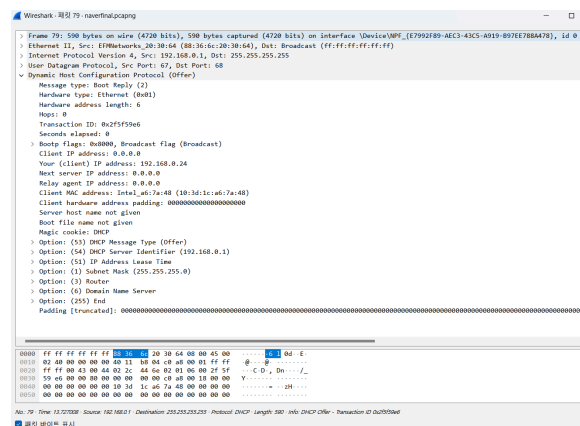




DHCP

Discover 패킷

Offer 패키지

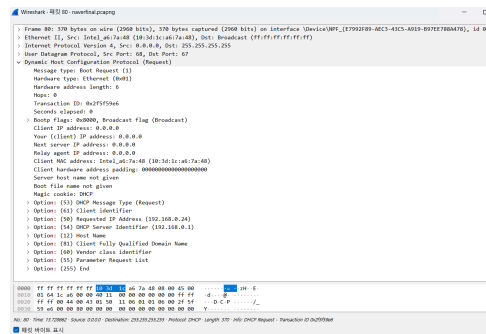


- 전송층 프로토콜로 UDP를 사용
- Message Type (1)으로 식별
- Discover 패킷의 필드는 비어 있음
- DHCP Message Type 필드는 유형 53인 옵션, 길이는 1, 값으로 1가짐

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



- 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

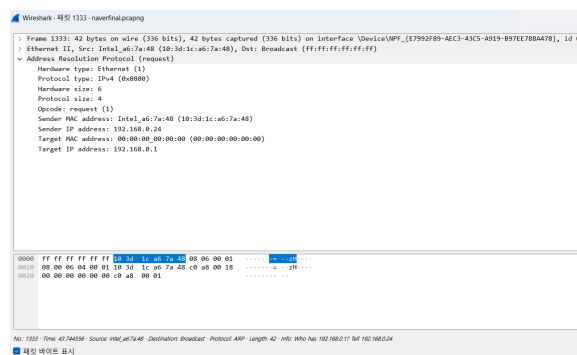
Acknowledge

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

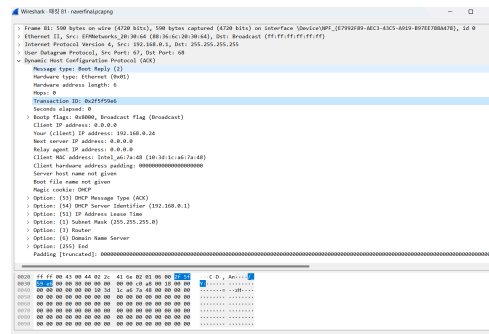
ARP

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

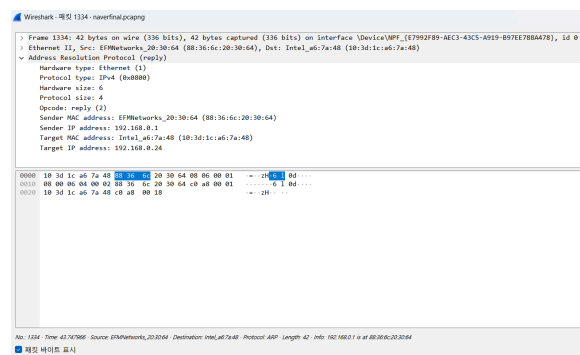
요청



Acknowledgement



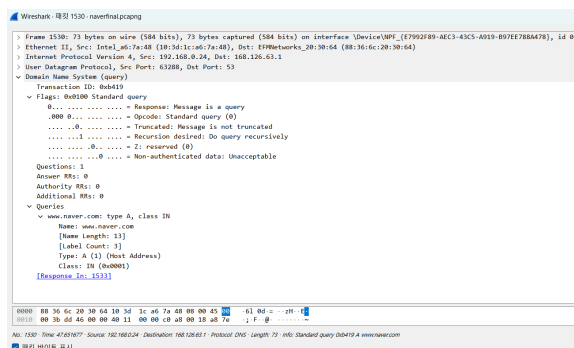
응답



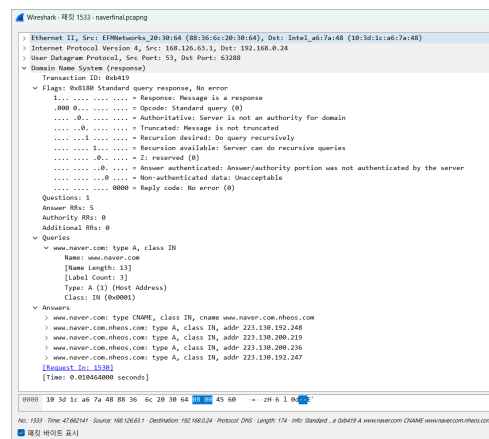
- 답이**

- # 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

```
Wireshark - 패킷 1534 - naver.nal.pcapng
> Frame 1534: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E7992F89-AEC3-43C5-A919-B97EE788A76E}, id 0
> Ethernet II, Src: Intel_a6:7a:48 (18:3d:1c:a6:7a:48), Dst: EPMNetworks_20:30:64 (08:36:6c:20:30:64)
> Destination: EPMNetworks_20:30:64 (08:36:6c:20:30:64)
> Source: Intel_a6:7a:48 (18:3d:1c:a6:7a:48)
> Type: IPv4 (2048)
> Internet Protocol Version 4, Src: 192.168.0.24, Dst: 223.130.192.248
> Transmission Control Protocol, Src Port: 10800, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 10800
  Destination Port: 443
  [Stream index: 46]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 896738478
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    0000 .... = Reserved: Not set
    ...0 .... = Accurate ESN: Not set
    ...0 .... = Congestion Window Reduced: Not set
    ...0 .... = ECH-echo: Not set
    ...0 .... = Urgent: Not set
    ...0 .... = Acknowledgment: Not set
    ...0 .... = Push: Not set
    ...0 .... = Reset: Not set
  > Window: 29200
    ...0 .... = Fin: Not set
    [TCP flags: .....S-]
    [Calculated window size: 29200]
    Checksum: 0x2572 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), SACK permitted
    [Timestamp]
```

SYN, ACK

```
Wireshark - 패킷 1535 - naver.nal.pcapng
> Frame 1535: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E7992F89-AEC3-43C5-A919-B97EE788A76E}, id 0
> Ethernet II, Src: EPMNetworks_20:30:64 (08:36:6c:20:30:64), Dst: Intel_a6:7a:48 (18:3d:1c:a6:7a:48)
> Internet Protocol Version 4, Src: 223.130.192.248, Dst: 192.168.0.24
> Transmission Control Protocol, Src Port: 443, Dst Port: 10800, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 10800
  [Stream index: 46]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 994620669
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 896738479
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    0000 .... = Reserved: Not set
    ...0 .... = Accurate ESN: Not set
    ...0 .... = Congestion Window Reduced: Not set
    ...0 .... = ECH-echo: Not set
    ...0 .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    ...0 .... = Push: Not set
    ...0 .... = Reset: Not set
  > Window: 29200
    ...0 .... = Fin: Not set
    [TCP flags: .....A-S-]
    [Calculated window size: 29200]
    Checksum: 0x2572 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    [Timestamp]
    > [SEQ/ACK analysis]
```

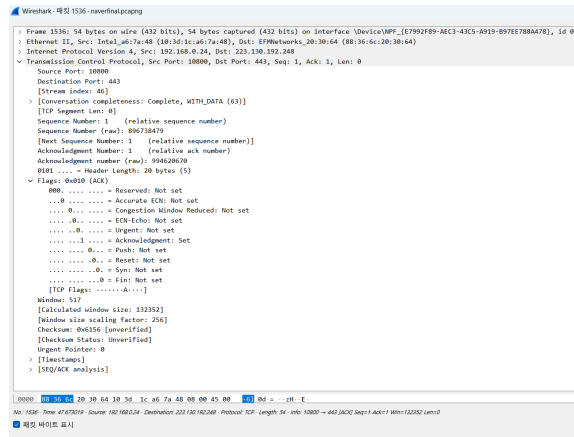
- www.naver.com 에 대한 IP주소 223.130.192.248 와 3-way-handshake를 TCP 프로토콜에서 진행함
- 게이트웨이에 대한 MAC 주소를 ARP에서 확인했으므로, Destination MAC 주소는 게이트웨이 MAC 주소
- Source MAC주소는 내 컴퓨터의 MAC 주소
- IP Source는 내 컴퓨터의 IP 주소
- IP Destination은 DNS 서버에서 찾은 도메인(naver)에 대한 IP주소
- Flags: 0x002 → SYN에 해당함
- Destination Port는 443으로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

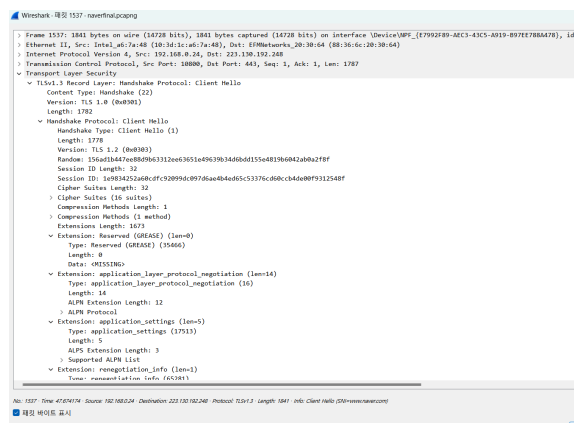
- Acknowledgement number: 1, 클라이언트 PC측이 보낸 순서 번호에 1을 더한 값
- Flags: 0x012, SYN+ACK 로 설정됨

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