Task 3: Networking Basics for Cyber Security

Tools: Wireshark

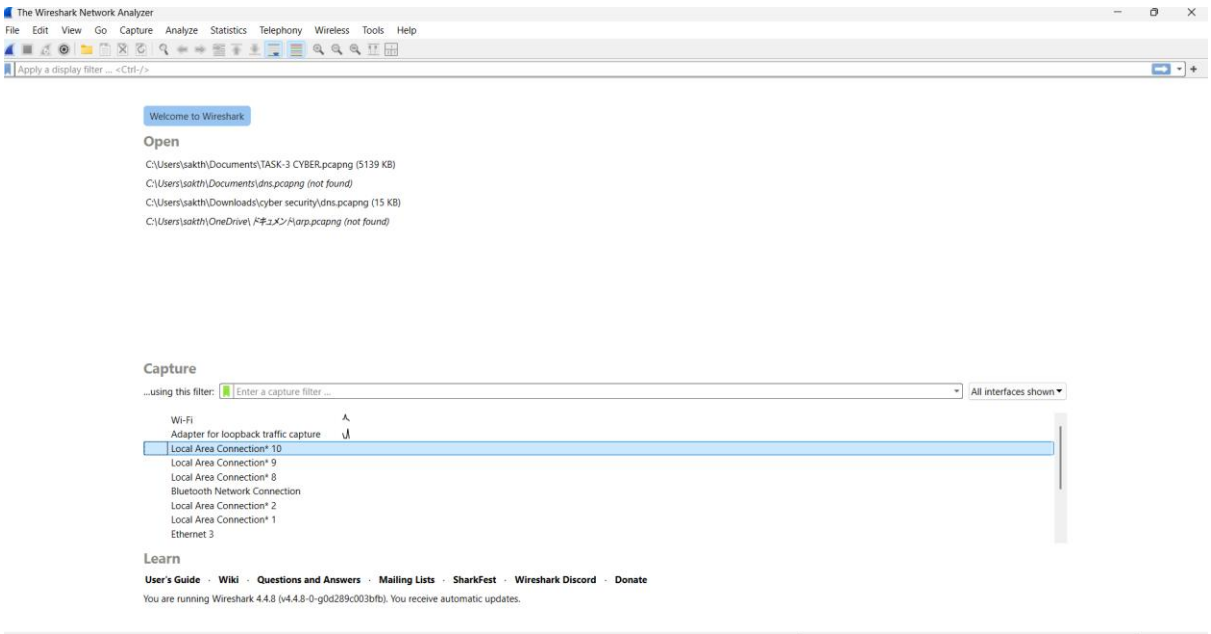
1. Learning Basic Networking Concepts:

Basic networking concepts such as IP address, MAC address, DNS, TCP, and UDP were studied to understand how data is transmitted over a network.

- **IP address** → Address of a device (like a house number)
- **MAC address** → Physical address of network card
- **DNS** → Converts website name → IP address
- **TCP** → Reliable connection (used by HTTP/HTTPS)
- **UDP** → Faster, no guarantee (used by DNS)

2. Installing Wireshark and Capturing Live Traffic:

Wireshark was installed on the system and live network traffic was captured by selecting the active Wi-Fi network interface.



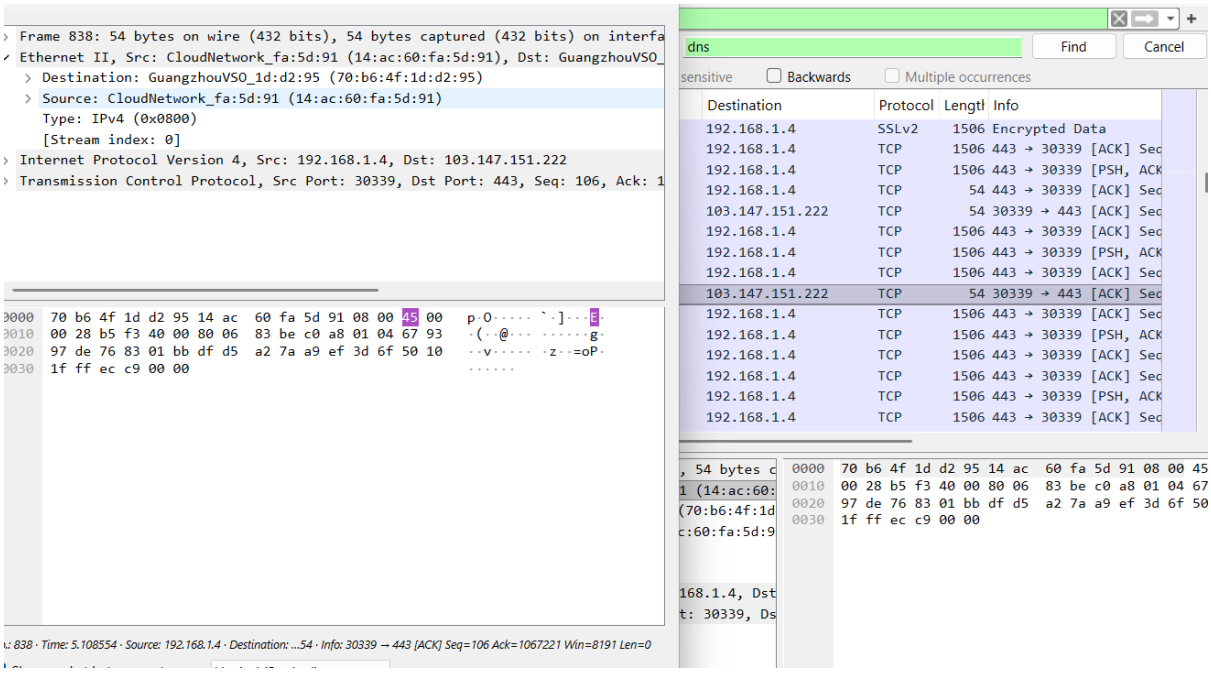
3. Filtering Packets by Protocol

Captured packets were filtered using display filters to analyze specific protocols:

- http for HTTP traffic
- dns for DNS packets
- tcp for TCP packets

4. Observing TCP Three-Way Handshake

The TCP connection establishment was observed by identifying the SYN, SYN-ACK, and ACK packets, which together form the TCP three-way handshake.

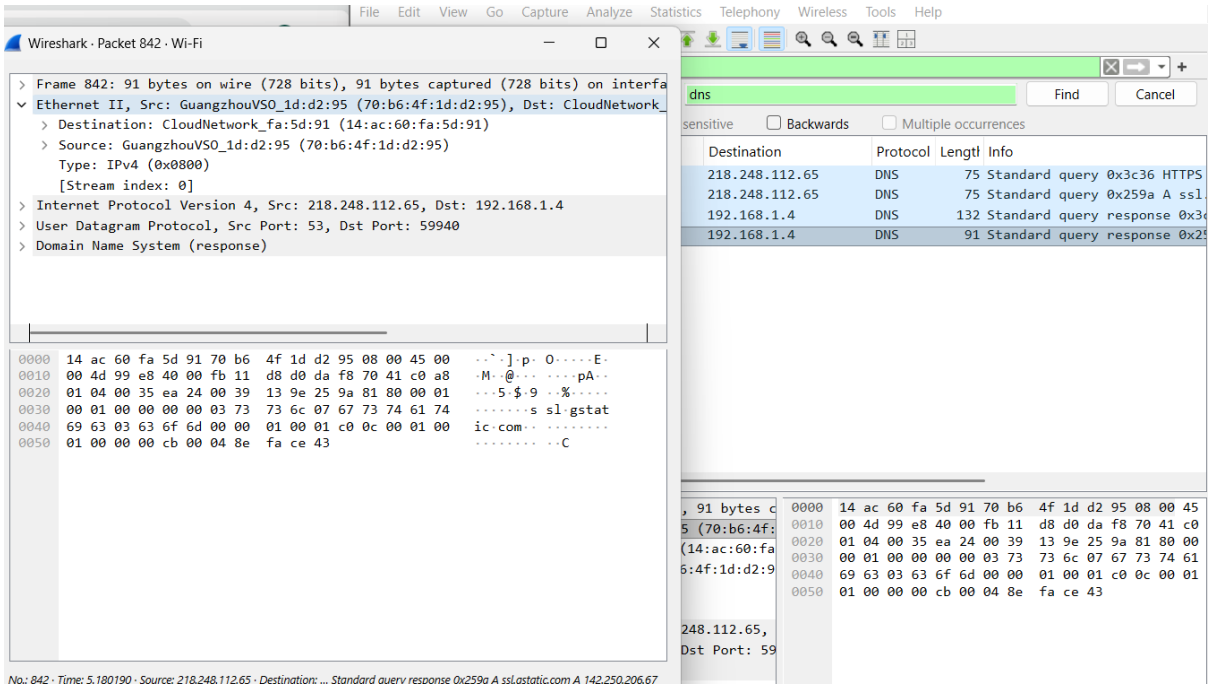


5. Identifying Plain-Text and Encrypted Traffic

- HTTP traffic was observed as plain-text and readable.
- HTTPS traffic (port 443) was observed as encrypted and unreadable.

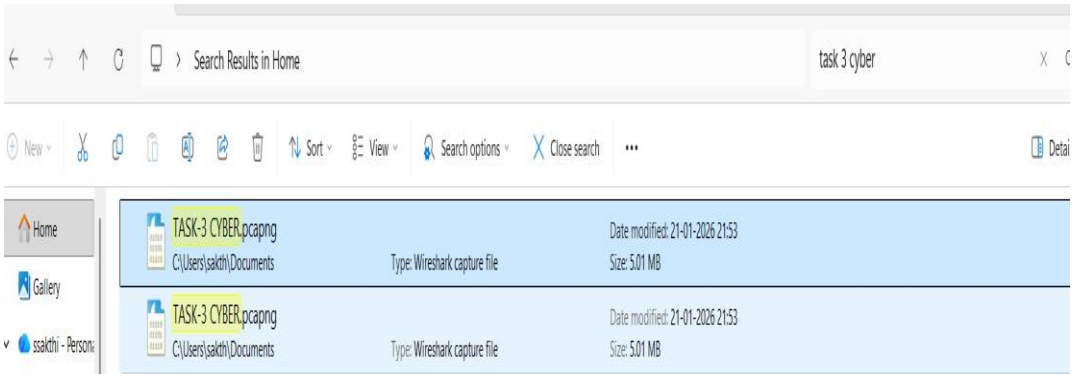
6. Capturing and Analyzing DNS Queries:

DNS packets using UDP port 53 were captured.
DNS queries and responses were analyzed to understand how domain names are resolved into IP addresses**.**



7. Saving Packet Captures:

The captured network traffic was saved in .pcapng format for future analysis and documentation**.**



8.Observations

- Live network traffic was successfully captured using Wireshark.
- Different types of packets were observed by applying protocol filters such as TCP, DNS, and HTTP/HTTPS.
- TCP packets showed reliable communication with control flags like SYN, ACK, and PSH, indicating connection establishment and data transfer.
- The TCP three-way handshake was observed during the start of a connection, confirming that TCP is a connection-oriented protocol.
- HTTP traffic was found to be in plain-text and readable, whereas HTTPS traffic was encrypted and unreadable, showing secure communication.
- DNS packets were captured using UDP port 53, and domain name queries and responses were clearly observed.
- DNS analysis showed how domain names are resolved into corresponding IP addresses.
- Packets were sometimes split into multiple segments and later reassembled by Wireshark, indicating normal data transmission behavior.
- Source and destination IP addresses and port numbers were identified for different network communications.
- The captured packets were successfully saved in .pcapng format for future analysis.