Walchand College of Engineering, Sangli *(Government Aided Autonomous Institute)*	
AY 2025-26	
Course Information	
Programme	B.Tech. (Computer Science and Engineering)
Class, Semester	Final Year B. Tech., Sem VII
Course Code	6CS451
Course Name	Cryptography and Network Security Lab

Experiment No. 11

Title – Demonstration of SSL using Wireshark.

Objectives:

To analyze and understand how **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** ensures secure communication over the internet by capturing and inspecting network packets using **Wireshark**. This includes identifying the SSL/TLS handshake process, encryption mechanisms, and certificate exchange.

Problem Statement:

Secure communication over the internet is essential to protect data from eavesdropping, tampering, or forgery. **SSL/TLS** protocols provide encryption, authentication, and integrity for data transmitted between a client and a server.

In this task, you are required to:

1. **Set up a secure HTTPS connection** (e.g., by visiting an HTTPS-enabled website using a browser).
2. **Capture network traffic using Wireshark** while the SSL/TLS handshake and data exchange occur.
3. **Identify and analyze the following** in Wireshark:
   - SSL/TLS handshake process (Client Hello, Server Hello)
   - Server certificate exchange
   - Key exchange and cipher suite negotiation
   - Session keys and encrypted data packets
4. **Highlight the encrypted nature of HTTPS traffic** and explain what information is still visible

   (e.g., IP addresses, port numbers, SNI).

5. Optionally, **use browser developer tools or import a private key** (if available) to decrypt SSL traffic and inspect actual HTTP data inside Wireshark.

The goal is to demonstrate how SSL/TLS protects data during transmission and to gain familiarity with analyzing encrypted traffic using **Wireshark**.

Equipment/Tools:

Theory:

Procedure:

Steps:

Observations and Conclusion: