

SSL / TLS

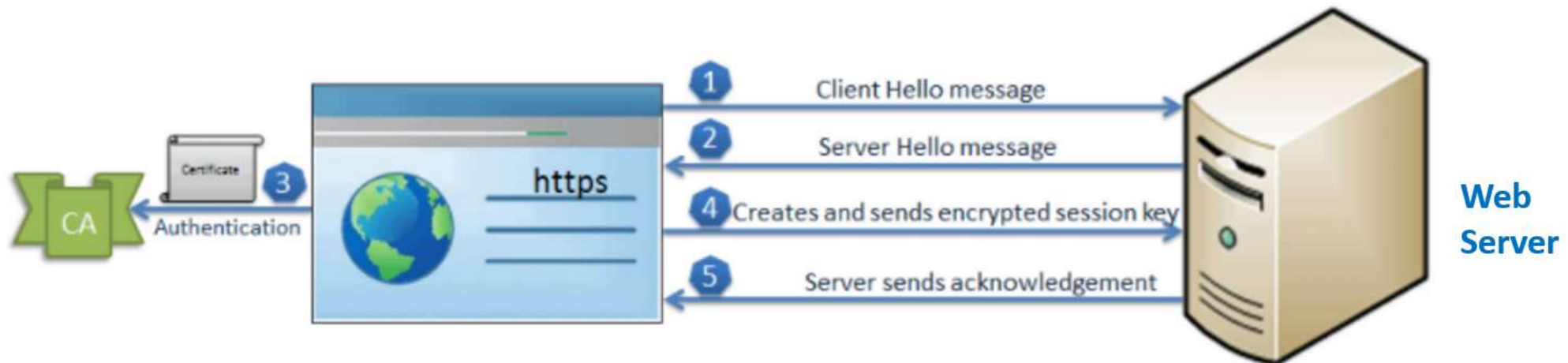
- **SSL** stands for **S**ecure **S**ocket **L**ayer
- **TLS** stands for **T**ransport **L**ayer **S**ecurity
- SSL is an encryption-based internet security protocol, developed by Netscape in 1995.
- In 1999 the Internet Engineering Task Force (IETF) proposed an update to SSL to enhance the security and changed the name as TLS.
- Some people still use SSL to refer to TLS, others use the term "SSL/TLS encryption" because SSL still has so much name recognition.
- This protocol helps to establish a secured, authenticated & encrypted links between the communicating devices

Advantages of SSL / TLS:

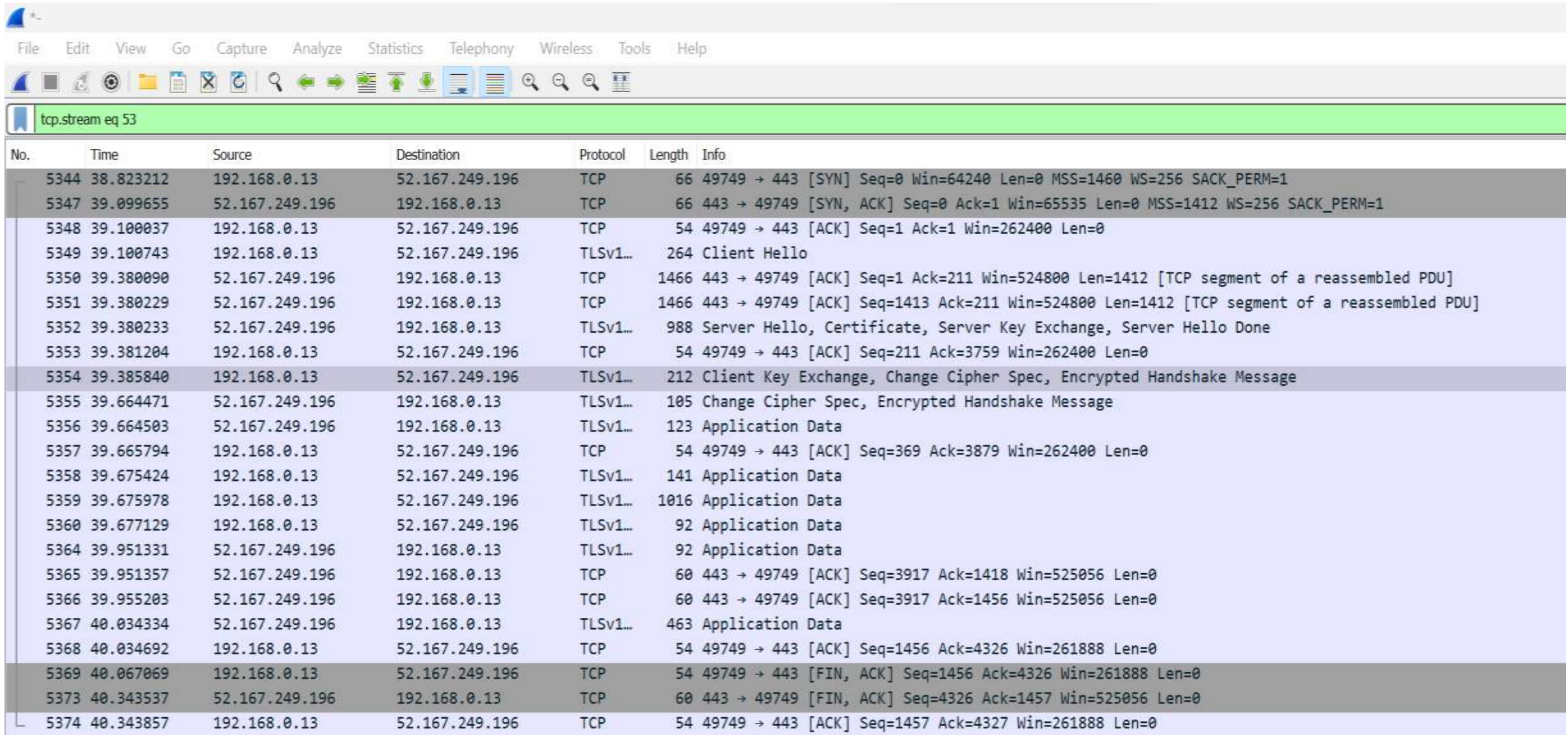
- Generally, data on the Web was transmitted in plaintext that anyone could read if they intercepted the message. In order to provide a high degree of **privacy**, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
- SSL initiates an **authentication** process called a **handshake** between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

SSL/TLS Handshake

- 1.The client sends a "**client hello**" message. This includes the client's SSL version number, cipher settings, session-specific data and other information that the server needs to communicate with the client using SSL.
- 2.The server responds with a "**server hello**" message. This includes the server's SSL version number, cipher settings, session-specific data, an SSL certificate with a public key and other information that the client needs to communicate with the server over SSL.
- 3.The client verifies the server's SSL certificate from list of Root **CA** (Certificate Authority) stored in its browser and authenticates the server. If the authentication fails, then the client refuses the connection and throws an exception. If the authentication succeeds, then proceed to step 4.
- 4.The client creates a **session key**, encrypts it with the server's public key and sends it to the server. If the server has requested client authentication (mostly in server to server communication), then the client sends his own certificate to the server.
- 5.The server decrypts the session key with its private key and sends the acknowledgement to the client encrypted with the session key.



SSL/TLS Wireshark capture



tcp.stream eq 53

No.	Time	Source	Destination	Protocol	Length	Info
5344	38.823212	192.168.0.13	52.167.249.196	TCP	66	49749 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5347	39.099655	52.167.249.196	192.168.0.13	TCP	66	443 → 49749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM=1
5348	39.100037	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0
5349	39.100743	192.168.0.13	52.167.249.196	TLSv1...	264	Client Hello
5350	39.380090	52.167.249.196	192.168.0.13	TCP	1466	443 → 49749 [ACK] Seq=1 Ack=211 Win=524800 Len=1412 [TCP segment of a reassembled PDU]
5351	39.380229	52.167.249.196	192.168.0.13	TCP	1466	443 → 49749 [ACK] Seq=1413 Ack=211 Win=524800 Len=1412 [TCP segment of a reassembled PDU]
5352	39.380233	52.167.249.196	192.168.0.13	TLSv1...	988	Server Hello, Certificate, Server Key Exchange, Server Hello Done
5353	39.381204	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=211 Ack=3759 Win=262400 Len=0
5354	39.385840	192.168.0.13	52.167.249.196	TLSv1...	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5355	39.664471	52.167.249.196	192.168.0.13	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
5356	39.664503	52.167.249.196	192.168.0.13	TLSv1...	123	Application Data
5357	39.665794	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=369 Ack=3879 Win=262400 Len=0
5358	39.675424	192.168.0.13	52.167.249.196	TLSv1...	141	Application Data
5359	39.675978	192.168.0.13	52.167.249.196	TLSv1...	1016	Application Data
5360	39.677129	192.168.0.13	52.167.249.196	TLSv1...	92	Application Data
5364	39.951331	52.167.249.196	192.168.0.13	TLSv1...	92	Application Data
5365	39.951357	52.167.249.196	192.168.0.13	TCP	60	443 → 49749 [ACK] Seq=3917 Ack=1418 Win=525056 Len=0
5366	39.952203	52.167.249.196	192.168.0.13	TCP	60	443 → 49749 [ACK] Seq=3917 Ack=1456 Win=525056 Len=0
5367	40.034334	52.167.249.196	192.168.0.13	TLSv1...	463	Application Data
5368	40.034692	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=1456 Ack=4326 Win=261888 Len=0
5369	40.067069	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [FIN, ACK] Seq=1456 Ack=4326 Win=261888 Len=0
5373	40.343537	52.167.249.196	192.168.0.13	TCP	60	443 → 49749 [FIN, ACK] Seq=4326 Ack=1457 Win=525056 Len=0
5374	40.343857	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=1457 Ack=4327 Win=261888 Len=0

Client Hello Message

The image shows a Wireshark packet capture of a TLS Client Hello message. The packet list at the top shows four packets. The fourth packet, number 5349, is a TLSv1.2 Client Hello from 192.168.0.13 to 52.167.249.196. This packet is highlighted with a red box. Below the packet list, the packet details pane shows the structure of the Client Hello message. The 'Version' field is highlighted with a red box, showing 'TLS 1.2 (0x0303)'. The 'Cipher Suites' field is also highlighted with a red box, showing a list of 19 cipher suites. The packet bytes pane shows the raw data of the message.

No.	Time	Source	Destination	Protocol	Length	Info
5344	38.823212	192.168.0.13	52.167.249.196	TCP	66	49749 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5347	39.099655	52.167.249.196	192.168.0.13	TCP	66	443 → 49749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM=1
5348	39.100037	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0
5349	39.100743	192.168.0.13	52.167.249.196	TLSv1...	264	Client Hello

> Frame 5349: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits) on interface 0
> Ethernet II, Src: 50:00:00:05:00:00 (50:00:00:05:00:00), Dst: Cambridg_ca:d6:60 (5c:1a:6f:ca:d6:60)
> Internet Protocol Version 4, Src: 192.168.0.13, Dst: 52.167.249.196
> Transmission Control Protocol, Src Port: 49749, Dst Port: 443, Seq: 1, Ack: 1, Len: 210
✓ Transport Layer Security
 ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 205
 ✓ Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 201
 Version: TLS 1.2 (0x0303)
 > Random: 64ce7fa8b0e2b7c68cf44fb911e5d5608c49f7fdcf497e57...
 Session ID Length: 0
 Cipher Suites Length: 38
 ✓ Cipher Suites (19 suites)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
 Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
 Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
 Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
 Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
 Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Server Hello message

The image shows a Wireshark packet capture of a TLS handshake. The packet list at the top shows four packets. Packet 5352, at time 39.380233, is a TLSv1.2 message from 52.167.249.196 to 192.168.0.13, containing a Server Hello, Certificate, Server Key Exchange, and Server Hello Done. The packet details pane below shows the structure of this message. The 'Handshake Protocol: Server Hello' section is expanded, showing fields like Handshake Type, Length, Version, Random, Session ID, Cipher Suite, and Extensions. The 'Handshake Protocol: Certificate' section is also expanded, showing the Certificate field, which contains a signedCertificate. The signedCertificate is further expanded, showing fields like version, serialNumber, signature, issuer, validity, subject, subjectPublicKeyInfo, and subjectPublicKey. The subjectPublicKeyInfo is expanded, showing the algorithm (rsaEncryption) and the subjectPublicKey (3082010a0282010100a904afebad704ab7bca1997e2cf319...). The subjectPublicKey is highlighted with a red box.

tcp.stream eq 53

No.	Time	Source	Destination	Protocol	Length	Info
5349	39.100743	192.168.0.13	52.167.249.196	TLSv1...	264	Client Hello
5350	39.380090	52.167.249.196	192.168.0.13	TCP	1466	443 → 49749 [ACK] Seq=1 Ack=211 Win=524800 Len=1412 [TCP segment of a reassembled PDU]
5351	39.380229	52.167.249.196	192.168.0.13	TCP	1466	443 → 49749 [ACK] Seq=1413 Ack=211 Win=524800 Len=1412 [TCP segment of a reassembled PDU]
5352	39.380233	52.167.249.196	192.168.0.13	TLSv1...	988	Server Hello, Certificate, Server Key Exchange, Server Hello Done

Length: 3753

- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 94
 - Version: TLS 1.2 (0x0303)
 - Random: 64ce1d39c11c0cf0e793434c1bf5b3af508af6a55f196d0b...
 - Session ID Length: 32
 - Session ID: fe4c0000bae5a0177ce7edaf4dc96b0cca6d19f3d466f85
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Compression Method: null (0)
 - Extensions Length: 22
 - Extension: application_layer_protocol_negotiation (len=5)
 - Extension: extended_master_secret (len=0)
 - Extension: renegotiation_info (len=1)
 - Extension: server_name (len=0)
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 3282
 - Certificates Length: 3279
- Certificates (3279 bytes)
 - Certificate Length: 1517
 - Certificate: 308205e9308203d1a003020102021333000001e21fef346d... (id-at-commonName=settings-win.data.microsoft.com,id-at-organizationalUnitName=WSE,id-at-organizationName=Microsoft,id-at-localityName=Redmond,id-at-stat...

signedCertificate

- version: v3 (2)
- serialNumber: 0x33000001e21fef346d38b5fb580000000001e2
- signature (sha256WithRSAEncryption)
- issuer: rdnSequence (0)
- validity
- subject: rdnSequence (0)
- subjectPublicKeyInfo
 - algorithm (rsaEncryption)
 - subjectPublicKey: 3082010a0282010100a904afebad704ab7bca1997e2cf319...

modulus: 0x00a904afebad704ab7bca1997e2cf3193403b04628fff384...

publicExponent: 65537

Client Key Exchange

tcp.stream eq 53

No.	Time	Source	Destination	Protocol	Length	Info
5351	39.380229	52.167.249.196	192.168.0.13	TCP	1466	443 → 49749 [ACK] Seq=1413 Ack=211 Win=524800 Len=1412 [TCP segment of a reassembled PDU]
5352	39.380233	52.167.249.196	192.168.0.13	TLSv1...	988	Server Hello, Certificate, Server Key Exchange, Server Hello Done
5353	39.381204	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=211 Ack=3759 Win=262400 Len=0
5354	39.385840	192.168.0.13	52.167.249.196	TLSv1...	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5355	39.664471	52.167.249.196	192.168.0.13	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
5356	39.664503	52.167.249.196	192.168.0.13	TLSv1...	123	Application Data
5357	39.665794	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=369 Ack=3879 Win=262400 Len=0
5358	39.675424	192.168.0.13	52.167.249.196	TLSv1...	141	Application Data

> Frame 5354: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface 0

> Ethernet II, Src: 50:00:00:05:00:00 (50:00:00:05:00:00), Dst: Cambridg_ca:d6:60 (5c:1a:6f:ca:d6:60)

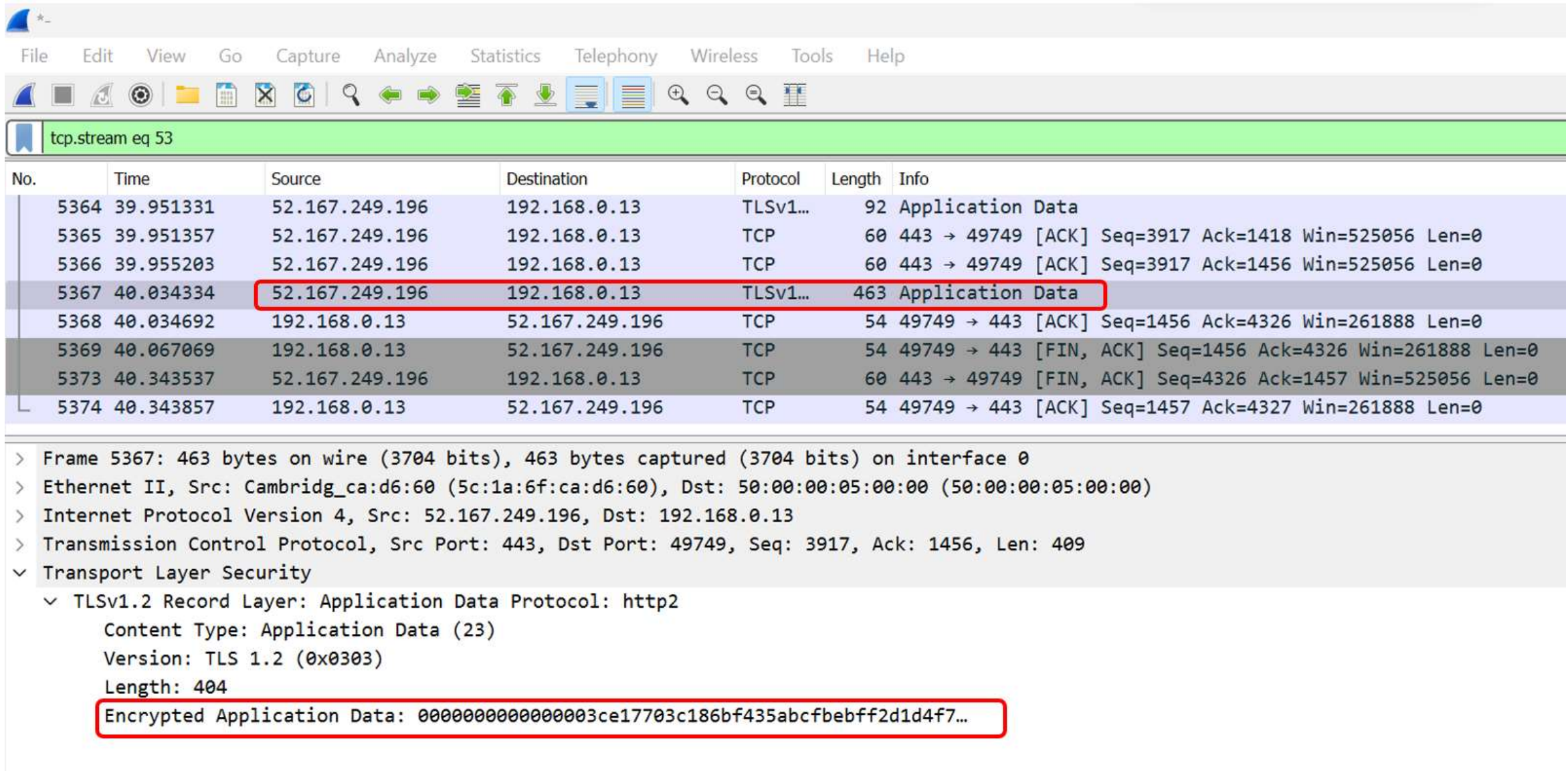
> Internet Protocol Version 4, Src: 192.168.0.13, Dst: 52.167.249.196

> Transmission Control Protocol, Src Port: 49749, Dst Port: 443, Seq: 211, Ack: 3759, Len: 158

▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 102
 - ▼ Handshake Protocol: Client Key Exchange
 - Handshake Type: Client Key Exchange (16)
 - Length: 98
 - ▼ EC Diffie-Hellman Client Params
 - Pubkey Length: 97
 - Pubkey: 0465295128806b681862da9034c3e78b91443087b3941837...
- ▼ 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

Encrypted data transactions:



The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows a list of captured packets. Packet 5367 is highlighted with a red box, showing it is a TLSv1.2 Application Data packet of 463 bytes. The packet details pane shows the structure of the packet, including the TLSv1.2 Record Layer, Application Data Protocol, Content Type, Version, Length, and Encrypted Application Data. The Encrypted Application Data field is also highlighted with a red box, showing a long hexadecimal string.

No.	Time	Source	Destination	Protocol	Length	Info
5364	39.951331	52.167.249.196	192.168.0.13	TLSv1...	92	Application Data
5365	39.951357	52.167.249.196	192.168.0.13	TCP	60	443 → 49749 [ACK] Seq=3917 Ack=1418 Win=525056 Len=0
5366	39.955203	52.167.249.196	192.168.0.13	TCP	60	443 → 49749 [ACK] Seq=3917 Ack=1456 Win=525056 Len=0
5367	40.034334	52.167.249.196	192.168.0.13	TLSv1...	463	Application Data
5368	40.034692	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=1456 Ack=4326 Win=261888 Len=0
5369	40.067069	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [FIN, ACK] Seq=1456 Ack=4326 Win=261888 Len=0
5373	40.343537	52.167.249.196	192.168.0.13	TCP	60	443 → 49749 [FIN, ACK] Seq=4326 Ack=1457 Win=525056 Len=0
5374	40.343857	192.168.0.13	52.167.249.196	TCP	54	49749 → 443 [ACK] Seq=1457 Ack=4327 Win=261888 Len=0

> Frame 5367: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0
> Ethernet II, Src: Cambridg_ca:d6:60 (5c:1a:6f:ca:d6:60), Dst: 50:00:00:05:00:00 (50:00:00:05:00:00)
> Internet Protocol Version 4, Src: 52.167.249.196, Dst: 192.168.0.13
> Transmission Control Protocol, Src Port: 443, Dst Port: 49749, Seq: 3917, Ack: 1456, Len: 409
✓ Transport Layer Security
 ✓ TLSv1.2 Record Layer: Application Data Protocol: http2
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 404
 Encrypted Application Data: 0000000000000003ce17703c186bf435abcfbebf2d1d4f7...