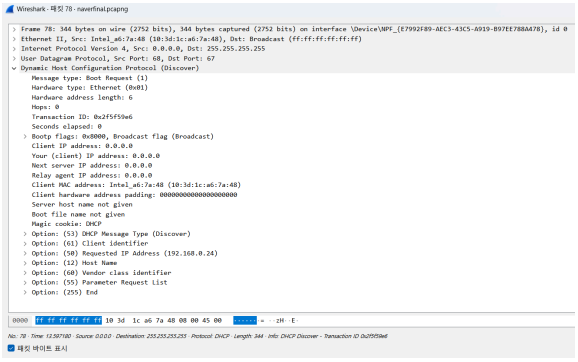
과제

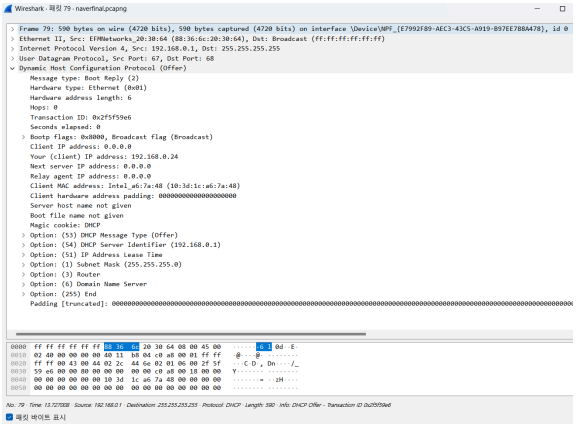
브라우저에서 www.naver.com 로 접속하는 과정을 분석

DHCP

Discover 패킷



Offer 패킷

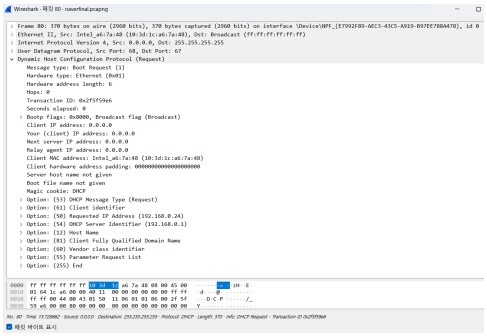


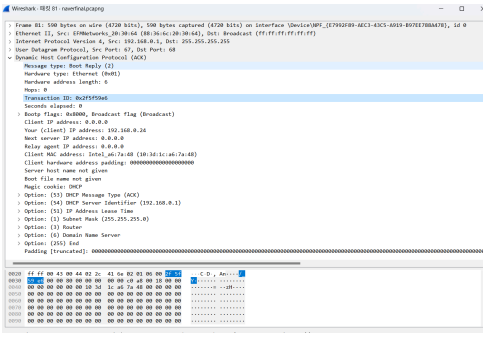
- 전송층 프로토콜로 UDP를 사용
- Message Type (1)으로 식별
- Discover 패킷의 필드는 비어 있음
- DHCP Message Type 필드는 유형 53인 옵션, 길이는 1, 값으로 1가짐

Offer

- 유효한 IP 주소를 전달함
- 아직 IP 주소를 가지고 있지 않으므로, 서버는 하드웨어 주소를 이용해 클라이언트와 통신을 시도함
- 메시지 유형: 응답
- 이전 패킷과 동일한 Transaction ID
- Client IP address 필드에 IP 주소 192.168.0.24을 제공함
- 패킷이 DHCP Offer임을 확인할 수 있음

Request **Acknowledgement**





- 아직 완전한 IP 주소 획득 절차를 완료하지 않음
- Destination이 Broadcast임
- 메시지 유형: 요청
- 새로운 요청/응답 트랜잭션이므로 새로운 transaction ID
- 패킷이 DHCP Request임을 확인할 수 있음

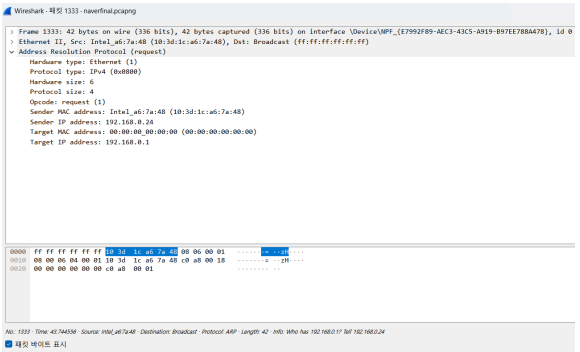
Acknowledge

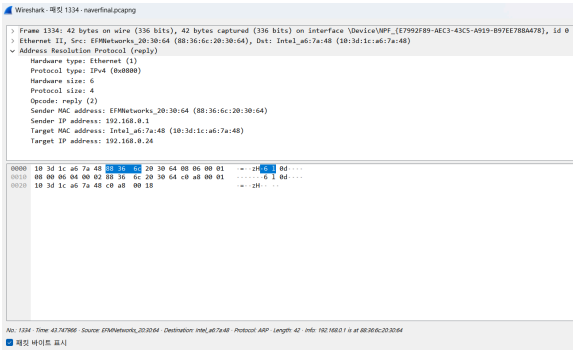
- DHCP 마지막 단계
- ACK 패킷을 클라이언트에 보내고 정보를 기록
- 클라이언트가 IP 주소를 가짐(192.168.0.24)

ARP

- 이더넷에서 탐색하므로 IP 프로토콜은 없음
- 게이트웨이의 IP주소에 대한 MAC 주소를 탐색함

요청 **응답**





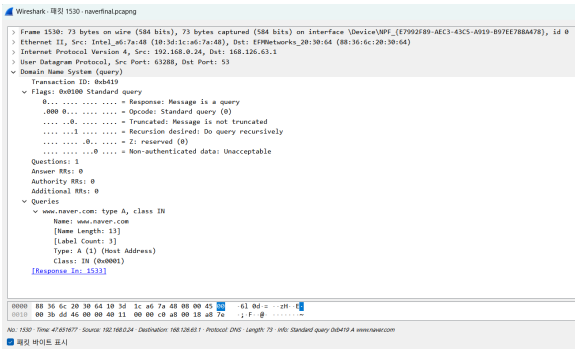
- Destination 필드가 Broadcast임: 패킷 바이트 정보 확인 시 'ff:ff:ff:ff:ff:ff'
- ARP 요청을 보내는 송신 PC의 MAC 주소는 내 컴퓨터의 MAC 주소: 10:3d:1c:a6:7a:48
- ARP 요청을 보내는 송신 PC의 IP 주소는 내 컴퓨터의 IP 주소: 192.168.0.24
- Target Mac address는 아직 아무것도 지정되지 않음
- Target IP address는 통신하고자 하는 IP 주소

응답

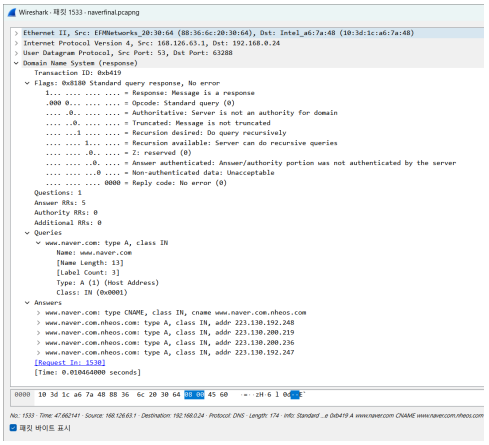
- ARP 요청을 보내는 송신 PC의 MAC 주소는 통신하고자 하는 위치의 MAC 주소: 88-36-6c-20-30-64
- ARP 요청을 보내는 송신 PC의 IP 주소는 통신하고자 하는 위치의 IP주소: 192.168.0.1
- Target Mac address는 내 컴퓨터의 MAC 주소: 10:3d:1c:a6:7a:48
- Target IP address는 내 컴퓨터의 MAC 주소: 192.168.0.24

DNS

조회 요청



조회 응답



- DNS 서버로 조회를 요청
- DNS 서버 주소값은 168.126.63.1: IP 프로토콜에서 확인 가능
- www.naver.com 에 대한 IP 주소를 탐색함

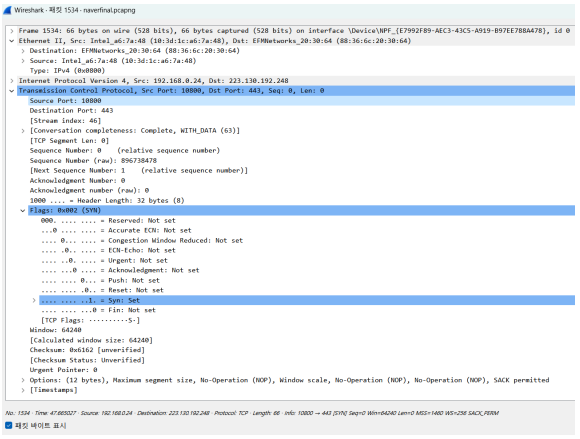
조회 응답

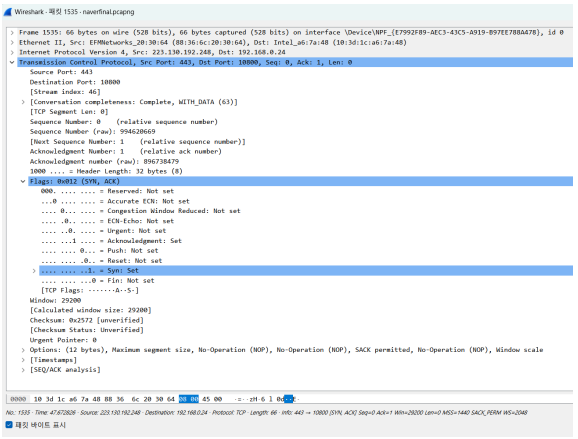
- DNS 서버에서 내 컴퓨터로 받는 응답

- IP 프로토콜을 보면 168.126.63.1(DNS 서버)에서 내 IP(192.168.0.24)로 오는 것을 알 수 있음
- www.naver.com 에 대한 IP 주소 값을 받아옴
  - type A 레코드의 응답값은 223.130.192.248 223.130.200.219 223.130.200.236 223.130.192.247

TCP

SYN **SYN, ACK**





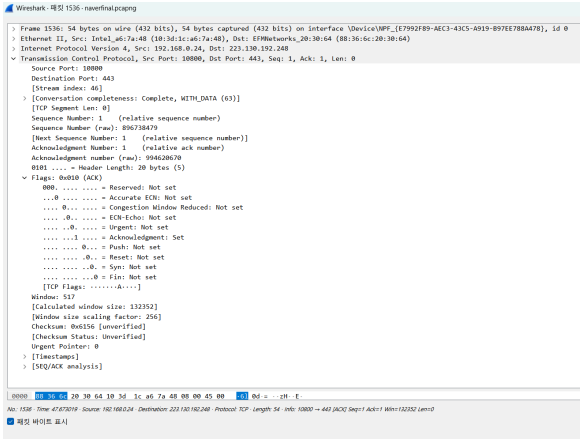
- www.naver.com 에 대한 IP주소 223.130.192.248 와 3-way-handshake를 TCP 프로토콜에서 진행함
- 게이트웨이에 대한 MAC 주소를 ARP에서 확인했으므로, Destinatino MAC 주소는 게이트웨이 MAC 주소
- Source MAC주소는 내 컴퓨터의 MAC 주소
- IP Source는 내 컴퓨터의 IP 주소
- IP Destination은 DNS 서버에서 찾은 도메인(naver)에 대한 IP주소
- Flags: 0x002 → SYN에 해당함
- Destination Port는 443으로 HTTPS로 통신함

SYN, ACK

- Source port는 HTTPS 포트 443
- Destination port는 클라이언트 PC가 송신한 임의의 번호 10800
- Sequence number: 0으로 되어있지만, 실제로 응답 측의 초기 순서 번호가 설정됨

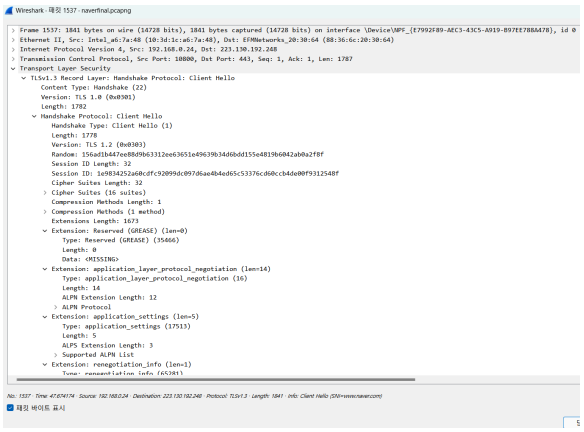
- Acknowledgement number: 1, 클라이언트 PC측이 보낸 순서 번호에 1을 더한 값
- Flags: 0x012, SYN+ACK 로 설정됨

ACK



- Source Port: 클라이언트 PC가 이용하고 있는 포트 번호 10800
- Destination Port: HTTPS의 포트 443
- Sequence number: 1, 실제로는 클라이언트 PC의 초기 순서 번호에 1을 더한 값
- Acknowledgement number: 1, 웹 서버의 초기 순서 번호에 1을 더한 값
- Flags: 0x010 ACK로 설정됨
- 3-way-handshake로 연결 완료함

HTTPS(TLS)



- www.naver.com 은 HTTP 프로토콜이 아닌 HTTPS로 통신함
- IP Source 는 클라이언트 IP 주소인 192.168.0.24

- IP Destination은 서버 IP 주소인 223.130.192.248
- Destination Port: HTTPS 443으로 통신함

인터넷 프로토콜.pptx

naverfinal.pcapng