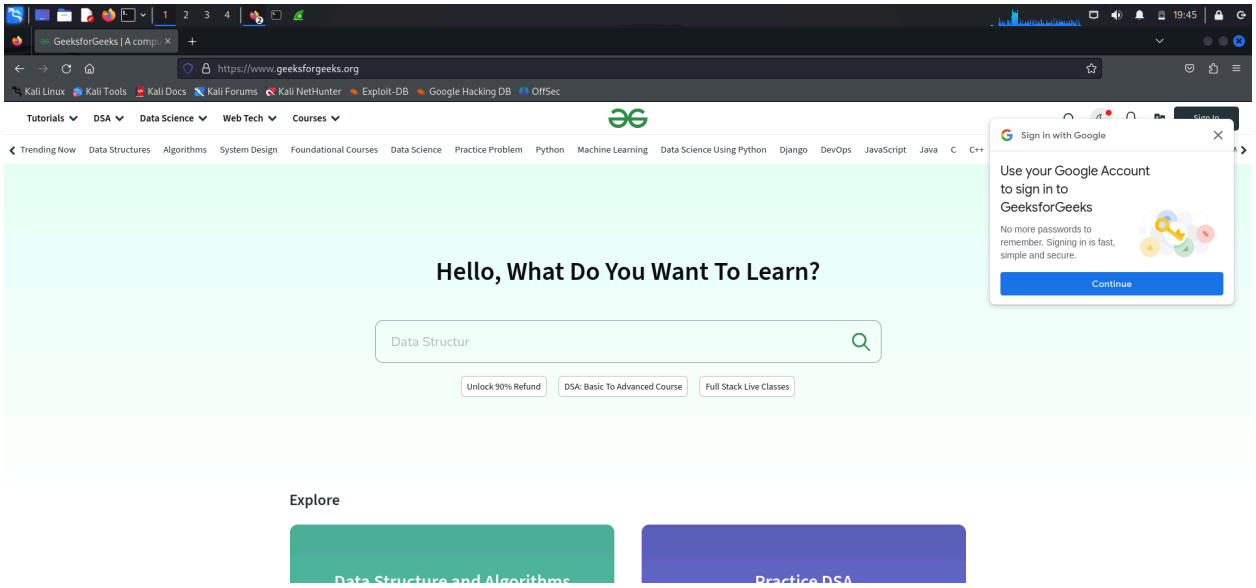
Secure Session Establishment with SSL/TLS

Bakka Ramyasree

Prepare the Environment:

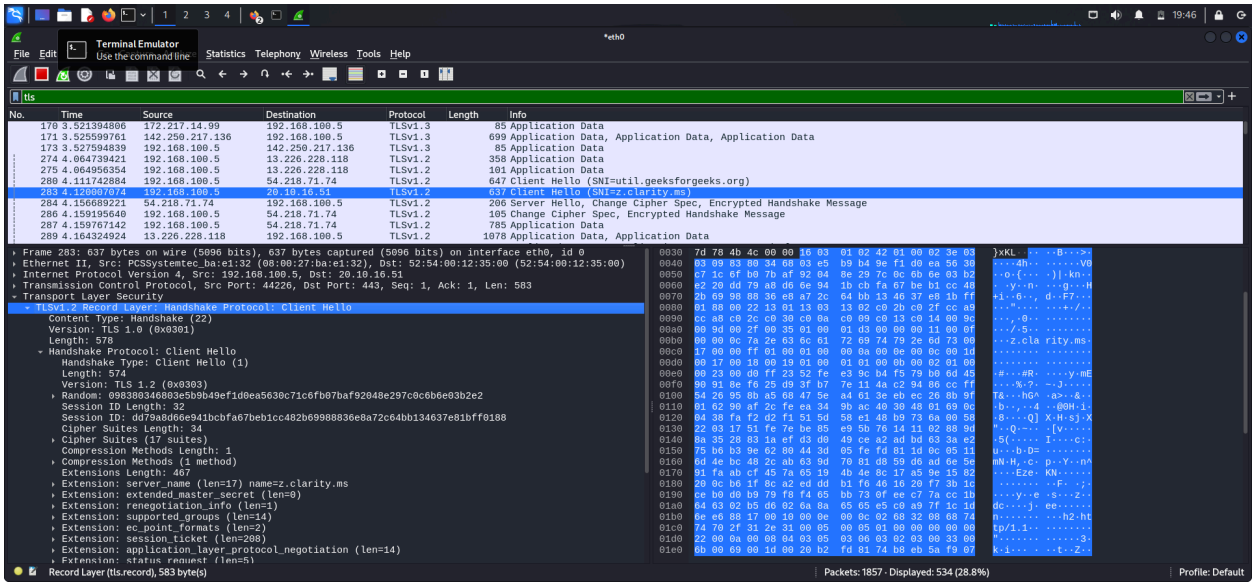
- Start a Wireshark capture and use a browser to visit an HTTPS website

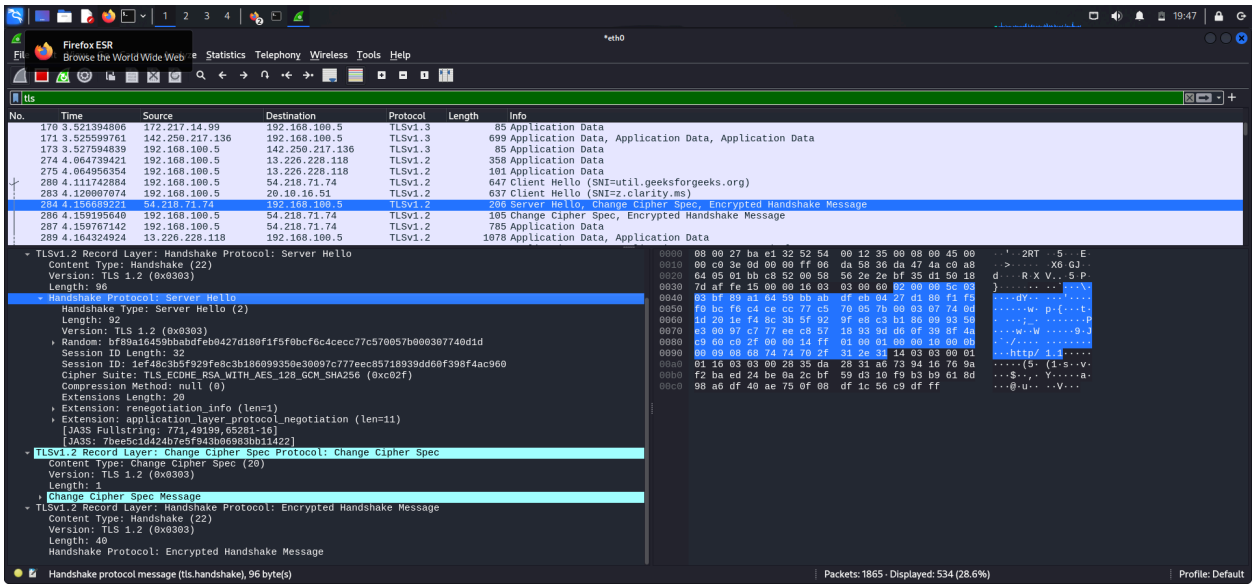


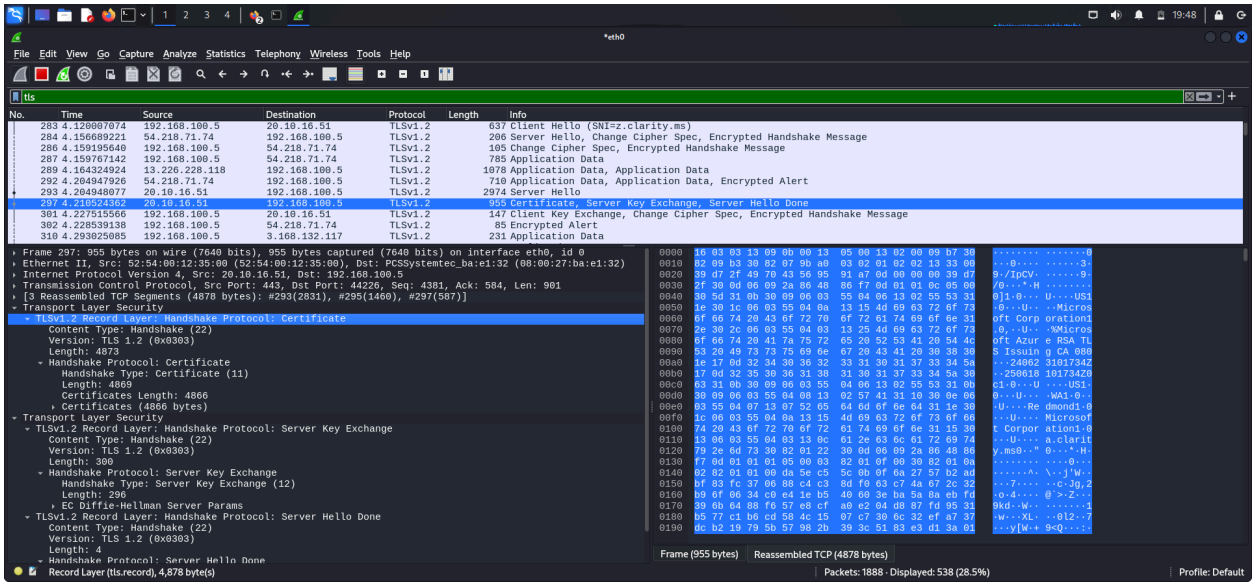
Filter for SSL/TLS Traffic:

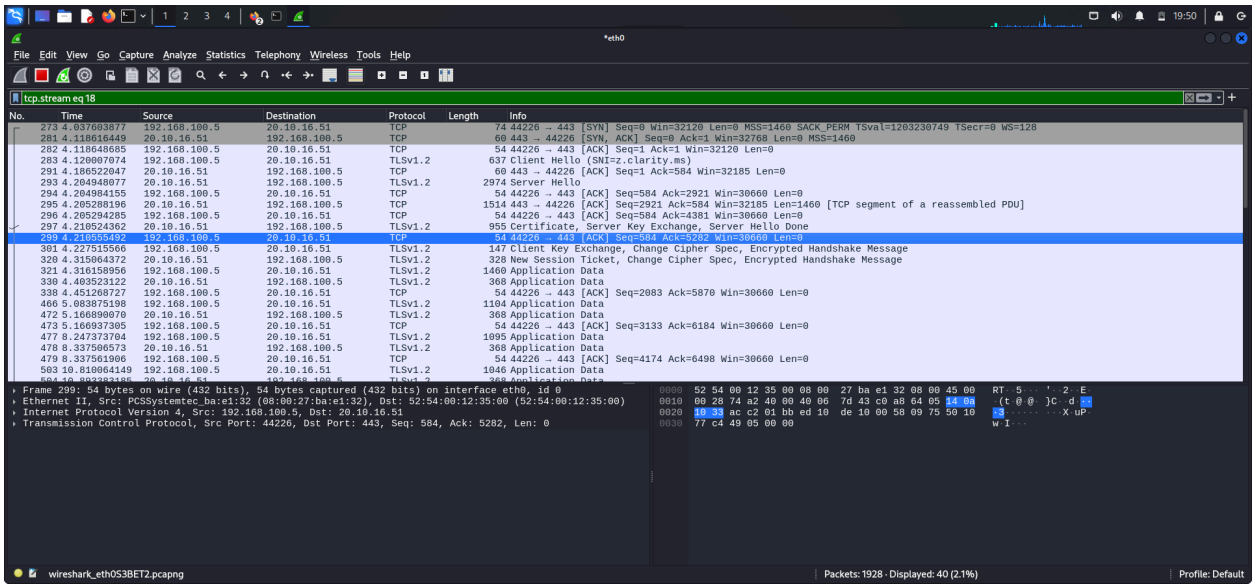
- Use the filter `ssl` or `tls` in Wireshark.

2. **Identify the SSL/TLS Handshake:**
   - Locate the packets involved in the SSL/TLS handshake process.
   - Identify key steps: ClientHello, ServerHello, Certificate exchange, Key exchange, etc.
   - Take screenshots of these packets.


Terminal Emulator
Use the command line
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
170 3.521394806 172.217.14.99 192.168.100.5 TLSv1.3 85 Application Data
171 3.525599761 142.250.217.136 192.168.100.5 TLSv1.3 699 Application Data, Application Data, Application Data
173 3.527594839 192.168.100.5 142.250.217.136 TLSv1.3 85 Application Data
274 4.064739421 192.168.100.5 13.226.228.118 TLSv1.2 358 Application Data
275 4.064956354 192.168.100.5 13.226.228.118 TLSv1.2 101 Application Data
280 4.111742884 192.168.100.5 54.218.71.74 TLSv1.2 647 Client Hello (SNI=util.geeksforgeeks.org)
283 4.120007074 192.168.100.5 20.10.16.51 TLSv1.2 637 Client Hello (SNI=z.clarity.ms)
284 4.156689221 54.218.71.74 192.168.100.5 TLSv1.2 206 Server Hello, Change Cipher Spec, Encrypted Handshake Message
286 4.159195640 192.168.100.5 54.218.71.74 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
287 4.159767142 192.168.100.5 54.218.71.74 TLSv1.2 785 Application Data
289 4.164324924 13.226.228.118 192.168.100.5 TLSv1.2 1078 Application Data, Application Data
Frame 283: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 20.10.16.51
Transmission Control Protocol, Src Port: 44226, Dst Port: 443, Seq: 1, Ack: 1, Len: 583
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 578
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 574
Version: TLS 1.2 (0x0303)
Random: 0983803468893e5b9b49ef1d0ea5630c71c6fb07baf92048e297c0c6b6e03b2e2
Session ID Length: 32
Session ID: dd79a8d66e941bcbfa67beb1cc482b69988836e8a72c64bb134637e81bff0188
Cipher Suites Length: 34
Cipher Suites (17 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 467
Extension: server_name (len=17) name=z.clarity.ms
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)
Extension: supported_groups (len=14)
Extension: ec_point_formats (len=2)
Extension: session_ticket (len=208)
Extension: application_layer_protocol_negotiation (len=14)
Extension: status_request (len=5)
Record Layer (tls.record), 583 byte(s)
Packets: 1857 · Displayed: 534 (28.8%)
Profile: Default

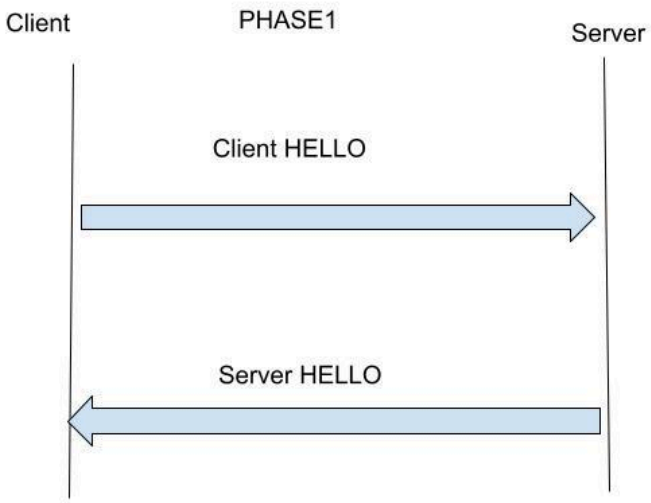

Firefox ESR
Browse the World Wide Web
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
170 3.521394806 172.217.14.99 192.168.100.5 TLSv1.3 85 Application Data
171 3.525599761 142.250.217.136 192.168.100.5 TLSv1.3 699 Application Data, Application Data, Application Data
173 3.527594839 192.168.100.5 142.250.217.136 TLSv1.3 85 Application Data
274 4.064739421 192.168.100.5 13.226.228.118 TLSv1.2 358 Application Data
275 4.064956354 192.168.100.5 13.226.228.118 TLSv1.2 101 Application Data
280 4.111742884 192.168.100.5 54.218.71.74 TLSv1.2 647 Client Hello (SNI=util.geeksforgeeks.org)
283 4.120007074 192.168.100.5 20.10.16.51 TLSv1.2 637 Client Hello (SNI=z.clarity.ms)
284 4.156689221 54.218.71.74 192.168.100.5 TLSv1.2 206 Server Hello, Change Cipher Spec, Encrypted Handshake Message
286 4.159195640 192.168.100.5 54.218.71.74 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
287 4.159767142 192.168.100.5 54.218.71.74 TLSv1.2 785 Application Data
289 4.164324924 13.226.228.118 192.168.100.5 TLSv1.2 1078 Application Data, Application Data
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 90
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 92
Version: TLS 1.2 (0x0303)
Random: bf89a16459bbabdfeb0427d180f1f5f0bcf6c4cecc77c570057b000307740d1d
Session ID Length: 32
Session ID: 1ef48c3b5f929fe8c3b18609935e30097c777eec85718939dd60f398f4ac960
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Compression Method: null (0)
Extensions Length: 20
Extension: renegotiation_info (len=1)
Extension: application_layer_protocol_negotiation (len=11)
[JA3S Fullstring: 771,49199,65281-16]
[JA3S: 7bee5c1d424b7e5f943b06983bb11422]
TLSv1.2 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
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 40
Handshake Protocol: Encrypted Handshake Message
Handshake protocol message (tls.handshake), 96 byte(s)
Packets: 1865 · Displayed: 534 (28.6%)
Profile: Default

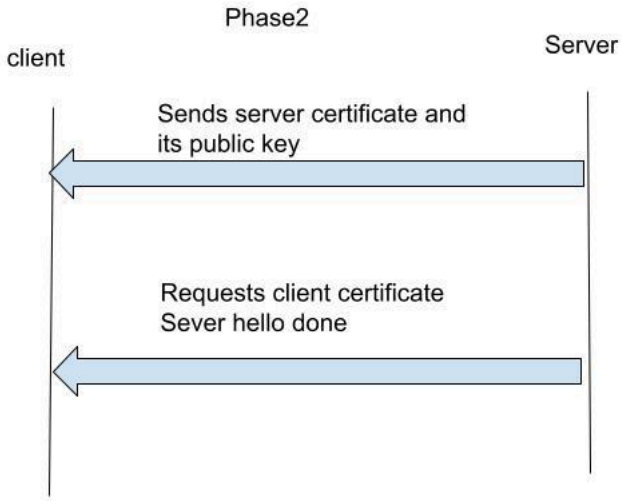


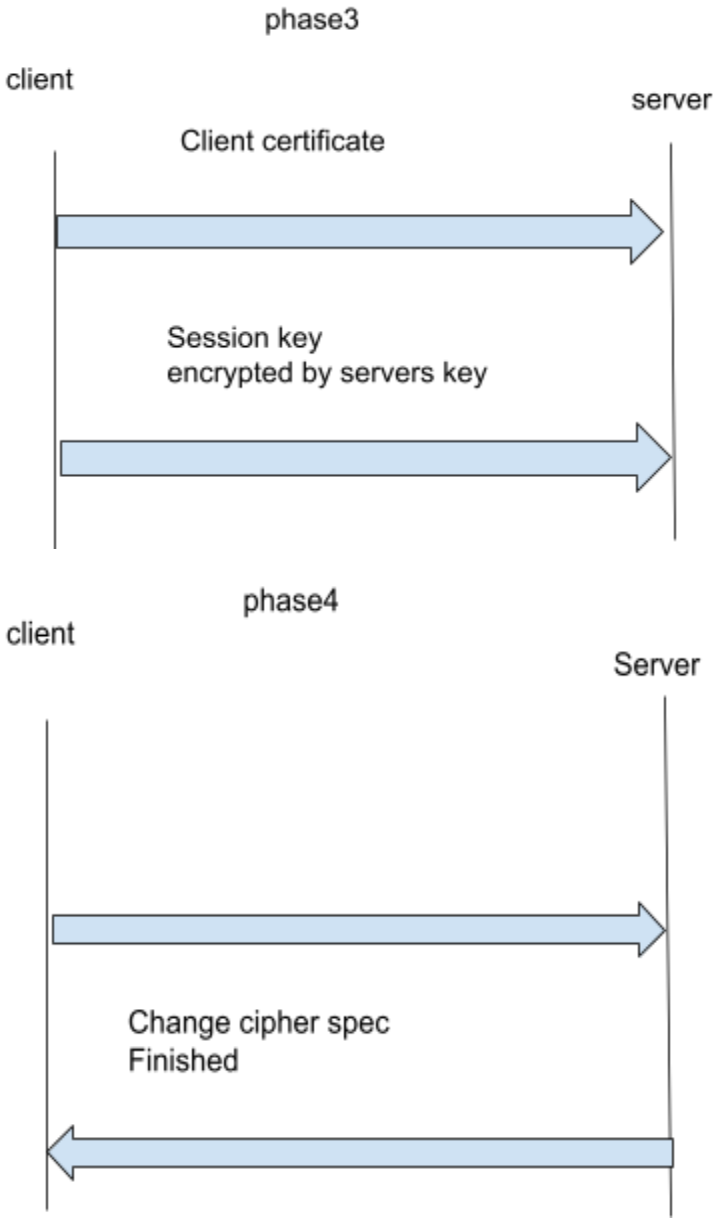


Analyze the Handshake:

Describe each step in the SSL/TLS handshake process.


Client
PHASE1
Server
Client HELLO
Server HELLO


Phase2
client
Server
Sends server certificate and
its public key
Requests client certificate
Sever hello done



Discuss the purpose of encryption and key exchange in securing the session.

- Key exchange and encryption are necessary for protecting internet communications.
- The goal of encryption is to maintain confidentiality by generating data inaccessible to those lacking the necessary key. It guarantees that your data cannot be understood even if it is intercepted.
- Key Exchange Goal: Safe Communication The process of safely exchanging encryption keys between participants in communication is known as key exchange. The data is encrypted and decrypted using these keys.

Create a report explaining how SSL/TLS secures a session.

Establishing the Link

Handshake: I went to greek for greek and the website engages in a handshake when you visit a secure website. It's similar to them presenting themselves and deciding on a safe communication style.
Certificates: To verify its legitimacy, the website sends a certificate. It's similar to them presenting their ID card as proof of identity.
Keys: To ensure that messages are unreadable by others, they trade unique codes, or keys.
Safeguarding Data
Encryption: All information passed between my browser and the website gets jumbled (encrypted) once they've decided on the keys. The data cannot be unlocked (decrypted) without the correct key.
Integrity: To make sure the data hasn't been altered during transmission, they append unique codes.