

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](#)

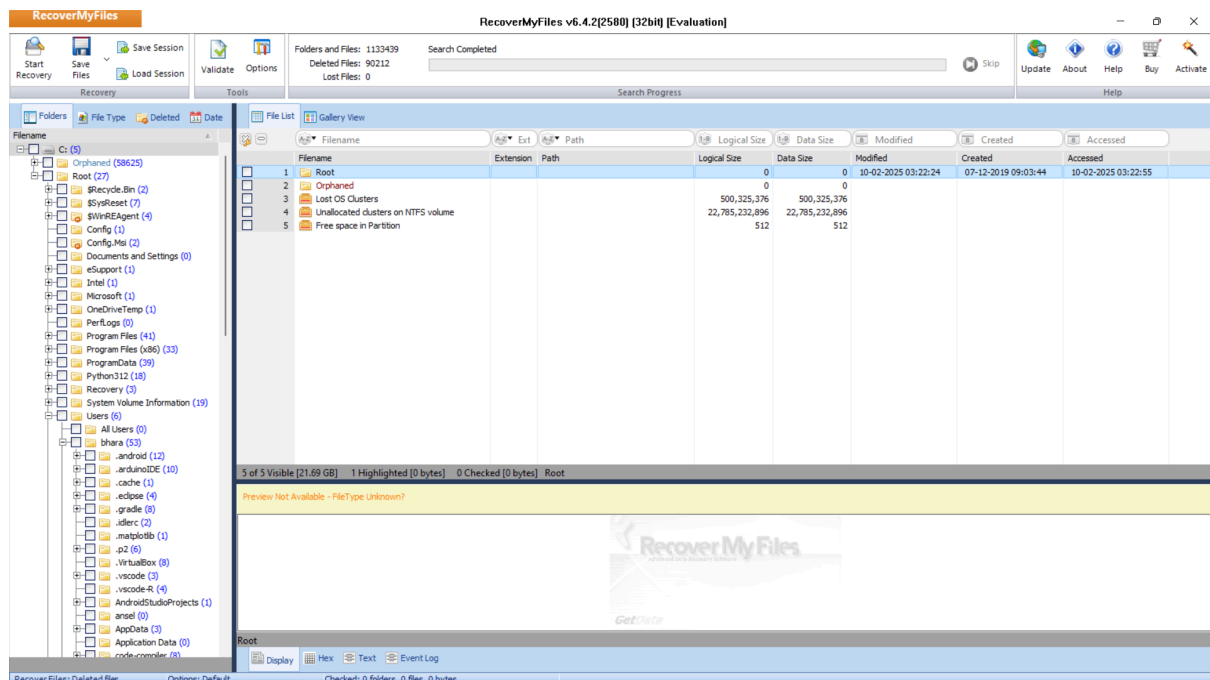
Step 2: Setup from the exe file downloaded

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:\Windows\System32\cmd.e  X  +  v
Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bhara\Downloads\Demo folder>copy /b B.jpg + A.txt C.jpg
B.jpg
A.txt
    1 file(s) copied.

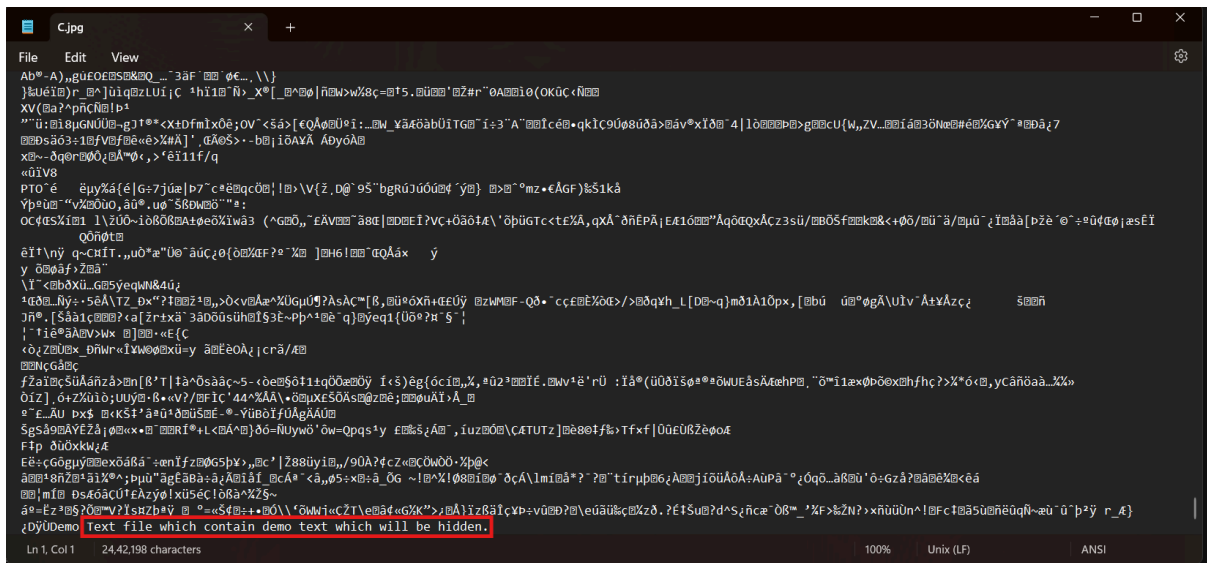
C:\Users\bhara\Downloads\Demo folder>|
```

"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?

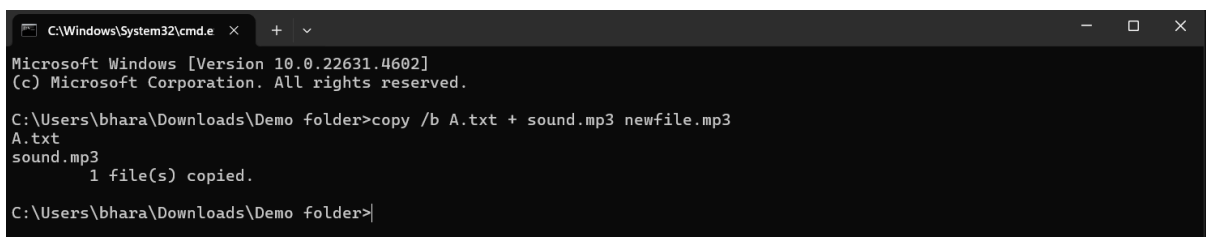
Suppose you have to hide a text file “A.txt” with the image file “sound.mp3” and combine them in a new file as “newfile.mp3”. Where “newfile.mp3” is our output file which contains the text hidden in the image file.

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*

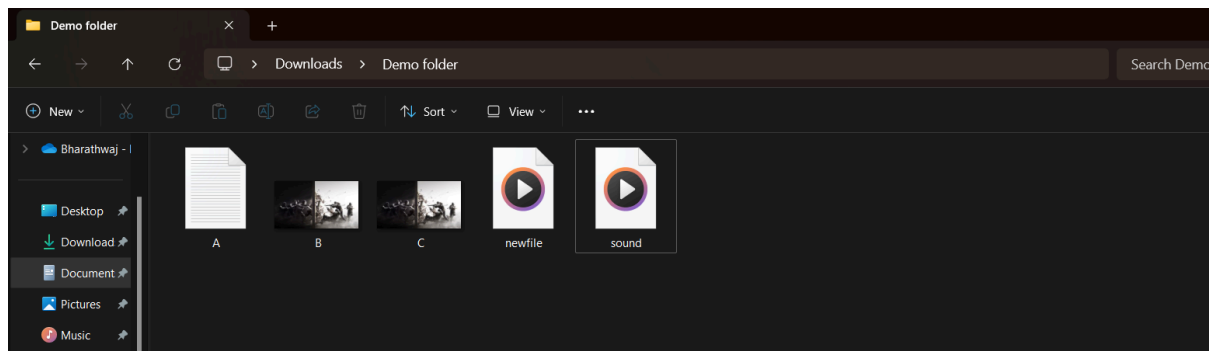


```
C:\Windows\System32\cmd.e  x  +  v
Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bhara\Downloads\Demo folder>copy /b A.txt + sound.mp3 newfile.mp3
A.txt
sound.mp3
1 file(s) copied.

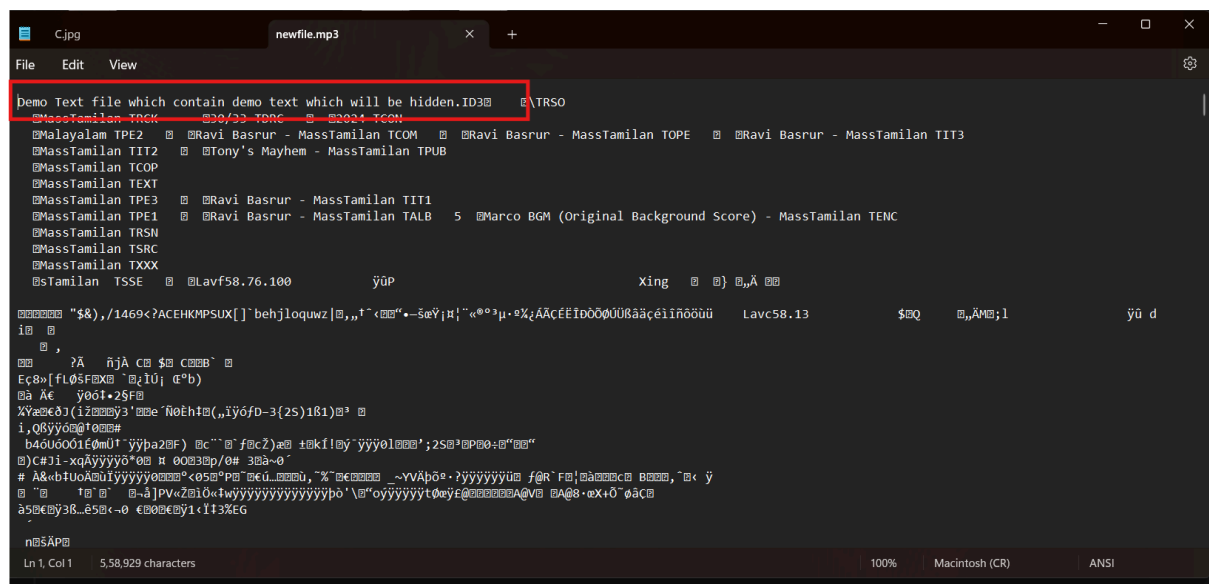
C:\Users\bhara\Downloads\Demo folder>|
```

"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](https://www.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:

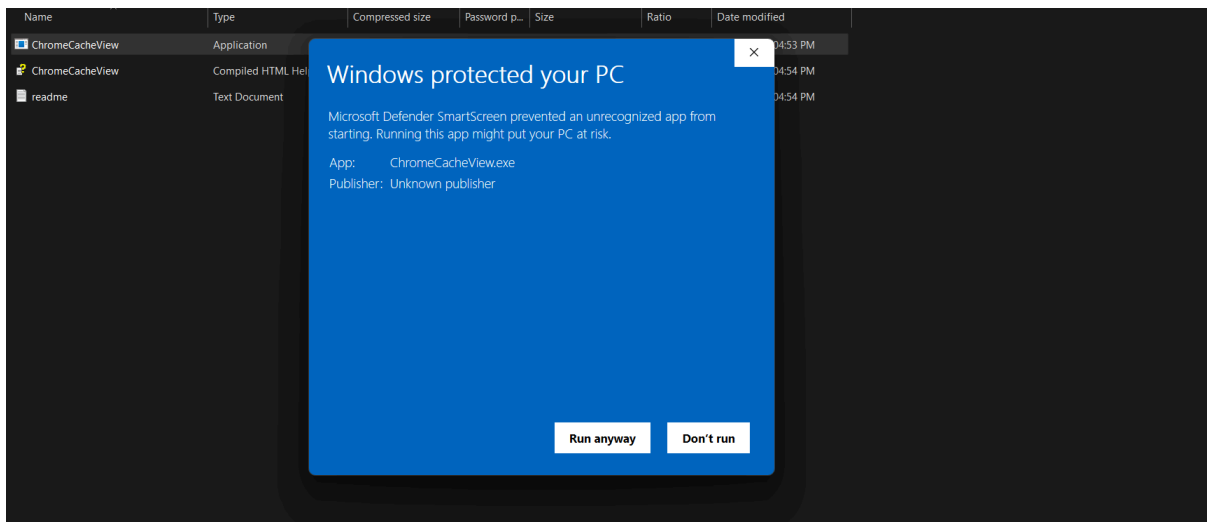
Step 1: Download Browsing History View tool

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.

BrowsingHistoryView								
File Edit View Options Help								
URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile
file:///C:/Users/HITESH...		2/20/2025 10:17:44 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/16/2025 7:34:31 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/13/2025 8:07:39 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/13/2025 8:11:10 AM	2				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/13/2025 10:04:18 AM	2				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/13/2025 10:04:27 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/13/2025 10:05:29 AM	5				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/20/2025 8:57:44 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/20/2025 8:04:04 AM	3				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/20/2025 8:59:08 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/19/2025 9:10:53 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/19/2025 11:41:31 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/21/2025 1:51:03 PM	3				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 8:09:37 AM	2				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 7:58:56 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/21/2025 1:14:10 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 7:38:11 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH... Energy Usage Tracking an...		2/19/2025 10:56:17 AM	1		Link		Chrome	HITESH
file:///C:/Users/HITESH... Energy Usage Tracking an...		2/19/2025 10:58:16 AM	1			00:02:40.926	Edge (Chromium-based)	HITESH
file:///C:/Users/HITESH...		2/19/2025 10:59:37 AM	2				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/19/2025 10:57:50 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/19/2025 11:42:07 AM	2				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/21/2025 1:10:32 PM	3				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 7:47:53 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 8:20:06 AM	2				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/19/2025 11:36:47 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/19/2025 11:38:43 AM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/21/2025 1:41:45 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 7:37:43 PM	1				Internet Explorer 10/11 / ...	HITESH
file:///C:/Users/HITESH...		2/17/2025 7:40:03 PM	1				Internet Explorer 10/11 / ...	HITESH

1180 item(s)

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.

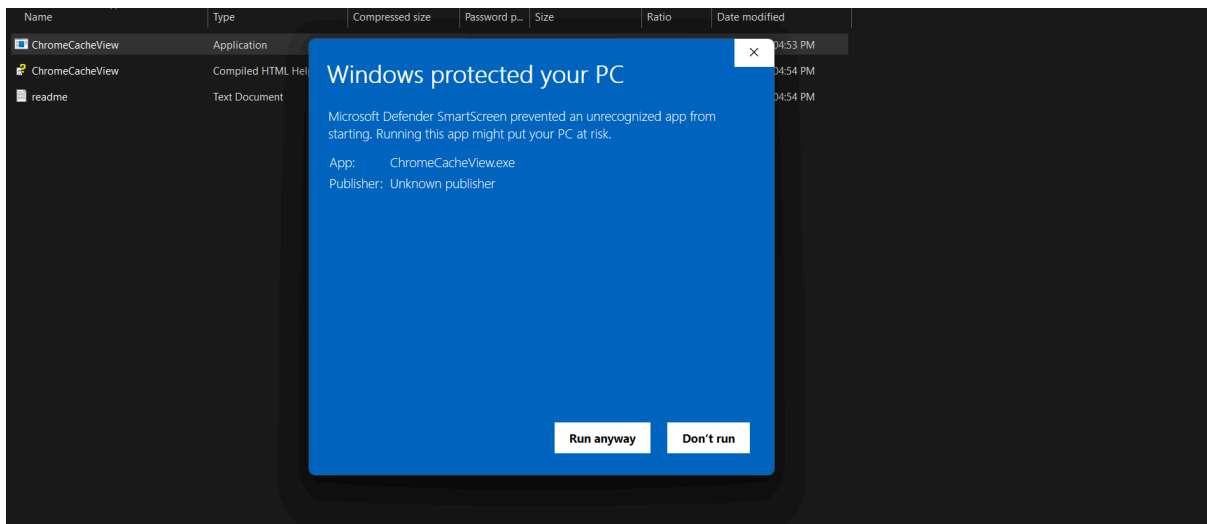
Procedure:

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



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\bhara\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	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.hackerczrl.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://hackerczrl.in	
	https://dsun-sec-casalemedia.com/trum?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.co	
	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://dsun-sec-casalemedia.com/trum?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.co	
	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	
11m181m121m...	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/PUIID.000340017075A9...		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%22id%22...	https://teams.microsoft.com/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	
%78%22x-siq-so...	https://in2-files.xohopublic.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	
-fwbane	https://www.linuxmint.com/web/wizoo/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-bhybp.yahoo.com/sync/open/1ee2H4a1-5d6d-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://d3njcbbhbjbot.cloudfront.net/webapps/r2-builds/br/f/...		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 15:48:29	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.

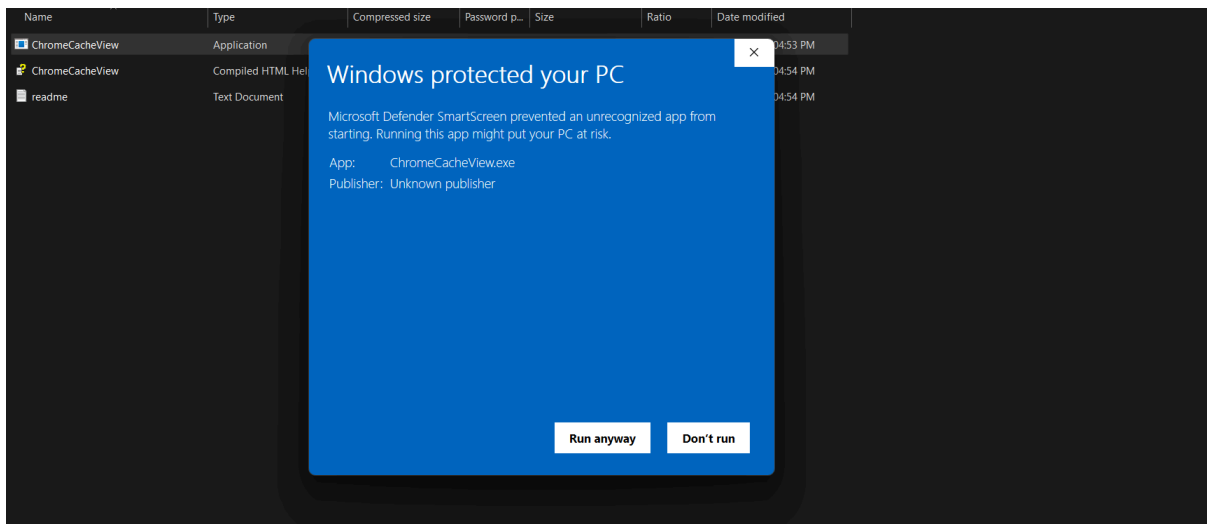
Procedure:

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.

LastActivityView						
File Edit View Options Help						
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-37D25F98.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	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.pf
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

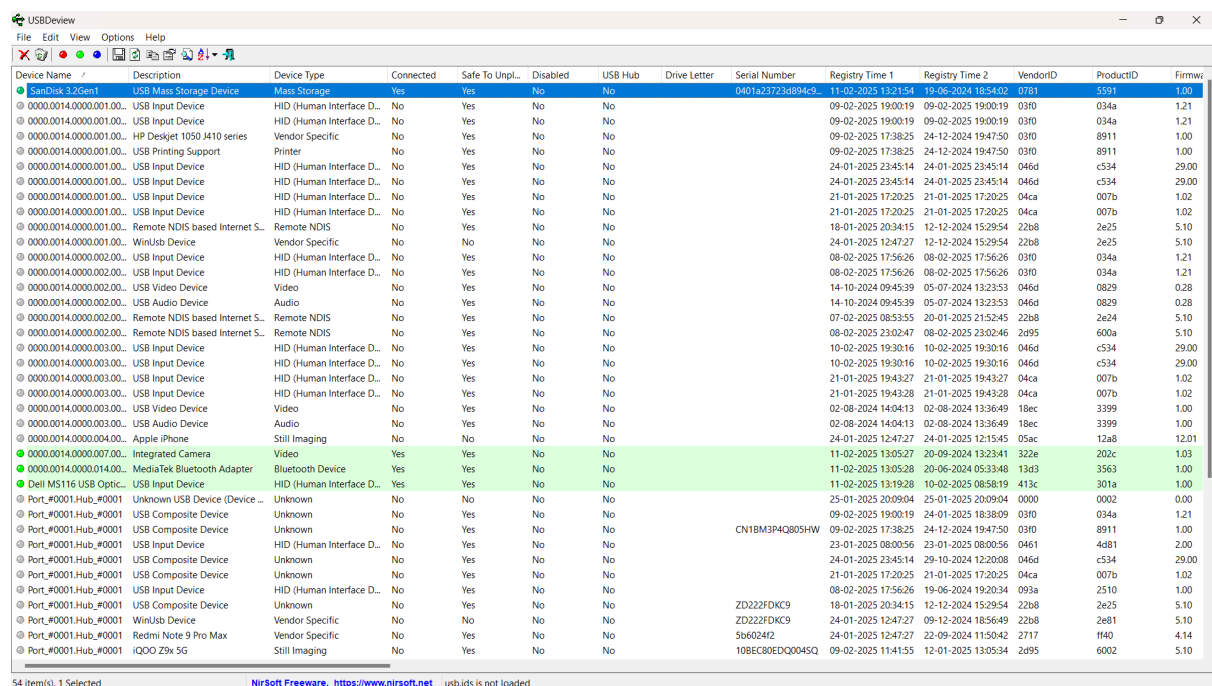
URL: [USBDeview download | SourceForge.net](#)

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
SanDisk 3.2Gbit/s	USB Mass Storage Device	Mass Storage	Yes	Yes	No	No		0401a23723d894c3	11-02-2025 13:21:54	13-09-2024 10:54:02	0381	5591	1.09
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			09-02-2025 19:00:19	09-02-2025 19:00:19	0380	034a	1.21
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			09-02-2025 19:00:19	09-02-2025 19:00:19	0380	034a	1.21
0000.0014.0000.001.00...	HP Deskjet 1050 J410 series	Vendor Specific	No	Yes	No	No			09-02-2025 17:38:25	24-12-2024 19:47:50	0380	8911	1.00
0000.0014.0000.001.00...	USB Printing Support	Printer	No	Yes	No	No			09-02-2025 17:38:25	24-12-2024 19:47:50	0380	8911	1.00
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			24-01-2025 23:45:14	24-01-2025 23:45:14	046d	c534	29.00
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			24-01-2025 23:45:14	24-01-2025 23:45:14	046d	c534	29.00
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			21-01-2025 17:20:25	21-01-2025 17:20:25	04ca	007b	1.02
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			21-01-2025 17:20:25	21-01-2025 17:20:25	04ca	007b	1.02
0000.0014.0000.001.00...	Remote NDIS based Internet S...	Remote NDIS	No	Yes	No	No			18-01-2025 20:34:15	12-12-2024 15:29:54	22b8	2e25	5.10
0000.0014.0000.001.00...	WinUsb Device	Vendor Specific	No	No	No	No			24-01-2025 12:47:27	12-12-2024 15:29:54	22b8	2e25	5.10
0000.0014.0000.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			08-02-2025 17:56:26	08-02-2025 17:56:26	0380	034a	1.21
0000.0014.0000.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			08-02-2025 17:56:26	08-02-2025 17:56:26	0380	034a	1.21
0000.0014.0000.002.00...	USB Video Device	Video	No	Yes	No	No			14-10-2024 09:45:39	05-07-2024 13:23:53	046d	0829	0.28
0000.0014.0000.002.00...	USB Audio Device	Audio	No	Yes	No	No			14-10-2024 09:45:39	05-07-2024 13:23:53	046d	0829	0.28
0000.0014.0000.002.00...	Remote NDIS based Internet S...	Remote NDIS	No	Yes	No	No			07-02-2025 08:53:55	20-01-2025 21:52:45	22b8	2e24	5.10
0000.0014.0000.002.00...	Remote NDIS based Internet S...	Remote NDIS	No	Yes	No	No			08-02-2025 23:02:47	08-02-2025 23:02:46	2995	600a	5.10
0000.0014.0000.003.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			10-02-2025 19:30:16	10-02-2025 19:30:16	046d	c534	29.00
0000.0014.0000.003.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			10-02-2025 19:30:16	10-02-2025 19:30:16	046d	c534	29.00
0000.0014.0000.003.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			21-01-2025 19:43:27	21-01-2025 19:43:27	04ca	007b	1.02
0000.0014.0000.003.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			21-01-2025 19:43:28	21-01-2025 19:43:28	04ca	007b	1.02
0000.0014.0000.003.00...	USB Video Device	Video	No	Yes	No	No			02-08-2024 14:04:13	02-08-2024 13:36:49	18ec	3399	1.00
0000.0014.0000.003.00...	USB Audio Device	Audio	No	Yes	No	No			02-08-2024 14:04:13	02-08-2024 13:36:49	18ec	3399	1.00
0000.0014.0000.004.00...	Apple iPhone	Still Imaging	No	No	No	No			24-01-2025 12:47:27	24-01-2025 12:15:45	05ac	12a8	12.01
0000.0014.0000.007.00...	Integrated Camera	Video	Yes	Yes	No	No			11-02-2025 13:05:27	20-09-2024 13:23:41	322e	202c	1.03
0000.0014.0000.014.00...	MediaTek Bluetooth Adapter	Bluetooth Device	Yes	Yes	No	No			11-02-2025 13:05:28	20-06-2024 05:33:48	13d3	3563	1.00
Dell M5116 USB Optic...	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			11-02-2025 13:19:28	10-02-2025 08:58:19	413c	301a	1.00
Port_#0001.Hub_#0001	Unknown USB Device (Device...	Unknown	No	No	No	No			25-01-2025 20:09:04	25-01-2025 20:09:04	0000	0002	0.00
Port_#0001.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No			09-02-2025 19:00:19	24-01-2025 18:38:09	0380	034a	1.21
Port_#0001.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No		CN18M3P4Q805HW	09-02-2025 17:38:25	24-12-2024 19:47:50	0380	8911	1.00
Port_#0001.Hub_#0001	USB Input Device	HID (Human Interface D...	No	Yes	No	No			23-01-2025 08:00:56	23-01-2025 08:00:56	0461	4d81	2.00
Port_#0001.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No			24-01-2025 23:45:14	29-10-2024 12:20:08	046d	c534	29.00
Port_#0001.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No			21-01-2025 17:20:25	21-01-2025 17:20:25	04ca	007b	1.02
Port_#0001.Hub_#0001	USB Input Device	HID (Human Interface D...	No	Yes	No	No			08-02-2025 17:56:26	19-06-2024 19:20:34	093a	2510	1.00
Port_#0001.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No		ZD222FDWC9	18-01-2025 20:34:15	12-12-2024 15:29:54	22b8	2e25	5.10
Port_#0001.Hub_#0001	WinUsb Device	Vendor Specific	No	No	No	No		ZD222FDWC9	24-01-2025 12:47:27	09-12-2024 18:56:49	22b8	2e81	5.10
Port_#0001.Hub_#0001	Redmi Note 9 Pro Max	Vendor Specific	No	Yes	No	No		5a6034f2	24-01-2025 12:47:27	22-09-2024 11:50:42	2717	ff40	4.14
Port_#0001.Hub_#0001	IQOO Z9x 5G	Still Imaging	No	Yes	No	No		108EC80EDQ0045Q	09-02-2025 11:41:55	12-01-2025 13:05:34	2d95	6002	5.10

Result:

The experiment has been successfully executed

EXPERIMENT 9

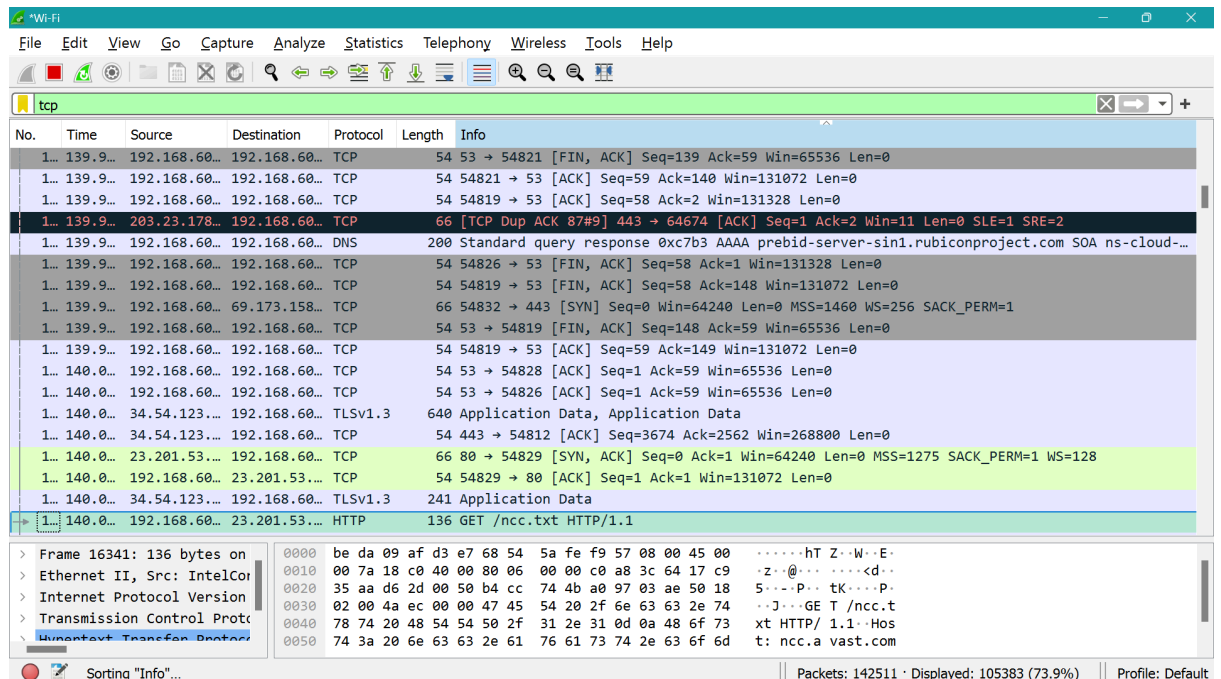
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-TCP

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

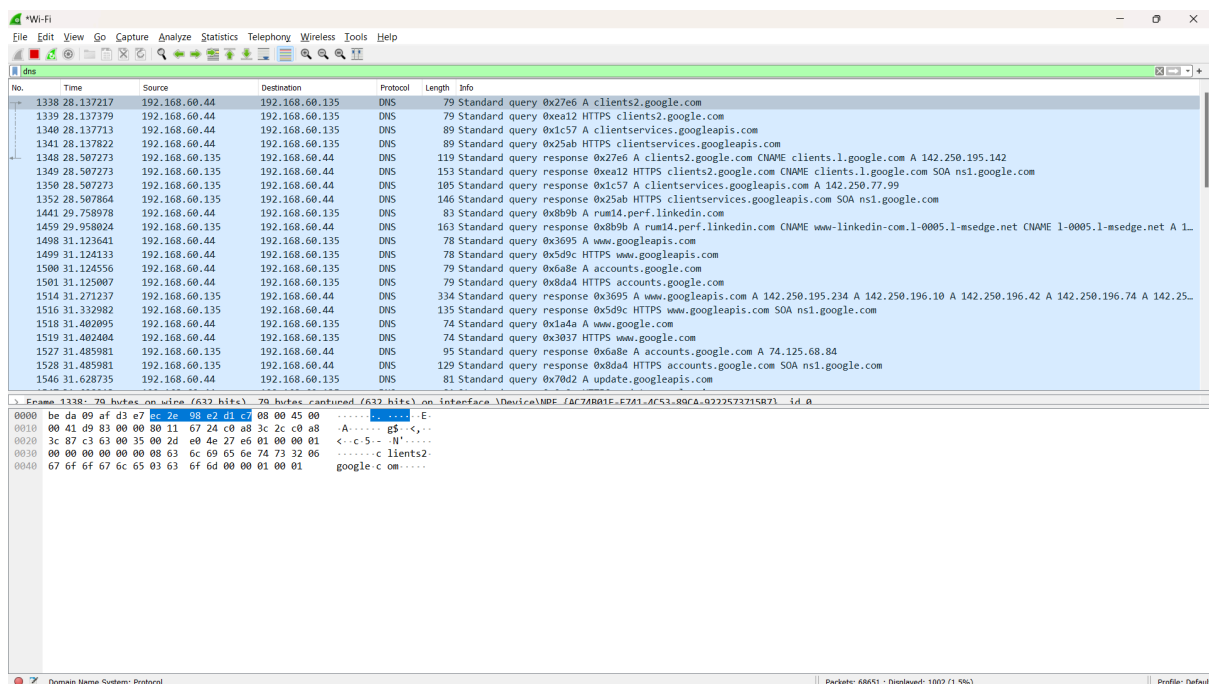
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-DNS

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

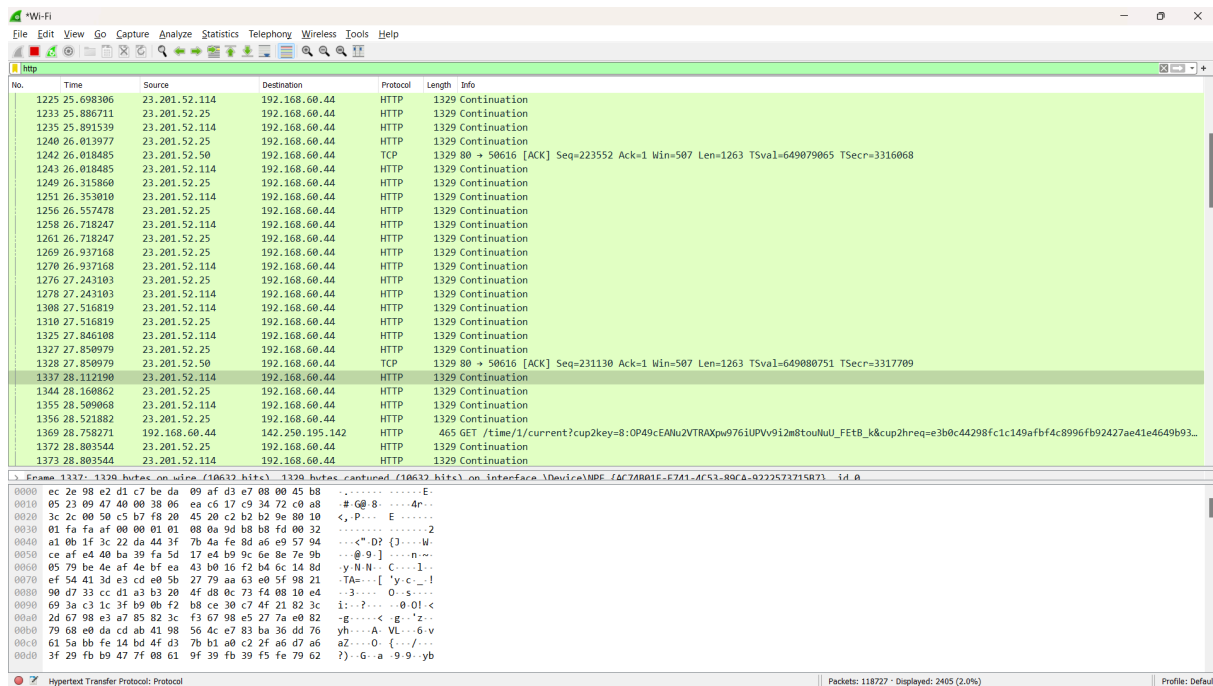
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-HTTP

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

```
C:\Windows\System32>tasklist
```

Image Name	PID	Session	Name	Session#	Mem Usage
System Idle Process	0	Services		0	8 K
System	4	Services		0	8,072 K
Registry	124	Services		0	59,284 K

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

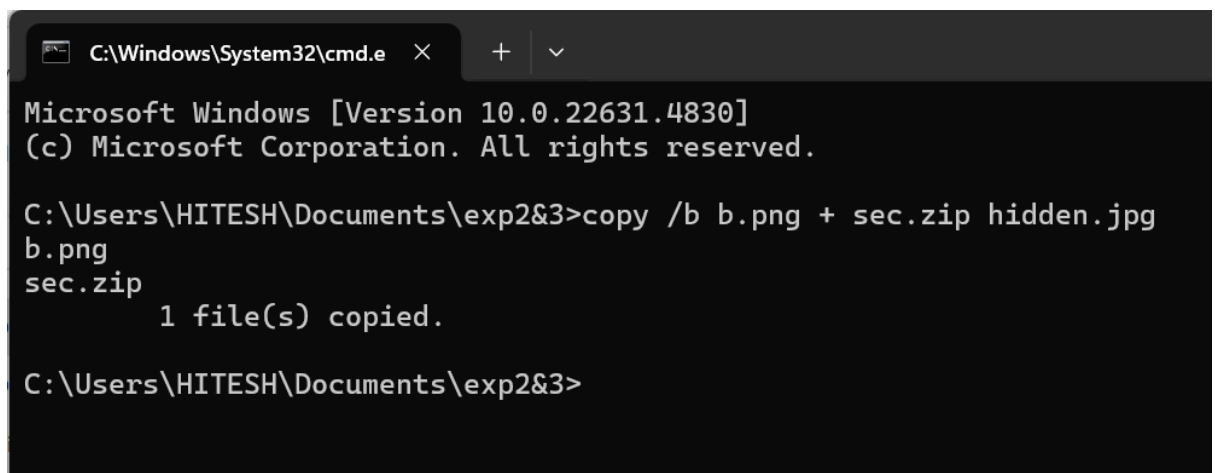
Aim: To Hide a ZIP File Inside an Image.

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



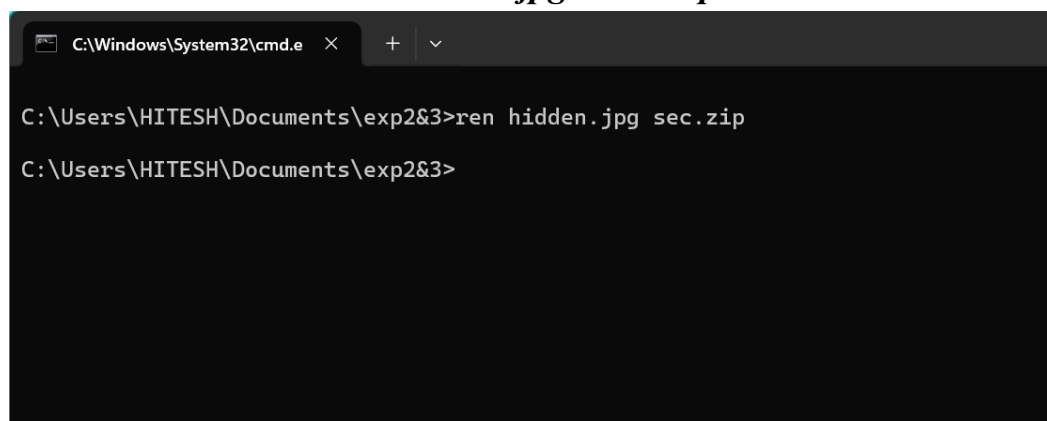
```
C:\Windows\System32\cmd.e  X  +  v
Microsoft Windows [Version 10.0.22631.4830]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HITESH\Documents\exp2&3>copy /b b.png + sec.zip hidden.jpg
b.png
sec.zip
        1 file(s) copied.

C:\Users\HITESH\Documents\exp2&3>
```

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:\Windows\System32\cmd.e  X  +  v

C:\Users\HITESH\Documents\exp2&3>ren hidden.jpg sec.zip

C:\Users\HITESH\Documents\exp2&3>
```

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

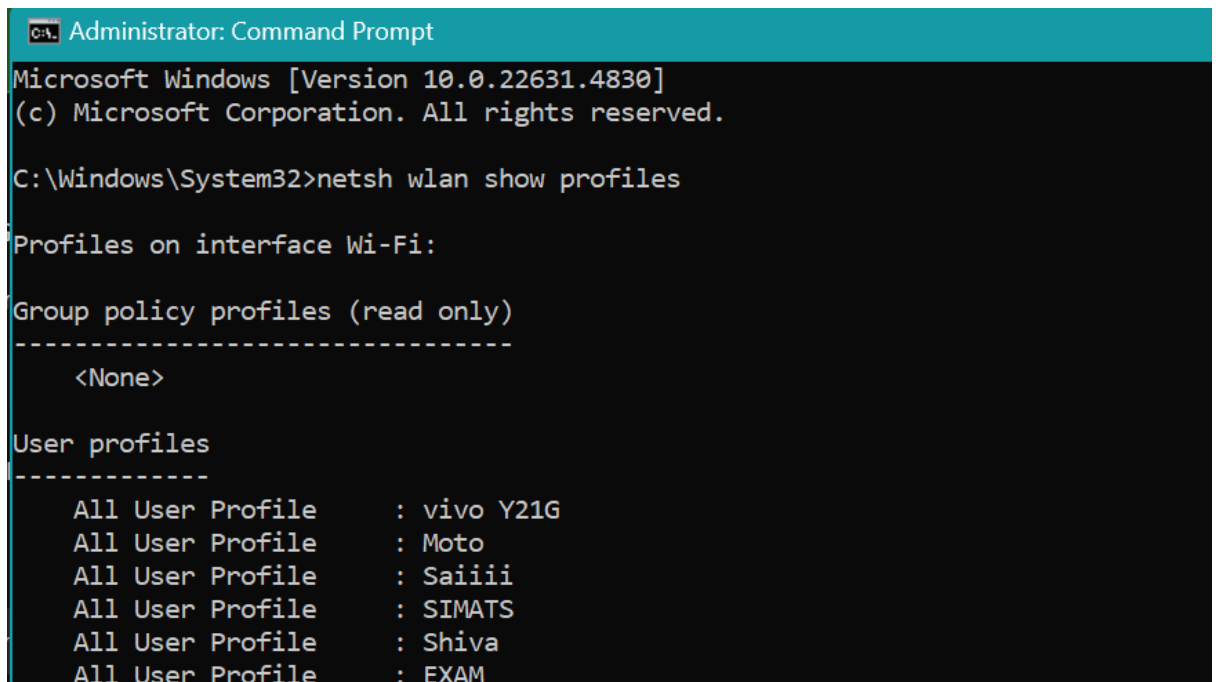
Aim: To View All Wi-Fi Passwords Saved on the Computer.

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:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.4830]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
-----
    <None>

User profiles
-----
    All User Profile      : vivo Y21G
    All User Profile      : Moto
    All User Profile      : Saiiii
    All User Profile      : SIMATS
    All User Profile      : Shiva
    All User Profile      : EXAM
```

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

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

Security settings

Authentication	: WPA2-Personal
Cipher	: CCMP
Authentication	: WPA2-Personal
Cipher	: GCMP
Security key	: Present
Key Content	: 456789123

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

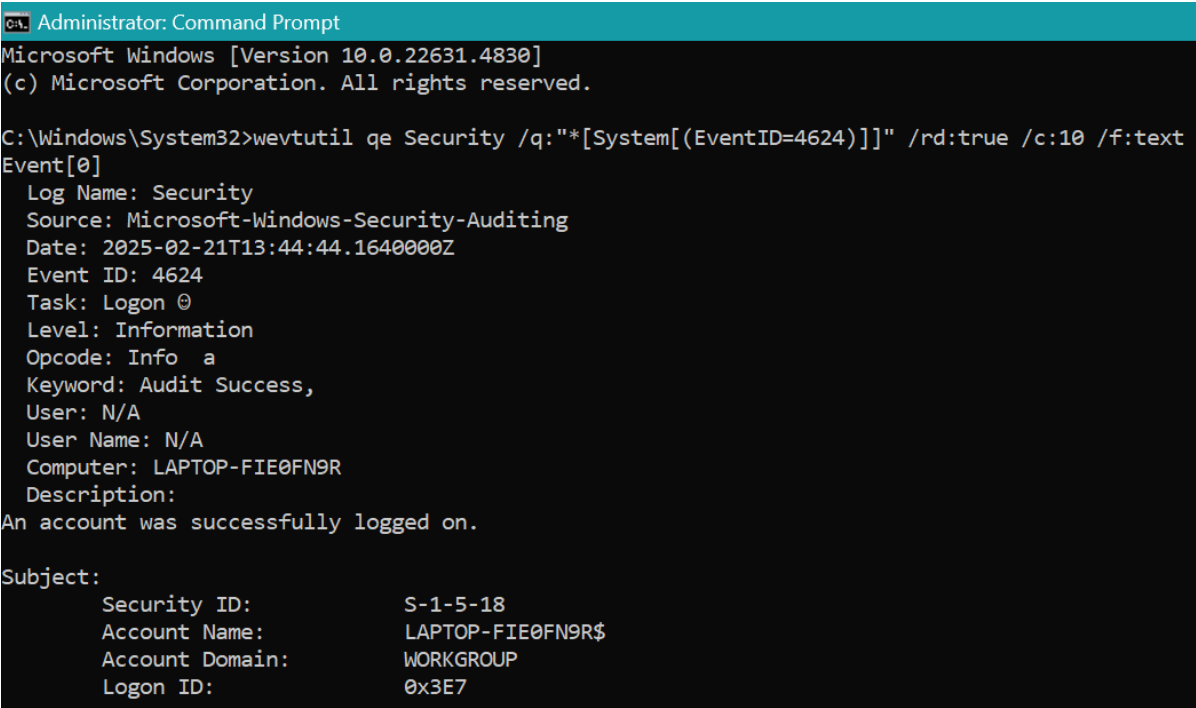
Aim: To extract the recent login and logout

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
```



```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.22631.4830]  
(c) Microsoft Corporation. All rights reserved.  
  
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: 2025-02-21T13:44:44.1640000Z  
  Event ID: 4624  
  Task: Logon 0  
  Level: Information  
  Opcode: Info  a  
  Keyword: Audit Success,  
  User: N/A  
  User Name: N/A  
  Computer: LAPTOP-FIE0FN9R  
  Description:  
An account was successfully logged on.  
  
Subject:  
  Security ID:          S-1-5-18  
  Account Name:         LAPTOP-FIE0FN9R$  
  Account Domain:      WORKGROUP  
  Logon ID:             0x3E7
```

7. Run below command to see to recent logout

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

```
Administrator: Command Prompt
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: 2025-02-21T13:09:12.7230000Z
  Event ID: 4634
  Task: Logoff
  Level: Information
  Opcode: Info a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
  Computer: LAPTOP-FIE0FN9R
  Description:
An account was logged off.

Subject:
  Security ID: S-1-5-21-822065749-965470762-2286924405-1009
  Account Name: HITESH
  Account Domain: LAPTOP-FIE0FN9R
  Logon ID: 0x10B43830
```

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

Result:

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