Networking Basics for Cyber Security

January 19, 2026

1 Introduction

Networking basics are essential for cybersecurity as they explain how devices communicate over a network. Network communication can introduce security risks such as unauthorized access and cyber attacks. Understanding IP addresses, ports, and protocols helps in detecting and preventing network-based threats.

1. Basic Networking Concepts

IP Address

An IP address is a unique numerical identifier assigned to each device on a network. Example: 192.168.1.1

MAC Address

A MAC address is a physical hardware address of a network interface. Example: 00:1A:2B:3C:4D:5E

DNS (Domain Name System)

DNS converts domain names into IP addresses. Example: google.com → 142.250.183.14

TCP and UDP

- TCP is connection-oriented and reliable.
- UDP is connectionless and faster.

2. Install Wireshark and Capture Live Traffic

Wireshark is installed from the official website. After installation, the active network interface such as Wi-Fi or Ethernet is selected and packet capture is started.

3. Filtering Packets by Protocol

Wireshark display filters used:

- HTTP: `http`
- DNS: `dns`
- TCP: `tcp`
- UDP: `udp`
- HTTPS: `tls`

1.1 Screenshots of Network Protocols

1.1.1 HTTP Protocol

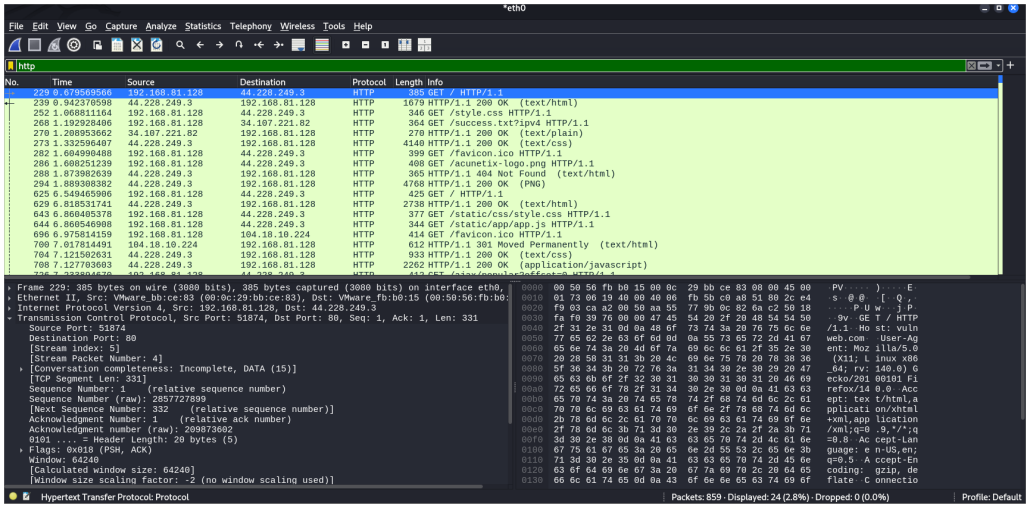

Figure 1: HTTP traffic captured in Wireshark

1.1.2 DNS Protocol

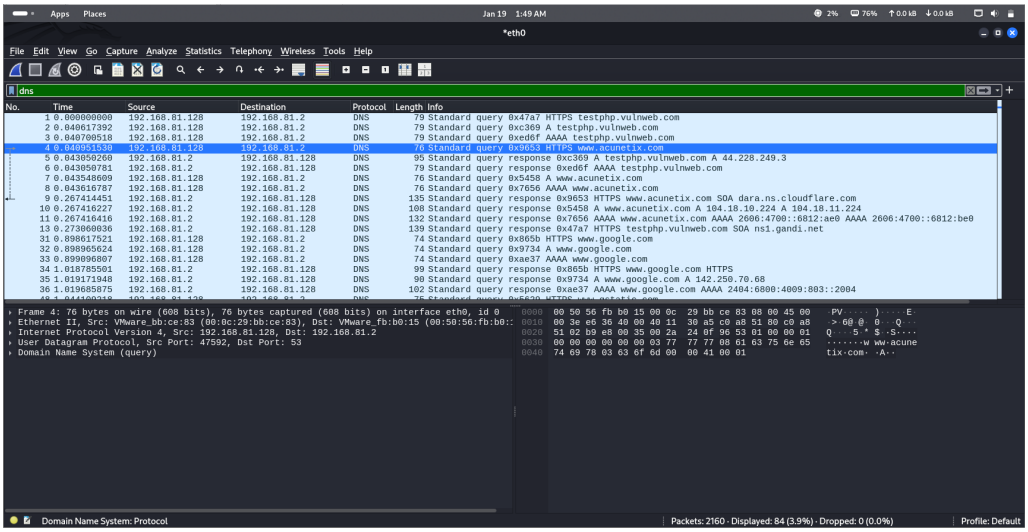

Figure 2: DNS query and response in Wireshark

1.1.3 TCP Protocol

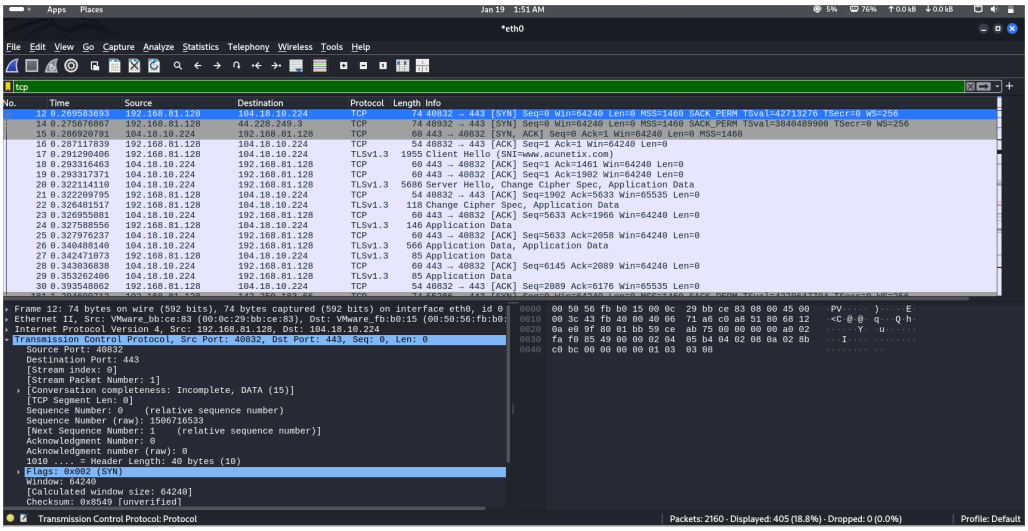

Figure 3: TCP packet communication

1.1.4 UDP Protocol

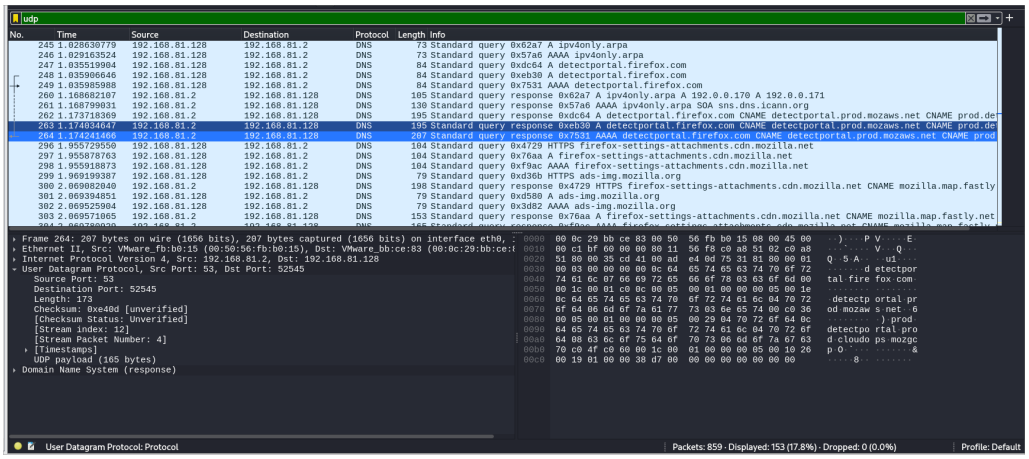

Figure 4: UDP packet transmission

1.1.5 HTTPS (TLS) Protocol

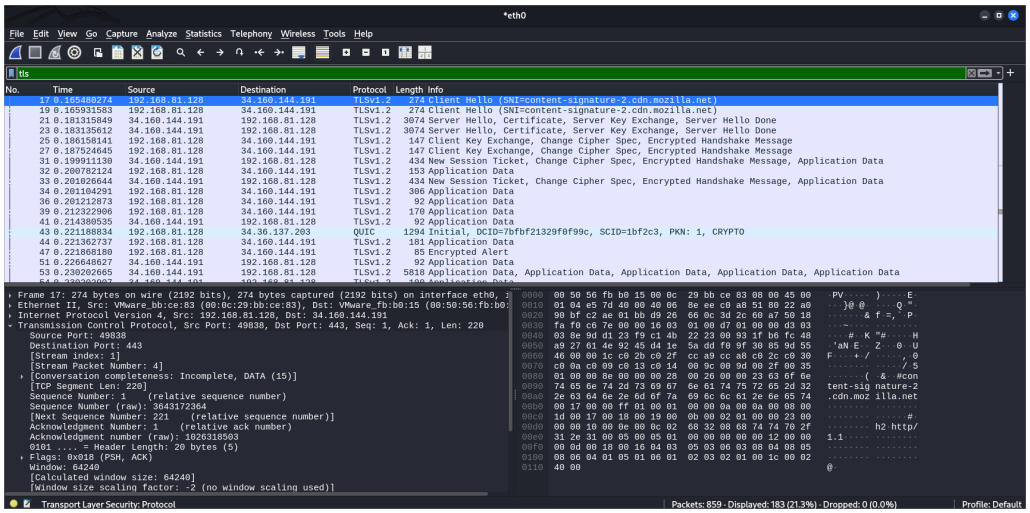

Figure 5: Encrypted HTTPS (TLS) traffic

4. Observing TCP Three-Way Handshake

TCP establishes a connection in three steps:

1. **SYN** – Client requests a connection.
2. **SYN-ACK** – Server accepts the connection request.
3. **ACK** – Client confirms the connection.

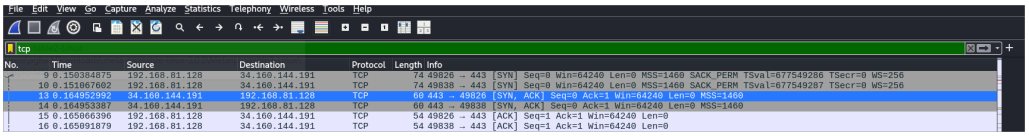

Figure 6: TCP Three way Handshake

5. Plain-Text Traffic vs Encrypted Traffic

- HTTP traffic is plain-text and readable.
- HTTPS traffic is encrypted and secure.

Screenshots: Plain-Text vs Encrypted Traffic

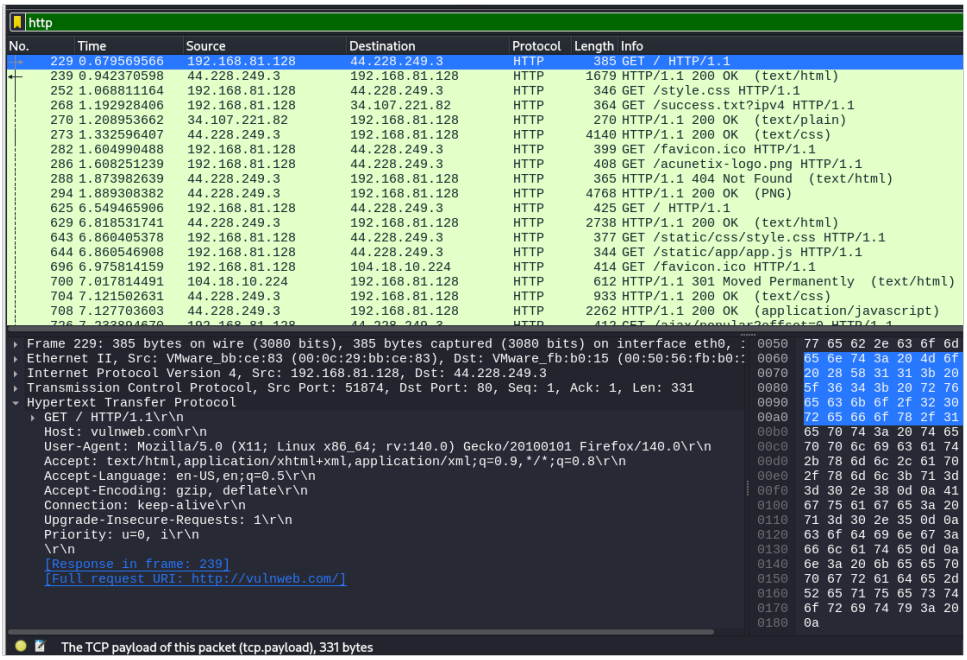

Figure 7: HTTP Plain-Text Traffic Captured in Wireshark

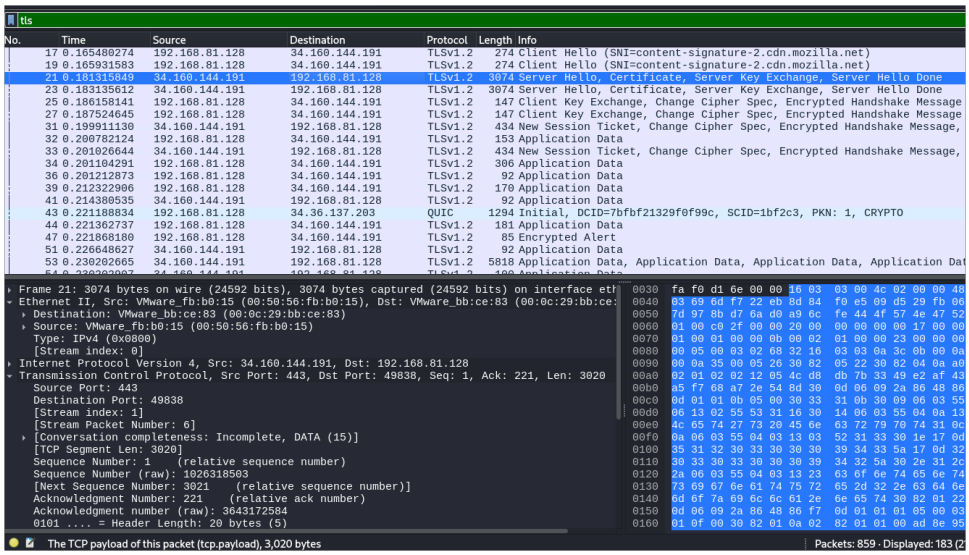

Figure 8: HTTPS Encrypted Traffic Captured in Wireshark

6. Capturing and Analyzing DNS Queries

DNS packets are captured using the `dns` filter to observe domain name resolution from domain names to IP addresses.

Screenshot: DNS Query Analysis

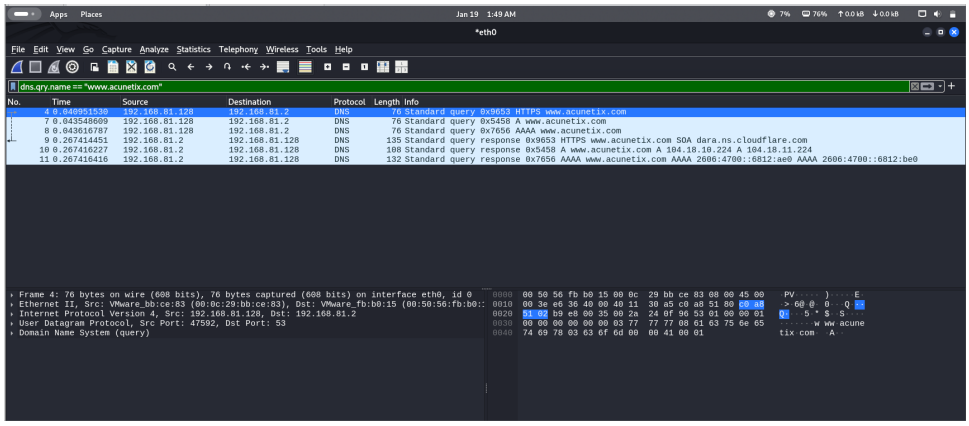

Figure 9: DNS Query and Response Captured in Wireshark

7. Saving Packet Captures

Captured packets are saved using **File** → **Save As** in `.pcapng` format.

Observations

- Wireshark captures real-time network traffic.
- DNS converts domain names to IP addresses.

- TCP uses a three-way handshake.
- HTTP traffic is insecure.
- HTTPS traffic is encrypted.

Summary

In this practical, basic networking concepts such as IP address, MAC address, DNS, TCP, and UDP were studied. Wireshark was installed and used to capture live network traffic. Packet filtering was performed using protocol-based filters such as HTTP, DNS, and TCP. The TCP three-way handshake was observed to understand connection establishment. Plain-text traffic (HTTP) and encrypted traffic (HTTPS) were identified and analyzed. DNS queries were captured to study domain name resolution. Finally, packet capture files were saved for future analysis, and observations were recorded in simple language.