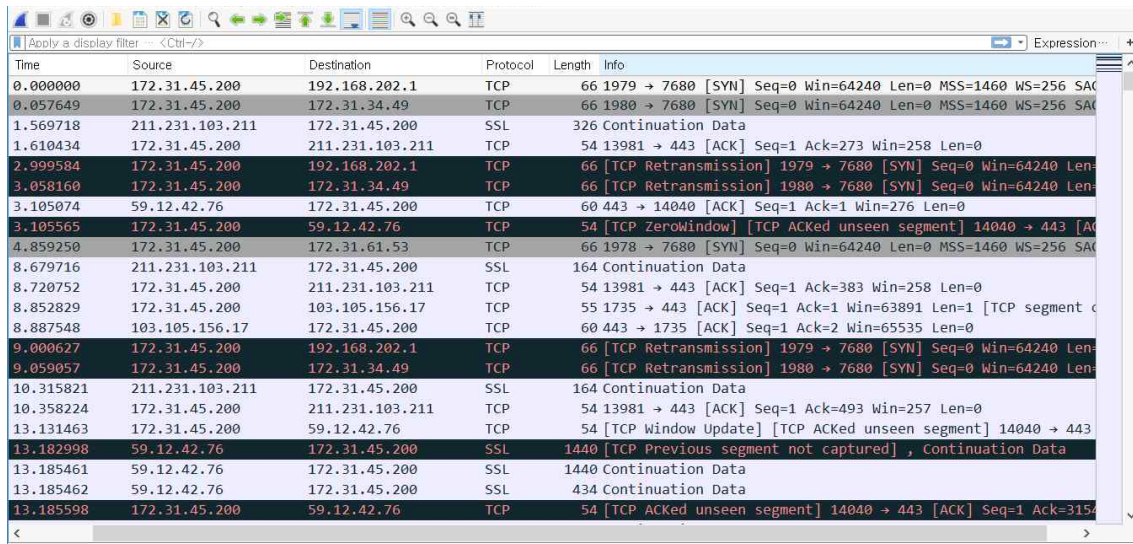




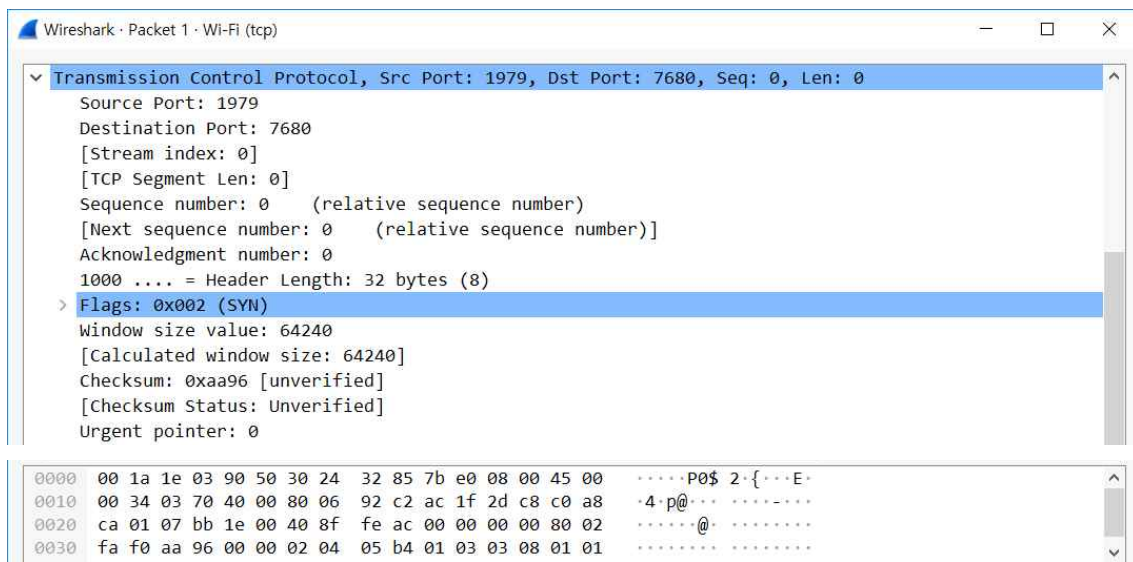
과목명	컴퓨터 네트워크
담당교수	조경산 교수님
학과	소프트웨어학과
학번	32153180
이름	이상민
제출일자	2019.06.05

## Chapter 25~26

1. Capture various Ethernet frames using Wireshark, and explain fields in the Ethernet, IP, and TCP header of SYN packet (Explain fields in the TCP header) and FIN packet



Time	Source	Destination	Protocol	Length	Info
0.000000	172.31.45.200	192.168.202.1	TCP	66	1979 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
0.057649	172.31.45.200	172.31.34.49	TCP	66	1980 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
1.569718	211.231.103.211	172.31.45.200	SSL	326	Continuation Data
1.610434	172.31.45.200	211.231.103.211	TCP	54	13981 → 443 [ACK] Seq=1 Ack=273 Win=258 Len=0
2.999584	172.31.45.200	192.168.202.1	TCP	66	[TCP Retransmission] 1979 → 7680 [SYN] Seq=0 Win=64240 Len=0
3.058160	172.31.45.200	172.31.34.49	TCP	66	[TCP Retransmission] 1980 → 7680 [SYN] Seq=0 Win=64240 Len=0
3.105074	59.12.42.76	172.31.45.200	TCP	60	443 → 14040 [ACK] Seq=1 Ack=1 Win=276 Len=0
3.105565	172.31.45.200	59.12.42.76	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 14040 → 443 [ACK]
4.859250	172.31.45.200	172.31.61.53	TCP	66	1978 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
8.679716	211.231.103.211	172.31.45.200	SSL	164	Continuation Data
8.720752	172.31.45.200	211.231.103.211	TCP	54	13981 → 443 [ACK] Seq=1 Ack=383 Win=258 Len=0
8.852829	172.31.45.200	103.105.156.17	TCP	55	1735 → 443 [ACK] Seq=1 Ack=1 Win=63891 Len=1 [TCP segment c
8.887548	103.105.156.17	172.31.45.200	TCP	60	443 → 1735 [ACK] Seq=1 Ack=2 Win=65535 Len=0
9.000627	172.31.45.200	192.168.202.1	TCP	66	[TCP Retransmission] 1979 → 7680 [SYN] Seq=0 Win=64240 Len=0
9.059057	172.31.45.200	172.31.34.49	TCP	66	[TCP Retransmission] 1980 → 7680 [SYN] Seq=0 Win=64240 Len=0
10.315821	211.231.103.211	172.31.45.200	SSL	164	Continuation Data
10.358224	172.31.45.200	211.231.103.211	TCP	54	13981 → 443 [ACK] Seq=1 Ack=493 Win=257 Len=0
13.131463	172.31.45.200	59.12.42.76	TCP	54	[TCP Window Update] [TCP ACKed unseen segment] 14040 → 443
13.182998	59.12.42.76	172.31.45.200	SSL	1440	[TCP Previous segment not captured] , Continuation Data
13.185461	59.12.42.76	172.31.45.200	SSL	1440	Continuation Data
13.185462	59.12.42.76	172.31.45.200	SSL	434	Continuation Data
13.185598	172.31.45.200	59.12.42.76	TCP	54	[TCP ACKed unseen segment] 14040 → 443 [ACK] Seq=1 Ack=315



Wireshark · Packet 1 · Wi-Fi (tcp)	
Transmission Control Protocol, Src Port: 1979, Dst Port: 7680, Seq: 0, Len: 0	
Source Port: 1979	
Destination Port: 7680	
[Stream index: 0]	
[TCP Segment Len: 0]	
Sequence number: 0 (relative sequence number)	
[Next sequence number: 0 (relative sequence number)]	
Acknowledgment number: 0	
1000 .... = Header Length: 32 bytes (8)	
Flags: 0x002 (SYN)	
Window size value: 64240	
[Calculated window size: 64240]	
Checksum: 0xaa96 [unverified]	
[Checksum Status: Unverified]	
Urgent pointer: 0	
0000 00 1a 1e 03 90 50 30 24 32 85 7b e0 08 00 45 00 .....P0\$ 2·{...E·	
0010 00 34 03 70 40 00 80 06 92 c2 ac 1f 2d c8 c0 a8 ·4·p@... .....	
0020 ca 01 07 bb 1e 00 40 8f fe ac 00 00 00 00 80 02 .....@· .....	
0030 fa f0 aa 96 00 00 02 04 05 b4 01 03 03 08 01 01 ..... .....	

ISN(Initial Sequence Number)은 408ffeac (random number)이다.

SYN packet이므로 acknowledgement number는 00000000이다.

Header length는 32byte이고, Code bit는 전부 NOT set, window size는 64240이다.

Urgent pointer는 0으로 없다.

2. Explain how we can get reliable transfer through unreliable protocol UDP

-> UDP에서 checksum은 header, payload 그리고 pseudo header에 적용된다. pseudo header에는 IP source address, IP destination address, UDP length 등이 들어 있다. pseudo header는 이러한 항목의 정보뿐만 아니라 IP에 의해 packet이 잘못 전송되는 것과 데이터의 분실을 검사해준다.

3. The following is a dump of a UDP header; 0045DF0000580000

1) Is the packet directed from a client to a server or vice versa?

-> UDP source port number : 00 (00000000)

UDP destination port number : 45 (01000101)

따라서 처음 부팅한 내 컴퓨터가 DHCP server에게 보내는, 즉 client가 server에게 보내는 packet이다.

2) What is the length of the data?

-> UDP length : DF (11011111) => 223byte / UDP header : 8byte

따라서 data 길이는  $223 - 8 = 215$ byte이다.

3) How the sender handled checksum for this packet?

-> UDP header contains a 16bit field named UDP checksum  
includes extra pseudo header that contains IP addresses

4. In TCP, how many sequence numbers are consumed by each segments?

a. SYN          b. ACK          c. FIN, ACK          d. PSH, ASK (data - 100bytes)

-> SYN :  $N+1$  / ACK :  $N+A$  / FIN, ACK :  $N+A$  / PSH, ASK :  $N+A$

(N : 이전 packet의 header size, A : 이전 packet의 payload size)

5. The intruder sends a SYN segment to the server using 철수's IP address. Can the intruder create a TCP connection with the server by pretending that he is 철수? Assume that the sever uses 1) a different ISN(Initial Sequence Number) for each connection or 2) the same ISN for each connection

-> ISN(Initial Sequence Number)을 같은 숫자로 하면 송신자를 spoofing 할 수 있다. spoofing은 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크 상에서 허가된 주소로 가장하여 접근 제어를 우회하는 공격 행위이다. 그러면 수신자는 SYN, ASK packet을 송신자의 IP 주소로 보낸다.

6. Following is the output from netstat command

Proto	Local Address	Foreign Address	State
TCP	192.13.201.215:1059	0.0.0.0:0	LISTENING
TCP	192.13.201.215:61032	211.234.249.226:1524	TIME_WAIT
TCP	192.13.201.215:62029	211.233.16.71:80	ESTABLISHED

1) Explain the values of state - LISTENING, ESTABLISHED, TIME\_WAIT

-> LISTENING : client로부터 연결을 기다리는 상태이다.

ESTABLISHED : client와 연결된 상태이다.

TIME\_WAIT : FIN packet을 받고 그에 대한 응답으로 ACK packet을 보내고 이 상태가 되는데, 한참 기다리다가 close 된다.

2) Is 192.13.201.215:1059 server or client?

-> 이 주소의 port number가 1059이므로 server이다.

3) Explain "21.240.16.226:80" in Foreign Address in two parts

-> IP address : 21.240.16.226

port number : 80

IP address와 port number를 통해 communication이 가능하다.

7. An HTTP client opens a TCP connection using an ISN of 100 and port number of 50,000. The server opens the connection with an ISN of 200. If the client defines receive buffer of 1024 and the server defines receive buffer of 4096, show the header of 2<sup>nd</sup> segment during the connection establishment. Ignore the calculation of checksum field

-> source port : sender address

destination port : receiver address

sequence number : 100

header length : 100/20byte = 5

code bits : ACK, PSH - 1 / 나머지 - 0

window : 1024

8. Explain flow control, congestion control, and SYN flooding

-> flow control : end-to-end communication 간 트래픽 용량이 초과하지 않도록 제어

congestion control : 네트워크 내에서 트래픽 용량이 초과하지 않도록 제어

SYN flooding : client가 packet을 계속적으로 보내고 ACK packet을 보내지 않으면 server는 RAM 공간을 계속 확보해둔 상태에서 대기하게 된다. 이 상태 그대로 둔다면 RAM을 모두 차지해버려 더 이상 연결을 받아들일 수 없는 상태가 된다.

9. Compare the TCP header and the UDP header. List the fields in the TCP header that are not part of the UDP header, and list the fields in the UDP header that are not part of the TCP header. Give the reason for each missing field

-> TCP header에는 있고 UDP header에는 없는 부분 : sequence number, acknowledgement number, header length, code bits, window, urgent pointer

UDP header에는 있고 TCP header에는 없는 부분 : UDP message length,  
pseudo header

10. Which of UDP and TCP is better for the communication between DNS server and client. (consist of two packets DNS request, DNS reply)

-> TCP는 3-way handshake를 필요로 하기 때문에 UDP가 훨씬 빠르다. 또한 UDP를 사용하면 DNS server가 연결을 유지할 필요가 없다. UDP는 신뢰성이 낮긴 하지만 application layer를 통해 신뢰성을 추가할 수 있다.