--CYBER SECURITY--

(MAJOR PROJECT)

NAME- ARTI GUPTA
ROLL NO- ……..
BATCH- DECEMBER(9)

SUBMITTED TO:
AMAN GUPTA
(INTERNSELITE)

SUBMITTED BY:
ARTI GUPTA(MCA)
ICFAI UNIVERSITY,
(DEHRADUN)

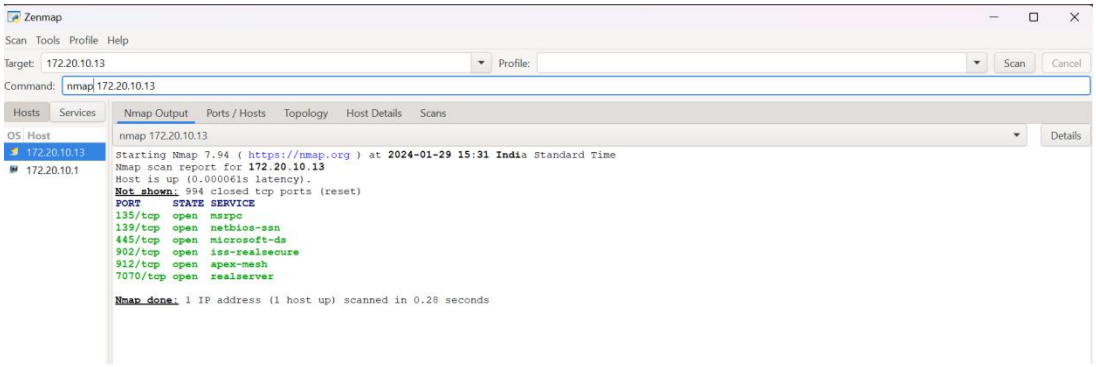
Use NMAP tool for finding information inside the network.

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.Nmap is a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing.

Now we are going to use following commands through which we get find different information inside the network:-

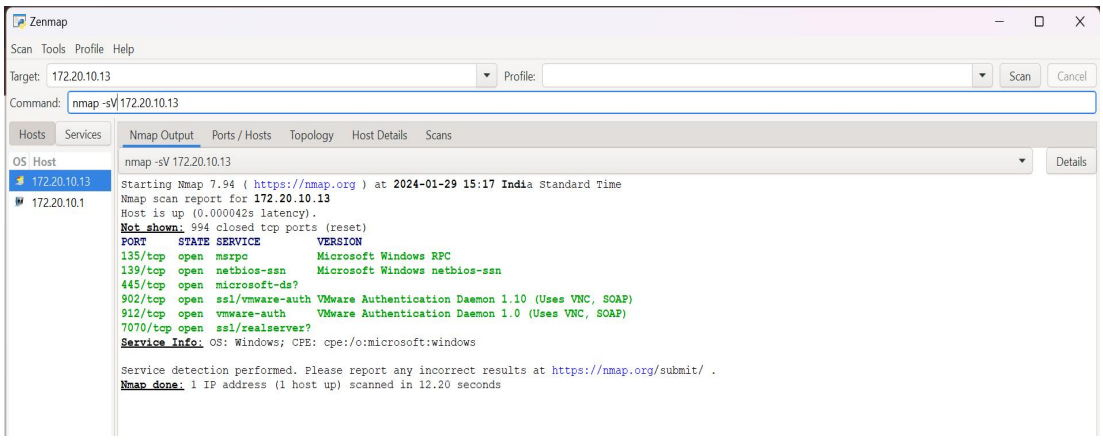
- **nmap 172.20.10.13**

  (Used for scanning the IP and gives information about host is up or not.)



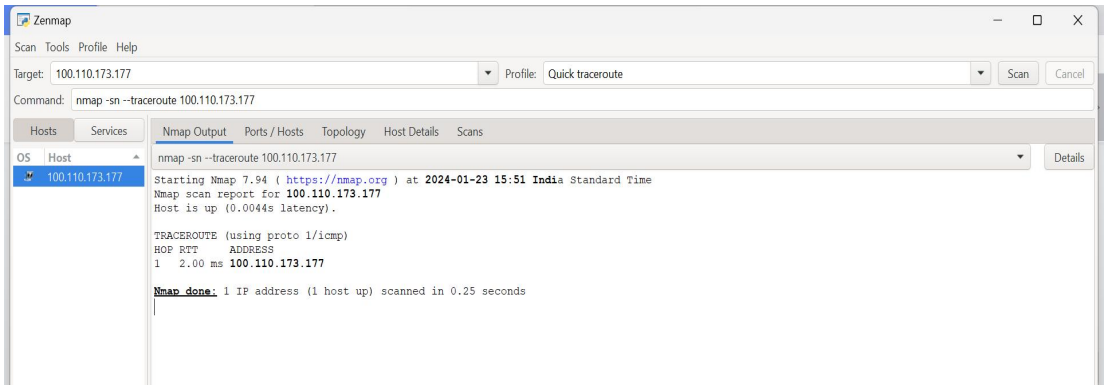
- **nmap -sV 172.20.10.13**

  (Used for service version detection with their services and state.)



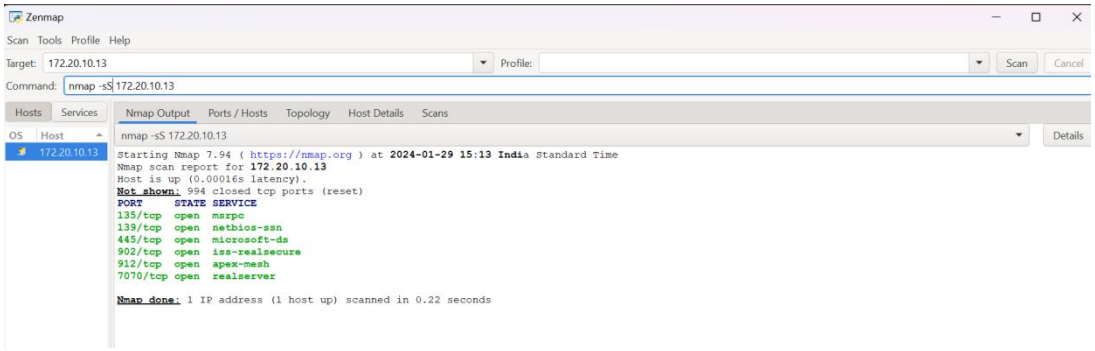
◆ nmap -sn -traceroute 100.110.173.177

(Used for tracing the route of IP with their HOP counts, delay time and protocol.)



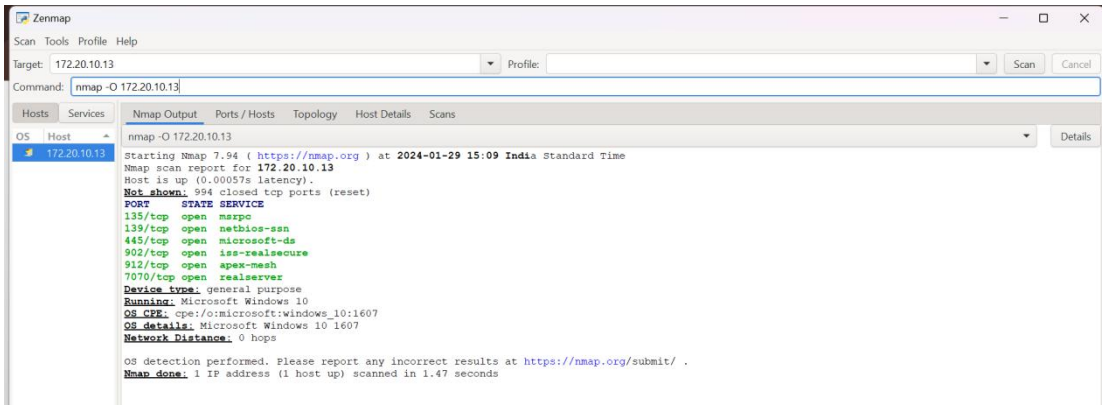
◆ nmap -sS 172.20.10.13

(Used for gathering the information of all TCP ports and connections.)



◆ nmap -O 172.20.10.13

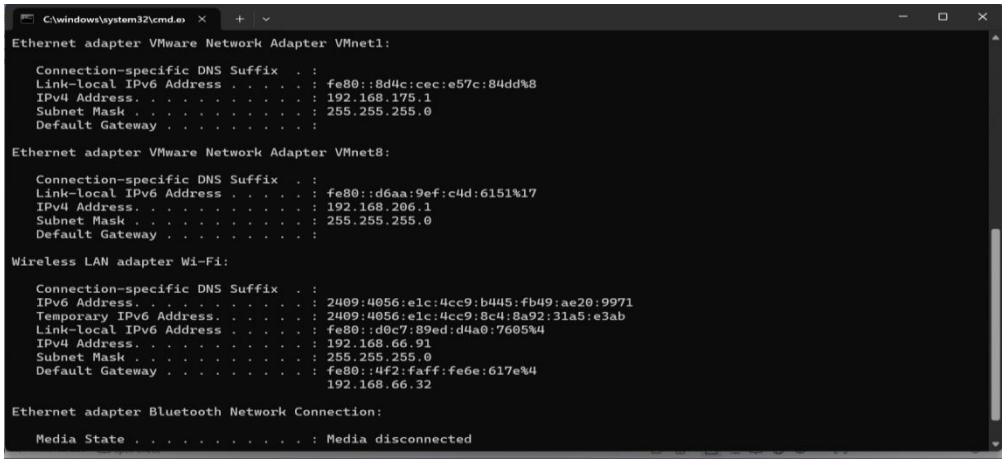
(Used for OS detection and gives the information about open ports.)



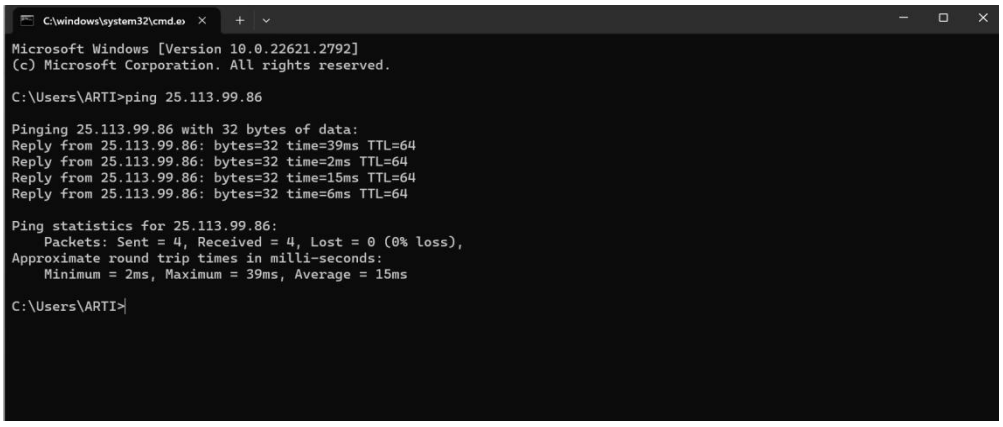
Write and explain commands in windows command prompt for network/server details.

◆ **Ipconfig:-** This networking commands is used to the IP configuration details. This command provides you the details like IPv4 address, Subnet Mask or Default Gateway.

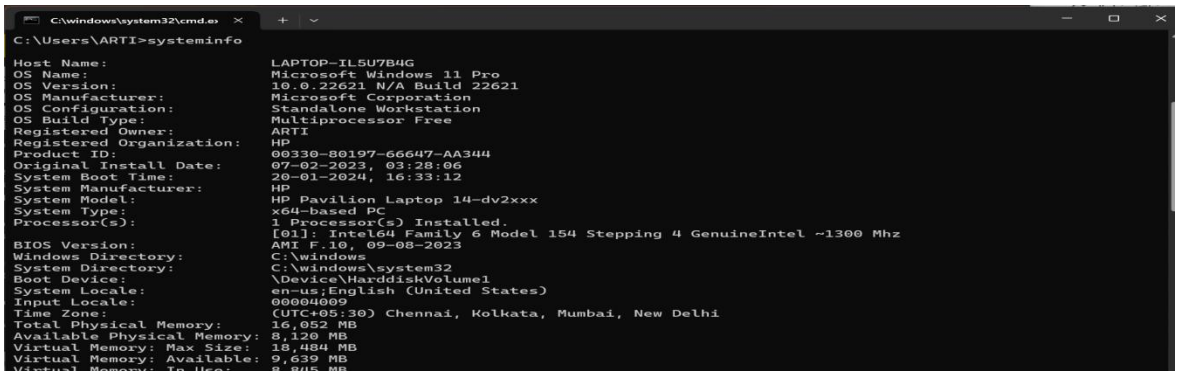
1. Subnet mask-It can be understood as the boundary of our internet connection.
2. Default Gateway-It is the address of the router to which our computer first hits when the device we want to connect is out of our local network.

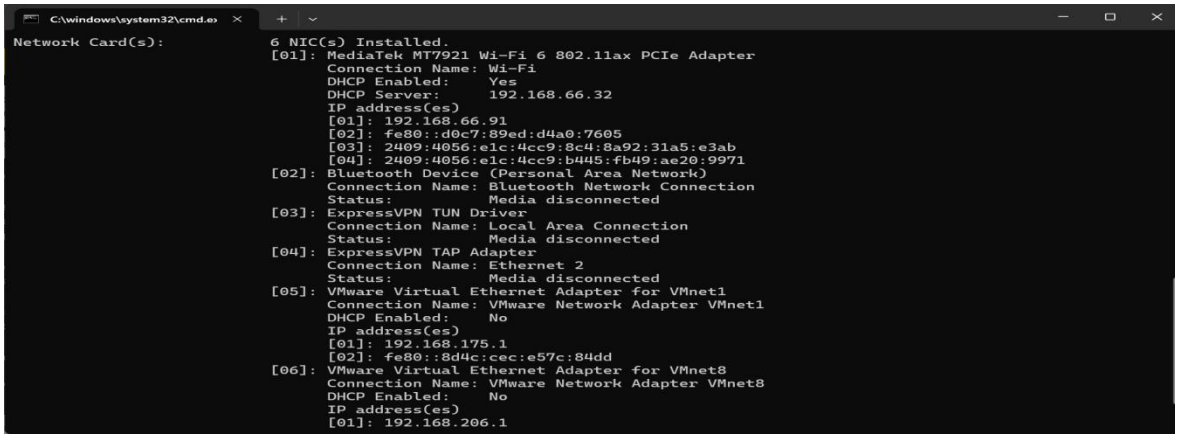


◆ **Ping:-** Ping command is used to get to know if the particular site can be reached by the ping command. The ping command checks this by sending the packets of data to the destination address and if the data returns to us in the given time frame then it means that the particular website can be reached .

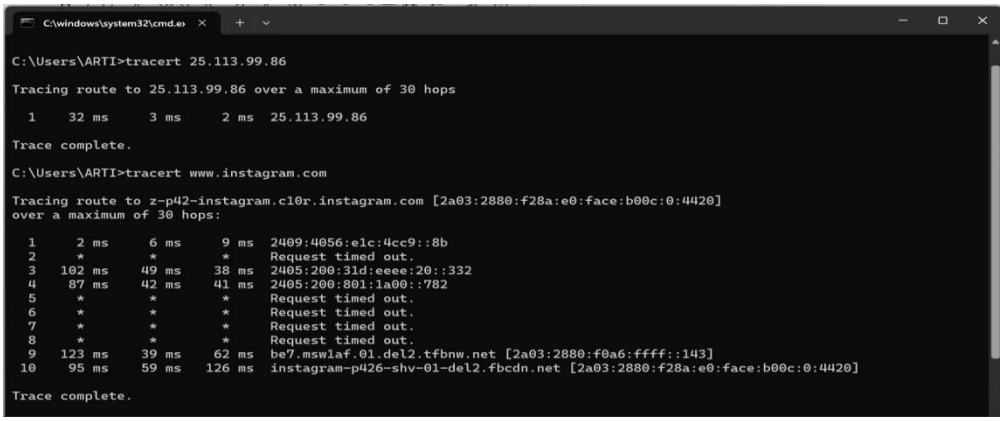


◆ **Systeminfo:-** This Command is used to display all the necessary information about our System such as configuration, version, hostname, processor details network card details etc.

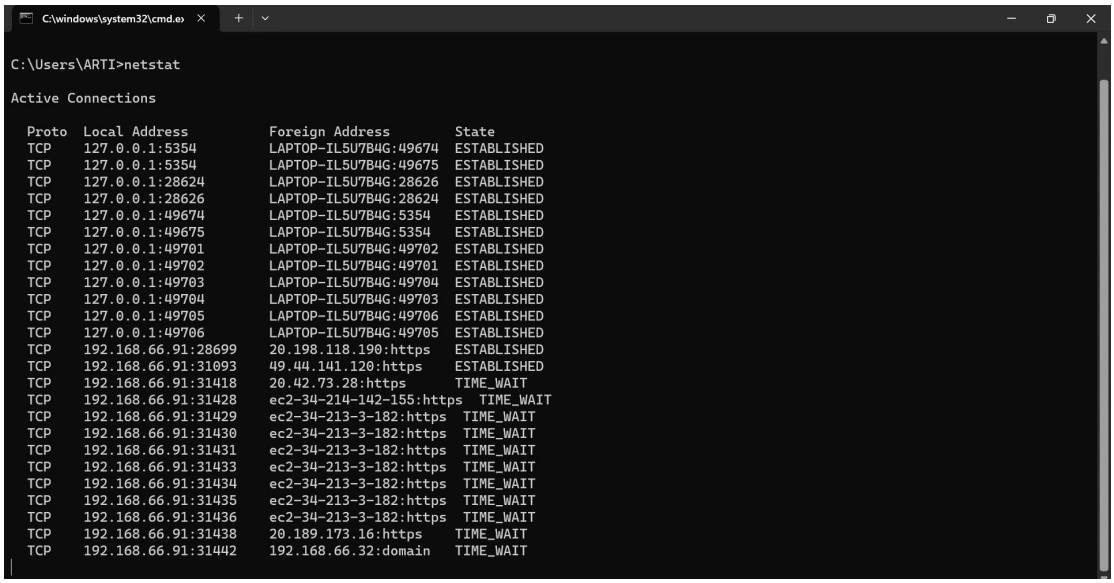




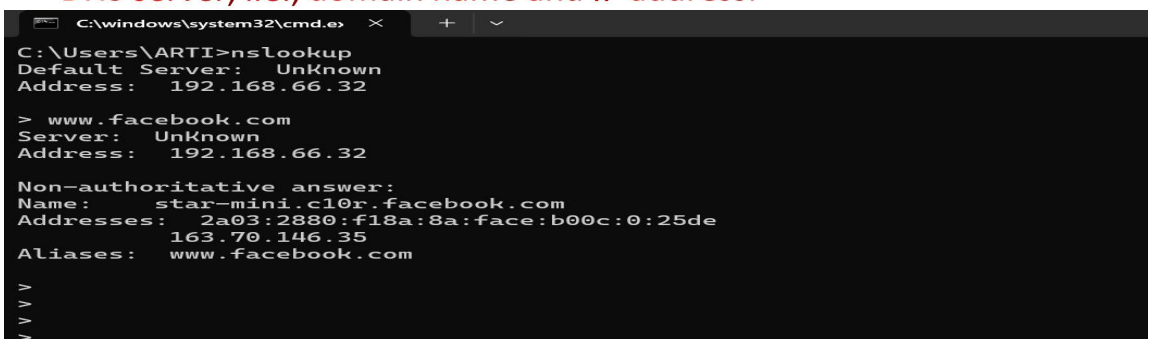
◆ **Tracert:-** This command can be understood as trace root. Which tells that our computer reaches or hits which-which server for reaching the particular root. We can search by giving the IP address and destination site name also.



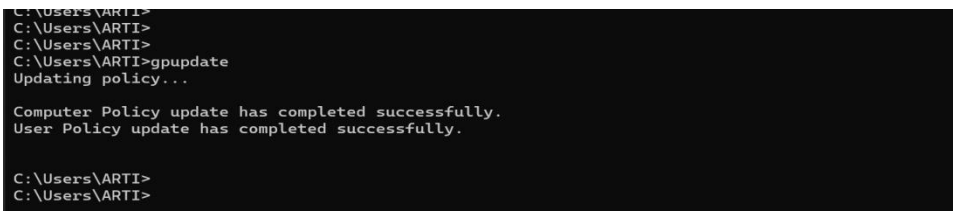
◆ **Netstat:-** It is a command line tool that is identify and display the connections and ports connected to our computer when we write netstat command on CLI.



◆ **Nslookup:-** The NSLOOKUP command is used to troubleshoot network connectivity issues in the system. Using the nslookup command, we can access the information related to our system's DNS server, i.e., domain name and IP address.



◆ **gpupdate:-** The gpupdate command is used to apply group policies on a computer in a windows domain.



◆ **getmac:-** This command returns the MAC address from all the network cards on a system.

```
C:\Users\ARTI>getmac

Physical Address    Transport Name
=================== ==========================================================
34-6F-24-C9-22-A9   \Device\Tcpip_{073E83F2-2A79-4C49-A9E3-EECBBAD7D833}
34-6F-24-C9-22-A8   Media disconnected
N/A                 Media disconnected
00-FF-98-E6-F0-1A   Media disconnected
00-50-56-C0-00-01   \Device\Tcpip_{798B0D28-20A1-4E4E-B0C3-D88698BF845F}
00-50-56-C0-00-08   \Device\Tcpip_{D4F1A9F8-5952-4DE9-8DCF-1C3B25626A4D}
```

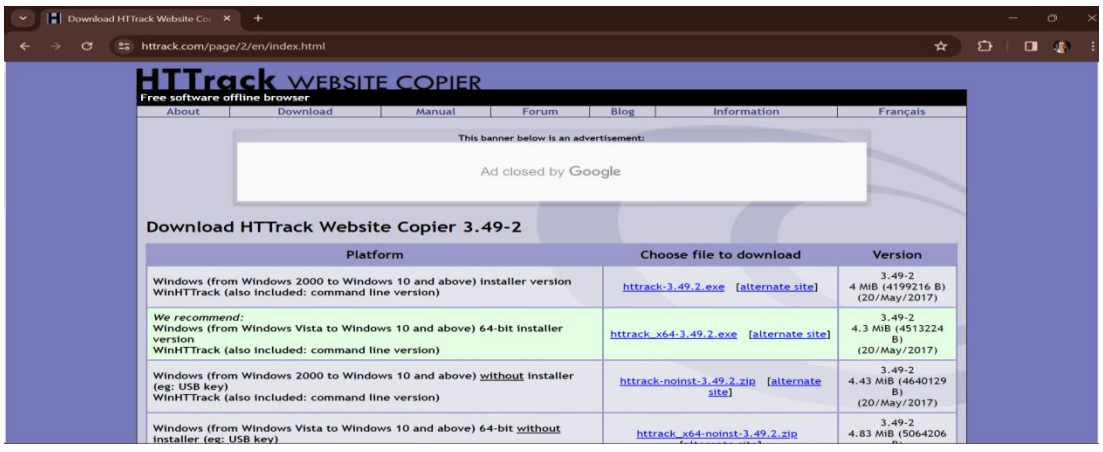
◆ **net user:-** The net user command displays user account information on a local computer or the domain.

```
C:\windows\system32\cmd.e×

C:\Users\ARTI>net user

User accounts for \\LAPTOP-IL5U7B4G

-------------------------------------------------------------------------------
Administrator            ARTI                     DefaultAccount
Guest                    WDAGUtilityAccount
The command completed successfully.
```

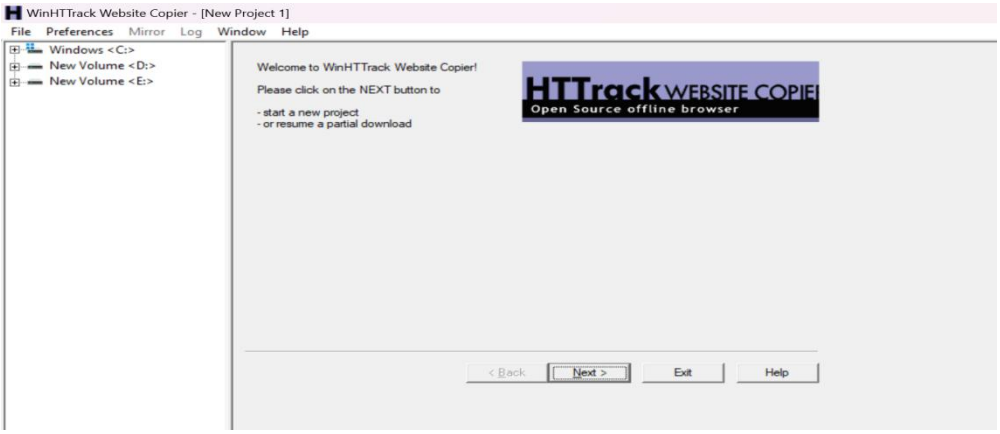
Use website copying tool for website copy (HT-TRACK).

HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

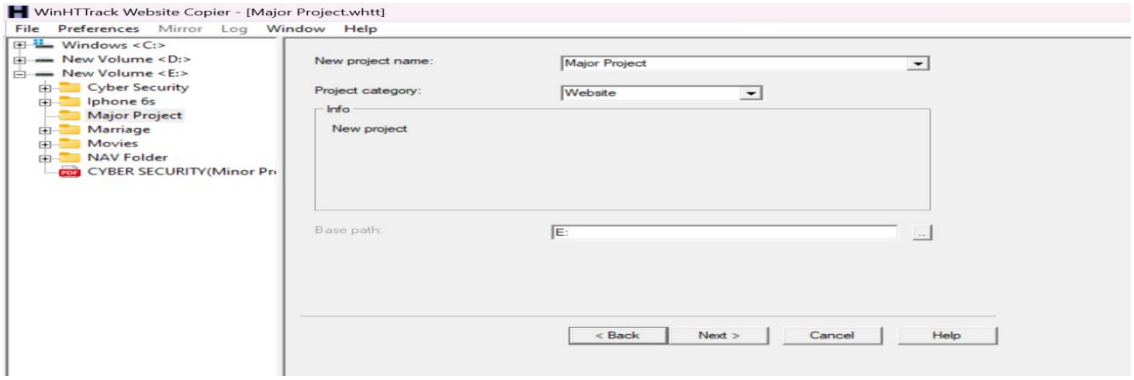
◆ Fisrtly we have to download and install HT-TRACK from https://www.httrack.com



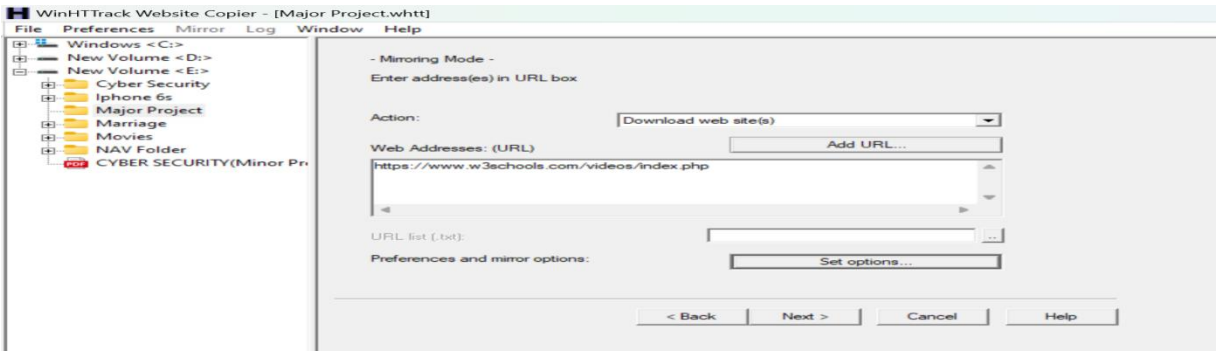
- After installing open the HT-TRACK and click next



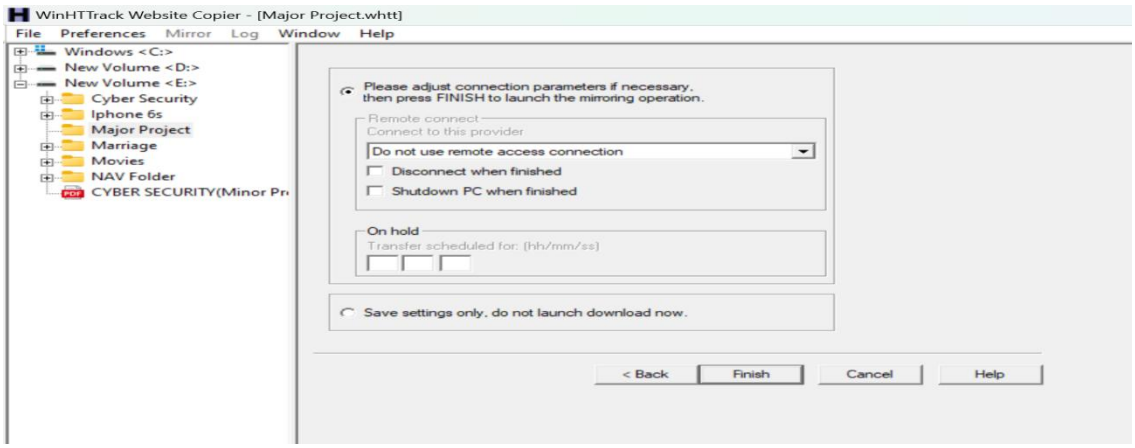
- Now fill the project name, project category and choose the path where website data will be saved.



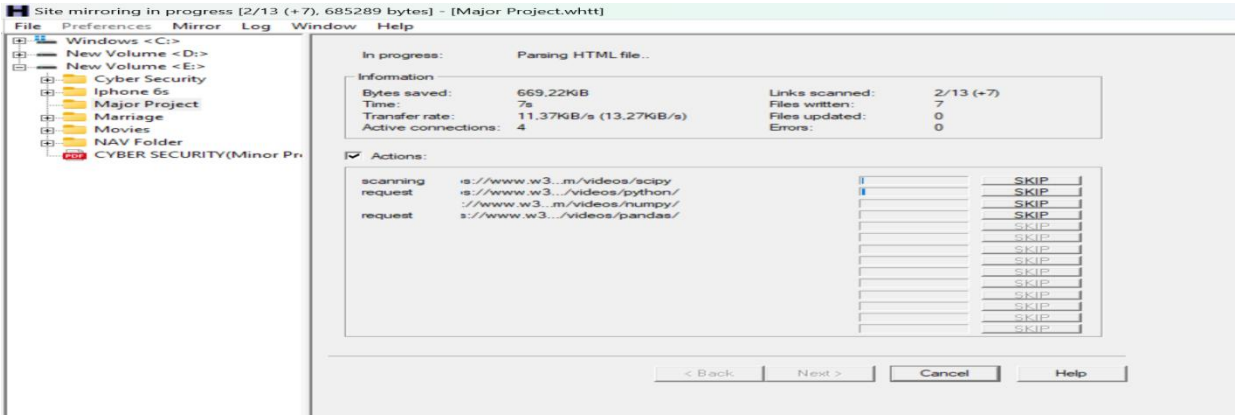
- Now choose action and type the website URL which you want to copy.



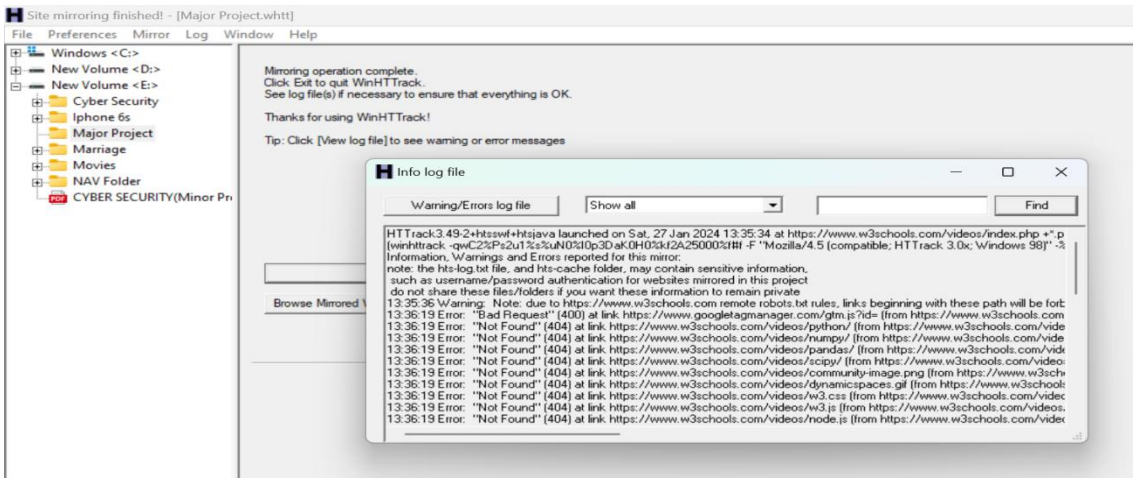
- Now select the options according to your requirements then click FINISH.



- Now the website contents are copying to your system.



- Now click on view error log to see errors and then click FINISH.

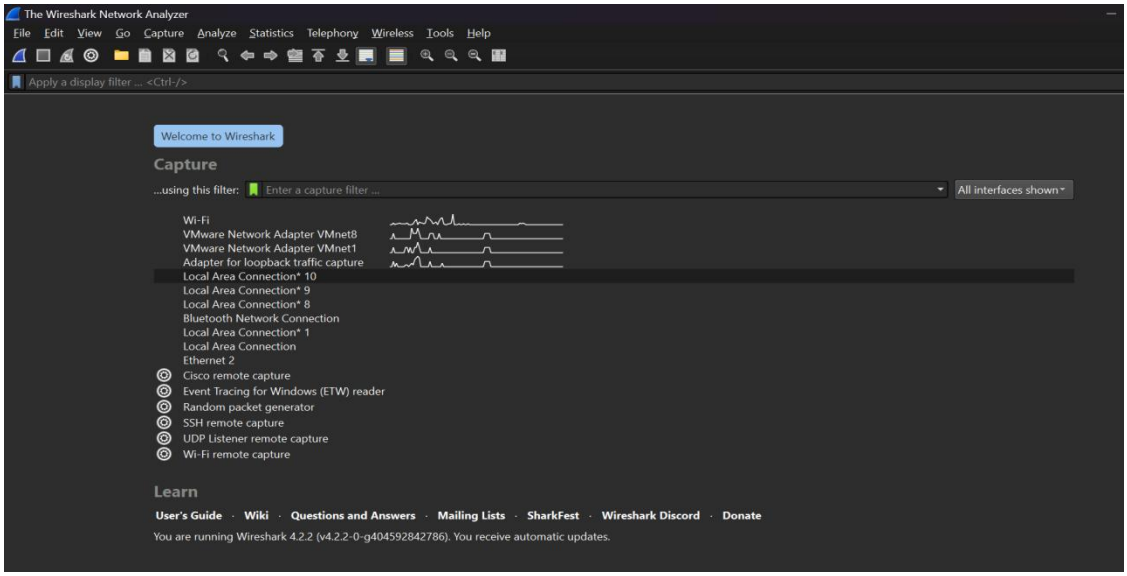


Use wireshark tool for packet capturing.

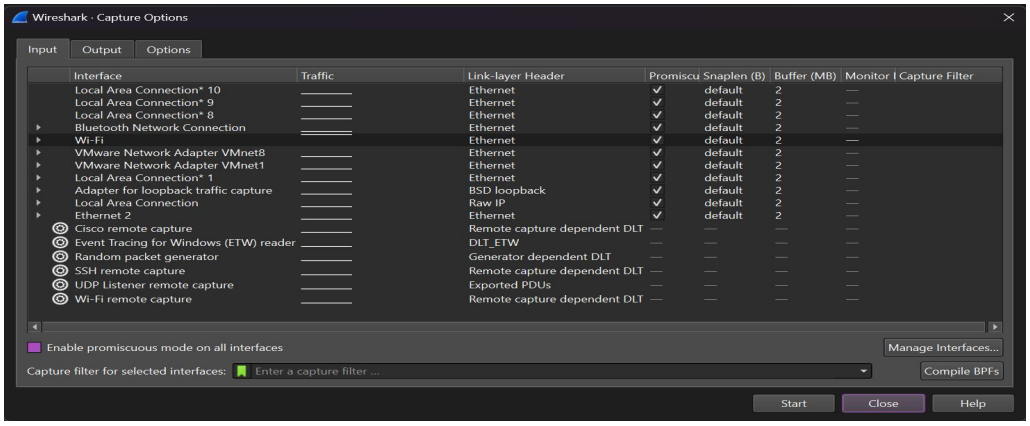
Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.

- Download and install wireshark tool from the link as :- https://www.wireshark.org/

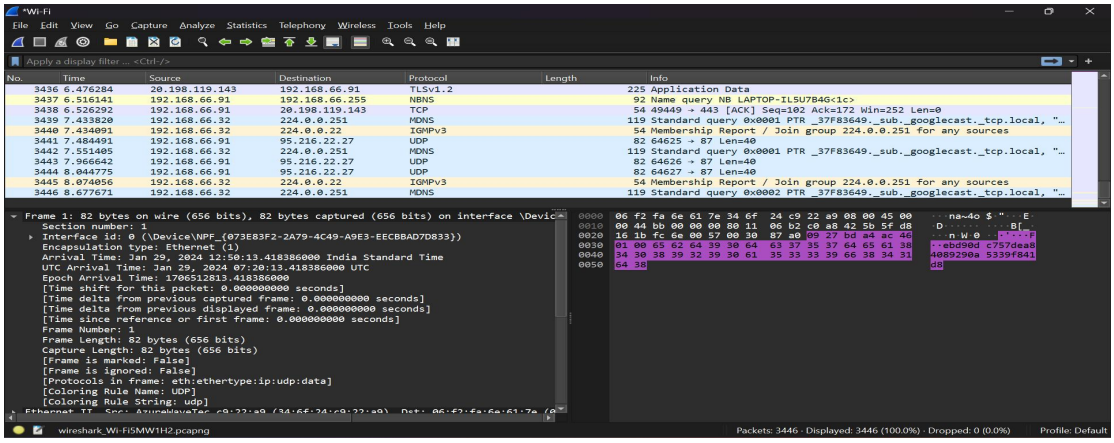
- After installing open the wireshark tool.



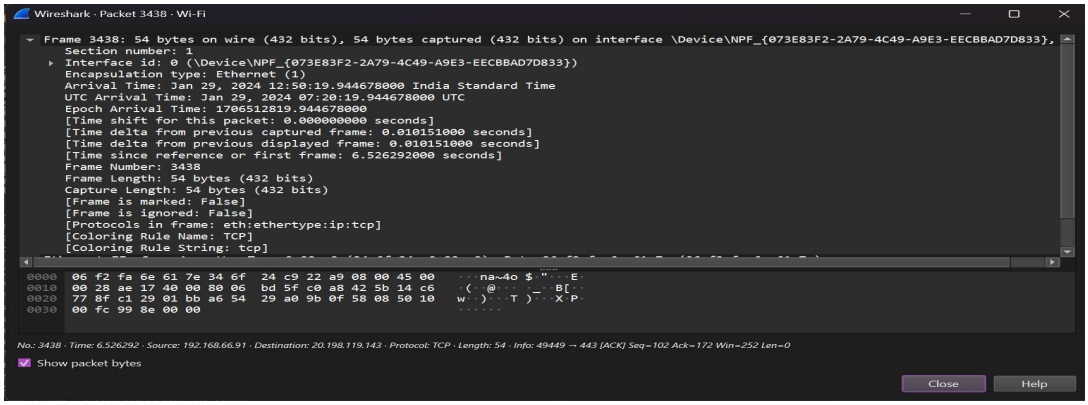
- Now click on capture then options, now select the network and click on START.



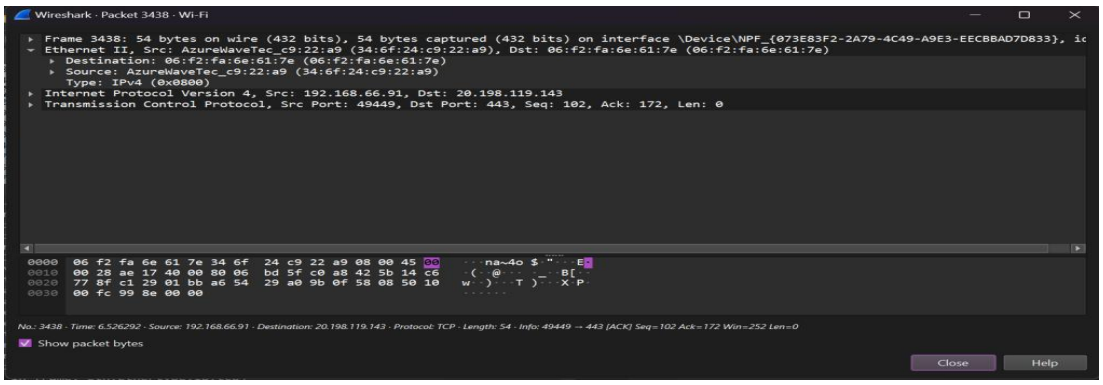
- Packets are capturing with showing their information.



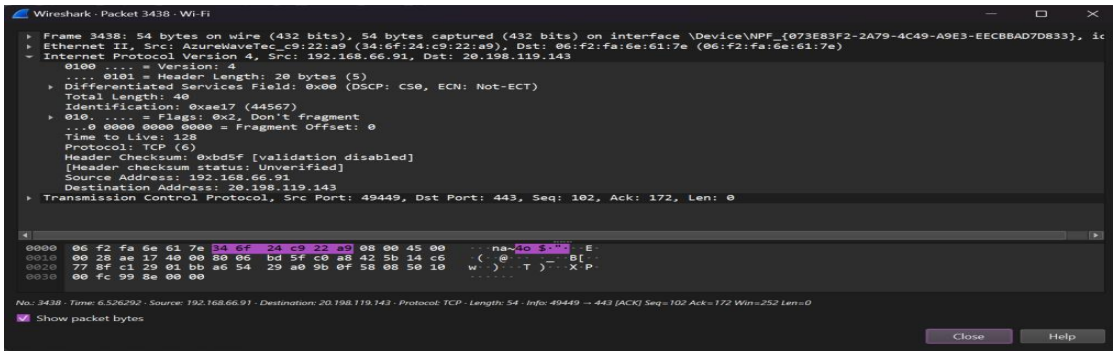
- Frame:- shows the complete information about frame like frame length, capture length, mac address,etc.



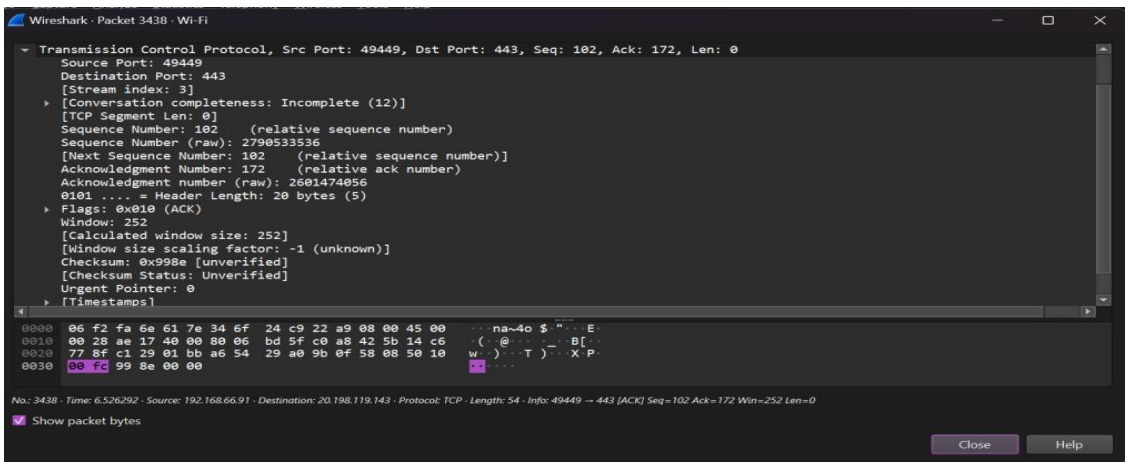
- It shows the type of network connection with source and destination address and the type of IP address.



- The next pop up shows the information about internet protocol like header length, time to leave, source and destination IP of packets, etc.



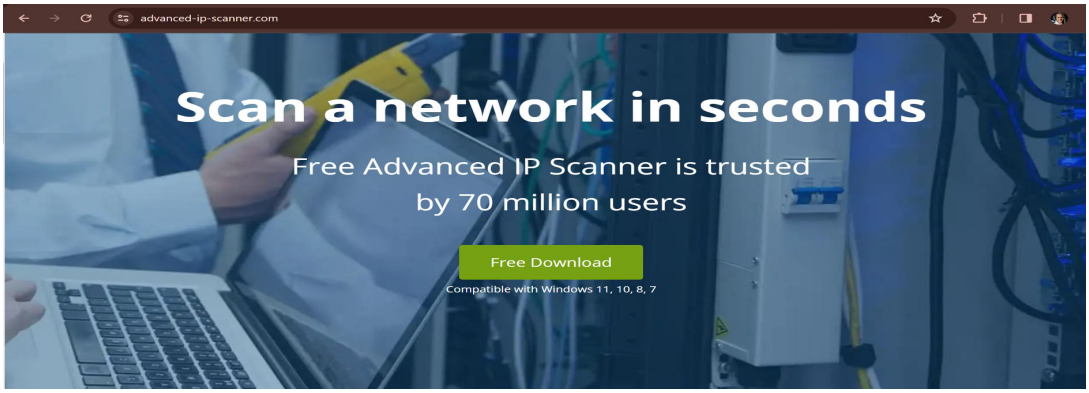
- The next pop up shows the information about TCP information with source and destination port no., acknowledgement of packet, etc.



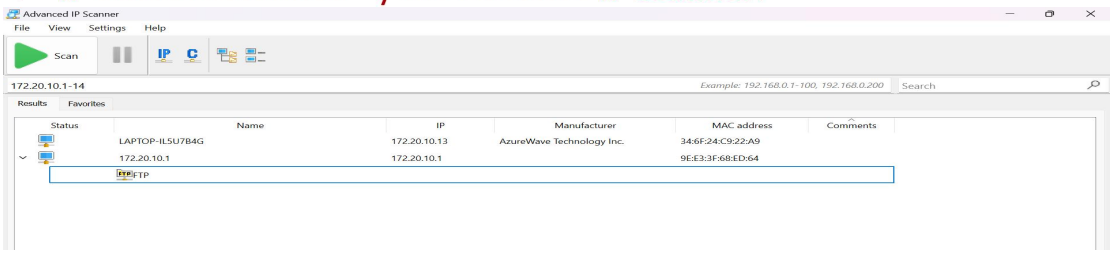
#Tools for finding details of any network/server/website (IP lookup website).

The IP lookup tool can give you exact location details of an IP address. If you already know the IP address, you can find out the city, state, zip code and country of an IP address instantly.

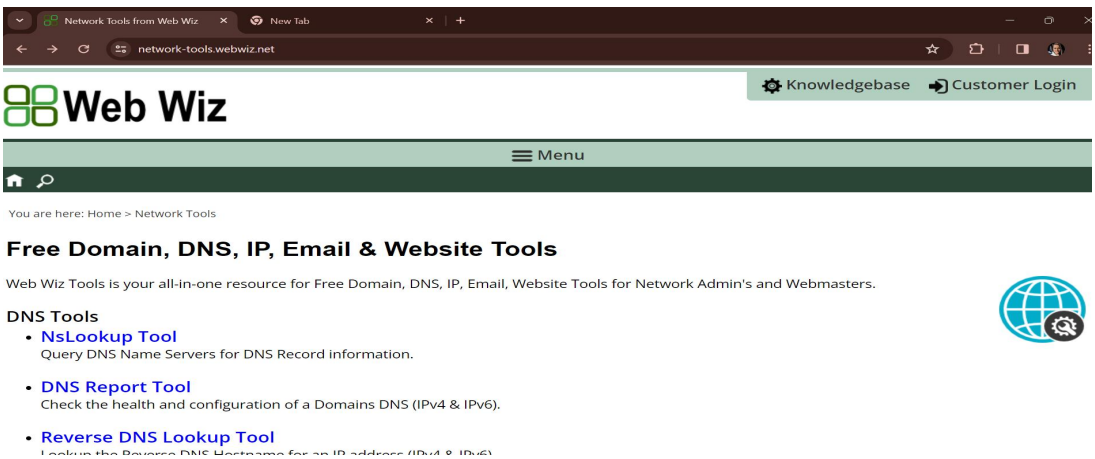
◆ Advance IP Scanner:-



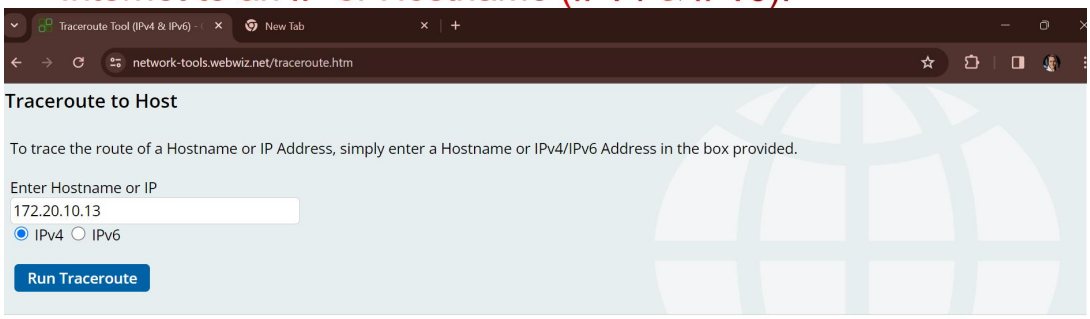
✧ IP address scanned by the Advance IP scanner.



◆ Web wiz tool:-



✧ It is used to trace the route network packets take across the Internet to an IP or Hostname (IPv4 & IPv6).

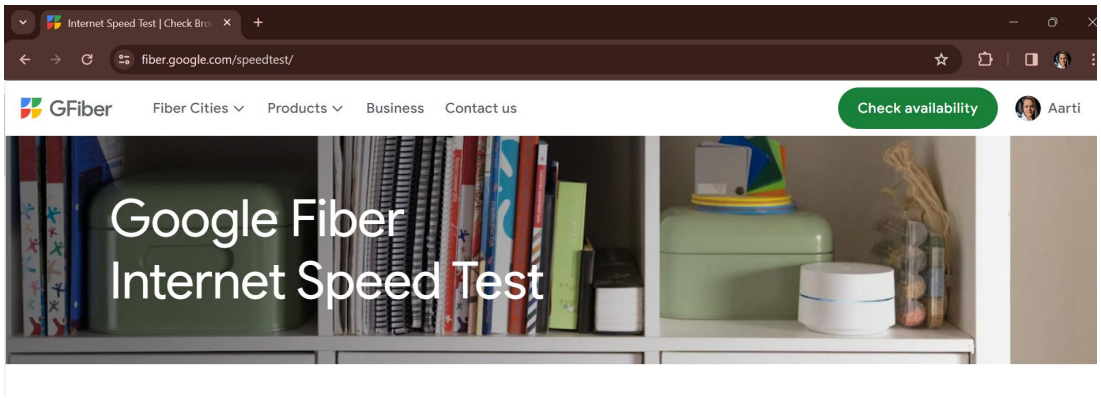


Trace Route to 172.20.10.13

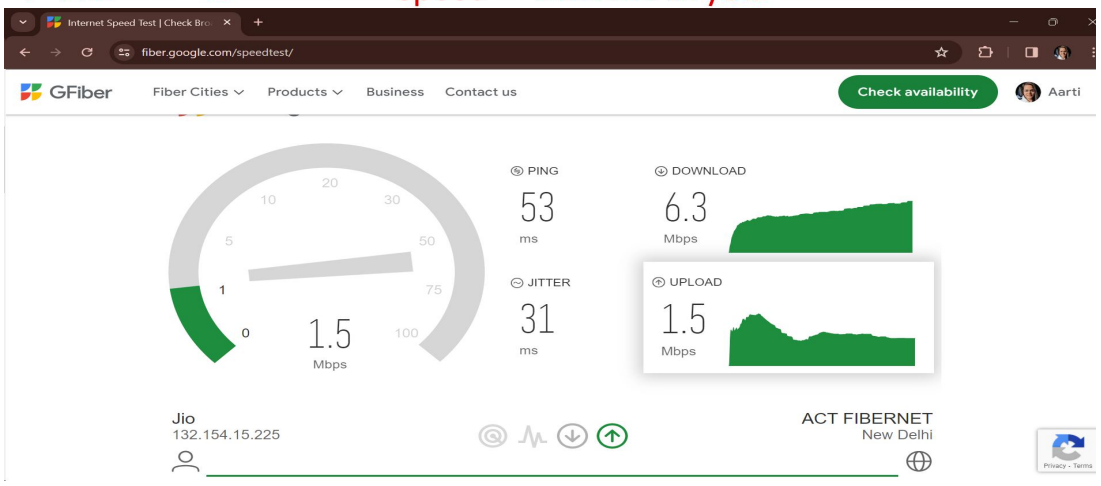
Trace Route from; Web Wiz [Poole - United Kingdom]

Hop	Time		IP Address	Hostname	Country
1	0 ms		92.53.240.2	xe-sh.cr-01.poole.webwiz.net.uk	United Kingdom
2	Timeout		Unknown	Host did not respond to ping	
3	Timeout		Unknown	Host did not respond to ping	

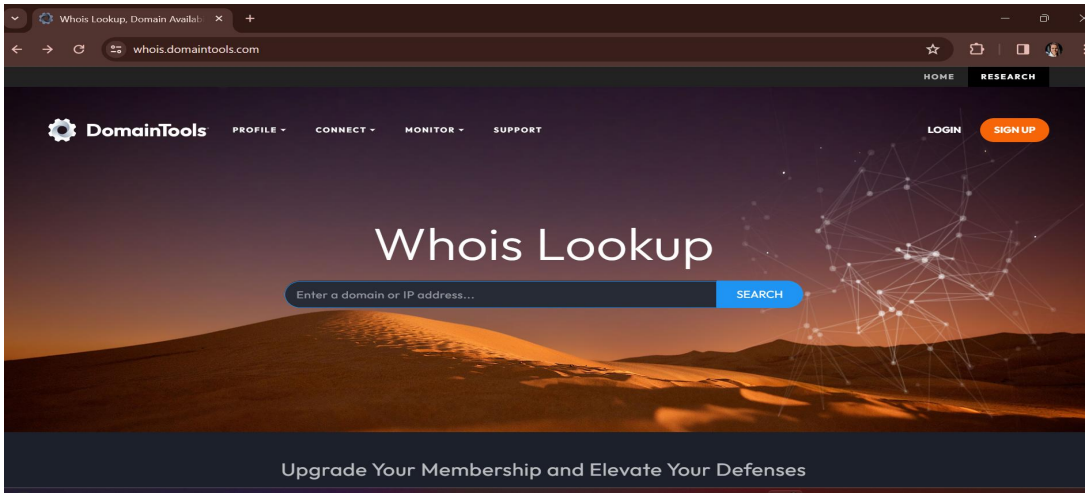
◆ Google Fibre:-



✧ It is used to check the speed of internet in your network.



◆ Domain tools:-



✧ It is used to find complete IP information.