* Google.com
  1. C
  2. Yes, there are some TLS under version 1.2
  3. Yes, we can see warnings
* x.com

1. A
2. No, there are no TLS under version 1.2
3. No, we can’t see any warnings

* facebook.com

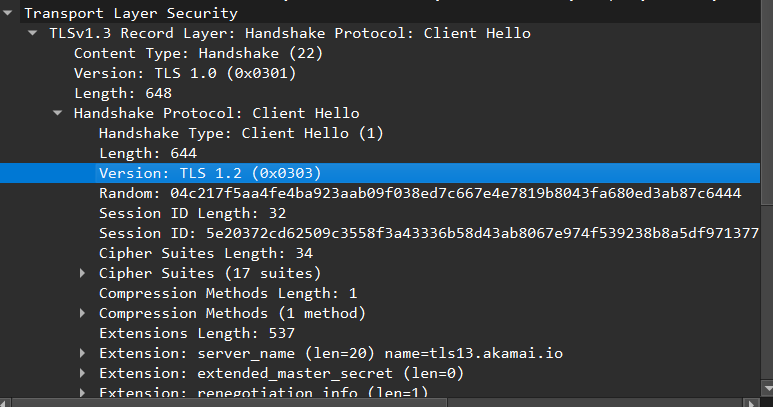
1. C
2. No, there are no TLS under version 1.2
3. Yes, we can see warnings

* ohel-shem.iscool.co.il

1. C
2. Yes, there are some TLS under version 1.2
3. Yes, we can see warnings
4. NO VIDEO IN ENGLISH
5. 53 packets. The filter is tls.handshake.type == 1
6. [www.hattrick.org](http://www.hattrick.org)
7. \_ws.col.info == "Client Hello (SNI=domain goes here)" && tls.handshake.type == 1
8. 1.2
   1. SHA384
   2. AES\_256\_GCM
   3. RSA
   4. Diffie Hellman
9. 2, Geotrust global and \*.hattrick.org
10. Yes
11. Between 30/06/2022 and 15/07/2023
12. DigiCert. It wasn’t sent to the client.
13. OCSP
14. \_
15. Client key exchange. It is not signed by the client
16. Using SSL session id, the name of the field is pre master secret
17. GET to /. Response is 301. It auto redirects to /en-us/
18. Username: wireshark1, Password: TLSrulez

Using https://tls13.akamai.io/

1. 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)

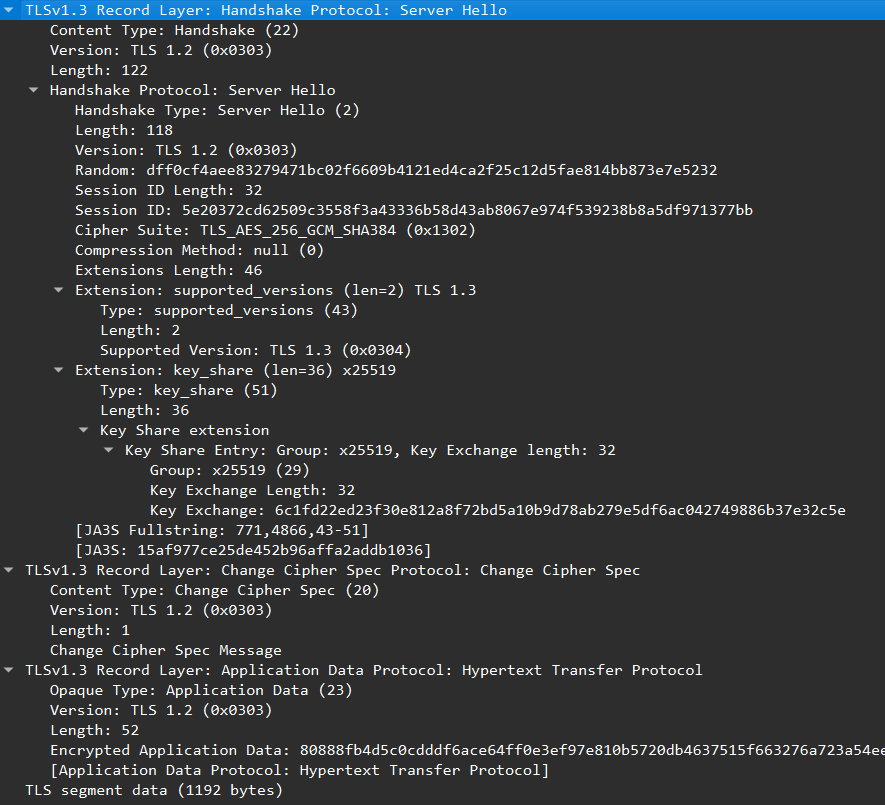


1. x25519 24. No

A computer screen shot of a program

Description automatically generated

1. 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.



1. ISRG Root X1 -> R10 -> check-tls.akamai.io
2. Subject Alternative Name