Task 3: Networking Basics for Cyber Security

1.Learn basic networking concepts (IP, MAC, DNS, TCP/UDP)

Answer (Concepts)

- **IP Address**
  A logical address used to identify a device on a network (example: 192.168.1.5).
- **MAC Address**
  A physical hardware address of a network interface (example: 00:1A:2B:3C:4D:5E).
- **DNS (Domain Name System)**
  Converts domain names (google.com) into IP addresses.
- **TCP (Transmission Control Protocol)**
  Reliable, connection-oriented protocol (used by HTTP, HTTPS).
- **UDP (User Datagram Protocol)**
  Faster, connectionless, no guarantee of delivery (used by DNS, streaming)

2.Install Wireshark and capture live network traffic

- Downloaded Wireshark from official website
- Installed it
- Opened Wireshark
- Selected your active interface:
  Wi-Fi
- Click Start

3.Filter packets by protocol (HTTP, DNS, TCP)

Filters used in Wireshark

Purpose	**Filter**
HTTP traffic	**http**
DNS traffic	**dns**
TCP traffic	**tcp**
UDP traffic	**udp**

4. Observe three-way TCP handshake

TCP handshake has 3 steps:

1. SYN – Client requests connection
2. SYN-ACK – Server acknowledges
3. ACK – Client confirms

This establishes a reliable connection.

5.Identify plain-text traffic vs encrypted traffic

- Plain-text traffic
  Data is readable (HTTP, FTP)
- Encrypted traffic
  Data is unreadable (HTTPS, TLS)

6.Capture DNS queries and analyze them

- Queried domain name
- Resolved IP address
- Source & destination

7.Save packet captures for analysis

SCREENSHOT ATTACHED IN REPO

8. Write observations in simple language

- I captured live network traffic using Wireshark.
- DNS queries showed domain name resolution.
- TCP handshake was observed using SYN, SYN-ACK, and ACK flags.
- HTTP traffic was readable, while HTTPS traffic was encrypted