CNSL Assignment 12

Secure Socket Layer

Aim

To study the **SSL protocol** by capturing the packets using **Wireshark** tool while visiting any SSL secure website (banking, e-commerce etc.).

Motivation

With the rise of online banking, e-commerce, and digital communication, protecting sensitive data has become essential. **SSL/TLS protocols** secure internet communication by providing encryption, authentication, and integrity. Studying SSL with Wireshark helps learners visualize how secure connections are established in real time, bridging theory with practical cybersecurity skills.

Learning Outcome

Students will be able to capture and analyze the **SSL handshake process** using Wireshark and understand how SSL ensures secure communication over the internet.

Software and Hardware Requirements Hardware:

- Computer/Laptop with Internet access
- Minimum **4GB RAM**, **20GB free disk space**
- Operating System: **Windows/Linux/Mac**
- **Wireshark** (latest version)
- Web browser (**Chrome/Firefox/Edge**)
- Access to an **SSL secured website** (e.g., https://www.amazon.com or https://www.hdfcbank.com)

Theory

SSL Protocol

SSL (Secure Socket Layer) and its successor **TLS (Transport Layer Security)** are cryptographic protocols designed to provide secure communication over the Internet. SSL works on top of the TCP layer and below the Application layer (HTTP/SMTP/FTP etc.).

It ensures:

- **Authentication** (server/client identity verification)
- **Confidentiality** (data encryption)
- **Integrity** (message integrity using MACs)

SSL Handshake Phases

1. **Client Hello**: Client sends supported cipher suites and a random number.
2. **Server Hello**: Server selects cipher suite, sends certificate and random number.

3. **Key Exchange**: Pre-master secret exchange (RSA/Diffie-Hellman).
4. **Session Key Generation**: Both parties generate session keys.
5. **Finished Messages**: Communication encrypted with symmetric keys begins.

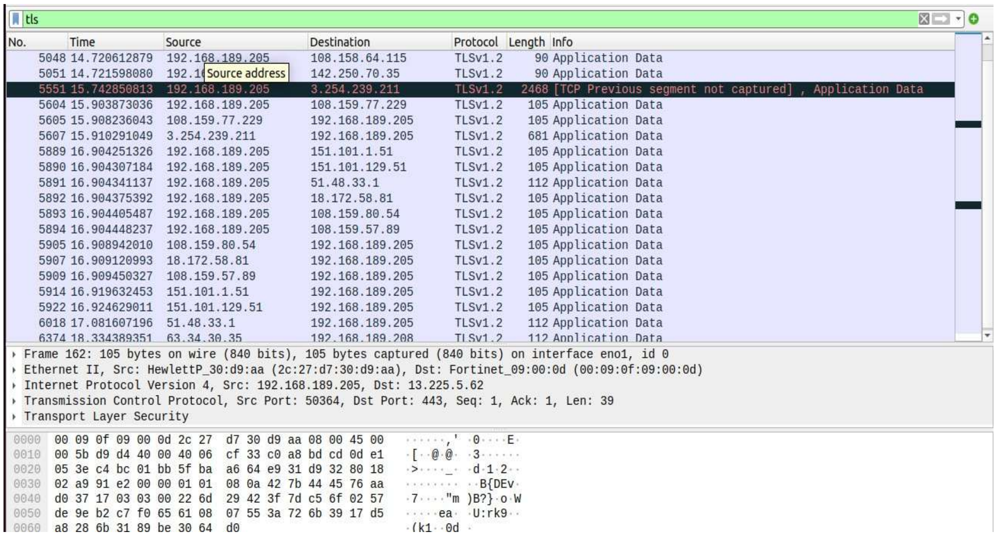
Procedure

1. Open **Wireshark**.
2. Select an active network interface (**Wi-Fi or Ethernet**).
3. In the filter bar, type: ssl || tls (to capture only SSL/TLS packets).
4. Open a web browser and visit any **SSL-secured site** (e.g., https://www.amazon.com).
5. Observe packets being captured in Wireshark.
6. Identify the following packets in the capture:
   - Client Hello
   - Server Hello
   - Certificate
   - Key Exchange
   - Finished messages
7. Stop the capture after sufficient packets are collected.
8. Analyze the details of **SSL handshake messages**.
   - Expand each packet in Wireshark to study fields such as cipher suite, certificates, key exchange, etc.
9. Save the capture for report/reference (**.pcap file**).

Expected Output with Steps

1) To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.)

- Open Wireshark with required interface to capture packets and start capture.
- Open browser and search "amazon.in".
- Login to your account and then log out.
- Close browser and stop the Wireshark capture.

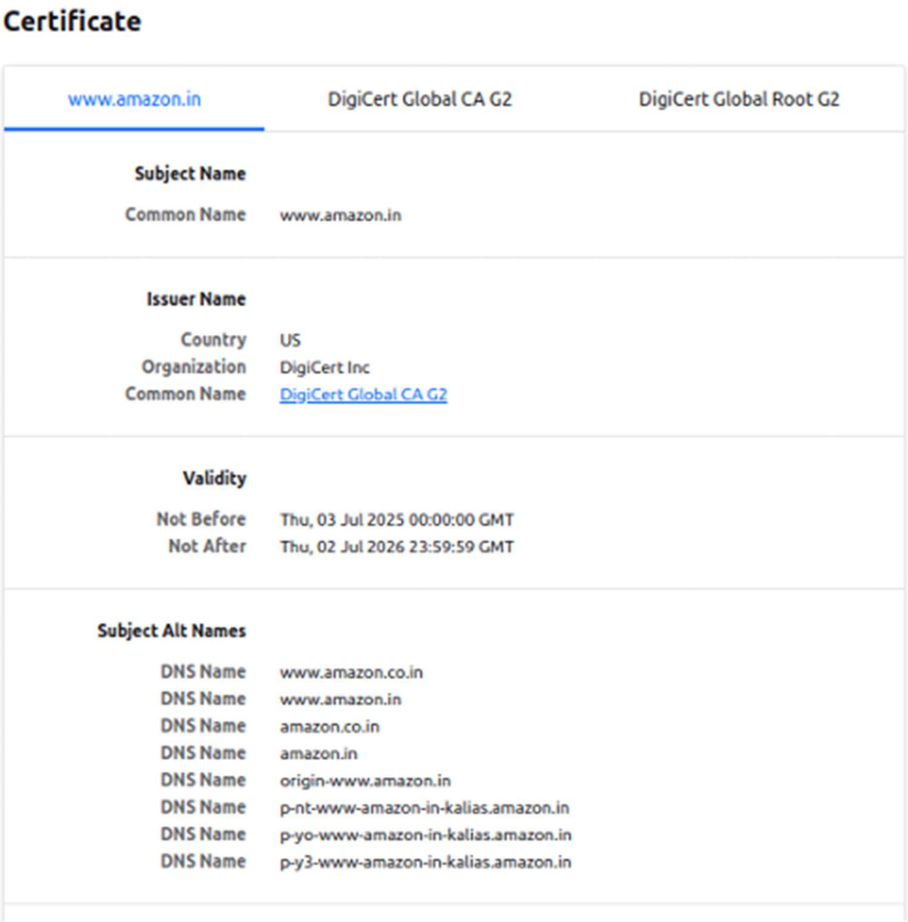


```
tls
No.      Time         Source            Destination       Protocol Length Info
    5048 14.720612879 192.168.189.205   108.158.64.115    TLSv1.2     90 Application Data
    5051 14.721598080 192.1 Source address 142.250.70.35  TLSv1.2     90 Application Data
    5551 15.742850813 192.168.189.205   3.254.239.211     TLSv1.2   2468 [TCP Previous segment not captured] , Application Data
    5604 15.903873036 192.168.189.205   108.159.77.229    TLSv1.2    105 Application Data
    5605 15.908236043 108.159.77.229    192.168.189.205   TLSv1.2    105 Application Data
    5607 15.910291049 3.254.239.211     192.168.189.205   TLSv1.2    681 Application Data
    5889 16.904251326 192.168.189.205   151.101.1.51      TLSv1.2    105 Application Data
    5890 16.904307184 192.168.189.205   151.101.129.51    TLSv1.2    105 Application Data
    5891 16.904341137 192.168.189.205   51.48.33.1        TLSv1.2    112 Application Data
    5892 16.904375392 192.168.189.205   18.172.58.81      TLSv1.2    105 Application Data
    5893 16.904405487 192.168.189.205   108.159.80.54     TLSv1.2    105 Application Data
    5894 16.904448237 192.168.189.205   108.159.57.89     TLSv1.2    105 Application Data
    5905 16.908942010 108.159.80.54     192.168.189.205   TLSv1.2    105 Application Data
    5907 16.909120993 18.172.58.81      192.168.189.205   TLSv1.2    105 Application Data
    5909 16.909450327 108.159.57.89     192.168.189.205   TLSv1.2    105 Application Data
    5914 16.919632453 151.101.1.51      192.168.189.205   TLSv1.2    105 Application Data
    5922 16.924629011 151.101.129.51    192.168.189.205   TLSv1.2    105 Application Data
    6018 17.081607196 51.48.33.1        192.168.189.205   TLSv1.2    112 Application Data
    6374 18.334389351 63.34.30.35       192.168.189.208   TLSv1.2    112 Application Data
› Frame 162: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface eno1, id 0
› Ethernet II, Src: HewlettP_30:d9:aa (2c:27:d7:30:d9:aa), Dst: Fortinet_09:00:0d (00:09:0f:09:00:0d)
› Internet Protocol Version 4, Src: 192.168.189.205, Dst: 13.225.5.62
› Transmission Control Protocol, Src Port: 50364, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
› Transport Layer Security
0000  00 09 0f 09 00 0d 2c 27  d7 30 d9 aa 08 00 45 00   ······,' ·0····E·
0010  00 5b d9 d4 40 00 40 06  cf 33 c0 a8 bd cd 0d e1   ·[··@·@· ·3······
0020  05 3e c4 bc 01 bb 5f ba  a6 64 e9 31 d9 32 80 18   ·>····_· ·d·1·2··
0030  02 a9 91 e2 00 00 01 01  08 0a 42 7b 44 45 76 aa   ········ ··B{DEv·
0040  d0 37 17 03 03 00 22 6d  29 42 3f 7d c5 6f 02 57   ·7····"m )B?}·o·W
0050  de 9e b2 c7 f0 65 61 08  07 55 3a 72 6b 39 17 d5   ·····ea· ·U:rk9··
0060  a8 28 6b 31 89 be 30 64  d0                        ·(k1··0d ·
```

Fig 1: Wireshark packets of Amazon login.

2) SSL Certificate To see the SSL certificate:

- Click on the **lock icon** displayed on the Address bar.
- Click on the "**connection is secure**" option.
- Now click on the "**certificate**" icon to enter the certificate viewer page.



Certificate

www.amazon.in | DigiCert Global CA G2 | DigiCert Global Root G2

Subject Name

Common Name www.amazon.in

Issuer Name

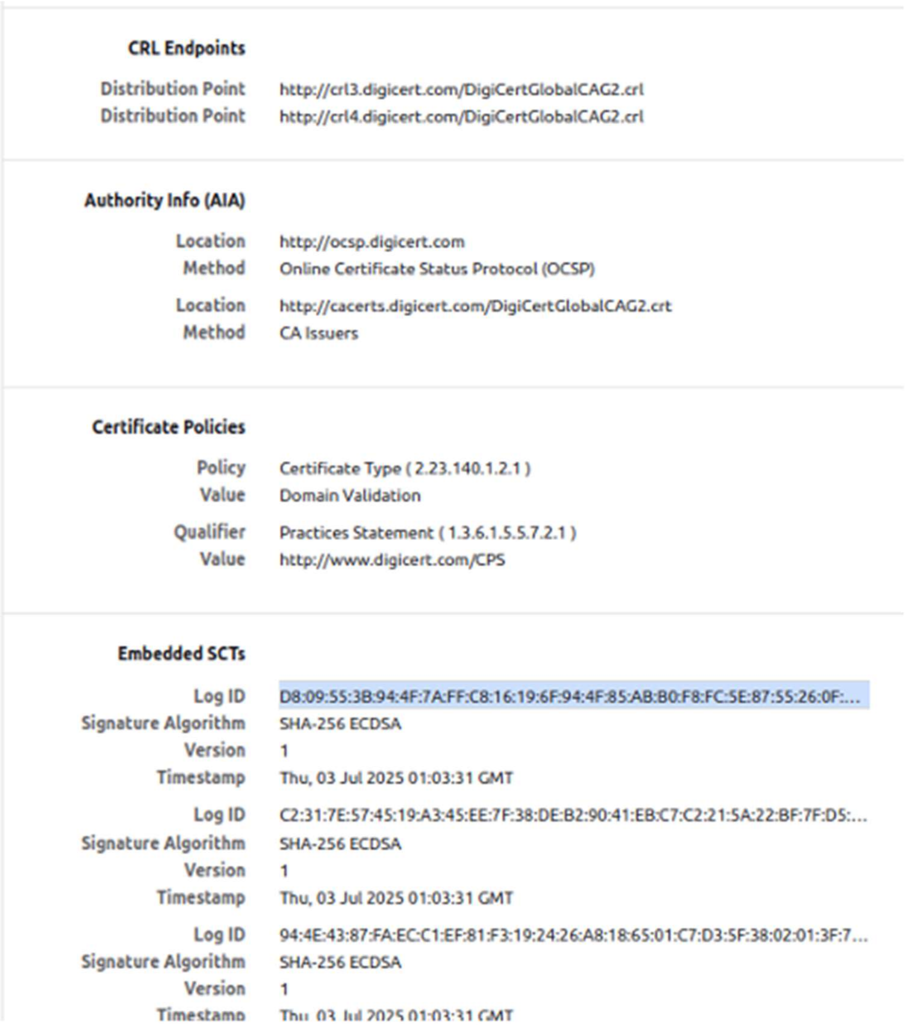
Country US
Organization DigiCert Inc
Common Name DigiCert Global CA G2

Validity

Not Before Thu, 03 Jul 2025 00:00:00 GMT
Not After Thu, 02 Jul 2026 23:59:59 GMT

Subject Alt Names

DNS Name www.amazon.co.in
DNS Name www.amazon.in
DNS Name amazon.co.in
DNS Name amazon.in
DNS Name origin-www.amazon.in
DNS Name p-nt-www-amazon-in-kalias.amazon.in
DNS Name p-yo-www-amazon-in-kalias.amazon.in
DNS Name p-y3-www-amazon-in-kalias.amazon.in



CRL Endpoints

Distribution Point	http://crl3.digicert.com/DigiCertGlobalCAG2.crl
Distribution Point	http://crl4.digicert.com/DigiCertGlobalCAG2.crl

Authority Info (AIA)

Location	http://ocsp.digicert.com
Method	Online Certificate Status Protocol (OCSP)
Location	http://cacerts.digicert.com/DigiCertGlobalCAG2.crt
Method	CA Issuers

Certificate Policies

Policy	Certificate Type (2.23.140.1.2.1)
Value	Domain Validation
Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	http://www.digicert.com/CPS

Embedded SCTs

Log ID	D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:B0:F8:FC:5E:87:55:26:0F:...
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Thu, 03 Jul 2025 01:03:31 GMT
Log ID	C2:31:7E:57:45:19:A3:45:EE:7F:38:DE:B2:90:41:EB:C7:C2:21:5A:22:BF:7F:D5:...
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Thu, 03 Jul 2025 01:03:31 GMT
Log ID	94:4E:43:87:FA:EC:C1:EF:81:F3:19:24:26:A8:18:65:01:C7:D3:5F:38:02:01:3F:7...
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Thu, 03 Jul 2025 01:03:31 GMT

Fig 2: SSL certificate of Amazon.

3) Web page showing secure connection (padlock) The padlock icon means that the website has an **SSL/TLS certificate**, which encrypts the data being transmitted between your browser and the server.

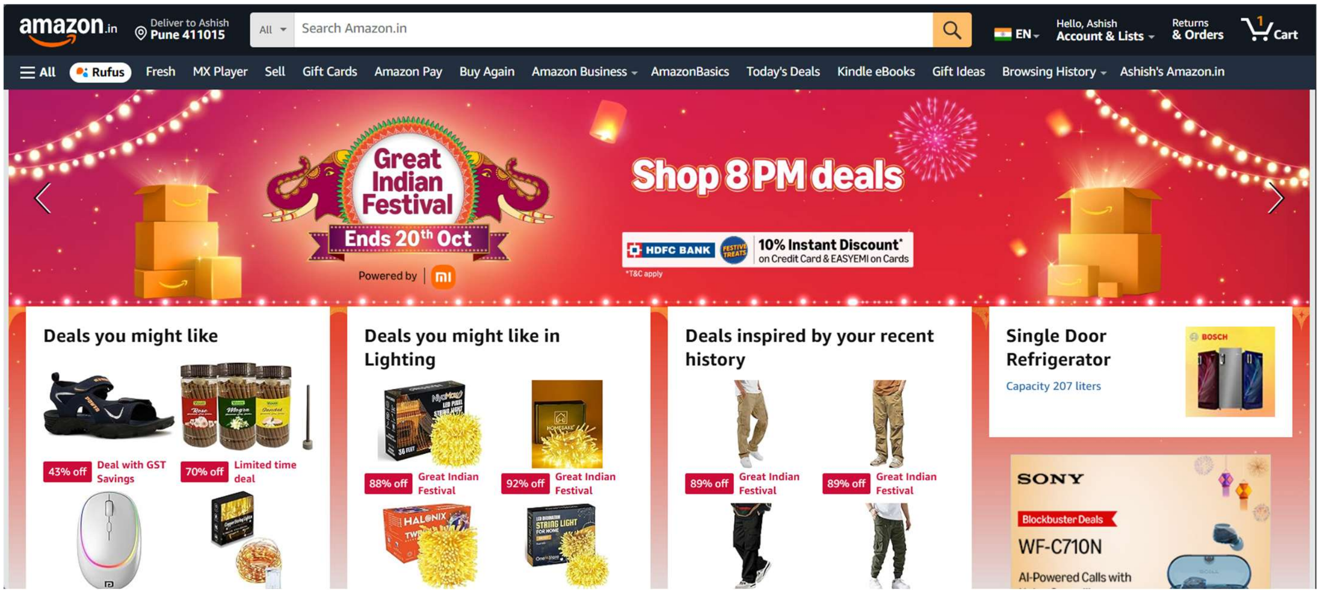
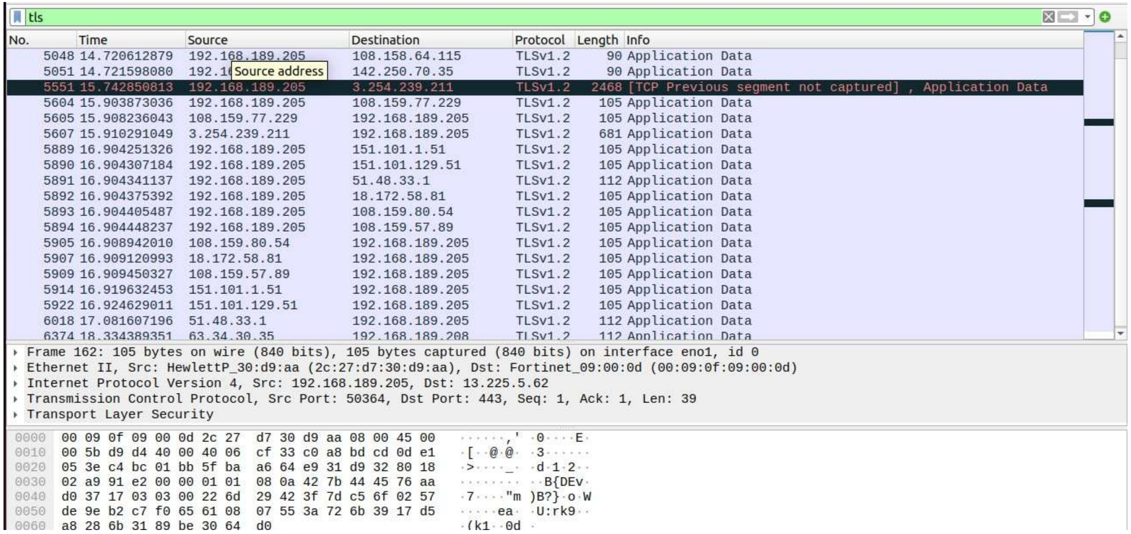


Fig 3: Amazon webpage.

4) Packets description

- Right click on the "**Client Hello**" packet → Follow → **TLS stream**.
- This will automatically prepopulate the display filter with the required filter.
- Now add **SSL condition** in that prepopulated filter and press "Enter". Now see the descriptions of the various data packets of the SSL stream. Our login credentials will be shown in the "**Application data**" packet and will be in **encrypted format**.



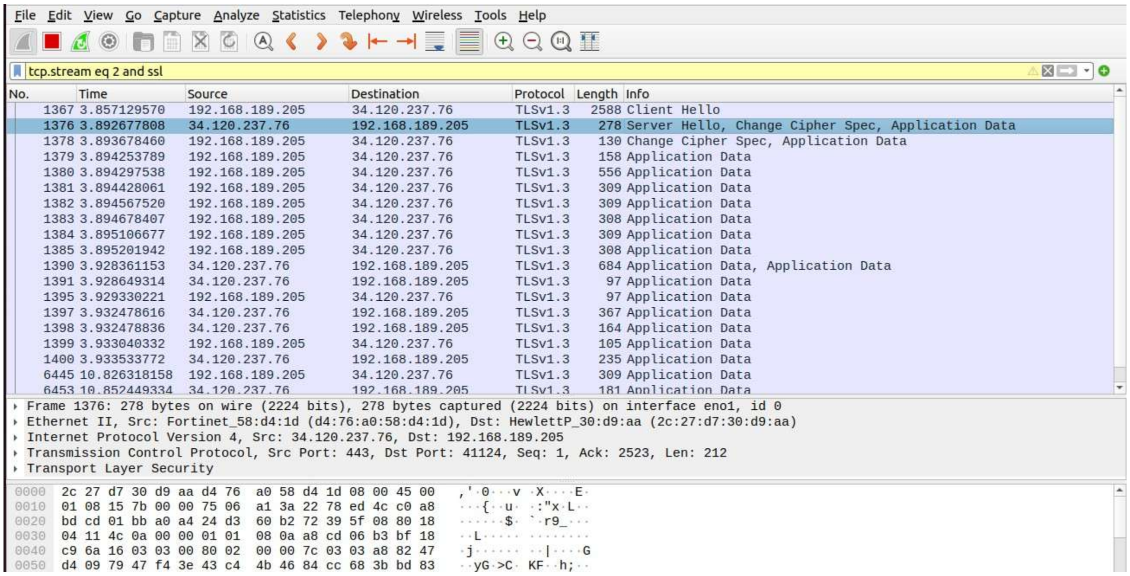
```
tls

No.       Time          Source           Destination      Protocol  Length Info
     5048 14.720612879  192.168.189.205  108.158.64.115   TLSv1.2     90 Application Data
     5051 14.721598080  192.1            142.250.70.35    TLSv1.2     90 Application Data
     5551 15.742850813  192.168.189.205  3.254.239.211    TLSv1.2   2468 [TCP Previous segment not captured] , Application Data
     5604 15.903873036  192.168.189.205  108.159.77.229   TLSv1.2    105 Application Data
     5605 15.908236043  108.159.77.229   192.168.189.205  TLSv1.2    105 Application Data
     5607 15.910291049  3.254.239.211    192.168.189.205  TLSv1.2    681 Application Data
     5889 16.904251326  192.168.189.205  151.101.1.51     TLSv1.2    105 Application Data
     5890 16.904307184  192.168.189.205  151.101.129.51   TLSv1.2    105 Application Data
     5891 16.904341137  192.168.189.205  51.48.33.1       TLSv1.2    112 Application Data
     5892 16.904375392  192.168.189.205  18.172.58.81     TLSv1.2    105 Application Data
     5893 16.904405487  192.168.189.205  108.159.80.54    TLSv1.2    105 Application Data
     5894 16.904448237  192.168.189.205  108.159.57.89    TLSv1.2    105 Application Data
     5905 16.908942010  108.159.80.54    192.168.189.205  TLSv1.2    105 Application Data
     5907 16.909120993  18.172.58.81     192.168.189.205  TLSv1.2    105 Application Data
     5909 16.909450327  108.159.57.89    192.168.189.205  TLSv1.2    105 Application Data
     5914 16.919632453  151.101.1.51     192.168.189.205  TLSv1.2    105 Application Data
     5922 16.924629011  151.101.129.51   192.168.189.205  TLSv1.2    105 Application Data
     6018 17.081607196  51.48.33.1       192.168.189.205  TLSv1.2    112 Application Data
     6374 18.334389351  63.34.30.35      192.168.189.208  TLSv1.2    112 Application Data

▸ Frame 162: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface eno1, id 0
▸ Ethernet II, Src: HewlettP_30:d9:aa (2c:27:d7:30:d9:aa), Dst: Fortinet_09:00:0d (00:09:0f:09:00:0d)
▸ Internet Protocol Version 4, Src: 192.168.189.205, Dst: 13.225.5.62
▸ Transmission Control Protocol, Src Port: 50364, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
▸ Transport Layer Security

0000  00 09 0f 09 00 0d 2c 27  d7 30 d9 aa 08 00 45 00   ······,' ·0····E·
0010  00 5b d9 d4 40 00 40 06  cf 33 c0 a8 bd cd 0d e1   ·[··@·@· ·3······
0020  05 3e c4 bc 01 bb 5f ba  a6 64 e9 31 d9 32 80 18   ·>····_· ·d·1·2··
0030  02 a9 91 e2 00 00 01 01  08 0a 42 7b 44 45 76 aa   ········ ··B{DEv·
0040  d0 37 17 03 03 00 22 6d  29 42 3f 7d c5 6f 02 57   ·7····"m )B?}·o·W
0050  de 9e b2 c7 f0 65 61 08  07 55 3a 72 6b 39 17 d5   ·····ea· ·U:rk9··
0060  a8 28 6b 31 89 be 30 64  d0                        ·(k1··0d ·
```

Fig 4: Client hello packet description.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

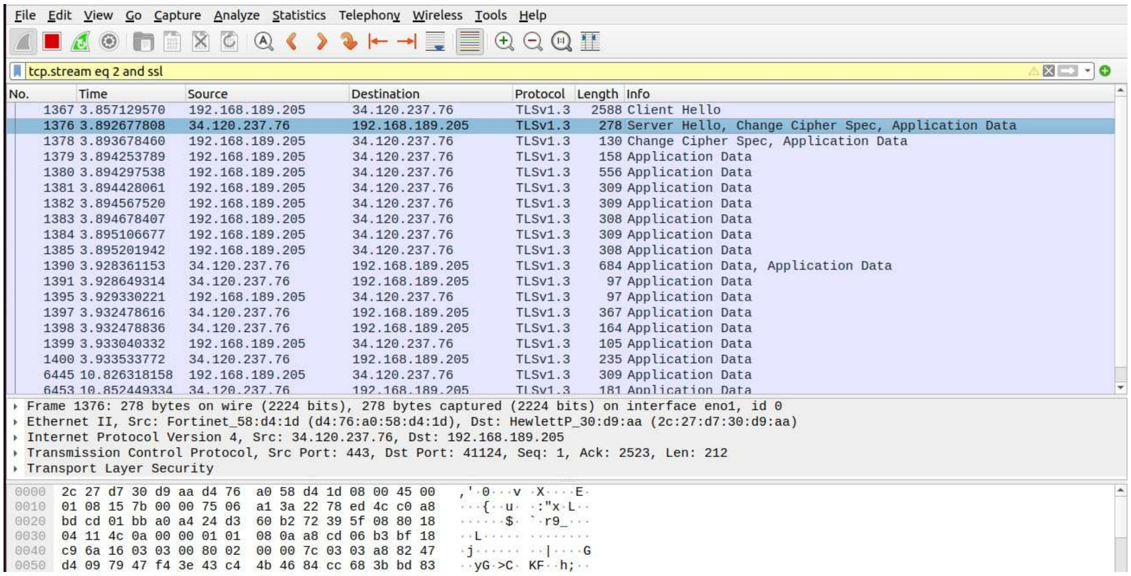
```
tcp.stream eq 2 and ssl

No.       Time          Source           Destination      Protocol  Length Info
     1367 3.857129570   192.168.189.205  34.120.237.76    TLSv1.3   2588 Client Hello
     1376 3.892677808   34.120.237.76    192.168.189.205  TLSv1.3    278 Server Hello, Change Cipher Spec, Application Data
     1378 3.893678460   192.168.189.205  34.120.237.76    TLSv1.3    130 Change Cipher Spec, Application Data
     1379 3.894253789   192.168.189.205  34.120.237.76    TLSv1.3    158 Application Data
     1380 3.894297538   192.168.189.205  34.120.237.76    TLSv1.3    556 Application Data
     1381 3.894428061   192.168.189.205  34.120.237.76    TLSv1.3    309 Application Data
     1382 3.894567520   192.168.189.205  34.120.237.76    TLSv1.3    309 Application Data
     1383 3.894678407   192.168.189.205  34.120.237.76    TLSv1.3    308 Application Data
     1384 3.895106677   192.168.189.205  34.120.237.76    TLSv1.3    309 Application Data
     1385 3.895201942   192.168.189.205  34.120.237.76    TLSv1.3    308 Application Data
     1390 3.928361153   34.120.237.76    192.168.189.205  TLSv1.3    684 Application Data, Application Data
     1391 3.928649314   34.120.237.76    192.168.189.205  TLSv1.3     97 Application Data
     1395 3.929330221   192.168.189.205  34.120.237.76    TLSv1.3     97 Application Data
     1397 3.932478616   34.120.237.76    192.168.189.205  TLSv1.3    367 Application Data
     1398 3.932478836   34.120.237.76    192.168.189.205  TLSv1.3    164 Application Data
     1399 3.933040332   192.168.189.205  34.120.237.76    TLSv1.3    105 Application Data
     1400 3.933533772   34.120.237.76    192.168.189.205  TLSv1.3    235 Application Data
     6445 10.826318158  192.168.189.205  34.120.237.76    TLSv1.3    309 Application Data
     6453 10.852449334  34.120.237.76    192.168.189.205  TLSv1.3    181 Application Data

▸ Frame 1376: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface eno1, id 0
▸ Ethernet II, Src: Fortinet_58:d4:1d (d4:76:a0:58:d4:1d), Dst: HewlettP_30:d9:aa (2c:27:d7:30:d9:aa)
▸ Internet Protocol Version 4, Src: 34.120.237.76, Dst: 192.168.189.205
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 41124, Seq: 1, Ack: 2523, Len: 212
▸ Transport Layer Security

0000  2c 27 d7 30 d9 aa d4 76  a0 58 d4 1d 08 00 45 00   ,'·0···v ·X····E·
0010  01 08 15 7b 00 00 75 06  a1 3a 22 78 ed 4c c0 a8   ···{··u· ·:"x·L··
0020  bd cd 01 bb a0 a4 24 d3  60 b2 72 39 5f 08 80 18   ······$· `·r9_···
0030  04 11 4c 0a 00 00 01 01  08 0a a8 cd 06 b3 bf 18   ··L····· ········
0040  c9 6a 16 03 03 00 80 02  00 00 7c 03 03 a8 82 47   ·j······ ··|····G
0050  d4 09 79 47 f4 3e 43 c4  4b 46 84 cc 68 3b bd 83   ··yG·>C· KF··h;··
```

Fig 5: Server hello packet description.

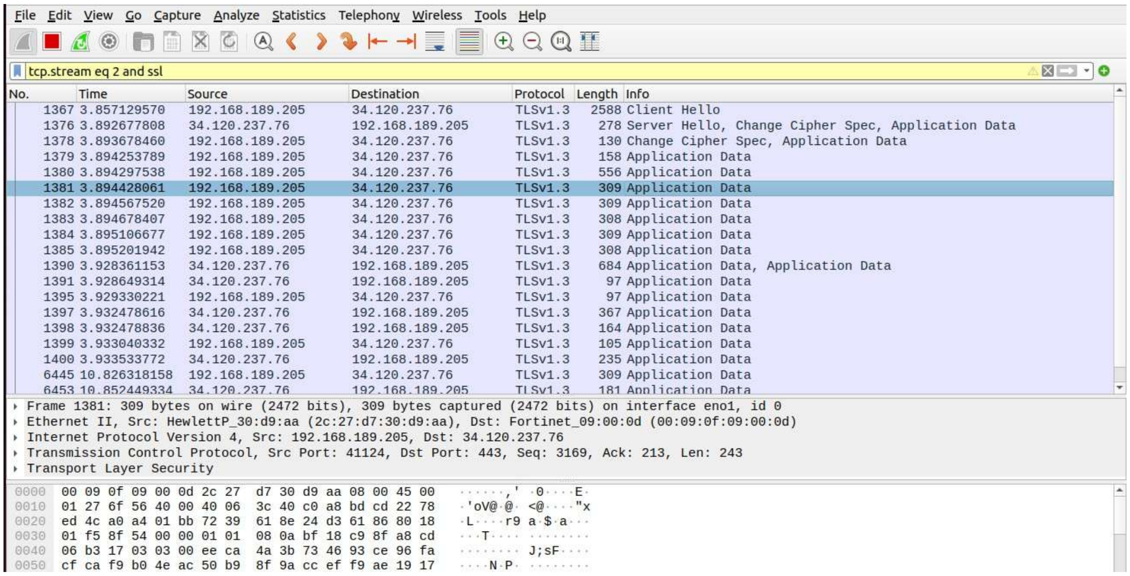

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2 and ssl

```
No.     Time          Source            Destination       Protocol Length Info
   1367 3.857129570   192.168.189.205   34.120.237.76     TLSv1.3   2588 Client Hello
   1376 3.892677808   34.120.237.76     192.168.189.205   TLSv1.3    278 Server Hello, Change Cipher Spec, Application Data
   1378 3.893678460   192.168.189.205   34.120.237.76     TLSv1.3    130 Change Cipher Spec, Application Data
   1379 3.894253789   192.168.189.205   34.120.237.76     TLSv1.3    158 Application Data
   1380 3.894297538   192.168.189.205   34.120.237.76     TLSv1.3    556 Application Data
   1381 3.894428061   192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   1382 3.894567520   192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   1383 3.894678407   192.168.189.205   34.120.237.76     TLSv1.3    308 Application Data
   1384 3.895106677   192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   1385 3.895201942   192.168.189.205   34.120.237.76     TLSv1.3    308 Application Data
   1390 3.928361153   34.120.237.76     192.168.189.205   TLSv1.3    684 Application Data, Application Data
   1391 3.928649314   34.120.237.76     192.168.189.205   TLSv1.3     97 Application Data
   1395 3.929330221   192.168.189.205   34.120.237.76     TLSv1.3     97 Application Data
   1397 3.932478616   34.120.237.76     192.168.189.205   TLSv1.3    367 Application Data
   1398 3.932478836   34.120.237.76     192.168.189.205   TLSv1.3    164 Application Data
   1399 3.933040332   192.168.189.205   34.120.237.76     TLSv1.3    105 Application Data
   1400 3.933533772   34.120.237.76     192.168.189.205   TLSv1.3    235 Application Data
   6445 10.826318158  192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   6453 10.852449334  34.120.237.76     192.168.189.205   TLSv1.3    181 Application Data
```

```
› Frame 1376: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface eno1, id 0
› Ethernet II, Src: Fortinet_58:d4:1d (d4:76:a0:58:d4:1d), Dst: HewlettP_30:d9:aa (2c:27:d7:30:d9:aa)
› Internet Protocol Version 4, Src: 34.120.237.76, Dst: 192.168.189.205
› Transmission Control Protocol, Src Port: 443, Dst Port: 41124, Seq: 1, Ack: 2523, Len: 212
› Transport Layer Security
```

```
0000  2c 27 d7 30 d9 aa d4 76  a0 58 d4 1d 08 00 45 00   ,'·0···v ·X····E·
0010  01 08 15 7b 00 00 75 06  a1 3a 22 78 ed 4c c0 a8   ···{··u· ·:"x·L··
0020  bd cd 01 bb a0 a4 24 d3  60 b2 72 39 5f 08 80 18   ······$· `·r9_···
0030  04 11 4c 0a 00 00 01 01  08 0a a8 cd 06 b3 bf 18   ··L····· ········
0040  c9 6a 16 03 03 00 80 02  00 00 7c 03 03 a8 82 47   ·j······ ··|····G
0050  d4 09 79 47 f4 3e 43 c4  4b 46 84 cc 68 3b bd 83   ··yG·>C· KF··h;··
```

Fig 6: Cipher sec packet description.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2 and ssl

```
No.     Time          Source            Destination       Protocol Length Info
   1367 3.857129570   192.168.189.205   34.120.237.76     TLSv1.3   2588 Client Hello
   1376 3.892677808   34.120.237.76     192.168.189.205   TLSv1.3    278 Server Hello, Change Cipher Spec, Application Data
   1378 3.893678460   192.168.189.205   34.120.237.76     TLSv1.3    130 Change Cipher Spec, Application Data
   1379 3.894253789   192.168.189.205   34.120.237.76     TLSv1.3    158 Application Data
   1380 3.894297538   192.168.189.205   34.120.237.76     TLSv1.3    556 Application Data
   1381 3.894428061   192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   1382 3.894567520   192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   1383 3.894678407   192.168.189.205   34.120.237.76     TLSv1.3    308 Application Data
   1384 3.895106677   192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   1385 3.895201942   192.168.189.205   34.120.237.76     TLSv1.3    308 Application Data
   1390 3.928361153   34.120.237.76     192.168.189.205   TLSv1.3    684 Application Data, Application Data
   1391 3.928649314   34.120.237.76     192.168.189.205   TLSv1.3     97 Application Data
   1395 3.929330221   192.168.189.205   34.120.237.76     TLSv1.3     97 Application Data
   1397 3.932478616   34.120.237.76     192.168.189.205   TLSv1.3    367 Application Data
   1398 3.932478836   34.120.237.76     192.168.189.205   TLSv1.3    164 Application Data
   1399 3.933040332   192.168.189.205   34.120.237.76     TLSv1.3    105 Application Data
   1400 3.933533772   34.120.237.76     192.168.189.205   TLSv1.3    235 Application Data
   6445 10.826318158  192.168.189.205   34.120.237.76     TLSv1.3    309 Application Data
   6453 10.852449334  34.120.237.76     192.168.189.205   TLSv1.3    181 Application Data
```

```
› Frame 1381: 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits) on interface eno1, id 0
› Ethernet II, Src: HewlettP_30:d9:aa (2c:27:d7:30:d9:aa), Dst: Fortinet_09:00:0d (00:09:0f:09:00:0d)
› Internet Protocol Version 4, Src: 192.168.189.205, Dst: 34.120.237.76
› Transmission Control Protocol, Src Port: 41124, Dst Port: 443, Seq: 3169, Ack: 213, Len: 243
› Transport Layer Security
```

```
0000  00 09 0f 09 00 0d 2c 27  d7 30 d9 aa 08 00 45 00   ······,' ·0····E·
0010  01 27 6f 56 40 00 40 06  3c 40 c0 a8 bd cd 22 78   ·'oV@·@· <@····"x
0020  ed 4c a0 a4 01 bb 72 39  61 8e 24 d3 61 86 80 18   ·L····r9 a·$·a···
0030  01 f5 8f 54 00 00 01 01  08 0a bf 18 c9 8f a8 cd   ···T···· ········
0040  06 b3 17 03 03 00 ee ca  4a 3b 73 46 93 ce 96 fa   ········ J;sF····
0050  cf ca f9 b0 4e ac 50 b9  8f 9a cc ef f9 ae 19 17   ····N·P· ········
```

Fig 7: Application Data packet description.