Wireshark Tool Exercises

1. Capturing Live Traffic – Use any website.
2. Applying Capture Filters:
    a. HTTP traffic: http
        i. For HTTP - Inspect request and response headers, URLs, and status codes.
        ii. For HTTPS, observe the handshake process (TLS).
    b. DNS requests: dns
        i. Observe how domain names are translated into IP addresses.
        ii. Identify DNS request and response packets.
    c. TCP packets: tcp
        i. Observe the 3-way handshake (SYN, SYN-ACK, ACK).
        ii. Identify sequence numbers and acknowledgment numbers.
    d. ICMP (ping): icmp
        i. Send ping requests (ping google.com) and observe request/reply packets.
3. Detecting Man-in-the-Middle (MITM) Attacks
    a. Monitor ARP poisoning attempts