Secure Session Establishment with SSL/TLS

Objective:

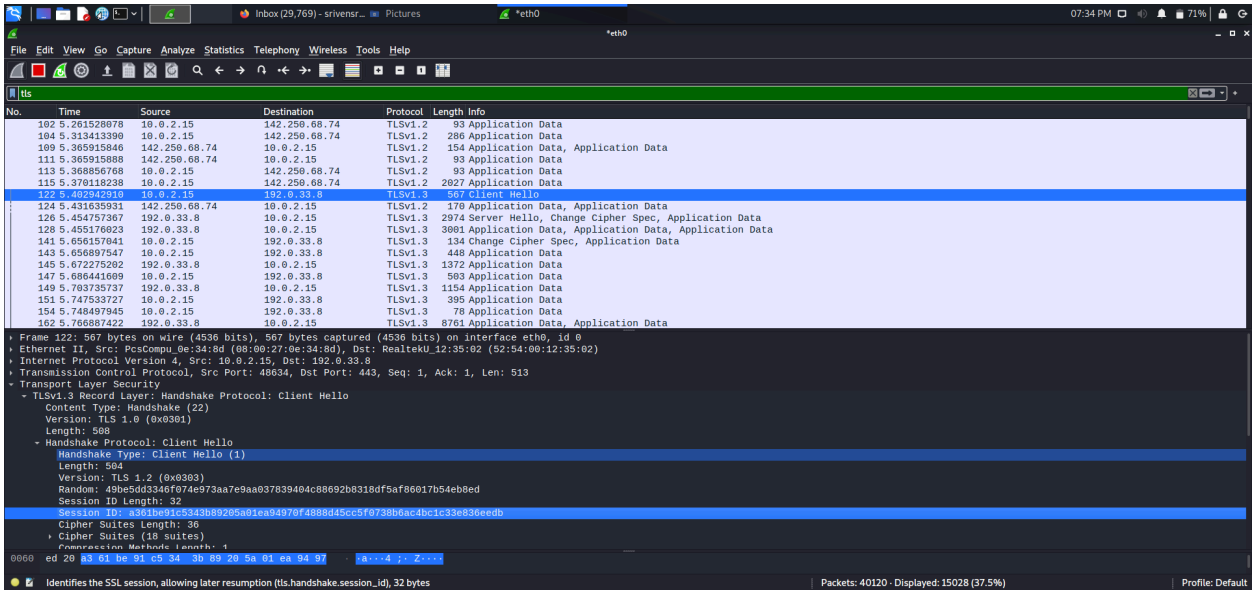
To understand how a secure session is established using SSL/TLS, including the handshake process and the exchange of encryption keys.

1. **Prepare the Environment:** Start a Wireshark capture and use a browser to visit an HTTPS website https://example.com
2. **Filter for SSL/TLS Traffic:** Use the filter ssl or tls in Wireshark.
3. **Identify the SSL/TLS Handshake:** Locate the packets involved in the SSL/TL handshake process. Identify key steps: ClientHello, ServerHello, Certificate exchange, Key exchange, etc.

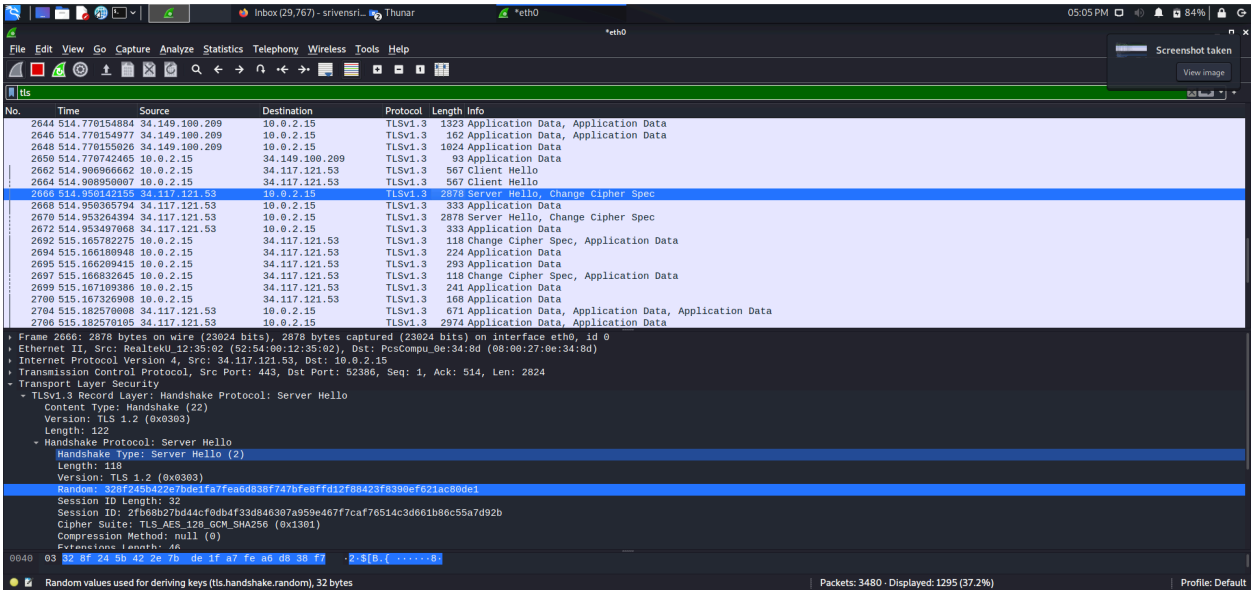
Contents in the handshakes

1. **Protocol Version**: Specifies the highest version of SSL/TLS that the client supports.
2. **Cipher Suites**: Lists the encryption algorithms (e.g., AES, RSA) that the client is capable of using.
3. **Compression Methods**: Lists the compression methods supported by the client.
4. **Random Data**: A randomly generated number used later in the key exchange.
5. **Session ID** : If resuming a previous session, this identifies the session to be resumed.
6. **Extensions**: Includes additional parameters such as server name indication (SNI) for virtual hosting.

Client Hello- A web browser initiates the handshake by sending a "Client Hello" message to the server. The client initiates the handshake by sending a "Client Hello" message to the server. This message includes information such as the SSL/TLS version the client supports, the cipher suites (encryption algorithms) it can use, and other options like compression methods.

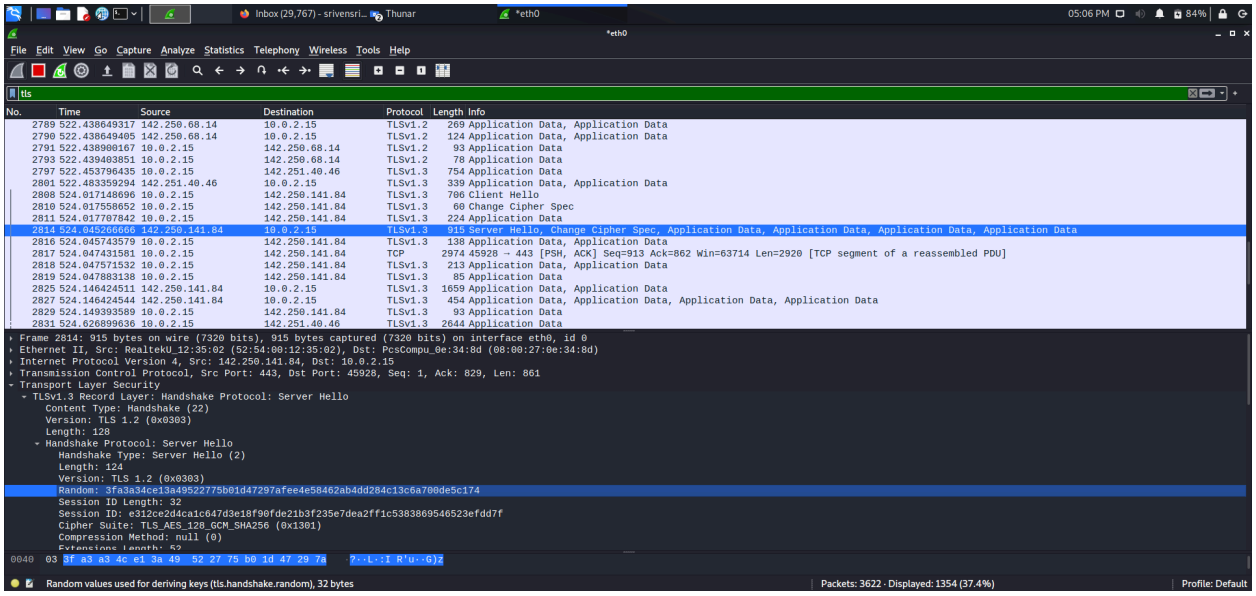


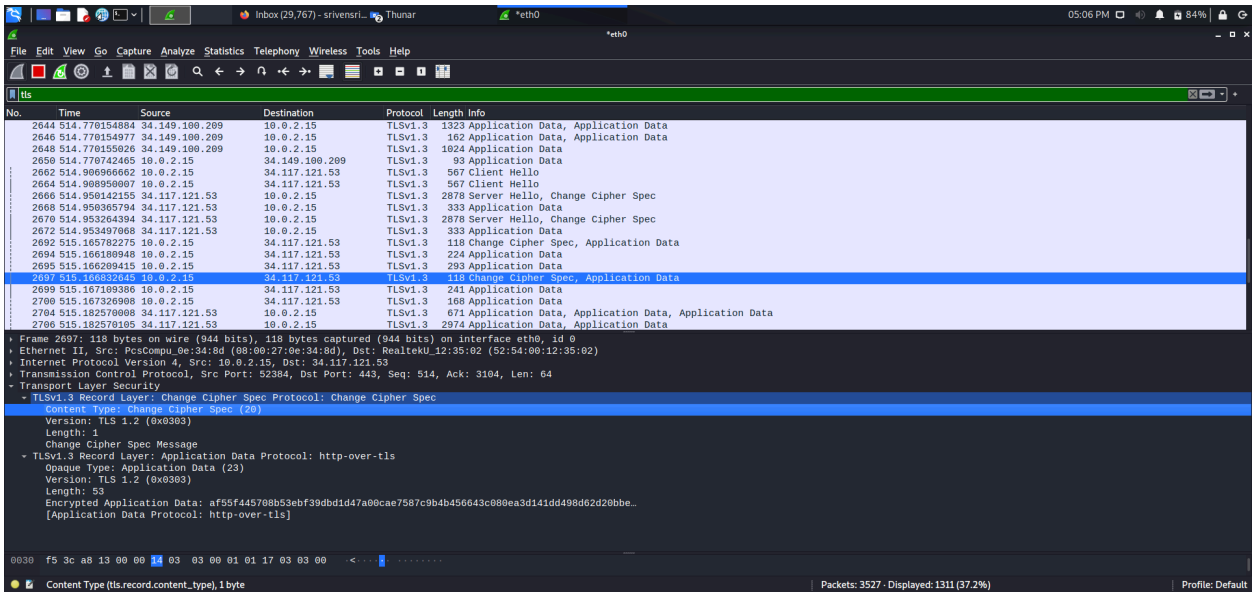
Server Hello Response: The server responds with a "Server Hello" message selecting the SSL/TLS version and cipher suite from the client's list. It also sends a random number and other information needed for the session.

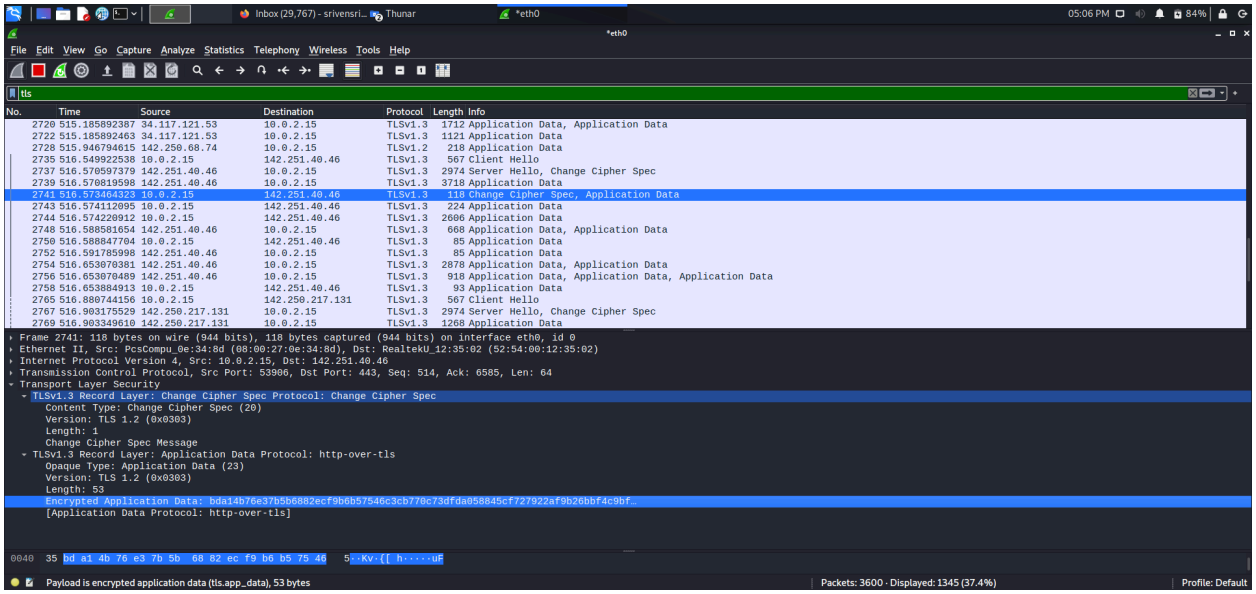


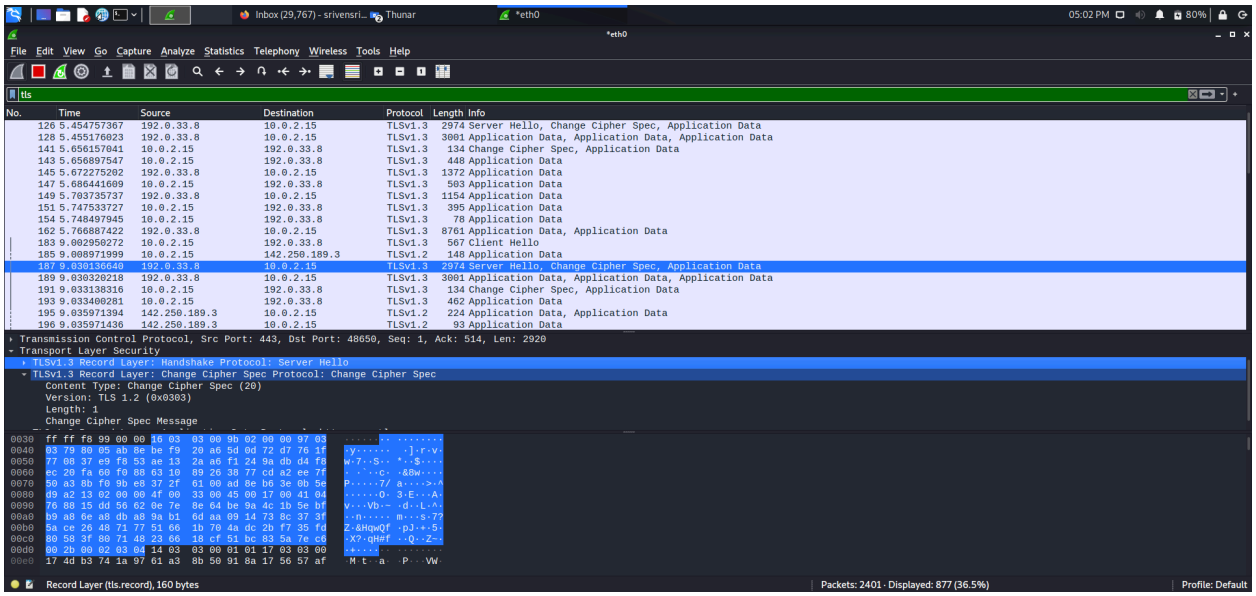
Change Cipher Spec

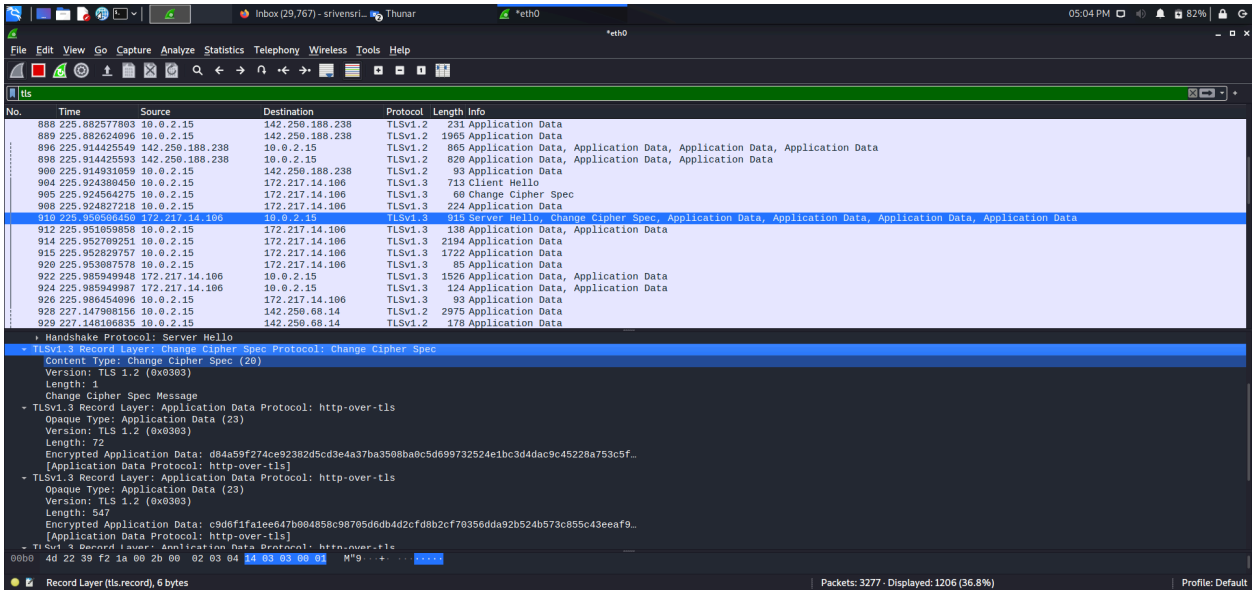
1. **Notification**: The client sends a "Change Cipher Spec" message to notify the server that subsequent messages will be encrypted with the newly agreed-upon keys and algorithms.
2. **Contents**: This is a single-byte message indicating that the client is switching to encrypted communication.






Inbox (29,767) - srivensri... Thunar
*eth0
05:06 PM
84%
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
2720 515.185892387 34.117.121.53 10.0.2.15 TLSv1.3 1712 Application Data, Application Data
2722 515.185892463 34.117.121.53 10.0.2.15 TLSv1.3 1121 Application Data
2728 515.946794615 142.250.68.74 10.0.2.15 TLSv1.2 218 Application Data
2735 516.549922538 10.0.2.15 142.251.40.46 TLSv1.3 567 Client Hello
2737 516.570597379 142.251.40.46 10.0.2.15 TLSv1.3 2974 Server Hello, Change Cipher Spec
2739 516.570819598 142.251.40.46 10.0.2.15 TLSv1.3 3718 Application Data
2741 516.573464323 10.0.2.15 142.251.40.46 TLSv1.3 118 Change Cipher Spec, Application Data
2743 516.574112095 10.0.2.15 142.251.40.46 TLSv1.3 224 Application Data
2744 516.574220912 10.0.2.15 142.251.40.46 TLSv1.3 2606 Application Data
2748 516.588581654 142.251.40.46 10.0.2.15 TLSv1.3 668 Application Data, Application Data
2750 516.588847704 10.0.2.15 142.251.40.46 TLSv1.3 85 Application Data
2752 516.591785998 142.251.40.46 10.0.2.15 TLSv1.3 85 Application Data
2754 516.653070381 142.251.40.46 10.0.2.15 TLSv1.3 2878 Application Data, Application Data
2756 516.653070489 142.251.40.46 10.0.2.15 TLSv1.3 918 Application Data, Application Data, Application Data
2758 516.653884913 10.0.2.15 142.251.40.46 TLSv1.3 93 Application Data
2765 516.880744156 10.0.2.15 142.250.217.131 TLSv1.3 567 Client Hello
2767 516.903175529 142.250.217.131 10.0.2.15 TLSv1.3 2974 Server Hello, Change Cipher Spec
2769 516.903349610 142.250.217.131 10.0.2.15 TLSv1.3 1268 Application Data
Frame 2741: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.40.46
Transmission Control Protocol, Src Port: 53906, Dst Port: 443, Seq: 514, Ack: 6585, Len: 64
Transport Layer Security
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: http-over-tls
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 53
Encrypted Application Data: bda14b76e37b5b6882ecf9b6b57546c3cb770c73dfda058845cf727922af9b26bbf4c9bf…
[Application Data Protocol: http-over-tls]
0040 35 bd a1 4b 76 e3 7b 5b 68 82 ec f9 b6 b5 75 46 5··Kv·{[h·····uF
Payload is encrypted application data (tls.app_data), 53 bytes
Packets: 3600 · Displayed: 1345 (37.4%)
Profile: Default


Inbox (29,767) - srivensri... Thunar
*eth0
05:02 PM
80%
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
126 5.454757367 192.0.33.8 10.0.2.15 TLSv1.3 2974 Server Hello, Change Cipher Spec, Application Data
128 5.455176023 192.0.33.8 10.0.2.15 TLSv1.3 3001 Application Data, Application Data, Application Data
141 5.656157041 10.0.2.15 192.0.33.8 TLSv1.3 134 Change Cipher Spec, Application Data
143 5.656897547 10.0.2.15 192.0.33.8 TLSv1.3 448 Application Data
145 5.672275202 192.0.33.8 10.0.2.15 TLSv1.3 1372 Application Data
147 5.686441609 10.0.2.15 192.0.33.8 TLSv1.3 503 Application Data
149 5.703735737 192.0.33.8 10.0.2.15 TLSv1.3 1154 Application Data
151 5.747533727 10.0.2.15 192.0.33.8 TLSv1.3 395 Application Data
154 5.748497945 10.0.2.15 192.0.33.8 TLSv1.3 78 Application Data
162 5.766887422 192.0.33.8 10.0.2.15 TLSv1.3 8761 Application Data, Application Data
183 9.002950272 10.0.2.15 192.0.33.8 TLSv1.3 567 Client Hello
185 9.008971999 10.0.2.15 142.250.189.3 TLSv1.2 148 Application Data
187 9.030136640 192.0.33.8 10.0.2.15 TLSv1.3 2974 Server Hello, Change Cipher Spec, Application Data
189 9.030320218 192.0.33.8 10.0.2.15 TLSv1.3 3001 Application Data, Application Data, Application Data
191 9.033138316 10.0.2.15 192.0.33.8 TLSv1.3 134 Change Cipher Spec, Application Data
193 9.033400281 10.0.2.15 192.0.33.8 TLSv1.3 462 Application Data
195 9.035971394 142.250.189.3 10.0.2.15 TLSv1.2 224 Application Data, Application Data
196 9.035971436 142.250.189.3 10.0.2.15 TLSv1.2 93 Application Data
Transmission Control Protocol, Src Port: 443, Dst Port: 48650, Seq: 1, Ack: 514, Len: 2920
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
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
0030 ff ff f8 99 00 00 16 03 03 00 9b 02 00 00 97 03
0040 03 79 80 05 ab 8e be f9 20 a6 5d 0d 72 d7 76 1f
0050 77 08 37 e9 f8 53 ae 13 2a a6 f1 24 9a db d4 f8
0060 ec 20 fa 60 f0 88 63 10 89 26 38 77 cd a2 ee 7f
0070 50 a3 8b f0 9b e8 37 2f 61 00 ad 8e b6 3e 0b 5e
0080 d9 a2 13 02 00 00 4f 00 33 00 45 00 17 00 41 04
0090 76 88 15 dd 56 02 0e 7e 8e 64 be 9a 4c 1b 5e bf
00a0 b9 a8 6e a8 db a8 9a b1 6d aa 09 14 73 8c 37 3f
00b0 5a ce 26 48 71 77 51 66 1b 70 4a dc 2b f7 35 fd
00c0 80 58 3f 80 71 48 23 66 18 cf 51 bc 83 5a 7e c6
00d0 00 2b 00 02 03 04 14 03 03 00 01 01 17 03 03 00
00e0 17 4d b3 74 1a 97 61 a3 8b 50 91 8a 17 56 57 af
Record Layer (tls.record), 160 bytes
Packets: 2401 · Displayed: 877 (36.5%)
Profile: Default



Necessity of Authentication:

Authentication is crucial for ensuring that the parties involved in the communication are who they claim to be:

1. **Server Authentication**: During the handshake, the server presents a digital certificate issued by a trusted CA. The client verifies this certificate to ensure it is communicating with the legitimate server.
2. **Securing the Session:** SSL/TLS ensures ongoing security throughout the session with the following features:

SSL/TLS secures a session through encryption, authentication, and key exchange processes:

1. **Encryption** ensures data confidentiality and integrity by converting data into unreadable ciphertext and including mechanisms to detect tampering.
2. **Key Exchange** securely establishes shared secrets that are used for symmetric encryption during the session.
3. **Authentication** verifies the identities of the communicating parties to prevent impersonation and ensure trust.

4. **Session Management** ensures that each session is unique and protected against future compromises. Together, these features create a secure environment for data transmission, safeguarding communications from various threats such as eavesdropping, tampering, and forgery.