CSA5207-CYBER FORENSICS

NAME:Eturi Hemasree

REG NO:192125021

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

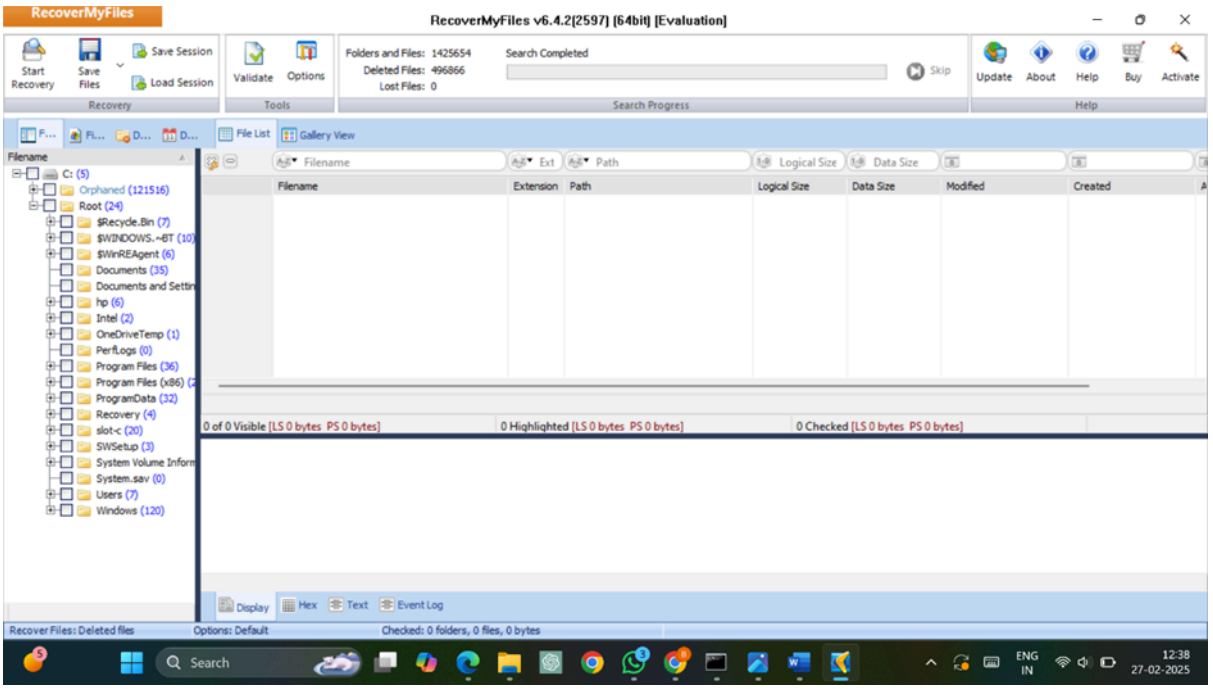
Step 2: Setup from the exe file downloaded

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)



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?

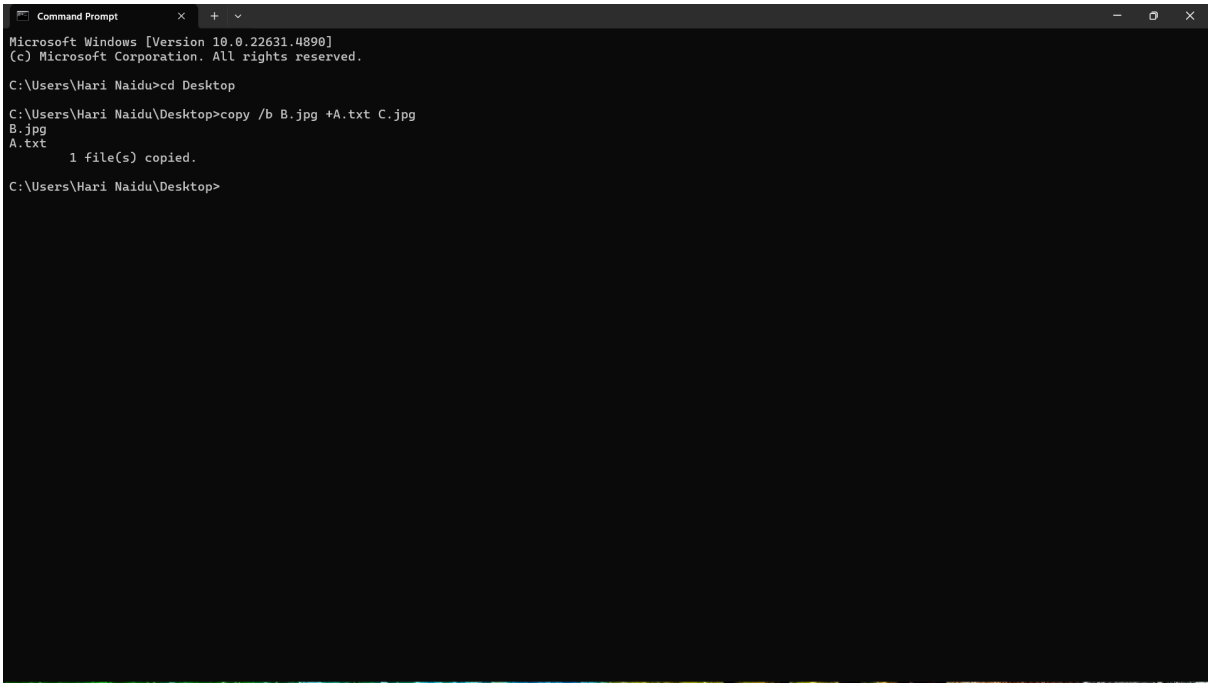
Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”. Where “C.jpg” is our output file which contains the text hidden in the image file.

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

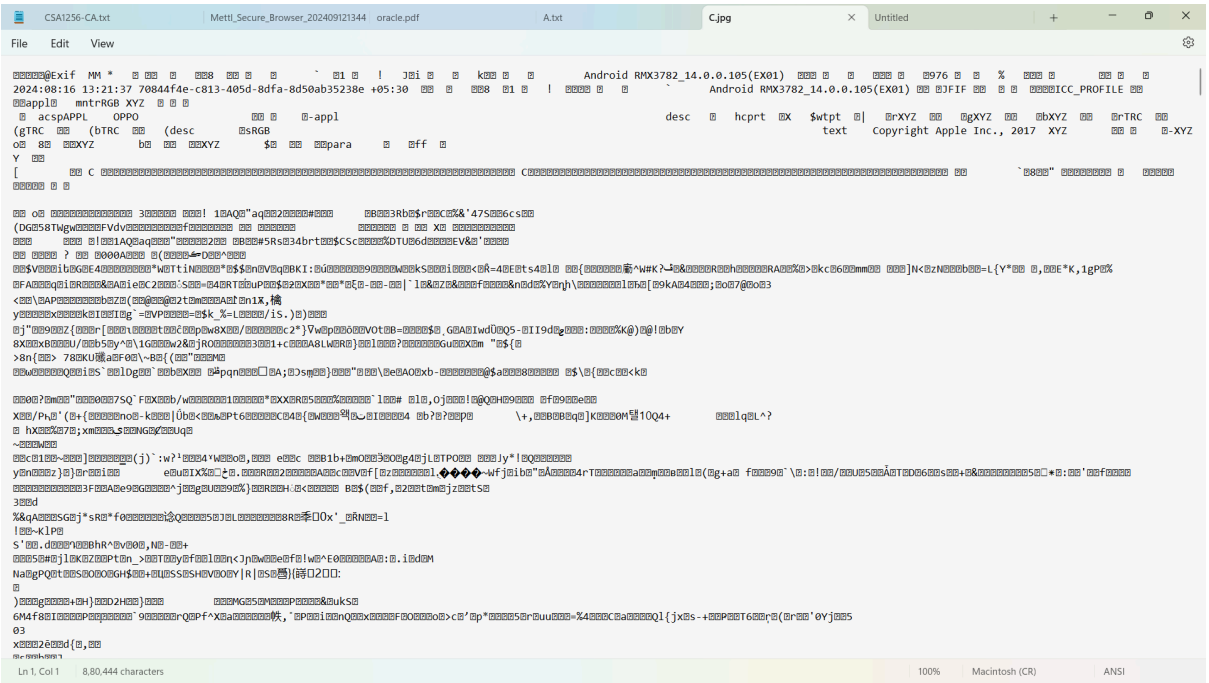
Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial- image.jpg Resulting-image-name.jpg*



"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?

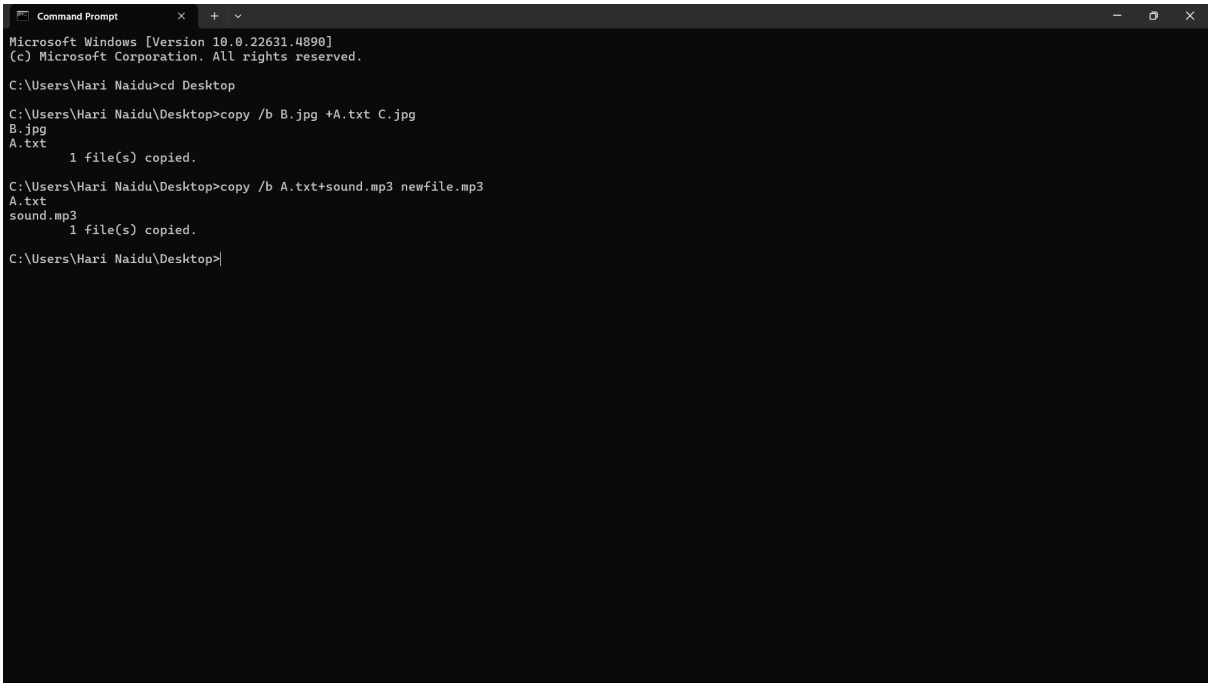
Suppose you have to hide a text file “A.txt” with the image file “sound.mp3” and combine them in a new file as “newfile.mp3”. Where “newfile.mp3” is our output file which contains the text hidden in the image file.

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

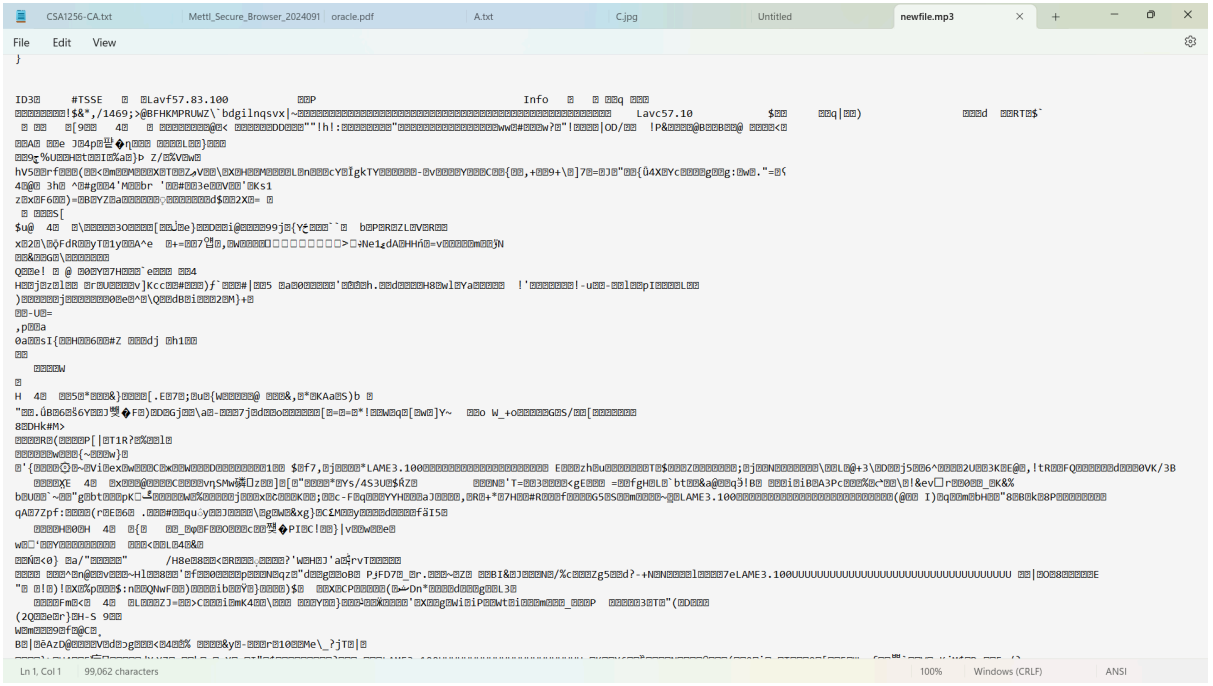
Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial- audio.mp3 Resulting-audio-name.mp3*



"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.

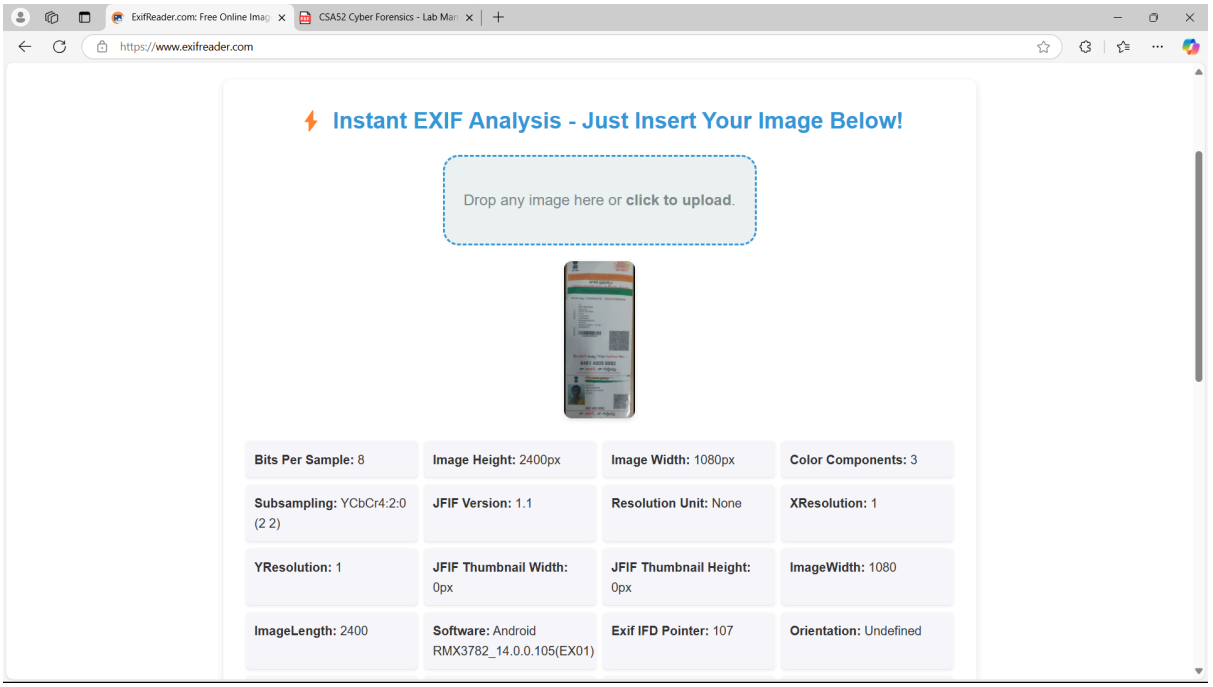
Procedure:

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

Step 2: Find an Appropriate image

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.

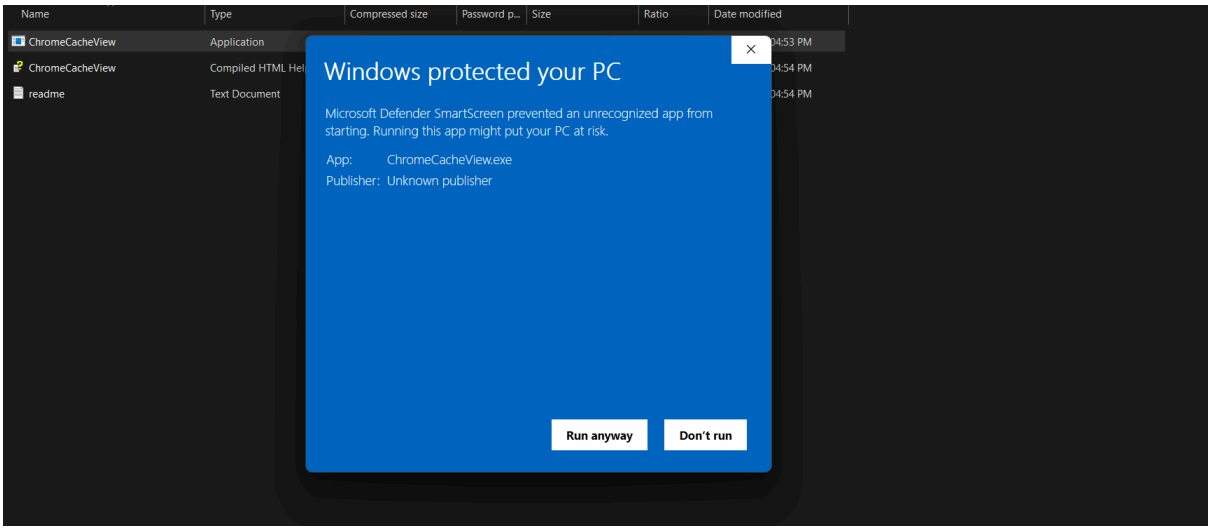
Procedure:

Step 1: Download Browsing History View tool
URL:

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

Step 2: Setup from the exe file downloaded

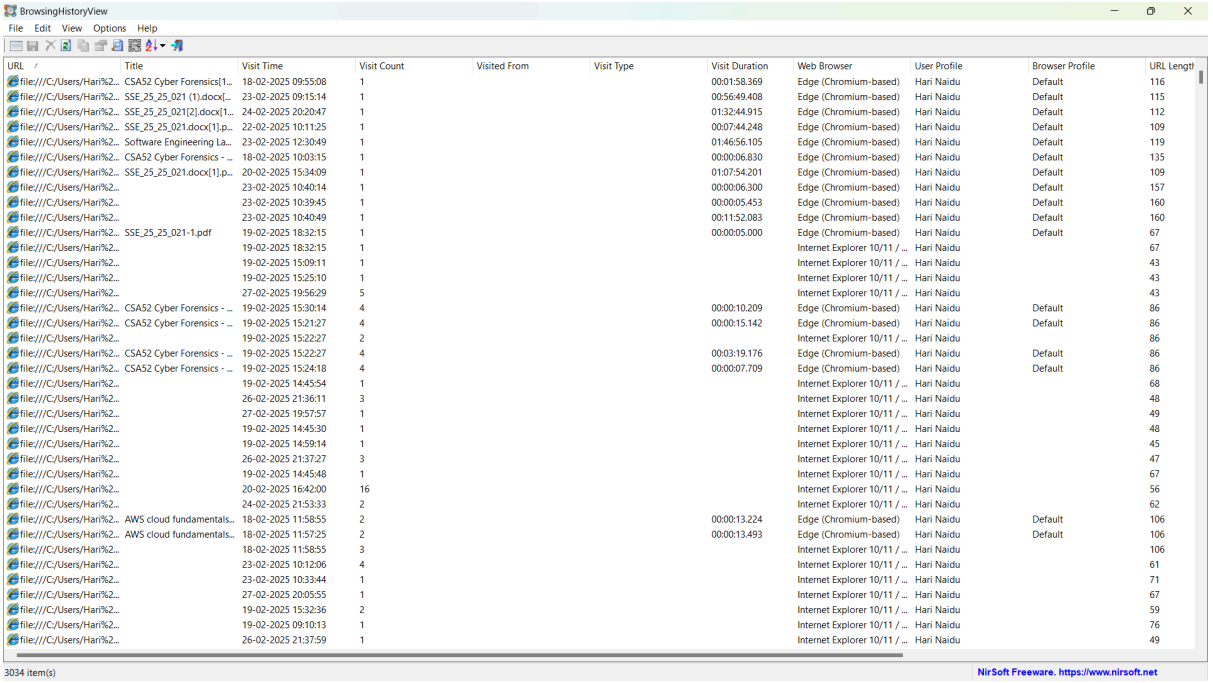
Step 3: Click run anyway when the below dialog box appears



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	Browser Profile	URL Length
file:///C:/Users/Hari%2...	CSA52 Cyber Forensics[1...	18-02-2025 09:55:08	1			00:01:58.369	Edge (Chromium-based)	Hari Naidu	Default	116
file:///C:/Users/Hari%2...	SSE_25_25_021 (1).docx[...	23-02-2025 09:15:14	1			00:56:49.408	Edge (Chromium-based)	Hari Naidu	Default	115
file:///C:/Users/Hari%2...	SSE_25_25_021[2].docx[1...	24-02-2025 20:20:47	1			01:32:44.915	Edge (Chromium-based)	Hari Naidu	Default	112
file:///C:/Users/Hari%2...	SSE_25_25_021.docx[1].p...	22-02-2025 10:11:25	1			00:07:44.248	Edge (Chromium-based)	Hari Naidu	Default	109
file:///C:/Users/Hari%2...	Software Engineering La...	23-02-2025 12:30:49	1			01:46:56.105	Edge (Chromium-based)	Hari Naidu	Default	119
file:///C:/Users/Hari%2...	CSA52 Cyber Forensics - ...	18-02-2025 10:03:15	1			00:00:06.830	Edge (Chromium-based)	Hari Naidu	Default	135
file:///C:/Users/Hari%2...	SSE_25_25_021.docx[1].p...	20-02-2025 15:34:09	1			01:07:54.201	Edge (Chromium-based)	Hari Naidu	Default	109
file:///C:/Users/Hari%2...		23-02-2025 10:40:14	1			00:00:06.300	Edge (Chromium-based)	Hari Naidu	Default	157
file:///C:/Users/Hari%2...		23-02-2025 10:39:45	1			00:00:05.453	Edge (Chromium-based)	Hari Naidu	Default	160
file:///C:/Users/Hari%2...		23-02-2025 10:40:49	1			00:11:52.083	Edge (Chromium-based)	Hari Naidu	Default	160
file:///C:/Users/Hari%2...	SSE_25_25_021-1.pdf	19-02-2025 18:32:15	1			00:00:05.000	Edge (Chromium-based)	Hari Naidu	Default	67
file:///C:/Users/Hari%2...		19-02-2025 18:32:15	1				Internet Explorer 10/11 / ...	Hari Naidu		67
file:///C:/Users/Hari%2...		19-02-2025 15:09:11	1				Internet Explorer 10/11 / ...	Hari Naidu		43
file:///C:/Users/Hari%2...		19-02-2025 15:25:10	1				Internet Explorer 10/11 / ...	Hari Naidu		43
file:///C:/Users/Hari%2...		27-02-2025 19:56:29	5				Internet Explorer 10/11 / ...	Hari Naidu		43
file:///C:/Users/Hari%2...	CSA52 Cyber Forensics - ...	19-02-2025 15:30:14	4			00:00:10.209	Edge (Chromium-based)	Hari Naidu	Default	86
file:///C:/Users/Hari%2...	CSA52 Cyber Forensics - ...	19-02-2025 15:21:27	4			00:00:15.142	Edge (Chromium-based)	Hari Naidu	Default	86
file:///C:/Users/Hari%2...		19-02-2025 15:22:27	2				Internet Explorer 10/11 / ...	Hari Naidu		86
file:///C:/Users/Hari%2...	CSA52 Cyber Forensics - ...	19-02-2025 15:22:27	4			00:03:19.176	Edge (Chromium-based)	Hari Naidu	Default	86
file:///C:/Users/Hari%2...	CSA52 Cyber Forensics - ...	19-02-2025 15:24:18	4			00:00:07.709	Edge (Chromium-based)	Hari Naidu	Default	86
file:///C:/Users/Hari%2...		19-02-2025 14:45:54	1				Internet Explorer 10/11 / ...	Hari Naidu		68
file:///C:/Users/Hari%2...		26-02-2025 21:36:11	3				Internet Explorer 10/11 / ...	Hari Naidu		48
file:///C:/Users/Hari%2...		27-02-2025 19:57:57	1				Internet Explorer 10/11 / ...	Hari Naidu		49
file:///C:/Users/Hari%2...		19-02-2025 14:45:30	1				Internet Explorer 10/11 / ...	Hari Naidu		48
file:///C:/Users/Hari%2...		19-02-2025 14:59:14	1				Internet Explorer 10/11 / ...	Hari Naidu		45
file:///C:/Users/Hari%2...		26-02-2025 21:37:27	3				Internet Explorer 10/11 / ...	Hari Naidu		47
file:///C:/Users/Hari%2...		19-02-2025 14:45:48	1				Internet Explorer 10/11 / ...	Hari Naidu		67
file:///C:/Users/Hari%2...		20-02-2025 16:42:00	16				Internet Explorer 10/11 / ...	Hari Naidu		56
file:///C:/Users/Hari%2...		24-02-2025 21:53:33	2				Internet Explorer 10/11 / ...	Hari Naidu		62
file:///C:/Users/Hari%2...	AWS cloud fundamentals...	18-02-2025 11:58:55	2			00:00:13.224	Edge (Chromium-based)	Hari Naidu	Default	106
file:///C:/Users/Hari%2...	AWS cloud fundamentals...	18-02-2025 11:57:25	2			00:00:13.493	Edge (Chromium-based)	Hari Naidu	Default	106
file:///C:/Users/Hari%2...		18-02-2025 11:58:55	3				Internet Explorer 10/11 / ...	Hari Naidu		106
file:///C:/Users/Hari%2...		23-02-2025 10:12:06	4				Internet Explorer 10/11 / ...	Hari Naidu		61
file:///C:/Users/Hari%2...		23-02-2025 10:33:44	1				Internet Explorer 10/11 / ...	Hari Naidu		71
file:///C:/Users/Hari%2...		27-02-2025 20:05:55	1				Internet Explorer 10/11 / ...	Hari Naidu		67
file:///C:/Users/Hari%2...		19-02-2025 15:32:36	2				Internet Explorer 10/11 / ...	Hari Naidu		59
file:///C:/Users/Hari%2...		19-02-2025 09:10:13	1				Internet Explorer 10/11 / ...	Hari Naidu		76
file:///C:/Users/Hari%2...		26-02-2025 21:37:59	1				Internet Explorer 10/11 / ...	Hari Naidu		49

3034 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:

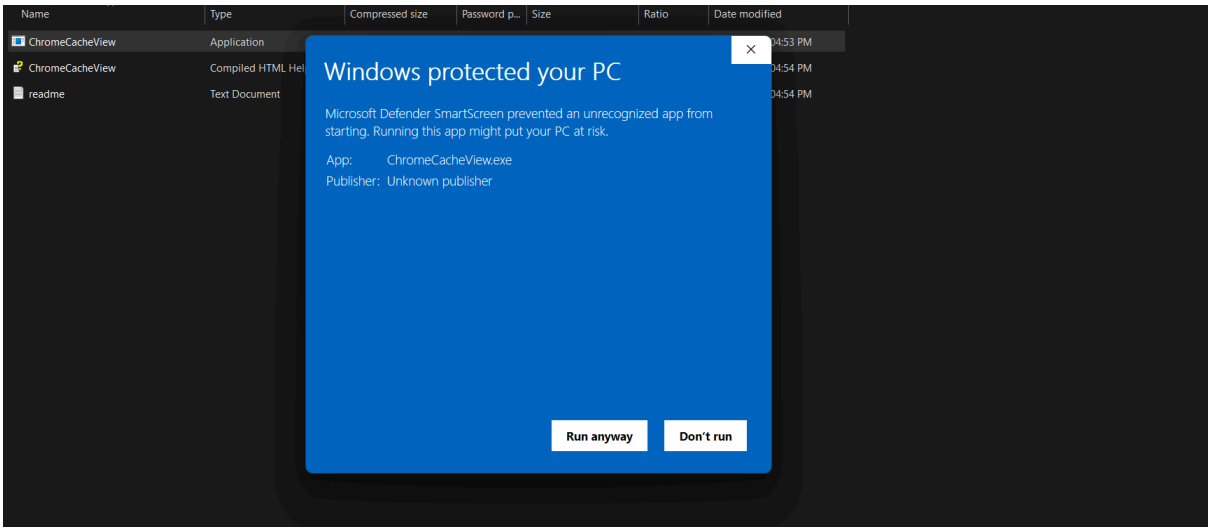
To Extract Chrome cache using forensic tools and analyse them.

Procedure:

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

Step 2: Setup from the exe file downloaded

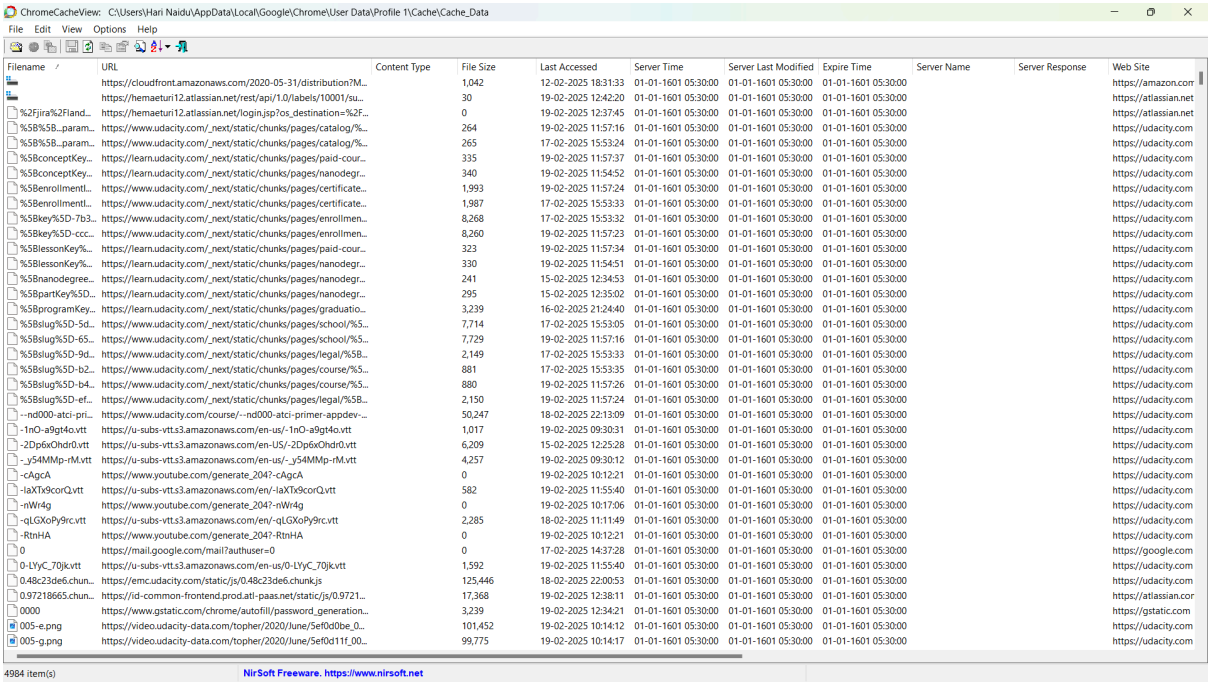
Step 3: Click run anyway when the below dialog box appears



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\Hari Naidu\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://cloudfront.amazonaws.com/2020-05-31/distribution?M...		1,042	12-02-2025 18:31:33	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://amazon.com
	https://hemaeturi12.atlassian.net/rest/api/1.0/labels/10001/su...		30	19-02-2025 12:42:20	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://atlassian.net
%2Fjira%2Fland...	https://hemaeturi12.atlassian.net/login.jsp?os_destination=%2F...		0	19-02-2025 12:37:45	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://atlassian.net
%5B%5B...param...	https://www.udacity.com/_next/static/chunks/pages/catalog/%...		264	19-02-2025 11:57:16	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5B%5B...param...	https://www.udacity.com/_next/static/chunks/pages/catalog/%...		265	17-02-2025 15:53:24	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BconceptKey...	https://learn.udacity.com/_next/static/chunks/pages/paid-cour...		335	19-02-2025 11:57:37	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BconceptKey...	https://learn.udacity.com/_next/static/chunks/pages/nanodegr...		340	19-02-2025 11:54:52	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BenrollmentI...	https://www.udacity.com/_next/static/chunks/pages/certificate...		1,993	19-02-2025 11:57:24	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BenrollmentI...	https://www.udacity.com/_next/static/chunks/pages/certificate...		1,987	17-02-2025 15:53:33	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bkey%5D-7b3...	https://www.udacity.com/_next/static/chunks/pages/enrollmen...		8,268	17-02-2025 15:53:32	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bkey%5D-ccc...	https://www.udacity.com/_next/static/chunks/pages/enrollmen...		8,260	19-02-2025 11:57:23	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BlessonKey%...	https://learn.udacity.com/_next/static/chunks/pages/paid-cour...		323	19-02-2025 11:57:34	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BlessonKey%...	https://learn.udacity.com/_next/static/chunks/pages/nanodegr...		330	19-02-2025 11:54:51	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bnanodegree...	https://learn.udacity.com/_next/static/chunks/pages/nanodegr...		241	15-02-2025 12:34:53	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BpartKey%5D...	https://learn.udacity.com/_next/static/chunks/pages/nanodegr...		295	15-02-2025 12:35:02	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5BprogramKey...	https://learn.udacity.com/_next/static/chunks/pages/graduatio...		3,239	16-02-2025 21:24:40	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bslug%5D-5d...	https://www.udacity.com/_next/static/chunks/pages/school/%5...		7,714	17-02-2025 15:53:05	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bslug%5D-65...	https://www.udacity.com/_next/static/chunks/pages/school/%5...		7,729	19-02-2025 11:57:16	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bslug%5D-9d...	https://www.udacity.com/_next/static/chunks/pages/legal/%5B...		2,149	17-02-2025 15:53:33	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bslug%5D-b2...	https://www.udacity.com/_next/static/chunks/pages/course/%5...		881	17-02-2025 15:53:35	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bslug%5D-b4...	https://www.udacity.com/_next/static/chunks/pages/course/%5...		880	19-02-2025 11:57:26	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
%5Bslug%5D-ef...	https://www.udacity.com/_next/static/chunks/pages/legal/%5B...		2,150	19-02-2025 11:57:24	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
--nd000-atci-pri...	https://www.udacity.com/course/--nd000-atci-primer-appdev-...		50,247	18-02-2025 22:13:09	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-1nO-a9gt4o.vtt	https://u-subs-vtt.s3.amazonaws.com/en-us/-1nO-a9gt4o.vtt		1,017	19-02-2025 09:30:31	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-2Dp6xOhdr0.vtt	https://u-subs-vtt.s3.amazonaws.com/en-US/-2Dp6xOhdr0.vtt		6,209	15-02-2025 12:25:28	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-_y54MMp-rM.vtt	https://u-subs-vtt.s3.amazonaws.com/en-us/-_y54MMp-rM.vtt		4,257	19-02-2025 09:30:12	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-cAgcA	https://www.youtube.com/generate_204?-cAgcA		0	19-02-2025 10:12:21	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-laXTx9corQ.vtt	https://u-subs-vtt.s3.amazonaws.com/en/-laXTx9corQ.vtt		582	19-02-2025 11:55:40	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-nWr4g	https://www.youtube.com/generate_204?-nWr4g		0	19-02-2025 10:17:06	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-qLGXoPy9rc.vtt	https://u-subs-vtt.s3.amazonaws.com/en/-qLGXoPy9rc.vtt		2,285	18-02-2025 11:11:49	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
-RtnHA	https://www.youtube.com/generate_204?-RtnHA		0	19-02-2025 10:12:21	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
0	https://mail.google.com/mail?authuser=0		0	17-02-2025 14:37:28	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://google.com
0-LYyC_70jk.vtt	https://u-subs-vtt.s3.amazonaws.com/en-us/0-LYyC_70jk.vtt		1,592	19-02-2025 11:55:40	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
0.48c23de6.chun...	https://emc.udacity.com/static/js/0.48c23de6.chunk.js		125,446	18-02-2025 22:00:53	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
0.97218665.chun...	https://id-common-frontend.prod.atl-paas.net/static/js/0.9721...		17,368	19-02-2025 12:38:11	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://atlassian.com
0000	https://www.gstatic.com/chrome/autofill/password_generation...		3,239	19-02-2025 12:34:21	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://gstatic.com
005-e.png	https://video.udacity-data.com/topher/2020/June/5ef0d0be_0...		101,452	19-02-2025 10:14:12	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com
005-g.png	https://video.udacity-data.com/topher/2020/June/5ef0d11f_00...		99,775	19-02-2025 10:14:17	01-01-1601 05:30:00	01-01-1601 05:30:00	01-01-1601 05:30:00			https://udacity.com

4984 item(s) NirSoft Freeware. https://www.nirsoft.net

Result:

The experiment has been successfully executed

EXPERIMENT-07

Extract last activity using forensic tools

Aim of the Experiment:

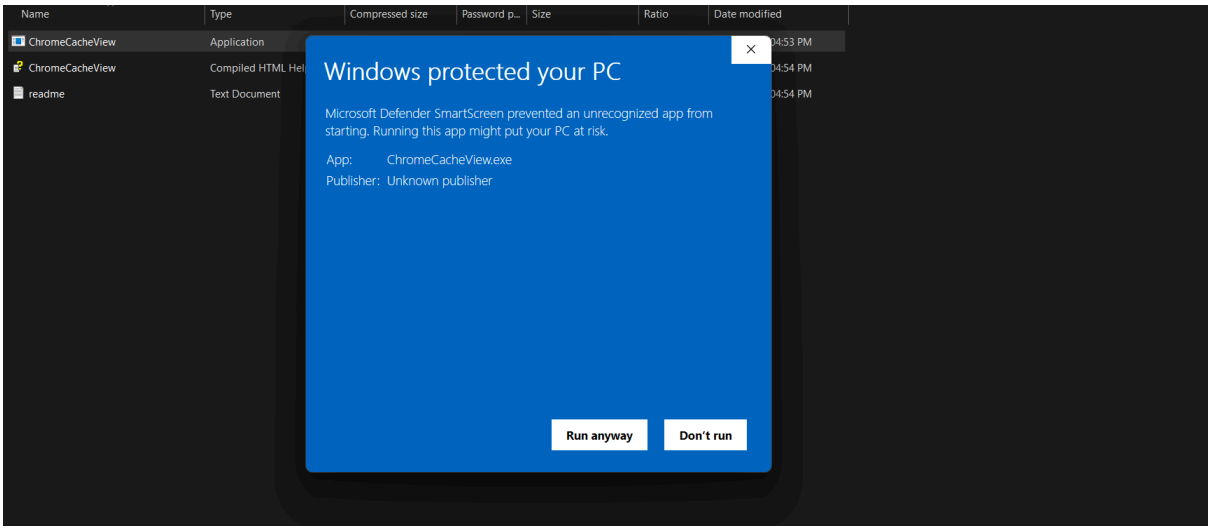
To Extract the last activity view using forensic tools and analyse them.

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

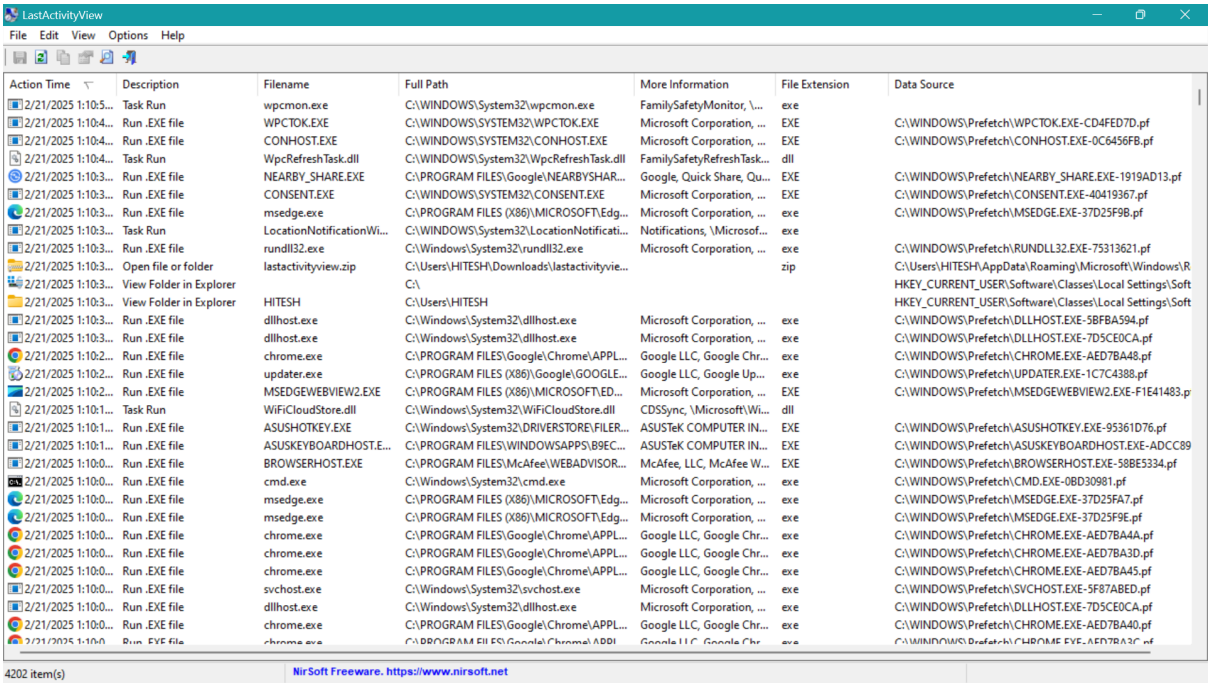
Step 3: Click run anyway when the below dialog box appears



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.



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

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:

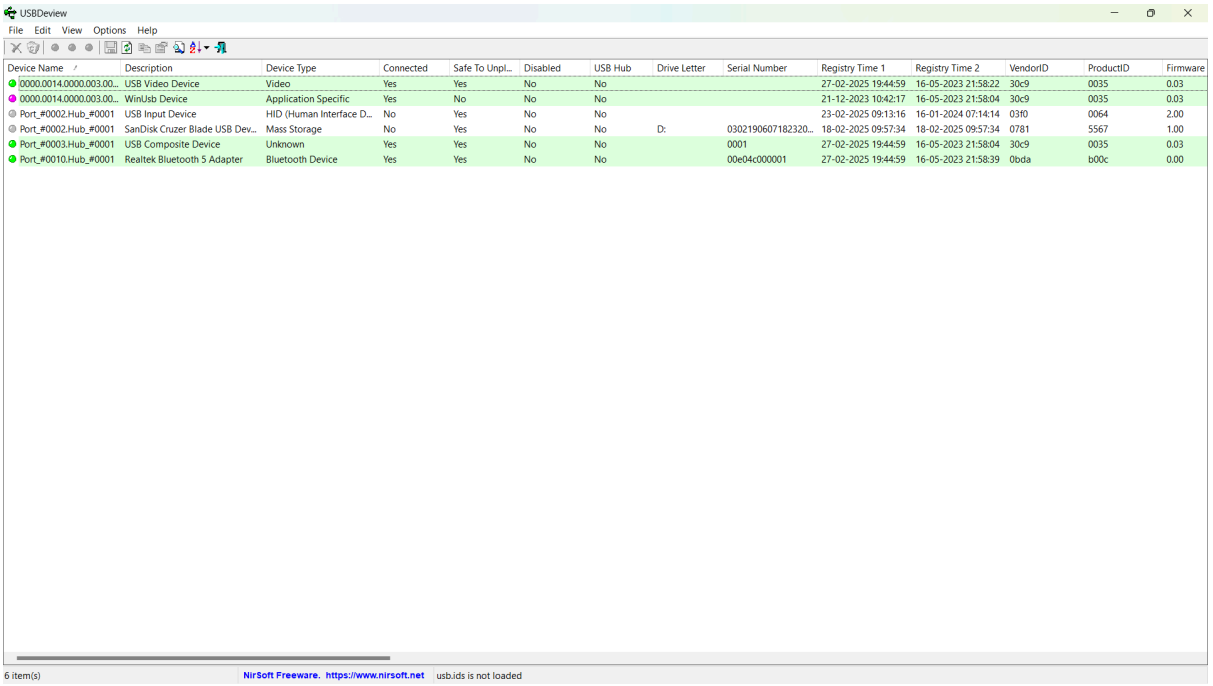
Step 1: Download previous USB devices view tool
URL: [USBDeview download | SourceForge.net]

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

Result:

The experiment has been successfully executed

EXPERIMENT 9

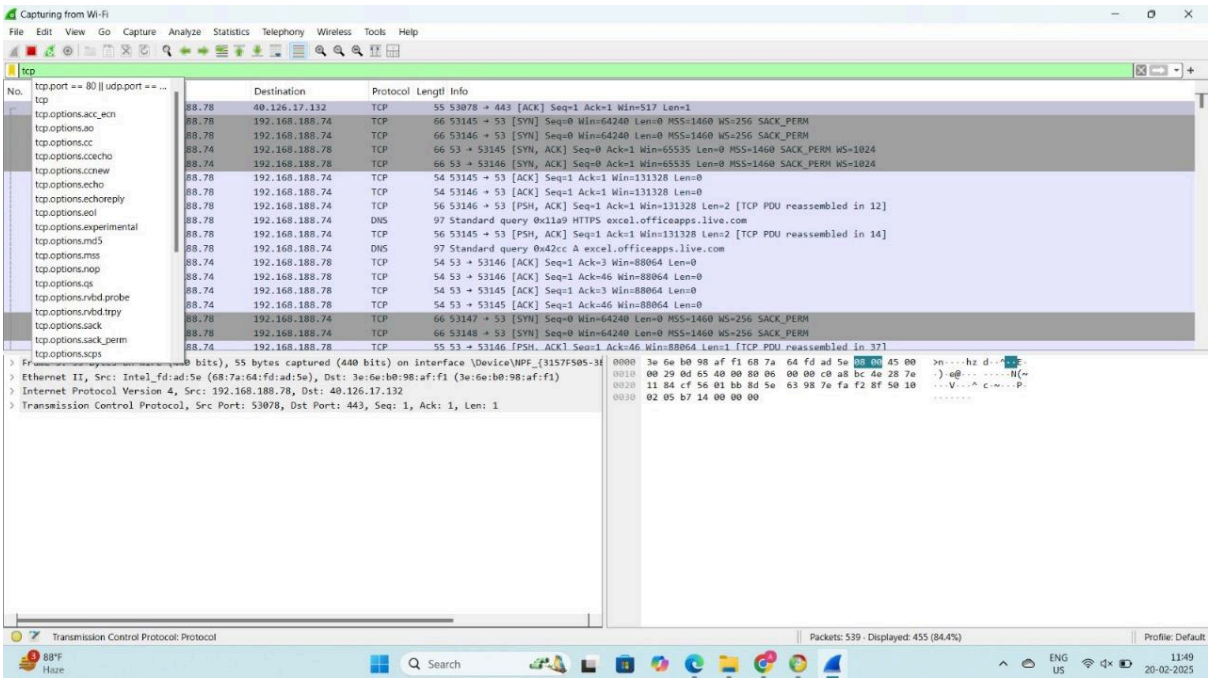
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-TCP

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

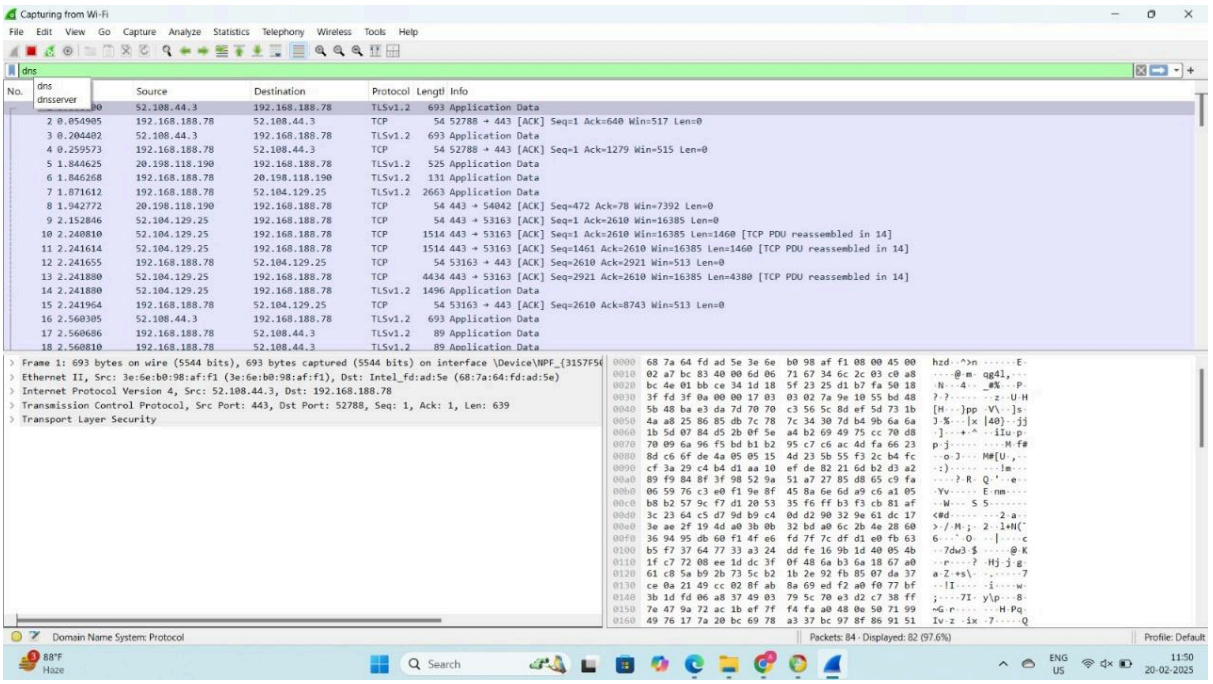
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-DNS

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

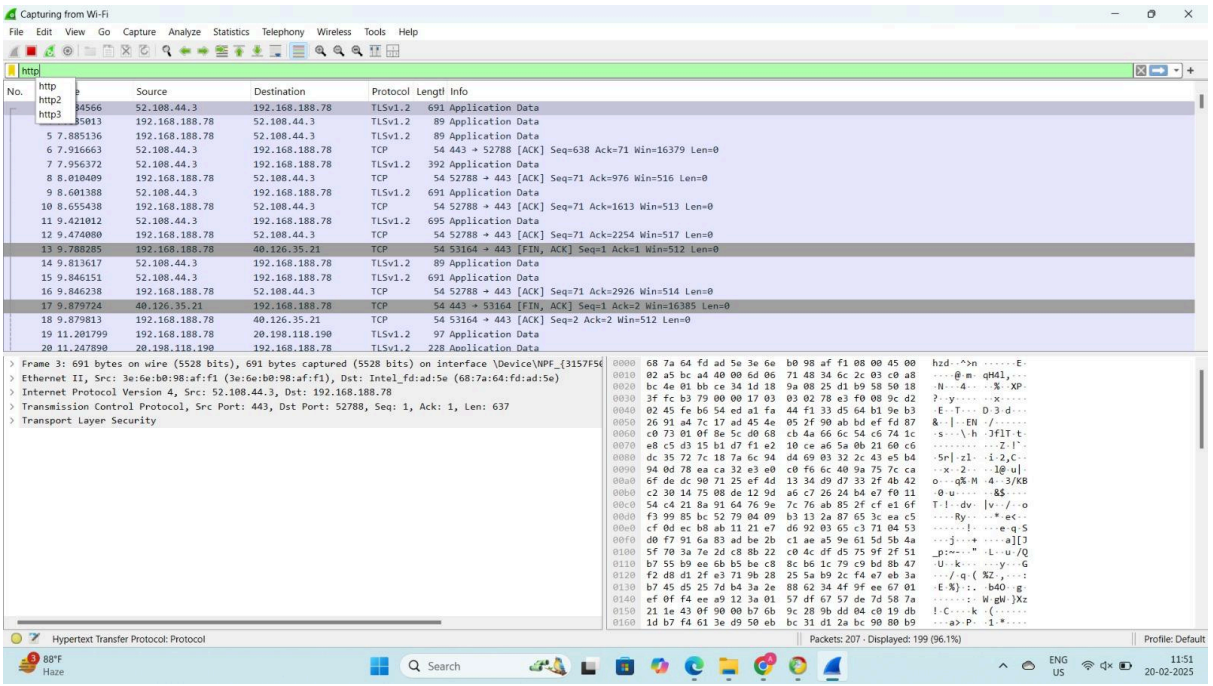
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-HTTP

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
```

```
Administrator: Command Prompt
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

```
Administrator: Command Prompt

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.

```
Administrator: Command Prompt

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

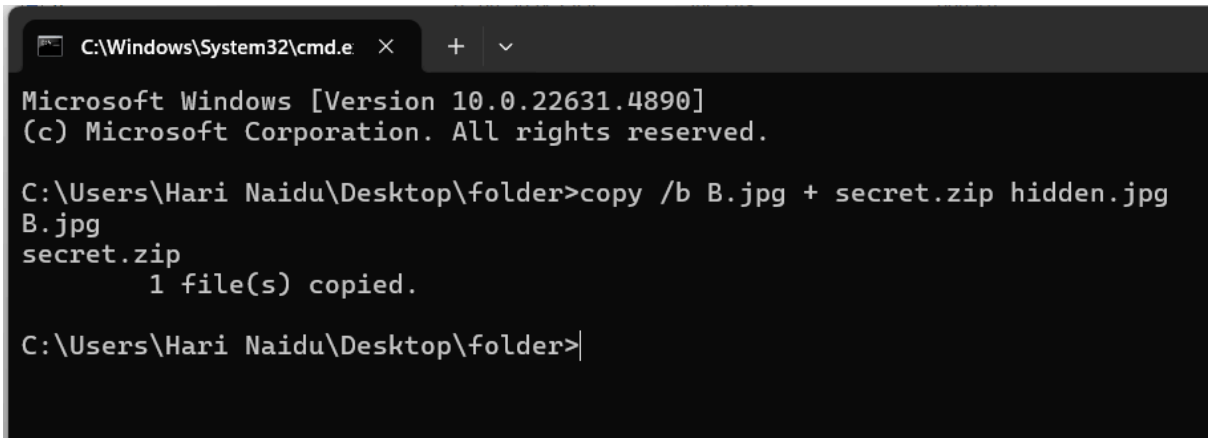
Aim: To Hide a ZIP File Inside an Image.

SOFTWARE USED: CMD prompt.

Procedure:

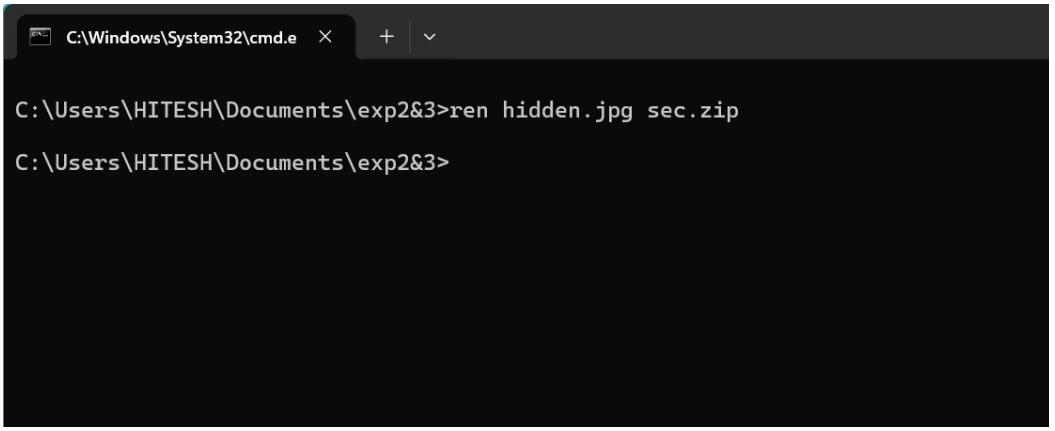
1. Place the image file (cover.jpg) and ZIP file (secret.zip) in the same folder.
2. Open cmd inside the folder.
3. Run the following cmd

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



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

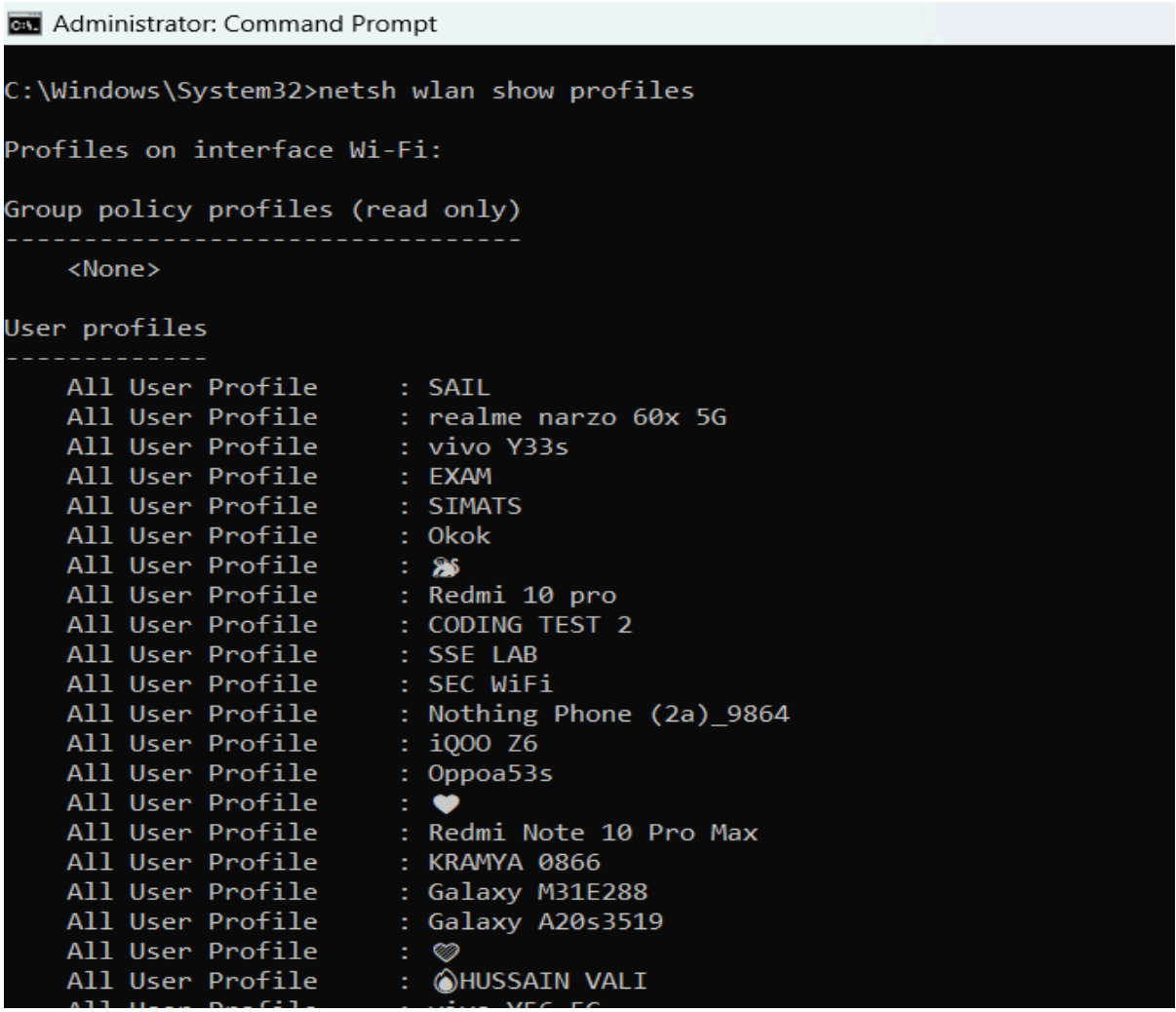
Aim: To View All Wi-Fi Passwords Saved on the Computer.

SOFTWARE USED: CMD prompt.

Procedure:

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

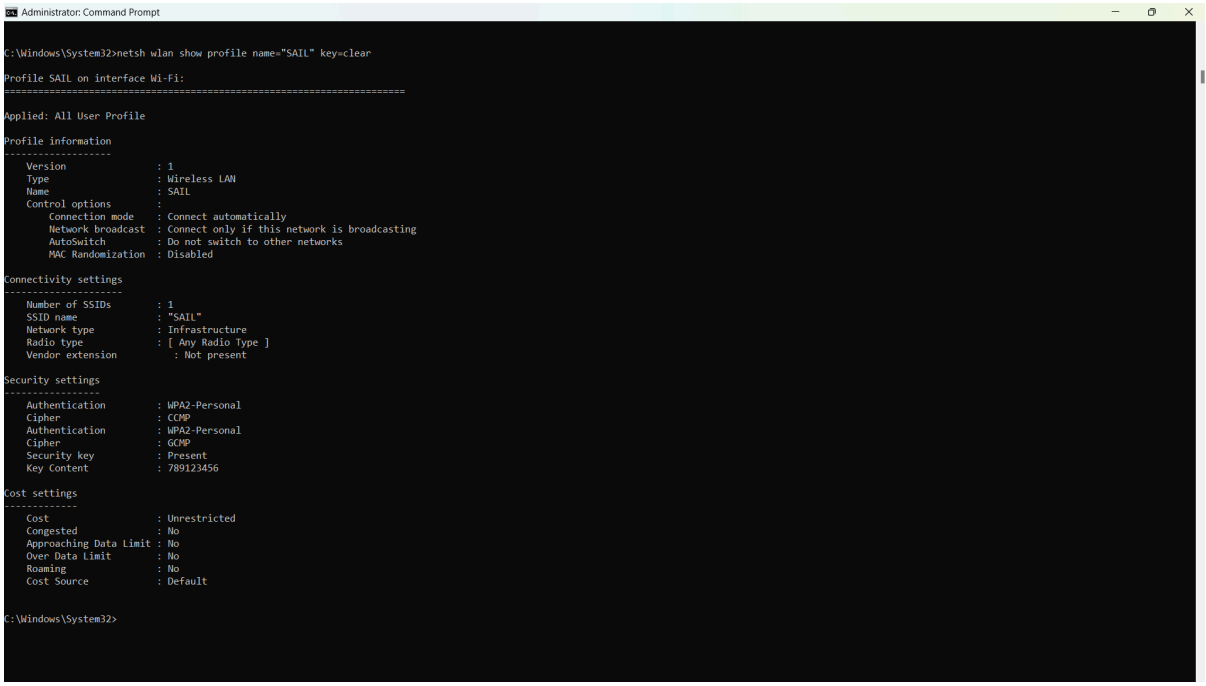
```
netsh wlan show profiles
```



```
Administrator: Command Prompt

C:\Windows\System32>netsh wlan show profiles

Profiles on interface Wi-Fi:

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

User profiles
-------------
    All User Profile     : SAIL
    All User Profile     : realme narzo 60x 5G
    All User Profile     : vivo Y33s
    All User Profile     : EXAM
    All User Profile     : SIMATS
    All User Profile     : Okok
    All User Profile     : [illegible]
    All User Profile     : Redmi 10 pro
    All User Profile     : CODING TEST 2
    All User Profile     : SSE LAB
    All User Profile     : SEC WiFi
    All User Profile     : Nothing Phone (2a)_9864
    All User Profile     : iQOO Z6
    All User Profile     : Oppoa53s
    All User Profile     : [illegible]
    All User Profile     : Redmi Note 10 Pro Max
    All User Profile     : KRAMYA 0866
    All User Profile     : Galaxy M31E288
    All User Profile     : Galaxy A20s3519
    All User Profile     : [illegible]
    All User Profile     : [illegible]HUSSAIN VALI
```

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

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



```
Administrator: Command Prompt

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

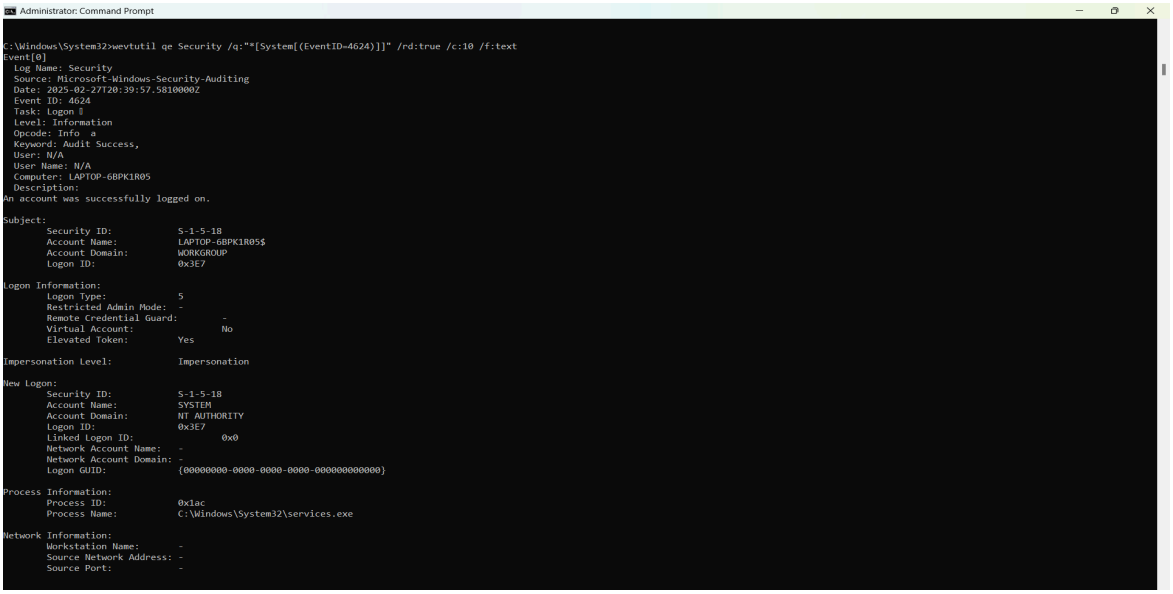
Aim: To extract the recent login and logout

SOFTWARE USED: CMD prompt.

Procedure:

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

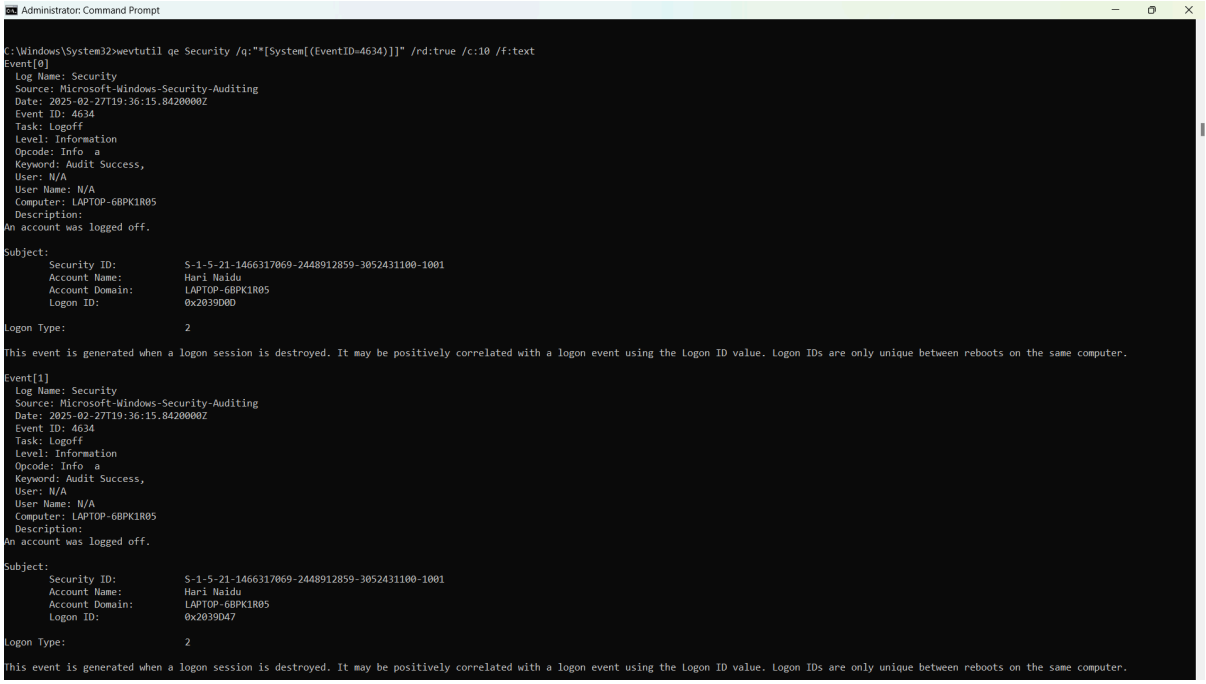
```
wevtutil qe Security /q:"*[System[(EventID=4624)]]"
/rd:true /c:10 /f:text
```



```
Administrator: Command Prompt

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: 2025-02-27T20:39:57.5810000Z
  Event ID: 4624
  Task: Logon 3
  Level: Information
  Opcode: Info  a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
  Computer: LAPTOP-6BPK1R05
  Description:
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           LAPTOP-6BPK1R05$
        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:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x1ac
        Process Name:           C:\Windows\System32\services.exe

Network Information:
        Workstation Name:       -
        Source Network Address: -
        Source Port:            -
```

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: 2025-02-27T19:36:15.8420000Z
  Event ID: 4634
  Task: Logoff
  Level: Information
  Opcode: Info  a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
  Computer: LAPTOP-6BPK1R05
  Description:
An account was logged off.

Subject:
        Security ID:            S-1-5-21-1466317069-2448912859-3052431100-1001
        Account Name:           Hari Naidu
        Account Domain:         LAPTOP-6BPK1R05
        Logon ID:               0x2039D0D

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 reboots on the same computer.

Event[1]
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2025-02-27T19:36:15.8420000Z
  Event ID: 4634
  Task: Logoff
  Level: Information
  Opcode: Info  a
  Keyword: Audit Success,
  User: N/A
  User Name: N/A
  Computer: LAPTOP-6BPK1R05
  Description:
An account was logged off.

Subject:
        Security ID:            S-1-5-21-1466317069-2448912859-3052431100-1001
        Account Name:           Hari Naidu
        Account Domain:         LAPTOP-6BPK1R05
        Logon ID:               0x2039D47

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 reboots on the same computer.
```

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

Result:

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