Network Basics For Cyber Security

1.What it is IP Address:-

An IP address is a unique number given to every device on a network so it can communicate.

Example: 192.168.1.10

Types:

Private IP → Used inside home/office networks

Example: 192.168.x.x

Public IP → Given by ISP, visible on the internet

2.What it is Mac Address:-

A MAC address is a hardware (physical) address of your network card.

Example:00:1A:2B:3C:4D:5E

Key points:

Fixed (does not change)

Assigned by manufacturer

Works at local network level

3.What it is DNS:-

DNS converts website names into IP addresses.

Example:google.com → 142.250.190.14

Why DNS exists:

Humans remember names, computers understand numbers.

4.What it is TCP:-

TCP is a reliable connection-oriented protocol.

Features:

Data arrives in order

Lost packets are retransmitted

Slower but very reliable

Used for:

Websites (HTTP/HTTPS)

Emails

File downloads

5.What it is UDP:-

UDP is a fast but unreliable protocol.

Features:

No connection setup

No packet confirmation

Faster than TCP

Used for:

Video calls

Online gaming

Live streaming

WIRESHAK

Step 1: Download Wireshark:-

> Open your browser

>Go to https://www.wireshark.org

>Click Download

>Choose your OS:

>Windows

>Linux

>macOS

Step 2: Install Wireshark:-

>Run the installer

>Keep default options

>IMPORTANT:

> Check Install Npcap (required to capture packets)

>Finish installation

Step 3: Launch Wireshark:-

>Open Wireshark

>You will see network interfaces:

>Wi-Fi

>Ethernet

>Loopback

Step 4: Start Live Capture:-

>Double-click the active interface

OR

>Select interface → Click Start (blue shark fin)

Live packets will start appearing immediately.

Step 5: Generate Traffic (for testing):-

Open a website (Google, YouTube)

Ping a site:Bash

ping google.com

Use WhatsApp Web / Email

You'll see packets instantly.

Step 6: Stop Capture & Save:-

Click Stop (red square)

File → Save As → .pcapng

Step 7: Basic Filters (Very Important):-

Use Display Filters (top bar):

Purpose

Filter

HTTP traffic

http

HTTPS

tls

DNS

dns

ICMP (ping)

icmp

Specific IP

ip.addr == 8.8.8.8

Three-Way TCPHandshake

What is TCP 3-Way Handshake (Quick Theory):-

TCP uses a 3-step process to establish a reliable connection between a client and a server:

SYN → Client asks to start a connection

SYN-ACK → Server agrees and acknowledges

ACK → Client confirms

connection established

Client Server

| ---- SYN ---------> |

| <--- SYN, ACK ----- |

| ---- ACK ---------> |

Step 1: Start Packet Capture in Wireshark:-

Open Wireshark

Select your active interface (Wi-Fi / Ethernet)

Click Start Capture (blue shark fin)

Step 2: Generate TCP Traffic:-

Do any one of these:

Open a website (example: google.com)

Use terminal:

Bash

curl http://example.com

or

Bash

ping google.com

Step 3: Apply TCP Filter:-

In Display Filter bar, type:

tcp

Press Enter

Step 4: Identify the 3-Way Handshake:-

Look at the Info column. You will see packets like:

Step

Packet

Meaning

1 . SYN

Client → Server

2. SYN, ACK

Server → Client

3. ACK

Client → Server

These three consecutive packets form the TCP handshake.

Step 5: Verify Using TCP Flags (Important):-

Click each packet and expand:

Transmission Control Protocol

You will see Flags:

Packet

Flags

SYN

0x002 (SYN)

SYN-ACK

0x012 (SYN, ACK)

ACK

0x010 (ACK)

✔ This confirms the handshake.

Step 6: (Optional) Use SYN Filter Only:-

To see only handshake start packets:

tcp.flags.syn == 1

To see only pure SYN (first step):

tcp.flags.syn == 1 && tcp.flags.ack == 0

Plain text vs Encrypted text

Plain Text:-Data is sent without encryption, so anyone capturing packets can read it.

How to identify:-

Protocols like HTTP, FTP, Telnet, SMTP

In Wireshark, the packet details show readable text

You can see: URLs, Usernames & passwords & Form data.

Example: username= admin & password=1234

Encrypted Text:-

Data is encrypted before transmission.

How to identify:-

Protocols like HTTPS (TLS/SSL), SSH, SFTP

In Wireshark:

Data looks random / unreadable

You see TLS Handshake, not actual content

No visible usernames or passwords

Example: 7f a9 3c b2 8e ... (cipher text)

DNS Queries

Capturing DNS Queries:-

1.Open Wireshark

2.Select active network interface (Wi-Fi / Ethernet)

3.Apply display filter: dns

4.Open a browser and visit any website (e.g., google.com)

Wireshark will immediately show DNS packets.

Analyzing DNS Traffic:-

What to observe in a DNS packet:

Source IP → Your device

Destination IP → DNS server (ISP / public DNS)

Query Name → Website domain (e.g., google.com)

Query Type →

A (IPv4 address)

AAAA (IPv6 address)

Response → IP address of the domain

Example: Query: www.google.com (Response: 142.250.182.36)

Saving Packet Captures

1.After capturing packets, click File → Save As

2.Choose file format:

.pcap / .pcapng (recommended)

3.Select location and filename

4.Click Save

PCAP files can be reopened anytime for offline analysis.

Observations

1. Network packets were successfully captured using Wireshark.
2. DNS queries were visible in plain text, showing the websites being accessed.
3. The TCP three-way handshake (SYN, SYN-ACK, ACK) was clearly observed before data transfer.
4. Plain text traffic (HTTP) showed readable information like URLs.
5. 6. Encrypted traffic (HTTPS/TLS) appeared unreadable and secure.
6. Source and destination IP addresses helped identify the communicating devices.
7. Saved packet capture files (.pcap/.pcapng) can be used later for offline analysis.
8. Encrypted traffic provides better security compared to plain text traffic.

One-Line Conclusion

Wireshark helps monitor, analyze, and understand network communication and security behavior.