

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](#)

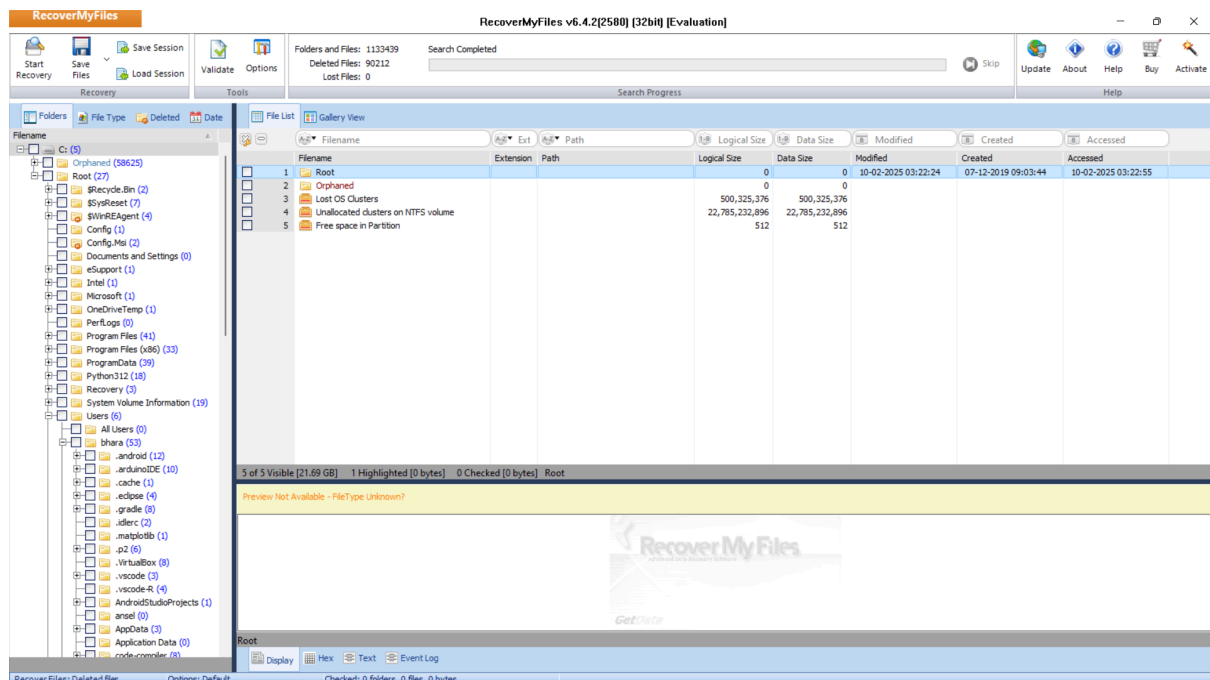
Step 2: Setup from the exe file downloaded

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.

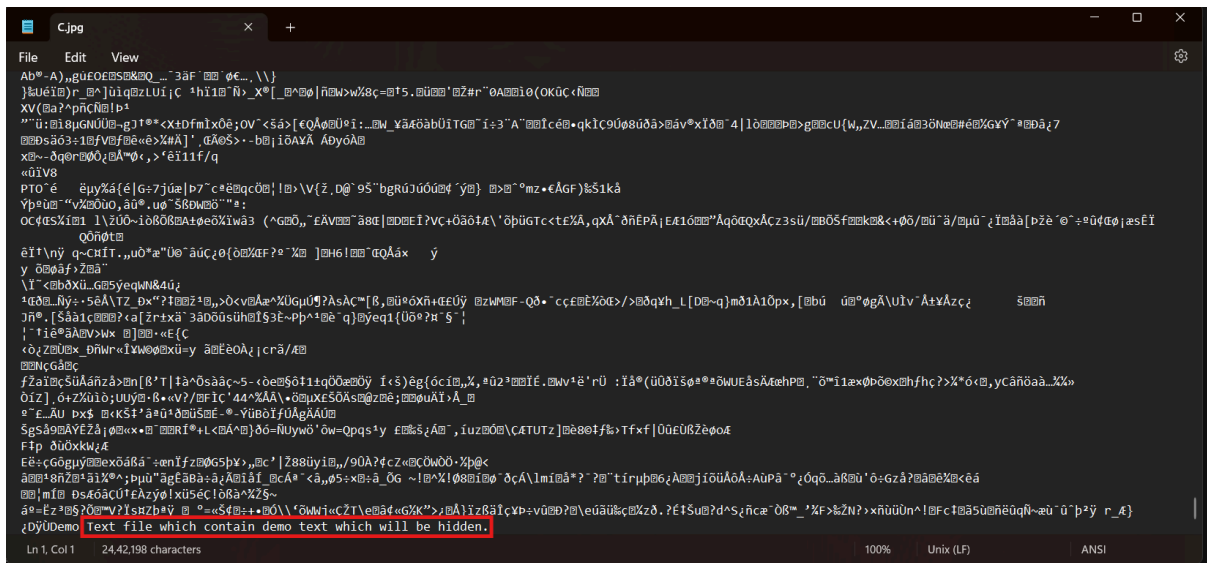
C:\Users\bhara\Downloads\Demo folder>|
```

"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



```
File Edit View
AB^A)uE0EBSBkEQ...`3aF` 0c_,\}
}kUe10)r_0^]u1qBzLUi1c`^hi10`N`X`[_0^00|ñ0M>wX8ç=0t5,0U00'0Z#r`0A0010(OKUC<N00
XV(0a?^pñCñ0!p^
""ü:018µGNUÜ0-gjT*~x±Dfmix0ë;0V`<5ä>[€QÀ00U°i:...0W_¥ä6ä0äbÜiTG0~i±3`A`00Icë0-qk1C9Ü008ü0ä>0äv*Xið0`4|l0000p0>g000cU{W,ZV...00iä0030ñw0#ë0YGY`^00äz7
000sä03÷10fV0f0ë«ë>X#A]'.0A0S>--b0ji0AYÄ`Ä0y0Ä0
x0~-0q0r000z0A^0ç,>^ëi11f/q
«üiV8
PTO`é`ëµy%ä{ë|g÷7jüæ|p7`c^ë0qç00!|0\|V{Z,D0`9S`bgrüjüü000`ý0] 0>0`^mz•€ÄGF)kS1kâ
Yp0u00`"vX0000,ä0^u0`S80W00`"a:
0C40SXi01 l\zÜ0-i0000A±0ë00ü0wä3 (^000,`EÄV00`ä0E|0000Ei?Vç+0ä0tÆ\`0püGtç<tE%Ä,qXÄ`ðñÉPÄjEÄ1000"Aq00QXÄCz3sü/000Sf00k0k<+00/0ü`ä/0µü`¿i0ä0[p0ë`0`÷0ü400j0sEi
Q0ñ0t0
ëi\`nÿ`q~cHfT,...u0^0`0ë`äüç¿0(00Y0F?0`X0 ]0H6!00`0QÄ0x`ý
y`0000äf>Z00`
\I`<00b0XÜ..G005y0qW0K4ü¿
^000.Nÿ÷.5EÄ\TZ`0x"?f000z^0,,>0c00A0^XÜ0µ0?AsÄC`=[0,0ü^0Xñ+0EÜ0`0zW00F-Q0•`cçE0E%00>/>00qVh_l[D0~q]m01A10px,[0bü`ü0^00Ä\U1v`Ä+XÄzç¿`S00ñ
jñ0`[Sä01ç000?<a|zr+xa`3ä000sü00I$3E~Pp^00ë`q]0y0q1{Ü0^?H`S`!
!`ti0^0A0V>Wx`0]00:«E(C
<0¿Z000x`0ñW0«IWX0000xü=y`ä0E0Ä¿jçr0/Ä0
00NçGä0ç
fZa10çSÜAänz0>0n{0^T|t0^0sääç~5<000$0t11q00000ÿ`I<S`0g{0c10,,X,^0z`00IÉ,0WV^0è`rÜ`iÄ*(ü00i000^*0WUEÄsÄ00P0,"0^i10x00b00x0hfhç?>X`0<0,yCän0ä0..X%»
0iZj`0+Z%ü0;UUY00•0^«v?/0FIC`44^%ÄÄ^00µX0S0Äs00z00;000uÄI>Ä`0
0`_ÄU`0x$`0<KSt^ä0^000S0E~0`YüB0IfÜÄgÄÄU0
SgS000AYÉZ0j00«x`0`00RI^+L<0Ä^0]00=Nuyw0`0w=Opqs^y`E00S¿Ä0`^iuz000ÇCATUTZj0000tF%>Tfxfl|Ü0EÜ0Z0000
Ffp`0ü0xkw¿
Eë÷cG00y00000ä0ä`÷0nIfz000G5pX>„0c`|Z80üyi0,,/90A?4cz«0C0W00`%p0<
ä00^8ñZ0^ä1X^0;µµü`ä0ä0ä0:ä¿Ä0iÄf`0cÄ0`<ä,,05÷x0÷ä`0G`~!0^X!000I00`0çÄ\lmi0ä^?`?0`tirµp00zÄ00ji0üÄ0Ä:AüP0`°¿0q0...ä00ü`0÷Gz0?0ä00000<0ä
00|mi0`0sÄ0äCÜfEÄz00!xü50C!000^XZ$~
ä0Ez00$?00V?IsH20y`0`0=«$00÷+00\\`0Wfi0CZT\00ä0«G%K">„0Ä\iz0äiçVp÷vü00?0\0ü0ä00ç0Z0.0?ÉtS00?d^S¿ñc0`00`_`%F>0Zn?>xñüü0n^|0Fc100äSü000üqñ~0ü`ü`p^y`r_Ä}
0YÜ0Demo
Ln 1, Col 1 24,42,198 characters 100% Unix (LF) ANSI
```

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

Hide A Message into Image:

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

Result:

The experiment has been successfully executed.

EXPERIMENT-03

Hiding and extracting a text file behind an audio file.

Aim of the Experiment:

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

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

How to Hide the FILE?

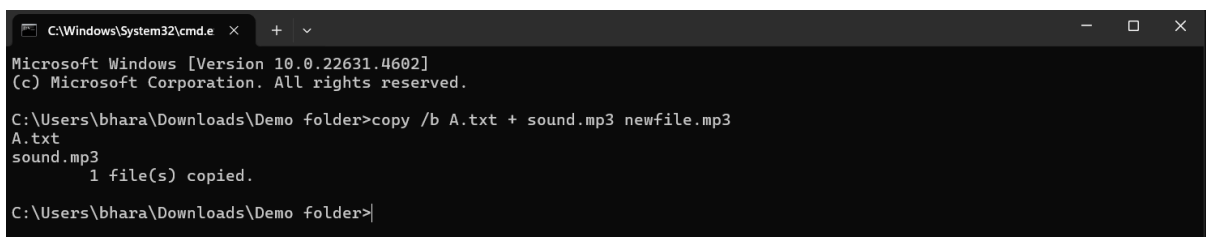
Suppose you have to hide a text file "A.txt" with the image file "sound.mp3" and combine them in a new file as "newfile.mp3". Where "newfile.mp3" is our output file which contains the text hidden in the image file.

Follow the steps:

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

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

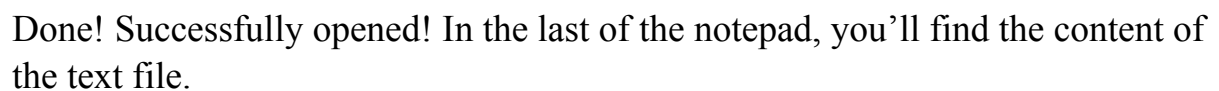
Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial- audio.mp3 Resulting-audio-name.mp3*



```
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>|
```

The screenshot shows a Windows File Explorer window. The address bar indicates the current location is 'Downloads > Demo folder'. The left sidebar shows the navigation pane with 'Desktop', 'Download', 'Document', 'Pictures', and 'Music' options. The main area displays five items: a document icon labeled 'A', two image thumbnails labeled 'B' and 'C', and two video file icons labeled 'newfile' and 'sound'.

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



7. Open 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.

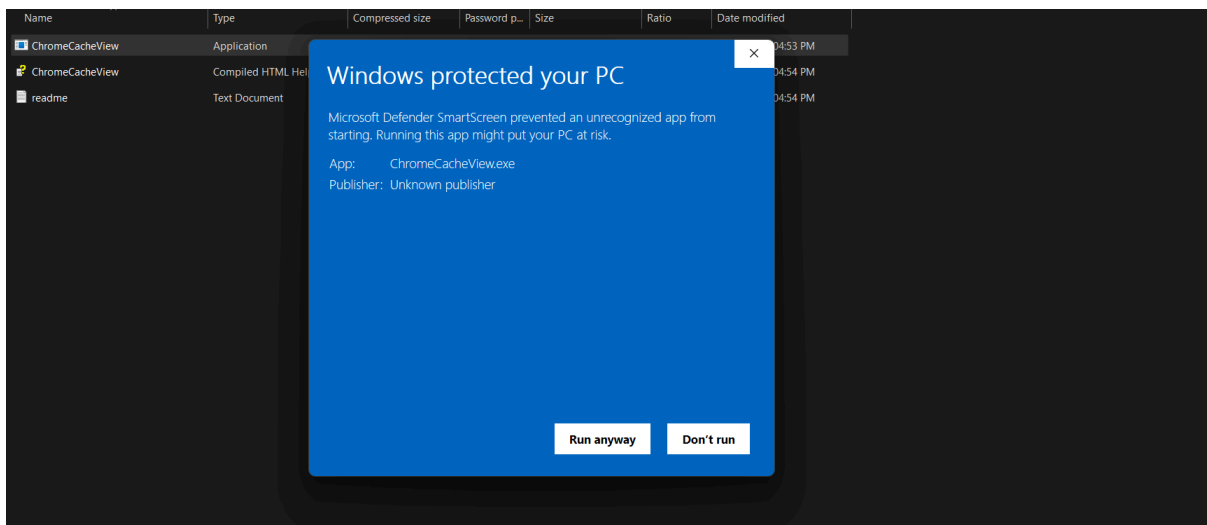
Procedure:

Step 1: Download Chrome History View tool

URL: <https://en.softonic.com/download/chromehistoryview/windows/post-download?ext=1>

Step 2: Setup from the exe file downloaded

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



Step 4: Start the Chrome 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.

ChromeCacheView: C:\Users\bhara\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data										
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...		126,160	08-02-2025 21:2309	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://accenture.co
	https://dsun-sec.casalemedia.com/num?cm_dsp_id=178&exte...		0	08-02-2025 14:27:13	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://programiz.co
	https://embed.tawk.to/_y/v4/assets/fonts/pawik-font-ico-2.wof...		0	09-02-2025 13:1048	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://electrowiz.in
	https://iaspire-learning.accenture.com/theme/font.php/materi...		124,076	08-02-2025 21:2309	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://accenture.co
	https://api.hackerzcity.in/v1/web/referral/debounced-search?q=		100	02-02-2025 20:2615	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://hackerzcity.in
	https://iaspire-learning.accenture.com/theme/font.php/materi...		126,644	08-02-2025 21:2309	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://accenture.co
	https://dsun-sec.casalemedia.com/num?cm_dsp_id=178&exte...		0	08-02-2025 14:27:13	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://programiz.co
	https://iaspire-learning.accenture.com/theme/font.php/materi...		121,752	08-02-2025 21:2309	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://accenture.co
	https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!...		0	09-02-2025 13:0359	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://electrowiz.in
	https://graph.microsoft.com/v1.0/users/PUI000340017075A9...		68,022	31-01-2025 17:3021	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://microsof.co
	https://teams.microsoft.com/j/1/meetup-join/19%3ameeting_M...		0	09-02-2025 13:2510	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://microsof.co
	https://teams.microsoft.com/j/1/meetup-join/19%3ameeting_Nz...		0	07-02-2025 18:0305	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://microsof.co
	https://in2-files.zohopublic.in/public/SalesIQ/download/d_600...		1,423	08-02-2025 21:2256	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://accenture.co
	https://docs.google.com/generate_2047-2FQhG		0	07-02-2025 18:0645	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://google.com
	https://www.linuxmint.com/web/wiziko/template/assets/ve/d...		56,108	02-02-2025 21:0505	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://linuxmint.co
	https://b.thumbs.redditmedia.com/-xdBj2yIcVZbHdJ95q7ANJKr...		0	08-02-2025 21:2240	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://reddit.co
	https://pr-bhybp.yahoo.com/sync/open?1ee2f4a1-5d6d-a2d0...		0	08-02-2025 14:2308	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://res-1.cdn.office.net/shellux/api/ShellBootInfo/consume...		6,115	31-01-2025 17:3020	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://microsof.co
	https://docs.google.com/forms/u/0/?authuser=0		0	07-02-2025 17:3800	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://google.com
	https://docs.google.com/forms/?authuser=0		0	07-02-2025 17:3800	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://google.com
	https://d3njchibhbjot.cloudfront.net/webapps/v2-builds/bf/fr...		4,855	09-02-2025 17:1234	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://coursera.org
	https://bat.bing.com/p/insights/u/0.7.66		16,001	09-02-2025 17:1234	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://coursera.org
	https://www.gptatic.com/chrome/ai/ocfill/password_generation...		3,239	10-02-2025 08:1312	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://gptatic.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0001.w...		380	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0004.w...		374	08-02-2025 14:2435	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0009.w...		2,990	08-02-2025 14:2435	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0010.w...		1,210	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0011.w...		2,526	08-02-2025 14:3542	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0013.w...		2,774	08-02-2025 14:2435	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0014.w...		1,210	08-02-2025 14:3542	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0019.w...		3,370	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0020.w...		1,206	08-02-2025 14:3542	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0023.w...		778	08-02-2025 14:3542	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0024.w...		379	08-02-2025 14:3542	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0025.w...		2,950	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0026.w...		3,882	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0027.w...		1,210	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com
	https://html.scribdassets.com/86k2cx7a9sc8dv0x/fonts/0028.w...		2,242	08-02-2025 14:2322	01-01-1601 05:3000	01-01-1601 05:3000	01-01-1601 05:3000			https://scribd.com

8583 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.

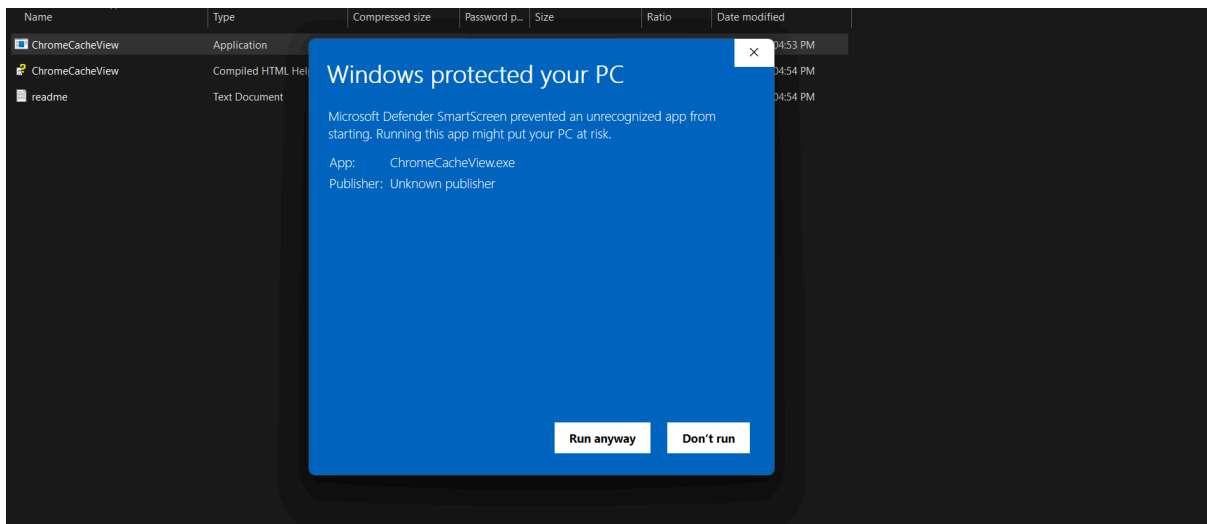
Procedure:

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.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	
-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.

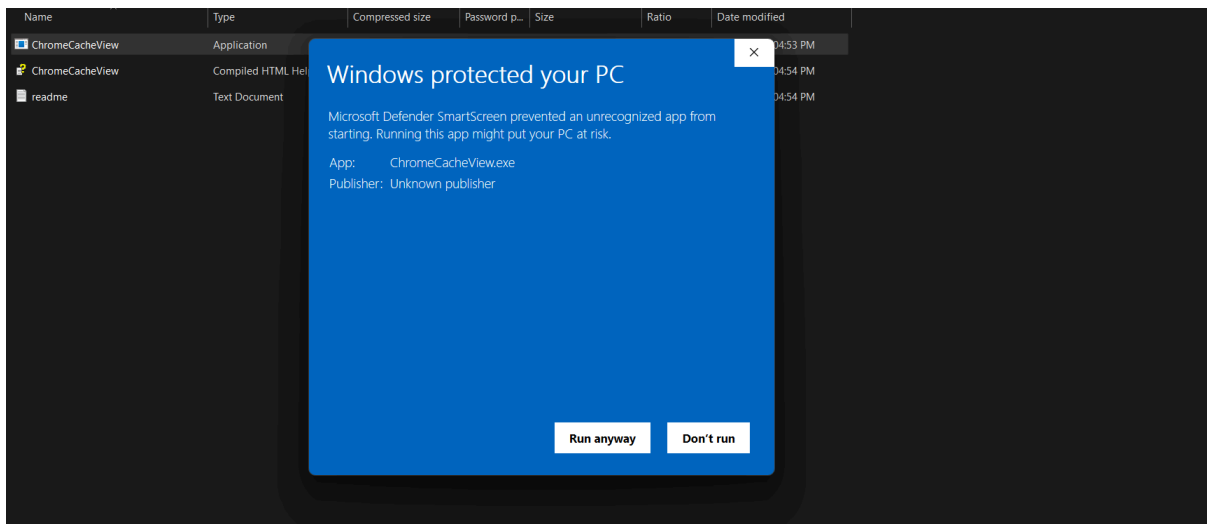
Procedure:

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.

USBDeview													
File Edit View Options Help													
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 2.0Gen1	USB Mass Storage Device	Mass Storage	Yes	Yes	No	No		0401a23723d894c9...	11-02-2025 15:21:54	19-06-2024 18:54:02	0781	5591	1.00
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	0300	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	0300	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 1947:50	0300	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 1947:50	0300	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	0300	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	0300	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	2d95	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
0000.01.0000.004.00...	Apple iPhone	Still Imaging	No	No	No	No			24-01-2025 12:47:27	24-01-2025 12:15:45	05ac	12ab	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 MS116 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	0300	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 1947:50	0300	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		ZD222FDKIC9	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		ZD222FDKIC9	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		5b602442	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

54 Item(s), 1 Selected

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

usblds is not loaded

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

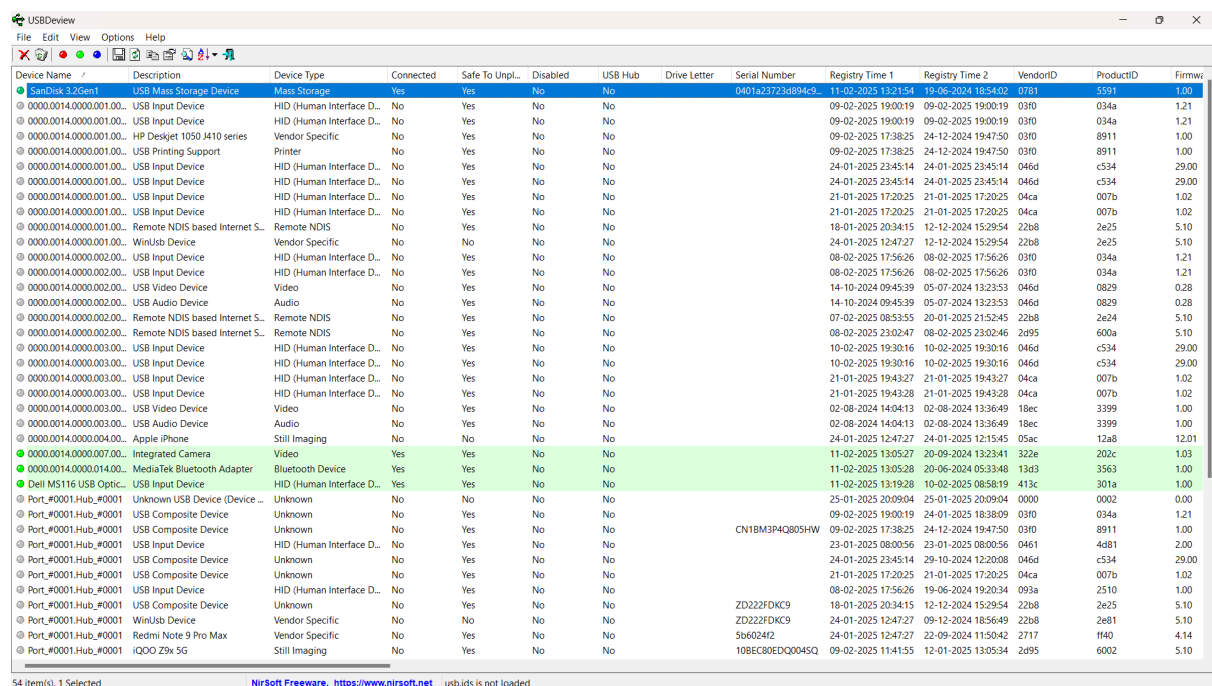
URL: [USBDeview download | SourceForge.net](#)

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

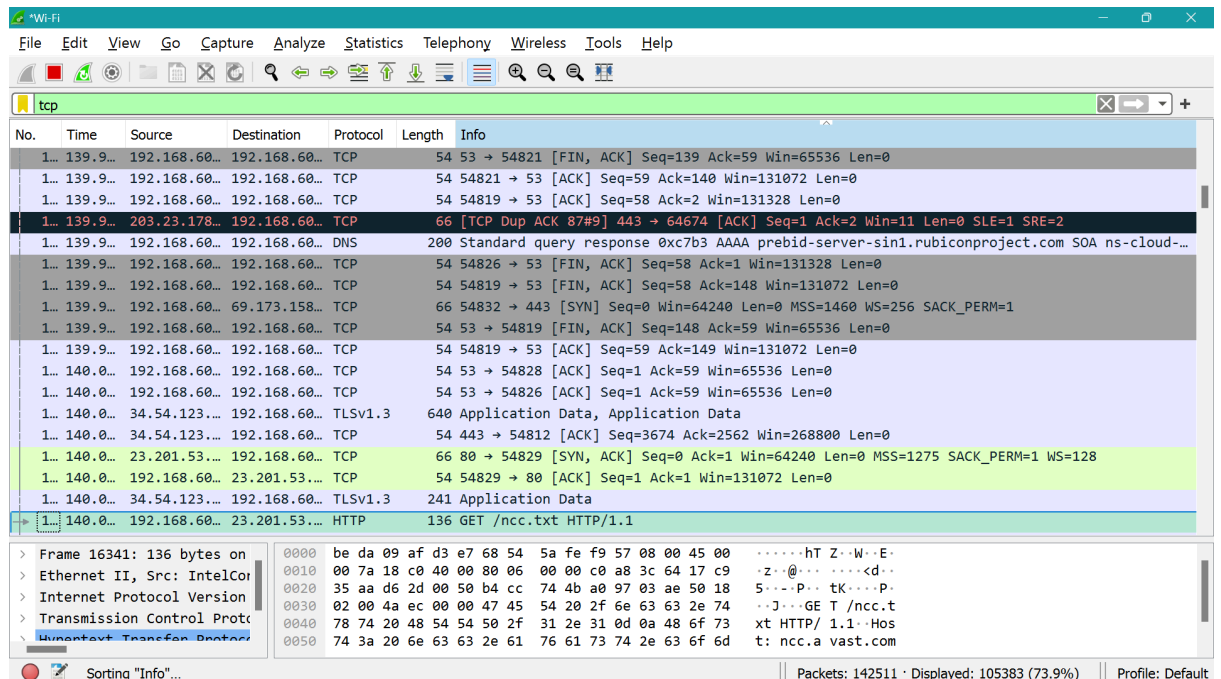
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-TCP

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

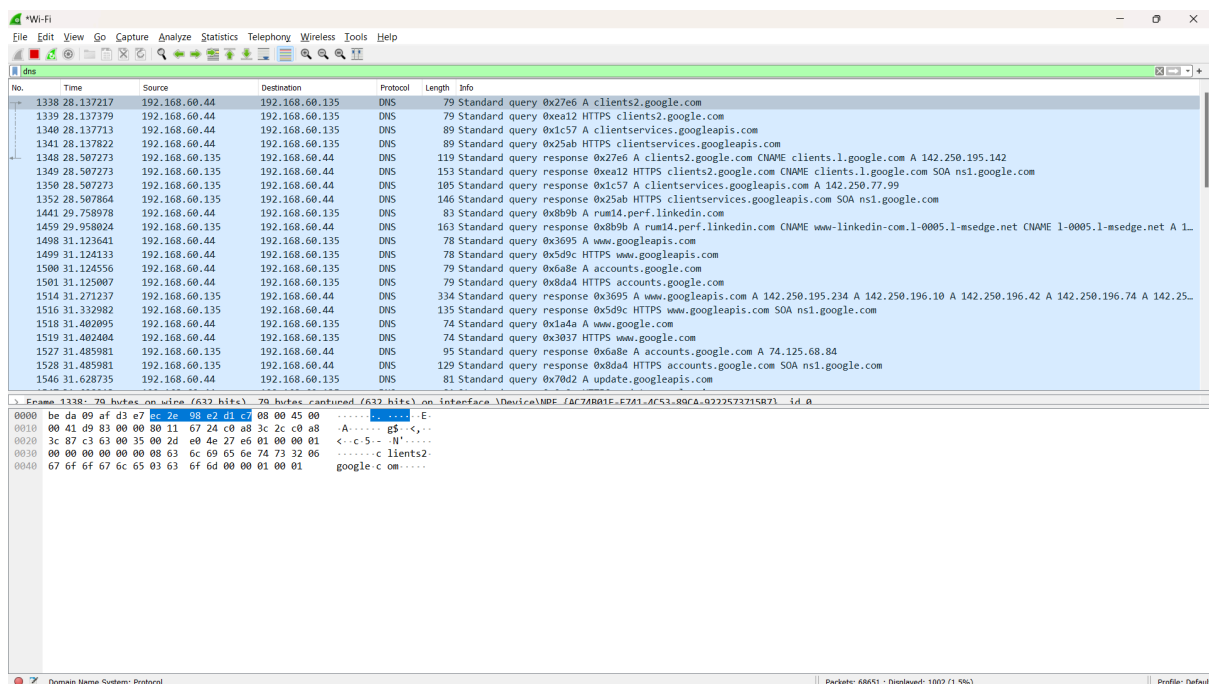
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-DNS

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

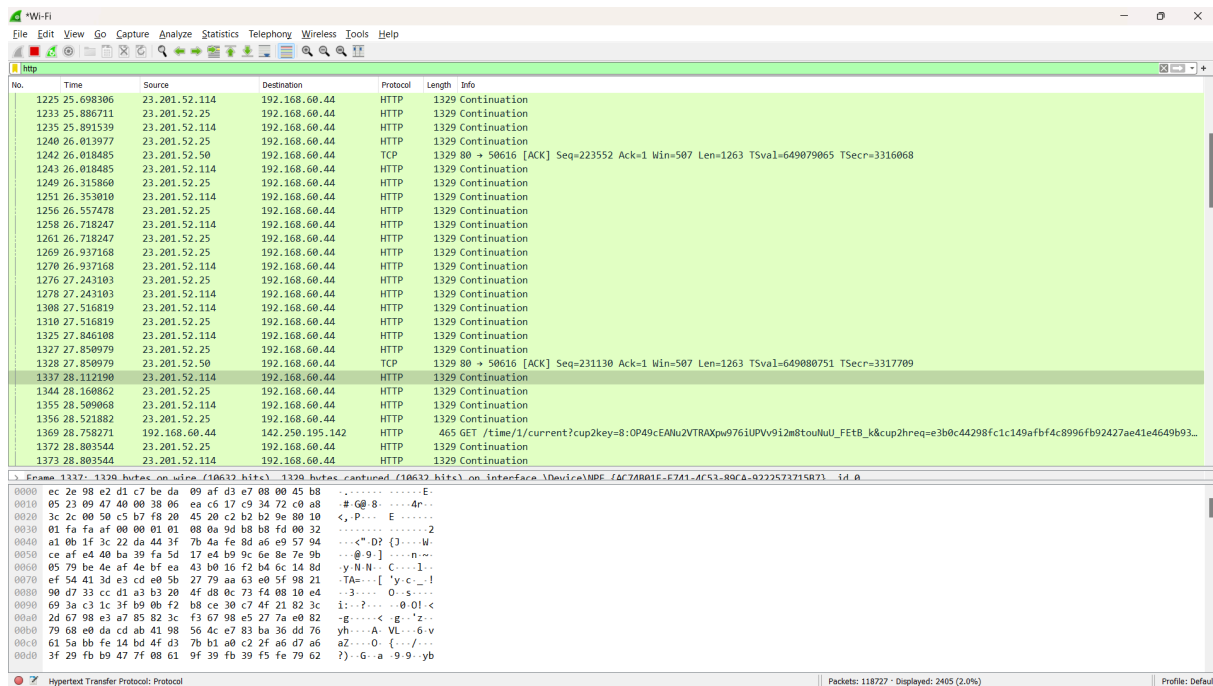
TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRESHARK-HTTP

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.