TCP 통신을 죽여봅시다

는 사실 가짜 제목입니다. 정확한 제목은

TCP 통신 자살(을 가장한 타살)시키기

ZeroPage 31기 김도엽

1시간짜리 목차

- TCP 소개
- Packet Injection
- packet 구성
- 원리 설명
- 코드 레벨 구현 방법

보험 하나만 깔게요

가르치신 분은 정석(정파, 무림맹)으로 해주셨는데, 제가 야매(사파, 마교)로 습득함

+

오늘 할 설명들도 기초를 야매로 때우고 넘어감

=

말 끊어도 되니까 질문 많이 해주세요

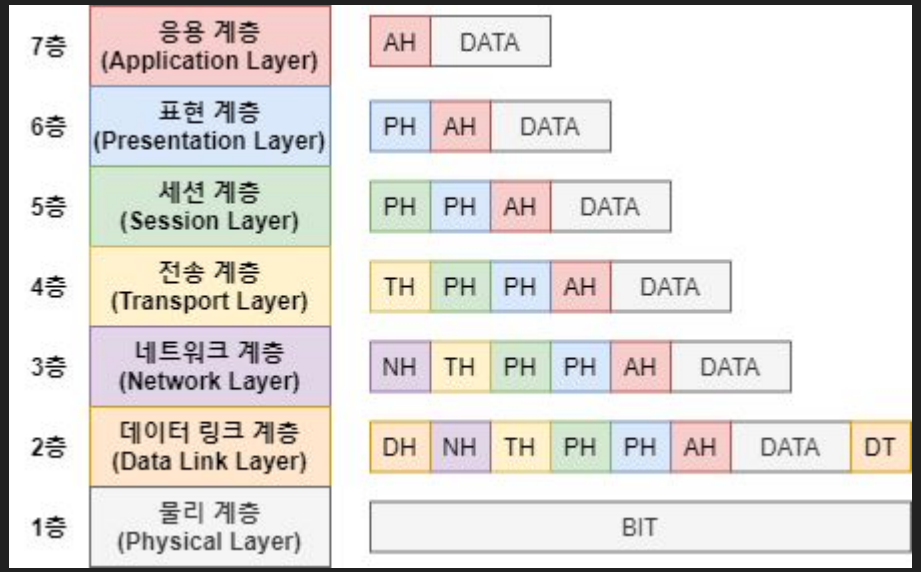
TCP?

Transmission Control Protocol

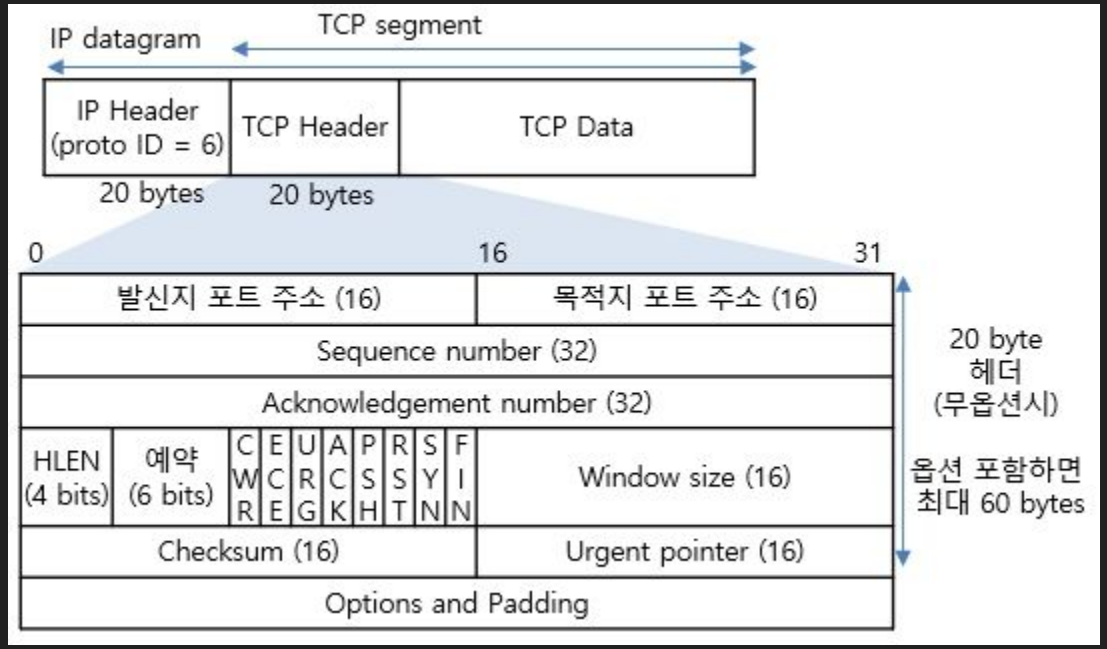
전송 제어 프로토콜

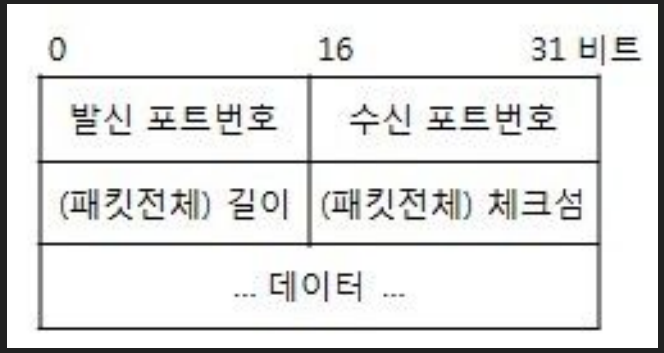
OSI 7계층 중 4층, 전송 계층에 해당

★신뢰성 있는 연결을 지향★



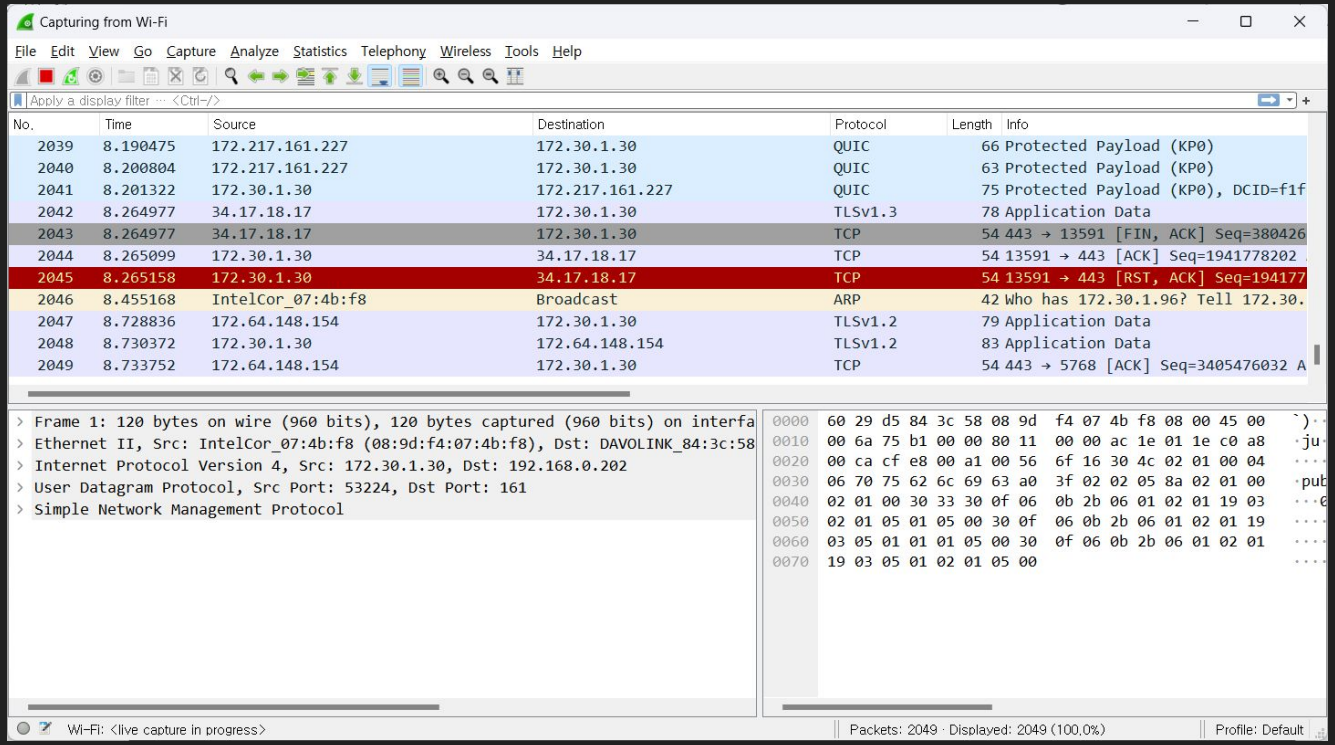
TCP vs UDP


IP datagram
TCP segment
IP Header (proto ID = 6)
TCP Header
TCP Data
20 bytes
20 bytes
0
16
31
발신지 포트 주소 (16)
목적지 포트 주소 (16)
Sequence number (32)
Acknowledgement number (32)
HLEN (4 bits)
예약 (6 bits)
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Window size (16)
Checksum (16)
Urgent pointer (16)
Options and Padding
20 byte 헤더 (무옵션시)
옵션 포함하면 최대 60 bytes

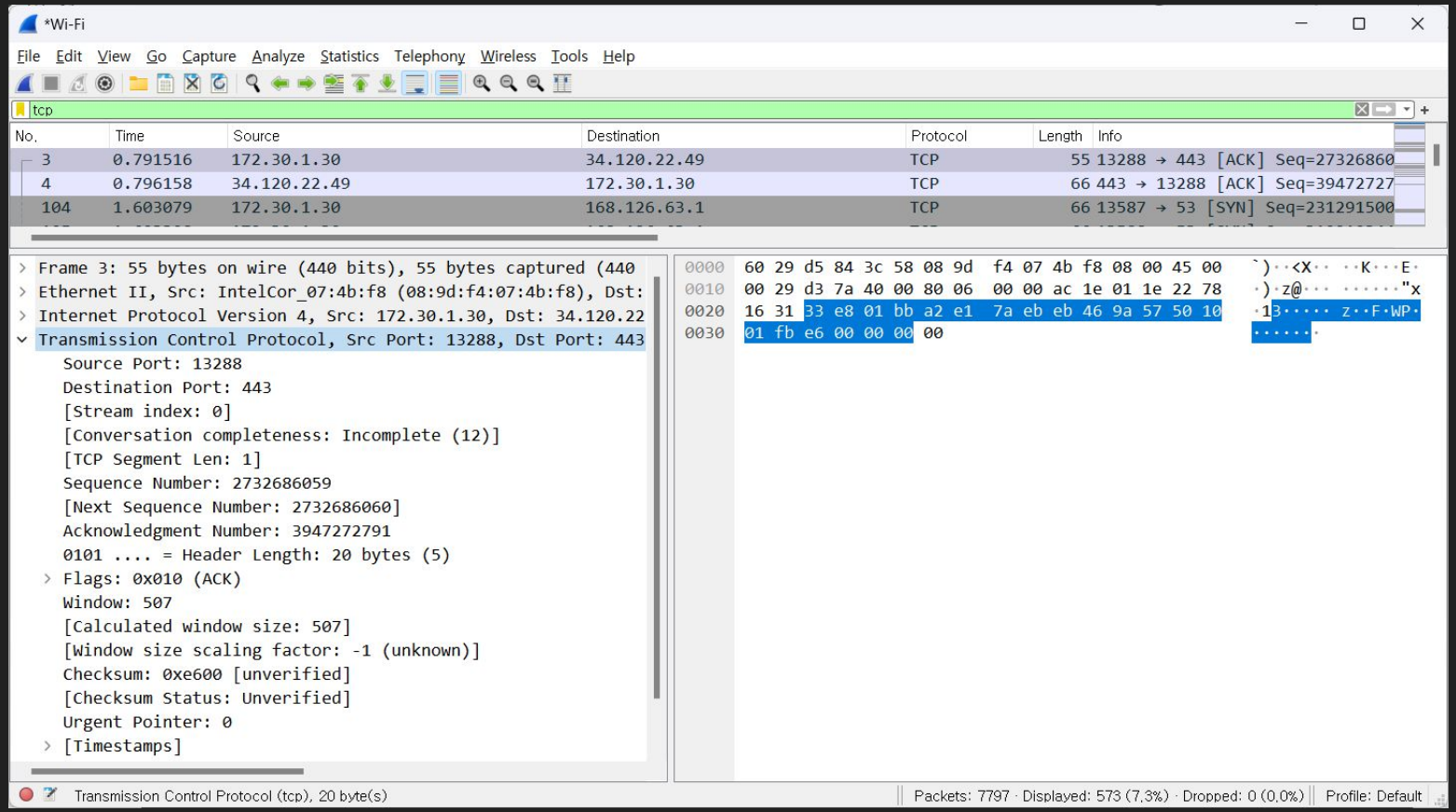

0
16
31 비트
발신 포트번호
수신 포트번호
(패킷전체) 길이
(패킷전체) 체크섬
... 데이터 ...

역시 그림으로만 보면 몰라요

직접 까봅시다



Wireshark를 통해 보는 TCP 구조



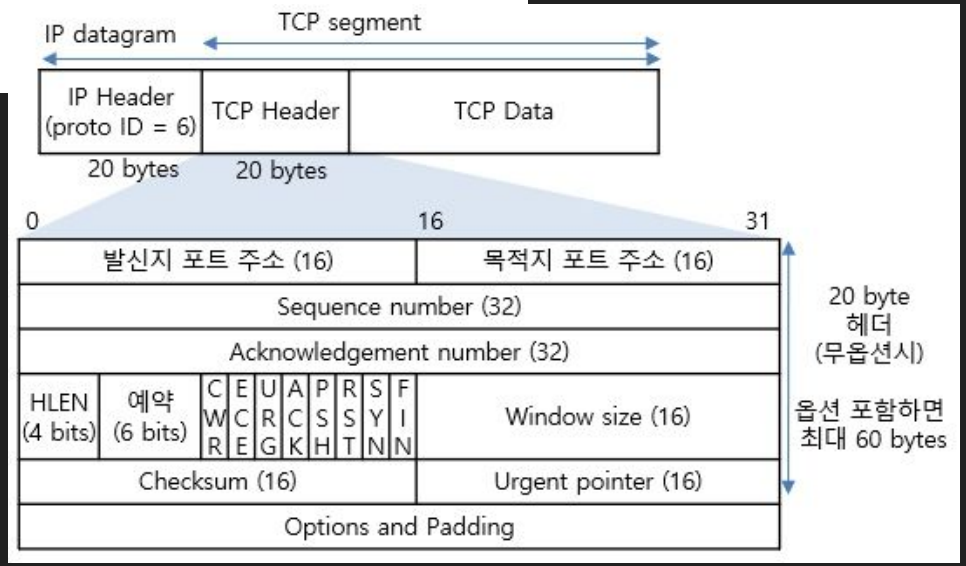
Wireshark를 통해 보는 TCP 구조

```
0000  60 29 d5 84 3c 58 08 9d  f4 07 4b f8 08 00 45 00
0010  00 29 d3 7a 40 00 80 06  00 00 ac 1e 01 1e 22 78
0020  16 31 33 e8 01 bb a2 e1  7a eb eb 46 9a 57 50 10
0030  01 fb e6 00 00 00 00
```

총 20바이트 구성

바이트 String으로 이루어져 있음

컴퓨터 메모리는 little-endian (host order)
패킷은 big-endian (network order)



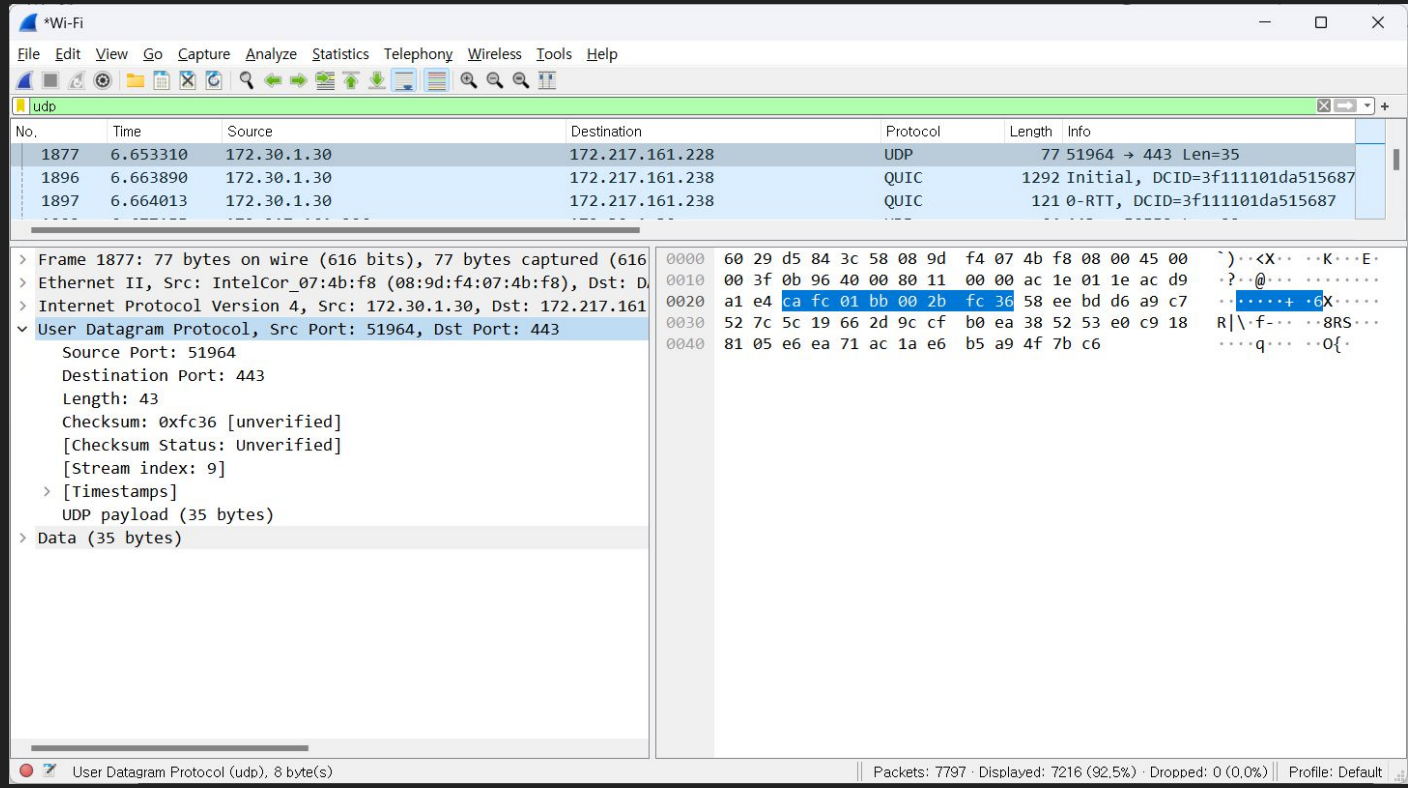
번외) 그럼 UDP는?

단 8바이트

포트 2개랑

패킷 길이

체크섬만 있으면 끗



그래서, 뭐 해야하는데

Packet Injection을 사용할 것. 잘 통신하던 둘한테 각각을 사칭해서 끔사리 끼기.

tcp 연결이 끊기는 피해자를 victim, 공격자를 attacker라고 하고
공격이 성공하기 위해 필요한 조건

1. packet sniffer
2. attacker가 victim에게 패킷을 보낼 수 있어야 함
3. seq, ack number가 정상처럼 보여야 함
4. checksum이 정확해야 함

누구한테 보내야하지

victim, server 둘 다 보내야 한다

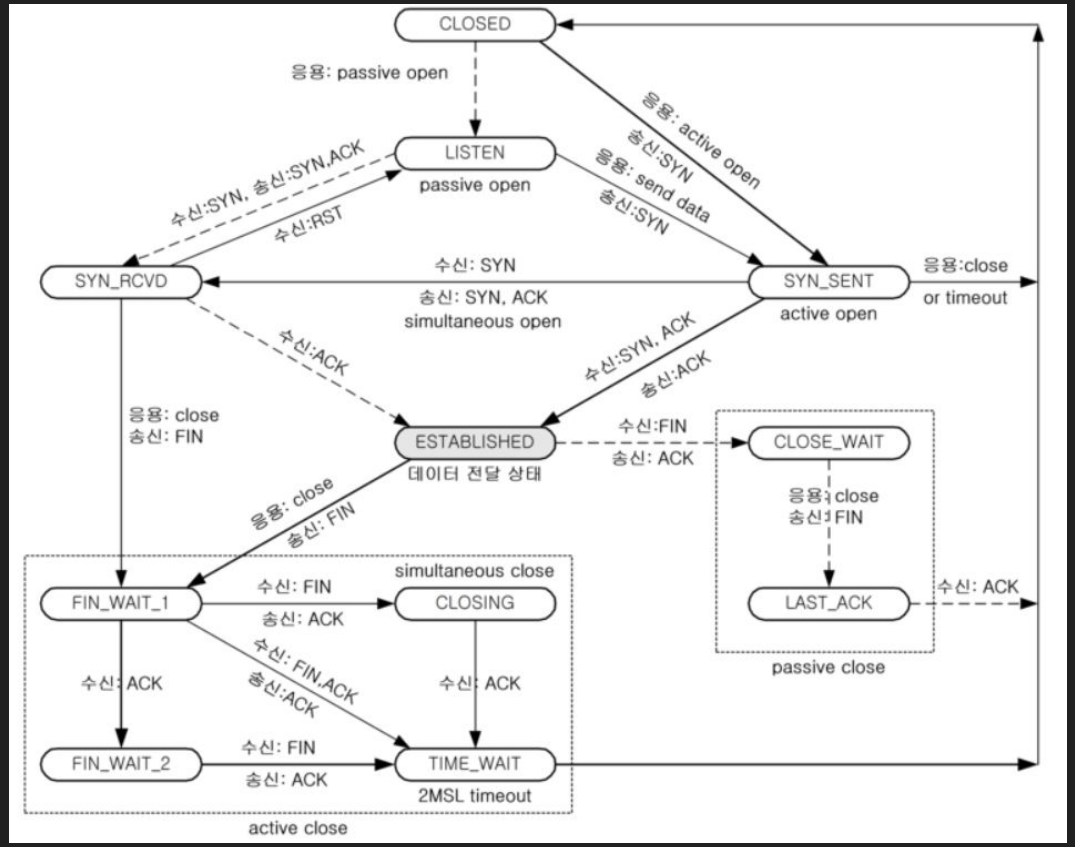
오른쪽은 'TCP 상태 전이도'

3 way handshake 연결 과정과

4 way handshake 연결 해제를

확인할 수 있는데

RST 패킷 하나면
죄다 CLOSED로 변화



구체적으로 패킷을 어떻게 만들어야 하죠

신경써야 하는 주요 필드 2가지

seq와 ack number

이 패킷이 제대로 된 순서를 지켰는지 + 주고받은 페이로드 크기가 정확한지 확인

checksum

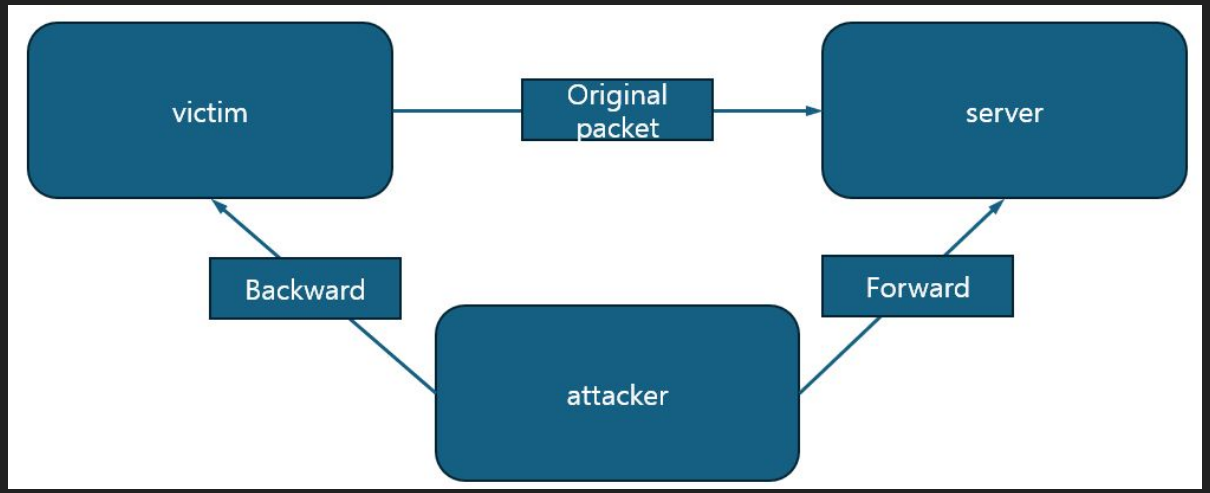
패킷에 네트워크 문제 등으로 발생한 오류가 있는지 탐지하기 위한 수.
우리는 임의로 패킷을 만들어서 보내기 때문에 따로 계산해줘야 됨.

구체적으로 패킷을 어떻게 만들어야 하죠

일단 패킷의 정의부터

original packet과 같은 방향의 패킷 = forward packet

“” 과 반대 방향의 패킷 = backward packet



구체적으로 패킷을 어떻게 만들어야 하죠

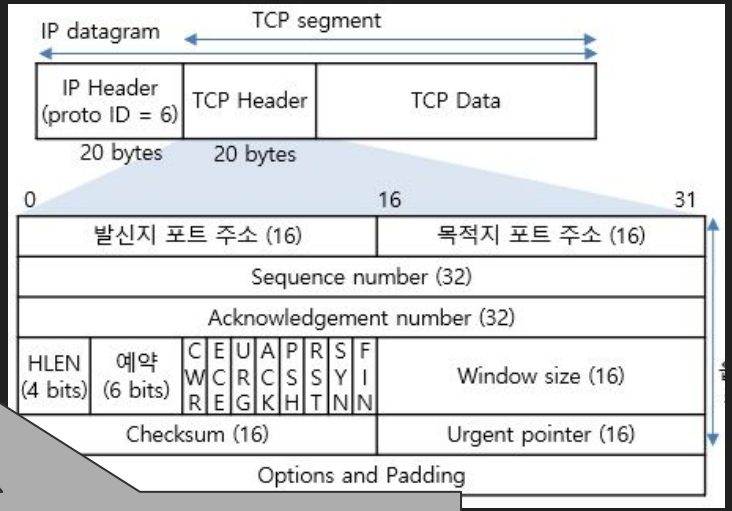
Forward와 Backward를 따로 구성해줘야 함

이 부분은 ethernet, ip, tcp 헤더의 구조와 각 필드의 역할을 알아야 할 수 있음

이번 시간에는 TCP 헤더 구성 방법만 알아봄

구체적으로 패킷을 어떻게 만들어야 하죠

필드명	Forward	Backward
port	src와 dst 동일하게	swap(src, dst)
seq number	seq + payload length	ack
ack	ack	seq
flag	RST flag on	
checksum	직접 계산	



server에 original packet이 도착하기 전에 RST 패킷을 보낸 것으로 가정

근데 왜 이게 성공하는 거임?

이론상 server가 다시 패킷을 보내는 시간보다

같은 라우터 안에서 쏘는 내 패킷이 client한테 먼저 도착함

그러면 내 패킷을 신뢰하고 나중에 오는 server의 패킷은 drop하게 됨

이는 후술할 warning.or.kr 사이트에도 적용되는 이야기

코드 레벨로 구경하러 가볼까요

https://github.com/bob12vpn/vpn-hater

(스타 누르지 마세요)

왜 제목을 그렇게 정했을까

오늘의 진짜 제목 : TCP 통신 자살(을 가장한 타살)시키기

client 시점 -> 서버가 RST 보냈네. 연결 끊어야지.

server 시점 -> 클라이언트가 RST 보냈네. 연결 끊어야지.

FIN flag도 사용할 수 있으나, 부득이하게 이 방법은 사용해보지 않아서 RST로 소개하였음.

Packet Injection은 어디서 사용되고 있는가

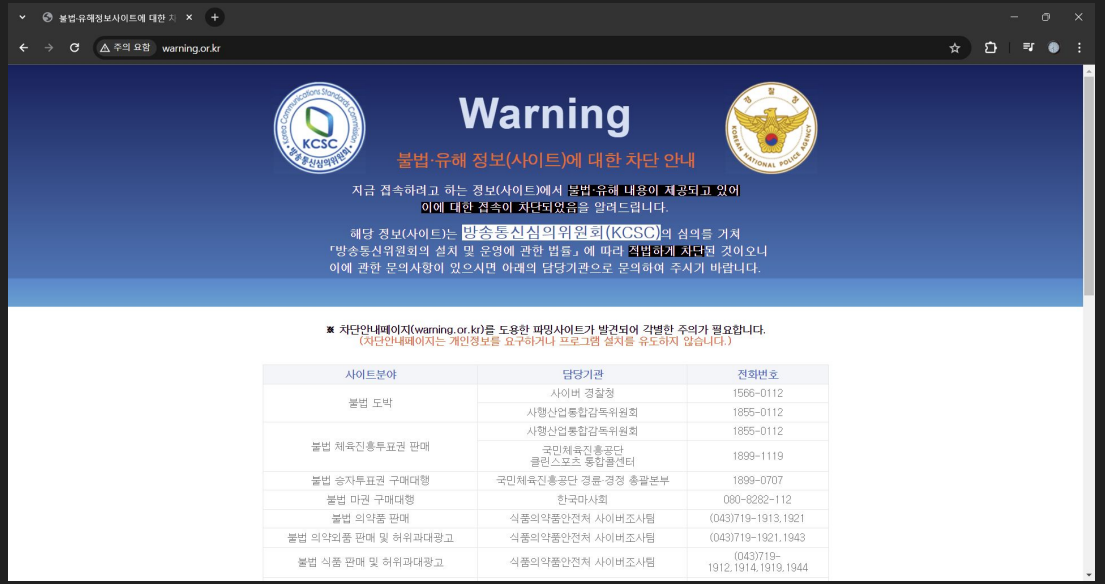
유해 사이트 접속 시 해당 사이트 정보를 받기 전에

먼저 packet을 보내서 warning.or.kr 페이지를 띄워버림

당연히 외국보다는

국내에서 쏜 패킷이

먼저 도달하기 때문



마무리

질문 받습니다

출처

- https://huimang2.github.io/etc/iso-standard-7498
- http://www.ktword.co.kr/test/view/view.php?m_temp1=1889
- https://velog.io/@kimyeji203/%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC-TCPUDP