

## Task 3: Networking Basics for Cyber Security

### Tools: Wireshark

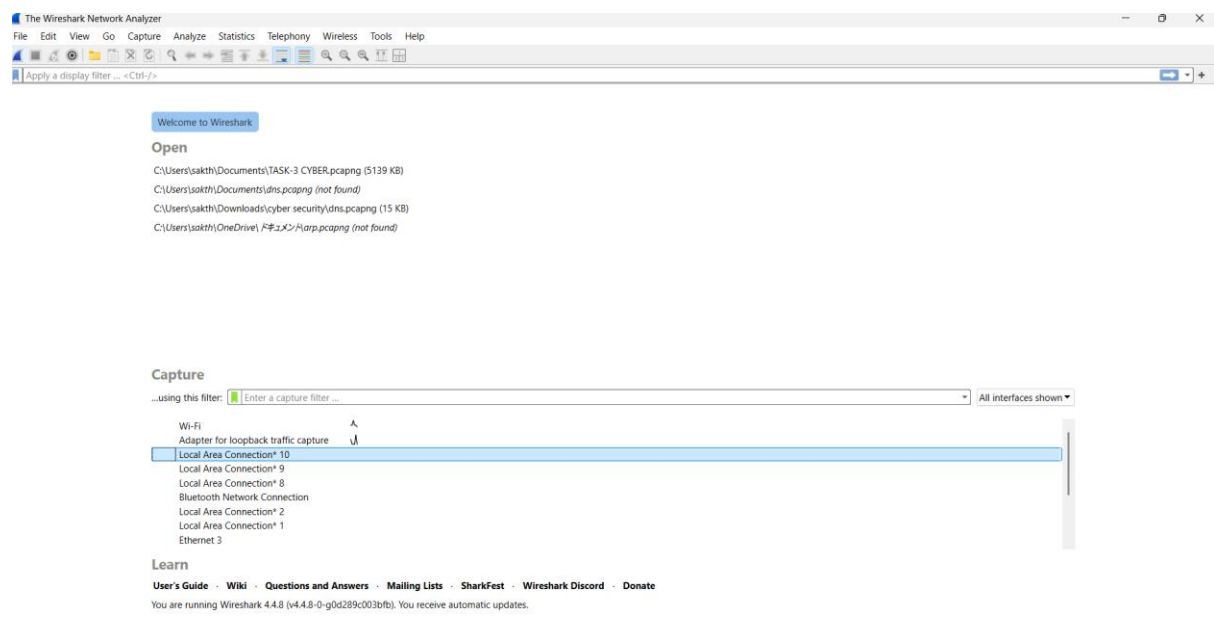
#### 1. Learning Basic Networking Concepts:

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.

The image displays two screenshots from the Wireshark network protocol analyzer. The left screenshot shows the packet details pane for a selected packet (Frame 838). It details the Ethernet II header (Source: CloudNetwork\_fa:5d:91, Destination: GuangzhouVSO\_1d:d2:95), the IPv4 header (Source: 192.168.1.4, Destination: 103.147.151.222), and the TCP header (Source Port: 30339, Destination Port: 443, Seq: 106, Ack: 1). The packet bytes pane shows the raw data in hexadecimal and ASCII. The right screenshot shows the packet list pane with a filter 'dns' applied. The list shows several packets, including a SYN packet (Seq: 30339) and a SYN-ACK packet (Seq: 443, Ack: 30339). The packet details pane for the selected packet (Frame 838) shows the TCP header (Source Port: 30339, Destination Port: 443, Seq: 106, Ack: 1067221, Win: 8191, Len: 0).

### 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.

The image shows a Wireshark packet capture window. The left pane displays the packet list and details for Frame 842, which is a DNS response from 192.168.1.4 to 218.248.112.65. The right pane shows the packet bytes and the packet hex view. The packet details pane is expanded to show the DNS response structure, including the query and response sections.

Wireshark - Packet 842 - Wi-Fi

> Frame 842: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface  
> Ethernet II, Src: GuangzhouVSO\_1d:d2:95 (70:b6:4f:1d:d2:95), Dst: CloudNetwork\_14:ac:60:fa:5d:91 (14:ac:60:fa:5d:91)  
> Destination: CloudNetwork\_fa:5d:91 (14:ac:60:fa:5d:91)  
> Source: GuangzhouVSO\_1d:d2:95 (70:b6:4f:1d:d2:95)  
> Type: IPv4 (0x0800)  
> [Stream index: 0]  
> Internet Protocol Version 4, Src: 218.248.112.65, Dst: 192.168.1.4  
> User Datagram Protocol, Src Port: 53, Dst Port: 59940  
> Domain Name System (response)

14 ac 60 fa 5d 91 70 b6 4f 1d d2 95 08 00 45 00 ... .j.p. 0....E.  
00 4d 99 e8 40 00 fb 11 d8 d0 da f8 70 41 c0 a8 ...M.@... ..pA..  
01 04 00 35 ea 24 00 39 13 9e 25 9a 81 80 00 01 ...5\$.9 ..%....  
00 01 00 00 00 00 03 73 73 6c 07 67 73 74 61 74 .....s sl gstat  
69 63 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 ic.com .....  
01 00 00 00 cb 00 04 8e fa ce 43 .....C

91 bytes captured (728 bits) on interface  
5 (70:b6:4f:1d:d2:95) (14:ac:60:fa:5d:91)  
6:4f:1d:d2:95  
248.112.65,  
Dst Port: 59

No.: 842 • Time: 5.180190 • Source: 218.248.112.65 • Destination: ... Standard query response 0x259a A sslstatic.com A 142.250.206.67

## 7. Saving Packet Captures:

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

The image shows a Windows File Explorer window displaying search results for 'task 3 cyber'. Two files are listed: 'TASK-3 CYBER.pcapng' and 'TASK-3 CYBER.pcapng', both located in 'C:\Users\sakthi\Documents'. Both files are of type 'Wireshark capture file' and have a size of 5.01 MB. The date modified is 21-01-2026 21:53.

task 3 cyber

Home  
Gallery  
ssakthi - Person

TASK-3 CYBER.pcapng  
C:\Users\sakthi\Documents  
Type: Wireshark capture file  
Date modified: 21-01-2026 21:53  
Size: 5.01 MB

TASK-3 CYBER.pcapng  
C:\Users\sakthi\Documents  
Type: Wireshark capture file  
Date modified: 21-01-2026 21:53  
Size: 5.01 MB

## 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.