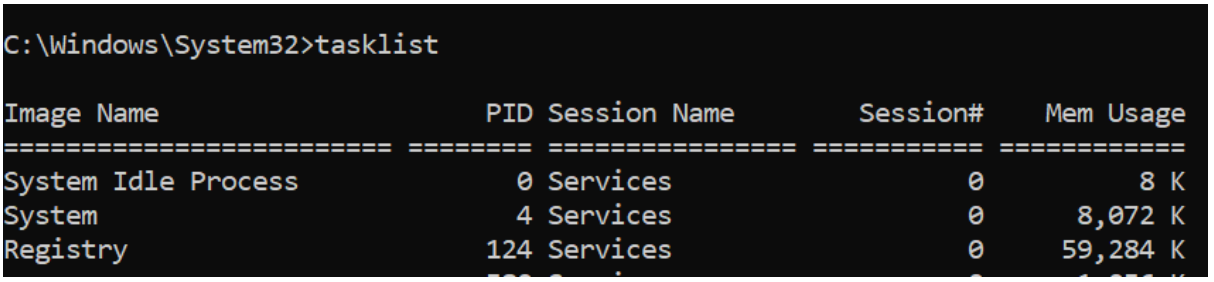
Aim: To Identify Hidden Processes and terminate processes.

SOFTWARE USED: CMD prompt.

Procedure:

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

`tasklist`



3. The above command will list all running tasks.
4. now run the below command to list all the hidden tasks

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

```
C:\Windows\System32>
C:\Windows\System32>wmic process where "SessionId=0" get Name, ProcessId
Name                         ProcessId
System Idle Process          0
System                       4
Registry                     124
```

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>
C:\Windows\System32>taskkill /F /PID 18232
SUCCESS: The process with PID 18232 has been terminated.
```

Result:

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

EXPERIMENT 13

Hiding a ZIP File Inside an Image

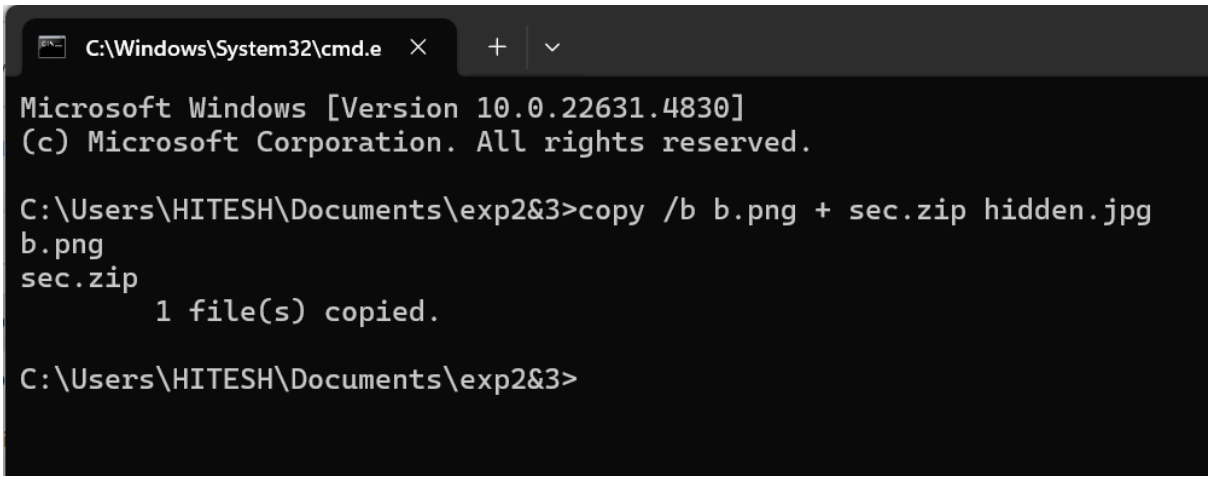
Aim: To Hide a ZIP File Inside an Image.

SOFTWARE USED: CMD prompt.

Procedure:

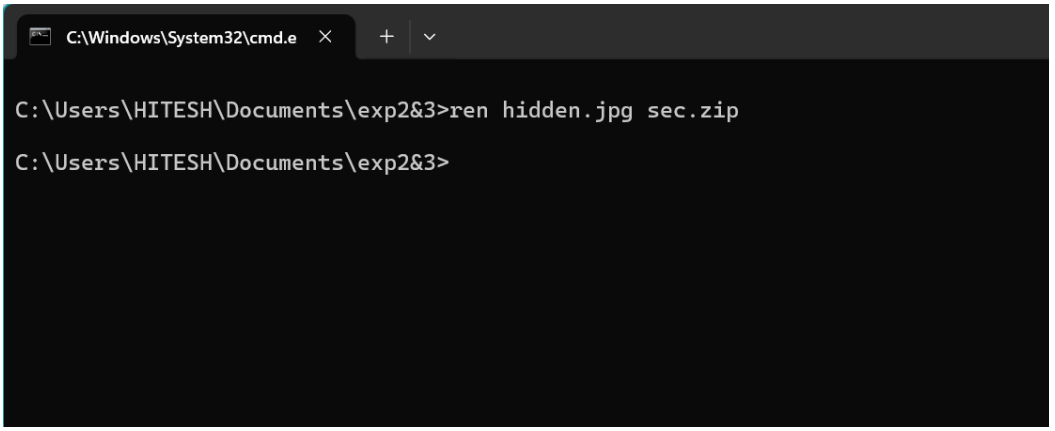
1. Place the image file (cover.jpg) and ZIP file (secret.zip) in the same folder.
2. Open cmd inside the folder.
3. Run the following cmd

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



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



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

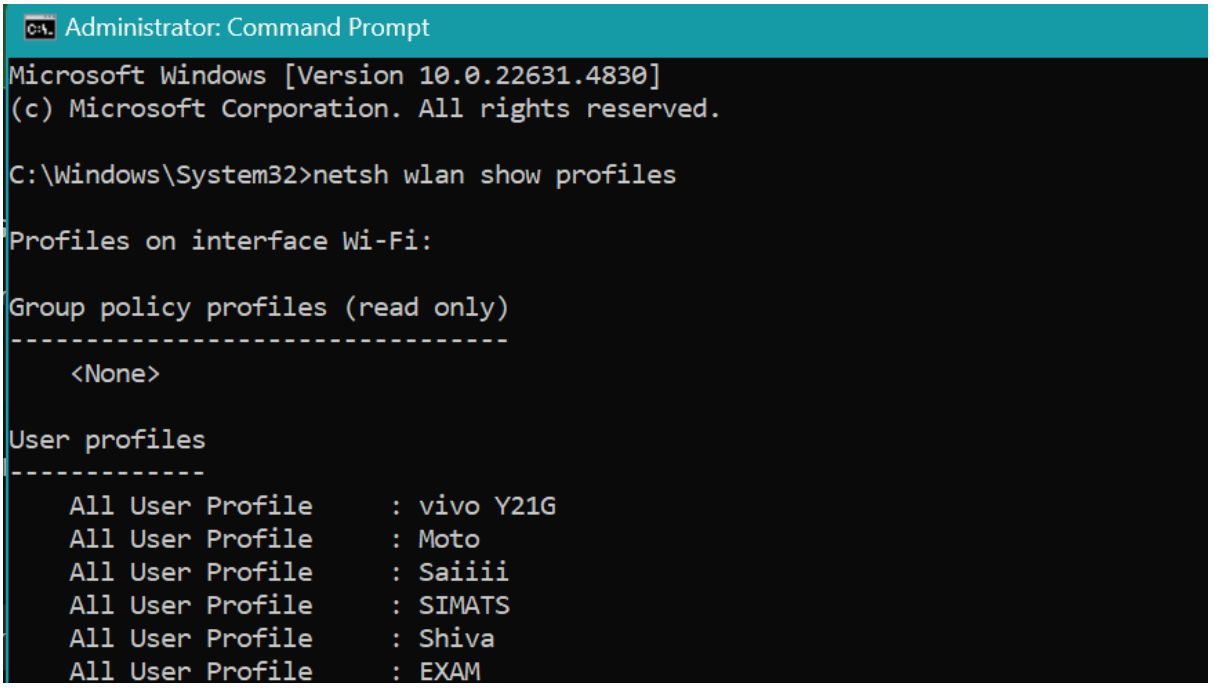
Aim: To View All Wi-Fi Passwords Saved on the Computer.

SOFTWARE USED: CMD prompt.

Procedure:

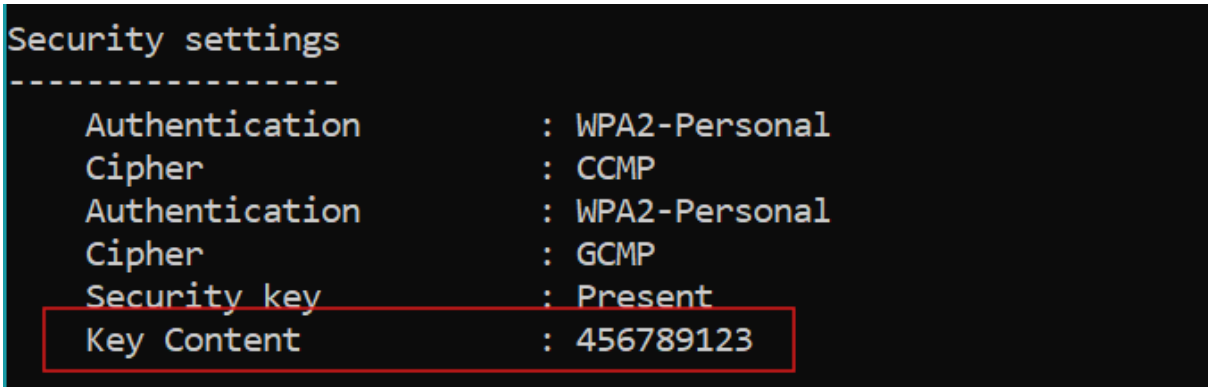
1. Open Command prompt as administrator
2. Run below command to see all saved Wi-Fi networks

```
netsh wlan show profiles
```



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

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



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

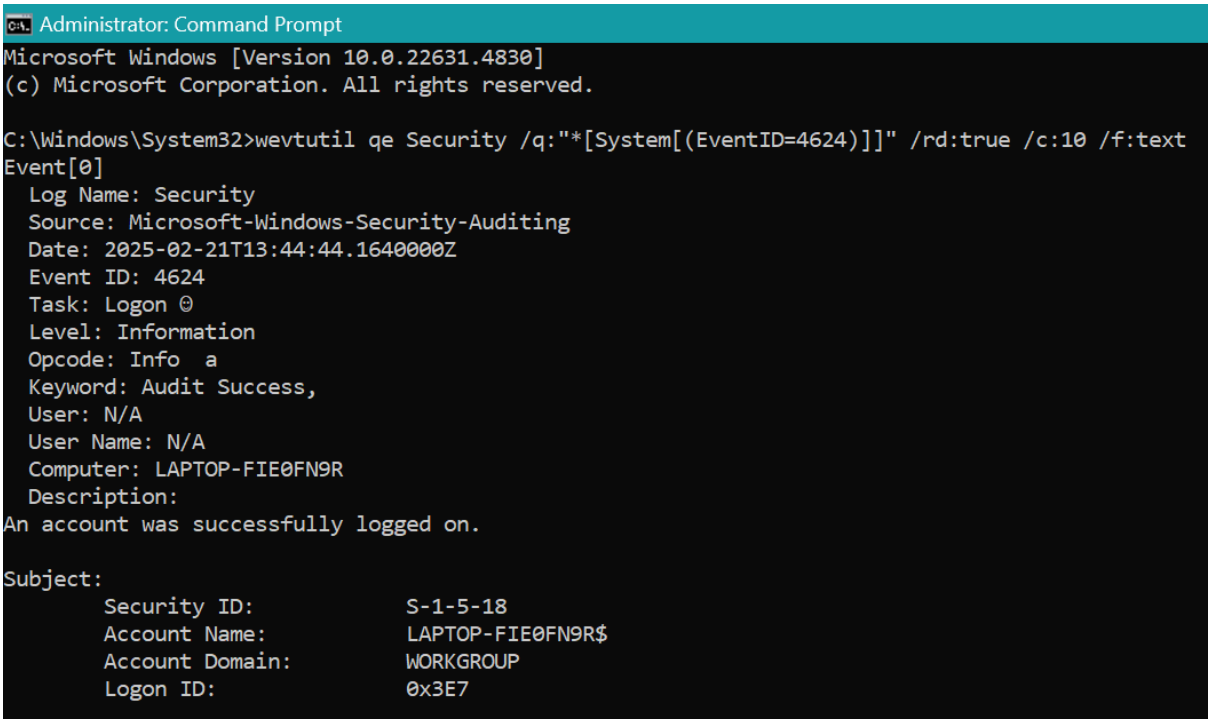
Aim: To extract the recent login and logout

SOFTWARE USED: CMD prompt.

Procedure:

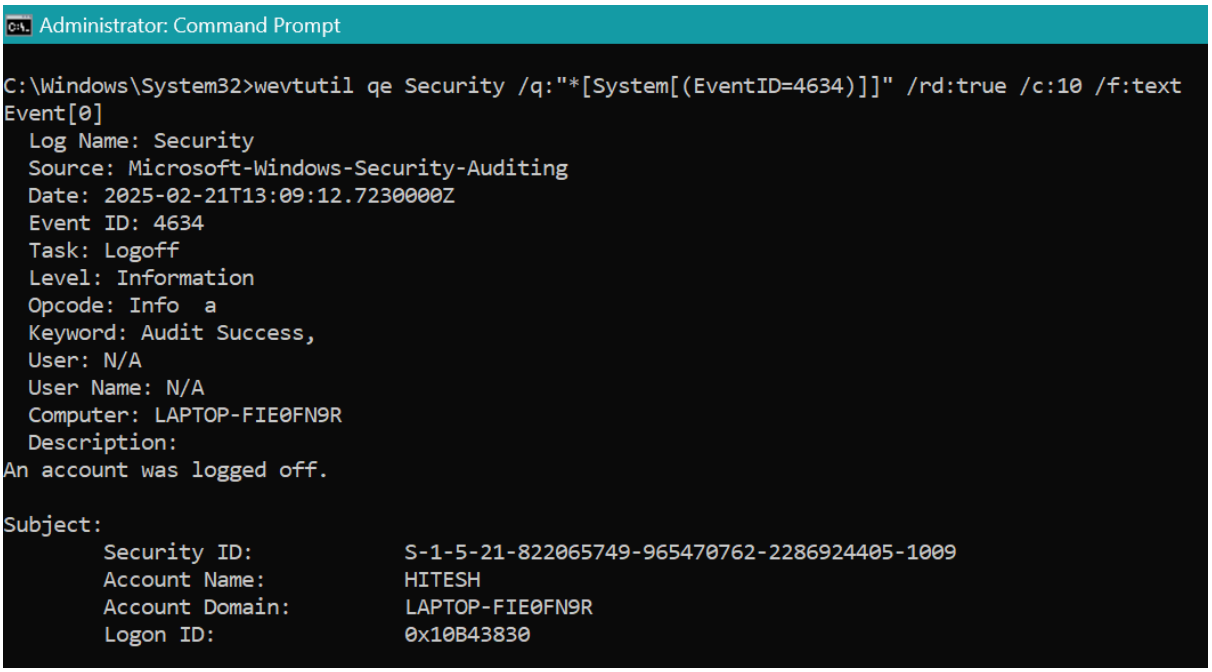
5. Open Command prompt as administrator
6. Run below command to see to recent logins

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



7. Run below command to see to recent logout

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



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

Result:

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