

# 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

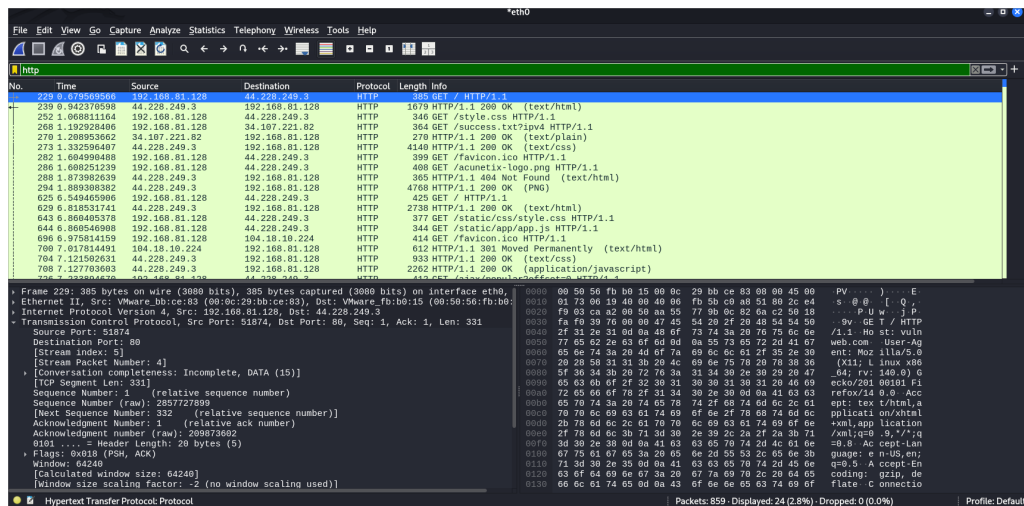


Figure 1: HTTP traffic captured in Wireshark

## 1.1.2 DNS Protocol

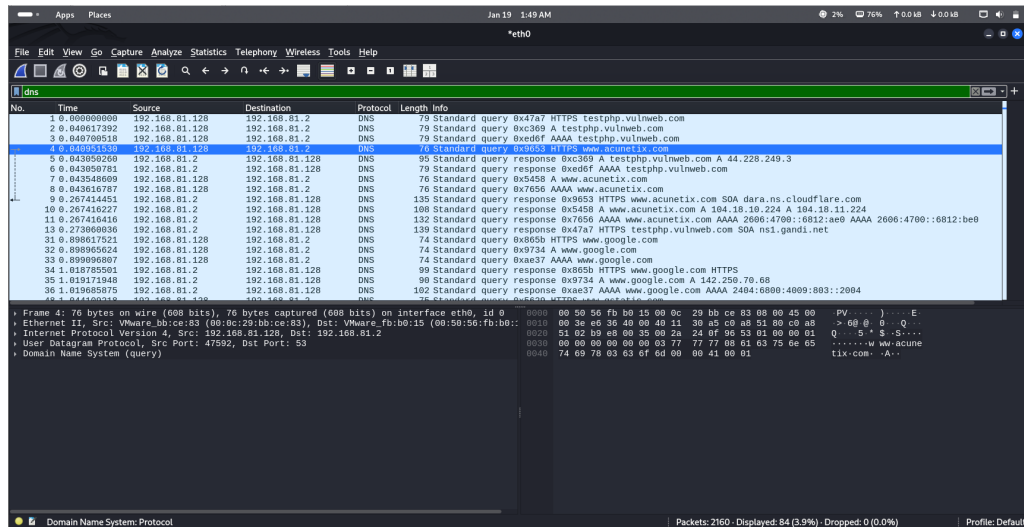


Figure 2: DNS query and response in Wireshark

## 1.1.3 TCP Protocol

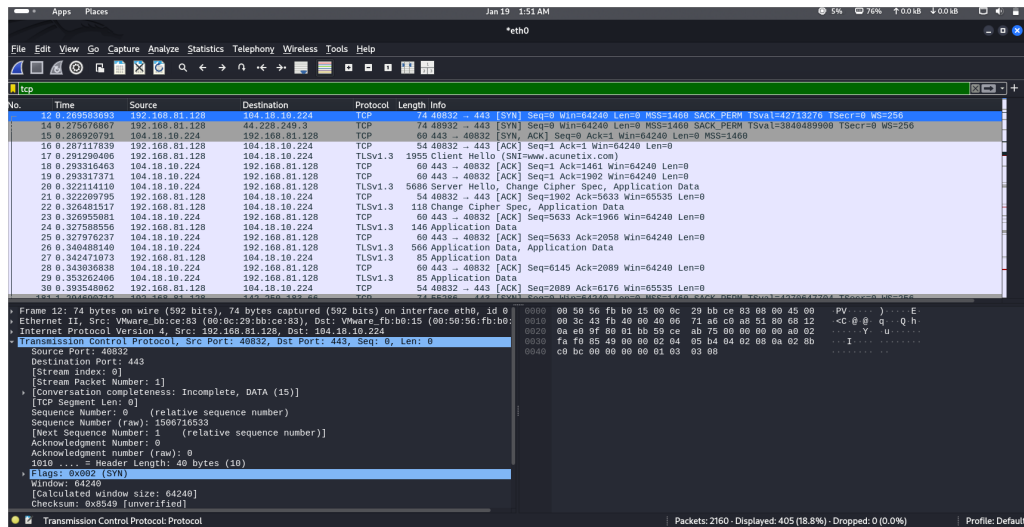


Figure 3: TCP packet communication

## 1.1.4 UDP Protocol

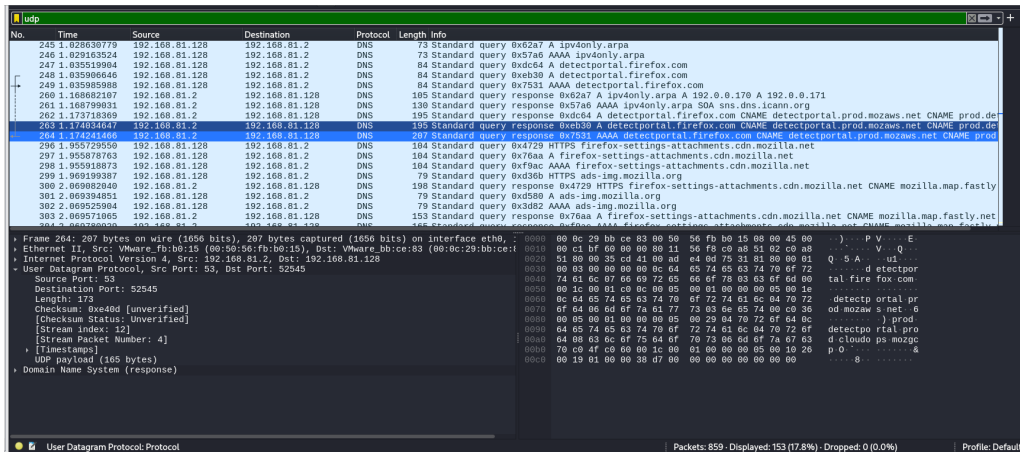


Figure 4: UDP packet transmission

## 1.1.5 HTTPS (TLS) Protocol

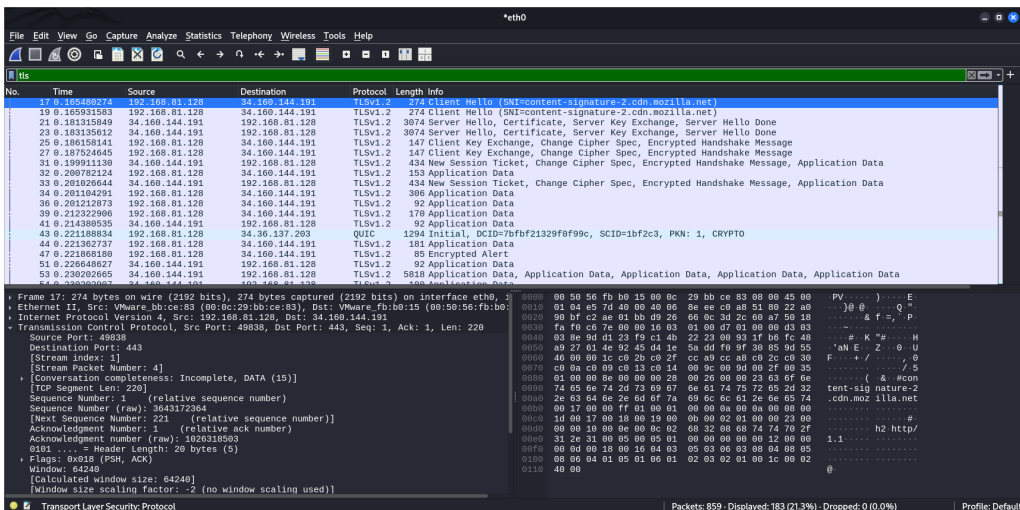


Figure 5: Encrypted HTTPS (TLS) traffic

# 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.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.150384875	192.168.81.128	34.109.144.191	TCP	74	49826 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=677549286 TSecr=0 WS=256
10	0.151087602	192.168.81.128	34.109.144.191	TCP	74	49838 → 443 [ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=677549287 TSecr=0 WS=256
16	0.165991879	192.168.81.128	34.109.144.191	TCP	54	49838 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

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

No.	Time	Source	Destination	Protocol	Length	Info
239	0.679569566	192.168.81.128	44.228.249.3	HTTP	385	GET / HTTP/1.1
239	0.942370598	44.228.249.3	192.168.81.128	HTTP	1679	HTTP/1.1 200 OK (text/html)
252	1.068811164	192.168.81.128	44.228.249.3	HTTP	346	GET /style.css HTTP/1.1
268	1.192928486	192.168.81.128	34.107.221.82	HTTP	364	GET /success.txt?ip=4 HTTP/1.1
270	1.208953662	34.107.221.82	192.168.81.128	HTTP	270	HTTP/1.1 200 OK (text/plain)
273	1.332596487	44.228.249.3	192.168.81.128	HTTP	4148	HTTP/1.1 200 OK (text/css)
282	1.604990488	192.168.81.128	44.228.249.3	HTTP	399	GET /favicon.ico HTTP/1.1
286	1.608251239	192.168.81.128	44.228.249.3	HTTP	408	GET /acunetix-logo.png HTTP/1.1
288	1.873982639	44.228.249.3	192.168.81.128	HTTP	365	HTTP/1.1 404 Not Found (text/html)
294	1.889308382	44.228.249.3	192.168.81.128	HTTP	4768	HTTP/1.1 200 OK (PNG)
625	6.549465906	192.168.81.128	44.228.249.3	HTTP	425	GET / HTTP/1.1
629	6.818531741	44.228.249.3	192.168.81.128	HTTP	2738	HTTP/1.1 200 OK (text/html)
643	6.860405378	192.168.81.128	44.228.249.3	HTTP	377	GET /static/css/style.css HTTP/1.1
644	6.860546908	192.168.81.128	44.228.249.3	HTTP	344	GET /static/app/app.js HTTP/1.1
696	6.975814159	192.168.81.128	104.18.10.224	HTTP	414	GET /favicon.ico HTTP/1.1
700	7.017814491	104.18.10.224	192.168.81.128	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
704	7.121502631	44.228.249.3	192.168.81.128	HTTP	933	HTTP/1.1 200 OK (text/css)
708	7.127703603	44.228.249.3	192.168.81.128	HTTP	2262	HTTP/1.1 200 OK (application/javascript)
726	7.223904670	192.168.81.128	44.228.249.3	HTTP	412	GET /static/popular-offers HTTP/1.1

Frame 239: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface eth0, ...  
 Ethernet II, Src: VMware\_b8:ce:83 (00:0c:29:bb:ce:83), Dst: VMware\_fb:b0:15 (00:50:56:fb:b0:15)  
 Internet Protocol Version 4, Src: 192.168.81.128, Dst: 44.228.249.3  
 Transmission Control Protocol, Src Port: 51874, Dst Port: 80, Seq: 1, Ack: 1, Len: 331  
 Hypertext Transfer Protocol  
 GET / HTTP/1.1  
 Host: vulnweb.com  
 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:140.0) Gecko/20100101 Firefox/140.0  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Connection: keep-alive  
 Upgrade-Insecure-Requests: 1  
 Priority: u=0, i  
 [Response in frame: 239]  
 [Full request URI: http://vulnweb.com/]

The TCP payload of this packet (tcp.payload), 331 bytes

Figure 7: HTTP Plain-Text Traffic Captured in Wireshark

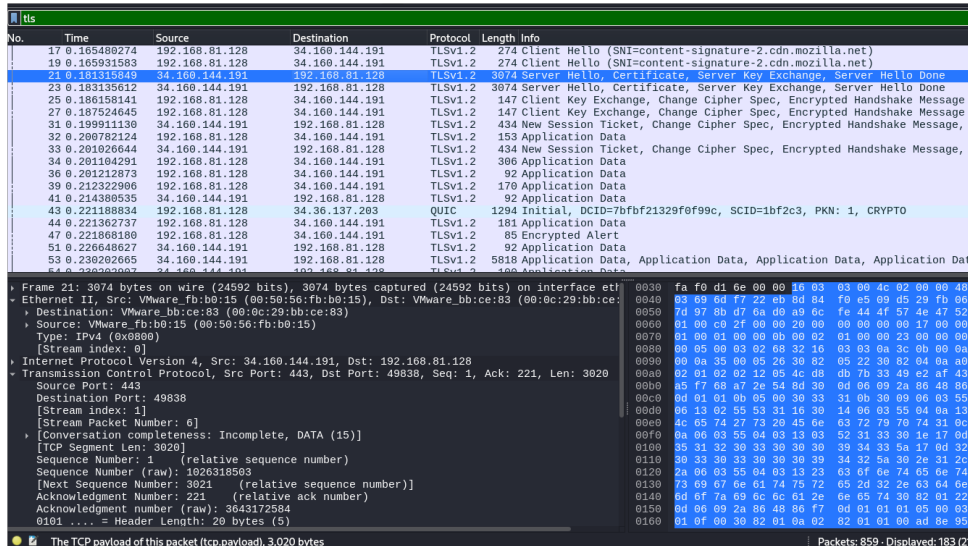


Figure 8: HTTPS Encrypted Traffic Captured in Wireshark

## 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

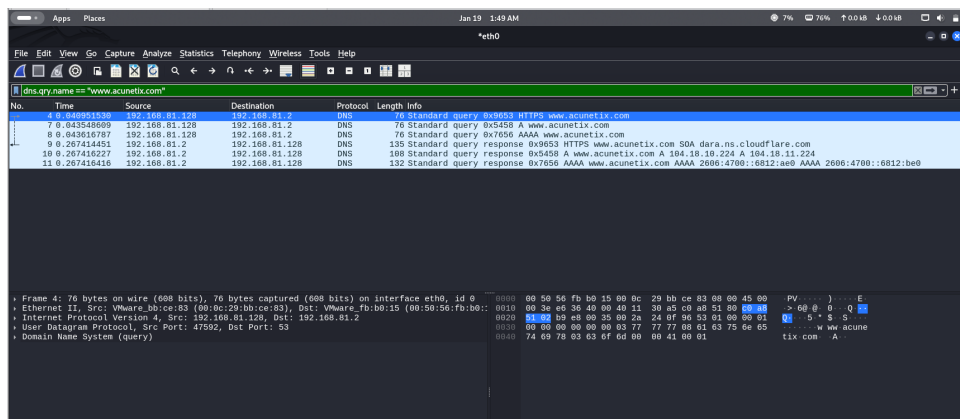


Figure 9: DNS Query and Response Captured in Wireshark

## 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.