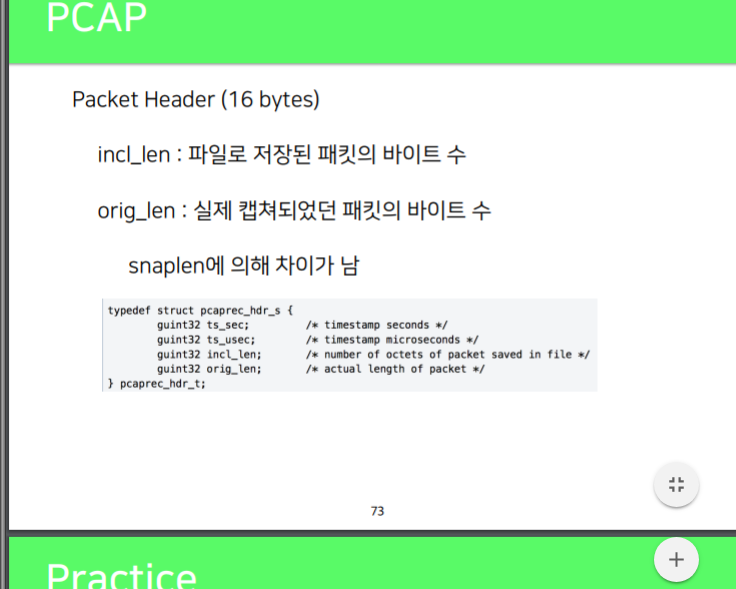


**24 + 16**

**1개의 패킷을 잡는다고 하였을 때 1개의 패킷 + 40 바이트가 된다.**

**Global 헤더**

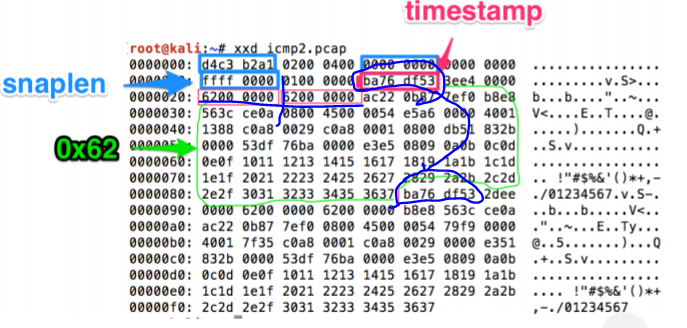
**패킷 헤더**

****

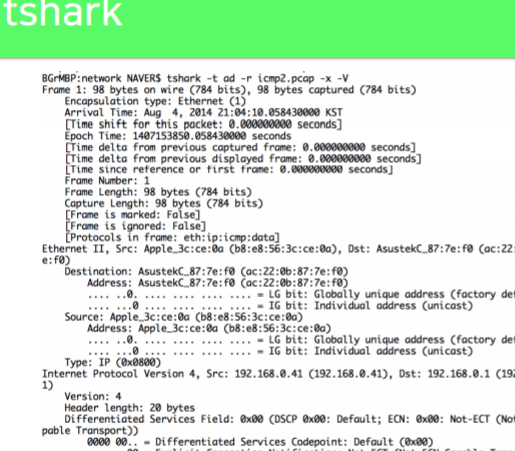
**-S 옵션을 준 경우 다르게 나온다**

**Timestamp는 1970년1월1일을 기준으로 …**

**인터넷에 치면 변환해주는 사이트가 많이 있다.**

****

**시간 단위로 패킷을 알 수 있다.**

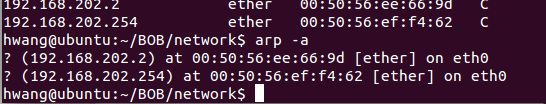
****

**tshark -t ad -r icmp2.pcap -x -V**

**ARP(Address Resolution Protocol)**

**게이트웨이**

**LAN에 있는 모든 노드들은 게이트를 거쳐 밖으로 나가야만 한다.**

****

**맥어드레스를 확인 할 수 있다.**

**컴퓨터가 IP주소를 뿌린다. 동일 IP를가진 노드가 MAC주소를 알려준다.**

**맥어드레스는 local에서 적용된다.**

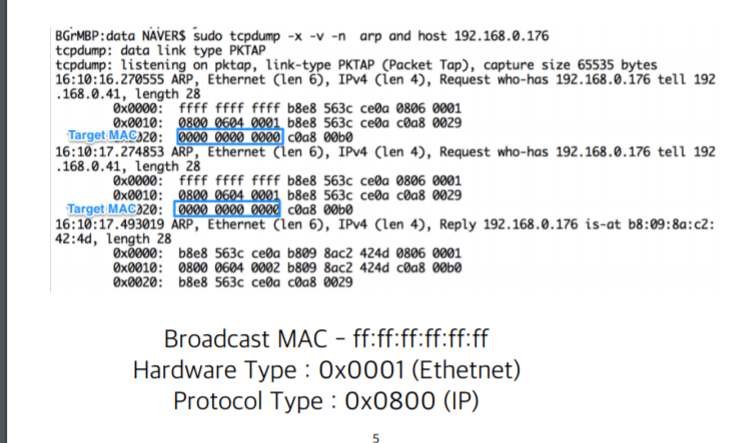
**구글로부터 http 응답을 받았다는 건**

**Destination 주소 부분이 엄청나게 변경되었다는 점이다.**

**스푸핑 공격은 같은 local내에서만 가능하다.**

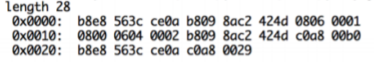
**맥주소를 바꿔서 하는 공격이니깐…**

**맥주소는 물리적으로 연결된 기기들끼리 .**

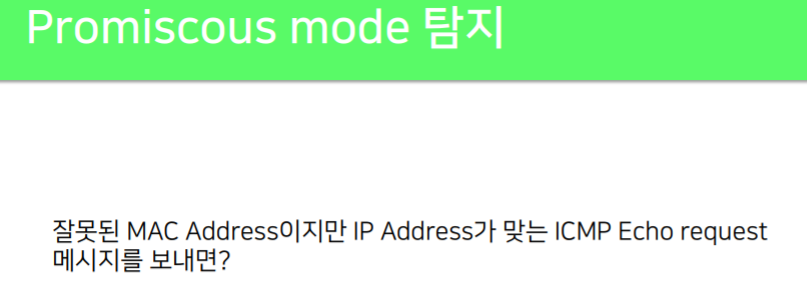
****

**0800 = ip**

**0806 = arp**

****

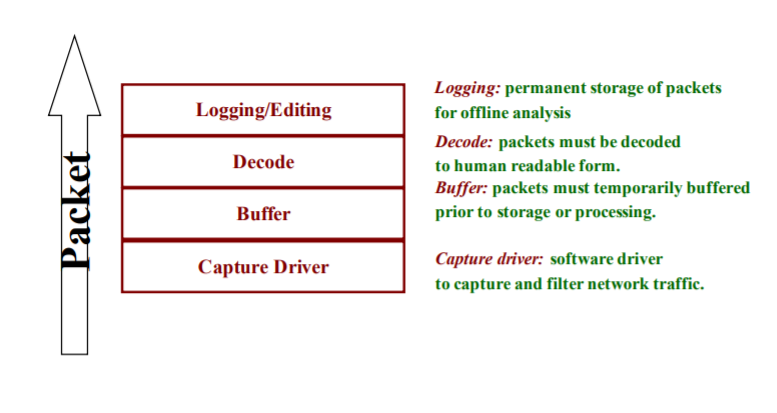
**1번째 줄과 3번째 줄에 같은 주소가 있다.**

****

**프리규어스 모드 = 모든 트래픽을 받는다.**

**잘못된 맥주소라도 IP가 같다면 그냥 받는다.**

**암호화 되어 있지 않으면 다 볼 수 있는 것이다.**

****

**버퍼의 크기가 제한 되어있기 때문에 개발할 떄 주의해야한다.**

**패킷 캡쳐를 통해서 복원할 수 있다.**

* **정리**

**맨 처음 destination 맥주소는 게이트웨이다.**

**ARP는 같은 물리적장소 내에서 적용된다(MAC주소를 바꾼다.)**

**라우터를 거칠 때마다 destination 맥주소는 업데이트 된다.**