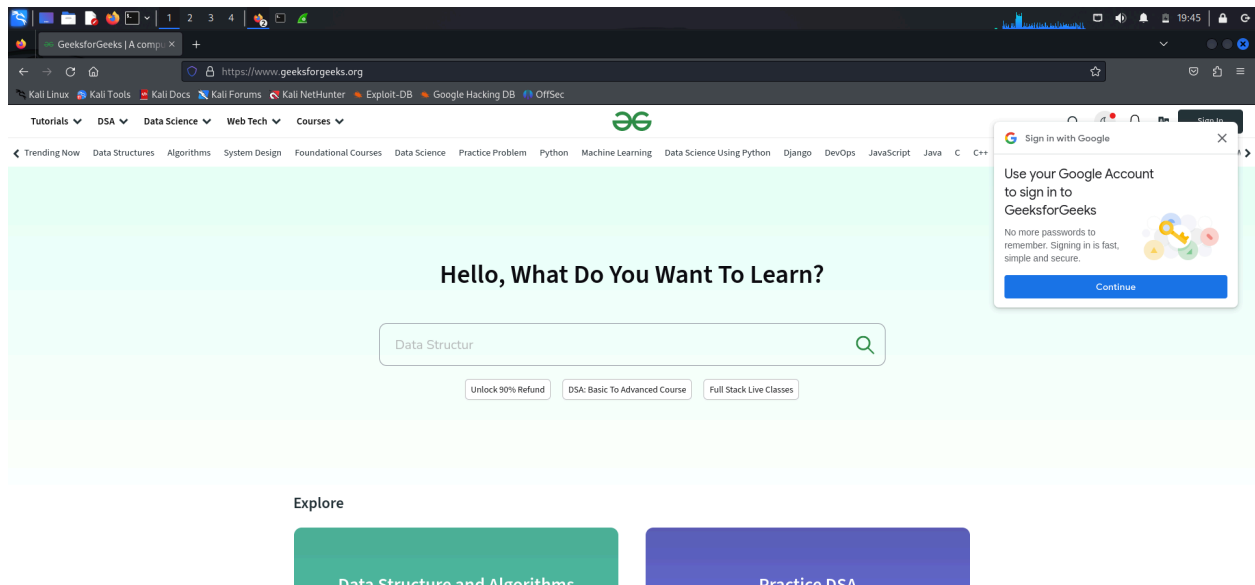


Secure Session Establishment with SSL/TLS

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 window showing network traffic analysis. The interface includes a menu bar (File, Edit, Terminal Emulator, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display shows a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 283) is a TLSv1.2 Record Layer: Handshake Protocol: Client Hello. The packet details are displayed on the right, showing the handshake process and the client's hello message. The packet is 583 bytes long and contains the following information:

- Content Type: Handshake (22)
- Version: TLS 1.0 (0x0301)
- Length: 578
- Handshake Protocol: Client Hello (1)
- Handshake Type: Client Hello (1)
- Length: 574
- Version: TLS 1.2 (0x0303)
- Random: 098380346803e5b9b49ef1d0ea5630c71c6fb07baf92048e2970c6b6e03b2e2
- Session ID Length: 32
- Session ID: dd79a8d0e0a1bcbfa67bebb1cc482b6998083ee8a72c64bb134637e81bfff018e
- 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)

Packets: 1857 - Displayed: 534 (28.8%)

Firefox ESR window showing network traffic analysis. The interface includes a menu bar (File, Edit, Firefox ESR, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display shows a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 284) is a TLSv1.2 Record Layer: Handshake Protocol: Server Hello. The packet details are displayed on the right, showing the handshake process and the server's hello message. The packet is 96 bytes long and contains the following information:

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 96
- Handshake Protocol: Server Hello (2)
- Handshake Type: Server Hello (2)
- Length: 92
- Version: TLS 1.2 (0x0303)
- Random: bf08a16459bbabdfbeb427d180f1f5f0bcbfc4cecc77c570057b090307748d1d
- Session ID Length: 32
- Session ID: 1ef48e305f029f8eb3b186099350e0907c777ec5b718930dd60f398f4ac960
- 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: 70ec5142407c5f943d0803011422]

Packets: 1865 - Displayed: 534 (28.6%)

Wireshark capture of an SSL/TLS handshake. The packet list shows the Client Hello, Server Hello, Certificate, Server Key Exchange, and Client Key Exchange. The packet details pane shows the structure of the Certificate and Server Key Exchange. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
283	4.126997074	192.168.100.5	20.10.16.51	TLSv1.2	637	Client Hello (SN#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	4.159195649	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
292	4.204947926	54.218.71.74	192.168.100.5	TLSv1.2	710	Application Data, Application Data, Encrypted Alert
293	4.204948077	20.10.16.51	192.168.100.5	TLSv1.2	2974	Server Hello
297	4.210524362	20.10.16.51	192.168.100.5	TLSv1.2	955	Certificate, Server Key Exchange, Server Hello Done
301	4.227515566	192.168.100.5	20.10.16.51	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
302	4.228359138	192.168.100.5	54.218.71.74	TLSv1.2	85	Encrypted Alert
310	4.293025085	192.168.100.5	3.168.132.117	TLSv1.2	231	Application Data

Frame 297: 955 bytes on wire (7640 bits), 955 bytes captured (7640 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32)
 Internet Protocol Version 4, Src: 20.10.16.51, Dst: 192.168.100.5
 Transmission Control Protocol, Src Port: 443, Dst Port: 44226, Seq: 4381, Ack: 584, Len: 901
 [3 Reassembled TCP Segments (4878 bytes): #293(2831), #295(1460), #297(587)]
 Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 4873
 Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 4869
 Certificates Length: 4866
 Certificates (4866 bytes)
 Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 308
 Handshake Protocol: Server Key Exchange
 Handshake Type: Server Key Exchange (12)
 Length: 298
 EC Diffie-Hellman Server Params
 - TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 4
 Handshake Protocol: Server Hello Done
 Record Layer (tlsrecord), 4878 byte(s)

Frame (955 bytes) Reassembled TCP (4878 bytes)
 Packets: 1888 - Displayed: 538 (28.5%) Profile: Default

Wireshark capture of a TCP stream. The packet list shows the Client Hello, Server Hello, Certificate, Server Key Exchange, and Client Key Exchange. The packet details pane shows the structure of the Certificate and Server Key Exchange. The packet bytes pane shows the raw data.

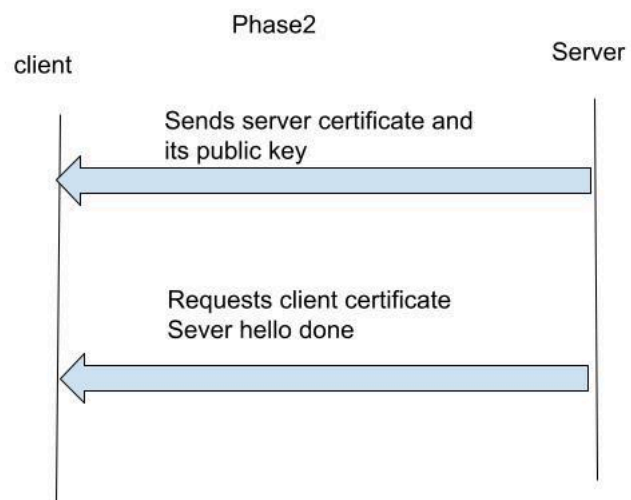
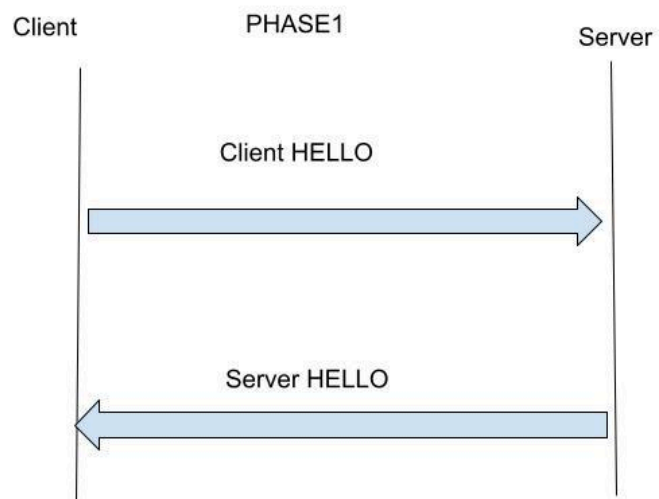
No.	Time	Source	Destination	Protocol	Length	Info
273	4.037663877	192.168.100.5	20.10.16.51	TCP	74	44226 -> 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1203230749 TSecr=0 WS=128
281	4.118616449	20.10.16.51	192.168.100.5	TCP	60	443 -> 44226 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
282	4.118648685	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=1 Win=32120 Len=0
283	4.126997074	192.168.100.5	20.10.16.51	TLSv1.2	637	Client Hello (SN#z.clarity.ms)
291	4.160522047	20.10.16.51	192.168.100.5	TCP	60	443 -> 44226 [ACK] Seq=1 Ack=584 Win=32185 Len=0
293	4.204948077	20.10.16.51	192.168.100.5	TLSv1.2	2974	Server Hello
294	4.204948135	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=584 Ack=2921 Win=30660 Len=0
295	4.205288196	20.10.16.51	192.168.100.5	TCP	1514	443 -> 44226 [ACK] Seq=2921 Ack=584 Win=32185 Len=1460 [TCP segment of a reassembled PDU]
296	4.205294285	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=584 Ack=4381 Win=30660 Len=0
297	4.210524362	20.10.16.51	192.168.100.5	TLSv1.2	955	Certificate, Server Key Exchange, Server Hello Done
299	4.210524362	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=584 Ack=4381 Win=30660 Len=0
301	4.227515566	192.168.100.5	20.10.16.51	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
320	4.315064372	20.10.16.51	192.168.100.5	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
321	4.316158956	192.168.100.5	20.10.16.51	TLSv1.2	1460	Application Data
330	4.403023122	20.10.16.51	192.168.100.5	TLSv1.2	368	Application Data
338	4.451268727	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=2083 Ack=5870 Win=30660 Len=0
466	5.083875198	192.168.100.5	20.10.16.51	TLSv1.2	1104	Application Data
472	5.168980970	20.10.16.51	192.168.100.5	TLSv1.2	368	Application Data
473	5.168937305	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=3133 Ack=6184 Win=30660 Len=0
477	5.247373704	192.168.100.5	20.10.16.51	TLSv1.2	1095	Application Data
478	5.337506073	20.10.16.51	192.168.100.5	TLSv1.2	368	Application Data
479	5.337561906	192.168.100.5	20.10.16.51	TCP	54	44226 -> 443 [ACK] Seq=4174 Ack=6498 Win=30660 Len=0
503	10.81064149	192.168.100.5	20.10.16.51	TLSv1.2	1046	Application Data

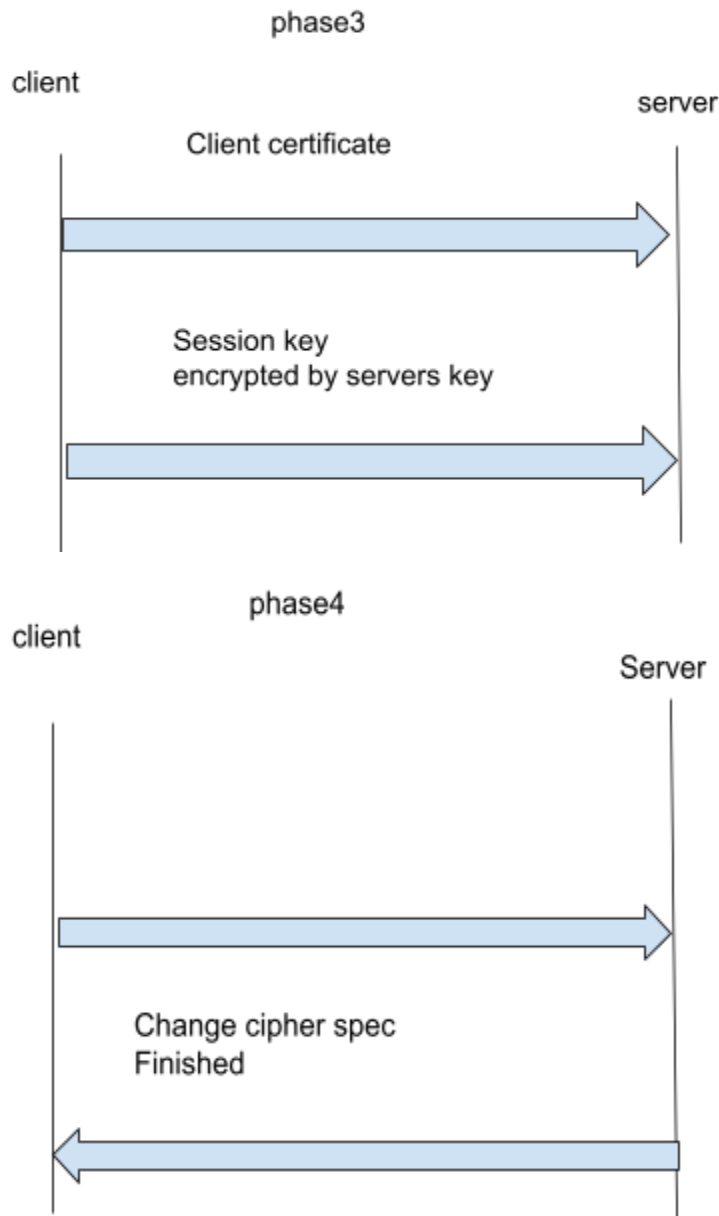
Frame 299: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
 Internet Protocol Version 4, Src: 192.168.100.5, Dst: 20.10.16.51
 Transmission Control Protocol, Src Port: 44226, Dst Port: 443, Seq: 584, Ack: 5282, Len: 0

wireshark_eth0538ET2.pcapng Packets: 1928 - Displayed: 40 (2.1%) Profile: Default

Analyze the Handshake:

Describe each step in the SSL/TLS handshake process.





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.