Task 2: Find a website that runs on HTTPS. Access this website from your device and capture network traces.

https://www.canva.com/

For the HTTPS based website access, answer the following:

7. What is the name of website?

<https://www.canva.com/>

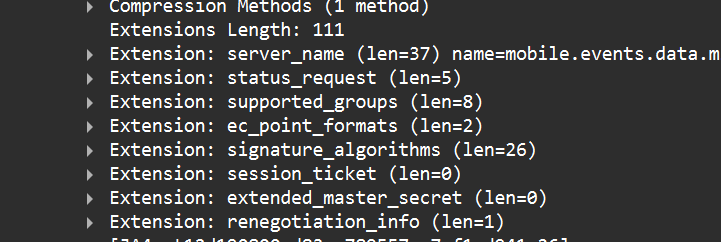
8. Find the packet that contains the ClientHello message for the website you are accessing.

Filter tls.handshake.type == 1



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

Filter tls.handshake.type == 1



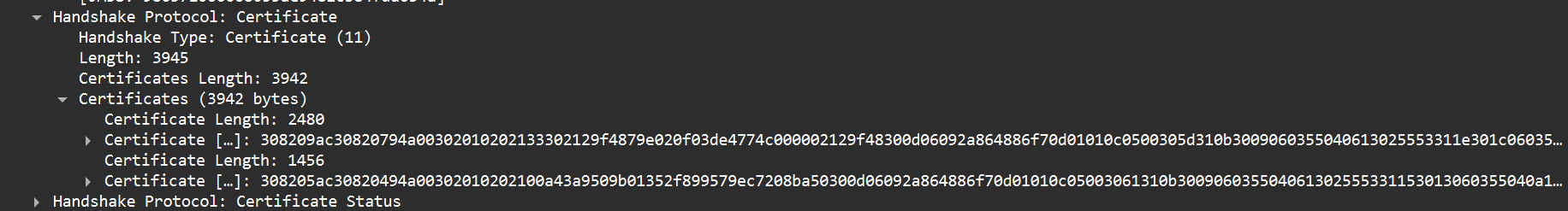
10. Identify the ServerHello message. What cipher suite is chosen by the server?

Filter tls.handshake.type == 2



11. Locate the Certificate message. Extract the server’s certificate information (issuer, subject, validity dates).

Filter tls.handshake.type == 11



12. After the TLS handshake, identify the first encrypted application data packet. Why can’t you directly see the

HTTP headers in this packet?filter tls.app\_data



The first encrypted application data packet appears immediately after the TLS handshake and is marked in Wireshark as \*\*“Application Data” (content type 23)\*\*. we cannot directly see the HTTP headers in this packet because HTTPS encrypts all HTTP requests and responses inside the TLS layer, so only ciphertext is visible instead of the plain HTTP headers.