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

>> SYN: N+1, ACK: N+A, FIN+ACK:N+A, ACK+data:N+A

2. 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 server uses 1) a different ISN(Initial Sequence Number) for each connection or 2) the same ISN for each connection.

>> 수신자가 전송받는 SYN패킷에 대해 SYN+ACK 패킷을 보내면 same ISN을 사용할 경우 패킷에 대답할 수 있지만 random ISN을 사용할 경우 대답할 수 없다.

3. Following is the output from netstat command.

Proto	Local Address	Foreign Address	State
TCP	192.13.201.215:1059	0.0.0.0:*	LISTEN
TCP	192.13.201.215:61032	211.234.249.226:59004	TIME_WAIT
TCP	192.13.201.215:62029	211.233.16.71:80	ESTABLISHED

1) Explain the values of state - LISTEN, ESTABLISHED, TIME_WAIT.

>> LISTEN - 연결 요구를 기다리는 상태
ESTABLISHED: 서로 연결이 수립된 상태
TIME_WAIT: 연결 종료되었지만 원격의 수신 보장을 위해 대기하는 상태

2) Is 192.13.201.215:61032 server or client?

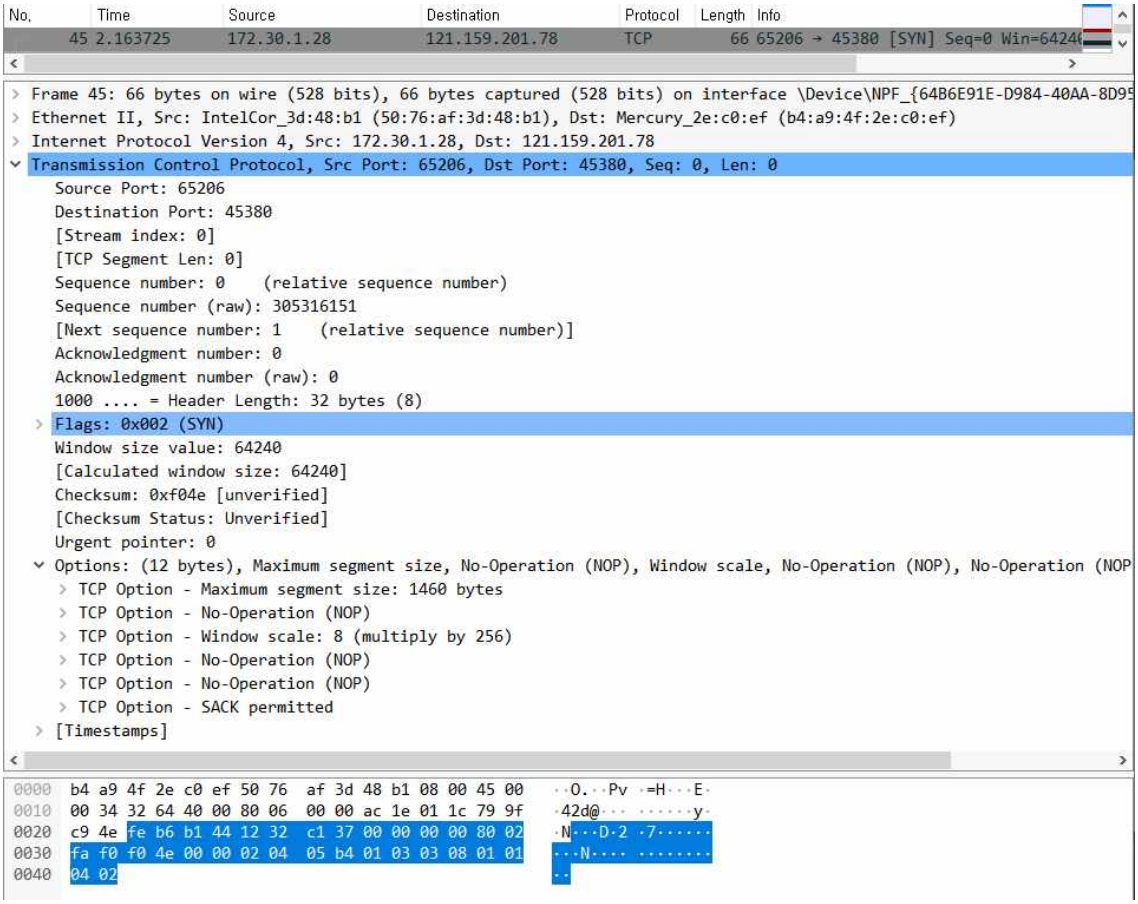
>> server (1059 포트)

3) Explain "219.240.16.226:80" in Foreign Address in two parts.

>> IP+Port(80:web), 해당 서버의 웹 포트와 연결이 수립된 상태(ESTABLISHED)

4. Capture various Ethernet frames using Wireshark and explain fields in the Ethernet, IP and TCP header.

>>



SYN segment이기 때문에

source(172.30.1.28:65206) : client / destination(121.159.201.78:45380) : server

인 것을 알 수 있다. 또 SYN segment이기 때문에 다양한 option들이 존재하는데 최대 패킷 크기를 나타내는 MSS(Maximum segment size)는 1460bytes임을 알 수 있고 Window sclae 즉 window의 size는 8임을 알 수 있다.

5. Run “netstat” command and explain the states of the process(server, client)

>>

```
C:₩Users₩showk>netstat

활성 연결

  프로토콜  로컬 주소          외부 주소              상태
  TCP    127.0.0.1:33915        DESKTOP-7LF8T0S:55960  ESTABLISHED
  TCP    127.0.0.1:33915        DESKTOP-7LF8T0S:64271  ESTABLISHED
  TCP    127.0.0.1:49671        DESKTOP-7LF8T0S:49672  ESTABLISHED
  TCP    127.0.0.1:49672        DESKTOP-7LF8T0S:49671  ESTABLISHED
  TCP    127.0.0.1:55960        DESKTOP-7LF8T0S:33915  ESTABLISHED
  TCP    127.0.0.1:64271        DESKTOP-7LF8T0S:33915  ESTABLISHED
  TCP    127.0.0.1:64337        DESKTOP-7LF8T0S:64338  ESTABLISHED
  TCP    127.0.0.1:64338        DESKTOP-7LF8T0S:64337  ESTABLISHED
  TCP    172.30.1.28:49469      40.90.189.152:https    ESTABLISHED
  TCP    172.30.1.28:64335      210.103.251.11:https   ESTABLISHED
  TCP    172.30.1.28:64343      121.53.203.203:https   ESTABLISHED
  TCP    172.30.1.28:64390      tk-in-f188:5228        ESTABLISHED
  TCP    172.30.1.28:64998      183.110.194.95:https   TIME_WAIT
  TCP    172.30.1.28:64999      121.53.205.229:https   TIME_WAIT
  TCP    172.30.1.28:65000      211.231.100.211:https  TIME_WAIT
```

40.90.189.152 서버의 https port와 연결이 수립된 상태

183.110.194.95 서버의 https 포트와 연결 종료되었지만 원격의 수신 보장을 위해 대기하는 상태