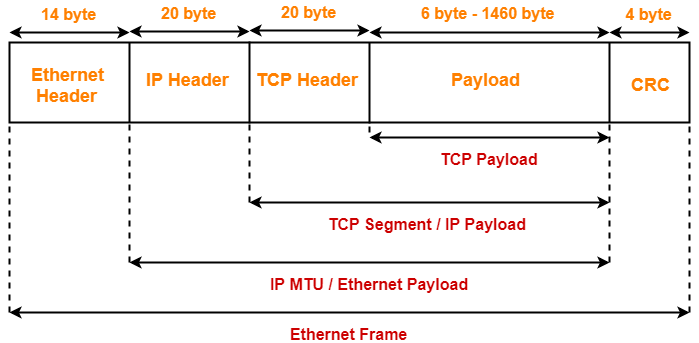
* Result for Packet sniffing



**①** Ethernet Header

1) Destination MAC 주소 → 00 : 00 : 00 : 00 : 00 : 00

2) Source MAC 주소 → 00 : 00 : 00 : 00 : 00 : 00

3) Type 08 00 → IP

**②** IP Header

1) Version(4) : IPv4

2) Header Length(5) : 5words (20bytes)

3) Type of Service(00)

4) Total Length : 003c → 60bytes

5) Identification : 89 3b → 1000 1001 0011 1011

6) Time to live(40) : 40

7) Protocol Type(00) : TCP

8) Header Checksum(40 06) : 0100 0000 0000 0110

9) Destination and Source IP Address : 7f.00.00.01, 7f.00.00.01 → 127.0.0.1, 127.0.0.1

**③** TCP Header

1) Source Port (e2 ca) : 58058 → Dynamic Ports

2) Destination Port (22 b8) : 8888

3) Sequence number(32bits) : 2f 05 f8 b4 → 00101111 00000101 11111000 10110100

- 송신 일련번호로, TCP는 세션별로 일련번호를 사용한다. 랜덤으로 생성되고, 전송 데이터의 각 바이트들을 순서대로 관리한다.

4) ACK(32bits) : 0000 0000

수신확인 일련번호로, 상대방으로부터 받기를 기대하는 일련번호이며, 시작과정에서 서버의 일련번호를 모르므로 0으로 채운다.

5) Header Length(4bits) : a → 1010

6) Reversed Field(6bits) : 0000 00

7) Control Flags(6bits) - URG : 0, ACK : 0, PSH : 0, RST : 0, SYN : 1, FIN : 0

SYN이 1이면 TCP 연결을 요청하는 SYN 신호를 보낸다.

8) Windows Size(16bits) : aa aa → 1010 1010 1010 1010

9) Cheksum(16bits) : fe 30 → 1111 1110 0011 0000

10) Urgent Point(16bits) : 00 00

**④** Data