

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)

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 648
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 644
    Version: TLS 1.2 (0x0303)
    Random: 04c217f5aa4fe4ba923aab09f038ed7c667e4e7819b8043fa680ed3ab87c6444
    Session ID Length: 32
    Session ID: 5e20372cd62509c3558f3a43336b58d43ab8067e974f539238b8a5df971377
    Cipher Suites Length: 34
    Cipher Suites (17 suites)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 537
    Extension: server_name (len=20) name=tls13.akamai.io
    Extension: extended_master_secret (len=0)
    Extension: renegotiation_info (len=1)
```

23. x25519 24. No

```
Extension: key_share (len=107) x25519, secp256r1
  Type: key_share (51)
  Length: 107
  Key Share extension
    Client Key Share Length: 105
    Key Share Entry: Group: x25519, Key Exchange length: 32
    Group: x25519 (29)
    Key Exchange Length: 32
    Key Exchange: 1ec4869f1829b1cd6c1cad2bfb3738d3e05ed4e5adf0c54e08t
    Key Share Entry: Group: secp256r1, Key Exchange length: 65
    Group: secp256r1 (23)
    Key Exchange Length: 65
    Key Exchange: 046d81b4611fffd5bc01ad5a48e4235fc05dbf7aa2edac3cb2c4
```

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.

```

▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 122
  ▼ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 118
    Version: TLS 1.2 (0x0303)
    Random: dff0cf4aee83279471bc02f6609b4121ed4ca2f25c12d5fae814bb873e7e5232
    Session ID Length: 32
    Session ID: 5e20372cd62509c3558f3a43336b58d43ab8067e974f539238b8a5df971377bb
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Method: null (0)
    Extensions Length: 46
    ▼ Extension: supported_versions (len=2) TLS 1.3
      Type: supported_versions (43)
      Length: 2
      Supported Version: TLS 1.3 (0x0304)
    ▼ Extension: key_share (len=36) x25519
      Type: key_share (51)
      Length: 36
      ▼ Key Share extension
        ▼ Key Share Entry: Group: x25519, Key Exchange length: 32
          Group: x25519 (29)
          Key Exchange Length: 32
          Key Exchange: 6c1fd22ed23f30e812a8f72bd5a10b9d78ab279e5df6ac042749886b37e32c5e
          [JA3S Fullstring: 771,4866,43-51]
          [JA3S: 15af977ce25de452b96affa2addb1036]
    ▼ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
    ▼ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 52
      Encrypted Application Data: 80888fb4d5c0cdddf6ace64ff0e3ef97e810b5720db4637515f663276a723a54ee
      [Application Data Protocol: Hypertext Transfer Protocol]
  TLS segment data (1192 bytes)

```

31. ISRG Root X1 -> R10 -> check-tls.akamai.io

32. Subject Alternative Name