# SSL/TLS Handshake with Packet Capture Analysis (Wireshark)

## 2. SSL vs TLS

- **SSL (Secure Sockets Layer)** is deprecated due to vulnerabilities.
- **TLS (Transport Layer Security)** is the modern and secure alternative (TLS 1.2 and TLS 1.3 are widely used).

## 4. TLS 1.3 Differences

TLS 1.3 significantly streamlines the handshake:

- Removes many insecure cipher suites.
- Merges steps to improve performance.
- Always uses forward secrecy.
- Faster (1-RTT instead of 2-RTT).

## 6. Interpreting Key Fields in Wireshark

- **Version**: TLS version being negotiated (e.g., TLS 1.2).
- **Cipher Suite**: The algorithm combination selected (e.g., TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).
- **Extensions**: ALPN, SNI, etc.
- **Certificate Info**: Issuer, subject, validity, etc.
- **Random values**: Used for key derivation.

## 8. Detecting Issues

Wireshark helps diagnose:

- **Certificate mismatches**
- **Handshake failures**
- **Unsupported cipher suite errors**
- **Version negotiation problems**
- **Improper certificate chains**

Look for `Alert` messages in the TLS stream:

- Level: **fatal**
- Description: e.g., **handshake_failure**, **bad_certificate**

## 10. Conclusion

Understanding the SSL/TLS handshake at the packet level is vital for secure communications troubleshooting, pentesting, and compliance checks. Wireshark provides an accessible, visual way to trace and validate each handshake phase, from cipher negotiation to certificate exchange.