🧪 EXPERIMENT 8 — SSL Protocol using Wireshark

Aim:
To study the **SSL protocol** by capturing packets using **Wireshark** while visiting an SSL-secured website (banking, e-commerce, etc.).

Theory (Summary):

- **SSL (Secure Sockets Layer)** — an encryption-based protocol ensuring privacy and data integrity.
- Developed by Netscape (1995); modern form is **TLS** (Transport Layer Security).

How SSL/TLS Works:

1. **Encryption:** data encrypted before transmission.
2. **Authentication:** handshake ensures both parties are genuine.
3. **Integrity:** prevents tampering during transit.

Steps in SSL Handshake:

1. **Client Hello** — client sends supported cipher suites.
2. **Server Hello** — server selects cipher and sends certificate.
3. **Certificate Exchange** — validates identity.
4. **Client Key Exchange** — establishes shared secret key.
5. **Change Cipher Spec** — both switch to encrypted mode.
6. **Application Data** — encrypted communication begins.
7. **Alert Message** — signals connection close.

Wireshark Observation Steps:

1. Apply display filter ssl or tls.
2. Capture packets while visiting an HTTPS site.
3. Analyze Hello, Certificate, and Key Exchange packets.

Conclusion:
Successfully studied SSL protocol and its handshake process using Wireshark.

🔹 Oral / Viva Questions and Answers

1. **What is SSL?**
   ➤ SSL is a protocol that encrypts data to ensure secure communication over the internet.
2. **What is the difference between SSL and TLS?**
   ➤ TLS is the newer, more secure version of SSL.

3. **Which OSI layer does SSL operate on?**
   ➤ Between the **Transport** and **Application** layers.

4. **Why is SSL important?**
   ➤ It protects data confidentiality and prevents unauthorized access or tampering.

5. **What is an SSL handshake?**
   ➤ A process where client and server authenticate and agree on encryption methods before communication.

6. **What is the function of a digital certificate?**
   ➤ It verifies the authenticity of the server's identity.

7. **What is the default port of HTTPS?**
   ➤ Port 443.