

<Global Header>

D4 C3 B2 A1 : magic number. pcap파일 포맷이기 때문에 저 값을 갖는다.

02 00 : major version number

04 00 : minor version number

00 00 00 00 : GMT to local correction

00 00 00 00 : accuracy of timestamps

00 00 04 00 : max length of captured packets, in octects 실제 수집된 패킷 길이.

01 00 00 00 : data link type. 1값이 세팅되었으므로 Ethernet임을 알 수 있다.

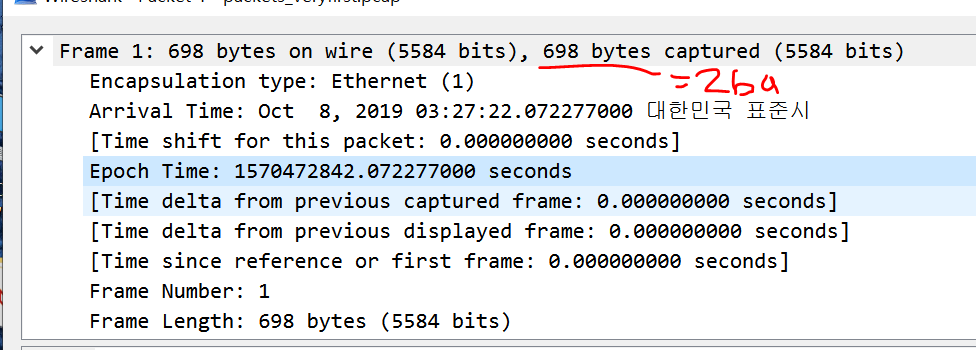
<Packet Header>

8A 83 9B 5D : timestamp seconds. => Epoch time의 앞 10진수 부분.

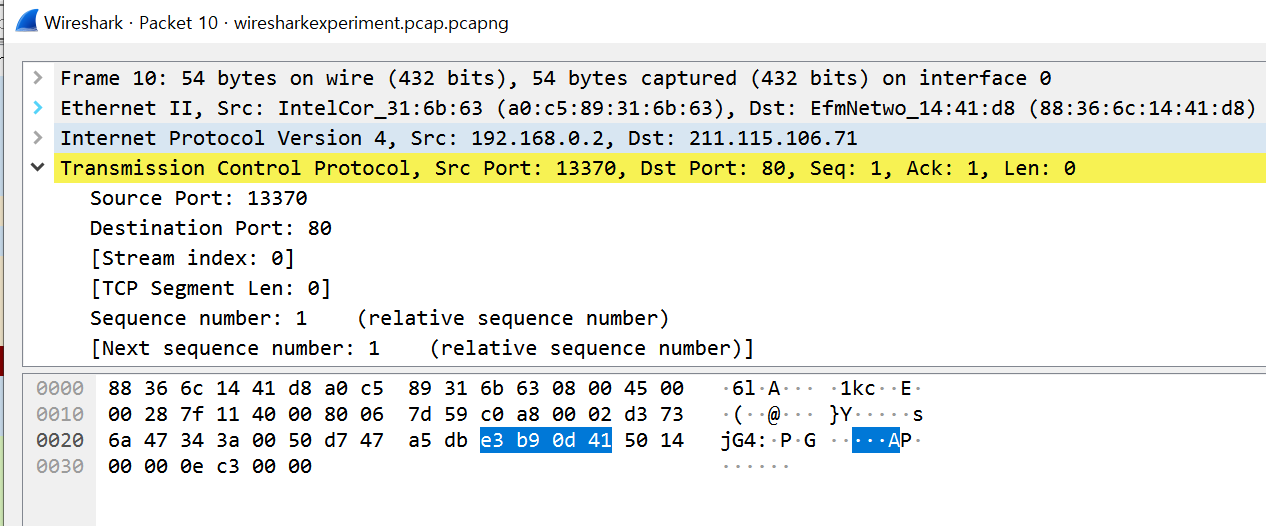
55 1A 01 00 : timestamp microseconds => Epoch time의 두 번째 자리 부분.

BA 02 00 00 : number of octets of packet saved in file => 와이어샤크의 capture length 부분.

BA 02 00 00 : actual length of packet => 와이어샤크의 frame length 부분.



* 검증!



88 36 6c 14 41 d8 : 목적지 MAC address

A0 c5 89 31 6b 63 : 발신지 MAC address

08 00 : 다음에 오는 프로토콜의 패킷 유형. IP프로토콜이므로 08 00이 온다.

45 : 4는 IP프로토콜의 버전인 4(Ver), 5는 헤더의 길이정보(IHL)

Type of Service : 00 사용되고 있지 않음.

Total length : . 00 28. 헤더와 데이터의 길이를 합한 값. 40을 16진수로 나타낸 값이다.

Identification : 7f 11

전송할 최대 사이즈를 초과하여 분할된 경우에 어떤 패킷에 소속되었는지를 나타내기 위한 고유번호이다. 만약 다른 패킷이 ID로 7f 11을 갖는다면 두 패킷은 본래 한 패킷이었다는 것을 알 수 있다.

40 00 : Flags 010, Don’t fragment. 분할된 패킷이 없다. Fragment Offset : 0, 분할된 경우 이 패킷은 첫 번째 조각. 이렇게 0 1 0 0 이 합쳐져서 ??? 40 00????

Time to live : 80. 패킷 수명을 제한한하기 위한 타이머.

Protocol : 06. IP헤더의 뒤에 올 상위 프로토콜을 지정하는 것. 이 경우엔 TCP(6).

Header Checksum : 7d 59. 이 체크섬 값을 이용해 수신 측에서 에러 발생 여부를 확인할 수 있게 한다.

Source Address : c0 a8 00 02. 송신자 IP주소를 16진수로 나타낸 것.

Destination Address : d3 73 6a 47. 수신자 Ip주소 값을 16진수로 나타낸 것.

34 3a : 송신자의 포트번호. 십진수로 13370

00 50 : 수신자 포트번호. 십진수로 80.

d7 47 a5 db : Sequence Number. 데이터의 순서를 나타내는 번호가 할당됨. 분할된 패킷이면 데이터 재조합에 사용됨.

E3 b9 0d 41 : Acknowledge number : 다음에 수신할 데이터 번호. 전체 데이터 중 몇 번째 데이터인지 파악.

50의 5 : Header Length. Offset으로, TCP 헤더의 길이.

50의 0 : Reserved. 예약된 필드. 0이므로 지금은 사용하지 않음.