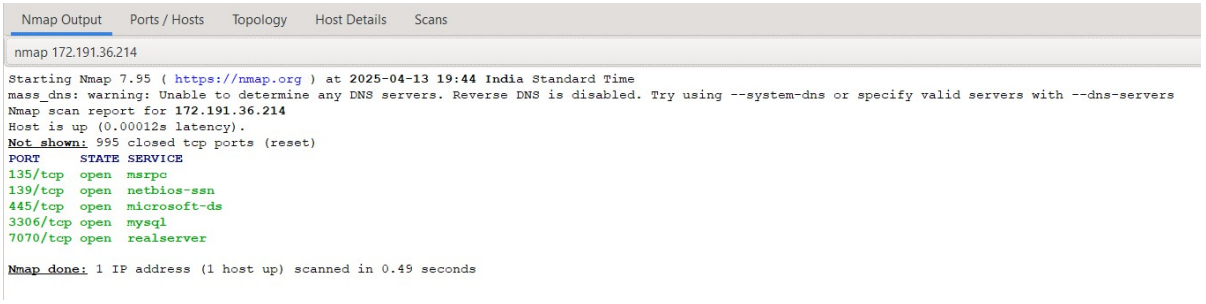
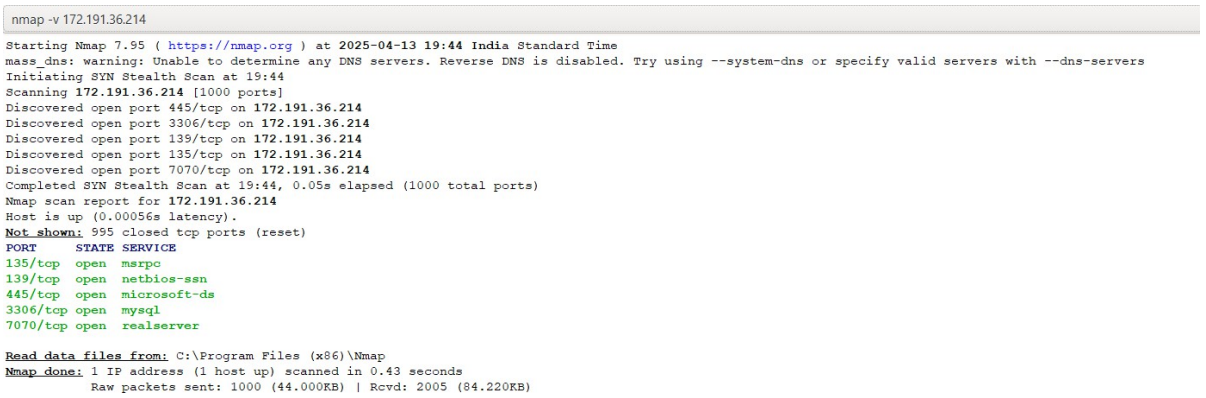
Assignment-11

1. Basic Nmap Commands

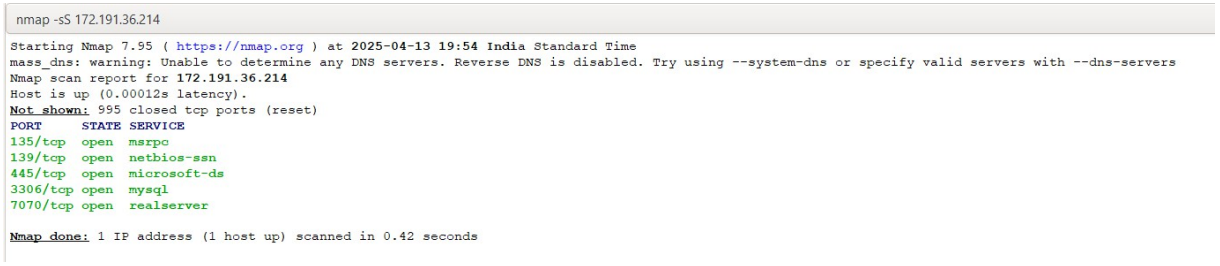
nmap<target> **Basic scan of a target (IP or hostname)**



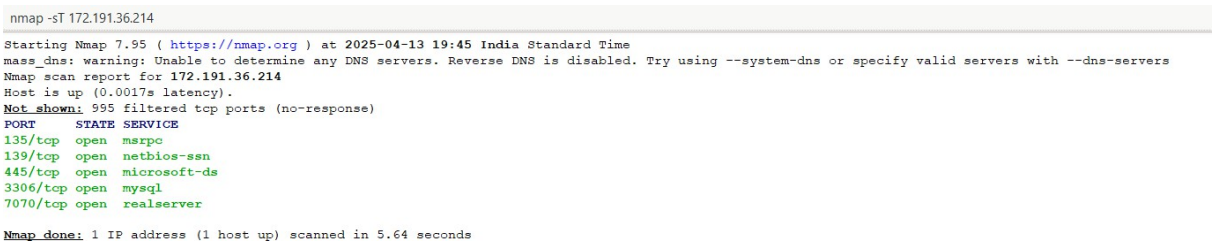
nmap – v <target> **Verbose output of the scan**



nmap -sS <target> **SYN (Stealth) scan**



nmap -sT <target> **TCP Connect scan (less stealthy)**



nmap -sU <target> **UDP scan**

nmap -sU 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:45 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00031s latency).
Not shown: 990 closed udp ports (port-unreach)
PORT     STATE         SERVICE
80/udp   open|filtered http
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
443/udp  open|filtered https
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 181.33 seconds
```

nmap -p <target> Scan all 65535 ports

nmap -p - 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:46 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00034s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3306/tcp  open     mysql
5040/tcp  open     unknown
7070/tcp  open     realserver
7680/tcp  open     pando-pub
8885/tcp  open     unknown
8886/tcp  open     unknown
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown
49672/tcp open     unknown
49688/tcp open     unknown
57272/tcp open     unknown
57621/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

nmap -O <target> Try to detect OS

nmap -O 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:47 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00042s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
7070/tcp open  realserver
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=4/13%OT=135%CT=1%CU=34769%PV=N%DS=0%DC=L%G=Y%TM=67FBC7
OS:84%P=i686-pc-windows-windows)SEQ(SP=103%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=
OS:1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=F2%GCD=1%ISR=10C%TI=I%CI=I%II=
OS:I%SS=S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD
OS:7NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFF
OS:F%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%
OS:DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=
OS:0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R
OS:=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=
OS:AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

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 10.70 seconds
```

nmap -A <target> Aggressive scan (OS, version, script scanning, traceroute)

nmap -A 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:48 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00051s latency).
Not shown: 995 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?
3306/tcp open  mysql            MySQL (unauthorized)
7070/tcp open  ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2023-07-27T16:15:58
|_Not valid after:  2073-07-14T16:15:58
|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=4/13%OT=135%CT=1%CU=32230%PV=N%DS=0%DC=L%G=Y%TM=67FBC7
OS:CA%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=106%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FC%GCD=1
OS:%ISR=FF%TI=I%CI=I%II=I%TS=A)SEQ(SP=FE%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%
OS:TS=A)SEQ(SP=FF%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD7NW8ST1
OS:1%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11%O6=MF
OS:FD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y
OS:%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q
OS:=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%
OS:A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%D
OS:F=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O
OS:=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80
OS:%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-04-13T14:18:39
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.82 seconds
```

nmap -sV <target> Detect service versions

nmap -sV 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:49 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00091s latency).
Not shown: 995 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?
3306/tcp open  mysql            MySQL (unauthorized)
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 11.96 seconds
```

nmap -T4 <target> Faster scan timing (T0 to T5, T4 is common for speed)

nmap -T4 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:50 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.000071s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

nmap -Pn <target> Skip host discovery (assume host is up)

nmap -Pn 172.191.36.214

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:50 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00016s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

nmap --script vuln <target> **Run common vulnerability scripts**

```
nmap --script vuln 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:52 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00034s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
7070/tcp open  realserver

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 29.05 seconds
```

2. Capturing and Analyzing Network Traffic Using Wireshark

1. Download and Install Wireshark:

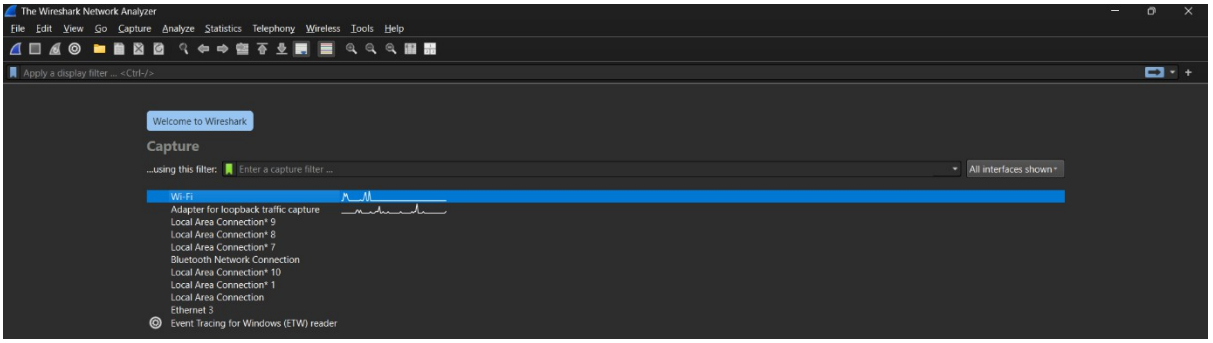
o Visit https://www.wireshark.org/

o Download and install the latest version for your operating system.

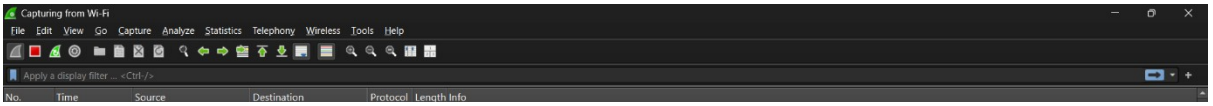
2. Start a Packet Capture Session:

o Open Wireshark.

o Select your active network interface (e.g., Wi-Fi or Ethernet).



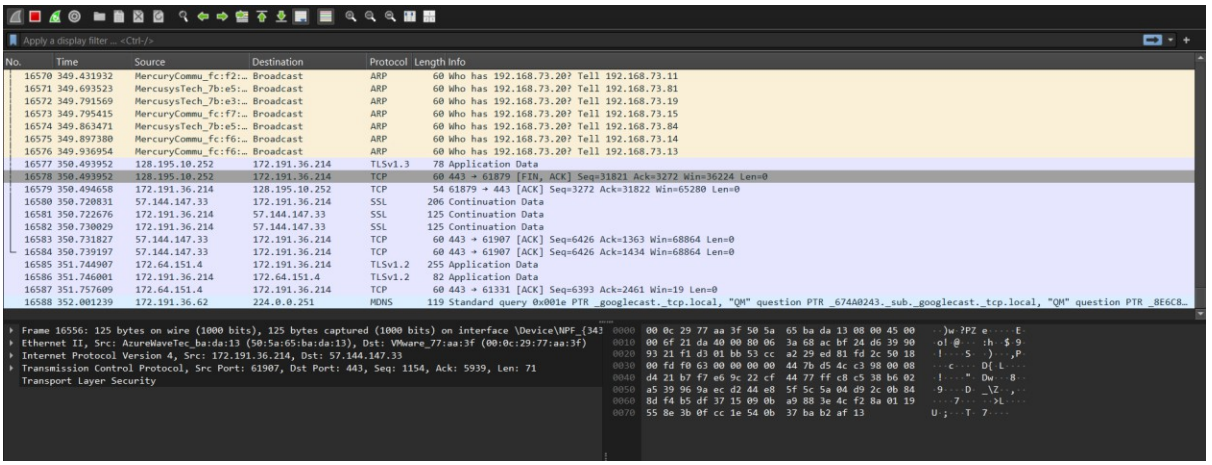
o Click the Start Capturing Packets button (shark fin icon).



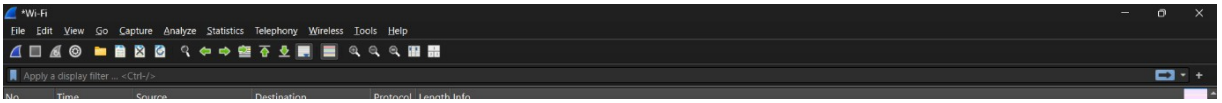
3. Generate Some Network Traffic:

o Open a web browser and visit a few websites.

o You may also open apps that use the internet like email or messaging tools.

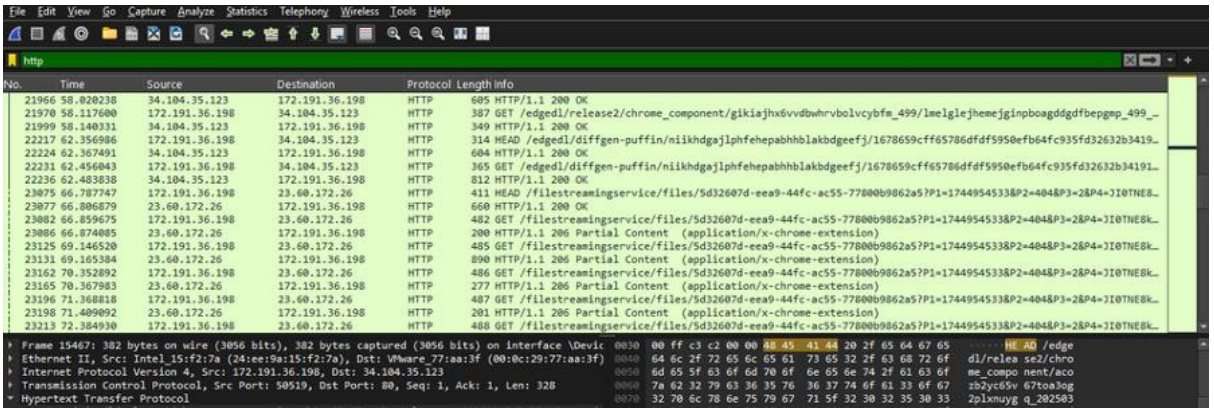


4. **Stop the Capture:**
   o After about 2–5 minutes, stop the capture using the red square icon in Wireshark.

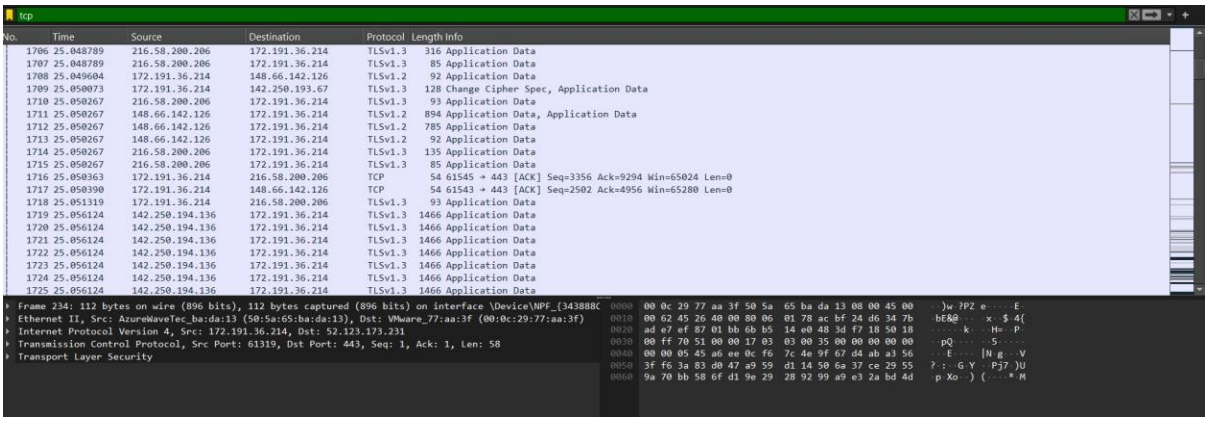


5. **Analyze the Traffic:**
   o Use filters Simple filter HTTP, DNS, or TCP to view specific types of traffic.

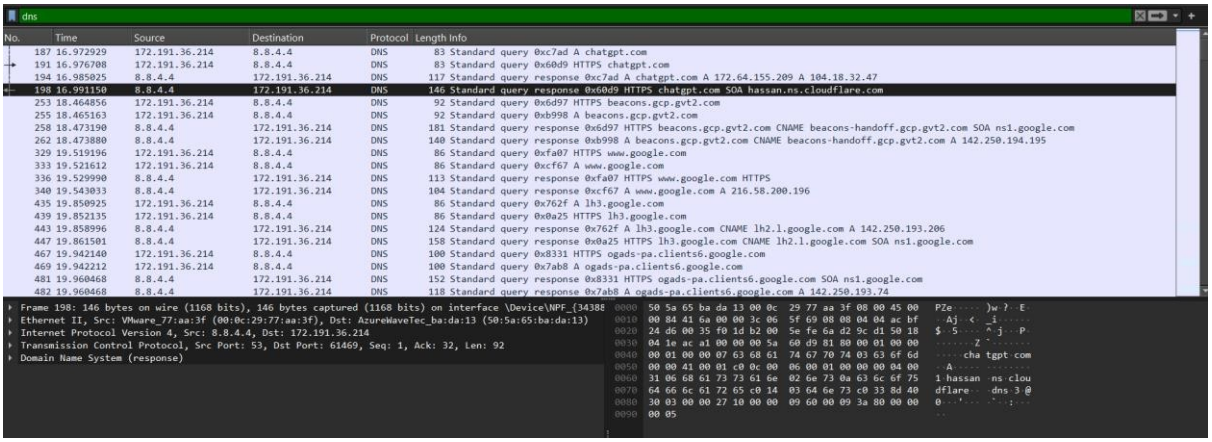
HTTP :



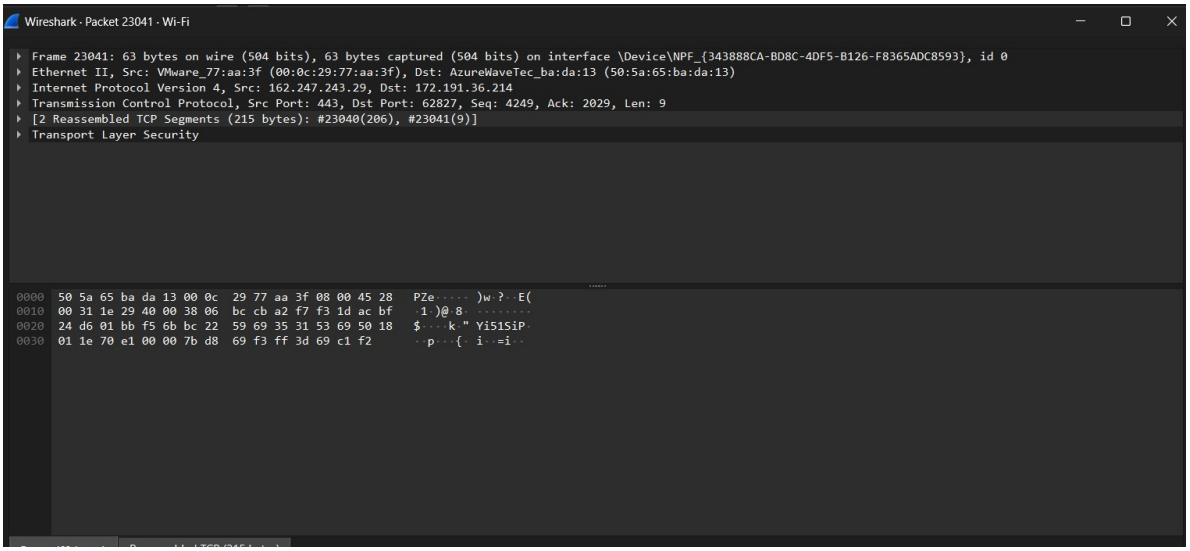
TCP :

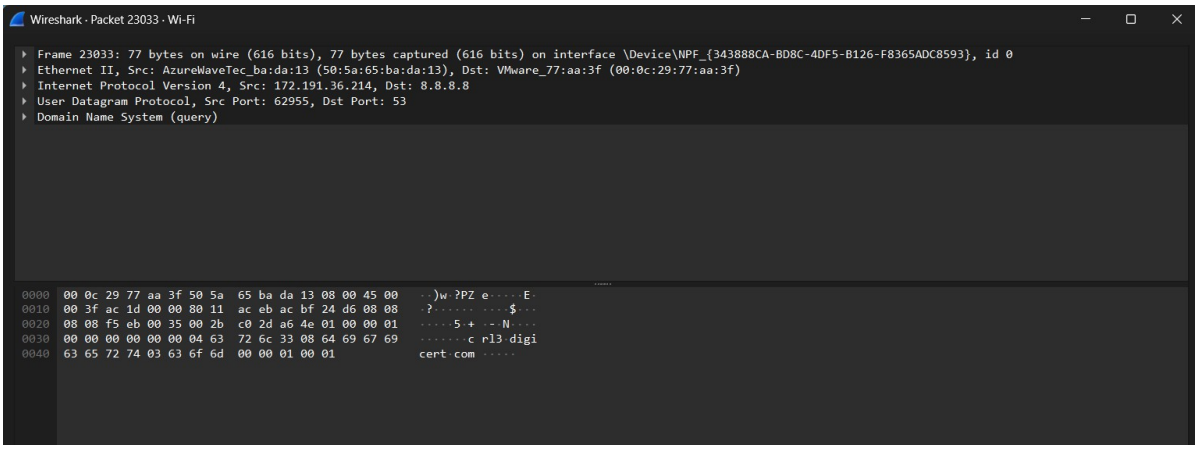


DNS :



o Select a few packets and inspect their details in the packet details pane.





6. **Export Your Capture: Save the capture as a .pcapng file for later review.**

   https://drive.google.com/drive/folders/1aHY89uyl8rcGuUdVozl8XzqsG5Se3KVf?usp=drive_link

Theory:-

Assignment-11

1) Basic Nmap Commands

	Command	Description
a)	nmap <target>	Basic scan of a target
b)	nmap -v <target>	verbose output of the scan
c)	nmap -sS <target>	SYN (stealth) scan
d)	nmap -sT <target>	TCP connect scan (less stealthy)
e)	nmap -sU <target>	UDP scan
f)	nmap -p <Port> <target>	scan specific port(s)
g)	nmap -p <target>	scan all 65535 ports
h)	nmap -O <target>	try to detect OS
i)	nmap -A <target>	aggressive scan (OS, version, script scanning)
j)	nmap -sV <target>	detect service versions
k)	nmap -T4 <target>	faster scan timing (T0 to T5, T4 is common for speed)
l)	nmap -Pn <target>	skip host discovery (assume host is up)
m)	nmap -iL target.txt	scan multiple targets from a file.
n)	nmap -oN output.txt <target>	save output in normal format
o)	nmap --script <script-name> <target>	run specific NSE script
p)	nmap --script vuln <target>	Run common vulnerability scripts.

2. Capturing and analyzing network traffic using wireshark.

Q1 What interface did you select for capturing packets?

Soln For capturing packets, I selected Wi-Fi interface because my computer is connected to the internet via a wireless network. In wireshark all available network interfaces are listed when the application is launched, and selecting the correct one is essential to monitor the traffic effectively. The Wi-Fi interface typically shows ongoing data transmission in the form of spikes which indicates active network traffic. This interface allows the capture of all incoming and outgoing packets from the wireless connection in real-time.

Q2 List 3 protocol you observed during the capture session?

Soln I observed the three commonly used network protocols.

1) HTTP (Hyper text transfer protocol) used for transferring web page over the internet. I noticed several HTTP requests when I opened different websites.

2) DNS (Domain name system)
this protocol translates domain names into IP addresses whenever I typed a URL, DNS packet generated to resolved the IP address.

3) TCP (Transmission control protocol)
A connection-oriented protocol that ensures reliable communication between devices. TCP packets were visible in every connection, especially during communications.

Q3 Pick one HTTP packet. What was the host website being accessed?

⇒ I selected an HTTP GET request packet during the session. The host accessed in that particular packet was:
www.example.com (Note: Replace this with actual domain name you saw during my session such as www.google.com, www.wikipedia.org etc.
In the packet details, under the HTTP section the 'Host' field displays the exact domain being requested. The host field shows which server my browser was typing to reach using the HTTP protocol.

Q4 What is the IP address of your system and the destination IP for the selected packet?

1) Ethernet II. This is the data link layer that includes the MAC addresses of the source and destination devices within the local network.

2) Internet Protocol version 4 (IPV4)
This is the network layer, responsible for identifying source and destination IP address.

3) Transmission control protocol. (TCP)
This is the transport layer, ensuring reliable transmission and providing ports to identify applications.

4) Hypertext Transfer Protocol (HTTP)
This is the application layer, where the actual web request (such as GET or POST) is visible.
Each layer wraps the data from the layer above, which is called encapsulation when the packet is received the layers are de-encapsulated in reverse order.

Q) What did you learn from this activity about how data travels over the internet?

⇒ This activity offered a hands-on understanding of how data travels through the internet using different Protocol layers.

Some Key takeaways :-

1) layer architecture - Data is encapsulated in layer (ethernet, IP, HTTP, TCP) during transmission and de-encapsulated at the receiver's end.

2) Protocol role :- Each protocol serves a specific function - for example, DNS resolves domain names, IP handles addressing and TCP ensures reliable delivery.

3) Traffic visibility - wireshark allows us to inspect the raw data being transmitted including requests to websites, responses from servers, and system interactions with network.

4) Security considerations: observing how easily HTTP data can be read underscores the importance of using HTTPS for secure communication.

5) Packet-level understanding - viewing each packet's structure gives a deeper appreciation of the technical details involved in something as simple as opening a web page.