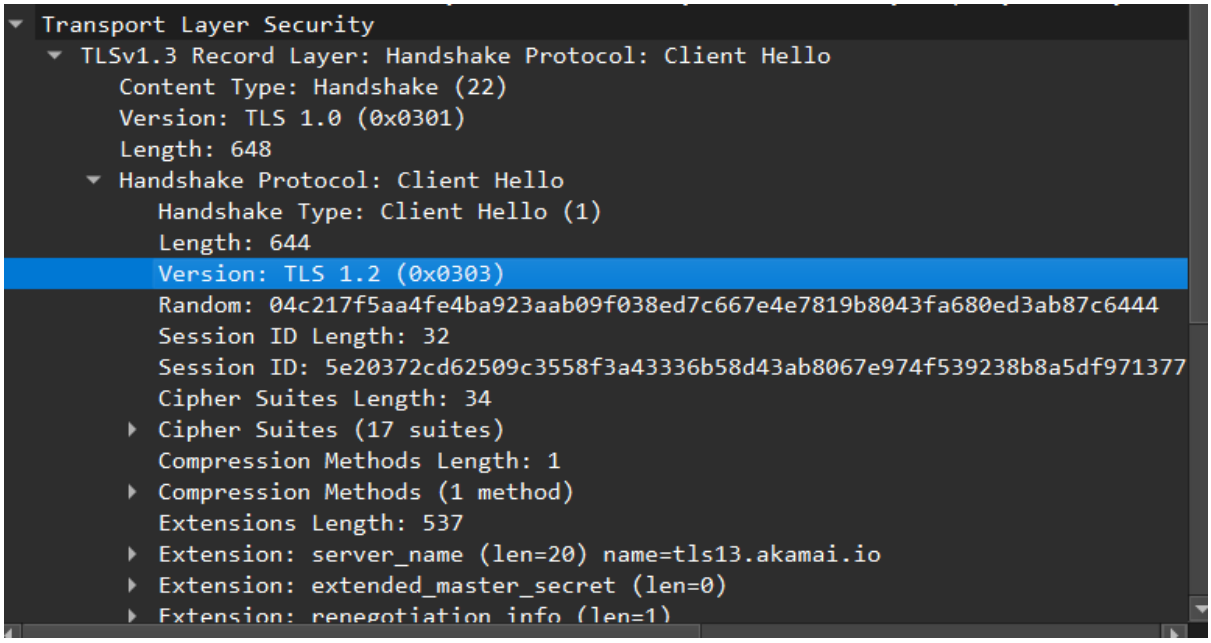
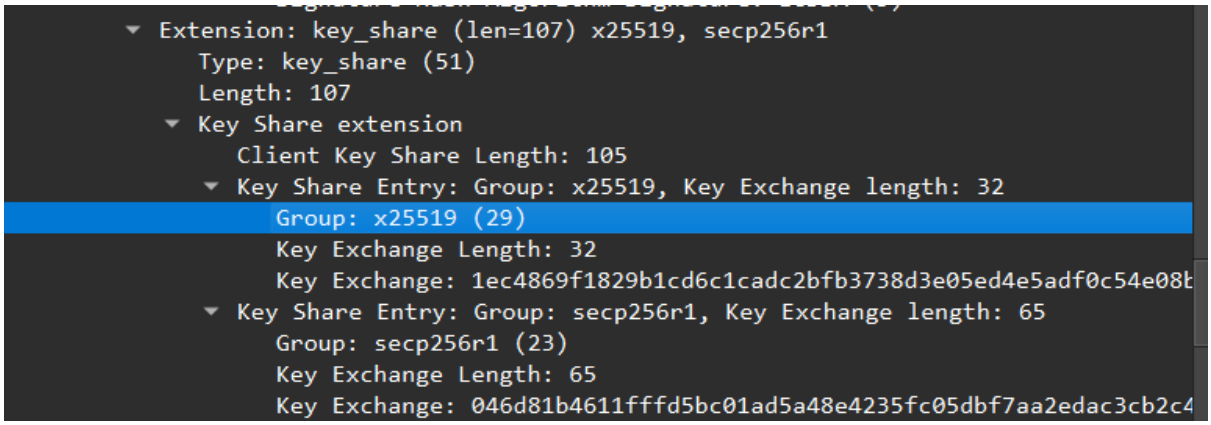
1.
    - Google.com
    a. C
    b. Yes, there are some TLS under version 1.2
    c. Yes, we can see warnings
    - x.com
    a. A
    b. No, there are no TLS under version 1.2
    c. No, we can't see any warnings
    - facebook.com
    a. C
    b. No, there are no TLS under version 1.2
    c. Yes, we can see warnings
    - ohel-shem.iscool.co.il
    a. C
    b. Yes, there are some TLS under version 1.2
    c. Yes, we can see warnings
2. NO VIDEO IN ENGLISH
3. 53 packets. The filter is tls.handshake.type == 1
4. www.hattrick.org
5. _ws.col.info == "Client Hello (SNI=domain goes here)" && tls.handshake.type == 1
6. 1.2
7.
    a. SHA384
    b. AES_256_GCM
    c. RSA
    d. Diffie Hellman
8. 2, Geotrust global and *.hattrick.org
9. Yes
10. Between 30/06/2022 and 15/07/2023
11. DigiCert. It wasn't sent to the client.
12. OCSP
13. _
14. Client key exchange. It is not signed by the client
15. Using SSL session id, the name of the field is pre master secret
16. GET to /. Response is 301. It auto redirects to /en-us/
17. Username: wireshark1, Password: TLSrulez

Using https://tls13.akamai.io/

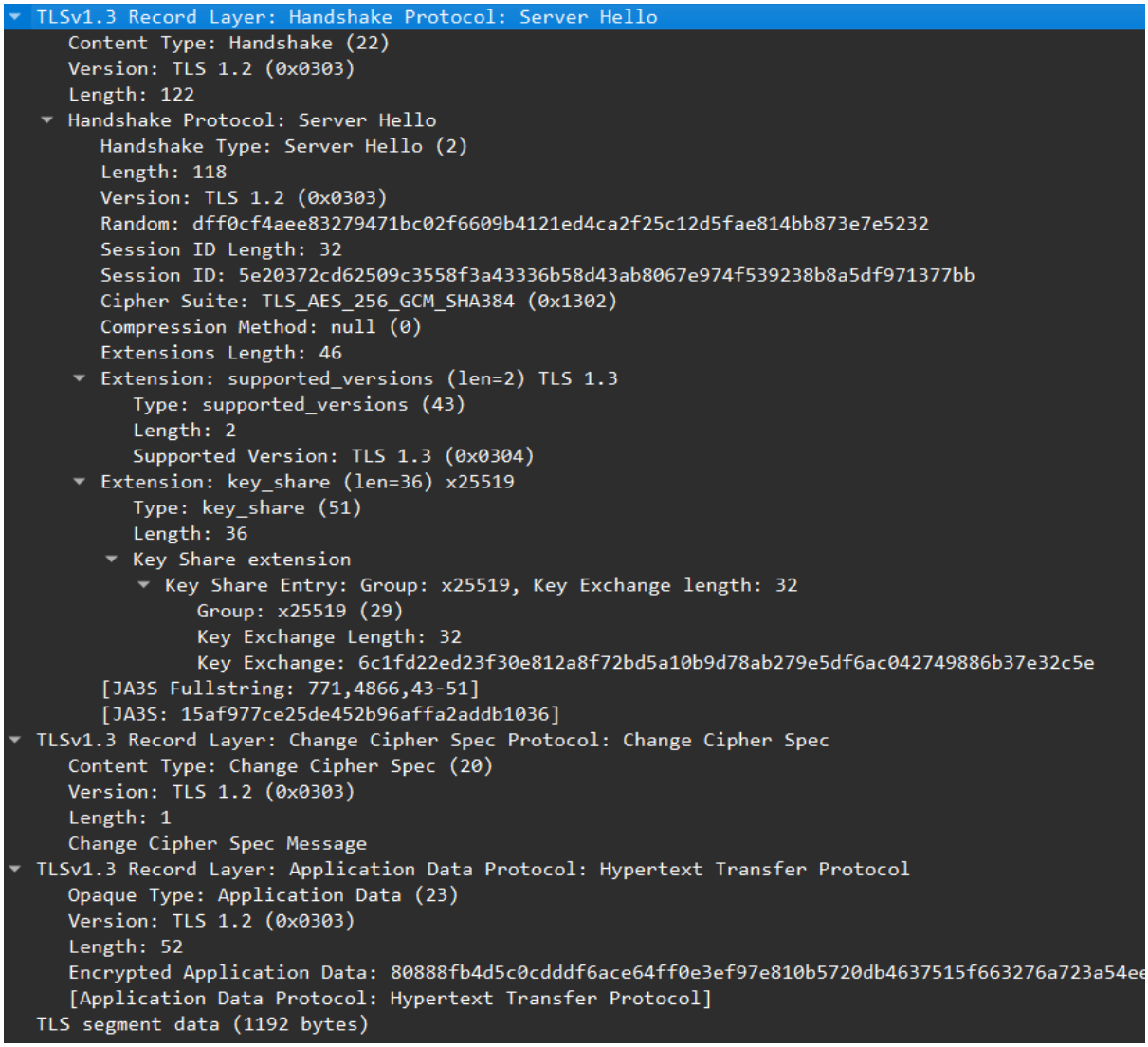
18. 1.2 19. 04c217 20. 5e2037 21. 17 22. TLS_AES_128_GCM_SHA256 (0x1301), TLS_CHACHA20_POLY1305_SHA256 (0x1303), TLS_AES_256_GCM_SHA384 (0x1302)



23. x25519 24. No



25. 1.2 26. Dff0cf 27. 5e2037 it's the same. We are in the same encrypted stream. 28. Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) 29. x25519 30. Yes. It would require trying again until they agree on a Diffie curve or close the connection.



31. ISRG Root X1 -> R10 -> check-tls.akamai.io
32. Subject Alternative Name