HTTPS Analysis " CN Assignment 01

Q7. What is the name of website?

The website is identified from the SNI (Server Name Indication) extension in the ClientHello.

Website: `www.gstatic.com`

Q8. Find the packet that contains the ClientHello message?

The ClientHello is found in quiz **Packet No. 37** with SNI = `www.gstatic.com`.

Q9. List all the TLS extensions included in the ClientHello.

The ClientHello included the following TLS extensions:

- server_name (SNI = www.gstatic.com)
- extended_master_secret
- renegotiation_info
- supported_groups
- ec_point_formats
- session_ticket
- application_layer_protocol_negotiation (ALPN)
- status_request
- delegated_credentials
- signed_certificate_timestamp
- key_share (X25519MLKEM768, x25519, secp256r1)
- supported_versions (TLS 1.3, TLS 1.2)
- signature_algorithms
- psk_key_exchange_modes
- record_size_limit
- compress_certificate
- encrypted_client_hello

Q10. Identify the ServerHello message. What cipher suite is chosen by the server?

The ServerHello is visible after the ClientHello.

- Cipher Suite chosen: `TLS_AES_128_GCM_SHA256 (0x1301)`
- This means the connection uses TLS 1.3 with AES-128-GCM and SHA-256.

Q11. Locate the Certificate message. Extract the serverâ€™s certificate information.

In this trace (for `www.gstatic.com`), the **Certificate message is not visible**.

This is because TLS 1.3 encrypts the certificate after the ServerHello.

Therefore, Issuer, Subject, and Validity cannot be extracted directly from the packet capture.

Q12. After the TLS handshake, identify the first encrypted application data packet. Why canâ€™t you directly see the HTTP headers in this packet?

- The first **Application Data** packet (Content Type = 23) appears immediately after the TLS handshake completes.
- This packet contains the encrypted HTTP request/response.
- **Reason headers are hidden:** All HTTP traffic is encrypted after TLS 1.3 handshake. Without the session keys, Wireshark cannot decrypt or display the HTTP headers.
