

# **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

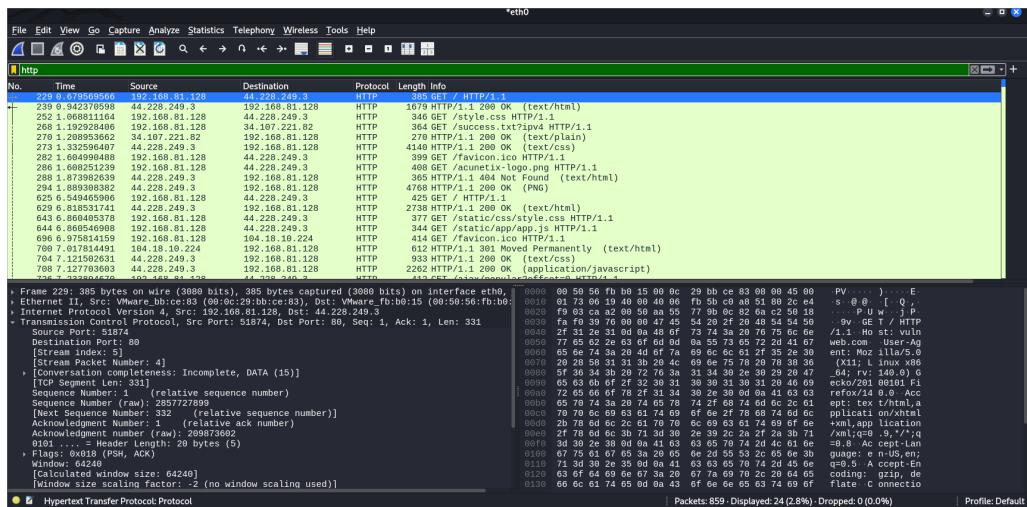


Figure 1: HTTP traffic captured in Wireshark

### 1.1.2 DNS Protocol

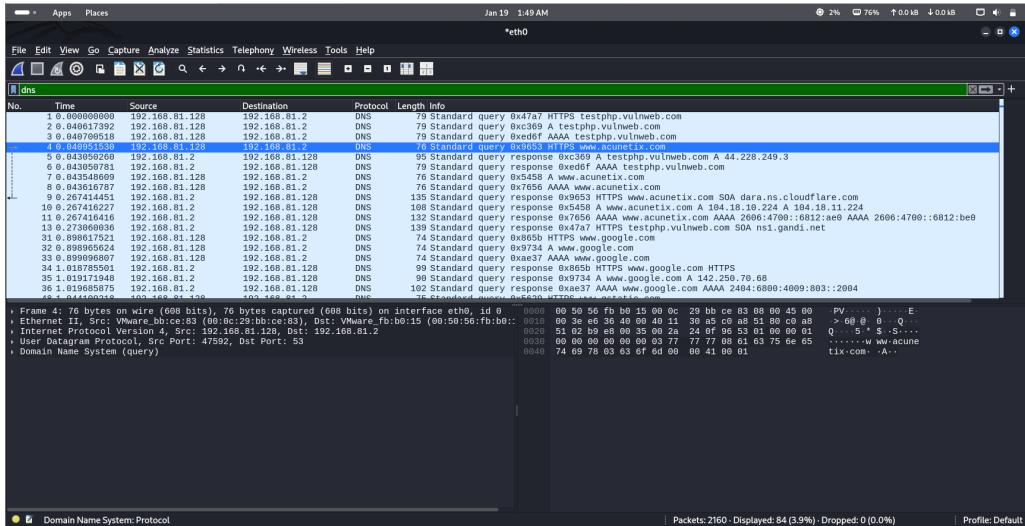


Figure 2: DNS query and response in Wireshark

### 1.1.3 TCP Protocol

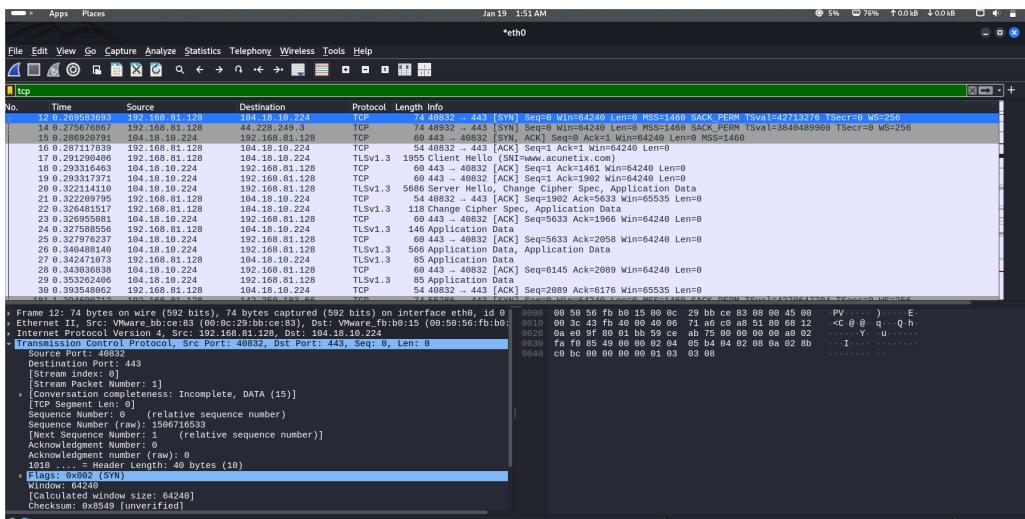


Figure 3: TCP packet communication

#### 1.1.4 UDP Protocol

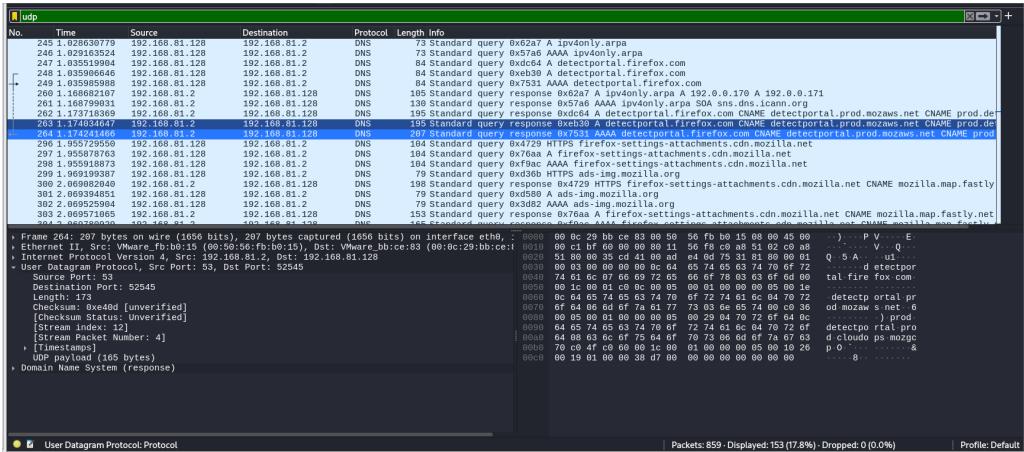


Figure 4: UDP packet transmission

### 1.1.5 HTTPS (TLS) Protocol

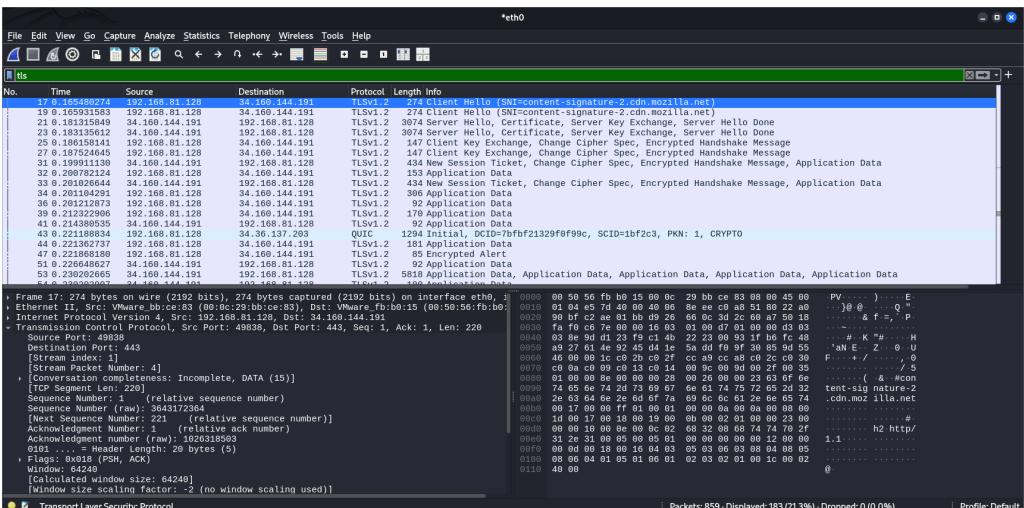


Figure 5: Encrypted HTTPS (TLS) traffic

## 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.

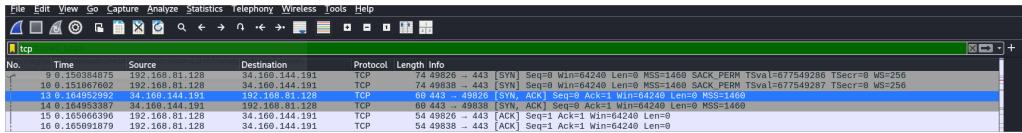


Figure 6: TCP Three way Handshake

## 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

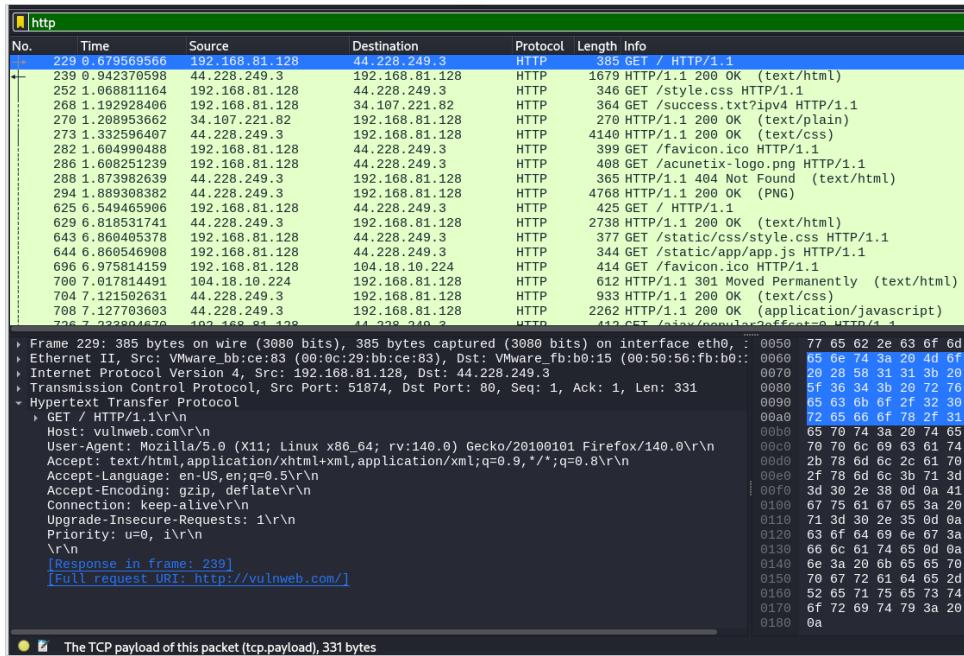


Figure 7: HTTP Plain-Text Traffic Captured in Wireshark

No.	Time	Source	Destination	Protocol	Length Info
17	2023-04-25 08:48:27.24	192.168.81.128	34.160.144.191	TLSV1.2	237 Client Hello (SNI=<content-signature-2.cdn.mozilla.net>)
19	0.165931583	192.168.81.128	34.160.144.191	TLSV1.2	274 Client Hello (SNI=<content-signature-2.cdn.mozilla.net>)
21	0.18313515849	34.168.144.191	192.168.81.128	TLSV1.2	3074 Server Hello, Certificate, Server Key Exchange, Server Hello Done
23	0.183135612	34.168.144.191	192.168.81.128	TLSV1.2	3074 Server Hello, Certificate, Server Key Exchange, Server Hello Done
25	0.186158141	192.168.81.128	34.160.144.191	TLSV1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	0.187524645	192.168.81.128	34.160.144.191	TLSV1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
31	0.199911133	34.168.144.191	192.168.81.128	TLSV1.2	434 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message,
32	0.209782124	192.168.81.128	34.160.144.191	TLSV1.2	153 Application Data
33	0.210104291	192.168.81.128	34.160.144.191	TLSV1.2	426 Application Data, Change Cipher Spec, Encrypted Handshake Message,
34	0.210104291	192.168.81.128	34.160.144.191	TLSV1.2	306 Application Data
36	0.291212873	192.168.81.128	34.160.144.191	TLSV1.2	92 Application Data
39	0.212322990	192.168.81.128	34.160.144.191	TLSV1.2	170 Application Data
41	0.214380535	34.168.144.191	192.168.81.128	TLSV1.2	92 Application Data
43	0.221188834	192.168.81.128	34.36.137.293	QUIP	1294 Initial, DCID=bfbf21329f0f99c, SCID=1bf2c3, PKN: 1, CRYPTO
44	0.221362737	192.168.81.128	34.160.144.191	TLSV1.2	184 Application Data
47	0.221818167	192.168.81.128	34.160.144.191	TLSV1.2	85 Encrypted Alert
51	0.223480697	192.168.81.128	192.168.81.128	TLSV1.2	22 Application Data
53	0.22802665	34.160.144.191	192.168.81.128	TLSV1.2	5838 Application Data, Application Data, Application Data, Application Data
54	0.322022097	34.160.144.191	192.168.81.128	TLSV1.2	100 Application Data
					... Packets: 859 - Displayed: 183 (2)
					The TCP payload of this packet (tcp.payload), 3020 bytes

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

No.	Time	Source	Destination	Protocol	Length Info
1	4.0.0.0:6991530	192.168.81.128	192.168.81.2	DNS	76 Standard query 0x9653 HTTPS www.acunetix.com
7	0.0.0.0:643548699	192.168.81.128	192.168.81.2	DNS	76 Standard query 0x5458 A www.acunetix.com
8	0.0.0.0:643548699	192.168.81.128	192.168.81.2	DNS	76 Standard query 0x5458 A www.acunetix.com
9	0.267414451	192.168.81.2	192.168.81.128	DNS	135 Standard query response 0x9653 HTTPS www.acunetix.com SDA dara.ns.cloudflare.com
10	0.267416227	192.168.81.2	192.168.81.128	DNS	108 Standard query response 0x5458 A www.acunetix.com A 104.18.10.224 A 104.18.11.224
11	0.267415416	192.168.81.2	192.168.81.128	DNS	132 Standard query response 0x7656 AAAA www.acunetix.com AAAA 2606:4700::6812:a0 AAAA 2606:4700::6812:be0
					... Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53
					Domain Name System (query)
					Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
					Ethernet II, Src: VMware_bb: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: 192.168.81.2
					User Datagram Protocol, Src Port: 47592, Dst Port: 53

- 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.