

# 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

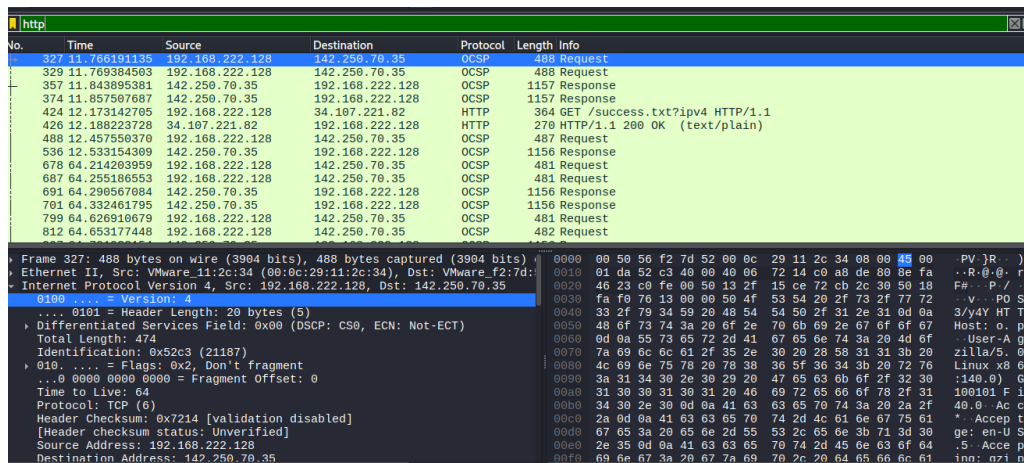


Figure 1: HTTP traffic captured in Wireshark

##### 1.1.2 DNS Protocol

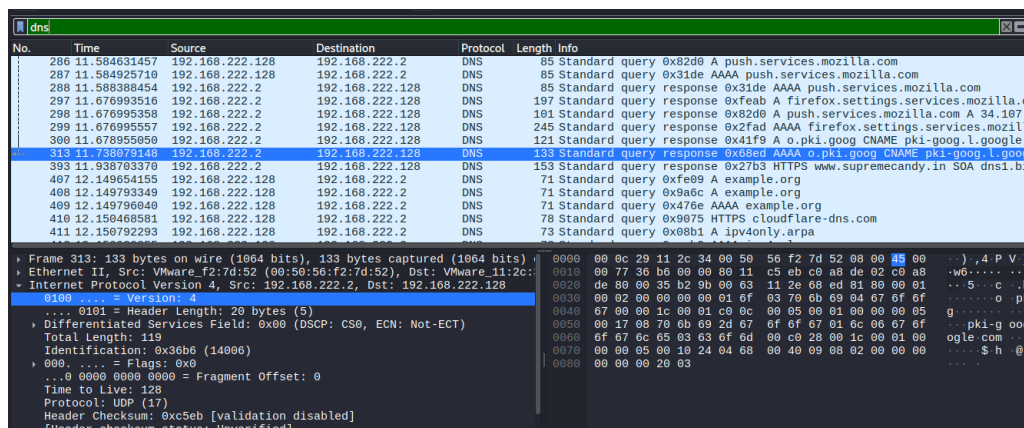


Figure 2: DNS query and response in Wireshark

### 1.1.3 TCP Protocol

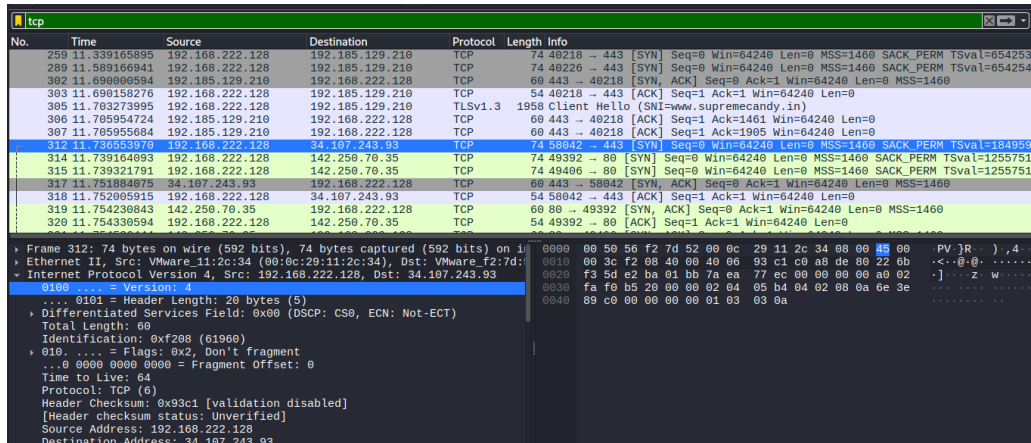


Figure 3: TCP packet communication

### 1.1.4 UDP Protocol

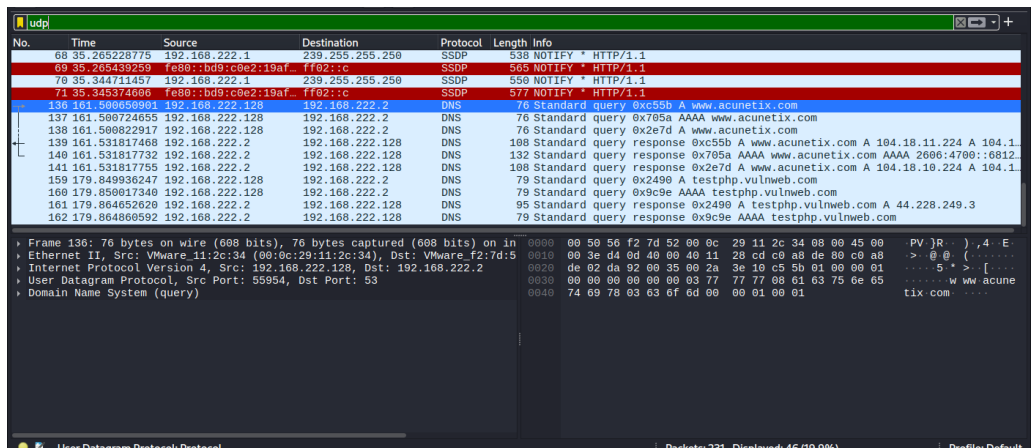


Figure 4: UDP packet transmission

### 1.1.5 HTTPS (TLS) Protocol

No.	Time	Source	Destination	Protocol	Length	Info
168	10.095239392	34.160.144.191	192.168.222.128	TLSv1.2	4074	Application Data, Application Data, Application Data
170	10.096119773	192.168.222.128	34.160.144.191	TLSv1.2	190	Application Data
177	10.678741956	192.168.222.128	34.36.137.203	QUIC	1294	Initial, DCID=5e19accec92e037a, SCID=4ec7e1, PKN: 1, CRYPT
184	10.726220302	192.168.222.128	34.36.137.203	TLSv1.3	1954	Client Hello (SNI=ads.mozilla.org)
191	10.761925083	34.36.137.203	192.168.222.128	QUIC	1294	Handshake, DCID=4ec7e1, SCID=fe19accec92e037a
200	10.821929790	34.36.137.203	192.168.222.128	TLSv1.3	4554	Server Hello, Change Cipher Spec, Application Data
305	11.703273995	192.168.222.128	192.185.129.210	TLSv1.3	1958	Client Hello (SNI=www.supremecandy.in)
323	11.703775367	192.168.222.128	34.107.243.93	TLSv1.3	1964	Client Hello (SNI=push.services.mozilla.com)
334	11.790603031	34.107.243.93	192.168.222.128	TLSv1.3	3139	Server Hello, Change Cipher Spec, Application Data
337	11.790287486	192.168.222.128	34.107.243.93	TLSv1.3	118	Change Cipher Spec, Application Data
340	11.802100310	192.168.222.128	34.107.243.93	TLSv1.3	146	Application Data
344	11.815279857	34.107.243.93	192.168.222.128	TLSv1.3	672	Application Data, Application Data
346	11.817053697	192.168.222.128	34.107.243.93	TLSv1.3	85	Application Data
350	11.827780576	34.107.243.93	192.168.222.128	TLSv1.3	85	Application Data

Frame 323: 1964 bytes on wire (15712 bits), 1964 bytes captured (15712 bits) on interface 0	0000	00 50 56 f2 7d 52 00 0c 29 11 2c 34 08 00 45 00
Ethernet II, Src: VMware_11:2c:34 (00:0c:29:11:2c:34), Dst: VMware_f2:7d:52	0010	07 9e f2 0a 40 00 40 06 8c 5d c0 a8 de 80 22 6b
Internet Protocol Version 4, Src: 192.168.222.128, Dst: 34.107.243.93	0020	f3 5d e2 ba 01 bb 7a ea 77 ed 2c d7 55 2f 50 18
TCP, Src Port: 443, Destination Port: 443	0030	fa f0 bc 82 00 00 16 03 01 07 71 01 00 07 6d 03
... 0101 = Header Length: 20 bytes (5)	0040	03 04 1e 99 0b f3 8b 14 d9 dc 68 7b ea 01 6c 00
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0050	a6 c2 27 cd 77 ee 70 c3 e8 01 8a cc 43 cd 21 b2
Total Length: 1950	0060	46 20 5e 7c 15 20 13 9e b2 8b 67 cf 4a 34 c5 31
Identification: 0xf20a (61962)	0070	e1 87 49 70 3d b4 a2 12 d5 bd be 48 14 57 24 45
010. .... = Flags: 0x2, Don't fragment	0080	f7 3d 00 22 13 01 13 03 13 02 c0 2b c0 2f cc a9
... 0 0000 0000 0000 = Fragment Offset: 0	0090	cc a8 c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 9c
Time to Live: 64	00a0	00 9d 00 2f 00 35 01 00 07 02 00 00 0e 00 1c
Protocol: TCP (6)	00b0	00 00 19 70 75 73 68 2e 73 65 72 76 69 63 65 73
Header Checksum: 0x8c5d [validation disabled]	00c0	2e 6d 6f 7a 69 6c 6c 61 2e 63 6f 6d 00 17 00 00
[Header checksum status: Unverified]	00d0	ff 01 00 01 00 00 0a 0a 10 00 0e 11 ec 00 1d 00
Source Address: 192.168.222.128	00e0	17 00 18 00 19 01 00 01 01 00 0b 00 02 01 00 00
Destination Address: 34.107.243.93	00f0	23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74 74

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
259	11.339105895	192.168.222.128	192.185.129.210	TCP	74	40218 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=6542
289	11.589106941	192.168.222.128	192.185.129.210	TCP	74	40226 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=6542
302	11.690000594	192.185.129.210	192.168.222.128	TCP	60	443 → 40218 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
303	11.690158276	192.168.222.128	192.185.129.210	TCP	54	40218 → 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

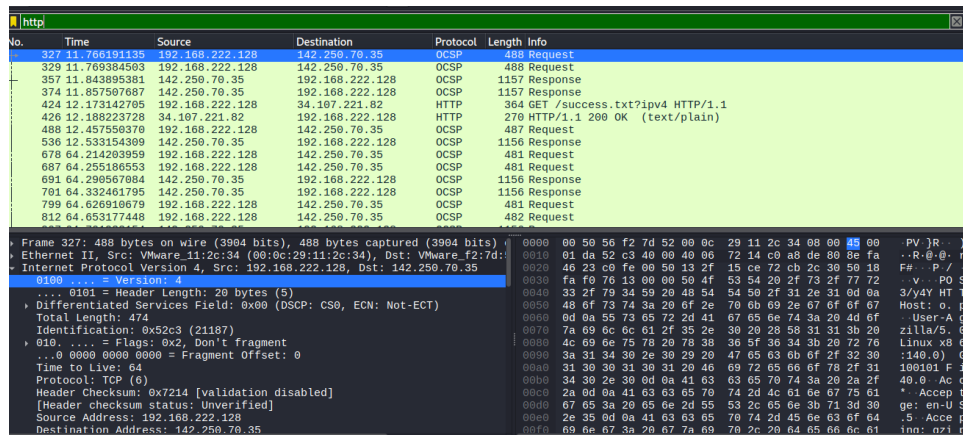


Figure 7: HTTP Plain-Text Traffic Captured in Wireshark

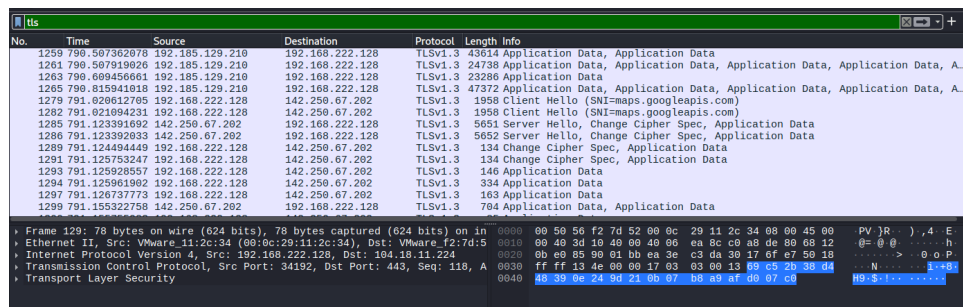


Figure 8: HTTPS Encrypted Traffic Captured in Wireshark

## 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

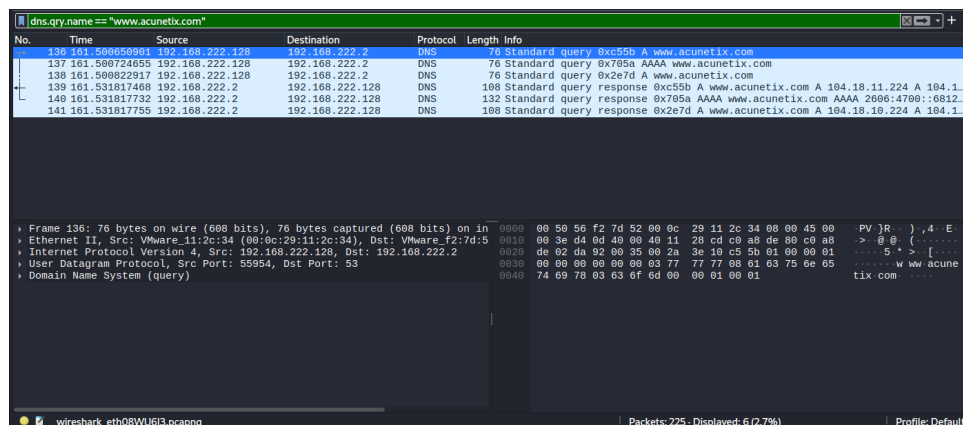


Figure 9: DNS Query and Response Captured in Wireshark

## 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.