

# **--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)**

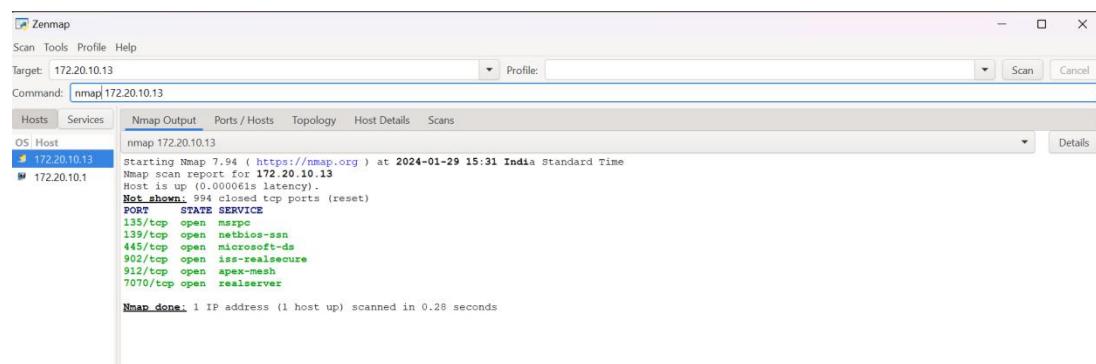
## # Use NMAP tool for finding information inside the network.

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.)

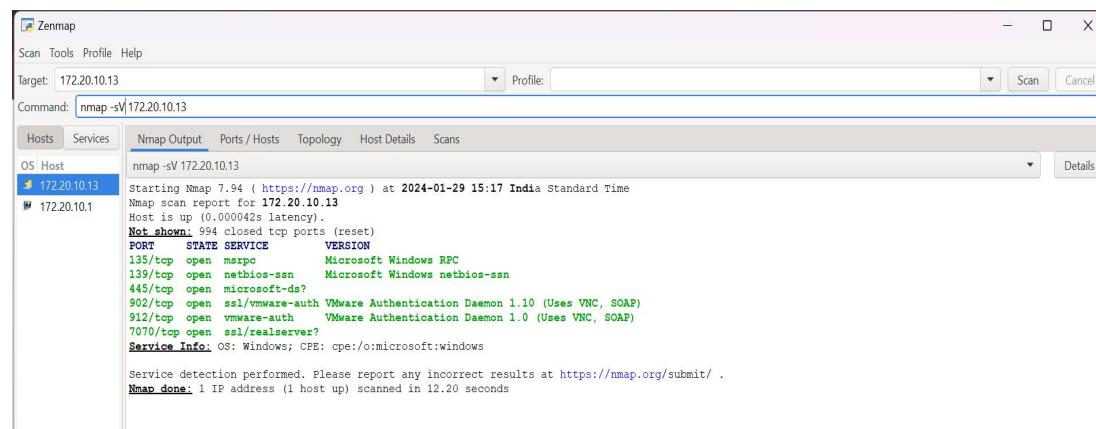


The screenshot shows the Zenmap interface with the target set to 172.20.10.13 and the command field containing "nmap 172.20.10.13". The "Services" tab is selected. The output pane displays the following Nmap report:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 15:31 India Standard Time
Nmap scan report for 172.20.10.13
Host is up (0.000061s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
7070/tcp   open  realserver
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

### ◆ nmap -sV 172.20.10.13

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



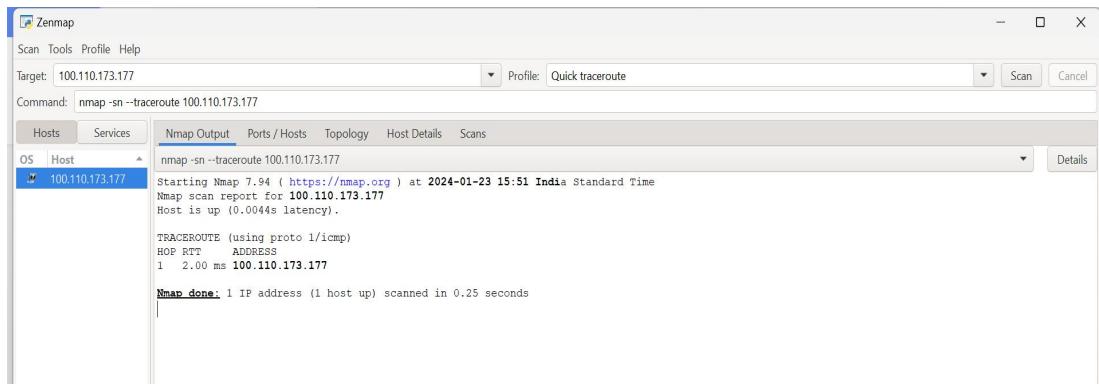
The screenshot shows the Zenmap interface with the target set to 172.20.10.13 and the command field containing "nmap -sV 172.20.10.13". The "Services" tab is selected. The output pane displays the following Nmap report:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 15:17 India Standard Time
Nmap scan report for 172.20.10.13
Host is up (0.000042s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open  vmware-auth   VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
7070/tcp   open  ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.20 seconds
```

## ◆ nmap -sn -traceroute 100.110.173.177

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



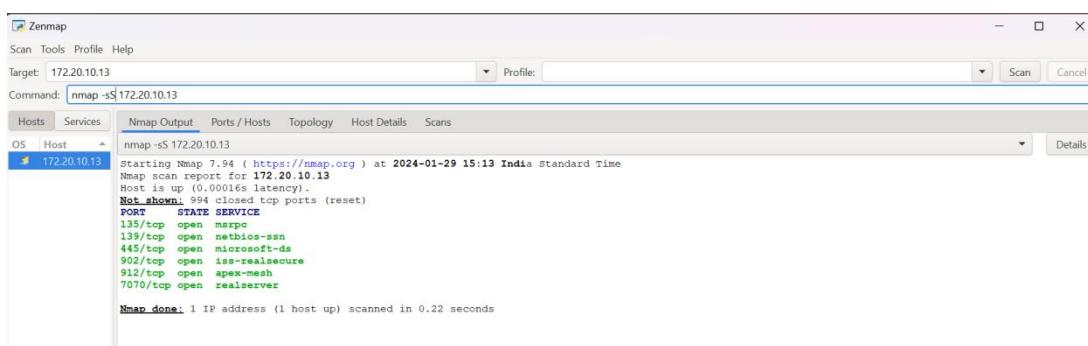
```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 15:51 India Standard Time
Nmap scan report for 100.110.173.177
Host is up (0.0044s latency).

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  2.00 ms  100.110.173.177

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

## ◆ nmap -sS 172.20.10.13

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

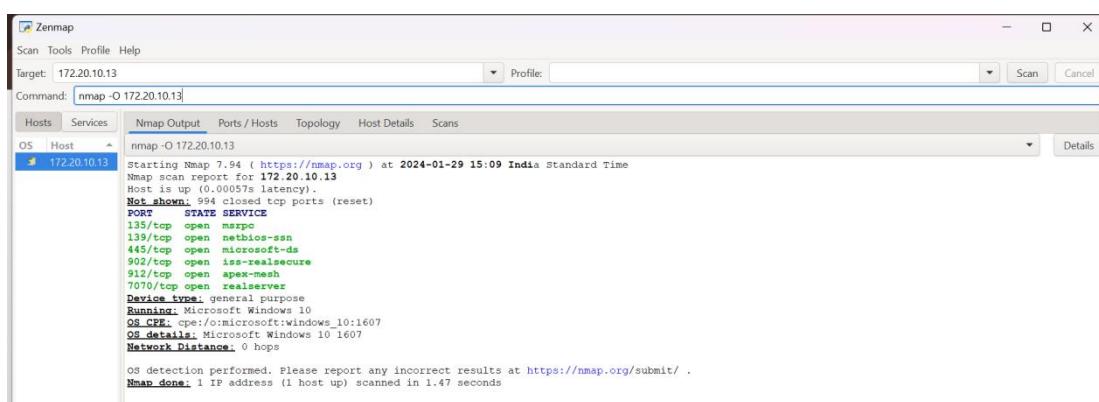


```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 15:13 India Standard Time
Nmap scan report for 172.20.10.13
Host is up (0.0101s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
7070/tcp  open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

## ◆ nmap -O 172.20.10.13

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



```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 15:09 India Standard Time
Nmap scan report for 172.20.10.13
Host is up (0.00057s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
7070/tcp  open  realserver

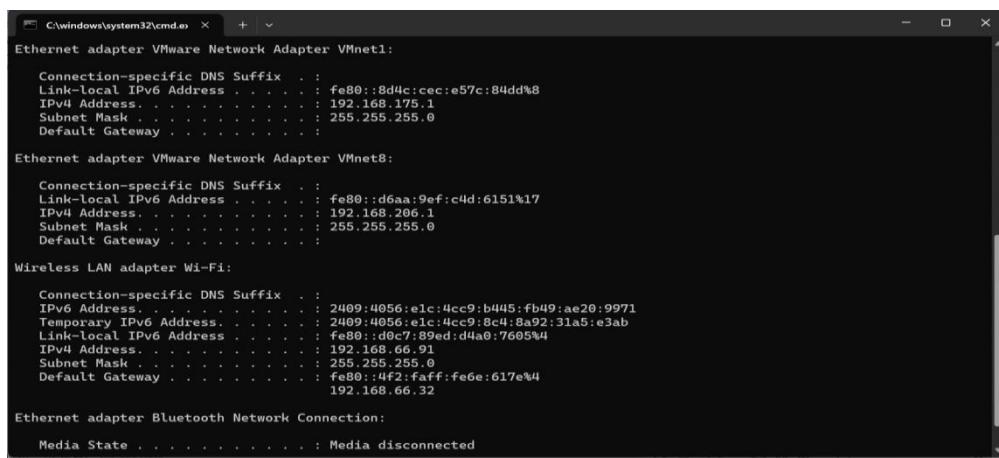
Device type: general purpose
Running: Microsoft Windows 10
OS_CPE: cpe:/o:microsoft:windows_10:1607
OS_details: Microsoft Windows 10 1607
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

## # 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.



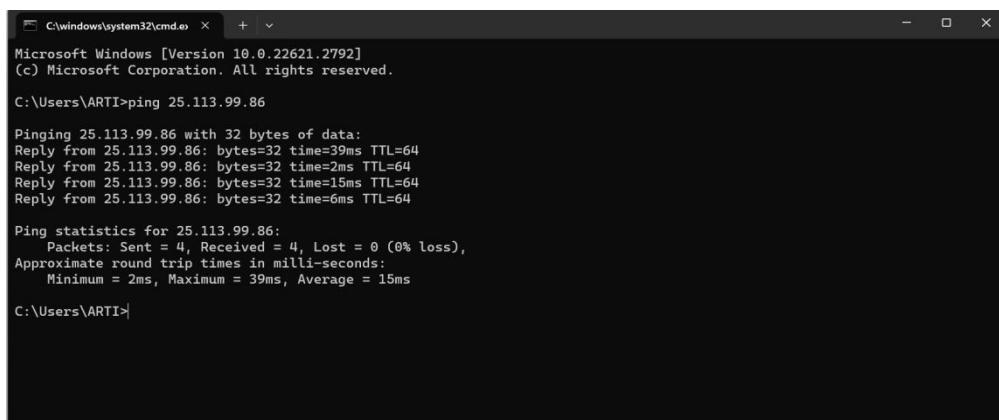
```
C:\Windows\system32\cmd.exe + x
Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix . .
  Link-local IPv6 Address . . . . . : fe80::8d4c:cec:e57c:84dd%8
  IPv4 Address . . . . . : 192.168.175.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . .

Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix . .
  Link-local IPv6 Address . . . . . : fe80::d6aa:9ef:c4d:6151%17
  IPv4 Address . . . . . : 192.168.206.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . .

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . .
  IPv6 Address . . . . . : 2409:4086:e1c:4cc9:b445:fb49:ae20:9971
  Temporary IPv6 Address . . . . . : 2409:4086:e1c:4cc9:8c92:31a5:e3ab
  Link-local IPv6 Address . . . . . : fe80::d0c7:89ed:d4a0:7605%4
  IPv4 Address . . . . . : 192.168.1.91
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::4f2:faff:fe6e:617e%4
  192.168.66.32

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
```

◆ **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 .



```
C:\Windows\system32\cmd.exe + x
Microsoft Windows [Version 10.0.22621.2792]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ARTI>ping 25.113.99.86

Pinging 25.113.99.86 with 32 bytes of data:
Reply from 25.113.99.86: bytes=32 time=39ms TTL=64
Reply from 25.113.99.86: bytes=32 time=2ms TTL=64
Reply from 25.113.99.86: bytes=32 time=15ms TTL=64
Reply from 25.113.99.86: bytes=32 time=6ms TTL=64

Ping statistics for 25.113.99.86:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 39ms, Average = 15ms

C:\Users\ARTI>
```

◆ **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.

```
C:\Windows\system32\cmd.exe + C:\Users\ARTI>systeminfo
Host Name: LAPTOP-IL5U7B4G
OS Name: Microsoft Windows 11 Pro
OS Version: 10.0.22626.1/A Build 22621
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: ARTI
Registered Organization: HP
Processor(s): Intel(R) Core(TM) i7-13650H CPU @ 2.50GHz
Original Install Date: 07-02-2023, 03:28:06
System Boot Time: 20-01-2024, 16:33:12
System Manufacturer: HP
System Model: HP Pavilion Laptop 14-dv2xxx
System Type: x64-based PC
Processor(s):
  1 Processor(s) Installed.
    [01]: Intel64 Family 6 Model 154 Stepping 4 GenuineIntel ~1300 Mhz
BIOS Version: AMI F.10, 09-08-2023
Windows Directory: C:\Windows
System Directory: C:\Windows\System32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: 00000409
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 16.000000 GB
Available Physical Memory: 15.90 MB
Virtual Memory: Max Size: 18,484 MB
Virtual Memory: Available: 9,639 MB
Virtual Memory: In Use: 8,815 MB
```

```
C:\Windows\system32\cmd.exe + C:\Users\ARTI>
Network Card(s):
  6 NIC(s) Installed.
    [01]: MediaTek MT7921 Wi-Fi 6 802.11ax PCIe Adapter
      Connection Name: Wi-Fi
      DHCP Enabled: Yes
      DHCP Server: 192.168.66.32
      IP address(es)
        [01]: 192.168.66.91
        [02]: fe80::d0c7:89ed:d4a0:7605
        [03]: 2409:4056:e1c:4cc9:8c4:8a92:31a5:e3ab
        [04]: 2409:4056:e1c:4cc9:b445:fb49:ae20:9971
    [02]: Bluetooth Device (Personal Area Network)
      Connection Name: Bluetooth Network Connection
      Status: Media disconnected
    [03]: ExpressVPN TUN Driver
      Connection Name: Local Area Connection
      Status: Media disconnected
    [04]: ExpressVPN TAP Adapter
      Connection Name: Ethernet 2
      Status: Media disconnected
    [05]: VMware Virtual Ethernet Adapter for VMnet1
      Connection Name: VMware Network Adapter VMnet1
      DHCP Enabled: No
      IP address(es)
        [01]: 192.168.175.1
        [02]: fe80::8d4c:ec:ce57c:84dd
    [06]: VMware Virtual Ethernet Adapter for VMnet8
      Connection Name: VMware Network Adapter VMnet8
      DHCP Enabled: No
      IP address(es)
        [01]: 192.168.206.1
```

◆ **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.

```
C:\Windows\system32\cmd.exe + C:\Users\ARTI>tracert 25.113.99.86
Tracing route to 25.113.99.86 over a maximum of 30 hops
  1  32 ms    3 ms    2 ms  25.113.99.86
Trace complete.

C:\Users\ARTI>tracert www.instagram.com
Tracing route to z-p42-instagram.c10r.instagram.com [2a03:2880:f28a:e0:face:b00c:0:4420]
over a maximum of 30 hops:
  1    2 ms    6 ms    9 ms  2409:4056:e1c:4cc9::8b
  2    *       *       *       Request timed out.
  3   102 ms   49 ms   38 ms  2405:200:31d:eeee:20::332
  4    87 ms   42 ms   41 ms  2405:200:801:1a00::782
  5    *       *       *       Request timed out.
  6    *       *       *       Request timed out.
  7    *       *       *       Request timed out.
  8    *       *       *       Request timed out.
  9   123 ms   39 ms   62 ms  be7.mswlaf.01.del2.tfbnw.net [2a03:2880:f0a6:ffff::143]
 10   95 ms   59 ms   126 ms  instagram-p426-shv-01-del2.fbcdn.net [2a03:2880:f28a:e0:face:b00c:0:4420]
Trace complete.
```

◆ **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.

```
C:\Users\ARTI>netstat -an
Active Connections

Proto Local Address      Foreign Address      State
TCP   127.0.0.1:5354    LAPTOP-IL5U7B4G:49674 ESTABLISHED
TCP   127.0.0.1:5354    LAPTOP-IL5U7B4G:49675 ESTABLISHED
TCP   127.0.0.1:28624   LAPTOP-IL5U7B4G:28626 ESTABLISHED
TCP   127.0.0.1:28626   LAPTOP-IL5U7B4G:28624 ESTABLISHED
TCP   127.0.0.1:49674   LAPTOP-IL5U7B4G:5354 ESTABLISHED
TCP   127.0.0.1:49675   LAPTOP-IL5U7B4G:5354 ESTABLISHED
TCP   127.0.0.1:49701   LAPTOP-IL5U7B4G:49702 ESTABLISHED
TCP   127.0.0.1:49702   LAPTOP-IL5U7B4G:49701 ESTABLISHED
TCP   127.0.0.1:49703   LAPTOP-IL5U7B4G:49704 ESTABLISHED
TCP   127.0.0.1:49704   LAPTOP-IL5U7B4G:49703 ESTABLISHED
TCP   127.0.0.1:49705   LAPTOP-IL5U7B4G:49706 ESTABLISHED
TCP   127.0.0.1:49706   LAPTOP-IL5U7B4G:49705 ESTABLISHED
TCP   192.168.66.91:28699 20.198.118.190:https ESTABLISHED
TCP   192.168.66.91:31093 49.44.141.120:https ESTABLISHED
TCP   192.168.66.91:31418 20.42.73.28:https TIME_WAIT
TCP   192.168.66.91:31428 ec2-34-214-142-155:https TIME_WAIT
TCP   192.168.66.91:31429 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31430 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31431 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31433 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31434 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31435 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31436 ec2-34-213-3-182:https TIME_WAIT
TCP   192.168.66.91:31438 20.189.173.16:https TIME_WAIT
TCP   192.168.66.91:31442 192.168.66.32:domain TIME_WAIT
```

◆ **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.

```
C:\Users\ARTI>nslookup
Default Server: Unknown
Address: 192.168.66.32

> www.facebook.com
Server: Unknown
Address: 192.168.66.32

Non-authoritative answer:
Name: star-mini.c10r.facebook.com
Addresses: 2a03:2880:f18a:8a:face:b00c:0:25de
           163.70.146.35
Aliases: www.facebook.com

>
>
>
```

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

```
C:\Users\ARTI>
C:\Users\ARTI>
C:\Users\ARTI>
C:\Users\ARTI>gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\ARTI>
C:\Users\ARTI>
```

◆ **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-EECBBD7D833}
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.

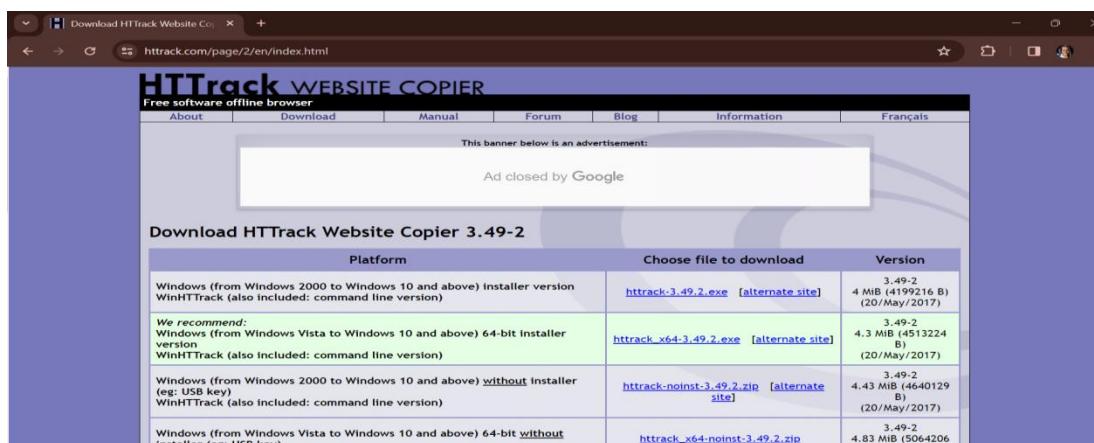
```
C:\Windows\system32\cmd.exe >
C:\Users\ARTI>net user
User accounts for \\LAPTOP-IL5U7B4G

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

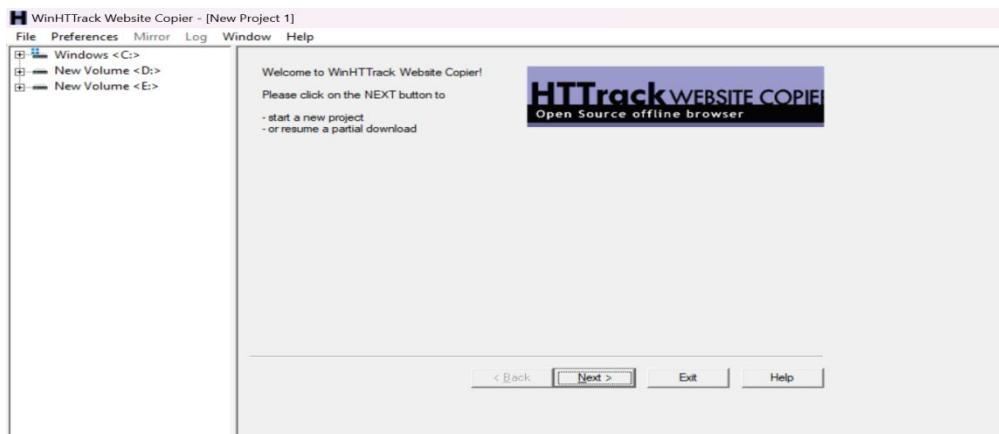
## # Use website copying tool for website copy (HT-TRACK).

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.

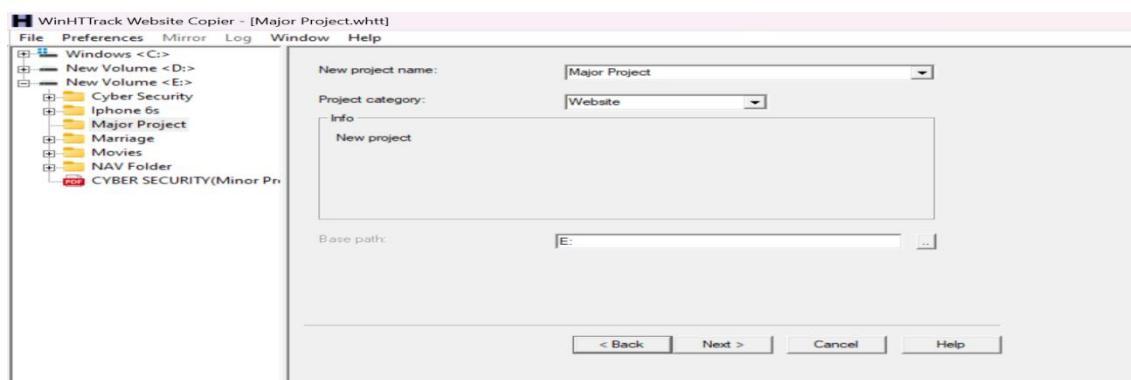
◆ Fisrtly we have to download and install HT-TRACK from <https://www.httrack.com>



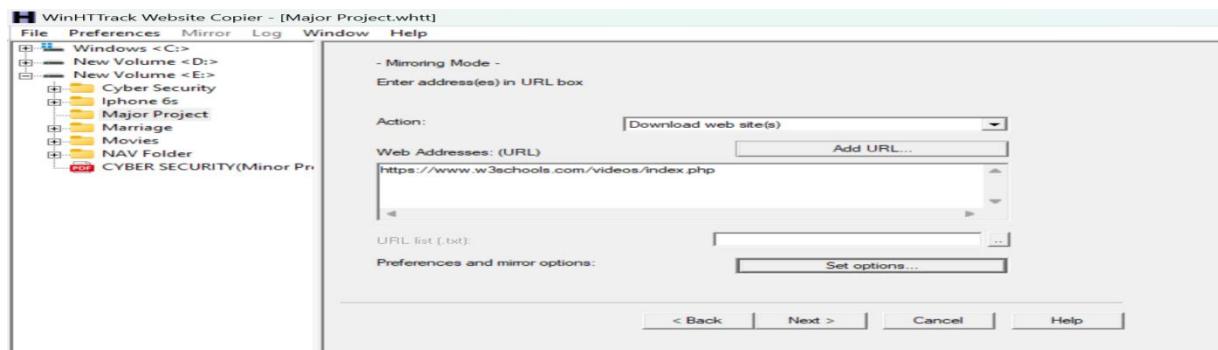
- ◆ After installing open the HT-TRACK and click next



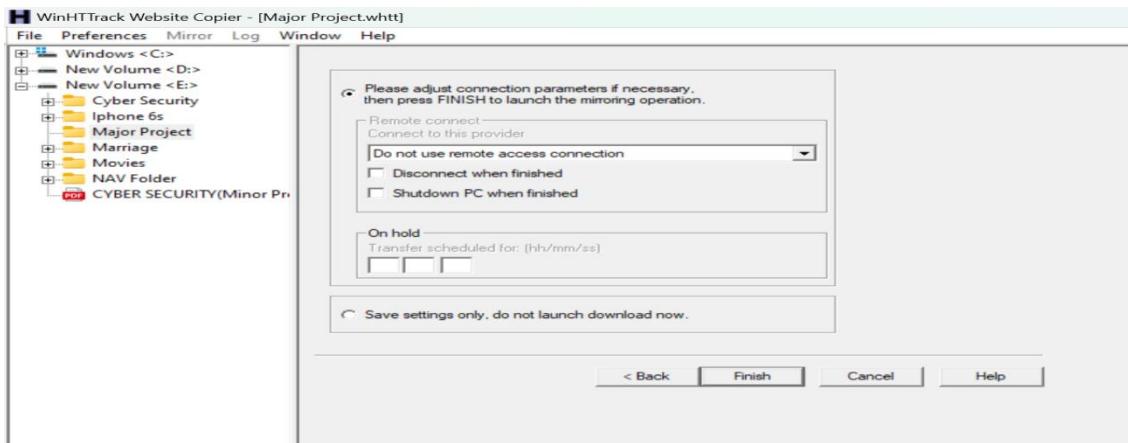
- ◆ Now fill the project name, project category and choose the path where website data will be saved.



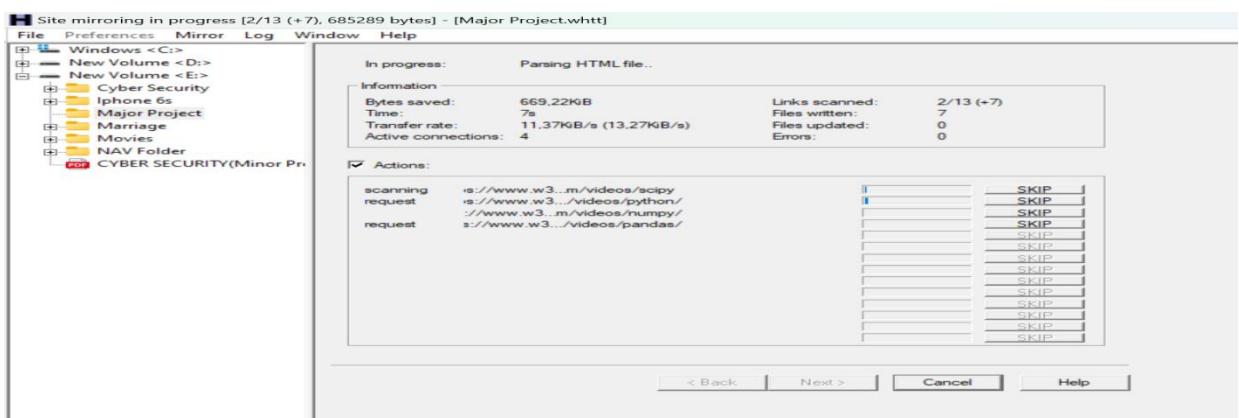
- ◆ Now choose action and type the website URL which you want to copy.



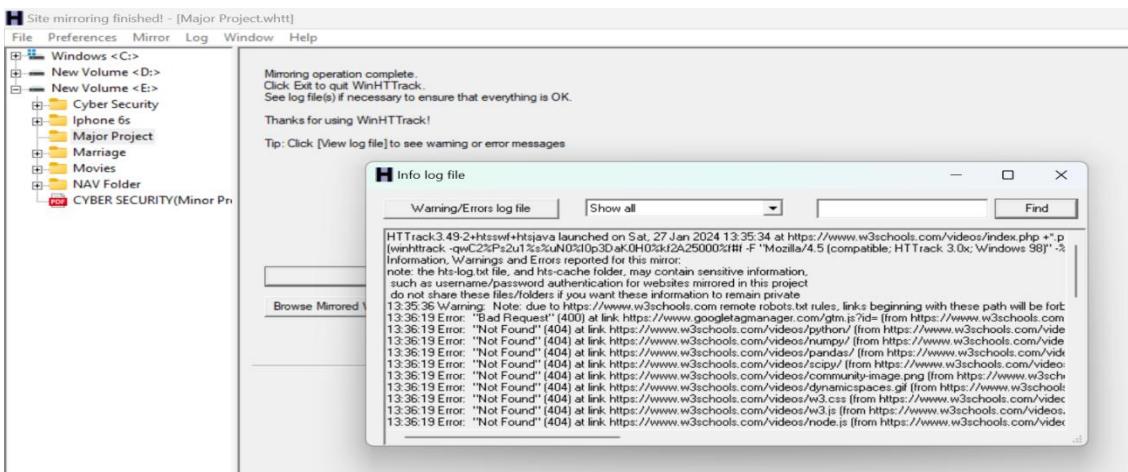
◆ Now select the options according to your requirements then click FINISH.



◆ Now the website contents are copying to your system.



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



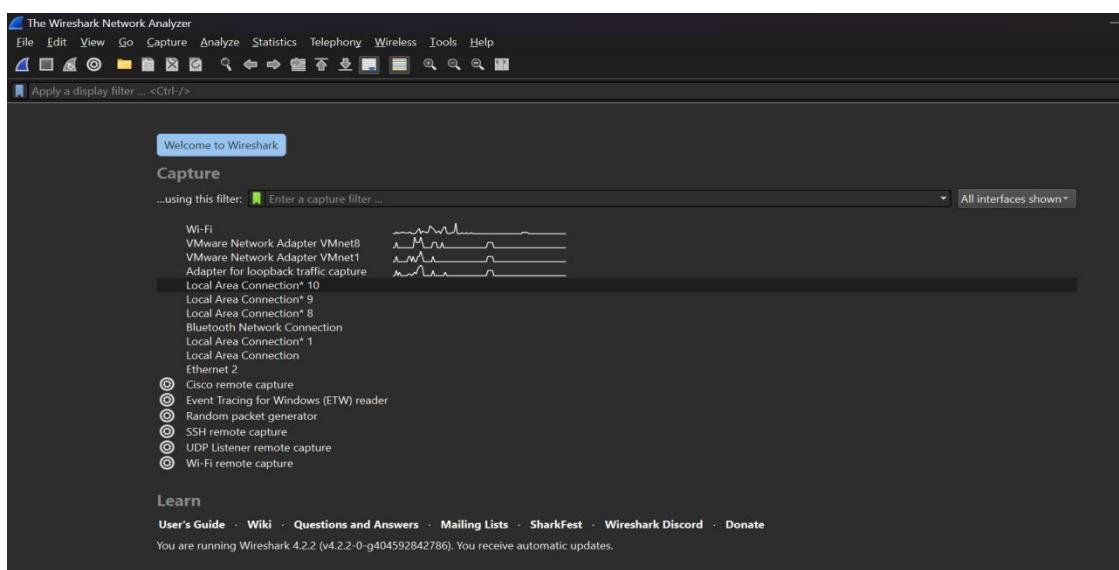
## # Use wireshark tool for packet capturing.

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.

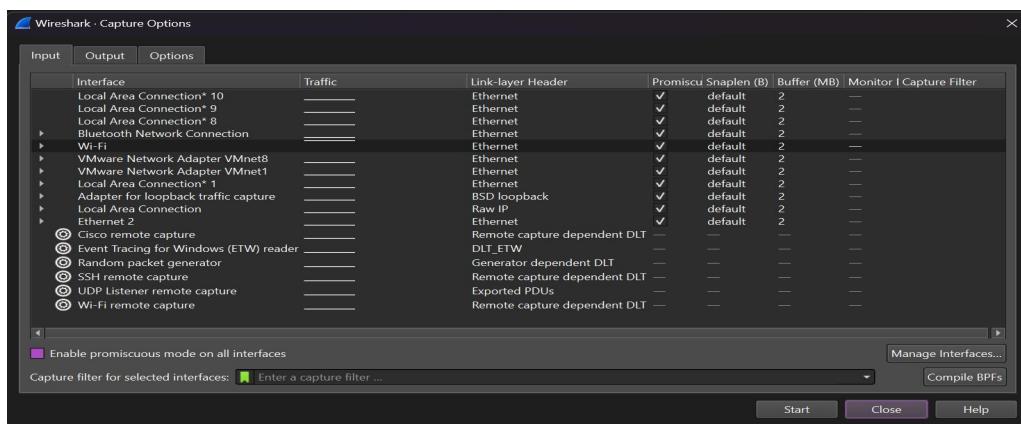
- ◆ Download and install wireshark tool from the link as :-  
<https://www.wireshark.org/>



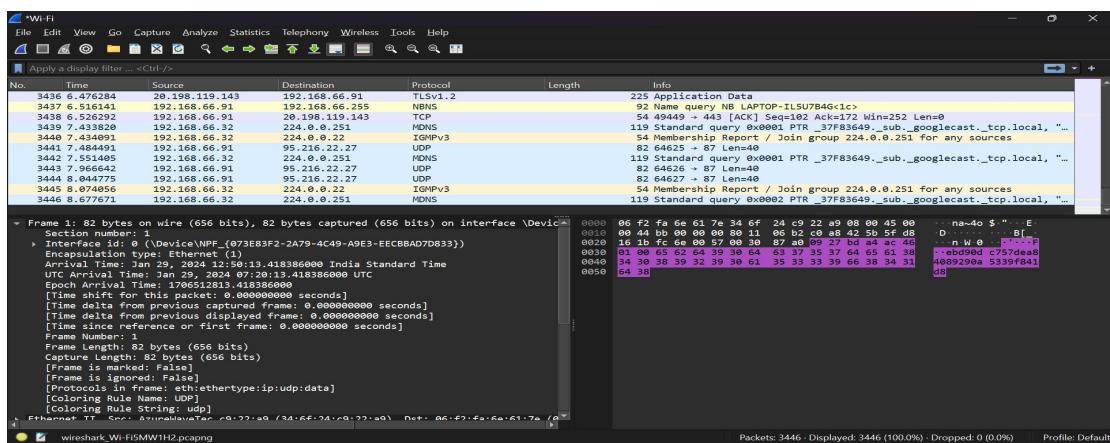
- ◆ After installing open the wireshark tool.



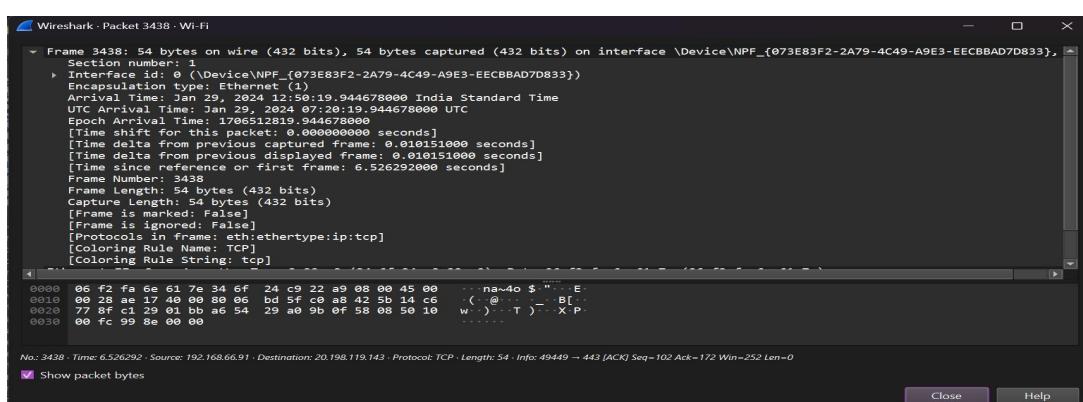
◆ Now click on capture then options, now select the network and click on START.



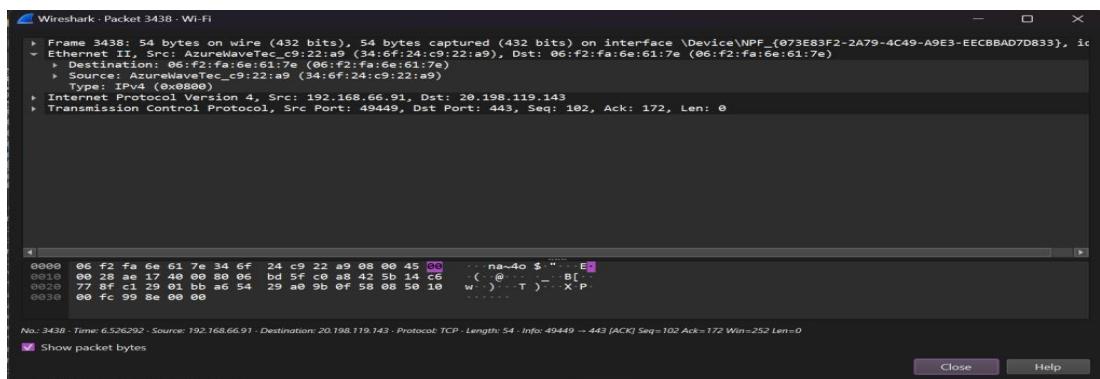
◆ Packets are capturing with showing their information.



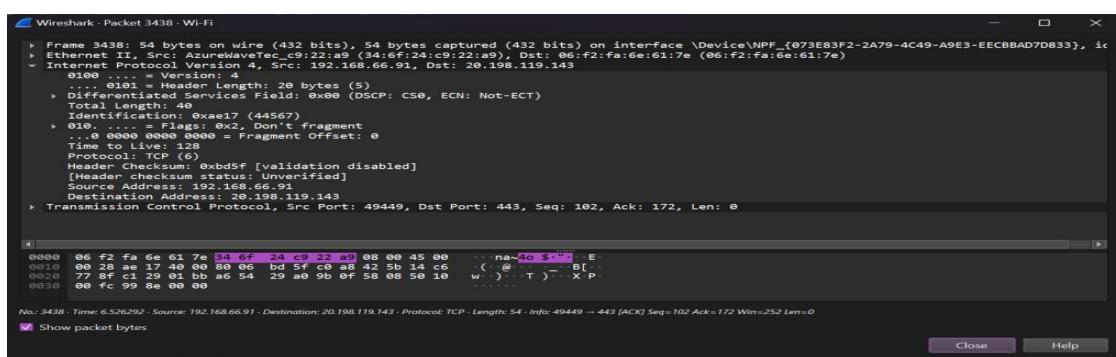
◆ Frame:- shows the complete information about frame like frame length, capture length, mac address,etc.



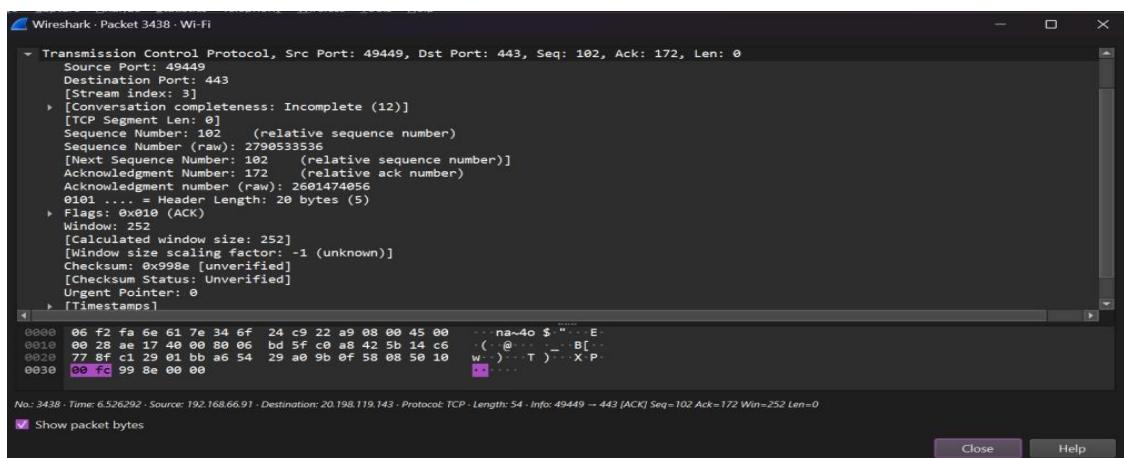
◆ It shows the type of network connection with source and destination address and the type of IP address.



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



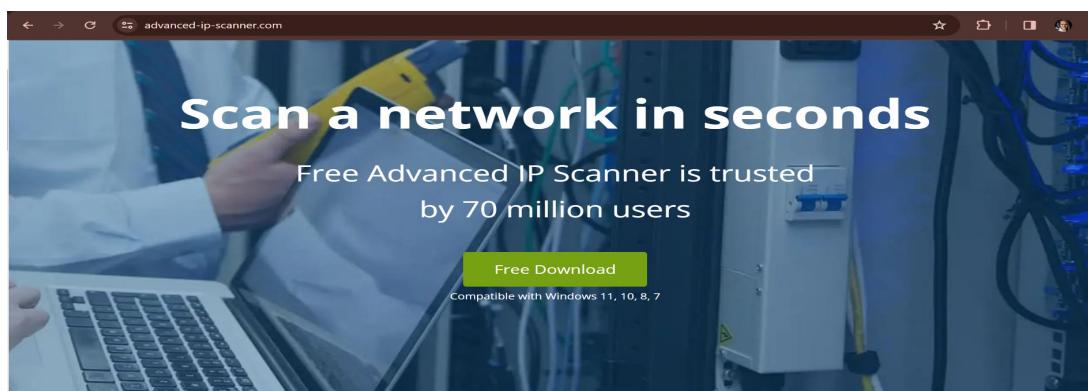
◆ The next pop up shows the information about TCP information with source and destination port no., acknowledgement of packet, etc.



# #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.

A screenshot of the Advanced IP Scanner software window. The interface includes a menu bar with File, View, Settings, and Help. Below the menu is a toolbar with icons for Scan, Stop, IP, C, and others. The main area displays a table of scan results for the IP 172.20.10.1-14. The table columns are Status, Name, IP, Manufacturer, MAC address, and Comments. One entry is shown: "LAPTOP-IL5U7B4G" with IP 172.20.10.1, manufacturer AzureWave Technology Inc., and MAC address 34:6F:24:C9:22:A9. A note below the table says "9E:E3:3F:68:ED:64".

## ◆ Web wiz tool:-

A screenshot of the Web Wiz Network Tools website. The header includes the Web Wiz logo, a menu icon, and links for Knowledgebase and Customer Login. The main content area has a dark green header with "Network Tools from Web Wiz" and a search bar. Below the header, a breadcrumb trail says "You are here: Home &gt; Network Tools". The main content area is titled "Free Domain, DNS, IP, Email &amp; Website Tools". It includes a sub-section for "DNS Tools" with links to "NsLookup Tool", "DNS Report Tool", and "Reverse DNS Lookup Tool". To the right of the content is a globe icon with a gear inside.

- ❖ 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

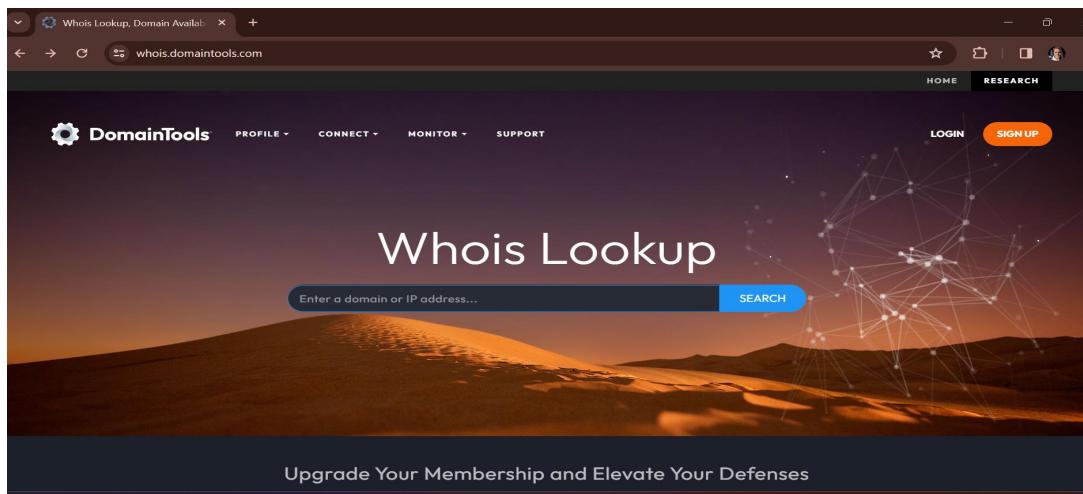
Trace Route from: Web Wiz [Poole - United Kingdom]

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.

A screenshot of the DomainTools website showing the IP Information page for the IP address 170.20.10.13. The page has a header with the same navigation and search bar as the previous screenshot. Below the header, the title is "IP Information for 170.20.10.13". There are two main sections: "Quick Stats" and a large table of detailed IP information. The "Quick Stats" section includes fields like IP Location (United States New York CBS Corporation), ASN (AS6102 CBSCORPORATE, US), Whois Server (whois.arin.net), and IP Address (170.20.10.13). The detailed table contains numerous entries such as NetRange, CIDR, NetName, NetHandle, Parent, NetType, OriginAS, Organization, RegDate, Updated, Ref, OrgName, OrgId, Address, City, StateProv, and more. To the right of the table, there's a sidebar for "DomainTools Iris" and a "Tools" section with dropdown menus for Monitor Domain Properties, Reverse IP Address Lookup, and Network Tools.