네트워크 WireShark 활용

■ 네트워크 개론
패킷
패킷이란 컴퓨터 간에 데이터를 주고 받을 때 네트워크를 통해 전송되는 데이터 전송 단위(작은 조각)이다.
용량이 큰 데이터를 전송할 때는 작게 나누어서 보내는 것이 규칙이다.
패킷으로 나누는 이유
통신선에서 보낼 수 있는 최대의 크기가 정해져 있음.
잘라서 보내야 함
어셈블(분해) 디셈블(조립)통해서 패킷을 주고 받음
세그먼트 프레임이라고도 표현함

OSI 7 계층 통신 규약 표준을 만들어서 사용하기 위해 사용
물리계층
데이터링크 계층 맥어드레스로 인식
네트워크 계층
전송 계층
세션 계층
표현 계층
응용 계층

아날로그와 디지털
아날로그는 연속적인 형태
디지털 전기가 없으면 작동 하지 않음
주파수 : Hz
1초에 한 사이클을 1Hz로 정의
주파수는 아날로그 주파수와 디지털 주파수가 있음

클록(클럭) 주파수
데이터 전송할 때에 동기화(타이밍)을 맞추어야 함.

대역폭(BandWidth)
최고 주파수와 최저 주파수의 차이

헤더 페이로드 제어요소 등을 포함하는 데이터 세그먼트가 패킷
헤더 : 편지의 보내는 사람 주소 받는 사람 주소 우표 등 정보들이 찍혀 있다. 네트워크에서는 헤더라고 한다.
트레일러 : 에러 정보들이 포함되있음
페이로드 : 실제 데이터 정보

| port | IP | Mac address | data | 정보
| 헤더 | 페이로드 | 트레일러

■ 네트워크 구성
컴퓨터 전송매체 접속 장치
전송매체(Serial, 동축케이블 등)
LAN MAN WAN

LAN 카드 = NIC(Network Interface Card) = Ethernet

● 허브(분배기)
더미허브와 스위칭허브로 나뉨
스태커블 허브

스위치
브릿지

게이트웨이
중계기(Repeater)
라우터

망의 형태
랜은 구성할 때 성형 링형 버스형 매쉬형(망형)으로 랜 구성

브로드밴드(아날로그)
베이스밴드(디지털)
10Base-T : 10Mbps의 디지털 통신의 Twisted-pair(꼬임선)

■ 통신 방식
서버와 클라이언트

유니캐스트 브로드캐스트 멀티캐스트

유니캐스트 1:1 통신 방식
브로드캐스트 1:다 통신 방식
멀티캐스트 1:그룹 통신 방식

Broadcast에서 MAC Address는 FF-FF-FF-FF-FF-FF로 미리 정해짐.
(IP에서 Broadcast는 서브넷 비트수에 따라 달라짐)

베이스밴드 방식
이더넷이 대표적이다. 디지털 신호
브로드밴드 방식
아날로그 신호 주파수로 신호 AM FM TV

■ 이더넷
1977년 제록스에서 동축케이블을 사용하여 10Mbps 전송속도를 지원할수 있는 이더넷 개발 하여 1985년 표준화하여 빠르게 확산됨.

고속 이더넷 : 100Base-T

FDDI : 백본망에서 주로 사용함.

■ OSI 참조 모델
4계층으로 만든 것을 TCP/IP 모델이라고 함

ISO OSI 7 계층모델
IEEE TCP/IP 모델
IEEE 802.11 와이파이

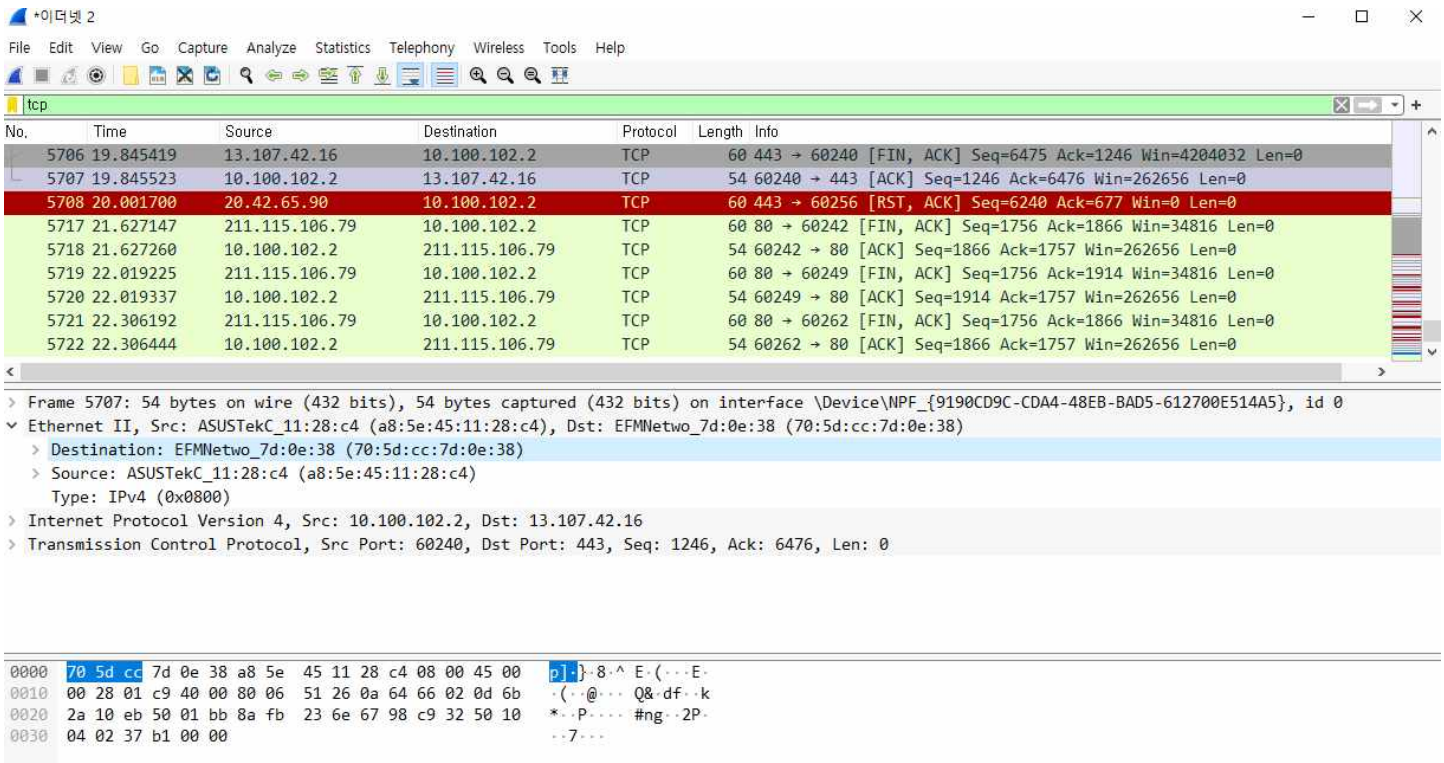
ISO OSI(Open System Interconnection) 모델
개방형 시스템 = 오픈 시스템 끼리 상호 연결하기 위한 규칙을 만듬.
물리, 데이터 링크, 네트워크 전송 = 하위 계층
세션, 표현, 응용 = 상위 계층

Ethernet II 데이터링크 계층
응용계층 = 서비스
표현계층 = 프로토콜 / 암.복호화
세션계층 = 포트번호 사용 연결 상태(연결설정에 관한 일을 함)

헤더를 붙여서 통신을 하는데 데이터링크 계층에서는 헤더에 트레일러 붙여서 통신을 함

TCP/IP 모델
IEEE에서 제정
ISO OSI 7 Layer와의 차이점
1(물리), 2(데이터 링크)계층 → 네트워크 접속 계층
3계층(네트워크 계층) 같음
4계층(전송 계층) 같음
5(세션), 6(표현), 7(응용) 계층 → 응용 계층

◆ Wireshark 활용하여 OSI 2계층(데이터링크 계층) 구조(Ethernet II Dump) 파악하기



● MAC(물리) 주소

6Byte = 48bit로 구성

앞의 3개는 밴드명(제조회사) 뒤의 3개 시리얼로 구성됨

ex) d4:5d:64:48:52:22

모든 컴퓨터에는 arp 테이블이 있음

(cmd창에서 arp –a로 확인 가능)

arp 프로토콜 = 인터넷 주소 + MAC주소

즉, 모든 컴퓨터에는 인터넷 주소와 MAC주소를 가지고 있음

ping 10.100.102.15를 입력하면 arp 테이블로 가서 MAC주소를 찾음

스위치에는 스위칭 테이블(포트 번호와 MAC Address)이 있음

OSI 2계층 데이터링크에서 사용하는 대표적인 프로토콜이 Ethernet II

ping → ICMP(3계층 데이터)

같은 네트워크 대역끼리는 SW를 통해서 연결되어 있음.

Ethernet II 출발지 MAC, 도착지 MAC, 타입으로 구성

14 Byte(6+6+2)로 구성

◆ 경로 테이블(라우팅 테이블) 확인하기

cmd → route print

MAC주소는 네트워크를 벗어날 수 없음.

도착지 MAC,출발지 MAC, Type → Header

패킷+헤더+트레일러 → 물리계층으로 보냄

데이터링크계층 (OSI Layer 2 계층)에서 하는 일
주소 지정, 순서 제어, 흐름 제어, 오류 처리, 프레임, 동기화, 데이터 링크 설정

```
[root@localhost ~]# ip a s ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group de
fault qlen 1000
    link/ether 00:0c:29:78:7a:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.100/24 brd 192.168.100.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::d089:76a5:6e39:6eff/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

○ MTU? 전송크기를 나타냄
네트워크 계층까지의 전송크기(MTU 1500 = 1480+20)
데이터링크 계층까지의 전송크기 MTU 1480+20+14 => 1514

데이터 링크 계층의 규칙
이더넷 헤더
→ 도착지 MAC 주소, 출발지 MAC 주소, 유형(타입) 6+6+2 = 14바이트

```
Type: IPv4 (0x0800)
```

◆ 프로토콜 타입
0800 = IPv4
0806 = ARP
8035 = RARP
814C = SNMP over Ethernet
86DD = IPv6

★ 스위치는 MAC주소를 학습을 한다.

LG bit와 IG bit

```
Destination: EFMNetwo_7d:0e:38 (70:5d:cc:7d:0e:38)
    Address: EFMNetwo_7d:0e:38 (70:5d:cc:7d:0e:38)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: ASUSTekC_11:28:c4 (a8:5e:45:11:28:c4)
    Address: ASUSTekC_11:28:c4 (a8:5e:45:11:28:c4)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

Globally unique address : 유일한 주소를 의미
factory default : MAC주소의 공장 기본값
0은 변조되지 않음을 의미

LG bit 공장에서 나온 그대로를 사용하고 있음을 나타냄
Multicast인지 Unicast인지 식별 하는 것이 IG bit

IG bit에서 Unicast일 때는 0으로 Multicast일 때는 1로 표시됨

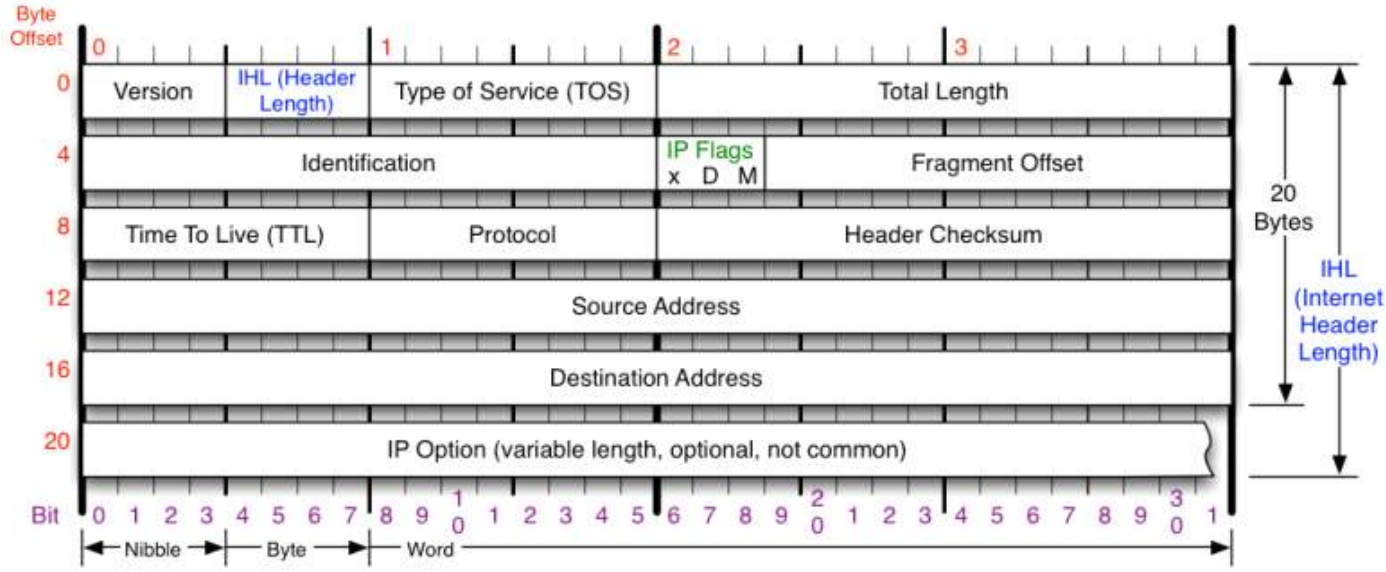
네트워크 보안에서 확인 할 때 아래 그림만 주고 네트워크 상태 파악하라고 함.

```
70 5d cc 7d 0e 38 a8 5e  45 11 28 c4 08 00
```

70 5d cc : Destination MAC Address

7d 0e 38 : Source MAC Address

08 00 : Type(IPv4)



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

패킷 4바이트 단위로 잘라서 표시함.