Zoom, Webex Traffic Analysis

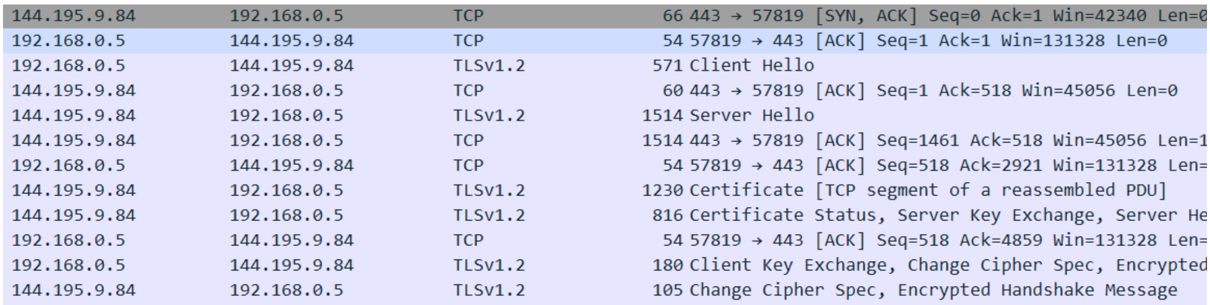
2017313135 소프트웨어학과 권동민

Q1. Uses WireShark to capture the live Zoom and Webex Traffic

- Saved separated files(zoom.pcap, webex.pcap)

Q2. What ports and protocols zoom traffic uses

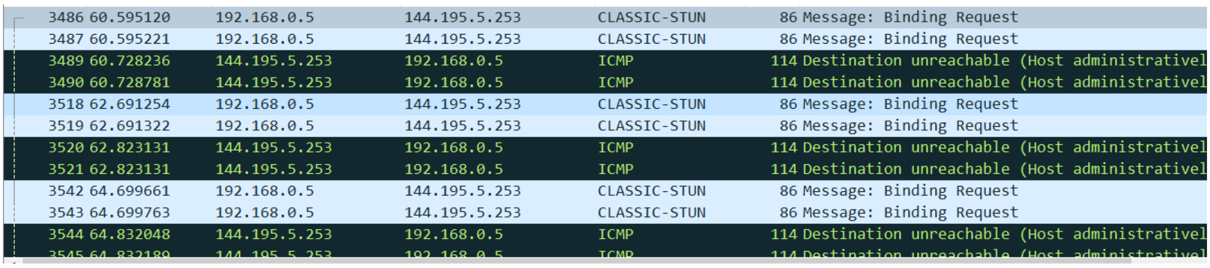
1. Three-hand-shaking



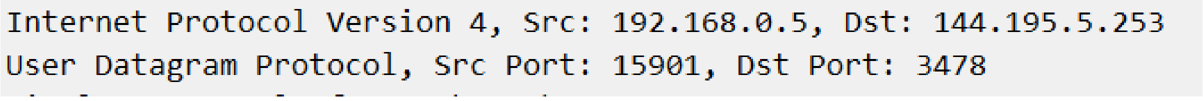
```
144.195.9.84   192.168.0.5    TCP        66 443 → 57819 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0
192.168.0.5    144.195.9.84   TCP        54 57819 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
192.168.0.5    144.195.9.84   TLSv1.2   571 Client Hello
144.195.9.84   192.168.0.5    TCP        60 443 → 57819 [ACK] Seq=1 Ack=518 Win=45056 Len=0
144.195.9.84   192.168.0.5    TLSv1.2  1514 Server Hello
144.195.9.84   192.168.0.5    TCP      1514 443 → 57819 [ACK] Seq=1461 Ack=518 Win=45056 Len=1
192.168.0.5    144.195.9.84   TCP        54 57819 → 443 [ACK] Seq=518 Ack=2921 Win=131328 Len=
144.195.9.84   192.168.0.5    TLSv1.2  1230 Certificate [TCP segment of a reassembled PDU]
144.195.9.84   192.168.0.5    TLSv1.2   816 Certificate Status, Server Key Exchange, Server He
192.168.0.5    144.195.9.84   TCP        54 57819 → 443 [ACK] Seq=518 Ack=4859 Win=131328 Len=
192.168.0.5    144.195.9.84   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted
144.195.9.84   192.168.0.5    TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
```

Port: TCP 443

2. When participants join the room



```
3486 60.595120  192.168.0.5    144.195.5.253  CLASSIC-STUN   86 Message: Binding Request
3487 60.595221  192.168.0.5    144.195.5.253  CLASSIC-STUN   86 Message: Binding Request
3489 60.728236  144.195.5.253  192.168.0.5    ICMP          114 Destination unreachable (Host administrativel
3490 60.728781  144.195.5.253  192.168.0.5    ICMP          114 Destination unreachable (Host administrativel
3518 62.691254  192.168.0.5    144.195.5.253  CLASSIC-STUN   86 Message: Binding Request
3519 62.691322  192.168.0.5    144.195.5.253  CLASSIC-STUN   86 Message: Binding Request
3520 62.823131  144.195.5.253  192.168.0.5    ICMP          114 Destination unreachable (Host administrativel
3521 62.823131  144.195.5.253  192.168.0.5    ICMP          114 Destination unreachable (Host administrativel
3542 64.699661  192.168.0.5    144.195.5.253  CLASSIC-STUN   86 Message: Binding Request
3543 64.699763  192.168.0.5    144.195.5.253  CLASSIC-STUN   86 Message: Binding Request
3544 64.832048  144.195.5.253  192.168.0.5    ICMP          114 Destination unreachable (Host administrativel
3545 64.832189  144.195.5.253  192.168.0.5    ICMP          114 Destination unreachable (Host administrativel
```

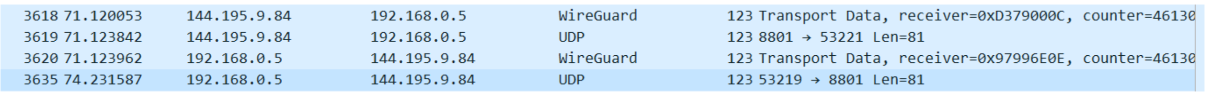


```
Internet Protocol Version 4, Src: 192.168.0.5, Dst: 144.195.5.253
User Datagram Protocol, Src Port: 15901, Dst Port: 3478
```

Port : UDP 3478

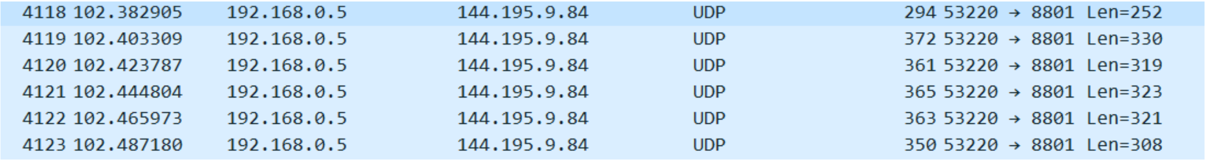
3. Send and receive data(video, audio)

- Send nothing(not video, audio)



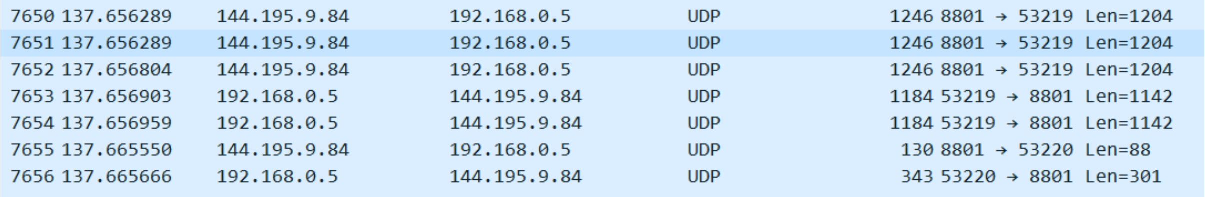
```
3618 71.120053  144.195.9.84  192.168.0.5   WireGuard  123 Transport Data, receiver=0xD379000C, counter=46130
3619 71.123842  144.195.9.84  192.168.0.5   UDP        123 8801 → 53221 Len=81
3620 71.123962  192.168.0.5   144.195.9.84  WireGuard  123 Transport Data, receiver=0x97996E0E, counter=46130
3635 74.231587  192.168.0.5   144.195.9.84  UDP        123 53219 → 8801 Len=81
```

- Send just audio



```
4118 102.382905    192.168.0.5         144.195.9.84        UDP             294 53220 → 8801 Len=252
4119 102.403309    192.168.0.5         144.195.9.84        UDP             372 53220 → 8801 Len=330
4120 102.423787    192.168.0.5         144.195.9.84        UDP             361 53220 → 8801 Len=319
4121 102.444804    192.168.0.5         144.195.9.84        UDP             365 53220 → 8801 Len=323
4122 102.465973    192.168.0.5         144.195.9.84        UDP             363 53220 → 8801 Len=321
4123 102.487180    192.168.0.5         144.195.9.84        UDP             350 53220 → 8801 Len=308
```

- Send audio and video



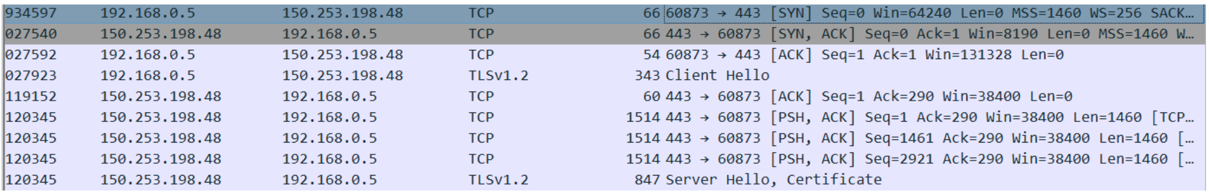
```
7650 137.656289   144.195.9.84        192.168.0.5         UDP            1246 8801 → 53219 Len=1204
7651 137.656289   144.195.9.84        192.168.0.5         UDP            1246 8801 → 53219 Len=1204
7652 137.656804   144.195.9.84        192.168.0.5         UDP            1246 8801 → 53219 Len=1204
7653 137.656903   192.168.0.5         144.195.9.84        UDP            1184 53219 → 8801 Len=1142
7654 137.656959   192.168.0.5         144.195.9.84        UDP            1184 53219 → 8801 Len=1142
7655 137.665550   144.195.9.84        192.168.0.5         UDP             130 8801 → 53220 Len=88
7656 137.665666   192.168.0.5         144.195.9.84        UDP             343 53220 → 8801 Len=301
```

We can see that the length of data increases. (123 -> 300 -> 1100)

Port : UDP 8801, wireGuard

Q3. What ports and protocols Webex traffic uses

1. Three-hand-shaking

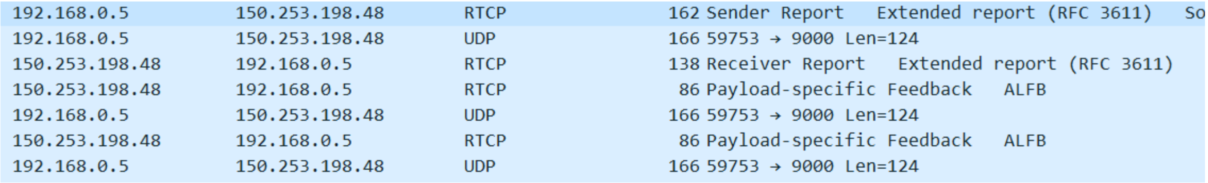


```
934597    192.168.0.5       150.253.198.48    TCP            66 60873 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK…
027540    150.253.198.48    192.168.0.5       TCP            66 443 → 60873 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 W…
027592    192.168.0.5       150.253.198.48    TCP            54 60873 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
027923    192.168.0.5       150.253.198.48    TLSv1.2       343 Client Hello
119152    150.253.198.48    192.168.0.5       TCP            60 443 → 60873 [ACK] Seq=1 Ack=290 Win=38400 Len=0
120345    150.253.198.48    192.168.0.5       TCP          1514 443 → 60873 [PSH, ACK] Seq=1 Ack=290 Win=38400 Len=1460 [TCP…
120345    150.253.198.48    192.168.0.5       TCP          1514 443 → 60873 [PSH, ACK] Seq=1461 Ack=290 Win=38400 Len=1460 […
120345    150.253.198.48    192.168.0.5       TCP          1514 443 → 60873 [PSH, ACK] Seq=2921 Ack=290 Win=38400 Len=1460 […
120345    150.253.198.48    192.168.0.5       TLSv1.2       847 Server Hello, Certificate
```

Port: TCP 443

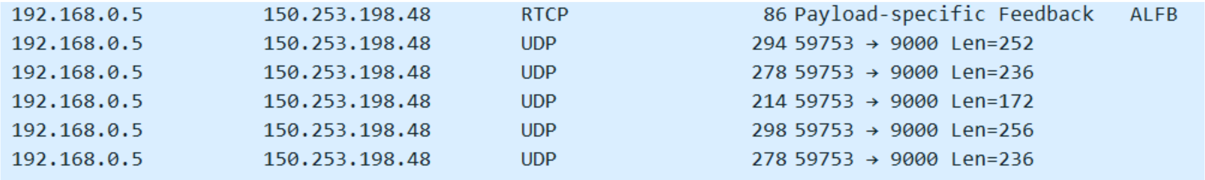
2. Send and receive data(video, audio)

- Send nothing(not video, audio)



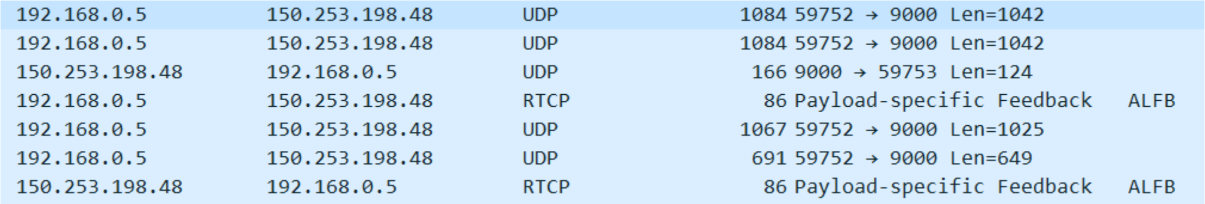
```
192.168.0.5         150.253.198.48      RTCP           162 Sender Report   Extended report (RFC 3611)   So
192.168.0.5         150.253.198.48      UDP            166 59753 → 9000 Len=124
150.253.198.48      192.168.0.5         RTCP           138 Receiver Report   Extended report (RFC 3611)
150.253.198.48      192.168.0.5         RTCP            86 Payload-specific Feedback   ALFB
192.168.0.5         150.253.198.48      UDP            166 59753 → 9000 Len=124
150.253.198.48      192.168.0.5         RTCP            86 Payload-specific Feedback   ALFB
192.168.0.5         150.253.198.48      UDP            166 59753 → 9000 Len=124
```

- Send just audio



```
192.168.0.5         150.253.198.48      RTCP            86 Payload-specific Feedback   ALFB
192.168.0.5         150.253.198.48      UDP            294 59753 → 9000 Len=252
192.168.0.5         150.253.198.48      UDP            278 59753 → 9000 Len=236
192.168.0.5         150.253.198.48      UDP            214 59753 → 9000 Len=172
192.168.0.5         150.253.198.48      UDP            298 59753 → 9000 Len=256
192.168.0.5         150.253.198.48      UDP            278 59753 → 9000 Len=236
```

- Send audio and video



```
192.168.0.5         150.253.198.48      UDP           1084 59752 → 9000 Len=1042
192.168.0.5         150.253.198.48      UDP           1084 59752 → 9000 Len=1042
150.253.198.48      192.168.0.5         UDP            166 9000 → 59753 Len=124
192.168.0.5         150.253.198.48      RTCP            86 Payload-specific Feedback   ALFB
192.168.0.5         150.253.198.48      UDP           1067 59752 → 9000 Len=1025
192.168.0.5         150.253.198.48      UDP            691 59752 → 9000 Len=649
150.253.198.48      192.168.0.5         RTCP            86 Payload-specific Feedback   ALFB
```

Port : UDP 9000

Q4. Sender's and receiver's information observed by traffic

- Ip, port, protocol(zoom and webex is not p2p communication so the ip is server ip)
- Mac address
- Transmission time
- Data(voice and video information are transferred)

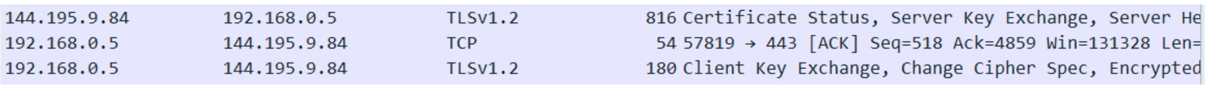
Q5. Authentication process of Zoom and Webex

- Zoom : Password Authentication.(if you don't set the password, zoom makes password automatically.) And people can participate zoom meeting by clicking url link.
- Webex : webex uses e-mail id of users for authentication. People can also participate by room link.

Q6. Key distribution protocol of Zoom and Webex

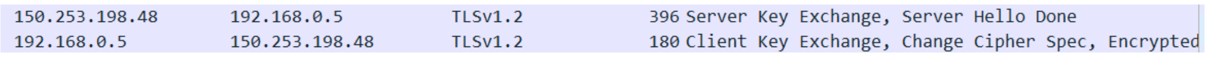
Zoom and Webex both support E2EE(End to End Encryption). So all client has their own private Key and public key. And sender make random key to encrypt data, also encrypt the key by receiver's public key.(uses public key encryption) Receiver finally encrypt the key and data to read. Zoom supports the E2EE in version 5.4.0 or higher.

Zoom:



```
144.195.9.84        192.168.0.5         TLSv1.2        816 Certificate Status, Server Key Exchange, Server He
192.168.0.5         144.195.9.84        TCP             54 57819 → 443 [ACK] Seq=518 Ack=4859 Win=131328 Len=
192.168.0.5         144.195.9.84        TLSv1.2        180 Client Key Exchange, Change Cipher Spec, Encrypted
```

Webex:



```
150.253.198.48      192.168.0.5         TLSv1.2        396 Server Key Exchange, Server Hello Done
192.168.0.5         150.253.198.48      TLSv1.2        180 Client Key Exchange, Change Cipher Spec, Encrypted
```

Q7. Encryption method of Zoom and Webex

Zoom : AES – 256 – GCM

암호화 알고리즘 AES-256-GCM

In Zoom version 5.0, all client are using "AES-256-GCM" algorithm to encrypt data.

Webex : AES 128, AES 256, SHA 256, RSA

During data transfer between server and client, Webex uses https(ssl). Also, Webex uses AES, SHA, RSA to encrypt.