Task 3: Networking Basics for Cyber Security

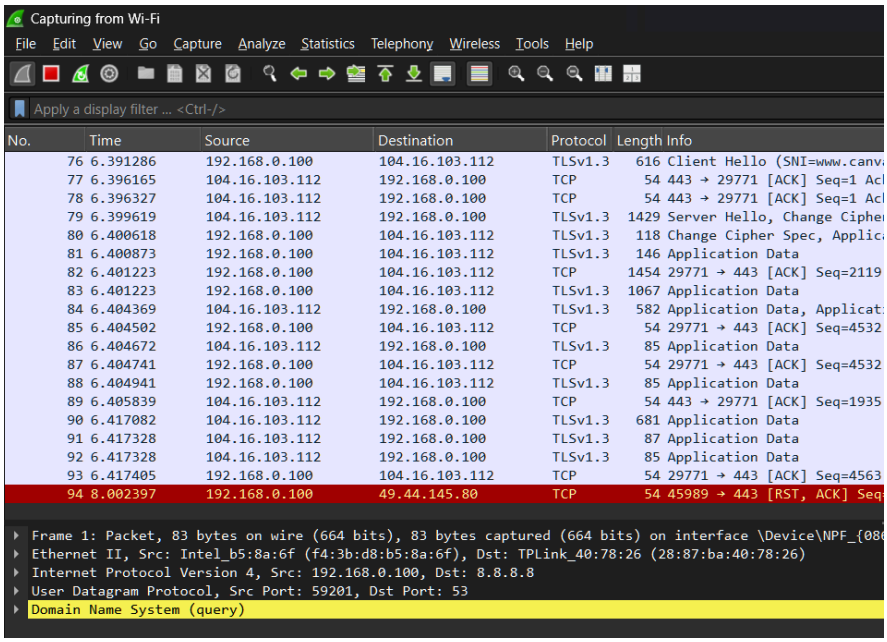
Task Execution

1. Learn Basic Networking Concepts

- IP Address: Identifies a device on a network.
- MAC Address: Physical address of a network interface.
- DNS: Resolves domain names into IP addresses.
- TCP: Reliable, connection-oriented protocol.
- UDP: Fast, connectionless protocol.

2. Capture Live Network Traffic

- Install Wireshark.
- Run Wireshark as administrator.
- Select an active network interface (Wi-Fi or Ethernet).
- Start capturing live packets.

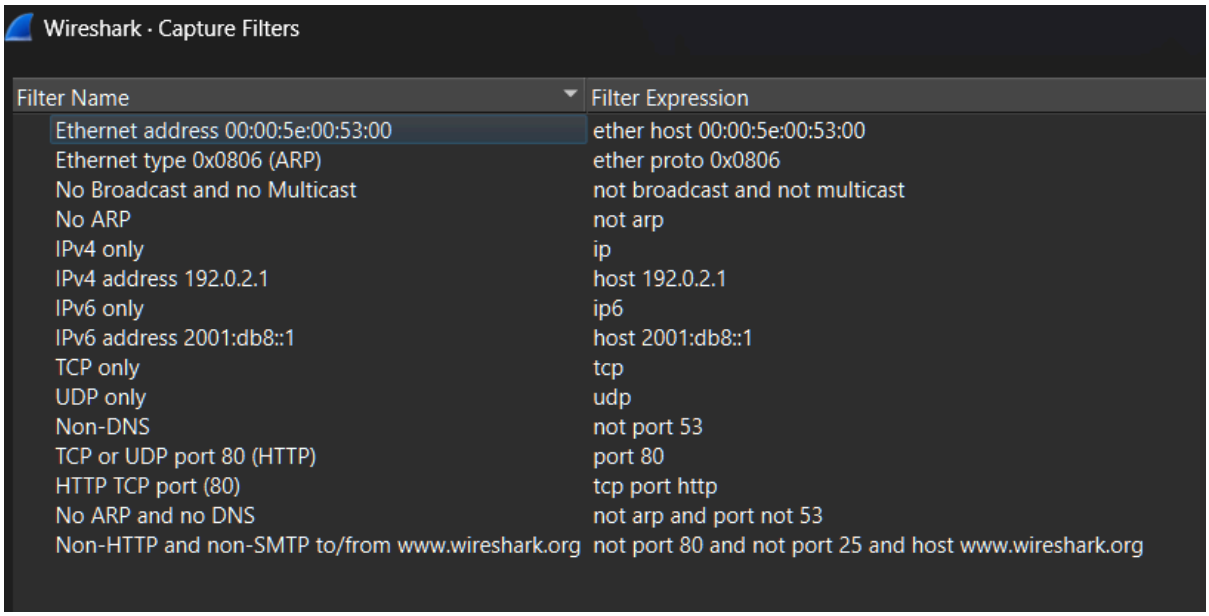


3. Filter Packets by Protocol

Use display filters in Wireshark:

- http
- dns
- tcp

This helps analyze specific types of traffic.



4. Observe TCP Three-Way Handshake

Identify the following TCP flags:

1. SYN
2. SYN-ACK
3. ACK

This handshake establishes a TCP connection between client and server.

TCP packets showing SYN, SYN-ACK, and ACK flags.

5. Identify Plain-Text vs Encrypted Traffic

- HTTP: Data is visible in plain text.
- HTTPS: Data is encrypted and not readable.

- HTTP traffic showing readable data.
- HTTPS/TLS traffic showing encrypted data.

6. Capture and Analyze DNS Queries

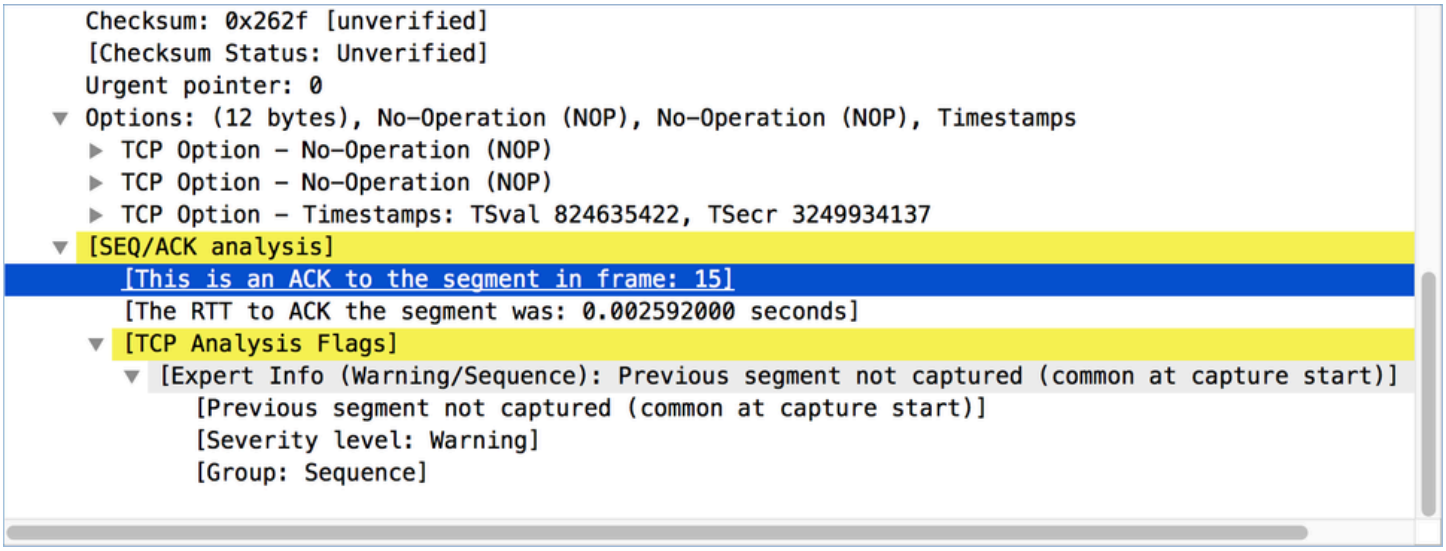
- Apply the dns filter.
- Open a website in a browser.
- Observe DNS queries and responses with IP addresses.

DNS query and response visible in Wireshark.

This file is mandatory for submission.

7. Write Observations in Simple Language

Write short observations based on what you captured.



Tools Used

- Primary Tool: Wireshark
- Alternative Tools: tcpdump, Microsoft Network Monitor

Task Execution (According to Given Steps)

1. Learn Basic Networking Concepts

- IP Address: Identifies a device on a network.
- MAC Address: Physical address of a network interface.
- DNS: Resolves domain names into IP addresses.
- TCP: Reliable, connection-oriented protocol.
- UDP: Fast, connectionless protocol.

2. Capture Live Network Traffic

- Install Wireshark.
- Run Wireshark as administrator.
- Select an active network interface (Wi-Fi or Ethernet).
- Start capturing live packets.

Live packet capture running in Wireshark.

3. Filter Packets by Protocol

Use display filters in Wireshark:

- http
- dns
- tcp

This helps analyze specific types of traffic.
Protocol filter applied (HTTP, DNS, or TCP).

4. Observe TCP Three-Way Handshake

Identify the following TCP flags:

1. SYN
2. SYN-ACK
3. ACK

This handshake establishes a TCP connection between client and server.

TCP packets showing SYN, SYN-ACK, and ACK flags.

5. Identify Plain-Text vs Encrypted Traffic

- HTTP: Data is visible in plain text.
- HTTPS: Data is encrypted and not readable.
- HTTP traffic showing readable data.
- HTTPS/TLS traffic showing encrypted data.

6. Capture and Analyze DNS Queries

- Apply the dns filter.
- Open a website in a browser.
- Observe DNS queries and responses with IP addresses.
  DNS query and response visible in Wireshark.