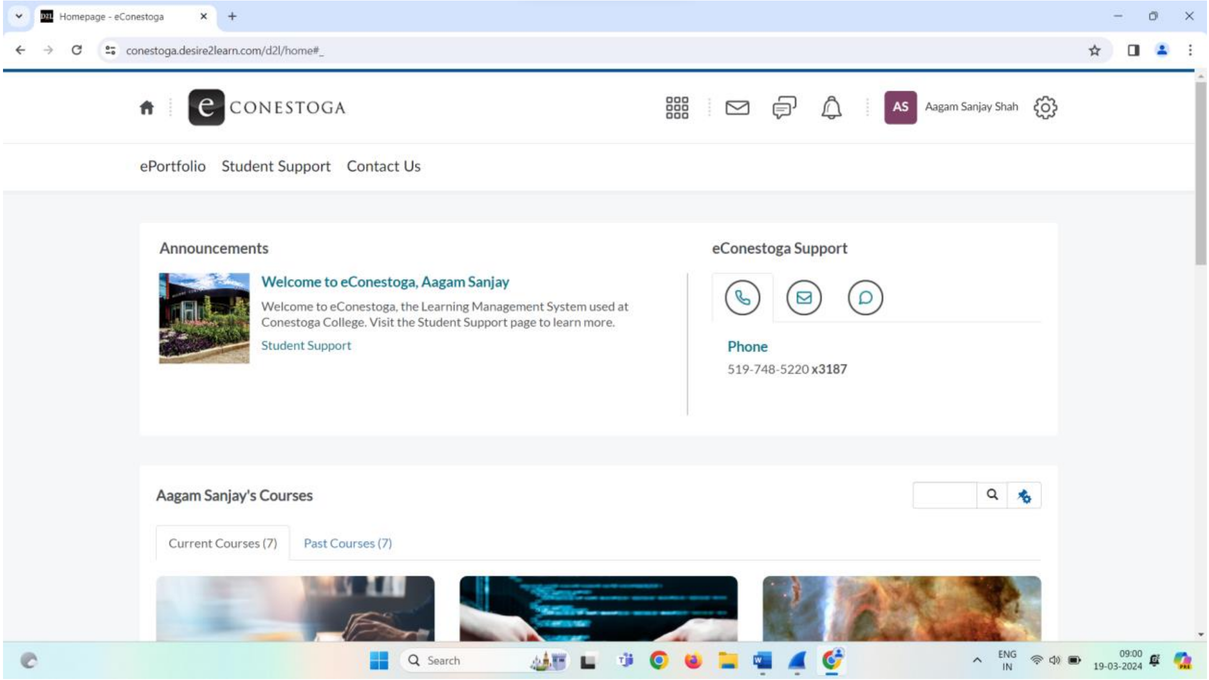
1. Start Wireshark and browse to https://conestoga.desire2learn.com/d2l/home#_ , stop and save capture, name it practicalassignment3
   - Include screenshot of saved capture



Announcements

Welcome to eConestoga, Aagam Sanjay

Welcome to eConestoga, the Learning Management System used at Conestoga College. Visit the Student Support page to learn more.

Student Support

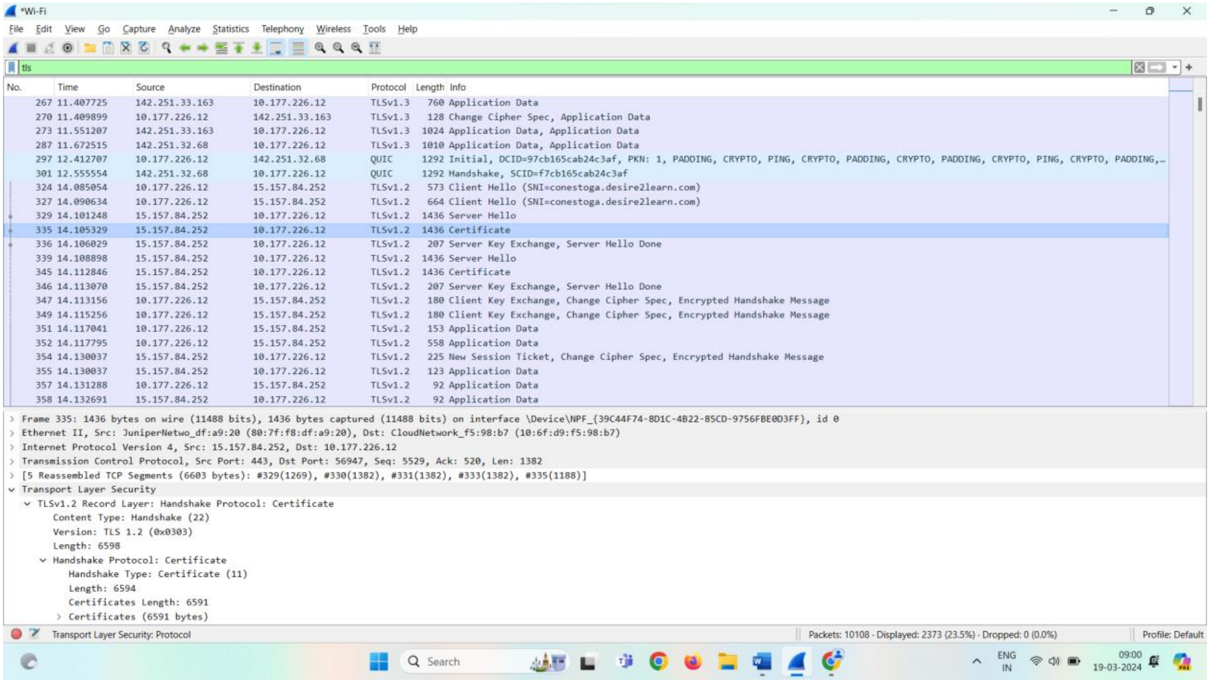
eConestoga Support

Phone

519-748-5220 x3187

Aagam Sanjay's Courses

Current Courses (7) Past Courses (7)

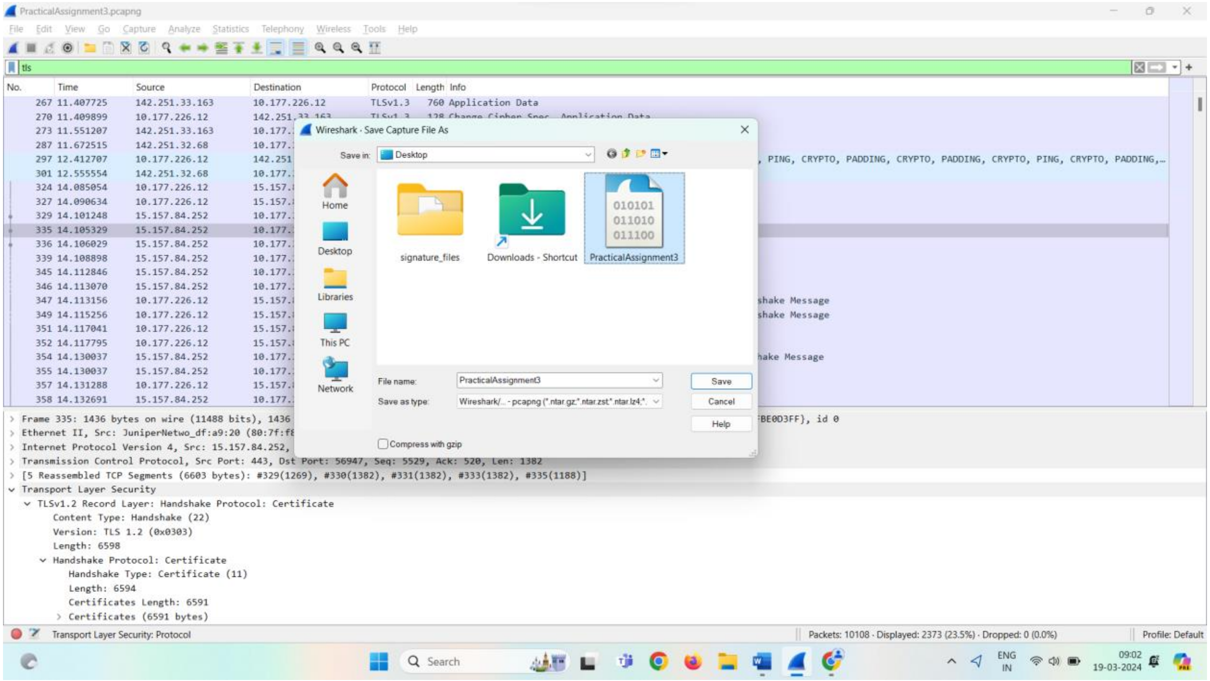


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Search
ENG
IN
09:00
19-03-2024

```
No.   Time        Source          Destination     Protocol Length Info
  267 11.407725   142.251.33.163  10.177.226.12   TLSv1.3   760 Application Data
  270 11.409899   10.177.226.12   142.251.33.163  TLSv1.3   128 Change Cipher Spec, Application Data
  273 11.551207   142.251.33.163  10.177.226.12   TLSv1.3  1024 Application Data, Application Data
  287 11.672515   142.251.32.68   10.177.226.12   TLSv1.3  1010 Application Data, Application Data
  297 12.412707   10.177.226.12   142.251.32.68   QUIC     1292 Initial, DCID=97cb165cab24c3af, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING,…
  301 12.555554   142.251.32.68   10.177.226.12   QUIC     1292 Handshake, SCID=f7cb165cab24c3af
  324 14.085054   10.177.226.12   15.157.84.252   TLSv1.2   573 Client Hello (SNI=conestoga.desire2learn.com)
  327 14.090634   10.177.226.12   15.157.84.252   TLSv1.2   664 Client Hello (SNI=conestoga.desire2learn.com)
  329 14.101248   15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  335 14.105329   15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  336 14.106029   15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  339 14.108898   15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  345 14.112846   15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  346 14.113070   15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  347 14.113156   10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  349 14.115256   10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  351 14.117041   10.177.226.12   15.157.84.252   TLSv1.2   153 Application Data
  352 14.117795   10.177.226.12   15.157.84.252   TLSv1.2   558 Application Data
  354 14.130037   15.157.84.252   10.177.226.12   TLSv1.2   225 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  355 14.130037   15.157.84.252   10.177.226.12   TLSv1.2   123 Application Data
  357 14.131288   10.177.226.12   15.157.84.252   TLSv1.2    92 Application Data
  358 14.132691   15.157.84.252   10.177.226.12   TLSv1.2    92 Application Data
```

```
> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface \Device\NPF_{39C44F74-8D1C-4B22-85CD-9756FBE0D3FF}, id 0
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (10:6f:d9:f5:98:b7)
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      > Certificates (6591 bytes)
```

Transport Layer Security: Protocol | Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%) | Profile: Default



PracticalAssignment3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Wireshark · Save Capture File As
Save in: Desktop
Home
Desktop
Libraries
This PC
Network
signature_files
Downloads - Shortcut
PracticalAssignment3
Save
Cancel
Help

```
No.   Time       Source          Destination    Protocol Length Info
  267 11.407725  142.251.33.163  10.177.226.12  TLSv1.3    760 Application Data
  270 11.409899  10.177.226.12   142.251.33.163 TLSv1.3    128 Change Cipher Spec, Application Data
  273 11.551207  142.251.33.163  10.177.
  287 11.672515  142.251.32.68   10.177.
  297 12.412707  10.177.226.12   142.251                     , PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING,…
  301 12.555554  142.251.32.68   10.177.
  324 14.085054  10.177.226.12   15.157.
  327 14.090634  10.177.226.12   15.157.
  329 14.101248  15.157.84.252   10.177.
  335 14.105329  15.157.84.252   10.177.
  336 14.106029  15.157.84.252   10.177.
  339 14.108898  15.157.84.252   10.177.
  345 14.112846  15.157.84.252   10.177.
  346 14.113070  15.157.84.252   10.177.
  347 14.113156  10.177.226.12   15.157.                     shake Message
  349 14.115256  10.177.226.12   15.157.                     shake Message
  351 14.117041  10.177.226.12   15.157.
  352 14.117795  10.177.226.12   15.157.
  354 14.130037  15.157.84.252   10.177.                     hake Message
  355 14.130037  15.157.84.252   10.177.
  357 14.131288  10.177.226.12   15.157.
  358 14.132691  15.157.84.252   10.177.

> Frame 335: 1436 bytes on wire (11488 bits), 1436                FBE0D3FF}, id 0
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8
> Internet Protocol Version 4, Src: 15.157.84.252,
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      > Certificates (6591 bytes)
```

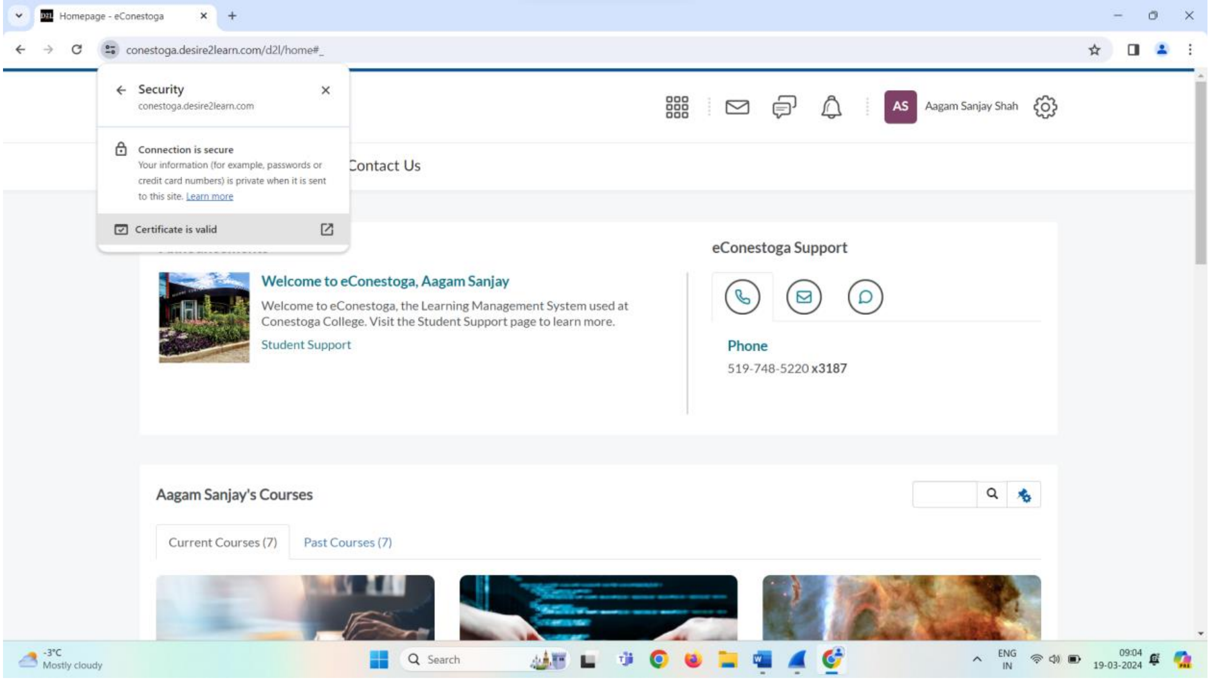
File name: PracticalAssignment3

Save as type: Wireshark/... - pcapng (*.ntar.gz;*.ntar.zst;*.ntar.lz4;*.

□ Compress with gzip

Transport Layer Security: Protocol | Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%) | Profile: Default

2. Identify the certificate used by the website and locate who it was issued to
   - Include screenshot showing the website certificate on the tab that shows who the certificate was issued to



Security
conestoga.desire2learn.com

Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

eConestoga Support

Welcome to eConestoga, Aagam Sanjay

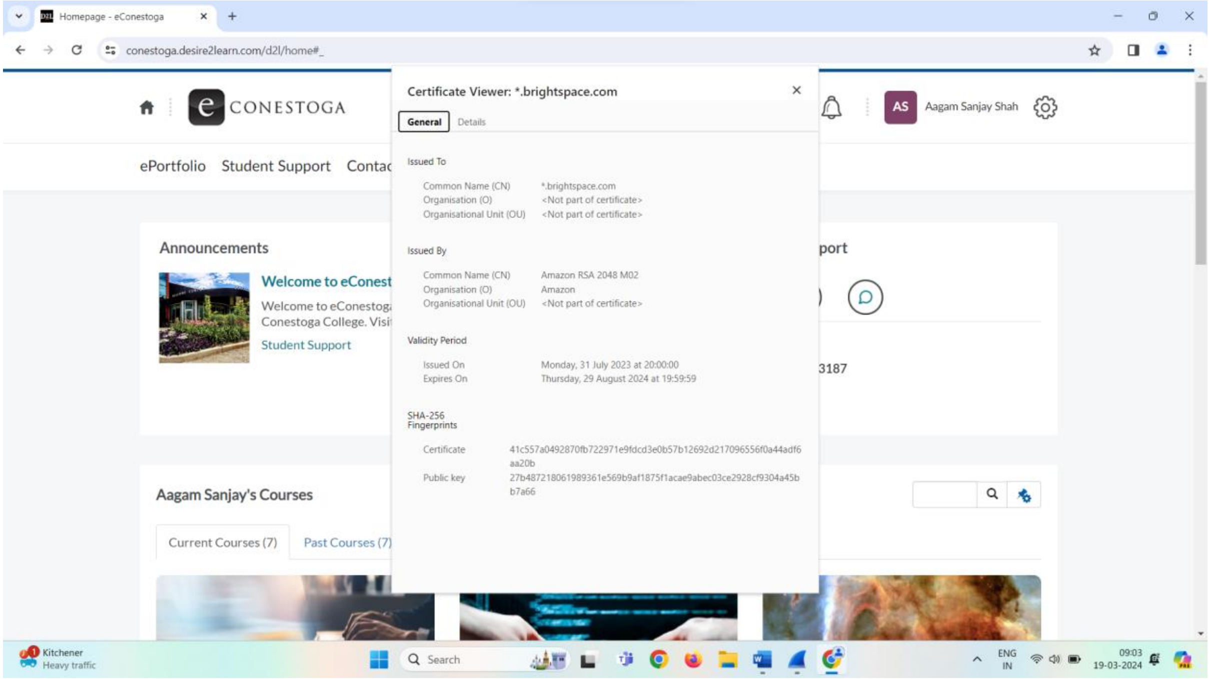
Welcome to eConestoga, the Learning Management System used at Conestoga College. Visit the Student Support page to learn more.

Student Support

Phone
519-748-5220 x3187

Aagam Sanjay's Courses

Current Courses (7) Past Courses (7)



Certificate Viewer: *.brightspace.com

General | Details

Issued To

Common Name (CN)	*.brightspace.com
Organisation (O)	<Not part of certificate>
Organisational Unit (OU)	<Not part of certificate>

Issued By

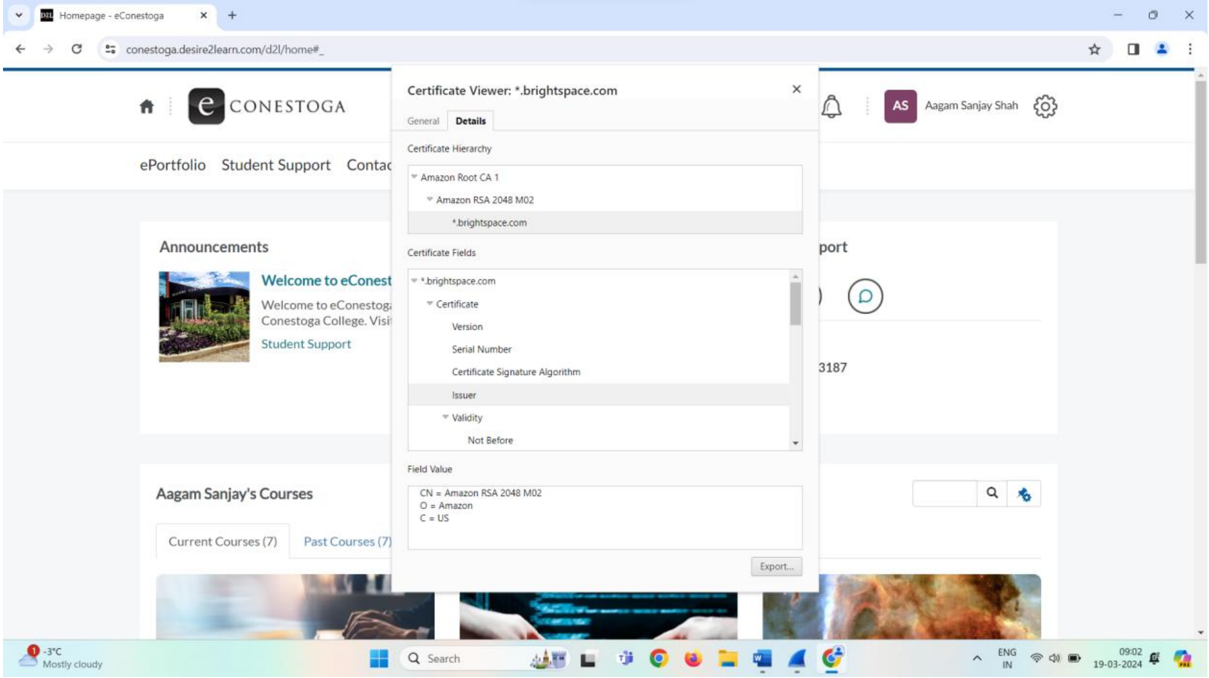
Common Name (CN)	Amazon RSA 2048 M02
Organisation (O)	Amazon
Organisational Unit (OU)	<Not part of certificate>

Validity Period

Issued On	Monday, 31 July 2023 at 20:00:00
Expires On	Thursday, 29 August 2024 at 19:59:59

SHA-256 Fingerprints

Certificate	41c557a0492870fb722971e9fdcd3e0b57b12692d217096556f0a44adf6aa20b
Public key	27b487218061989361e569b9af1875f1acae9abec03ce2928cf9304a45bb7a66



Certificate Viewer: *.brightspace.com

General | Details

Certificate Hierarchy

```
▾ Amazon Root CA 1
    ▾ Amazon RSA 2048 M02
        *.brightspace.com
```

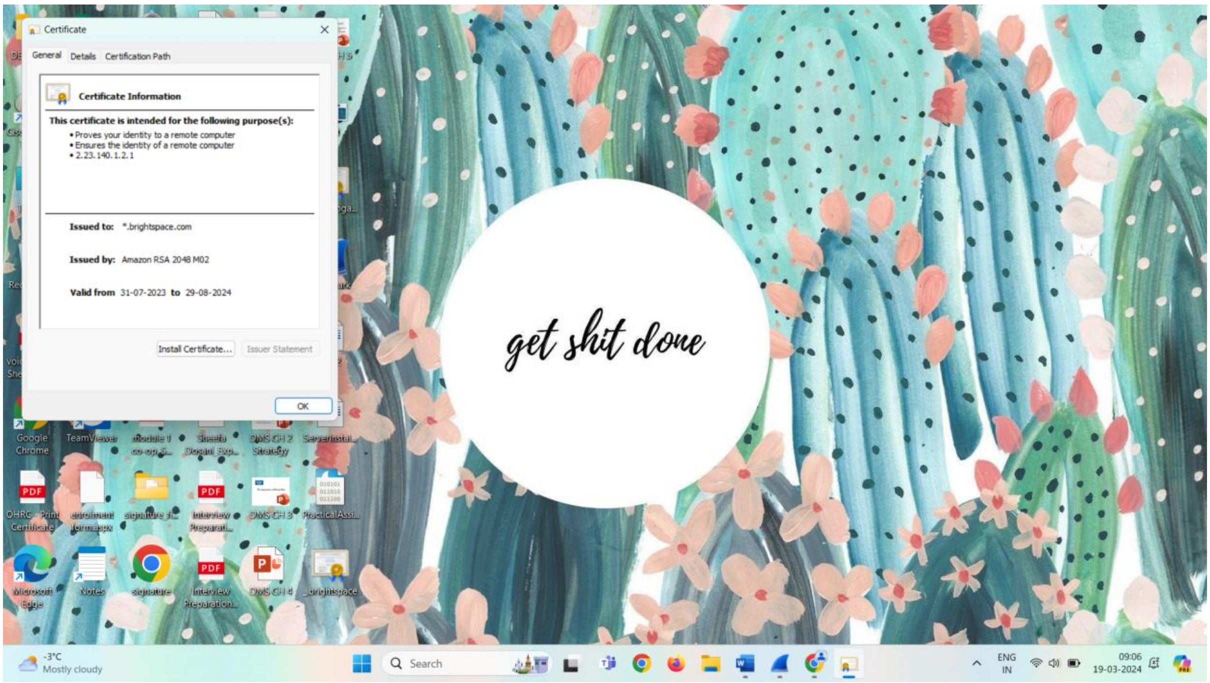
Certificate Fields

```
▾ *.brightspace.com
    ▾ Certificate
        Version
        Serial Number
        Certificate Signature Algorithm
        Issuer
        ▾ Validity
            Not Before
```

Field Value

```
CN = Amazon RSA 2048 M02
O = Amazon
C = US
```

Export...



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

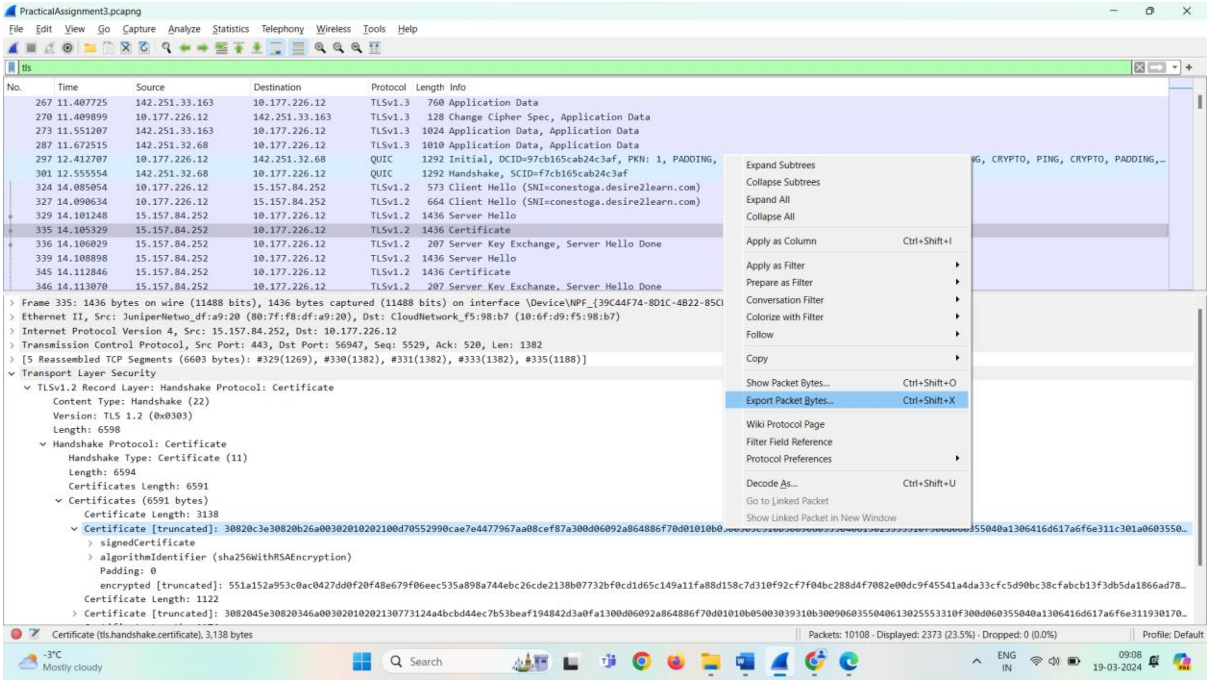
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: *.brightspace.com

Issued by: Amazon RSA 2048 M02

Valid from 31-07-2023 **to** 29-08-2024

3. Search in the packet capture and find the Server Hello frame that contains that certificate
    - Include screenshot showing how to search for the frame that includes the website certificate (hint search for key certificate terms, like who the certificate was issued to)
    - Include a screenshot showing the frame that contains the website certificate

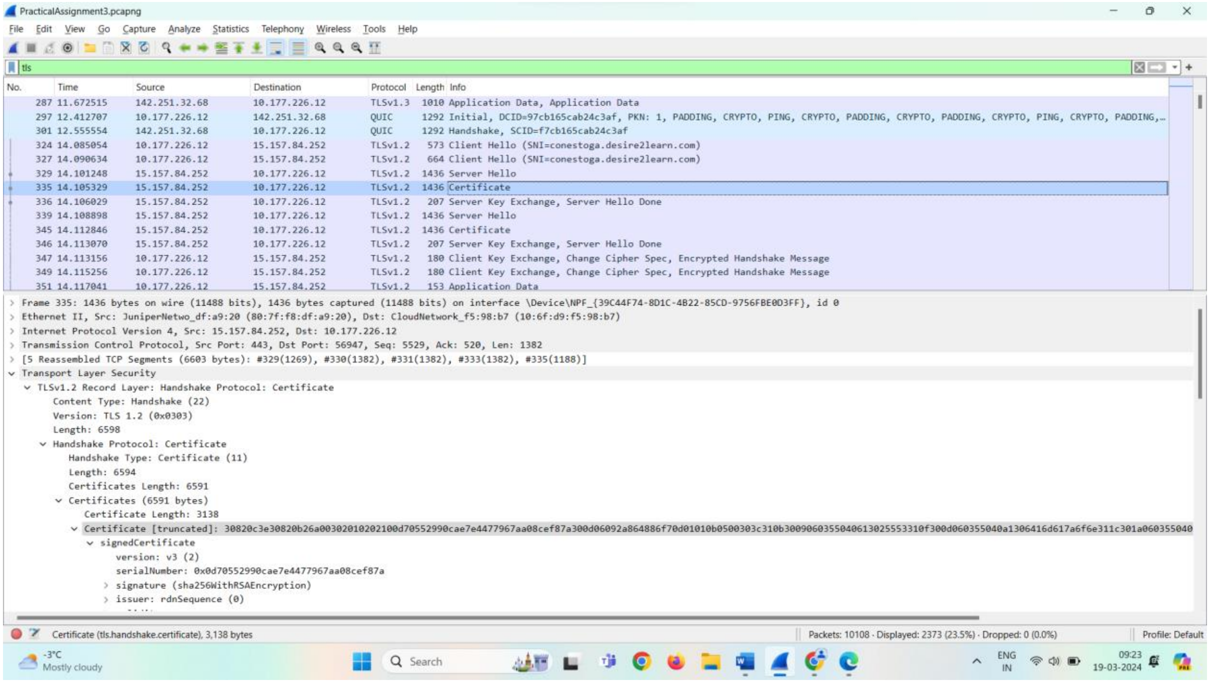


PracticalAssignment3.pcapng

```
tls
No.   Time       Source          Destination     Protocol Length Info
  267 11.407725  142.251.33.163  10.177.226.12   TLSv1.3   760 Application Data
  270 11.409899  10.177.226.12   142.251.33.163  TLSv1.3   128 Change Cipher Spec, Application Data
  273 11.551207  142.251.33.163  10.177.226.12   TLSv1.3  1024 Application Data, Application Data
  287 11.672515  142.251.32.68   10.177.226.12   TLSv1.3  1010 Application Data, Application Data
  297 12.412707  10.177.226.12   142.251.32.68   QUIC     1292 Initial, DCID=97cb165cab24c3af, PKN: 1, PADDING, ...NG, CRYPTO, PING, CRYPTO, PADDING,…
  301 12.555554  142.251.32.68   10.177.226.12   QUIC     1292 Handshake, SCID=f7cb165cab24c3af
  324 14.085054  10.177.226.12   15.157.84.252   TLSv1.2   573 Client Hello (SNI=conestoga.desire2learn.com)
  327 14.090634  10.177.226.12   15.157.84.252   TLSv1.2   664 Client Hello (SNI=conestoga.desire2learn.com)
  329 14.101248  15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  335 14.105329  15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  336 14.106029  15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  339 14.108898  15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  345 14.112846  15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  346 14.113070  15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done

> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface \Device\NPF_{39C44F74-8D1C-4B22-85C
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (10:6f:d9:f5:98:b7)
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      v Certificates (6591 bytes)
          Certificate Length: 3138
        v Certificate [truncated]: 30820c3e30820b26a00302010202100d70552990cae7e4477967aa08cef87a300d06092a864886f70d01010b0...55040a1306416d617a6f6e311c301a0603550…
          > signedCertificate
          > algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted [truncated]: 551a152a953c0ac0427dd0f20f48e679f06eec535a898a744ebc26cde2138b07732bf0cd1d65c149a11fa88d158c7d310f92cf7f04bc288d4f7082e00dc9f45541a4da33cfc5d90bc38cfabcb13f3db5da1866ad78…
          Certificate Length: 1122
        > Certificate [truncated]: 3082045e30820346a003020102021307731244a4bcbd44ec7b53beaf194842d3a0fa1300d06092a864886f70d01010b05003039310b3009060355040613025553310f300d060355040a1306416d617a6f6e311930170…

Certificate (tls.handshake.certificate), 3,138 bytes    Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%)    Profile: Default
```



PracticalAssignment3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

```
No.   Time          Source          Destination     Protocol  Length Info
  287 11.672515     142.251.32.68   10.177.226.12   TLSv1.3   1010 Application Data, Application Data
  297 12.412707     10.177.226.12   142.251.32.68   QUIC      1292 Initial, DCID=97cb165cab24c3af, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING,…
  301 12.555554     142.251.32.68   10.177.226.12   QUIC      1292 Handshake, SCID=f7cb165cab24c3af
  324 14.085054     10.177.226.12   15.157.84.252   TLSv1.2    573 Client Hello (SNI=conestoga.desire2learn.com)
  327 14.090634     10.177.226.12   15.157.84.252   TLSv1.2    664 Client Hello (SNI=conestoga.desire2learn.com)
  329 14.101248     15.157.84.252   10.177.226.12   TLSv1.2   1436 Server Hello
  335 14.105329     15.157.84.252   10.177.226.12   TLSv1.2   1436 Certificate
  336 14.106029     15.157.84.252   10.177.226.12   TLSv1.2    207 Server Key Exchange, Server Hello Done
  339 14.108898     15.157.84.252   10.177.226.12   TLSv1.2   1436 Server Hello
  345 14.112846     15.157.84.252   10.177.226.12   TLSv1.2   1436 Certificate
  346 14.113070     15.157.84.252   10.177.226.12   TLSv1.2    207 Server Key Exchange, Server Hello Done
  347 14.113156     10.177.226.12   15.157.84.252   TLSv1.2    180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  349 14.115256     10.177.226.12   15.157.84.252   TLSv1.2    180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  351 14.117041     10.177.226.12   15.157.84.252   TLSv1.2    153 Application Data
```

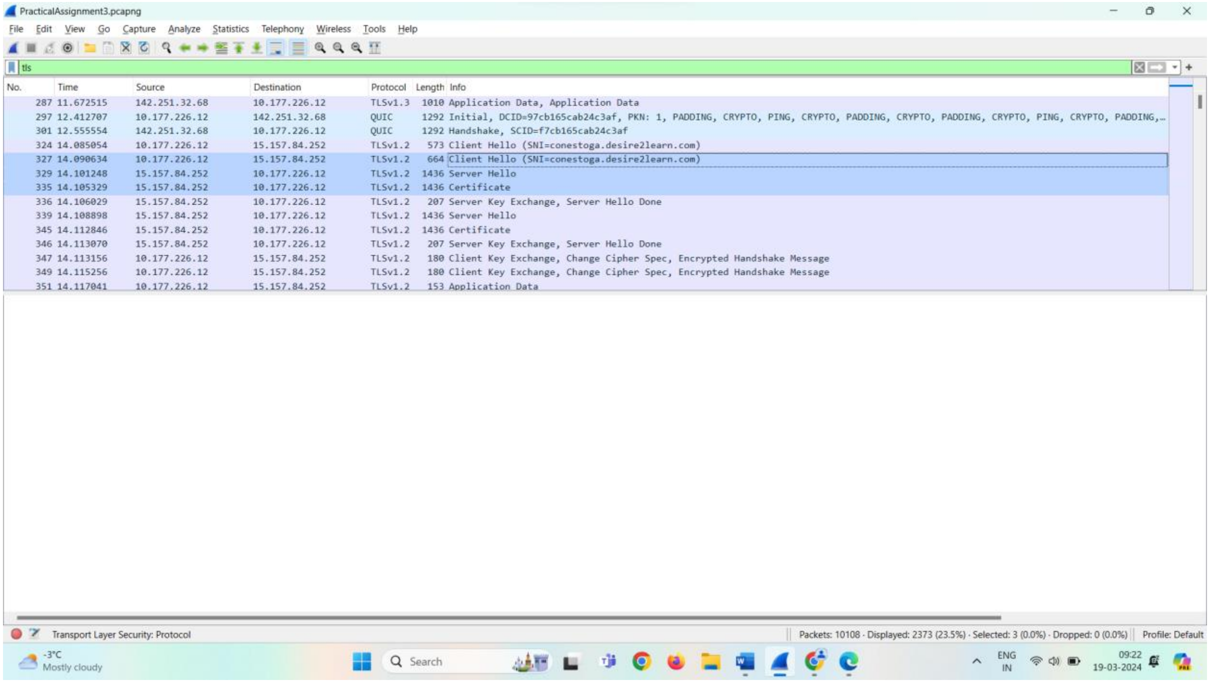
```
> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface \Device\NPF_{39C44F74-8D1C-4B22-85CD-9756FBE0D3FF}, id 0
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (10:6f:d9:f5:98:b7)
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      v Certificates (6591 bytes)
          Certificate Length: 3138
        v Certificate [truncated]: 30820c3e30820b26a00302010202100d70552990cae7e4477967aa08cef87a300d06092a864886f70d01010b0500303c310b3009060355040613025553310f300d060355040a1306416d617a6f6e311c301a060355040
          v signedCertificate
              version: v3 (2)
              serialNumber: 0x0d70552990cae7e4477967aa08cef87a
            > signature (sha256WithRSAEncryption)
            > issuer: rdnSequence (0)
```

Certificate (tls.handshake.certificate), 3,138 bytes

Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%)

Profile: Default

-3°C
Mostly cloudy
Search
ENG
IN
09:23
19-03-2024



PracticalAssignment3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

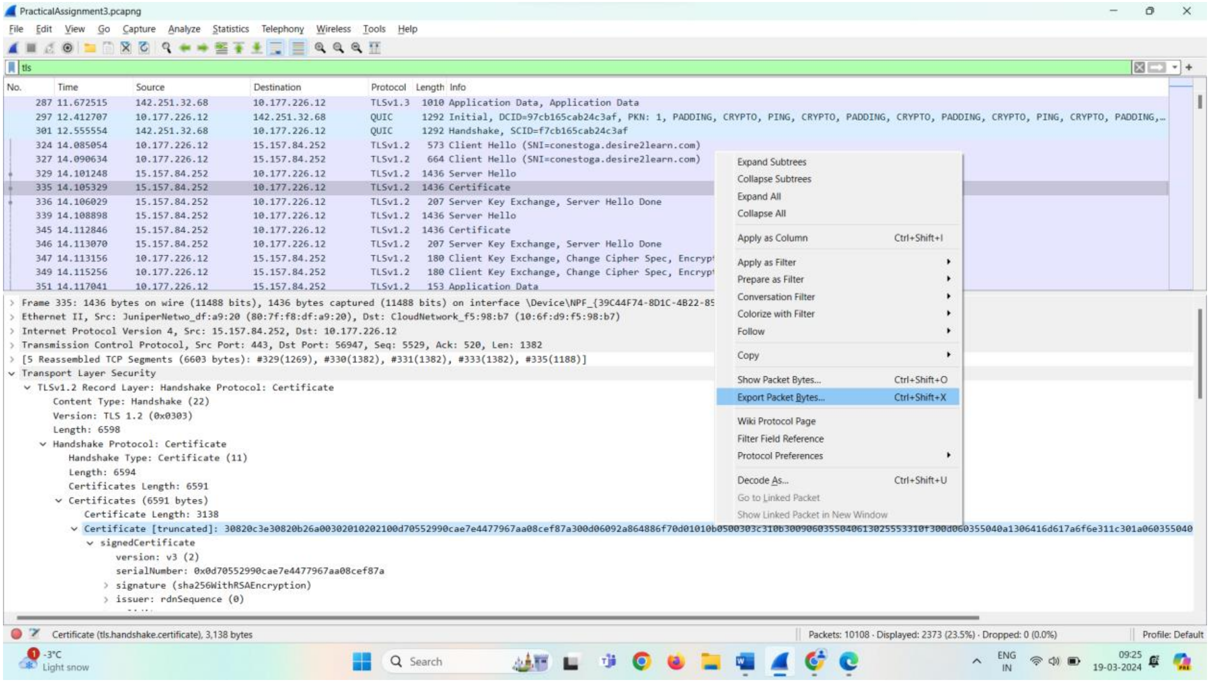
```
No.   Time          Source          Destination     Protocol  Length Info
  287 11.672515     142.251.32.68   10.177.226.12   TLSv1.3   1010 Application Data, Application Data
  297 12.412707     10.177.226.12   142.251.32.68   QUIC      1292 Initial, DCID=97cb165cab24c3af, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING,…
  301 12.555554     142.251.32.68   10.177.226.12   QUIC      1292 Handshake, SCID=f7cb165cab24c3af
  324 14.085054     10.177.226.12   15.157.84.252   TLSv1.2    573 Client Hello (SNI=conestoga.desire2learn.com)
  327 14.090634     10.177.226.12   15.157.84.252   TLSv1.2    664 Client Hello (SNI=conestoga.desire2learn.com)
  329 14.101248     15.157.84.252   10.177.226.12   TLSv1.2   1436 Server Hello
  335 14.105329     15.157.84.252   10.177.226.12   TLSv1.2   1436 Certificate
  336 14.106029     15.157.84.252   10.177.226.12   TLSv1.2    207 Server Key Exchange, Server Hello Done
  339 14.108898     15.157.84.252   10.177.226.12   TLSv1.2   1436 Server Hello
  345 14.112846     15.157.84.252   10.177.226.12   TLSv1.2   1436 Certificate
  346 14.113070     15.157.84.252   10.177.226.12   TLSv1.2    207 Server Key Exchange, Server Hello Done
  347 14.113156     10.177.226.12   15.157.84.252   TLSv1.2    180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  349 14.115256     10.177.226.12   15.157.84.252   TLSv1.2    180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  351 14.117041     10.177.226.12   15.157.84.252   TLSv1.2    153 Application Data
```

Transport Layer Security: Protocol

Packets: 10108 · Displayed: 2373 (23.5%) · Selected: 3 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

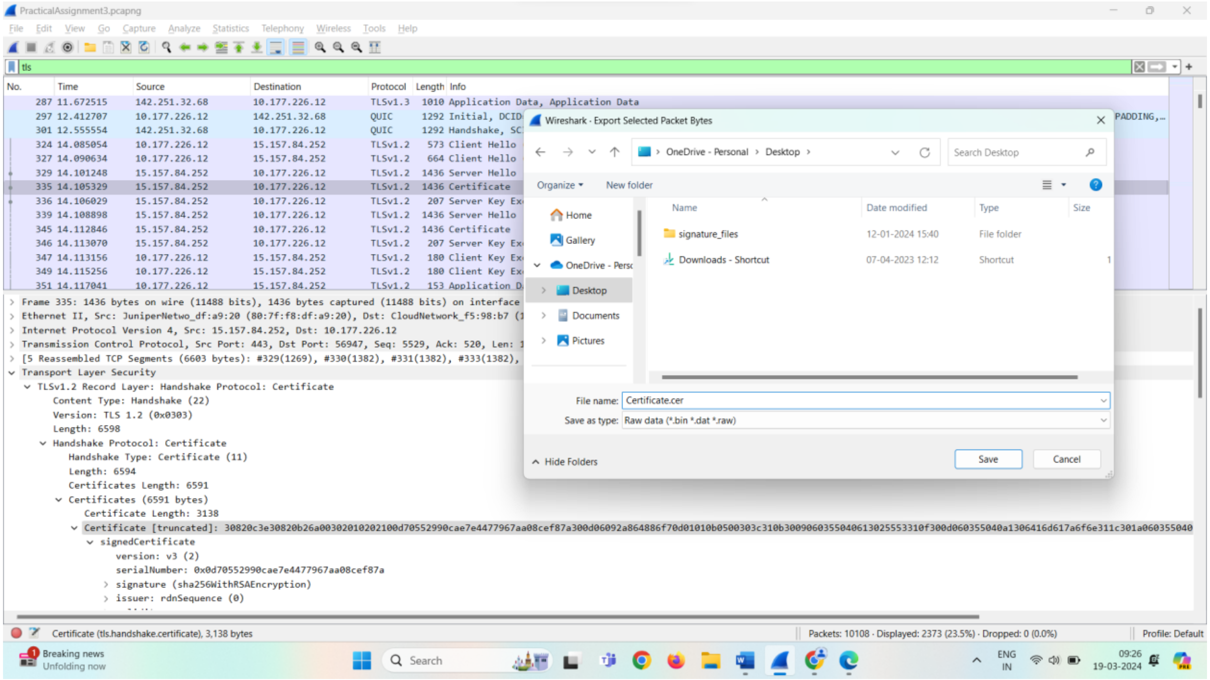
4. Extract the certificate from the network capture
    - Include screenshot(s) of the process to extract the certificate and of the extracted certificate on the details tab



```
No.   Time       Source          Destination     Protocol Length Info
  287 11.672515  142.251.32.68   10.177.226.12   TLSv1.3  1010 Application Data, Application Data
  297 12.412707  10.177.226.12   142.251.32.68   QUIC     1292 Initial, DCID=97cb165cab24c3af, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING,…
  301 12.555554  142.251.32.68   10.177.226.12   QUIC     1292 Handshake, SCID=f7cb165cab24c3af
  324 14.085054  10.177.226.12   15.157.84.252   TLSv1.2   573 Client Hello (SNI=conestoga.desire2learn.com)
  327 14.090634  10.177.226.12   15.157.84.252   TLSv1.2   664 Client Hello (SNI=conestoga.desire2learn.com)
  329 14.101248  15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  335 14.105329  15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  336 14.106029  15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  339 14.108898  15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  345 14.112846  15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  346 14.113070  15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  347 14.113156  10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypt
  349 14.115256  10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypt
  351 14.117041  10.177.226.12   15.157.84.252   TLSv1.2   153 Application Data

> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface \Device\NPF_{39C44F74-8D1C-4B22-85
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (10:6f:d9:f5:98:b7)
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      v Certificates (6591 bytes)
          Certificate Length: 3138
        v Certificate [truncated]: 30820c3e30820b26a00302010202100d70552990cae7e4477967aa08cef87a300d06092a864886f70d01010b0500303c310b3009060355040613025553310f300d060355040a1306416d617a6f6e311c301a060355040
          v signedCertificate
              version: v3 (2)
              serialNumber: 0x0d70552990cae7e4477967aa08cef87a
            > signature (sha256WithRSAEncryption)
            > issuer: rdnSequence (0)

Certificate (tls.handshake.certificate), 3,138 bytes     Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%)     Profile: Default
```

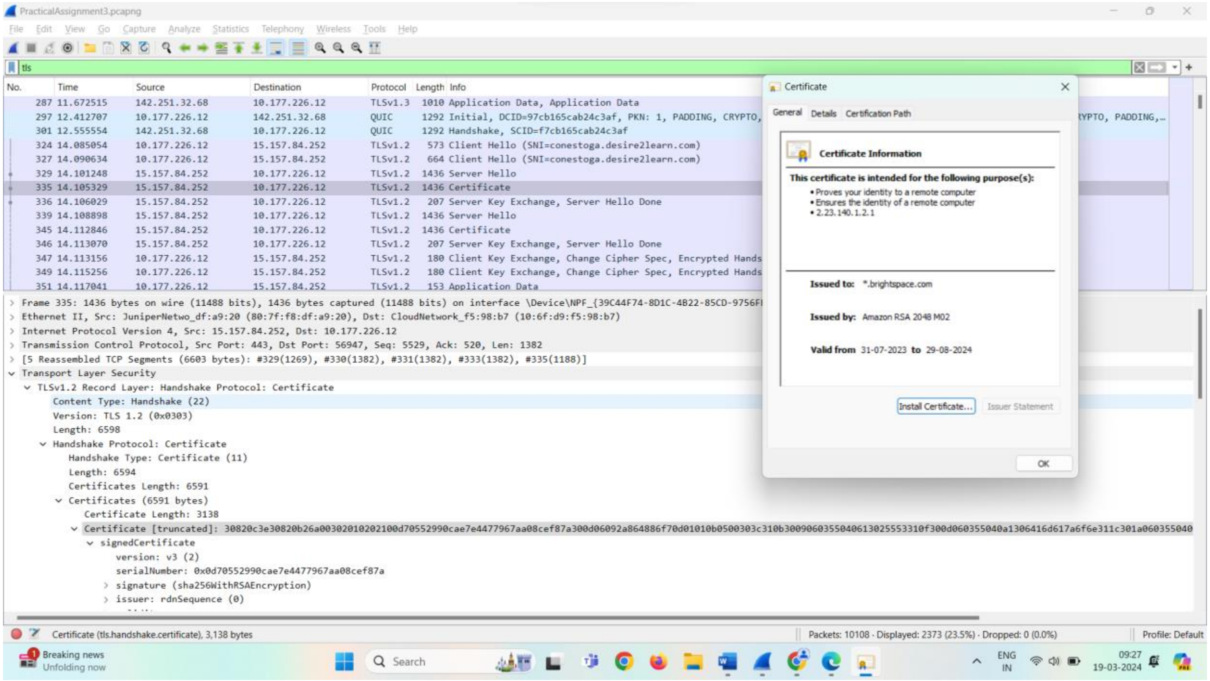


Name	Date modified	Type	Size
signature_files	12-01-2024 15:40	File folder	
Downloads - Shortcut	07-04-2023 12:12	Shortcut	1

File name: Certificate.cer

Save as type: Raw data (*.bin *.dat *.raw)

```
Certificate (tls.handshake.certificate), 3,138 bytes     Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%)     Profile: Default
```


PracticalAssignment3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
No.      Time       Source          Destination     Protocol Length Info
  287 11.672515   142.251.32.68   10.177.226.12   TLSv1.3  1010 Application Data, Application Data
  297 12.412707   10.177.226.12   142.251.32.68   QUIC     1292 Initial, DCID=97cb165cab24c3af, PKN: 1, PADDING, CRYPTO,
  301 12.555554   142.251.32.68   10.177.226.12   QUIC     1292 Handshake, SCID=f7cb165cab24c3af
  324 14.085054   10.177.226.12   15.157.84.252   TLSv1.2   573 Client Hello (SNI=conestoga.desire2learn.com)
  327 14.090634   10.177.226.12   15.157.84.252   TLSv1.2   664 Client Hello (SNI=conestoga.desire2learn.com)
  329 14.101248   15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  335 14.105329   15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  336 14.106029   15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  339 14.108898   15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  345 14.112846   15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  346 14.113070   15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  347 14.113156   10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Hands
  349 14.115256   10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Hands
  351 14.117041   10.177.226.12   15.157.84.252   TLSv1.2   153 Application Data
```

```
> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface \Device\NPF_{39C44F74-8D1C-4B22-85CD-9756F
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (10:6f:d9:f5:98:b7)
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      v Certificates (6591 bytes)
          Certificate Length: 3138
        v Certificate [truncated]: 30820c3e30820b26a00302010202100d70552990cae7e4477967aa08cef87a300d06092a864886f70d01010b0500303c310b3009060355040613025553310f300d060355040a1306416d617a6f6e311c301a060355040
          v signedCertificate
              version: v3 (2)
              serialNumber: 0x0d70552990cae7e4477967aa08cef87a
            > signature (sha256WithRSAEncryption)
            > issuer: rdnSequence (0)
```

Certificate (tls.handshake.certificate), 3,138 bytes

Packets: 10108 · Displayed: 2373 (23.5%) · Dropped: 0 (0.0%)

Profile: Default

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

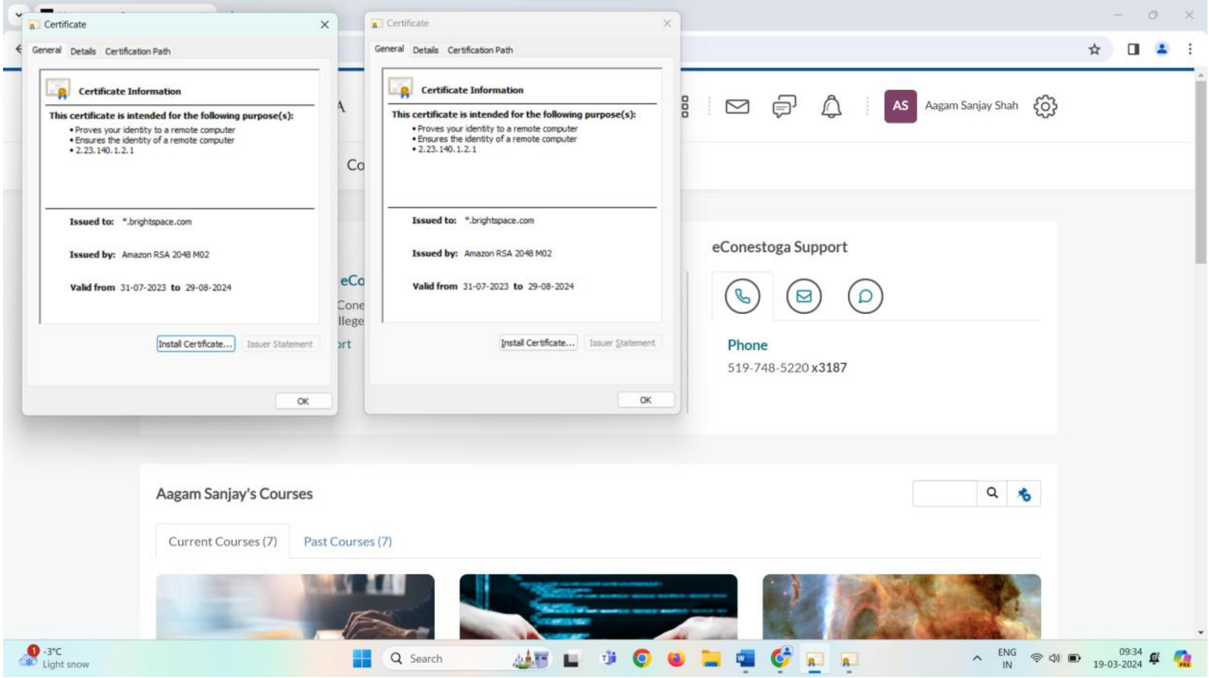
Issued to: *.brightspace.com

Issued by: Amazon RSA 2048 M02

Valid from 31-07-2023 **to** 29-08-2024

5. Compare Certificates

Include a screenshot that shows the details tab from both certificates highlighting a key attribute that can be used to determine if they are the same certificate


Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: *.brightspace.com

Issued by: Amazon RSA 2048 M02

Valid from 31-07-2023 **to** 29-08-2024

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: *.brightspace.com

Issued by: Amazon RSA 2048 M02

Valid from 31-07-2023 **to** 29-08-2024

AS Aagam Sanjay Shah

eConestoga Support

Phone

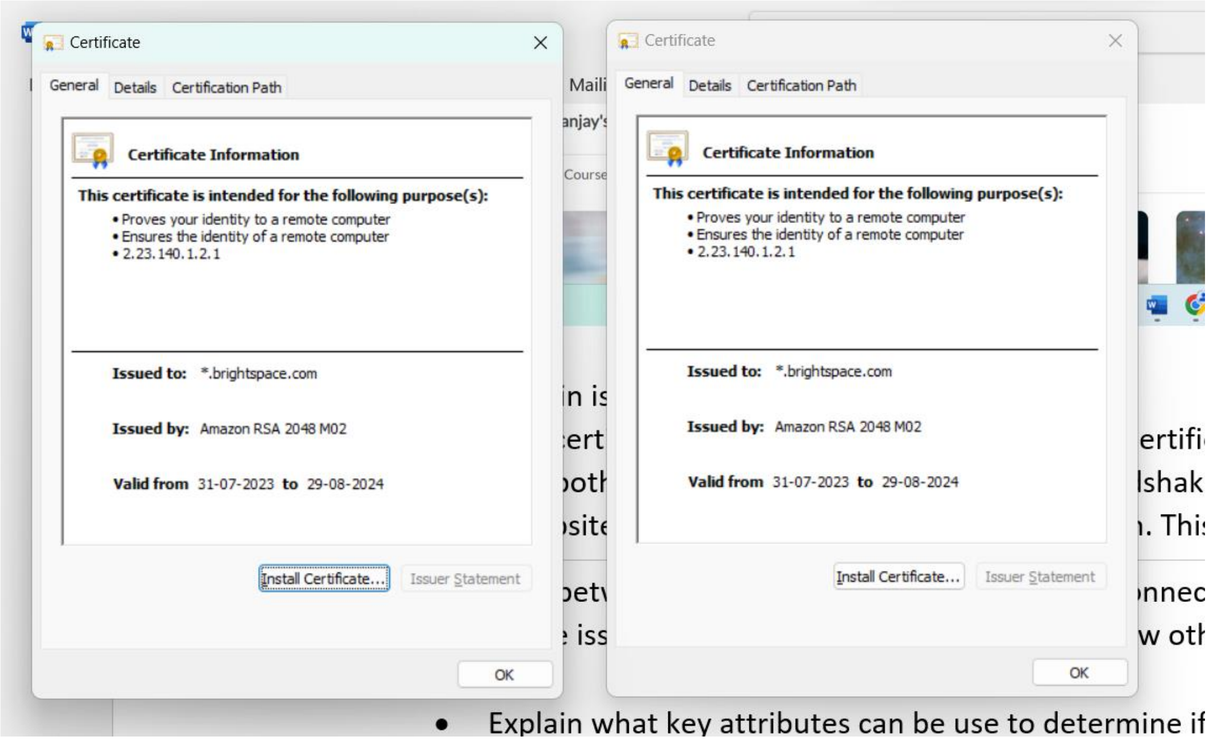
519-748-5220 x3187

Aagam Sanjay's Courses

Current Courses (7) | Past Courses (7)

- Explain is it the same certificate?

➔ Yes, The certificate we saved from browser and the certificate saved from wireshark capture, both are same as it’s the part of the tls handshake process when we try to connect https website, which performs secure the connection. This handshake of TLS certificate happens between client and server to validate the connection, which includes details like certificate issued to, public key, serial number and few other parameters.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: *.brightspace.com

Issued by: Amazon RSA 2048 M02

Valid from 31-07-2023 to 29-08-2024

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: *.brightspace.com

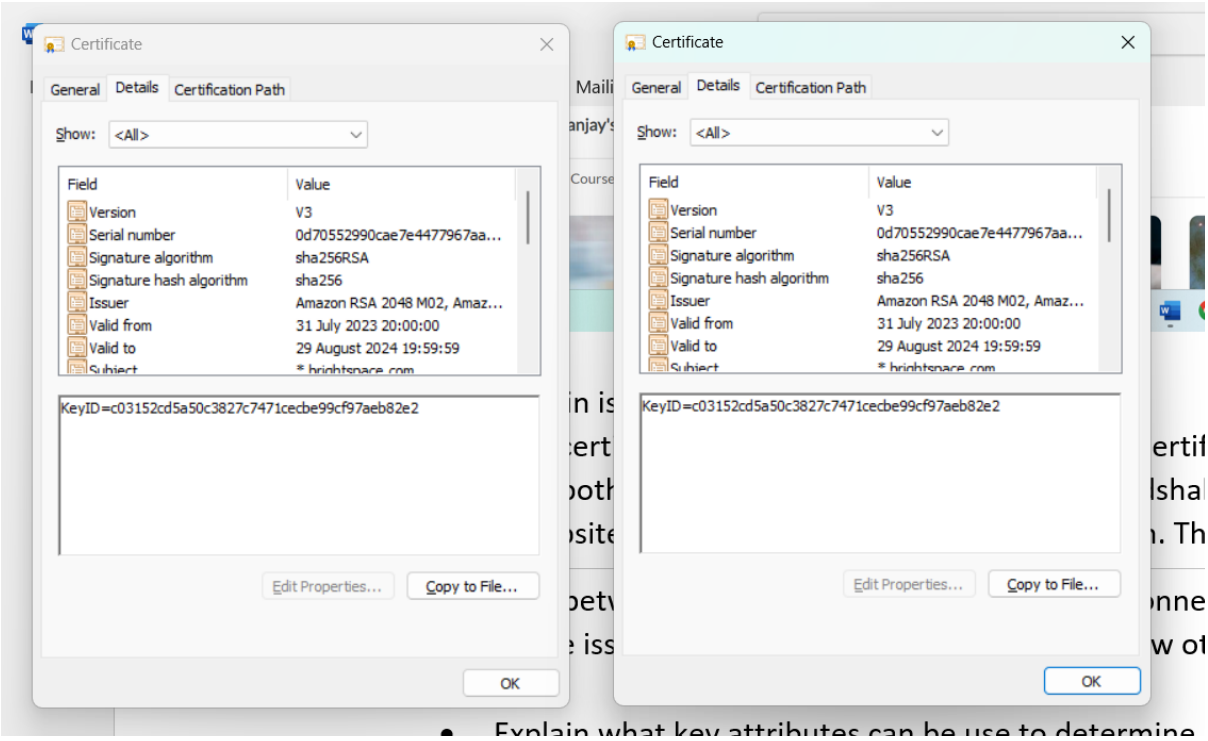
Issued by: Amazon RSA 2048 M02

Valid from 31-07-2023 to 29-08-2024

- Explain what key attributes can be use to determine if the certificate is the same?

➔ There are various key attributes to check whether the certificate is same or not, Such as

  - Serial number: unique serial number.
  - “Valid to” and “Valid from”.
  - Authority Key Identifier
  - Signature Algorithm
  - Signature Hash Algorithm
  - Issuer



Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	0d70552990cae7e4477967aa...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	31 July 2023 20:00:00
Valid to	29 August 2024 19:59:59
Subject	*.brightspace.com

KeyID=c03152cd5a50c3827c7471cecbe99cf97aeb82e2

Certificate

General | Details | Certification Path

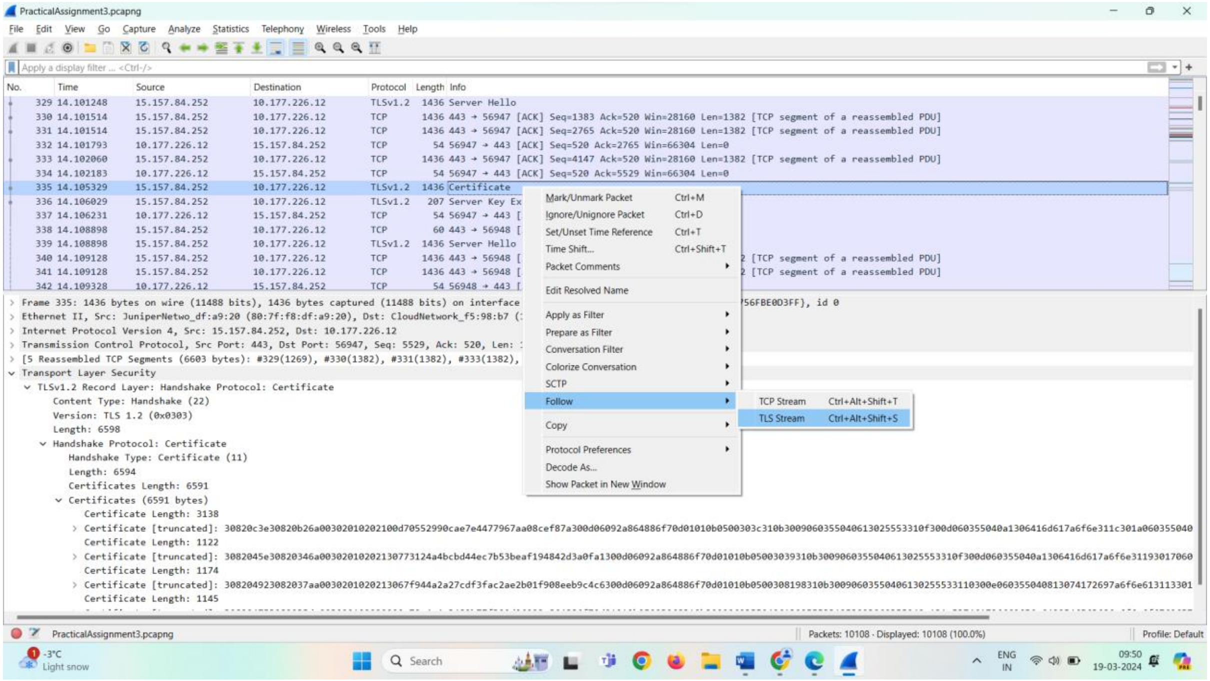
Show: <All>

Field	Value
Version	V3
Serial number	0d70552990cae7e4477967aa...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	31 July 2023 20:00:00
Valid to	29 August 2024 19:59:59
Subject	*.brightspace.com

KeyID=c03152cd5a50c3827c7471cecbe99cf97aeb82e2

- Explain what key attributes can be use to determine

6. Follow the TLS stream
   - Include screenshot showing you have followed the TLS stream

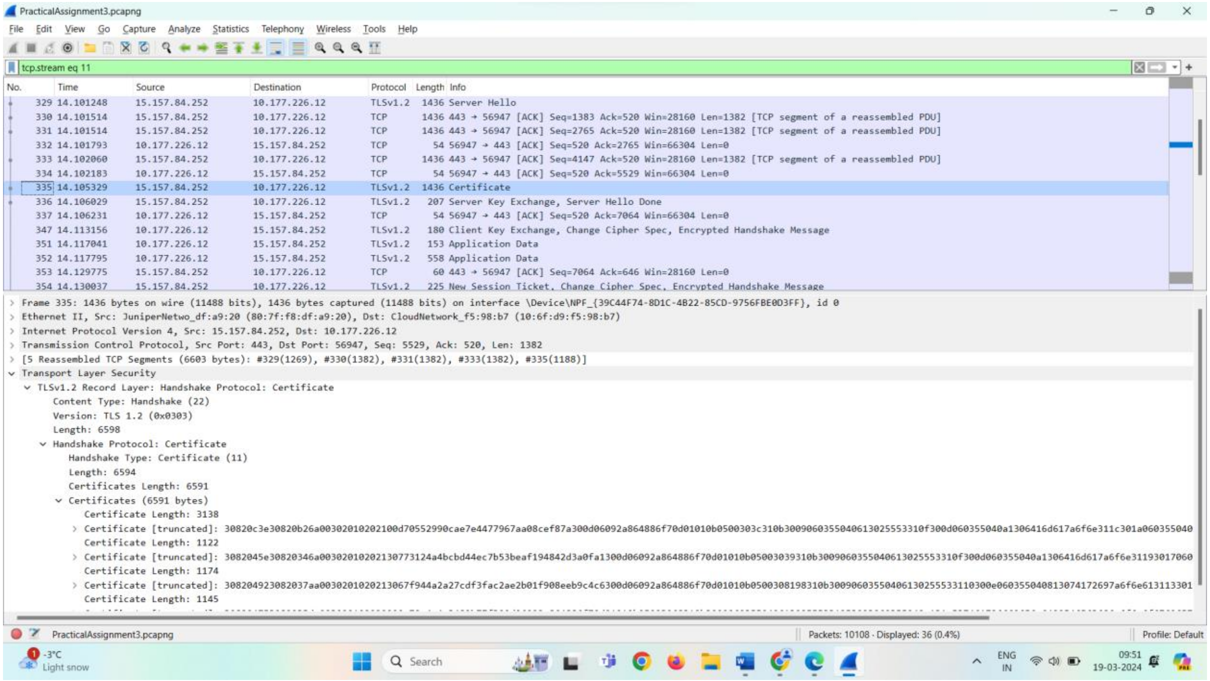


PracticalAssignment3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination     Protocol Length Info
  329 14.101248  15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  330 14.101514  15.157.84.252   10.177.226.12   TCP      1436 443 → 56947 [ACK] Seq=1383 Ack=520 Win=28160 Len=1382 [TCP segment of a reassembled PDU]
  331 14.101514  15.157.84.252   10.177.226.12   TCP      1436 443 → 56947 [ACK] Seq=2765 Ack=520 Win=28160 Len=1382 [TCP segment of a reassembled PDU]
  332 14.101793  10.177.226.12   15.157.84.252   TCP        54 56947 → 443 [ACK] Seq=520 Ack=2765 Win=66304 Len=0
  333 14.102060  15.157.84.252   10.177.226.12   TCP      1436 443 → 56947 [ACK] Seq=4147 Ack=520 Win=28160 Len=1382 [TCP segment of a reassembled PDU]
  334 14.102183  10.177.226.12   15.157.84.252   TCP        54 56947 → 443 [ACK] Seq=520 Ack=5529 Win=66304 Len=0
  335 14.105329  15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  336 14.106029  15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Ex
  337 14.106231  10.177.226.12   15.157.84.252   TCP        54 56947 → 443 [
  338 14.108898  15.157.84.252   10.177.226.12   TCP        60 443 → 56948 [
  339 14.108898  15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  340 14.109128  15.157.84.252   10.177.226.12   TCP      1436 443 → 56948 [                         2 [TCP segment of a reassembled PDU]
  341 14.109128  15.157.84.252   10.177.226.12   TCP      1436 443 → 56948 [                         2 [TCP segment of a reassembled PDU]
  342 14.109328  10.177.226.12   15.157.84.252   TCP        54 56948 → 443 [
```

```
> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface          56FBE0D3FF}, id 0
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (:
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: :
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382),
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      v Certificates (6591 bytes)
          Certificate Length: 3138
        > Certificate [truncated]: 30820c3e30820b26a00302010202100d70552990cae7e4477967aa08cef87a300d06092a864886f70d01010b0500303c310b3009060355040613025553310f300d060355040a1306416d617a6f6e311c301a060355040
          Certificate Length: 1122
        > Certificate [truncated]: 3082045e30820346a00302010202130773124a4bcbd44ec7b53beaf194842d3a0fa1300d06092a864886f70d01010b05003039310b3009060355040613025553310f300d060355040a1306416d617a6f6e31193017060
          Certificate Length: 1174
        > Certificate [truncated]: 308204923082037aa0030201020213067f944a2a27cdf3fac2ae2b01f908eeb9c4c6300d06092a864886f70d01010b0500308198310b30090603550406130255533110300e060355040813074172697a6f6e613113301
          Certificate Length: 1145
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
TLS Stream Ctrl+Alt+Shift+S
PracticalAssignment3.pcapng
Packets: 10108 · Displayed: 10108 (100.0%)
Profile: Default
-3°C
Light snow
Search
ENG
IN
09:50
19-03-2024


PracticalAssignment3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 11

```
No.   Time        Source          Destination     Protocol Length Info
  329 14.101248   15.157.84.252   10.177.226.12   TLSv1.2  1436 Server Hello
  330 14.101514   15.157.84.252   10.177.226.12   TCP      1436 443 → 56947 [ACK] Seq=1383 Ack=520 Win=28160 Len=1382 [TCP segment of a reassembled PDU]
  331 14.101514   15.157.84.252   10.177.226.12   TCP      1436 443 → 56947 [ACK] Seq=2765 Ack=520 Win=28160 Len=1382 [TCP segment of a reassembled PDU]
  332 14.101793   10.177.226.12   15.157.84.252   TCP        54 56947 → 443 [ACK] Seq=520 Ack=2765 Win=66304 Len=0
  333 14.102060   15.157.84.252   10.177.226.12   TCP      1436 443 → 56947 [ACK] Seq=4147 Ack=520 Win=28160 Len=1382 [TCP segment of a reassembled PDU]
  334 14.102183   10.177.226.12   15.157.84.252   TCP        54 56947 → 443 [ACK] Seq=520 Ack=5529 Win=66304 Len=0
  335 14.105329   15.157.84.252   10.177.226.12   TLSv1.2  1436 Certificate
  336 14.106029   15.157.84.252   10.177.226.12   TLSv1.2   207 Server Key Exchange, Server Hello Done
  337 14.106231   10.177.226.12   15.157.84.252   TCP        54 56947 → 443 [ACK] Seq=520 Ack=7064 Win=66304 Len=0
  347 14.113156   10.177.226.12   15.157.84.252   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  351 14.117041   10.177.226.12   15.157.84.252   TLSv1.2   153 Application Data
  352 14.117795   10.177.226.12   15.157.84.252   TLSv1.2   558 Application Data
  353 14.129775   15.157.84.252   10.177.226.12   TCP        60 443 → 56947 [ACK] Seq=7064 Ack=646 Win=28160 Len=0
  354 14.130037   15.157.84.252   10.177.226.12   TLSv1.2   225 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

> Frame 335: 1436 bytes on wire (11488 bits), 1436 bytes captured (11488 bits) on interface \Device\NPF_{39C44F74-8D1C-4B22-85CD-9756FBE0D3FF}, id 0
> Ethernet II, Src: JuniperNetwo_df:a9:20 (80:7f:f8:df:a9:20), Dst: CloudNetwork_f5:98:b7 (10:6f:d9:f5:98:b7)
> Internet Protocol Version 4, Src: 15.157.84.252, Dst: 10.177.226.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 56947, Seq: 5529, Ack: 520, Len: 1382
> [5 Reassembled TCP Segments (6603 bytes): #329(1269), #330(1382), #331(1382), #333(1382), #335(1188)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 6598
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 6594
        Certificates Length: 6591
      v Certificates (6591 bytes)
          Certificate Length: 3138
        > Certificate [truncated]: 30820c3e30820b26a00302010202100d70552990cae7e4477967aa08cef87a300d06092a864886f70d01010b0500303c310b3009060355040613025553310f300d060355040a1306416d617a6f6e311c301a060355040
          Certificate Length: 1122
        > Certificate [truncated]: 3082045e30820346a0030201020213077312 4a4bcbd44ec7b53beaf194842d3a0fa1300d06092a864886f70d01010b05003039310b3009060355040613025553310f300d060355040a1306416d617a6f6e31193017060
          Certificate Length: 1174
        > Certificate [truncated]: 308204923082037aa0030201020213067f944a2a27cdf3fac2ae2b01f908eeb9c4c6300d06092a864886f70d01010b0500308198310b300906035504061302555331103000e0603550408130741726 97a6f6e613113301
          Certificate Length: 1145
```

PracticalAssignment3.pcapng
Packets: 10108 · Displayed: 36 (0.4%)
Profile: Default
-3°C
Light snow
Search
ENG
IN
09:51
19-03-2024

- Explain 3 differences between the TCP and TLS handshake?

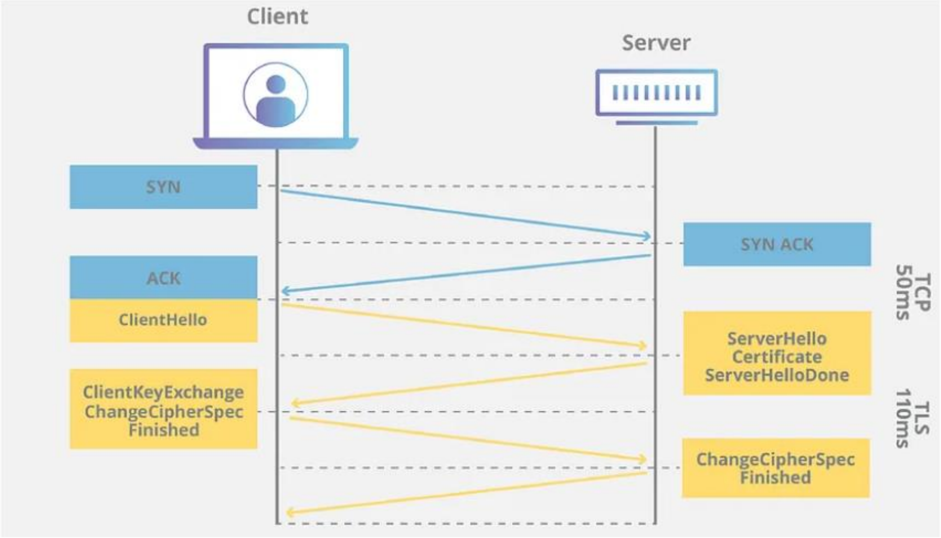
"TCP:

- ➔ SYN: Browser sends a SYN packet to server, with a random sequence number x. The packet also includes TCP flags and options
- ➔ SYN-ACK: Server receives the SYN packet from the browser. It needs to return a SYN-ACK packet that includes two sequence numbers. For ACK, it is x+1 which acknowledges the packet sent from the client. For SYN, the server picks a random sequence number y on its side. Then it sends the packet to the client
- ➔ ACK: The client receives the SYN-ACK packet. Similarly, the client acknowledges the packet from server, by incrementing the sequence number picked by the server, i.e y+1. Then, the client sends a ACK packet to the server with the sequence numbers y+1 and x+1.

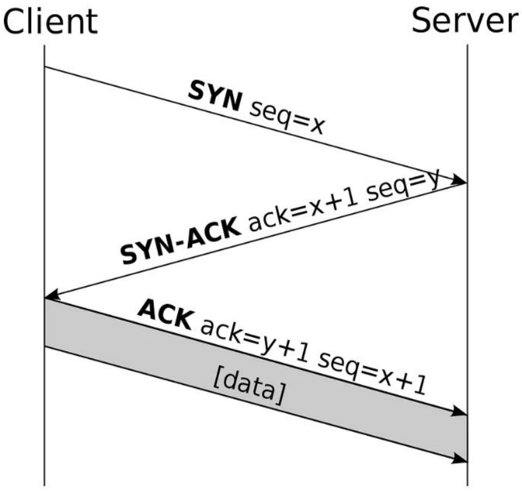
TLS:

- ➔ Authentication Server is always authenticated but client is optionally to be authenticated, by using different cryptography (RSA, ECSDA…)
- ➔ Confidentiality Data is only visible to the endpoints.
- ➔ Integrity Data cannot be modified." (Chan, 2022)

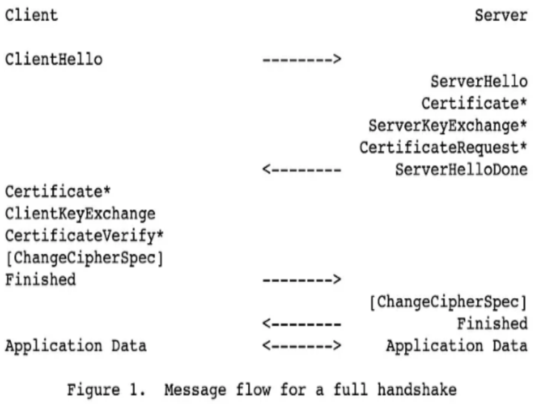
TCP three-way handshake and TLS handshake



TCP three-way handshake



Full handshake of TLS 1.2



```
Client                                               Server

ClientHello                  -------->
                                                ServerHello
                                               Certificate*
                                         ServerKeyExchange*
                                        CertificateRequest*
                             <--------      ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     -------->
                                         [ChangeCipherSpec]
                             <--------             Finished
Application Data             <------->     Application Data

         Figure 1.  Message flow for a full handshake
```

Reference: Chan, A. (2022, April 30). TCP and TLS handshake: What happens from typing in a URL to displaying a website? (Part 2). Medium. https://medium.com/@alysachan830/tcp-and-tls-handshake-what-happens-from-typing-in-a-url-to-displaying-a-website-part-2-243862438cd9