Task 1:

Root CA

Generate 512-bit ECC Private Key

```
$ openssl ecparam -name brainpoolP512r1 -genkey -noout -out root-ca-private-key.pem
```

Generate Public Key from 512-bit ECC Private Key

```
$ openssl ec -in root-ca-private-key.pem -pubout -out root-ca-public-key.pem
```

Create a root.cnf file to specify the Certificate details like Extensions, Key Usages

```
$ nano root.cnf
```

Root CA self signed certificate generation from private key

```
$ openssl req -x509 -new -nodes -key root-ca-private-key.pem -days 1825 -out root.pem -config root.cnf
-extensions v3_ca
```

Viewing the Root CA self-signed certificate

```
$ openssl x509 -in root.pem -text -noout
```

Intermediate CA

Intermediate CA private key generation

```
$ openssl genpkey -algorithm RSA -out int-ca-private-key.pem -pkeyopt rsa_keygen_bits:4096
```

Intermediate CA public key generation from private key

```
$ openssl rsa -in int-ca-private-key.pem -pubout -out int-ca-public-key.pem
```

Create a int.cnf file to specify the Certificate details like Extensions, Key Usages

```
$ nano int.cnf
```

CSR by Intermediate CA certificate that must be signed by the root CA

```
$ openssl req -config int.cnf -new -sha256 -key int-ca-private-key.pem -out int.csr -extensions v3_ca
```

CSR verified and signed by Root CA

```
$ openssl x509 -req -in int.csr -CA root.pem -CAkey root-ca-private-key.pem -CAcreateserial -out int.pem
-days 365 -extensions v3_ca -extfile int.cnf
```

View the Intermediate CA certificate

```
$ openssl x509 -in int.pem -text -noout
```

Alice

Generate 1024-bit RSA private key

```
$ openssl genpkey -algorithm RSA -out alice-private-key.pem -pkeyopt rsa_keygen_bits:1024
```

Generate public key

```
$ openssl rsa -in alice-private-key.pem -pubout -out alice-public-key.pem
```

Create a alice.cnf file to specify the Certificate details like Extensions, Key Usages

```
$ nano alice.cnf
```

CSR by Alice that must be signed by the Intermediate CA

```
$ openssl req -config alice.cnf -new -sha256 -key alice-private-key.pem -out alice.csr -extensions v3_req
```

CSR verified and signed by Intermediate CA

```
$ openssl x509 -req -in alice.csr -CA int.pem -CAkey int-ca-private-key.pem -CAcreateserial -out alice.pem
-days 90 -extensions v3_req -extfile alice.cnf
```

Viewing the Certificate

```
$ openssl x509 -in alice.pem -text -noout
```

Bob

Generate 256-bit ECC private key

```
$ openssl ecparam -name brainpoolP256r1 -genkey -noout -out bob-private-key.pem
```

Generate public key

```
$ openssl ec -in bob-private-key.pem -pubout -out bob-public-key.pem
```

Create a bob.cnf file to specify the Certificate details like Extensions, Key Usages

```
$ nano bob.cnf
```

CSR by Alice that must be signed by the Intermediate CA

```
$ openssl req -config bob.cnf -new -sha256 -key bob-private-key.pem -out bob.csr -extensions v3_req
```

CSR verified and signed by Intermediate CA

```
$ openssl x509 -req -in bob.csr -CA int.pem -CAkey int-ca-private-key.pem -CAcreateserial -out bob.pem
-days 90 -extensions v3_req -extfile bob.cnf
```

Viewing the Certificate

```
$ openssl x509 -in bob.pem -text -noout
```

Task 2:

Compiling the Code

```
$ c++ -o secure_chat_app secure_chat_app.cpp -lssl -lcrypto -Wall
```

Starting the server

```
$ lxc exec bob1 bash
$ ./secure_chat_app -s
```

Starting the client

```
$ lxc exec alice1 bash
$ ./secure_chat_app -c bob1
```

```
ubuntu@cs23mtech11009:~$ lxc exec alice1 bash
root@alice1:~# c++ -o secure_chat_app secure_chat_app.cpp -lssl -lcrypto -Wall
root@alice1:~# ./
.ssh/                  alice-private-key.pem  secure_chat_app
CA-Certs.pem           alice.pem              snap/
root@alice1:~# ./secure_chat_app -c bob1
<~> CLIENT STARTED!
<~> Trying to connect to bob1
<~> Connected to bob1
<~> Sent: chat_hello
<~> Received from Server: chat_ok_reply
<~> Sent: chat_START_SSL
<~> Received from Server: chat_START_SSL_ACK
<~> Initiating DTLS Handshake...
<~> Server accepted DTLS connection
<~> DTLS Handshake successful
</> Client: Hi Server
<~> Sent to Server: Hi Server
<~> Received from Server: Hi Client
</> Client: How are you?
<~> Sent to Server: How are you?
<~> Received from Server: I am good
</> Client: Thanks, IITH close
<~> Sent to Server: Thanks, IITH close
<~> Received chat_close from Server.
<~> Closing the connection...
root@alice1:~#
```

```
ubuntu@cs23mtech11009:~$ lxc exec bob1 bash
root@bob1:~# c++ -o secure_chat_app secure_chat_app.cpp -lssl -lcrypto -Wall
root@bob1:~# ./secure_chat_app -s
<~> SERVER STARTED!
<~> Waiting for client to connect...
<~> Client connected: alice1 (172.31.0.2)
<~> Received from Client: chat_hello
<~> Sent: chat_ok_reply
<~> Received from Client: chat_START_SSL
<~> Sent: chat_START_SSL_ACK
<~> Initializing SSL Handshake...
<~> Server accepted DTLS connection
<~> DTLS Handshake successful
<~> Received from Client: Hi Server
</> Server: Hi Client
<~> Sent to Client: Hi Client
<~> Received from Client: How are you?
</> Server: I am good
<~> Sent to Client: I am good
<~> Received from Client: Thanks, IITH close
</> Server: chat_close
<~> Sent chat_close to Client.
<~> Closing the connection...
root@bob1:~#
```

alice.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

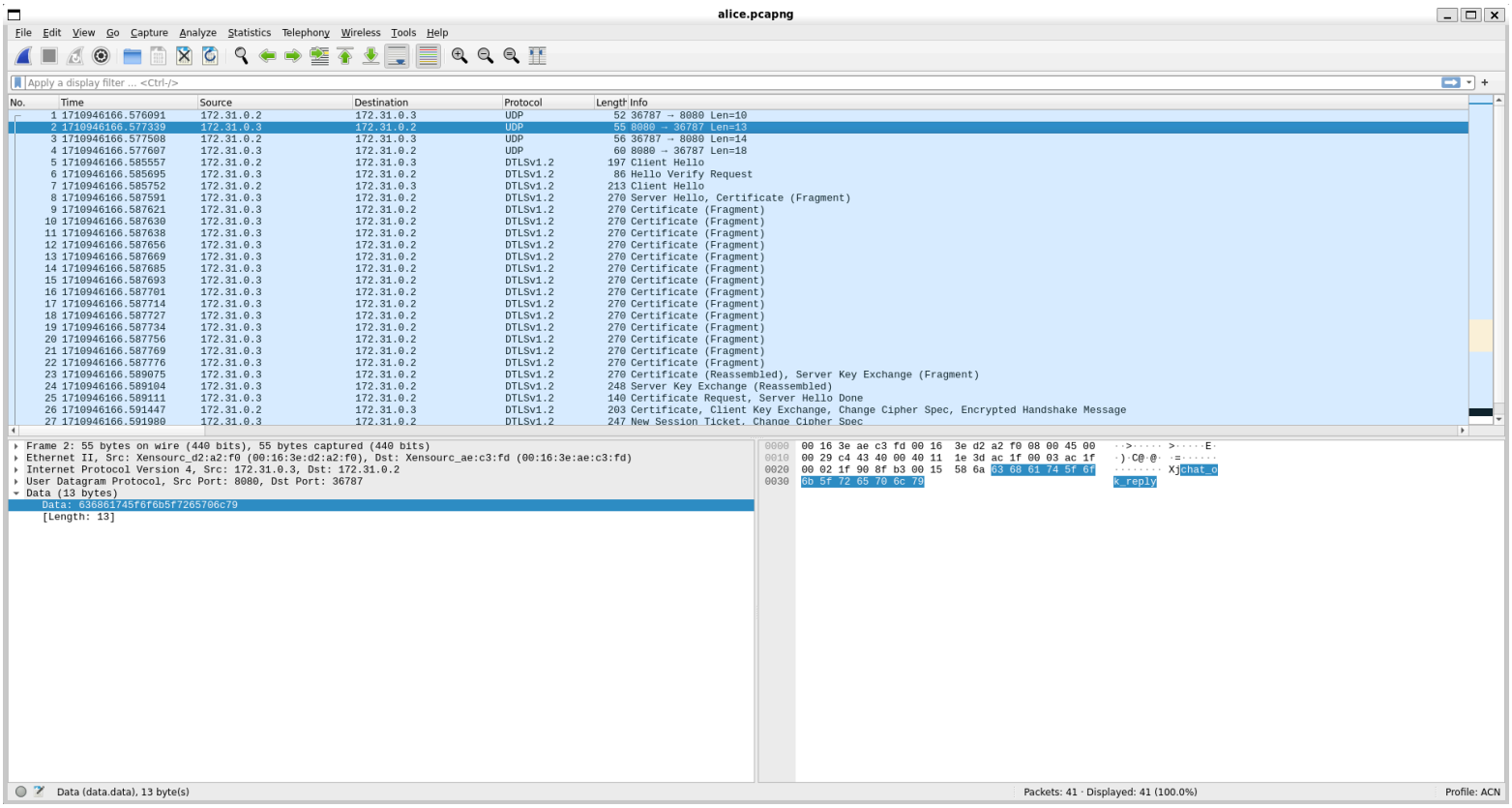
Apply a display filter ... <Ctrl-/>

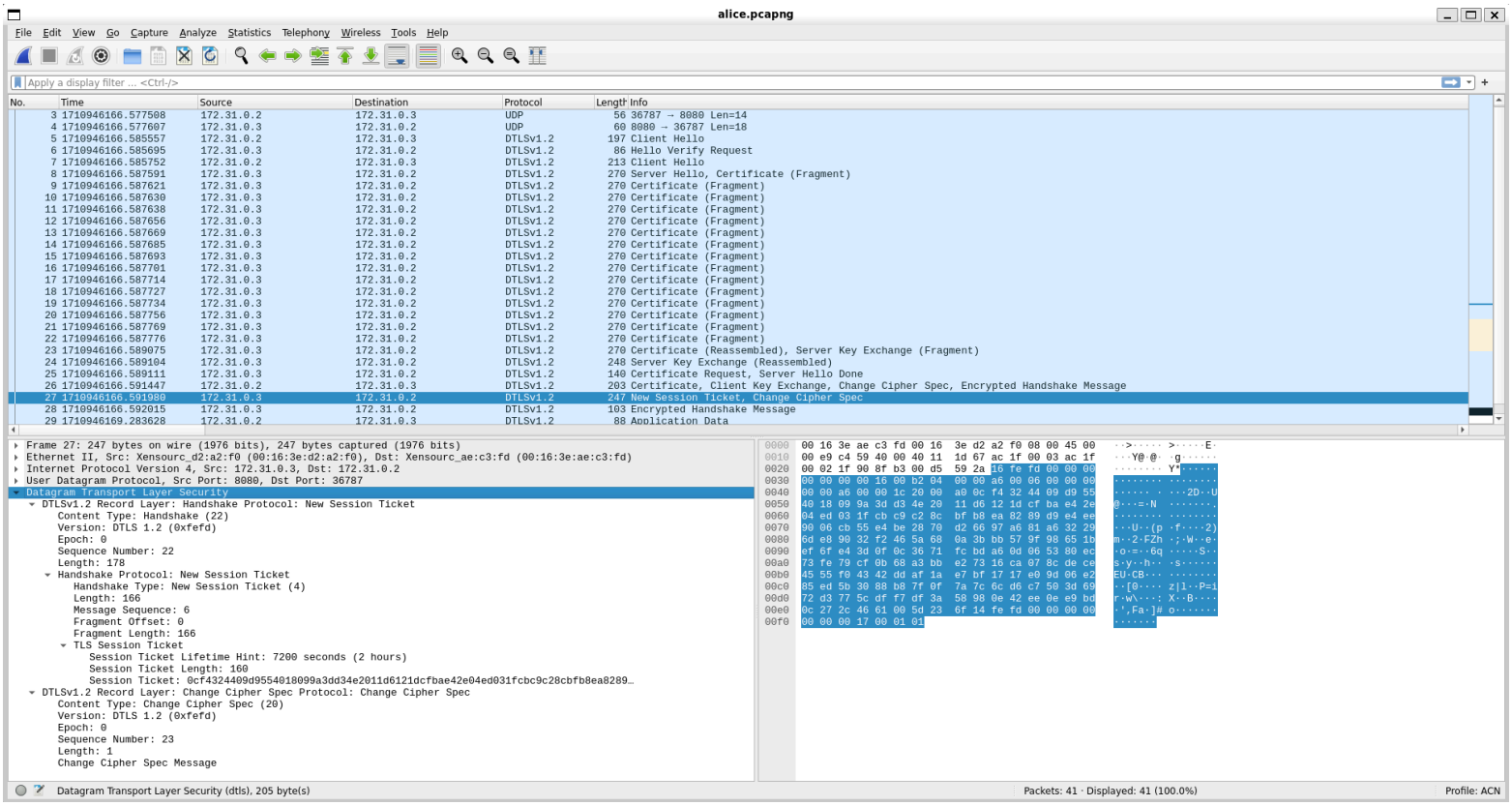
No.	Time	Source	Destination	Protocol	Length	Info
1	1710946166.576091	172.31.0.2	172.31.0.3	UDP	52	36787 → 8080 Len=10
2	1710946166.577339	172.31.0.3	172.31.0.2	UDP	55	8080 → 36787 Len=13
3	1710946166.577508	172.31.0.2	172.31.0.3	UDP	56	36787 → 8080 Len=14
4	1710946166.577607	172.31.0.3	172.31.0.2	UDP	60	8080 → 36787 Len=18
5	1710946166.585557	172.31.0.2	172.31.0.3	DTLSv1.2	197	Client Hello
6	1710946166.585695	172.31.0.3	172.31.0.2	DTLSv1.2	86	Hello Verify Request
7	1710946166.585752	172.31.0.2	172.31.0.3	DTLSv1.2	213	Client Hello
8	1710946166.587591	172.31.0.3	172.31.0.2	DTLSv1.2	270	Server Hello, Certificate (Fragment)
9	1710946166.587621	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
10	1710946166.587630	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
11	1710946166.587638	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
12	1710946166.587656	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
13	1710946166.587669	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
14	1710946166.587685	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
15	1710946166.587693	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
16	1710946166.587701	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
17	1710946166.587714	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
18	1710946166.587727	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
19	1710946166.587734	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
20	1710946166.587756	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
21	1710946166.587769	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
22	1710946166.587776	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Fragment)
23	1710946166.589075	172.31.0.3	172.31.0.2	DTLSv1.2	270	Certificate (Reassembled), Server Key Exchange (Fragment)
24	1710946166.589104	172.31.0.3	172.31.0.2	DTLSv1.2	248	Server Key Exchange (Reassembled)
25	1710946166.589111	172.31.0.3	172.31.0.2	DTLSv1.2	140	Certificate Request, Server Hello Done
26	1710946166.591447	172.31.0.2	172.31.0.3	DTLSv1.2	203	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	1710946166.591980	172.31.0.3	172.31.0.2	DTLSv1.2	247	New Session Ticket, Change Cipher Spec

```
▸ Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
▸ Ethernet II, Src: Xensourc_ae:c3:fd (00:16:3e:ae:c3:fd), Dst: Xensourc_d2:a2:f0 (00:16:3e:d2:a2:f0)
▸ Internet Protocol Version 4, Src: 172.31.0.2, Dst: 172.31.0.3
▸ User Datagram Protocol, Src Port: 36787, Dst Port: 8080
▾ Data (10 bytes)
    Data: 636861745f68656c6c6f
    [Length: 10]
```

```
0000  00 16 3e d2 a2 f0 00 16  3e ae c3 fd 08 00 45 00   ··>····· >·····E·
0010  00 26 e9 73 40 00 40 11  f9 0f ac 1f 00 02 ac 1f   ·&·s@·@· ········
0020  00 03 8f b3 1f 90 00 12  58 67 63 68 61 74 5f 68   ········ Xgchat_h
0030  65 6c 6c 6f                                       ello
```

Data (data.data), 10 byte(s) | Packets: 41 · Displayed: 41 (100.0%) | Profile: ACN


alice.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 1710946166.576091 172.31.0.2 172.31.0.3 UDP 52 36787 → 8080 Len=10
2 1710946166.577339 172.31.0.3 172.31.0.2 UDP 55 8080 → 36787 Len=13
3 1710946166.577500 172.31.0.2 172.31.0.3 UDP 56 36787 → 8080 Len=14
4 1710946166.577607 172.31.0.3 172.31.0.2 UDP 60 8080 → 36787 Len=18
5 1710946166.585557 172.31.0.2 172.31.0.3 DTLSv1.2 197 Client Hello
6 1710946166.585695 172.31.0.3 172.31.0.2 DTLSv1.2 86 Hello Verify Request
7 1710946166.585752 172.31.0.2 172.31.0.3 DTLSv1.2 213 Client Hello
8 1710946166.587591 172.31.0.3 172.31.0.2 DTLSv1.2 270 Server Hello, Certificate (Fragment)
9 1710946166.587621 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
10 1710946166.587630 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
11 1710946166.587638 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
12 1710946166.587656 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
13 1710946166.587669 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
14 1710946166.587685 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
15 1710946166.587693 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
16 1710946166.587701 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
17 1710946166.587714 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
18 1710946166.587727 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
19 1710946166.587734 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
20 1710946166.587756 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
21 1710946166.587769 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
22 1710946166.587776 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
23 1710946166.589075 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Reassembled), Server Key Exchange (Fragment)
24 1710946166.589104 172.31.0.3 172.31.0.2 DTLSv1.2 248 Server Key Exchange (Reassembled)
25 1710946166.589111 172.31.0.3 172.31.0.2 DTLSv1.2 140 Certificate Request, Server Hello Done
26 1710946166.591447 172.31.0.2 172.31.0.3 DTLSv1.2 203 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27 1710946166.591980 172.31.0.3 172.31.0.2 DTLSv1.2 247 New Session Ticket, Change Cipher Spec
Frame 2: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)
Ethernet II, Src: Xensourc_d2:a2:f0 (00:16:3e:d2:a2:f0), Dst: Xensourc_ae:c3:fd (00:16:3e:ae:c3:fd)
Internet Protocol Version 4, Src: 172.31.0.3, Dst: 172.31.0.2
User Datagram Protocol, Src Port: 8080, Dst Port: 36787
Data (13 bytes)
Data: 636861745f6f6b5f7265706c79
[Length: 13]
0000 00 16 3e ae c3 fd 00 16 3e d2 a2 f0 08 00 45 00
0010 00 29 c4 43 40 00 40 11 1e 3d ac 1f 00 03 ac 1f
0020 00 02 1f 90 8f b3 00 15 58 6a 63 68 61 74 5f 6f
0030 6b 5f 72 65 70 6c 79
Data (data.data), 13 byte(s)
Packets: 41 · Displayed: 41 (100.0%)
Profile: ACN


alice.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3 1710946166.577508 172.31.0.2 172.31.0.3 UDP 56 36787 → 8080 Len=14
4 1710946166.577607 172.31.0.3 172.31.0.2 UDP 60 8080 → 36787 Len=18
5 1710946166.585557 172.31.0.2 172.31.0.3 DTLSv1.2 197 Client Hello
6 1710946166.585695 172.31.0.3 172.31.0.2 DTLSv1.2 86 Hello Verify Request
7 1710946166.585752 172.31.0.2 172.31.0.3 DTLSv1.2 213 Client Hello
8 1710946166.587591 172.31.0.3 172.31.0.2 DTLSv1.2 270 Server Hello, Certificate (Fragment)
9 1710946166.587621 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
10 1710946166.587630 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
11 1710946166.587638 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
12 1710946166.587656 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
13 1710946166.587669 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
14 1710946166.587685 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
15 1710946166.587693 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
16 1710946166.587701 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
17 1710946166.587714 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
18 1710946166.587727 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
19 1710946166.587734 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
20 1710946166.587756 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
21 1710946166.587769 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
22 1710946166.587776 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Fragment)
23 1710946166.589075 172.31.0.3 172.31.0.2 DTLSv1.2 270 Certificate (Reassembled), Server Key Exchange (Fragment)
24 1710946166.589104 172.31.0.3 172.31.0.2 DTLSv1.2 248 Server Key Exchange (Reassembled)
25 1710946166.589111 172.31.0.3 172.31.0.2 DTLSv1.2 140 Certificate Request, Server Hello Done
26 1710946166.591447 172.31.0.2 172.31.0.3 DTLSv1.2 203 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27 1710946166.591980 172.31.0.3 172.31.0.2 DTLSv1.2 247 New Session Ticket, Change Cipher Spec
28 1710946166.592015 172.31.0.3 172.31.0.2 DTLSv1.2 103 Encrypted Handshake Message
29 1710946169.283628 172.31.0.2 172.31.0.3 DTLSv1.2 88 Application Data
Frame 27: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)
Ethernet II, Src: Xensourc_d2:a2:f0 (00:16:3e:d2:a2:f0), Dst: Xensourc_ae:c3:fd (00:16:3e:ae:c3:fd)
Internet Protocol Version 4, Src: 172.31.0.3, Dst: 172.31.0.2
User Datagram Protocol, Src Port: 8080, Dst Port: 36787
Datagram Transport Layer Security
DTLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
Content Type: Handshake (22)
Version: DTLS 1.2 (0xfefd)
Epoch: 0
Sequence Number: 22
Length: 178
Handshake Protocol: New Session Ticket
Handshake Type: New Session Ticket (4)
Length: 166
Message Sequence: 6
Fragment Offset: 0
Fragment Length: 166
TLS Session Ticket
Session Ticket Lifetime Hint: 7200 seconds (2 hours)
Session Ticket Length: 160
Session Ticket: 0cf4324409d9554018099a3dd34e2011d6121dcfbae42e04ed031fcbc9c28cbfb8ea8289…
DTLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: DTLS 1.2 (0xfefd)
Epoch: 0
Sequence Number: 23
Length: 1
Change Cipher Spec Message
0000 00 16 3e ae c3 fd 00 16 3e d2 a2 f0 08 00 45 00
0010 00 e9 c4 59 40 00 40 11 1d 67 ac 1f 00 03 ac 1f
0020 00 02 1f 90 8f b3 00 d5 59 2a 16 fe fd 00 00 00
0030 00 00 00 00 10 00 b2 04 00 00 a6 00 06 00 00 00
0040 00 00 a6 00 00 1c 20 00 a0 0c f4 32 44 09 d9 55
0050 40 18 09 9a 3d d3 4e 20 11 d6 12 1d cf ba e4 2e
0060 04 ed 03 1f cb c9 c2 8c bf b8 ea 82 89 d9 e4 ee
0070 90 06 cb 55 e4 be 28 70 d2 66 97 a6 81 a6 32 29
0080 6d e8 90 32 f2 46 5a 68 0a 3b bb 57 9f 98 65 1b
0090 ef 6f e4 3d 0f 0c 36 71 fc bd a6 0d 06 53 80 ec
00a0 73 fe 79 cf 0b 68 a3 bb e2 73 16 ca 07 8c de ce
00b0 45 55 f0 43 42 dd af 1a e7 bf 17 17 e0 9d 06 e2
00c0 85 ed 5b 30 88 b8 7f 0f 7a 7c 6c d6 c7 50 3d 69
00d0 72 d3 77 5c df f7 df 3a 58 98 0e 42 ee 0e e9 bd
00e0 0c 27 2c 46 61 00 5d 23 6f 14 fe fd 00 00 00 00
00f0 00 00 00 17 00 01 01
Datagram Transport Layer Security (dtls), 205 byte(s)
Packets: 41 · Displayed: 41 (100.0%)
Profile: ACN