

PART A EXPERIMENTS

EXPERIMENT 1

JOHN THE RIPPER

John the Ripper is an open source cross-platform package that is typically used for password security auditing and password recovery. This software is supported across various operating systems.

AIM:

- I. Decrypting a password hash to find the password.
- II. Cracking the password of a password protected zip file.
- III. Using Brute Force method to crack the MD5 hash.

TOOLS USED: John the Ripper

- I. Decrypting a password hash to find the password.

PROCEDURE:

Step 1:

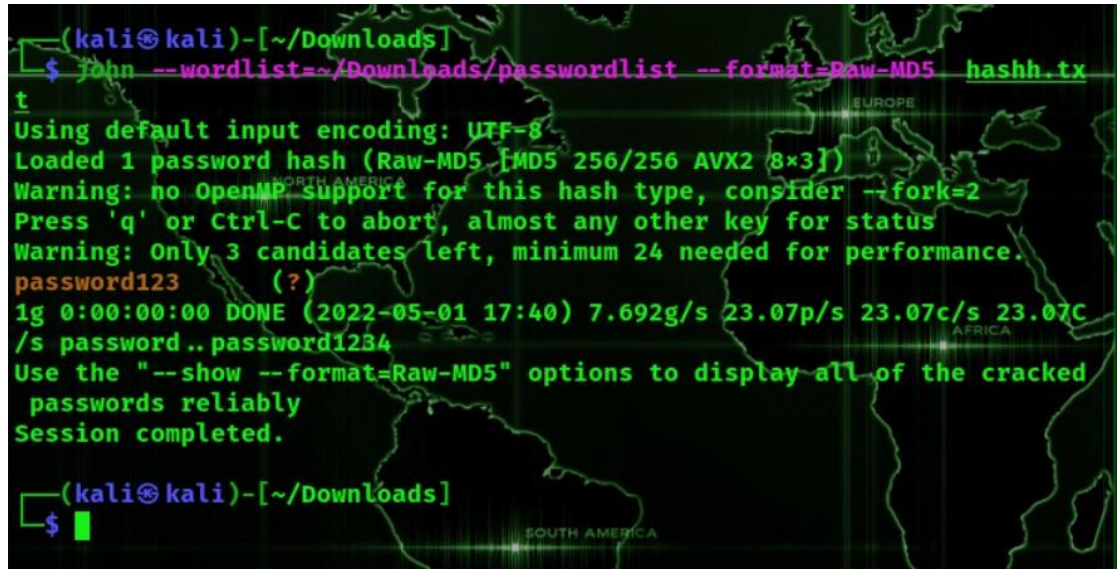
Store the hash value in a text format file.

```
echo 482c811da5d5b4bc6d497ffa98491e38 > hash.txt
```

Fig 1.1 Storing the hash value

Step 2:

Use **john --wordlist=~/.Downloads/passwordlist --format=Raw-MD5 hash.txt** to decrypt the hash value and retrieve the password.

A terminal window with a world map background. The prompt is (kali@kali)-[~/Downloads]. The command is \$ john --wordlist=~/.Downloads/passwordlist --format=Raw-MD5 hashh.txt. The output shows: Using default input encoding: UTF-8, Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3]), Warning: no OpenMP support for this hash type, consider --fork=2, Press 'q' or Ctrl-C to abort, almost any other key for status, Warning: Only 3 candidates left, minimum 24 needed for performance, password123 (?), 1g 0:00:00:00 DONE (2022-05-01 17:40) 7.692g/s 23.07p/s 23.07c/s 23.07C, /s password.. password1234, Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably, Session completed. The prompt returns to (kali@kali)-[~/Downloads].

```
(kali@kali)-[~/Downloads]
$ john --wordlist=~/.Downloads/passwordlist --format=Raw-MD5 hashh.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates left, minimum 24 needed for performance.
password123 (?)
1g 0:00:00:00 DONE (2022-05-01 17:40) 7.692g/s 23.07p/s 23.07c/s 23.07C
/s password.. password1234
Use the "--show --format=Raw-MD5" options to display all of the cracked
passwords reliably
Session completed.

(kali@kali)-[~/Downloads]
$
```

Fig 1.2 Decrypting the Hash Value

II. Cracking the password of a password protected zip file.

PROCEDURE:

Step 1:

Install zip on the kali linux terminal using the **sudo apt install zip** command.

Step 2:

Create a password encrypted zip file using the syntax **zip -password <password><name of zip file><directory of zip>** as shown in the diagram below.

A terminal window with a world map background. The prompt is (kali@kali)-[~/Downloads]. The command is \$ zip2john linuxhint.zip > linuxhint_password.txt. The output shows: ver 2.0 efh 5455 efh 7875 linuxhint.zip/external-content.duckduckgo.com.jpeg PKZIP Encr: TS_chk, cmplen=1234252, decmplen=1286899, crc=384E1CA, 3 ts=5181 cs=5181 type=8. The prompt returns to (kali@kali)-[~/Downloads].

```
(kali@kali)-[~/Downloads]
$ zip2john linuxhint.zip > linuxhint_password.txt
ver 2.0 efh 5455 efh 7875 linuxhint.zip/external-content.duckduckgo.com
.jpeg PKZIP Encr: TS_chk, cmplen=1234252, decmplen=1286899, crc=384E1CA
3 ts=5181 cs=5181 type=8

(kali@kali)-[~/Downloads]
$
```

Fig 1.3 Creating a password encrypted zip file

Step 3:

Use **zip2john test.zip > test_password.txt** to store the hash value of the zip file.

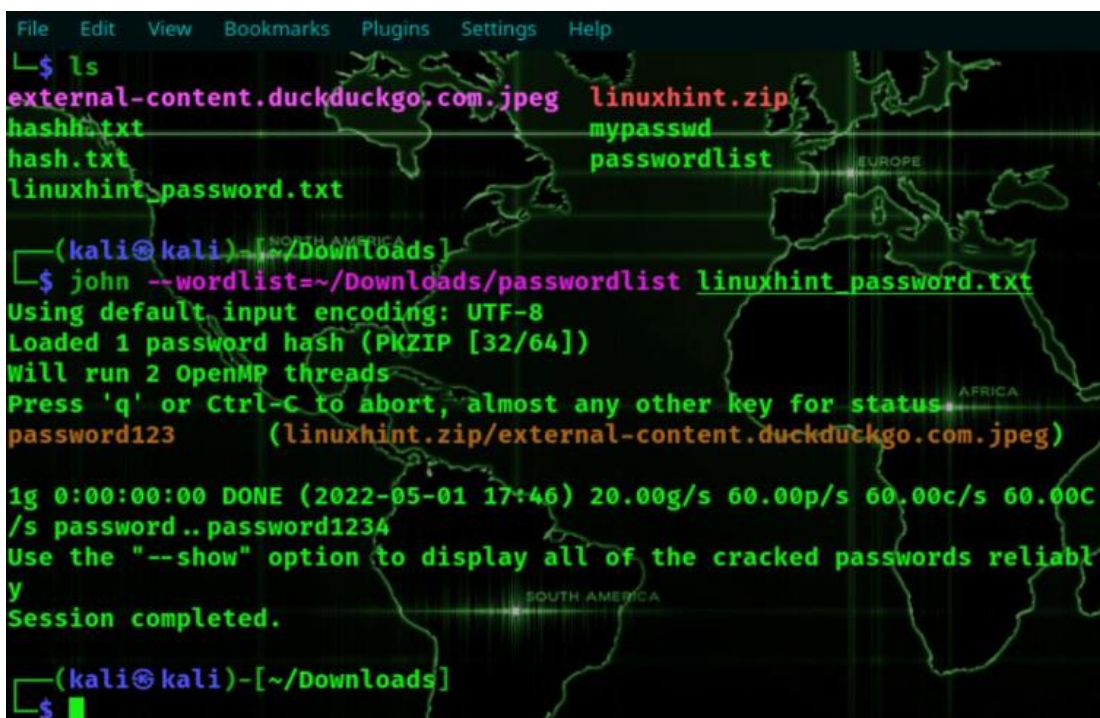


```
(kali@kali)-[~/Downloads]
$ zip2john linuxhint.zip > linuxhint_password.txt
ver 2.0 efh 5455 efh 7875 linuxhint.zip/external-content.duckduckgo.com
.jpeg PKZIP Encr: TS_chk, cmplen=1234252, decmplen=1286899, crc=384E1CA
3 ts=5181 cs=5181 type=8
(kali@kali)-[~/Downloads]
$
```

Fig 1.4 Storing the hash value of the zip file

Step 4:

Use the command **john --wordlist=~/.Downloads/passwordlist --format=Raw-MD5 hash.txt** to find the password.



```
File Edit View Bookmarks Plugins Settings Help
$ ls
external-content.duckduckgo.com.jpeg linuxhint.zip
hash.txt mypasswd
hash.txt passwordlist
linuxhint_password.txt
(kali@kali)-[~/Downloads]
$ john --wordlist=~/.Downloads/passwordlist linuxhint_password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (linuxhint.zip/external-content.duckduckgo.com.jpeg)
1g 0:00:00:00 DONE (2022-05-01 17:46) 20.00g/s 60.00p/s 60.00c/s 60.00C
/s password..password1234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(kali@kali)-[~/Downloads]
$
```

Fig 1.5 Cracking the password of the zip file

III. Using brute force method to crack MD5 hash.

PROCEDURE:

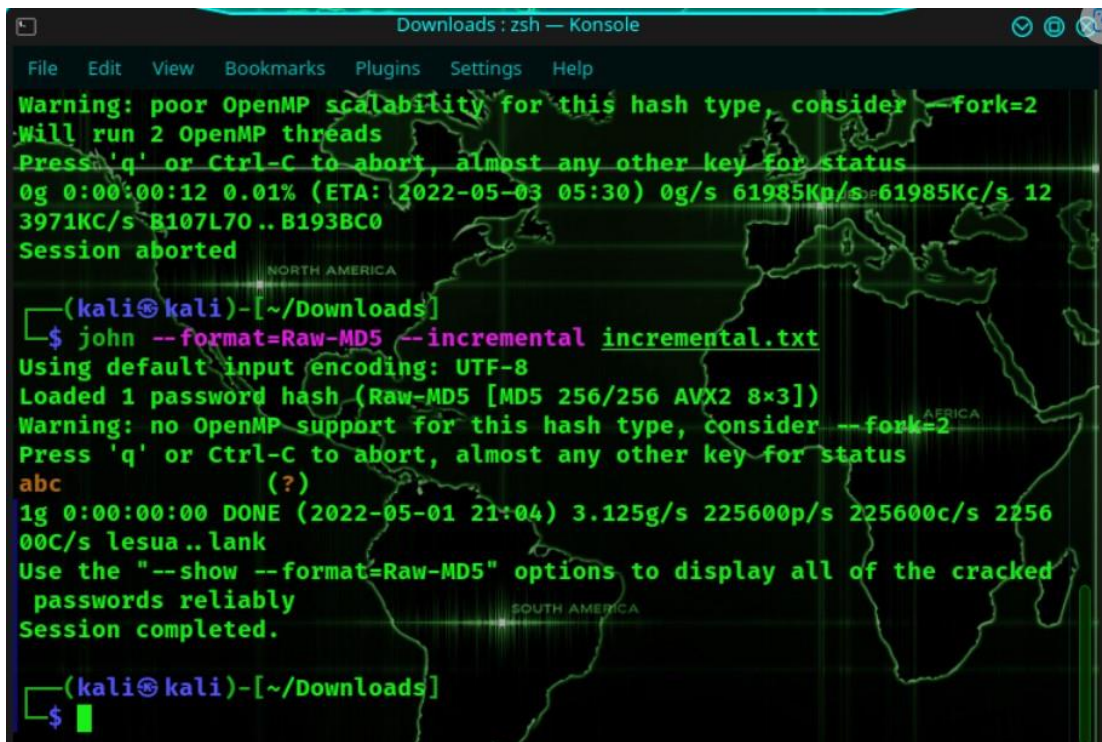
Step 1:

Store the hash value in a text file.

```
echo 900150983cd24fb0d6963f7d28e17f72 > incremental.txt
```

Step 2:

Finding the hash value using the brute force method.



```
Downloads : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:12 0.01% (ETA: 2022-05-03 05:30) 0g/s 61985Kp/s 61985Kc/s 12
3971KC/s B107L70..B193BC0
Session aborted
(kali@kali)-[~/Downloads]
$ john --format=Raw-MD5 --incremental incremental.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc (?)
1g 0:00:00:00 DONE (2022-05-01 21:04) 3.125g/s 225600p/s 225600c/s 2256
00C/s lesua..lank
Use the "--show --format=Raw-MD5" options to display all of the cracked
passwords reliably
Session completed.
(kali@kali)-[~/Downloads]
$
```

RESULT: The hash values of the password is cracked in various methods using the john the ripper tool.

EXPERIMENT 2

THE HARVESTER

theHarvester is a command-line tool included in Kali Linux that acts as a wrapper for a variety of search engines and is used to find email accounts, subdomain names, virtual hosts, open ports / banners, and employee names related to a domain from different public sources (such as search engines and PGP key servers). In recent versions, the authors added the capability of doing DNS brute force, reverse IP resolution, and Top-Level Domain (TLD) expansion.

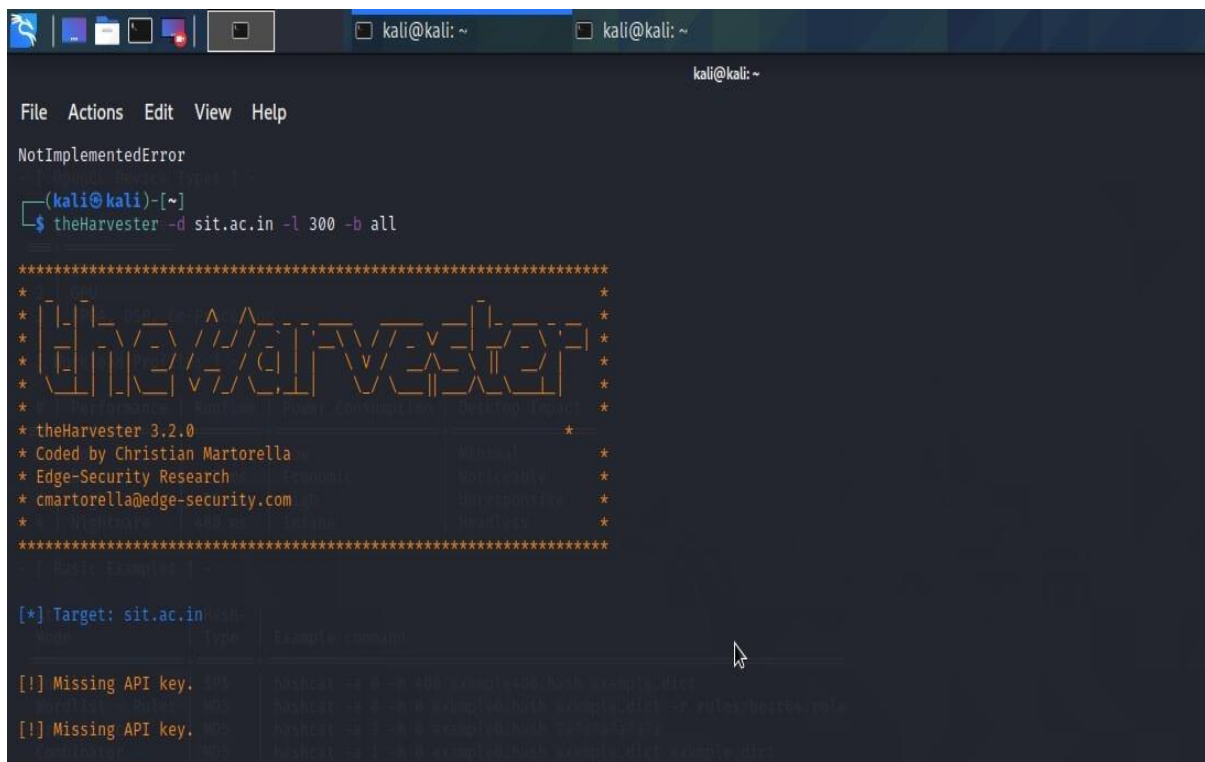
AIM: To Harvest the list of the Emails of an organization using Harvester tool.

TOOLS USED: The Harvester

PROCEDURE:

Step 1:

Open the kali linux terminal and type 'the harvester'.



```
File Actions Edit View Help
NotImplementedError
(kali@kali)-[~]
└─$ theHarvester -d sit.ac.in -l 300 -b all

*****
*                                     *
* [theHarvester]                     *
*                                     *
* theHarvester 3.2.0                  *
* Coded by Christian Martorella        *
* Edge-Security Research               *
* cmartorella@edge-security.com        *
*                                     *
*****

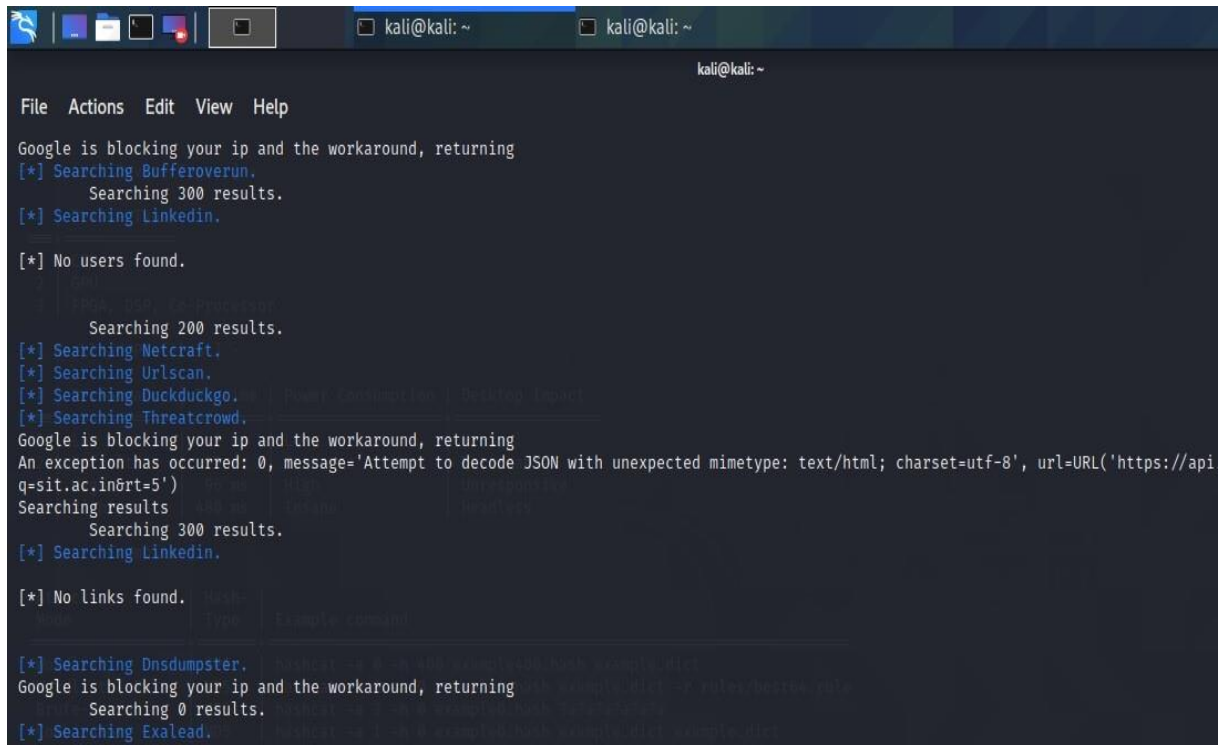
[*] Target: sit.ac.in
[*] Example command: theHarvester -d sit.ac.in -l 300 -b all

[!] Missing API key.
[!] Missing API key.
```

Fig 2.1 Open theHarvester on Kali Linux Terminal

Step 2:

Use the command **theHarvester -d sit.ac.in -l 300 -b google**



```

File Actions Edit View Help
Google is blocking your ip and the workaround, returning
[*] Searching Bufferoverrun.
    Searching 300 results.
[*] Searching Linkedin.

[*] No users found.

    IP: 139.226.237.74
    Searching 200 results.
[*] Searching Netcraft.
[*] Searching Urlscan.
[*] Searching Duckduckgo.
[*] Searching Threatcrowd.
Google is blocking your ip and the workaround, returning
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api
q=sit.ac.in&rt=5')
Searching results
    Searching 300 results.
[*] Searching Linkedin.

[*] No links found.
    Hash:
    Type: Example command

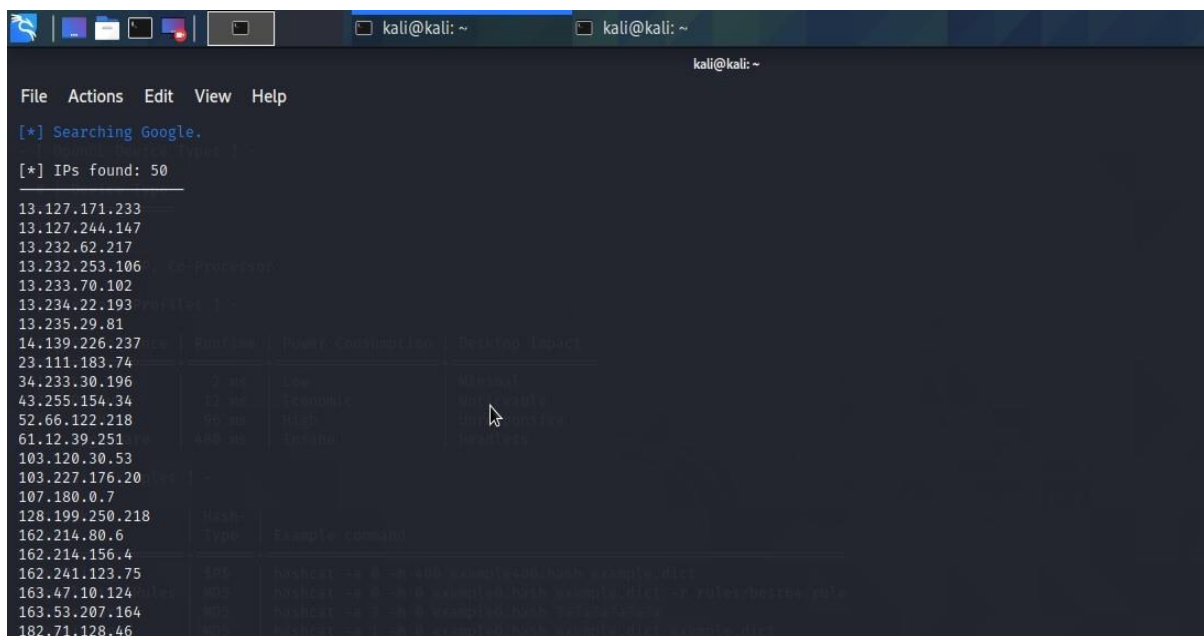
[*] Searching Dnsdumpster.
Google is blocking your ip and the workaround, returning
    Searching 0 results.
[*] Searching Exalead.

```

Fig 2.2 Searching for the result

Step 3:

Use the command **theHarvester -d sit.ac.in -l 300 -b all**



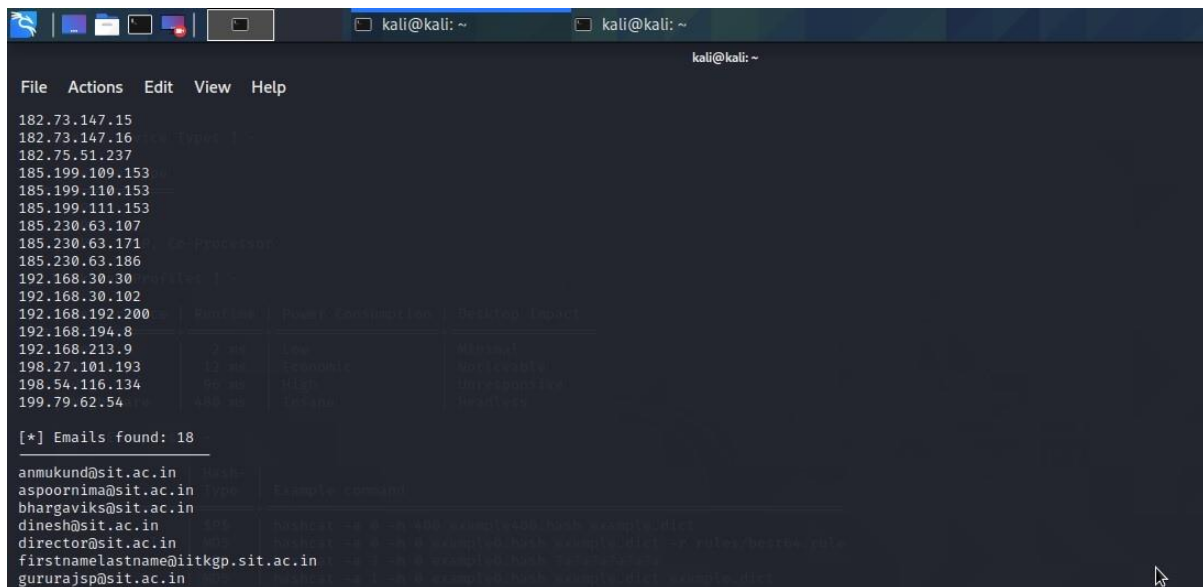
```

File Actions Edit View Help
[*] Searching Google.
    Searching 300 results.
[*] IPs found: 50

13.127.171.233
13.127.244.147
13.232.62.217
13.232.253.106
13.233.70.102
13.234.22.193
13.235.29.81
14.139.226.237
23.111.183.74
34.233.30.196
43.255.154.34
52.66.122.218
61.12.39.251
103.120.30.53
103.227.176.20
107.180.0.7
128.199.250.218
162.214.80.6
162.214.156.4
162.241.123.75
163.47.10.124
163.53.207.164
182.71.128.46

```

Fig 2.3 Display the Ips



```
File Actions Edit View Help
182.73.147.15
182.73.147.16
182.75.51.237
185.199.109.153
185.199.110.153
185.199.111.153
185.230.63.107
185.230.63.171
185.230.63.186
192.168.30.30
192.168.30.102
192.168.192.200
192.168.194.8
192.168.213.9
198.27.101.193
198.54.116.134
199.79.62.54

[*] Emails found: 18
anmukund@sit.ac.in
aspoornima@sit.ac.in
bhargaviks@sit.ac.in
dinesh@sit.ac.in
director@sit.ac.in
firstnamelastname@iitkgp.sit.ac.in
gururajsp@sit.ac.in
```

Fig 2.4 Display the Emails

RESULT: The list of Emails is harvested from the targeted organization which can belater used for the social engineering attacks.

EXPERIMENT 3

HTTRACK

HTTrack is a free and open-source Web crawler and offline browser, developed by Xavier Roche and licensed under the GNU General Public License Version 3. HTTrack allows users to download World Wide Web sites from the Internet to a local computer.

AIM: Website mirroring using HTTRACK.

TOOLS USED: HTTRACK

PROCEDURE:

Step 1:

Choose a project name and destination folder.

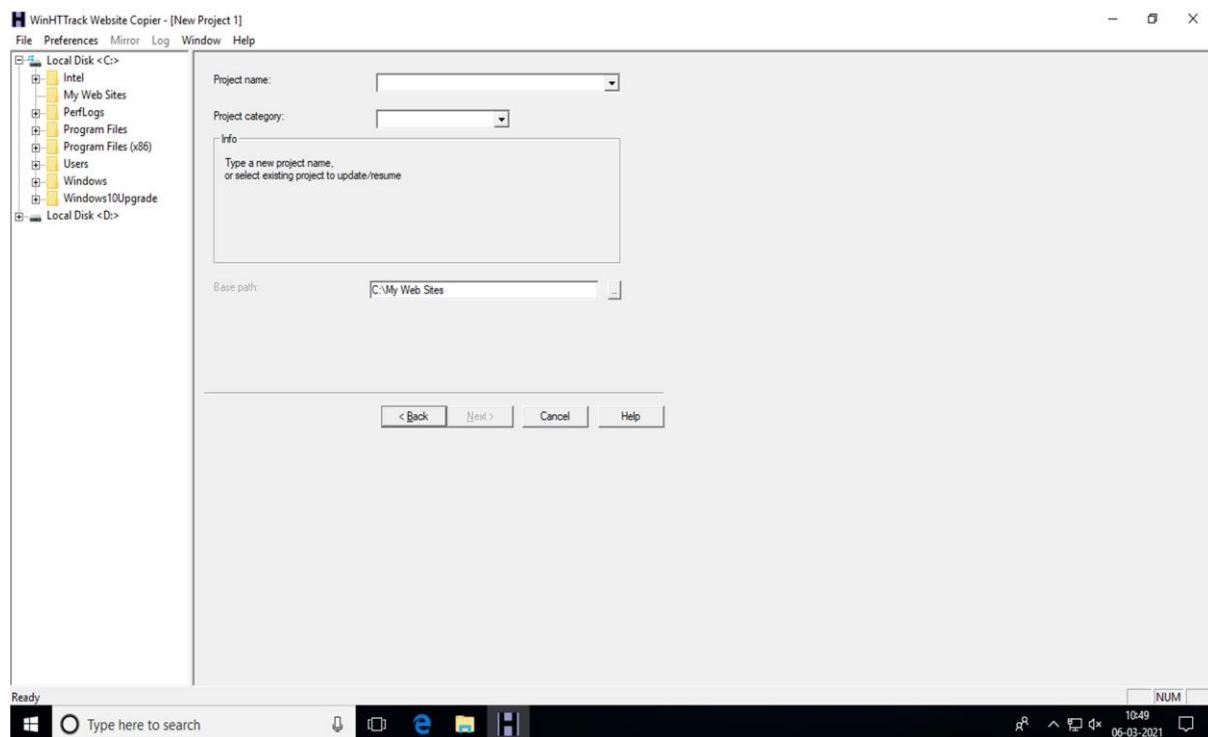


Fig 3.1 Choosing project name and destination folder

Step 2:

Paste the URL of the website to be mirrored.

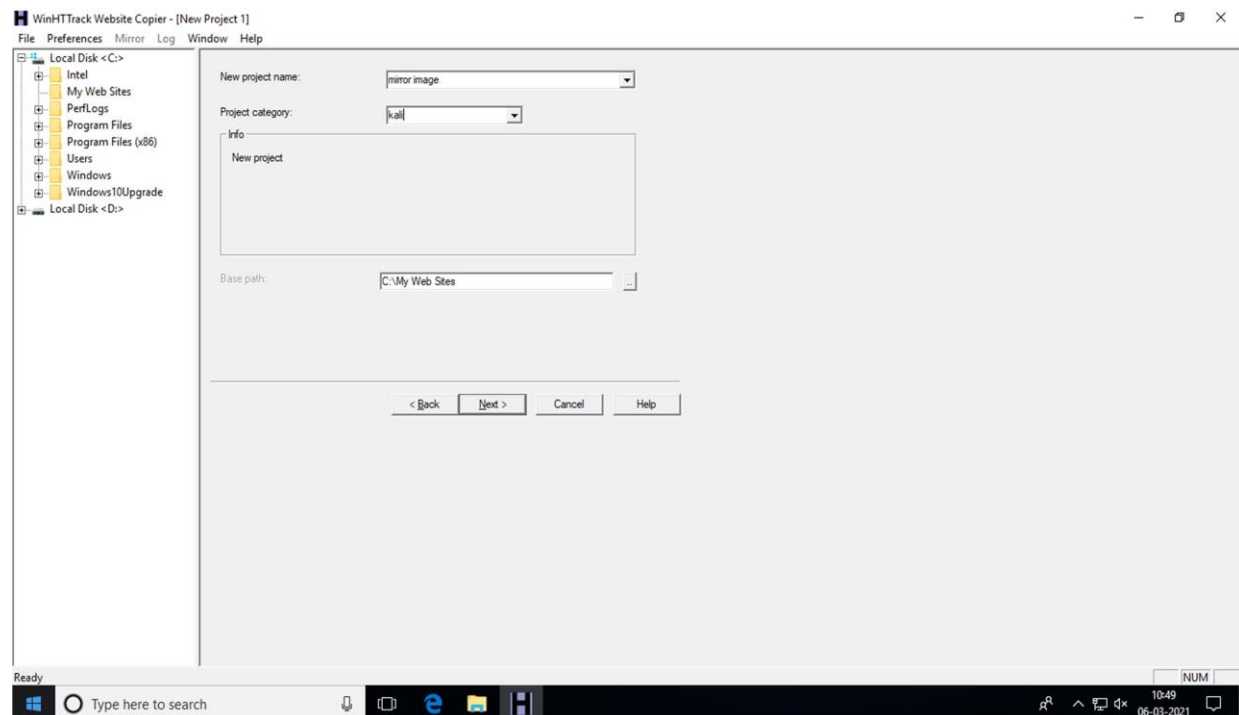


Fig 3.2 Fill the address of the website to be mirrored

Step 3: Start the mirroring process.

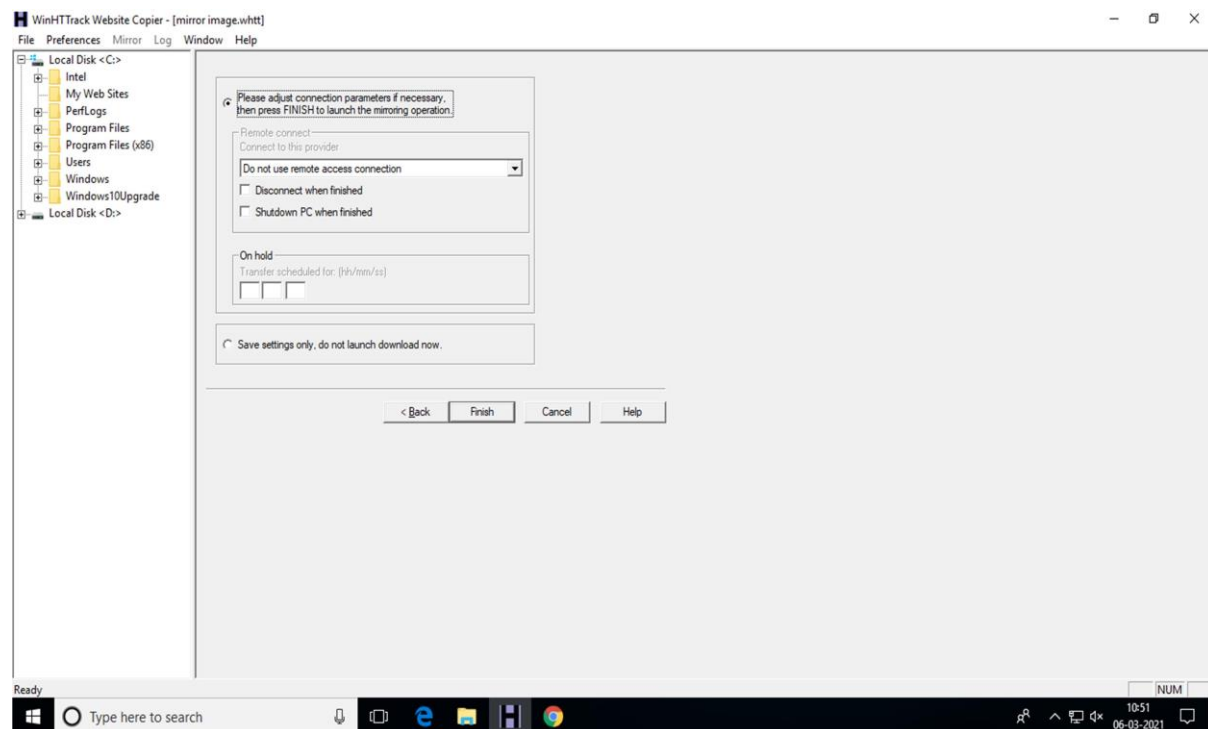


Fig 3.3 HTTrack is ready to mirror

Step 4:

Wait- User can cancel the mirror at any time or cancel the files currently downloaded.

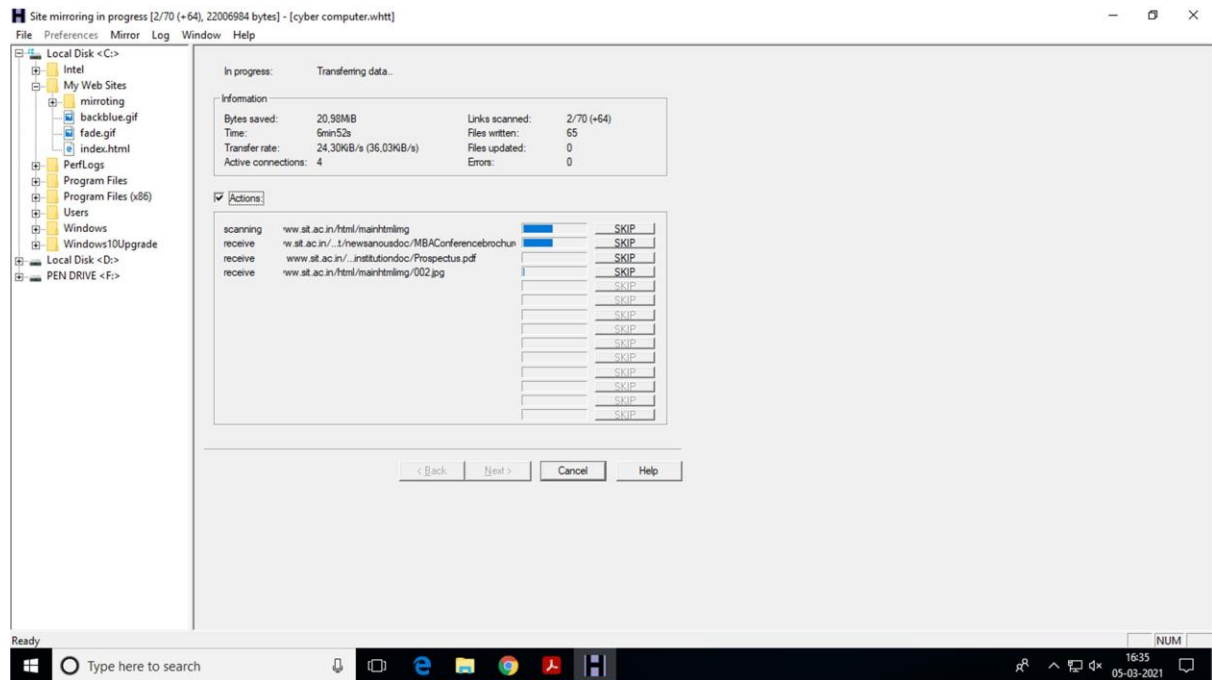


Fig 3.4 HTTrack starts mirroring

Step 5:

View the mirrored website.

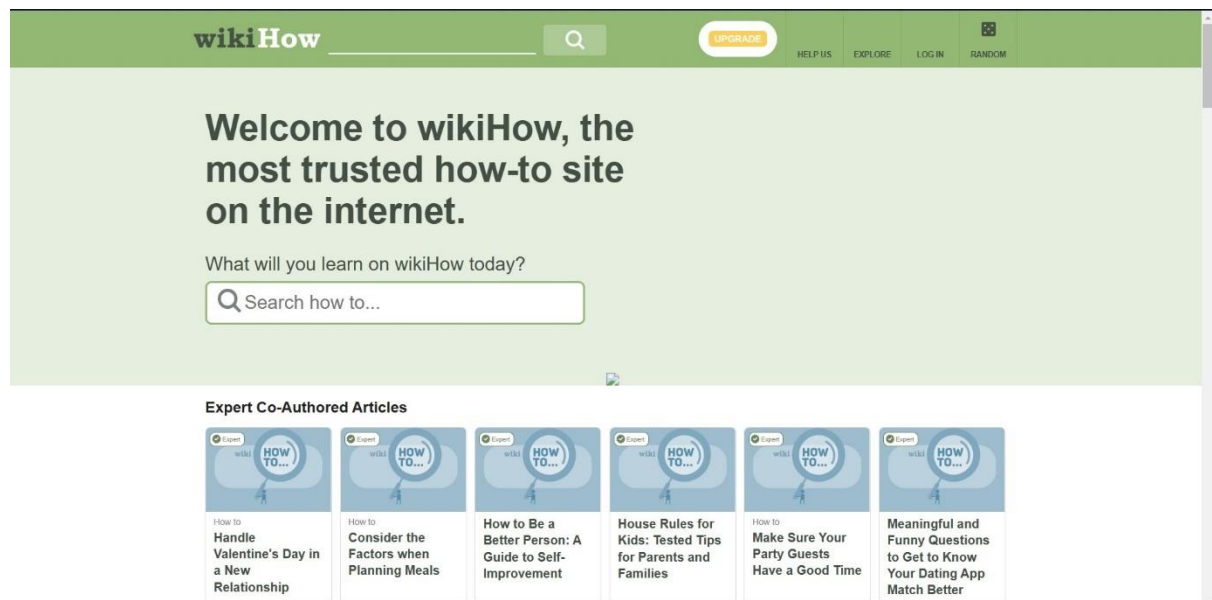


Fig 3.5 View of the Mirrored Website

RESULT: A mirror of a website has been created with the help of a tool HTTrack.

EXPERIMENT 4

LAST ACTIVITY OF THE PC

LastActivityView is a tool for Windows operating system that collects information from various sources on a running system, display a log of actions made by the user and the events occurred on this computer.

The activity displayed by LastActivityView includes: Running.exe file, opening open/save dialog-box, Opening file/folder from Explorer or other system, software installation, system shutdown/start, application or system crash, network connection/disconnection.

AIM: Display latest activities of the system

TOOLS USED: LastActivityView

PROCEDURE:

After running LastActivityView, it scans your computer and displays all actions and events found on your system.

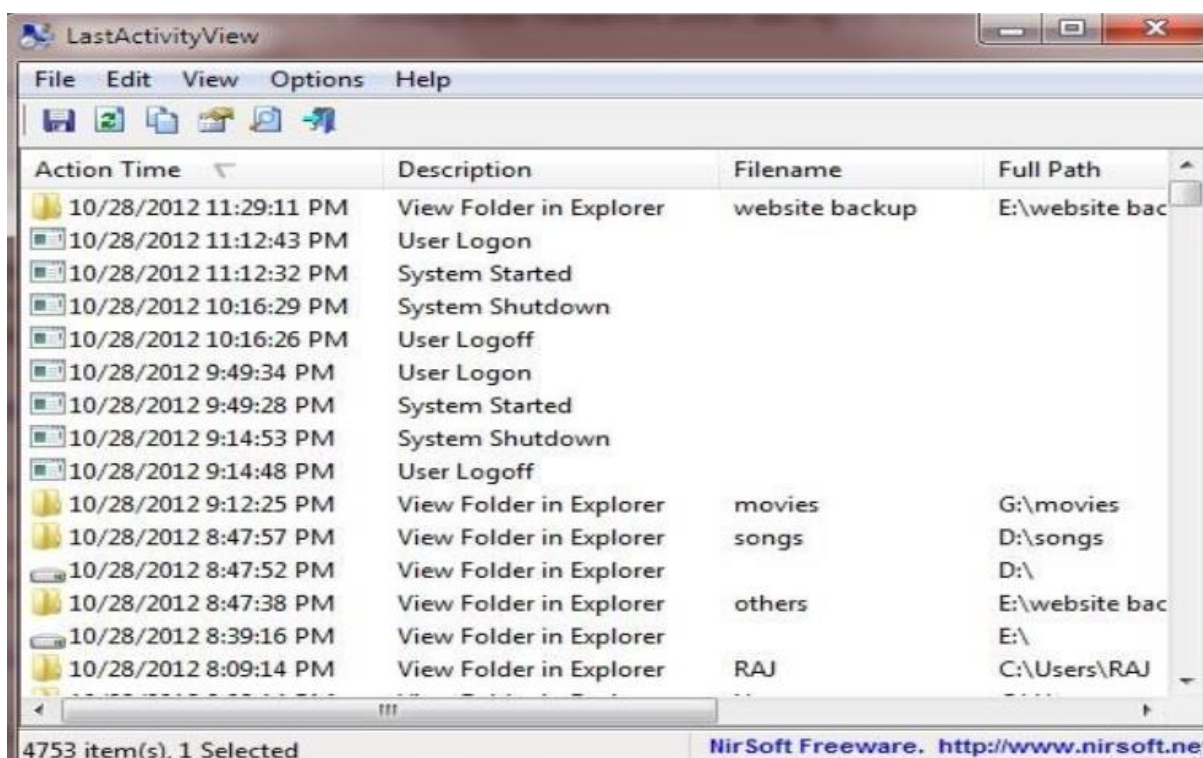


Fig 4.1 List of all actions and events found on the system

EXPERIMENT 5

USBDEVIEW

USBDeview is a small utility that lists all USB devices that currently connected to your computer, as well as all USB devices that you previously used.

For each USB device, extended information is displayed: Device name/description, device type, serial number (for mass storage devices), the date/time that device was added, VendorID, ProductID, and more.

AIM: Find the currently connected and previously connected USB devices.

TOOLS USED: USBDeview

PROCEDURE:

After running USBDeview, it scans the system's USB ports and displays the currently connected and previously connected devices.














Device Na...	Description	Device Type	Safe...	Conne...	Last Plug/Unplug ...	VendorID
 Nokia 7210 Supern...	Nokia 7210 Supern...	Communication	No	No	7/26/2011 5:49:04 ...	0421
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 8:54:29 PM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 8:54:27 PM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 8:54:26 PM	12d1
 0000.001d.00...	USB Mass Storage ...	Mass Storage	Yes	No	8/1/2011 8:54:23 PM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/5/2011 9:44:46 AM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/5/2011 9:44:46 AM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/5/2011 9:44:46 AM	12d1
 0000.001d.00...	USB Mass Storage ...	Mass Storage	Yes	No	8/5/2011 9:44:46 AM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 9:59:58 AM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 9:59:58 AM	12d1
 0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 9:59:58 AM	12d1
 0000.001d.00...	USB Mass Storage ...	Mass Storage	Yes	No	8/1/2011 9:59:58 AM	12d1

Fig 5.1 Displaying the list of USB devices

EXPERIMENT 6

WORKING OF AUTOPSY

An autopsy is a surgical procedure that consists of a thorough examination of a corpse by dissection to determine the cause, mode, and manner of death; or the exam may be performed to evaluate any disease or injury that may be present for research or educational purposes.

AIM: Live forensics case investigation using Autopsy

TOOLS USED: Autopsy

PROCEDURE:

Step 1:

Open Kali Linux OS using VMware or Oracle VirtualBox

Step 2:

Download the img file for file analysis from the link: [JPEG Search Test #1 \(sourceforge.net\)](https://sourceforge.net/projects/jpegsearchtest/).

Extract the zip file and change the extension of the .dd file to .img to analyze in autopsy.

Step 3:

Open Autopsy on Kali Linux

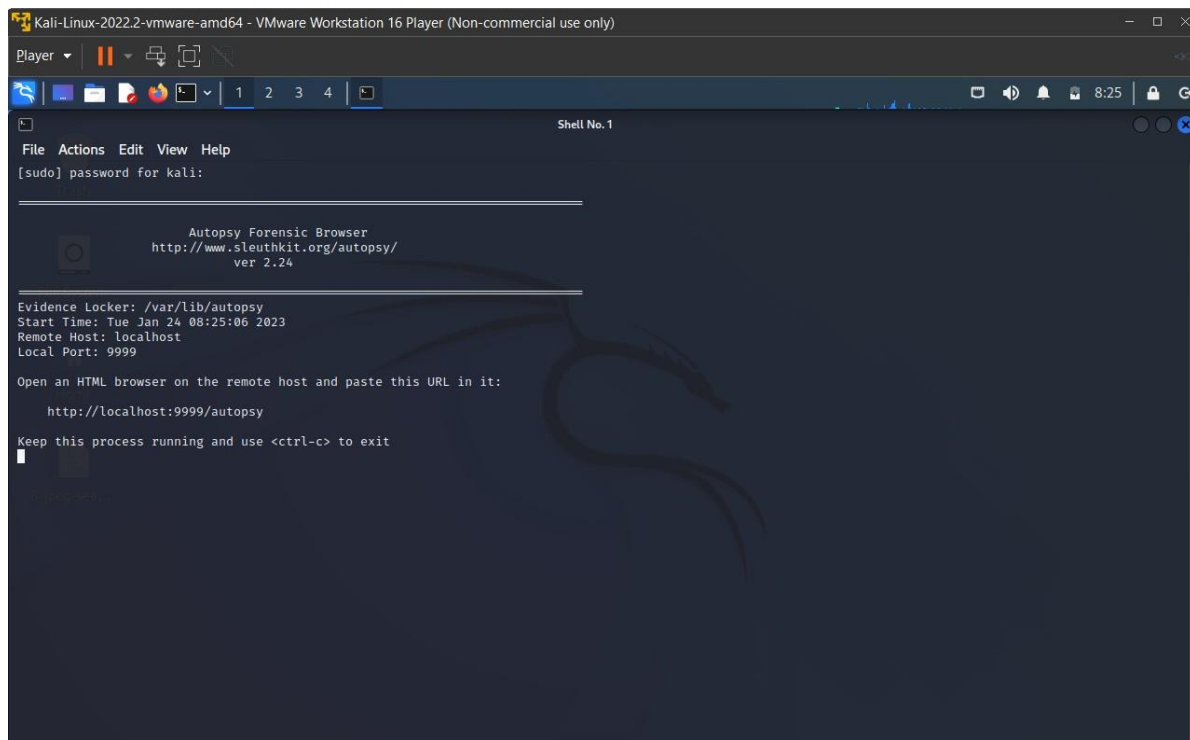


Fig 6.1 Opening Autopsy on Kali Linux

Step 4:

Click on the local host link to open the Graphical User Interface (GUI).

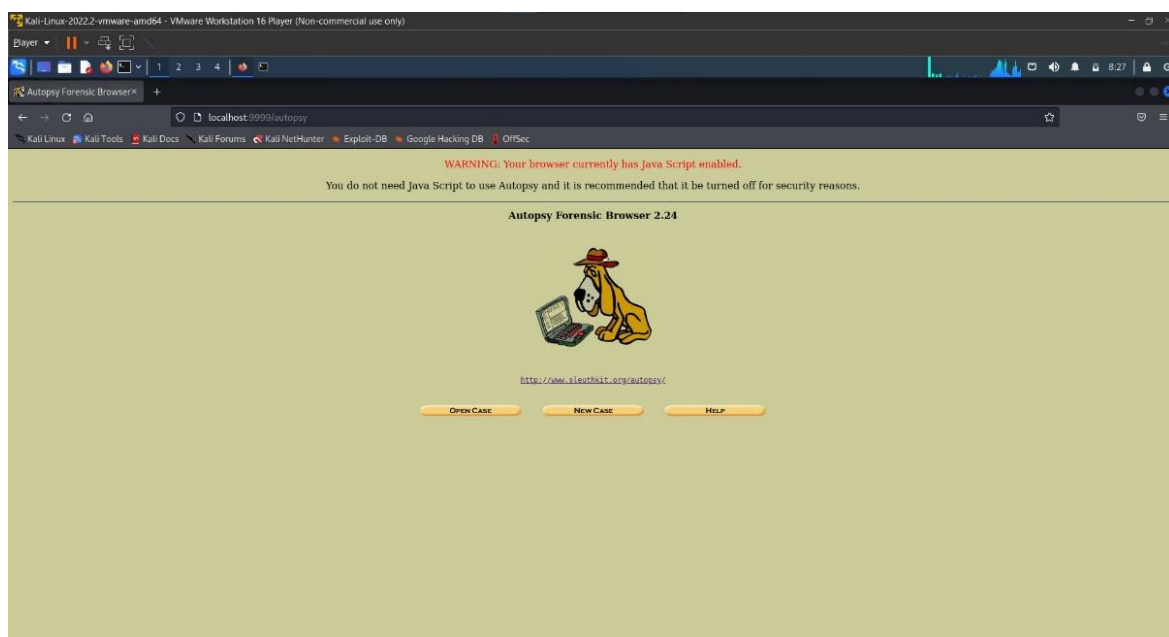


Fig. 6.2 Graphical User Interface

Step 5:

Click on the New Case button on the interface.

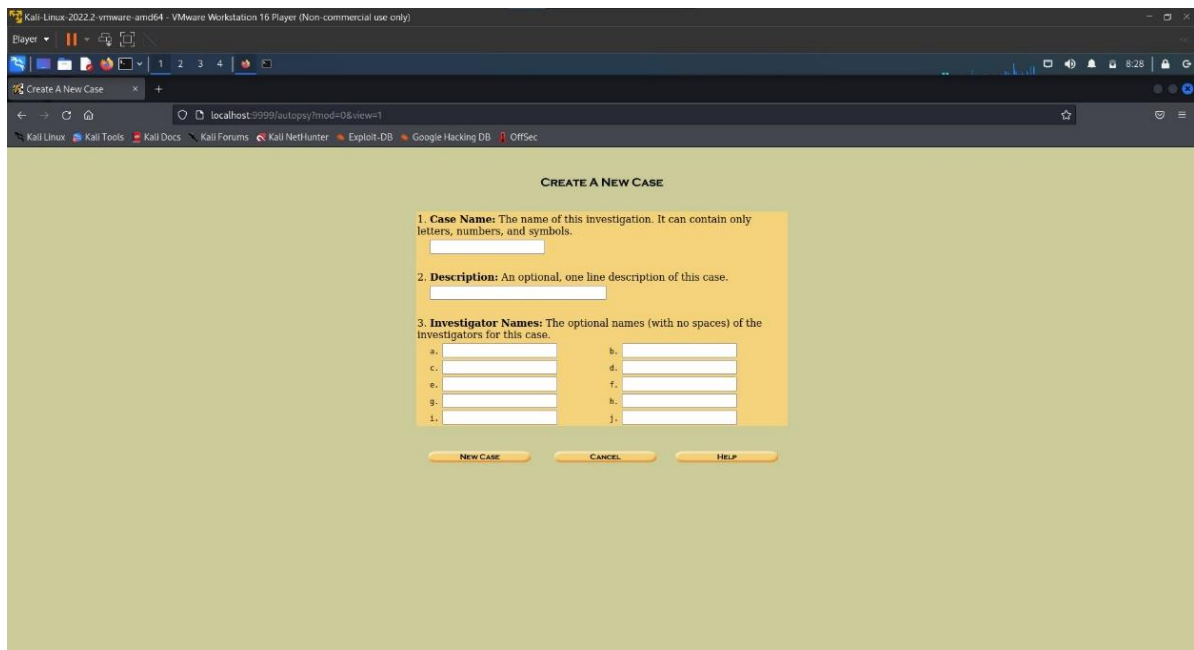


Fig. 6.3 New Case on Autopsy

Step 6:

Enter the case name without spaces in case number along with the Invigilator names who can work on the case. After entering the details, click on new case.

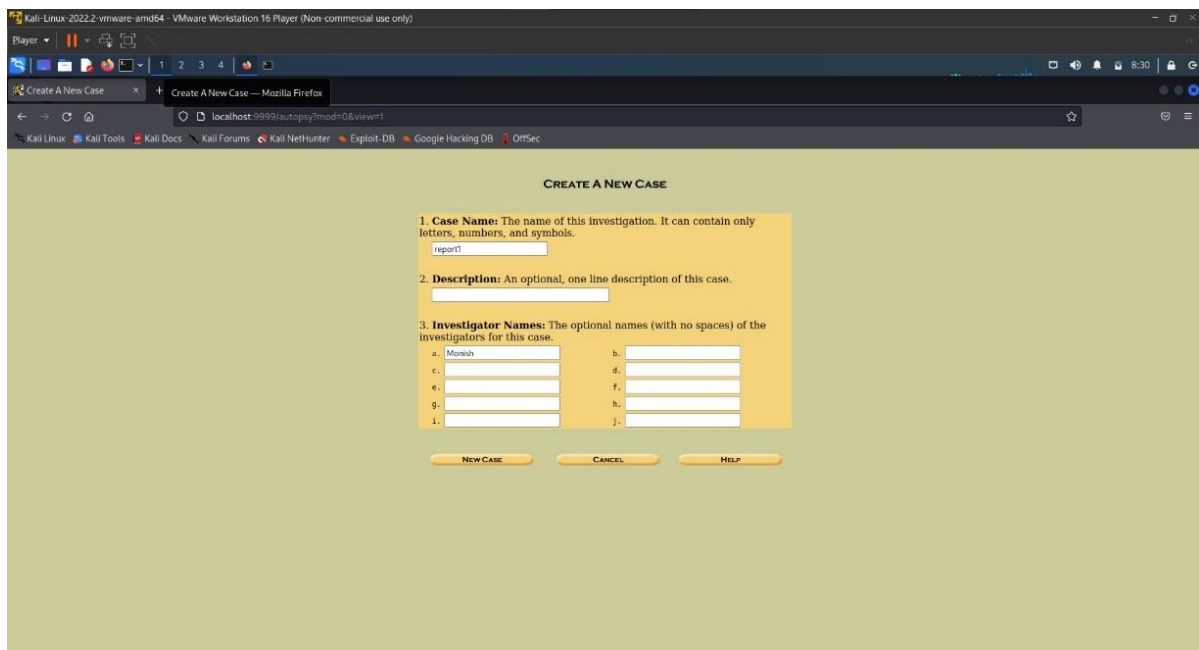


Fig. 6.4 Entering the Host and Case Details

Step 7:

Click on the investigator's name who is working on the case and click on Add Host

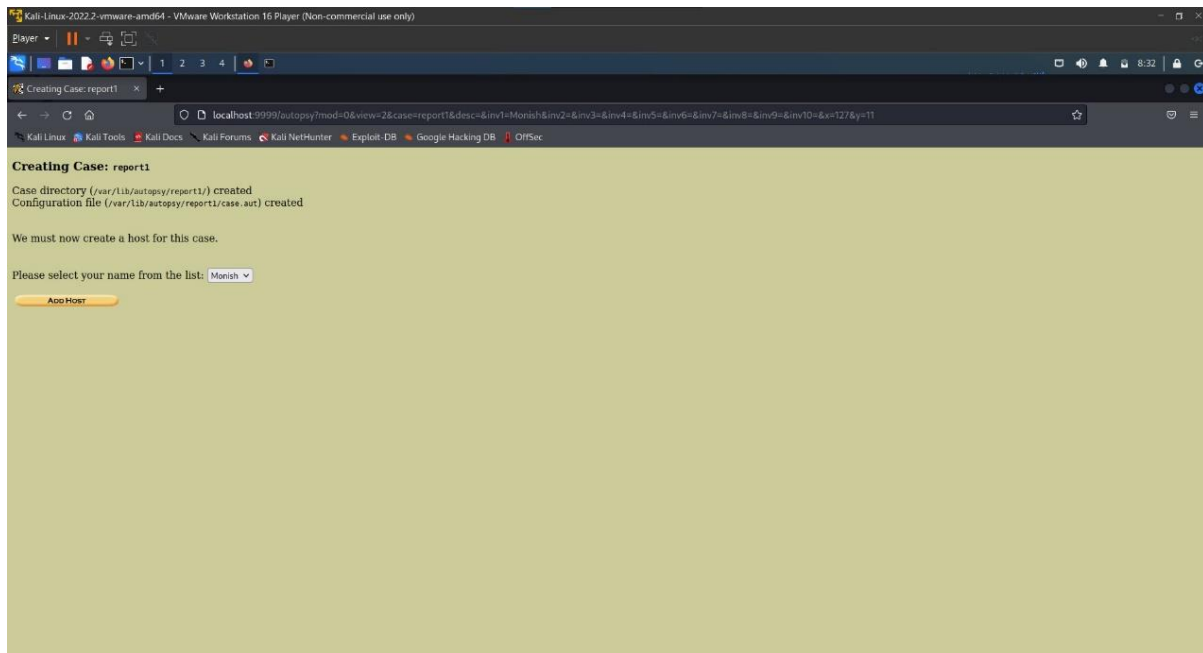


Fig 6.5 Adding the host

Step 8:

To import the img file, click on add image.

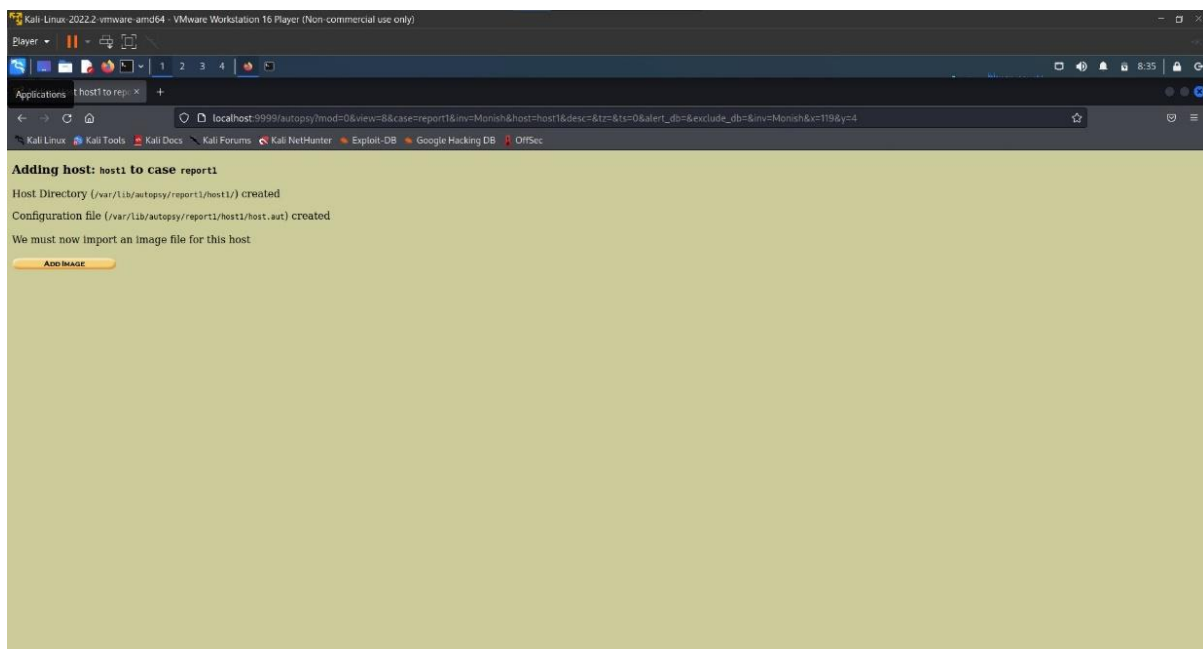


Fig. 6.6 Step 1 to adding the image file

Step 9:

On the next page, click on add new image.

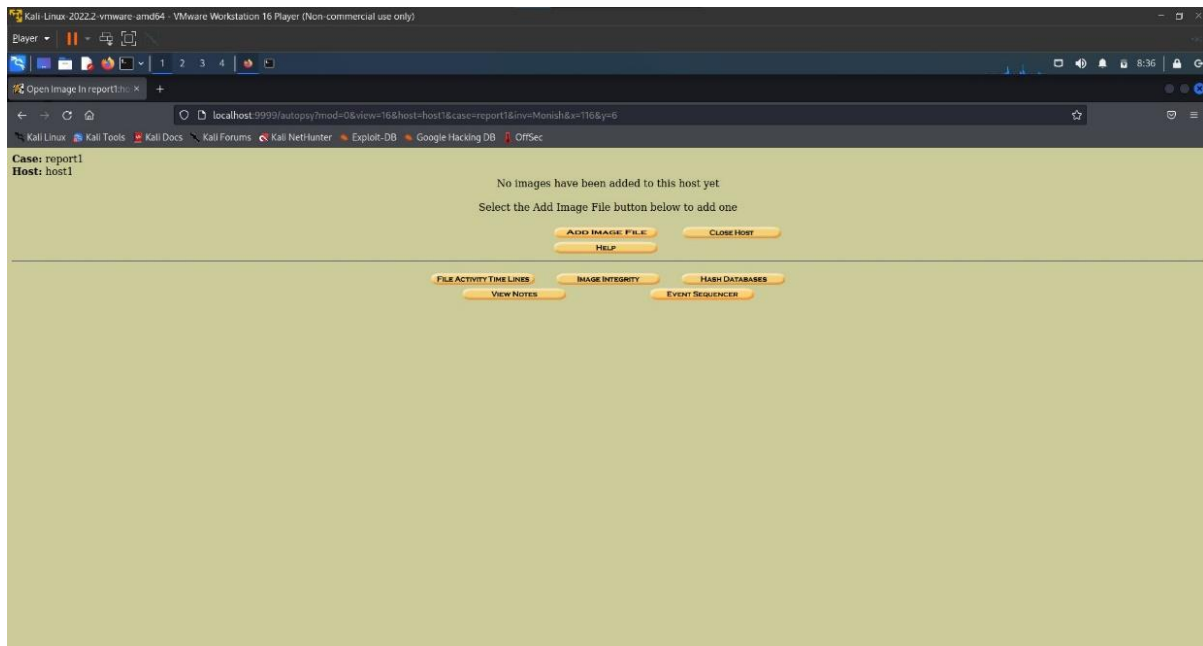


Fig 6.7 Step 2 to adding the image file

Step 10:

Add the location of the img file, choose that the file is a partition and take a copy of the img file as the input method.

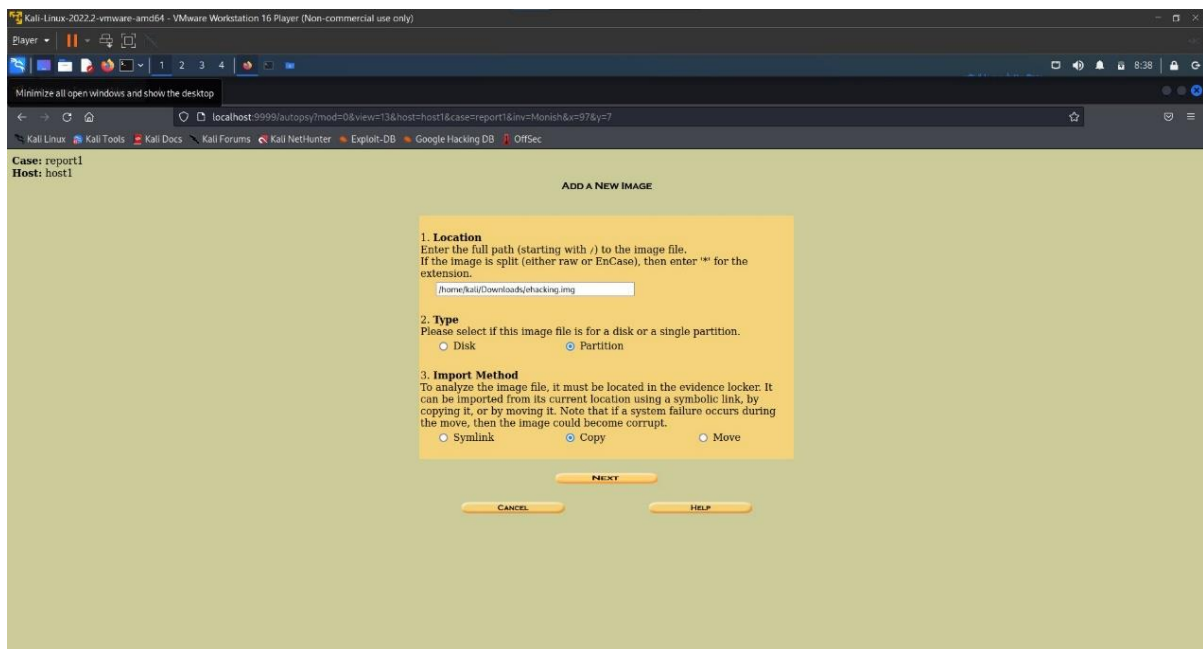


Fig. 6.8 Adding the image path and choosing import method

Step 11:

On the next page, we can calculate the hash value for the image and must ensure that the File System Type is ntfs.

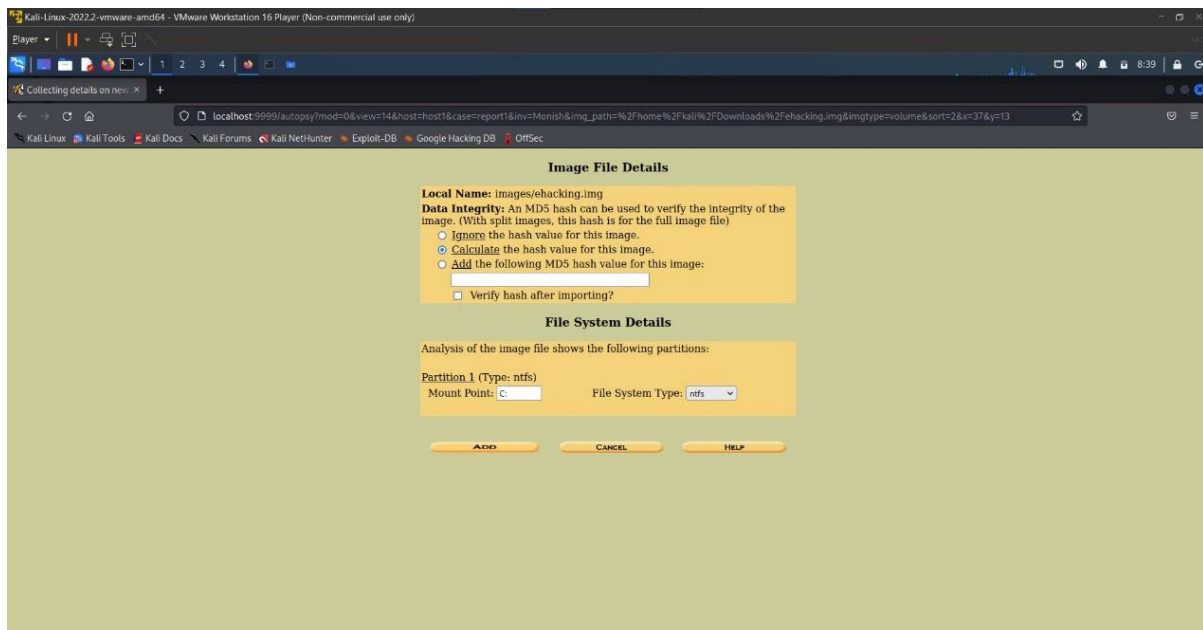


Fig. 6.9 Calculating the hash value

Step 12:

Upon clicking add, the calculated hash value.

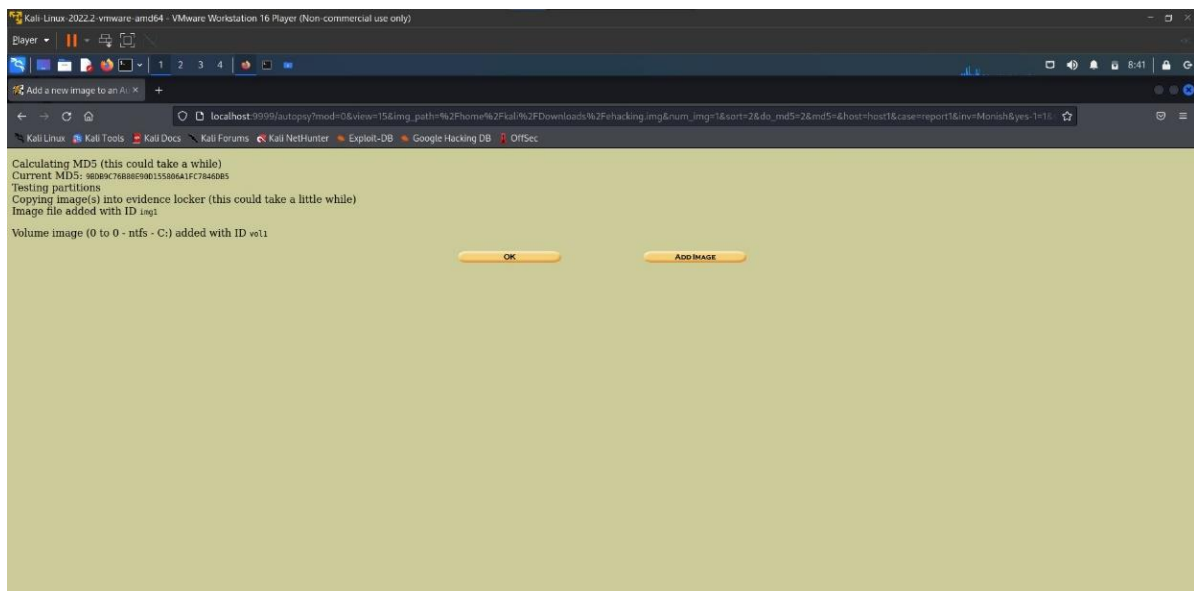


Fig. 6.10 Calculated hash value

Step 13:

Upon clicking ok, click the option to analyze the input.

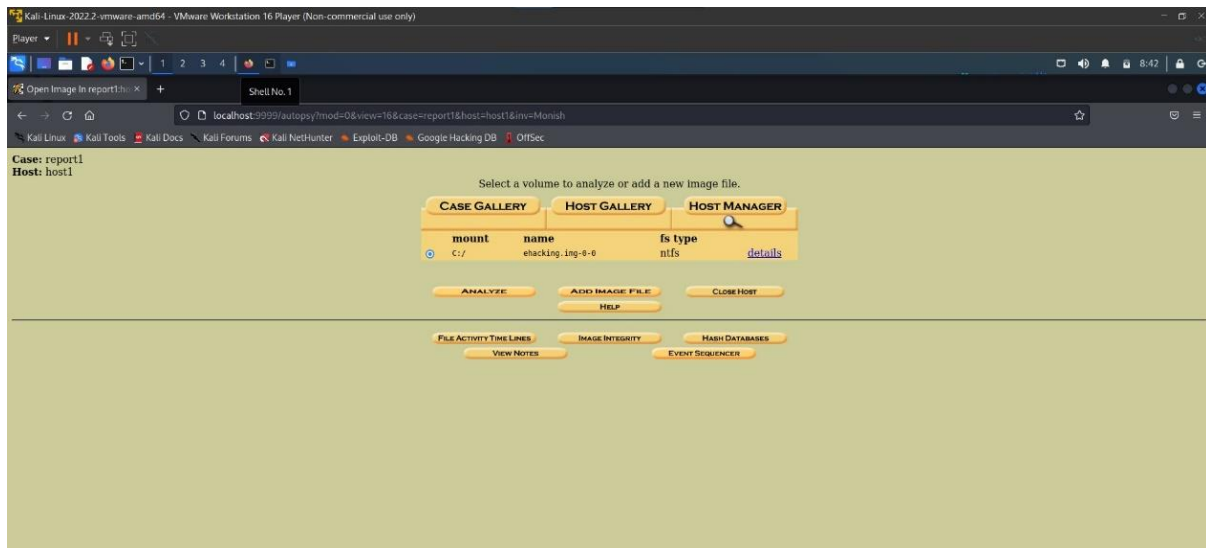


Fig. 6.11 Step 1 to file analysis

Step 14:

Click analyze and File analysis, the user will get a detailed analysis of input file.

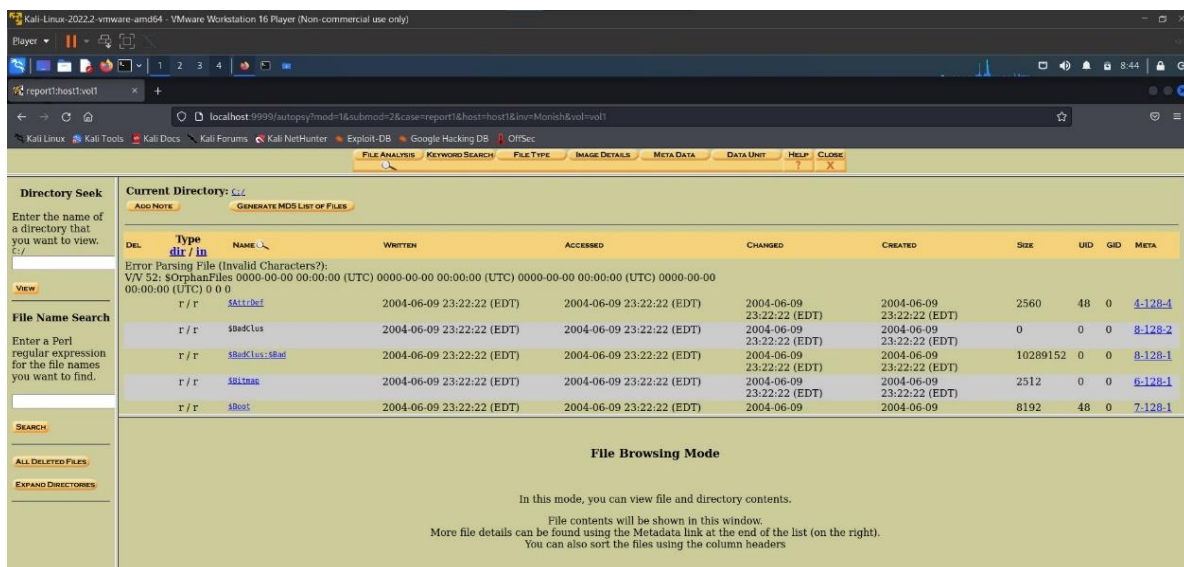


Fig. 6.12 Output to file analysis

RESULT: A detailed file analysis is performed on the copy of the input img file.

EXPERIMENT 7

CREATING EVIDENCE IMAGE

FTK imager is a data preview and imaging file that lets you quickly access electronic evidence to determine if further analysis with a forensic tool such as Forensic ToolKit is warranted. Create forensic images of hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places in the media. FTK imager can create perfect copies, or forensic images of computer data without making changes to the original evidence. FTKImager can be used to verify that the image hash and the drive hash match after the image is created, and that the image has remained unchanged since acquisition.

AIM: To create evidence image of a drive

TOOLS USED: FTKImager

PROCEDURE:

Step1:

Partition the drive.

- **Win + R** > type **diskmgmt.msc**. Disk management is displayed.
- If unallocated space is available, right click on it and select '**New Simple Partition**' > **Next**. Set partition size (256MB or less), drive letter, file system > **finish**.
- If unallocated space is not available, right click on the partition to shrink and select '**Shrink Volume**'. Confirm shrink and follow the previous step for the new unallocated space created.

Step 2:

Creating the evidence image.

- Install FTKImager from Access Data > [FTK Imager - Exterro](#).
- Open FTKImager. The FTKImager dashboard is displayed.
- In the menu navigation bar > File > Create Disk Image

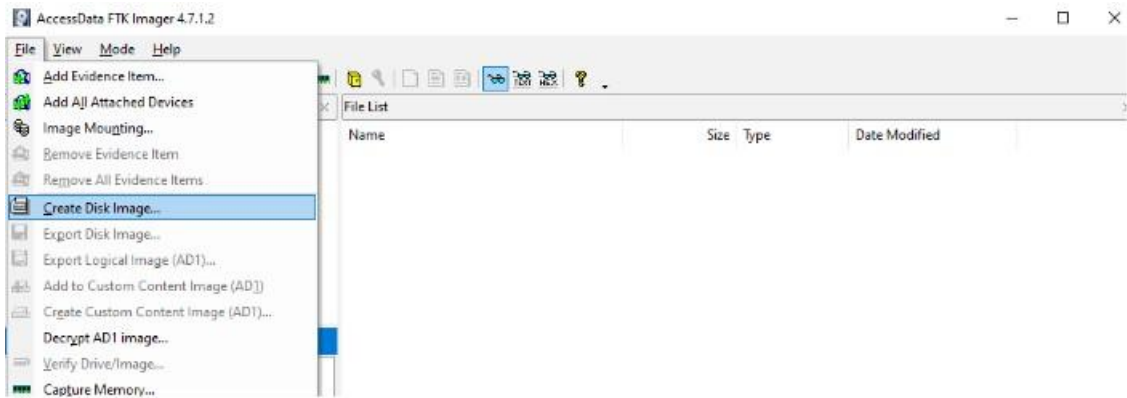


Fig 7.1 Menu access to creating the disk image

- As we are using local disk, select logical drive as the source of evidence type > Next

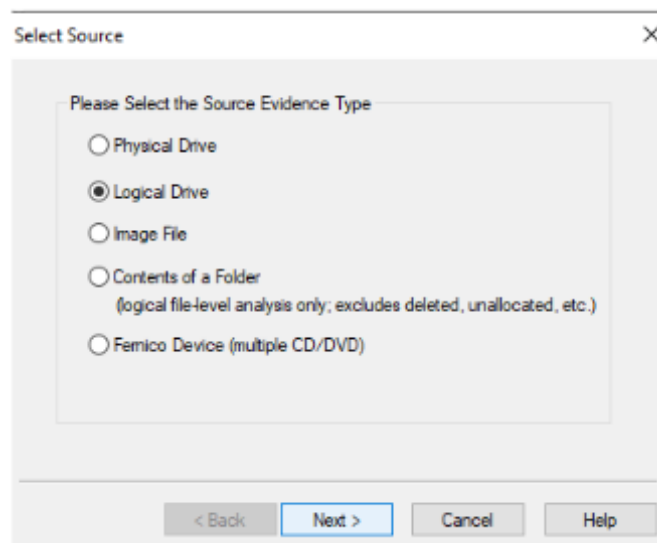


Fig. 7.2 Source Selection

- Select source drive > finish.

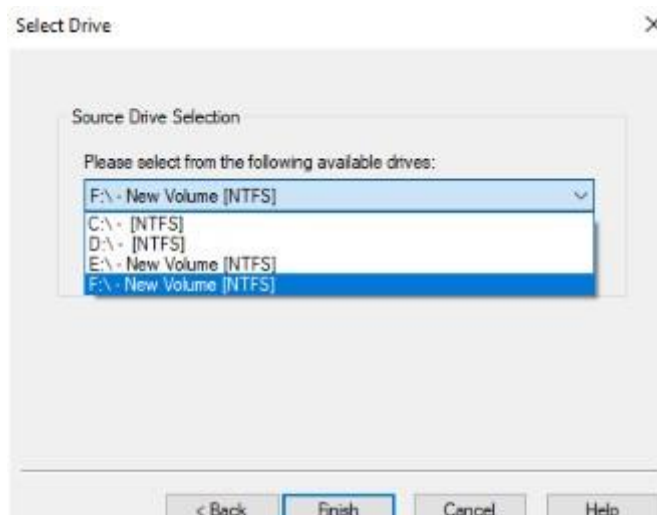


Fig. 7.3 Source drive selection

- Click the add button for the image destination. Select the type of the forensics image that must be created. Here, Raw(dd) > Next is selected.

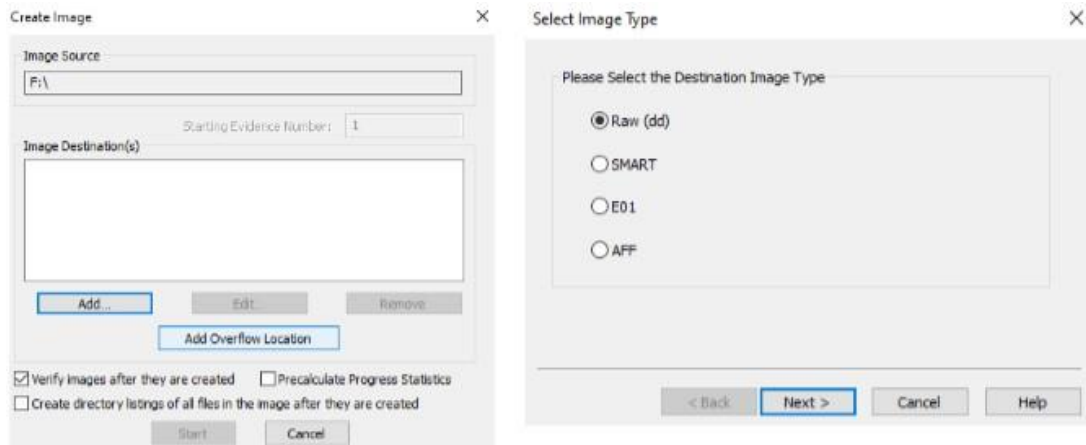


Fig. 7.4 Creating the image and selecting the type

- Choose the destination for the image and a name for the image, followed by finish. Select verify image > Start.

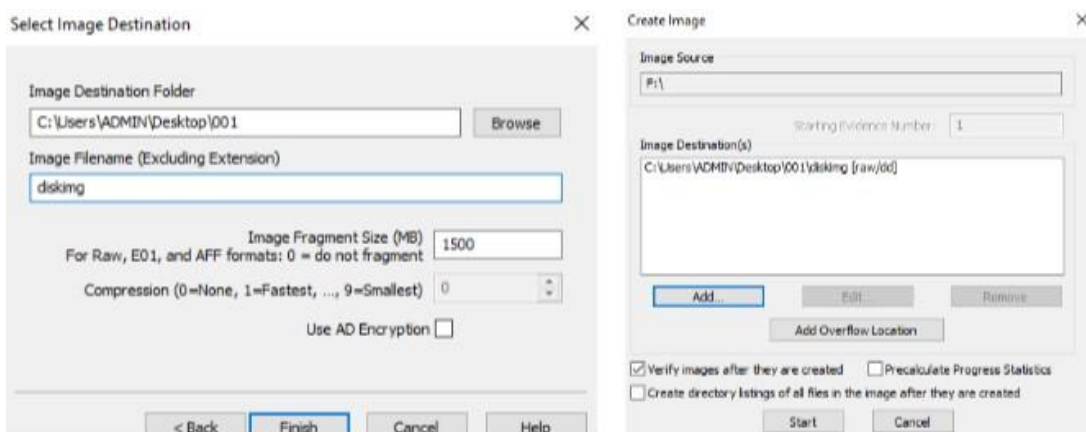


Fig. 7.5 Selecting image destination and creating the image

- If the MD5 hash and SHA1 hash has match status, the image is created accurate to the drive.

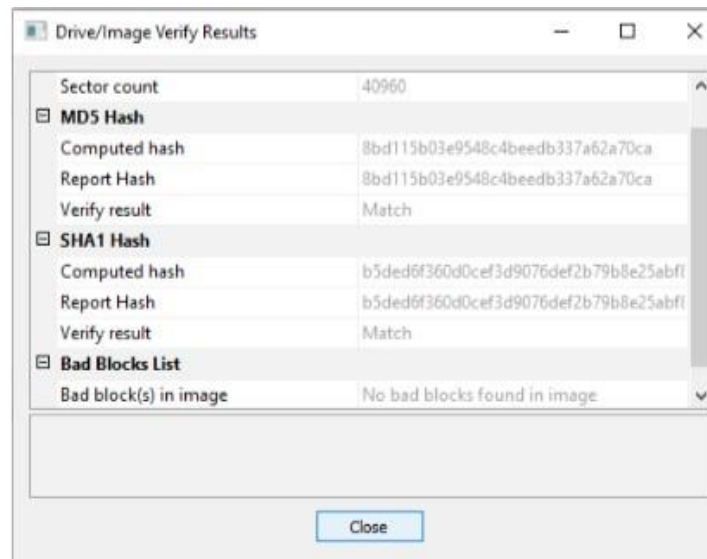


Fig. 7.6 MD5 and SHA1 match status

RESULT: Image of the drive is created using FTKImager.

EXPERIMENT 8

RECOVERING A DRIVE FROM AN EVIDENCE IMAGE

FTK imager is a data preview and imaging file that lets you quickly access electronic evidence to determine if further analysis with a forensic tool such as Forensic ToolKit is warranted. Create forensic images of hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places in the media. FTK imager can create perfect copies, or forensic images of computer data without making changes to the original evidence.

AIM: To recover a drive from its evidence image.

TOOLS USED: FTKImager

PROCEDURE:

Step 1:

Open FTKImager. FTKImager dashboard displayed.

Step 2:

In menu navigation bar > File > Image Mounting

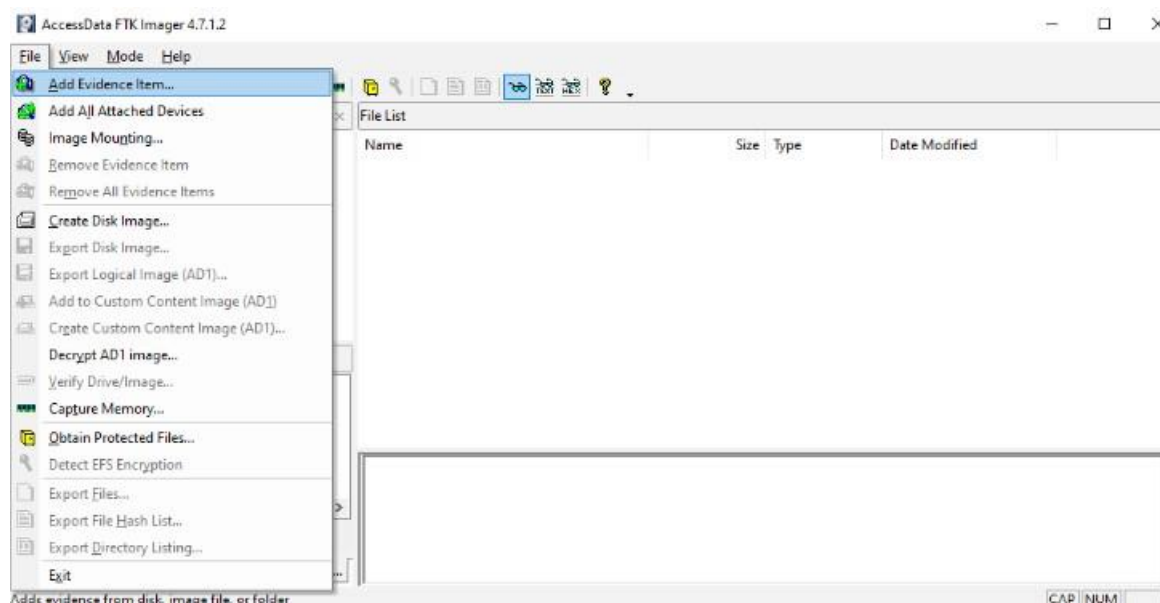


Fig. 8.1 Mounting the Image

Step 3:

Browse the image (select zip or rar file) > Mount

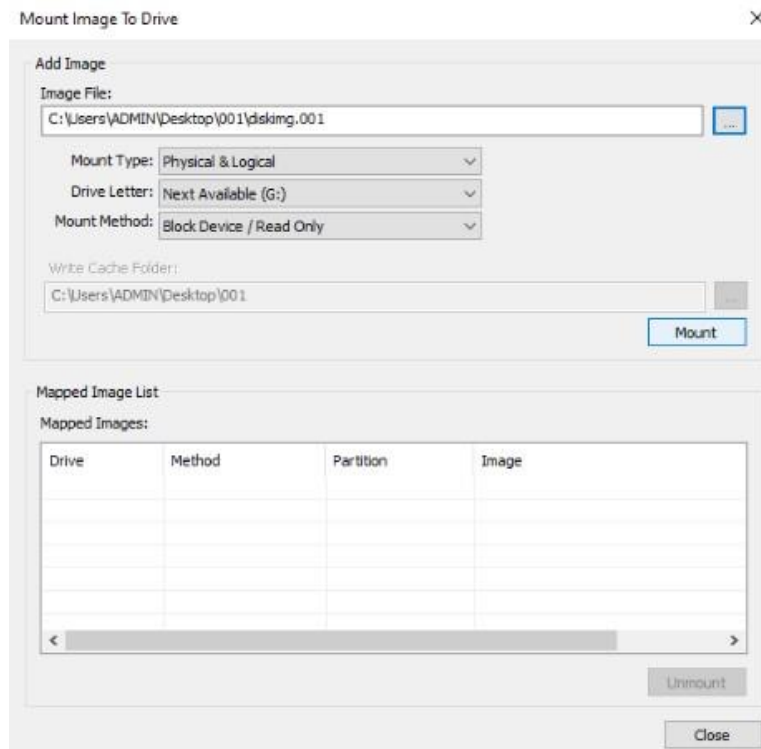


Fig. 8.2 Mounting the image to drive

Step 4:

A new drive is temporarily mounted in your system. This drive consists of data from the evidence image and can be recovered.

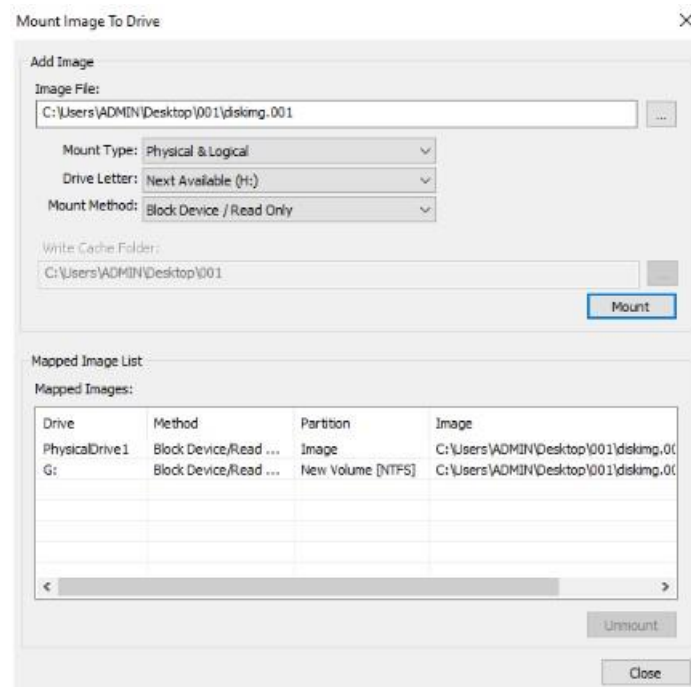


Fig. 8.3 Disk Recovery

RESULT: Disk is recovered from the evidence image.

EXPERIMENT 9

HIDING TEXT DATA IN AN IMAGE FILE

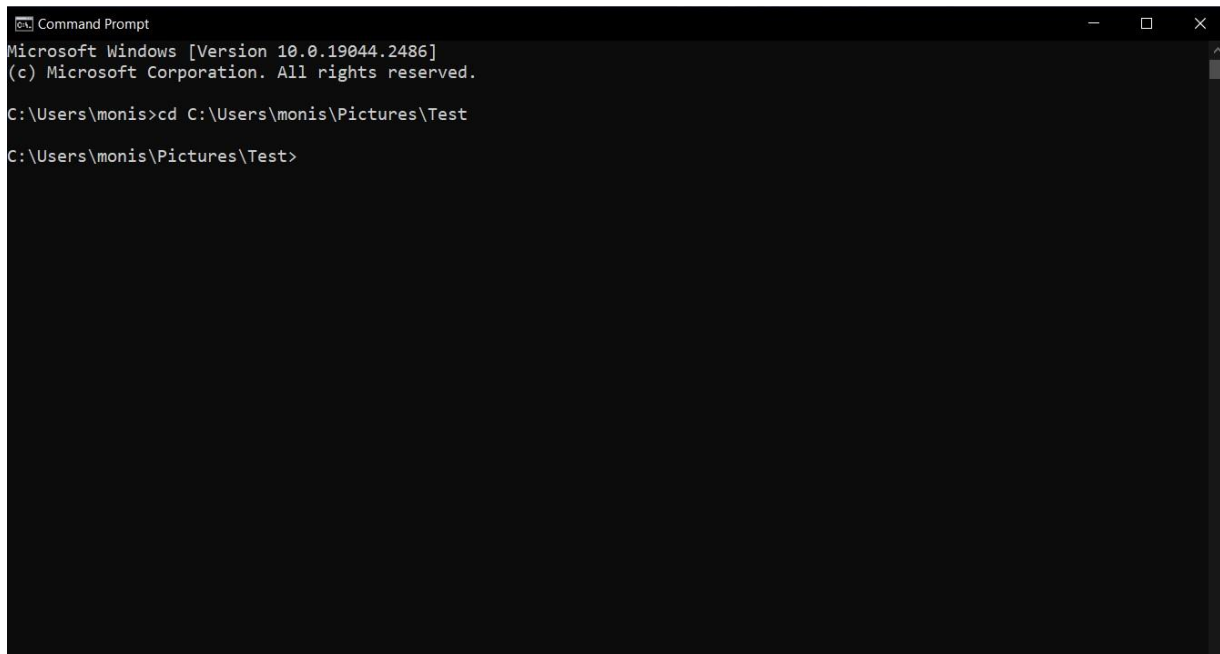
AIM: To hide the data of a text file in an image (png or jpg) file.

TOOLS USED: Command Prompt

PROCEDURE:

Step 1:

Open command prompt and change the directory to the folder in which the image and the text file are available.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.19044.2486] (c) Microsoft Corporation. All rights reserved. C:\Users\monis>cd C:\Users\monis\Pictures\Test C:\Users\monis\Pictures\Test>". The background is black and the text is white.

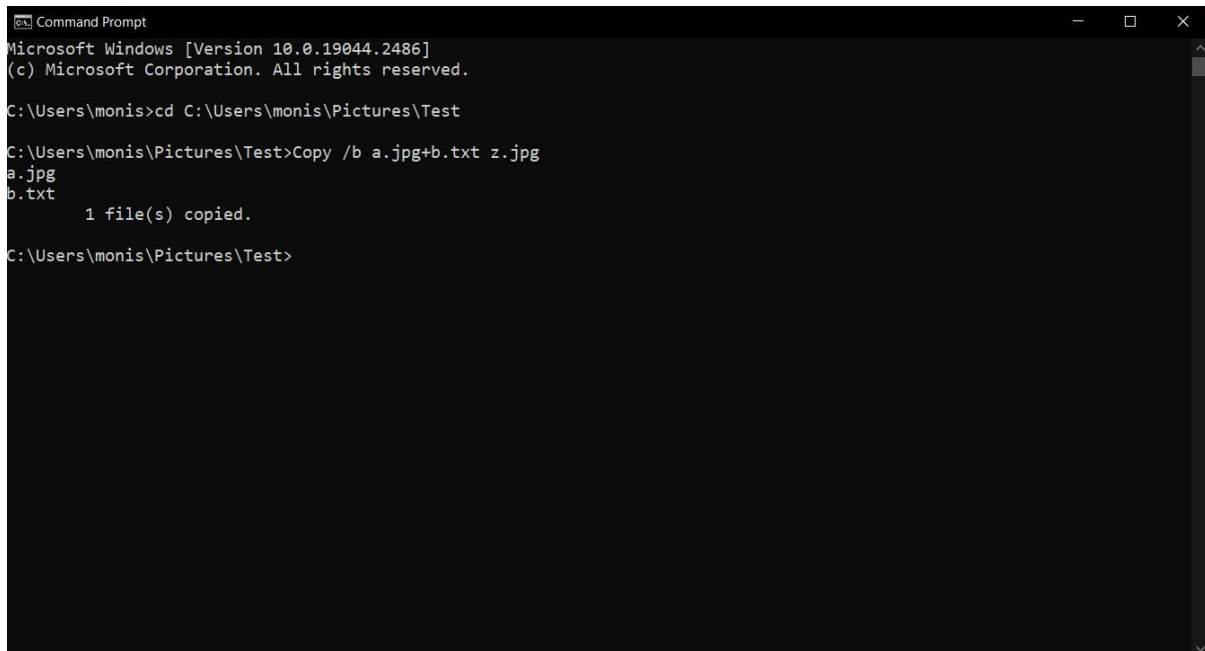
```
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\monis>cd C:\Users\monis\Pictures\Test
C:\Users\monis\Pictures\Test>
```

Fig. 9.1 Changing command prompt directory

Step 2:

Considering the image file is stored as a.jpg and the text file is stored as b.txt, use the following command to hide the data in the image and create a new copy of the image.



```
Command Prompt
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\monis>cd C:\Users\monis\Pictures\Test

C:\Users\monis\Pictures\Test>Copy /b a.jpg+b.txt z.jpg
a.jpg
b.txt
1 file(s) copied.

C:\Users\monis\Pictures\Test>
```

Fig. 9.2 Hiding the data

Step 3:

Open the new image file using notepad to view the hidden data.

```

z.jpg - Notepad
File Edit Format View Help

Ë“[+¼’ÿÆzÙóœ,½ä†¹Æ”·Š+p(üãç[]8C% .♣1,,S []&Zx`%:ÕÀ@íÄBèã[]%f#Ëžð*[]ó-^†ûÄ-€!

^½dÔE¹rDó.../aÝÀ^a;ÈŽ@Î1Ri$Â^úÓ‘W·W‘Ä@†Dó-[]'Bňgj#_±óŠ*îÓ-[]<,--Î5Eœ[]€&--“p[]
28 Û%[]U×Xf€uî[]”0%[]Rë[]~·(+[]R^9dÁ«®      Îñ€°°,,-c5Ûç
"$ùÈ~~À´9,B%1“X#|` )R-v£[]{}[]»[])8|â£°eiÊ& []q,,[]]`
'=[~ó%·ã6mÖ[]Ú<u€[]‘ç[]êd†-[]%v™^:ñŠ†%†ñ"•õž,,q[Šç$Ž0`4váz`<.0mãønor@šj8i-b
]Î0û[]%j†ð>DZnÃ[]4      š^...ã[]"ÆG\~ì%$,,•  `yø;eñSTÁÈ]çxC[]ÆÎ[]âç(ÔF%:’š$XèÁy

â$Ã[]RyÄ[]Jpà[]b\...!’ ’      q4’ à-²f¥AÂM[]%†g[]@<ñL  æ†8Á$þ3Sç  ii%Ôk[]£0ìè[]ó‘  ó%I
;[]ê)’ ♣[]ç[]³5[]c’ÆfCC- UQÃD+q!vb±dÅ[]p™UM, ÎÛPÚ![]
A>'YK[]v¹[]çœ°•Û’[]ëY«&·Æ)küb^^0[]´<³[]Qn(:ã0übĐå      Æ[]...±@L[]m~ñasCYÏY^œ[]

:[]i[]+ÆHa†ð  Èa`[]%^æ♣[]¥Ph-*/ç7[]øÆ[]V`Q[]`P-y@l:~NP@[]Á«...HI1r
-;5,,[]4,ì·(šÖn|ó€Fc[]`Še~:Äòp"pë[]#>;ÏÿÜHiding data in an image
  
```

Fig. 9.3 Viewing the hidden data

RESULT: The data of the text file is hidden in the image.

EXPERIMENT 10

WIRESHARK

AIM: Monitor live network capturing packets and analyzing over the live network.

TOOLS USED: Wireshark

PROCEDURE:

Wireshark is free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. It allows the user to put network interface controllers that support promiscuous mode into that mode, in order to see all traffic visible on the interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all of the traffic travelling through the switch will necessarily be sent to the port on which the capture is being done, so capturing in promiscuous mode will not necessarily be sufficient to see all traffic on the network.

- 1) Select the interface that needs to be analyzed.

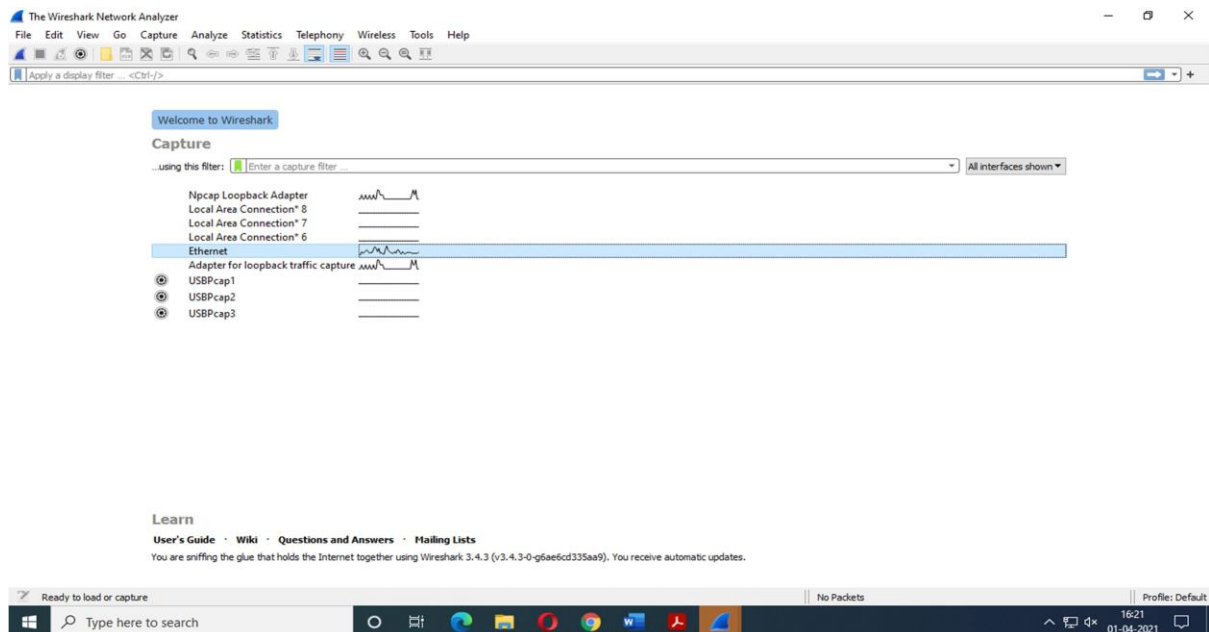


Fig .1.1 Interface Selection

2) Click start and the packet start getting captured.

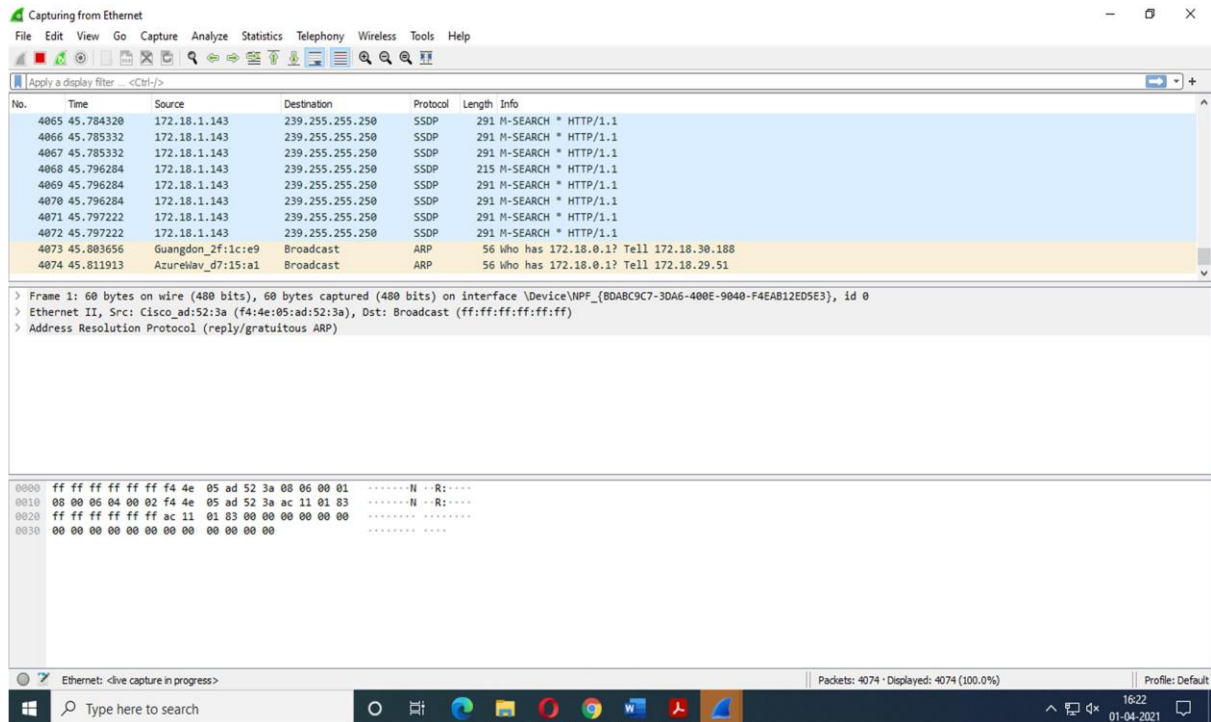


Fig 1.2 Packet Capturing

3) Other options include Stop, Restart and Capture filters

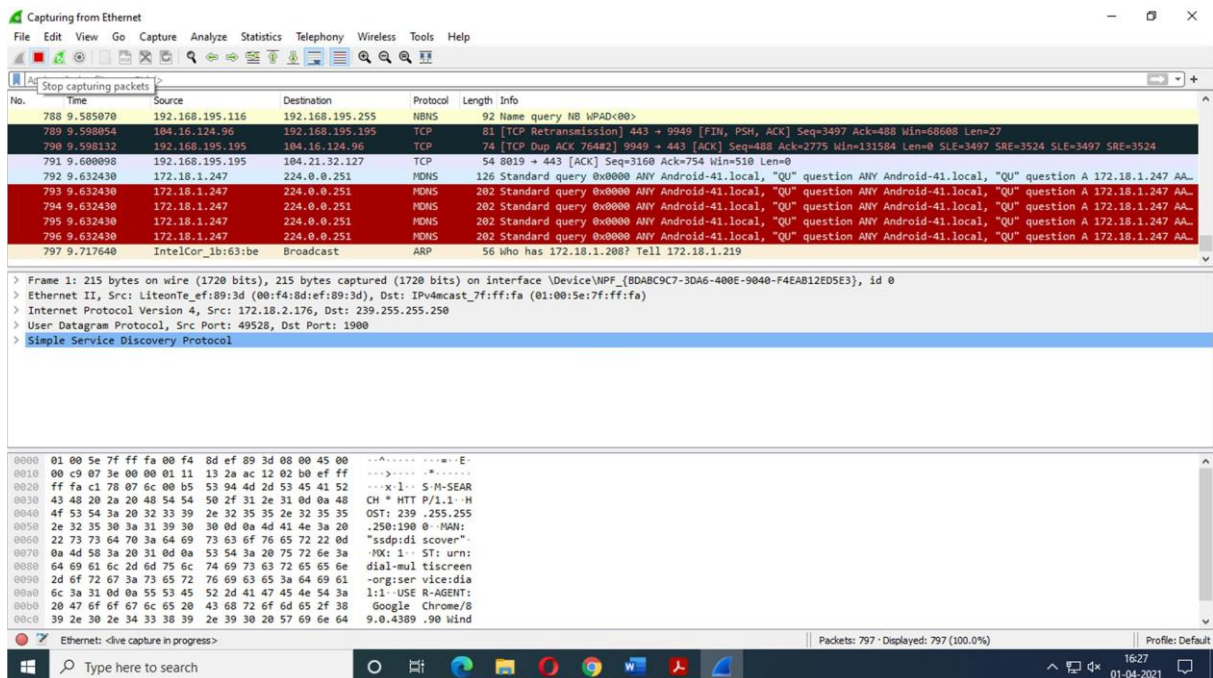


Fig 1.3 Stop, Restart and Capture Filters

- 4) The display filter can be used to display a specific type of packet that was transmitted.

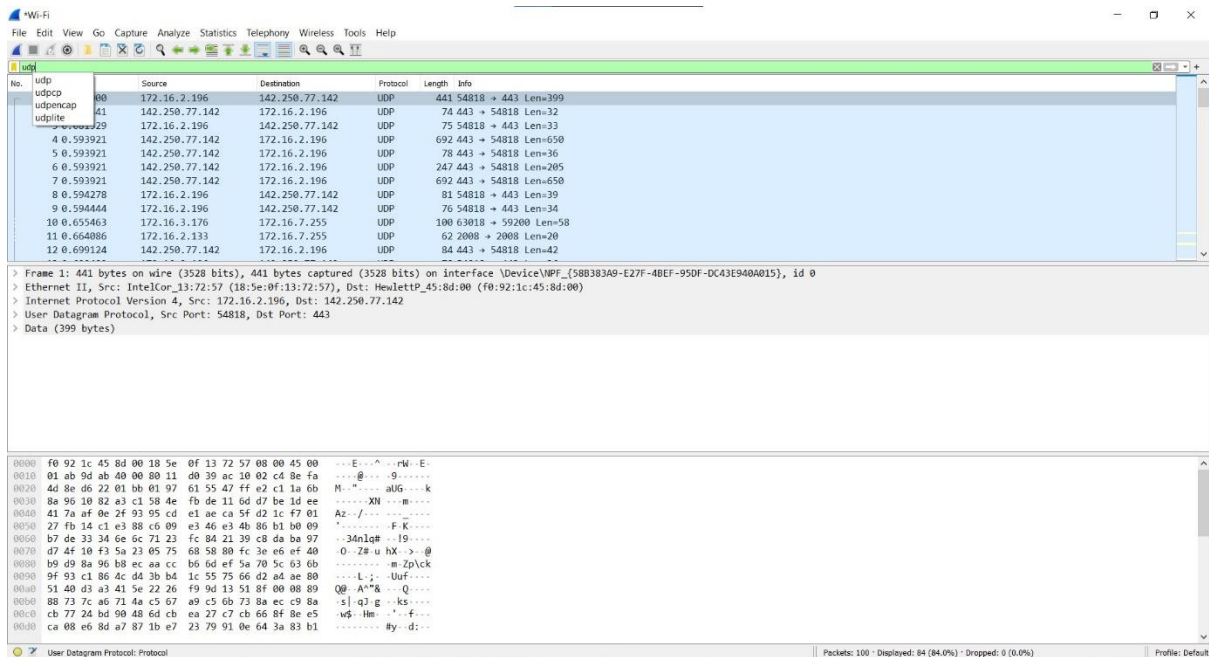


Fig 1.4 Applying a Display Filter

RESULT:

Different packets have been captured and analyzed using Wireshark tool in a live network.

EXPERIMENT 11

NMAP

Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides several features for probing computer networks, including host discovery and service and operating system detection.

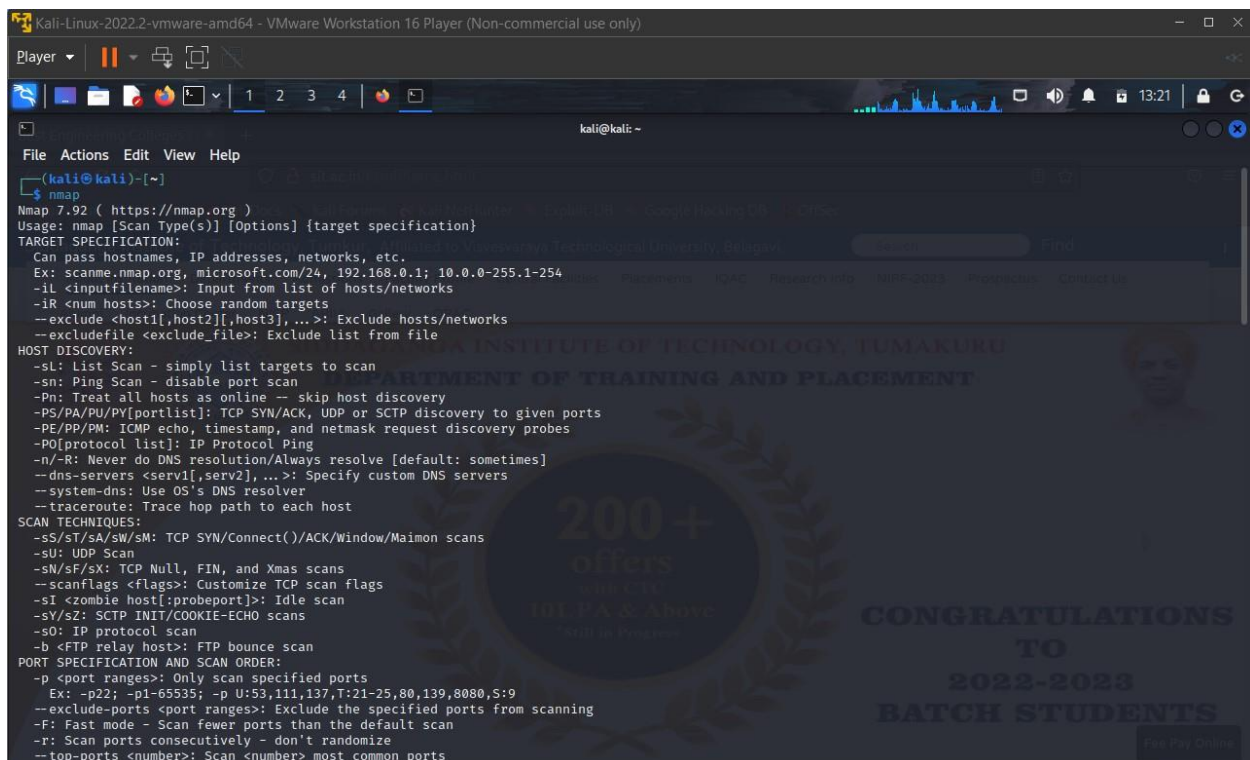
AIM: IP and network analysis using NMAP

TOOLS USED: NMAP

PROCEDURE:

Step 1:

Open NMAP on Kali Linux terminal.

The image shows a screenshot of a Kali Linux terminal window. The terminal title bar reads "Kali-Linux-2022.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)". The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The prompt is "(kali@kali)-[~]". The user has entered the command "nmap". The terminal displays the Nmap version "7.92" and its usage instructions. It lists various options for target specification, host discovery, scan techniques, and port specification. The background of the terminal window features a watermark logo for "200+ offers" and a congratulatory message for "2022-2023 BATCH STUDENTS".

```
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] [target specification]

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iI <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/sT/sA/sw/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
```

Fig. 11.1 Opening NMAP

Step 2:

Use NMAP to analyze a particular website using the command **nmap URL**.

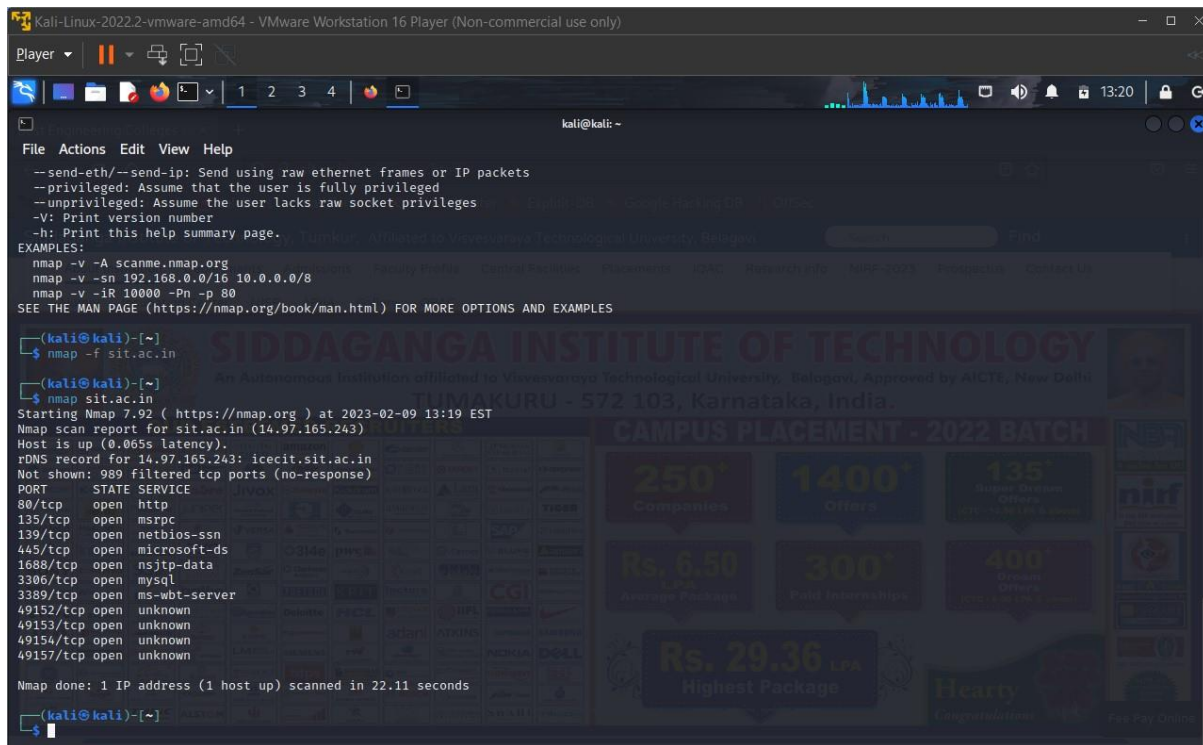


Fig. 11.2 NMAP analysis of URL

Step 3:

Use NMAP to analyze a particular IP address using the command **nmap ip_address**.

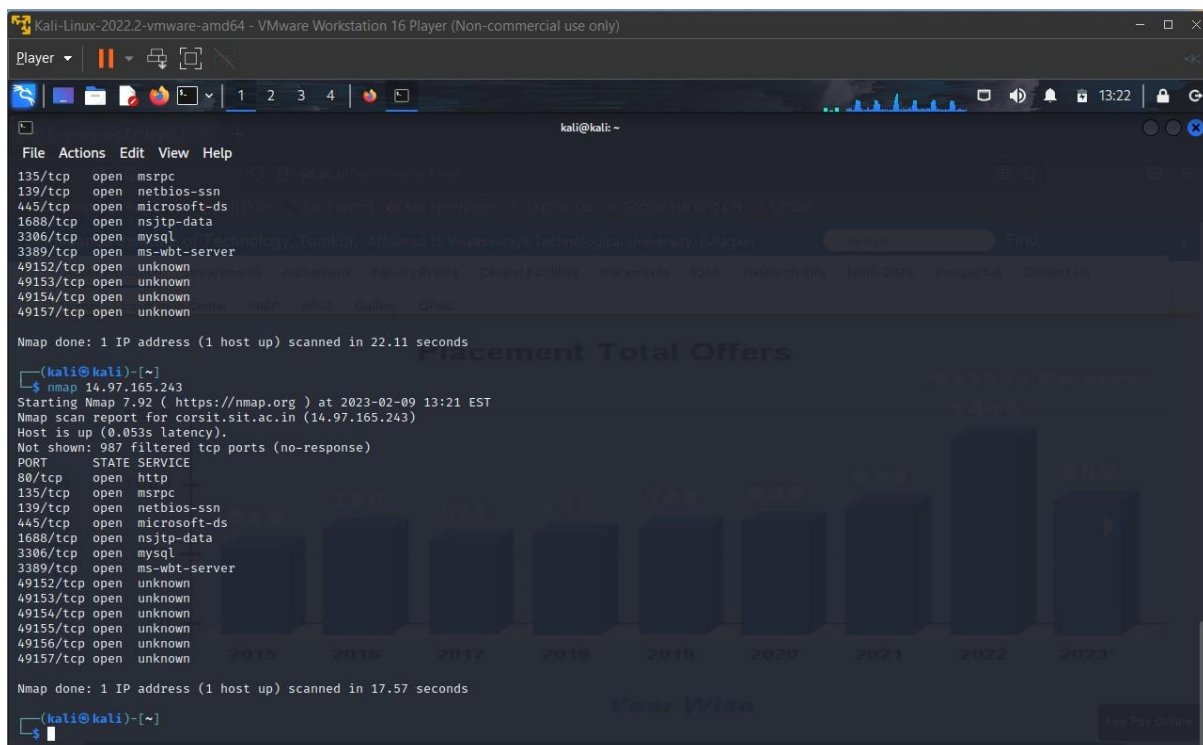


Fig. 11.3 NMAP analysis of IP address

Step 4:

Using NMAP to scan 100 most common ports using the command **nmap -F ip_address**.

```
kali@kali: ~  
File Actions Edit View Help  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
1688/tcp open nsjtp-data  
3306/tcp open mysql  
3389/tcp open ms-wbt-server  
49152/tcp open unknown  
49153/tcp open unknown  
49154/tcp open unknown  
49155/tcp open unknown  
49156/tcp open unknown  
49157/tcp open unknown  
Nmap done: 1 IP address (1 host up) scanned in 17.57 seconds  
  
kali@kali: ~  
$ nmap -F 14.97.165.243  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-09 13:22 EST  
Nmap scan report for ncsts22.sit.ac.in (14.97.165.243)  
Host is up (0.059s latency).  
Not shown: 88 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  mspc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3306/tcp   open  mysql  
3389/tcp   open  ms-wbt-server  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds  
kali@kali: ~
```

Fig. 11.4 Scanning the 100 most common ports

RESULT: Analysis of websites using URLs, IP addresses and scanning the 100 most common ports of the website.