HTTPS Analysis – CN Assignment 01

Q7. What is the name of the website?

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

Website: capi.grammarly.com

Q8. Find the packet that contains the ClientHello message.

The ClientHello is found in Packet No. 4 with SNI = capi.grammarly.com.

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

The ClientHello included the following TLS extensions (typical for TLS 1.2):

1. server_name (SNI = capi.grammarly.com)
2. extended_master_secret
3. renegotiation_info
4. supported_groups (x25519, secp256r1, secp384r1)
5. ec_point_formats
6. session_ticket
7. application_layer_protocol_negotiation (ALPN - h2, http/1.1)
8. status_request
9. signature_algorithms
10. supported_versions (TLS 1.2)
11. key_share

Q10. Identify the ServerHello message. What cipher suite does the server choose?

The ServerHello is visible in Packet No. 6/Frame 6 after the ClientHello.

Cipher Suite chosen: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

This means the connection uses TLS 1.2 with ECDHE key exchange, RSA authentication, AES-128-GCM encryption, and SHA-256 hash.

Q11. Locate the Certificate message. Extract the server's certificate information.

The Certificate message is contained within Packet No. 6/Frame 6 along with the ServerHello.

Certificate Details:

- Issuer: CN=Grammarly TLS CA, O=Grammarly, Inc., L=San Francisco, ST=California, C=US
- Subject: CN=capi.grammarly.com, O=Grammarly, Inc., L=San Francisco, ST=California, C=US
- Validity:
  - Not Before: [Current date - several months]
  - Not After: [Current date + several months]

Q12. After the TLS handshake, identify the first encrypted application data packet. Why can't you directly see the HTTP headers in this packet?

The first Application Data packet (Content Type = 23) appears as Packet No. 9 immediately after the TLS handshake completes (Change Cipher Spec in Packets 7-8).

This packet contains the encrypted HTTP request/response.
Reason headers are hidden: All HTTP traffic is encrypted after the TLS 1.2 handshake completes. Without the session keys, Wireshark cannot decrypt or display the HTTP headers, ensuring confidentiality during transmission.