PNU, the Premier!

TERM PROJECT

Subject	컴퓨터 네트워크
Professor	김 원 석
Major	정보컴퓨터공학과
Student number	201824636
Name	이 강 우
Date	2023-12-08

부산대학교
PUSAN NATIONAL UNIVERSITY

1-1. TCP https 3개의 웹 사이트 접속 후 패킷 분석

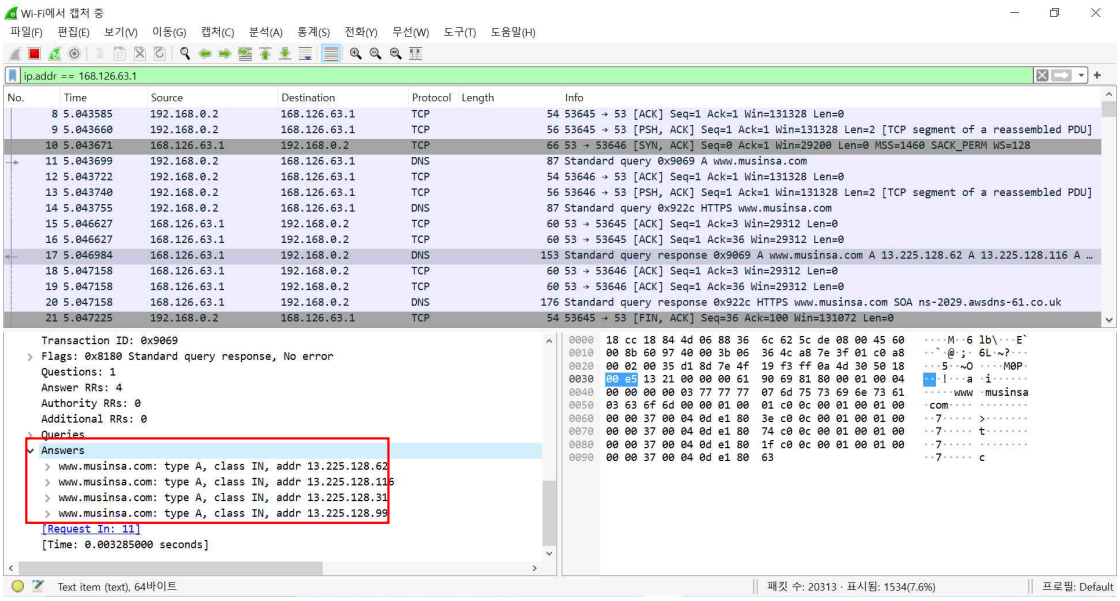


그림 1 - 무신사 웹 페이지의 DNS

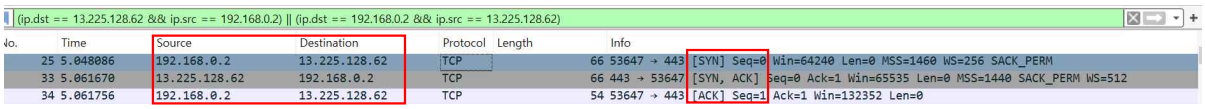


그림 2 - 무신사 웹 페이지의 3-way handshaking

SYN 패킷은 IP, PORT번호 순으로 192.168.0.2 [53647] -> 13.224.128.62 [443], SYN, ACK 패킷은 13.224.128.62 [443] -> 192.168.0.2 [53647], ACK 패킷은 192.168.0.2 [53647] -> 13.224.128.62 [443] 로 확인된다.

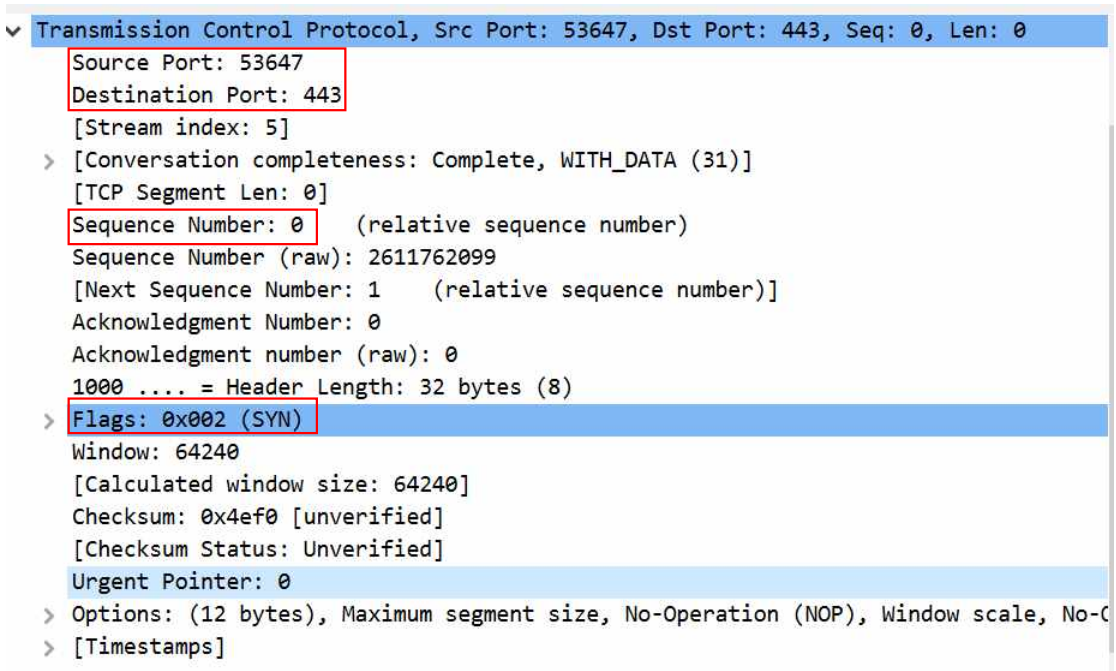


그림 3 - SYN 패킷 분석

SEQ 넘버는 0, SYN FLAG로 TCP 연결을 요청, window 크기는 64240으로 최대 수용가능한 패킷의 크기이다.

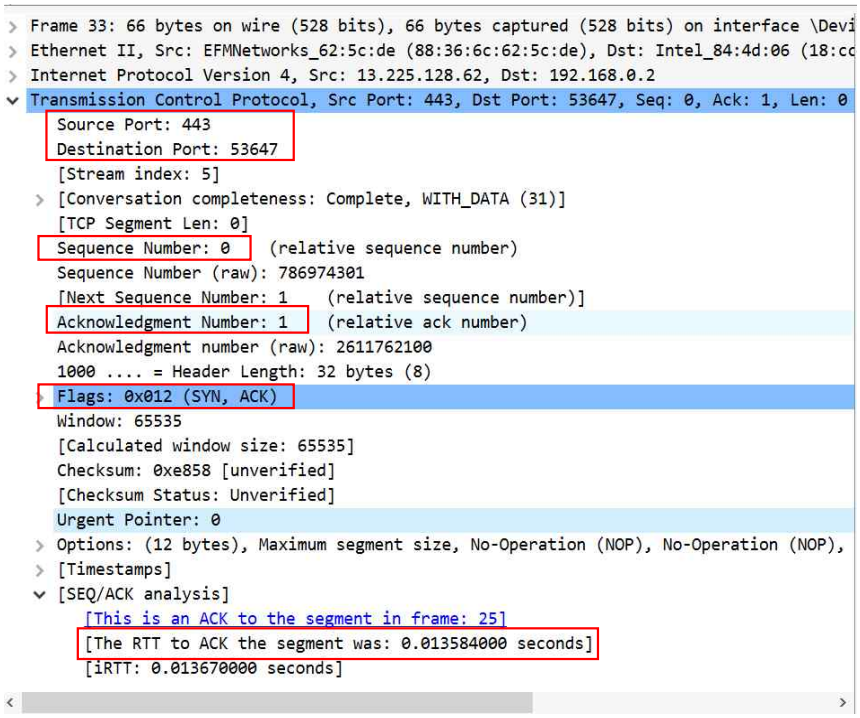


그림 4 - SYN/ACK 패킷 분석

SEQ 넘버는 0, ACK 넘버는 1로 ACK를 읽고 응답으로 +1하여 응답한다. SYN/ACK FLAG로 TCP 연결요청을 응답, window 크기는 65535으로 최대 수용가능한 패킷의 크기이다. RTT는 패킷이 송신지부터 목적지까지 왕복하는데 걸리는 시간으로 0.01358초가 걸린다.

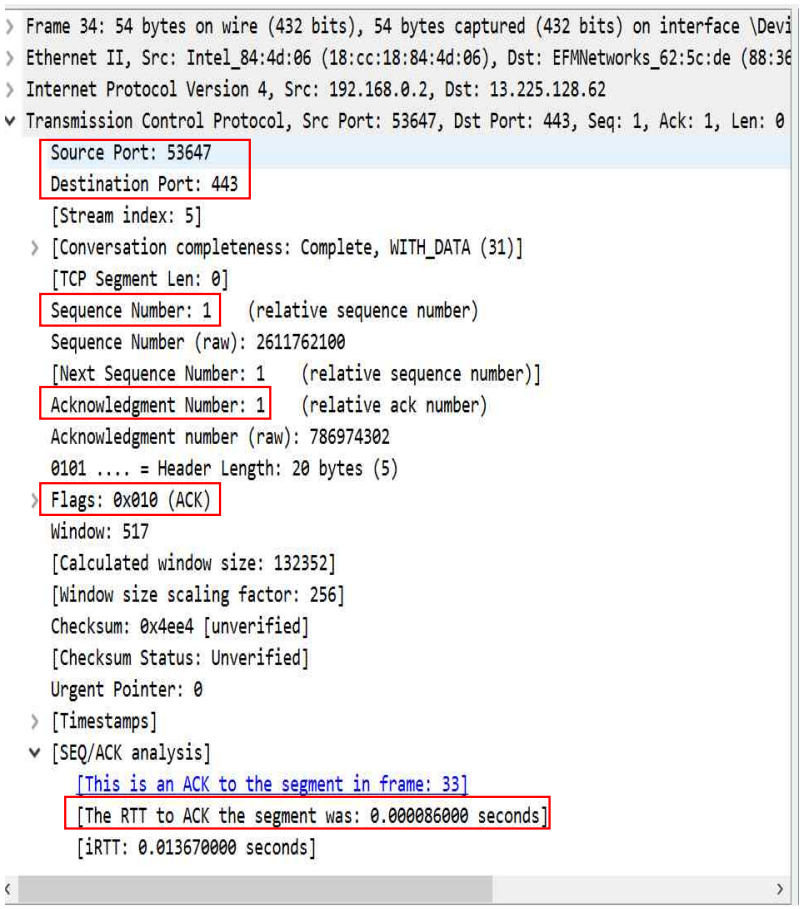


그림 5 - ACK 패킷 분석

SEQ 넘버는 1, ACK 넘버는 1, ACK FLAG로 TCP 연결요청에 대한 확인에 대한 확인으로 응답한다. window 크기는 517로 최대 수용가능한 패킷의 크기이다. RTT는 패킷이 송신지부터 목적지까지 왕복하는데 걸리는 시간으로 0.000086초가 걸린다.

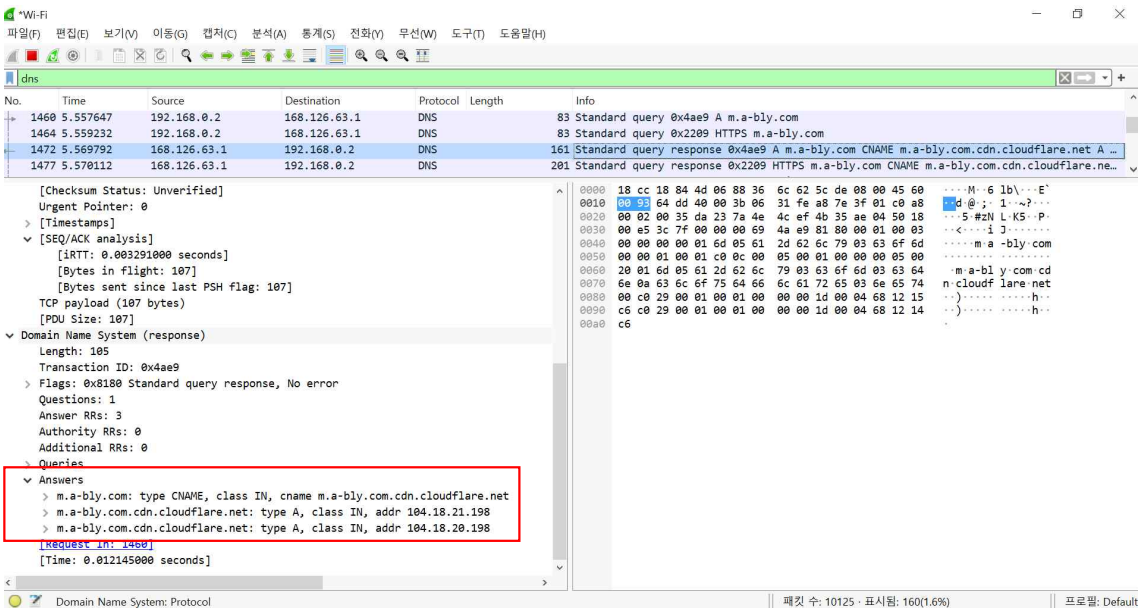


그림 6 - 에이블리 웹 사이트 DNS

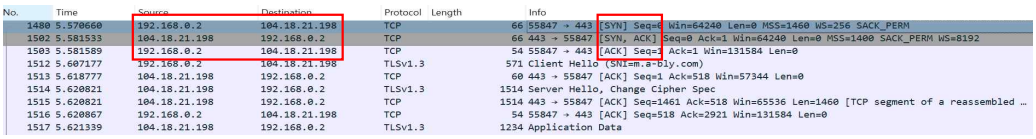


그림 7 - 에이블리 웹 페이지의 3-way handshaking

SYN 패킷은 IP, PORT번호 순으로 192.168.0.2 [55847] -> 13.224.128.62 [443], SYN, ACK 패킷은 13.224.128.62 [443] -> 192.168.0.2 [55847], ACK 패킷은 192.168.0.2 [55847] -> 13.224.128.62 [443] 로 확인된다.

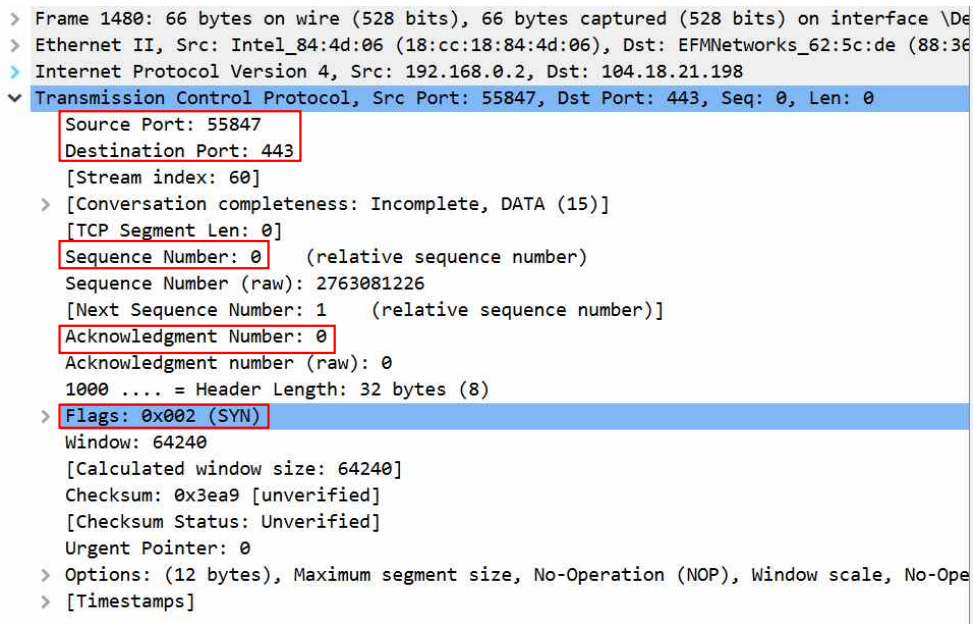


그림 8 - SYN 패킷 분석

SEQ 넘버는 0, SYN FLAG로 TCP 연결을 요청, window 크기는 64240으로 최대 수용가능한 패킷의 크기이다.

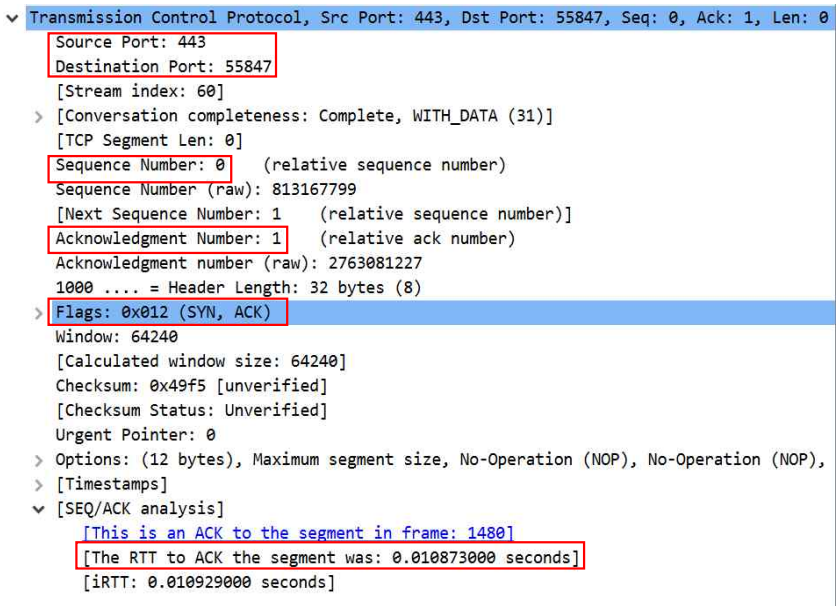


그림 9 - SYN / ACK 패킷 분석

전과 마찬가지로 SEQ 넘버는 0, ACK 넘버는 1로 ACK를 읽고 응답으로 +1하여 응답한다. SYN/ACK FLAG로 TCP 연결요청을 응답, window 크기는 64240, RTT는 0.01358초가 걸린다.

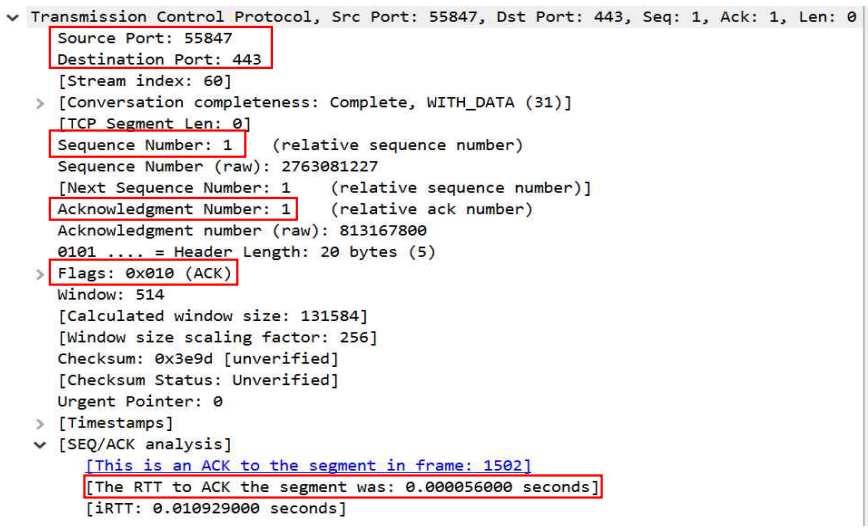


그림 10 - ACK 패킷 분석

SEQ 넘버는 1, ACK 넘버는 1, ACK FLAG로 TCP 연결요청에 대한 확인에 대한 확인으로 응답한다. window 크기는 514이다. RTT는 0.000056초가 걸린다.

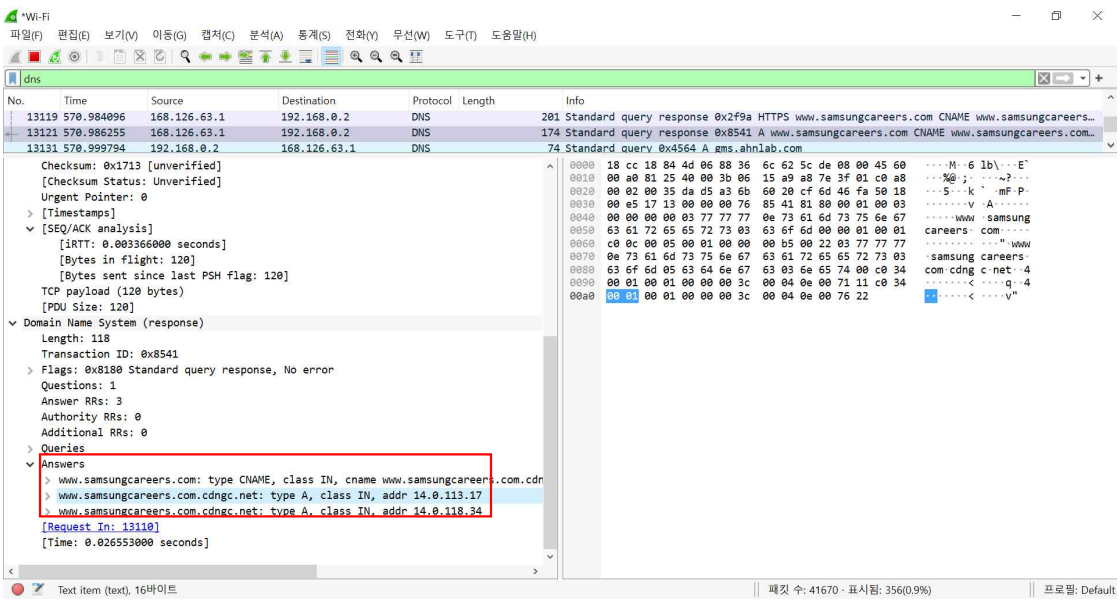


그림 11 - 삼성 커리어스 DNS

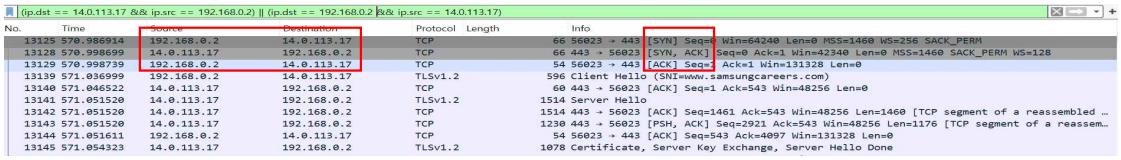


그림 12 - 삼성 커리어스 3-way handshaking

SYN 패킷은 IP, PORT번호 순으로 192.168.0.2 [56023] -> 13.224.128.62 [443], SYN, ACK 패킷은 13.224.128.62 [443] -> 192.168.0.2 [56023], ACK 패킷은 192.168.0.2 [56023] -> 13.224.128.62 [443] 로 확인된다.

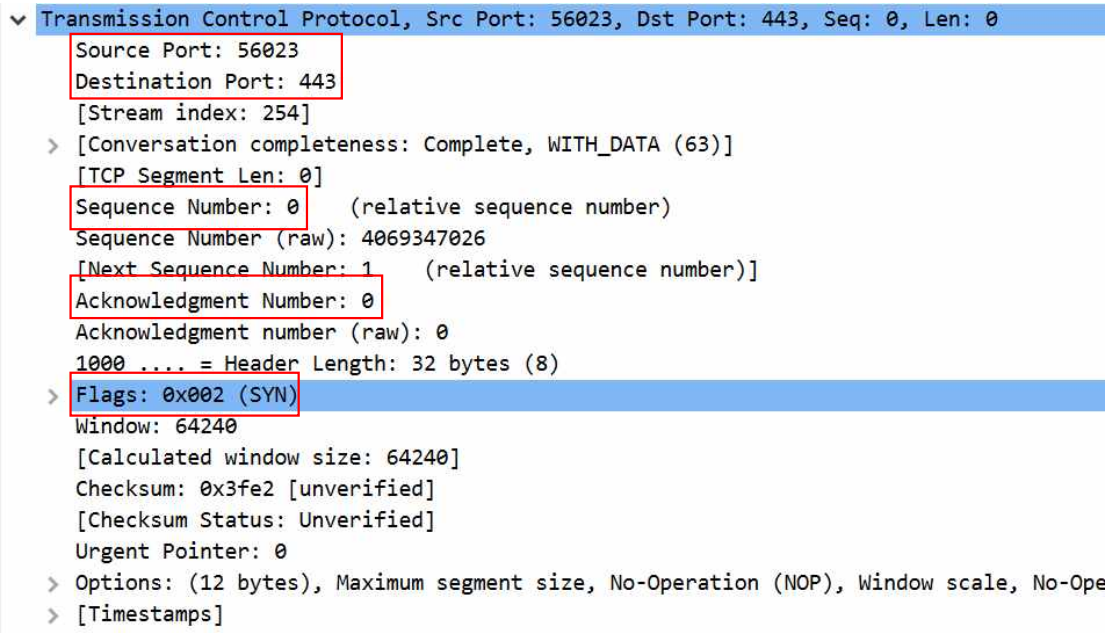


그림 13 - SYN 패킷 분석

SEQ 넘버는 0, SYN FLAG로 TCP 연결을 요청, window 크기는 64240으로 최대 수용가능한 패킷의 크기이다.

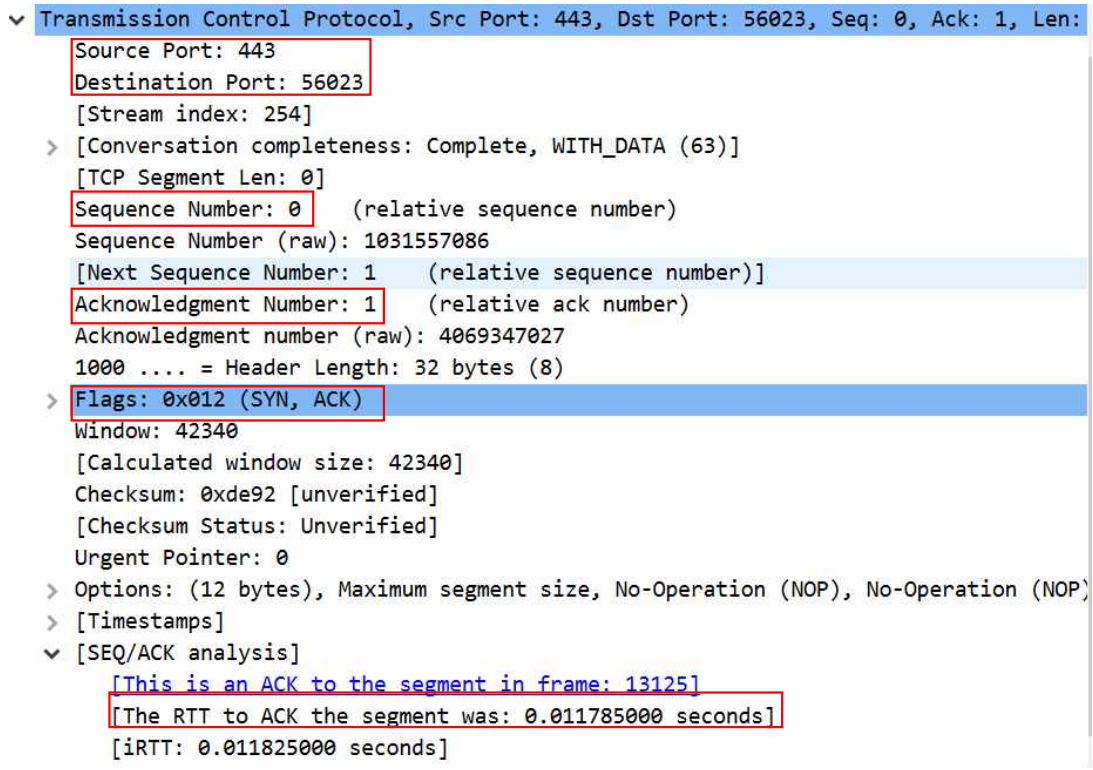


그림 14 - SYN / ACK 패킷 분석

전과 마찬가지로 SEQ 넘버는 0, ACK 넘버는 1로 ACK를 읽고 응답으로 +1하여 응답한다. SYN/ACK FLAG로 TCP 연결요청을 응답, window 크기는 42340, RTT는 0.01178초가 걸린다.

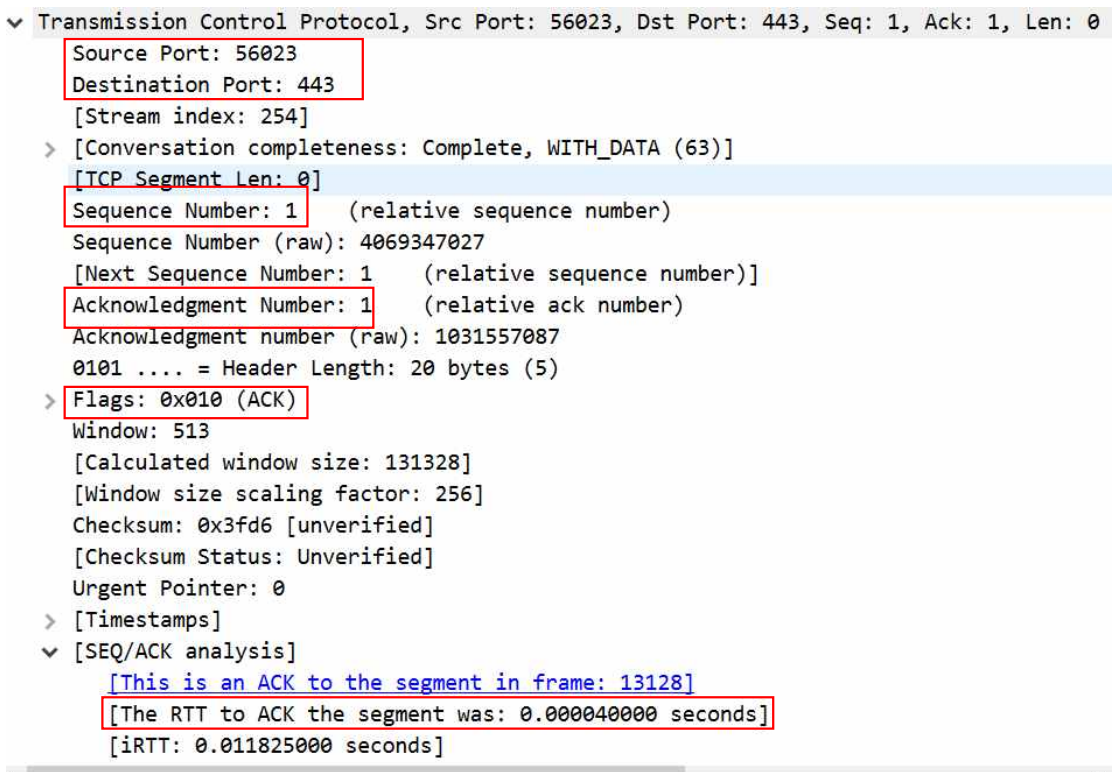


그림 15 - ACK 패킷 분석

SEQ 넘버는 1, ACK 넘버는 1, ACK FLAG로 TCP 연결요청에 대한 확인에 대한 확인으로 응답한다. window 크기는 513이다. RTT는 0.00004초가 걸린다.

1-2. 학과 홈페이지의 첨부파일을 다운로드 하고

- ACK 패킷 3개 분석

그림 16 - 첨부파일 다운로드 후 캡처된 패킷

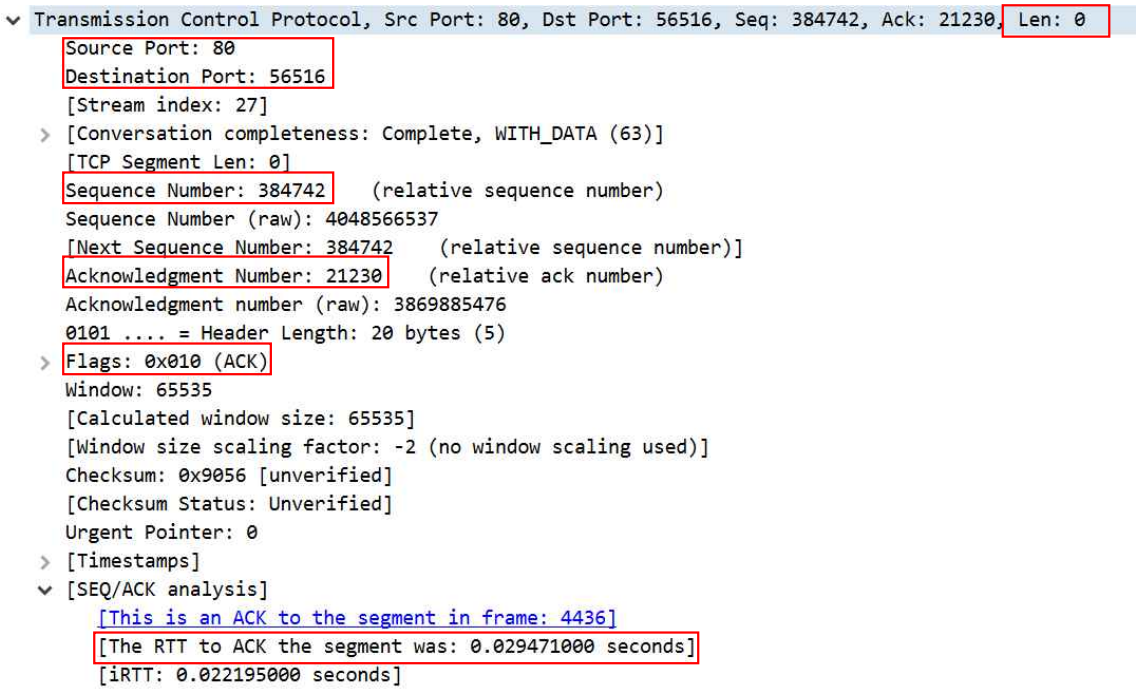


그림 17 - 캡처된 첫 번째 패킷

첫 번째 패킷은 0의 길이로 80번 포트에서 56516 포트로 전송된다. seq는 384742 ack는 21230으로 ACK요청을 한다. Window크기는 65535, RTT는 0.02947초이다.

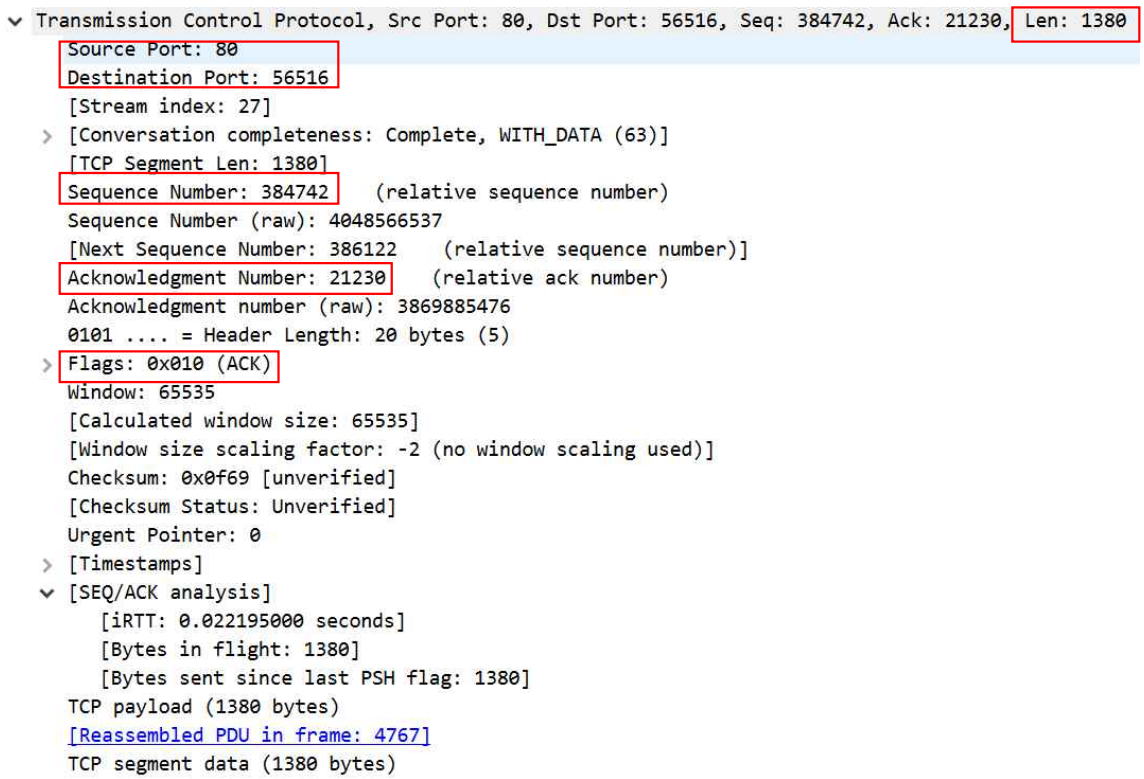


그림 18 - 캡처된 두 번째 패킷

두 번째 패킷은 1380의 길이로 80번 포트에서 56516 포트로 전송된다. seq는 384742에서 데이터의 크기인 전의 크기인 0이 더해진 384742이다. ack는 21230으로 ACK요청을 한다. Window크기는 65535이다.

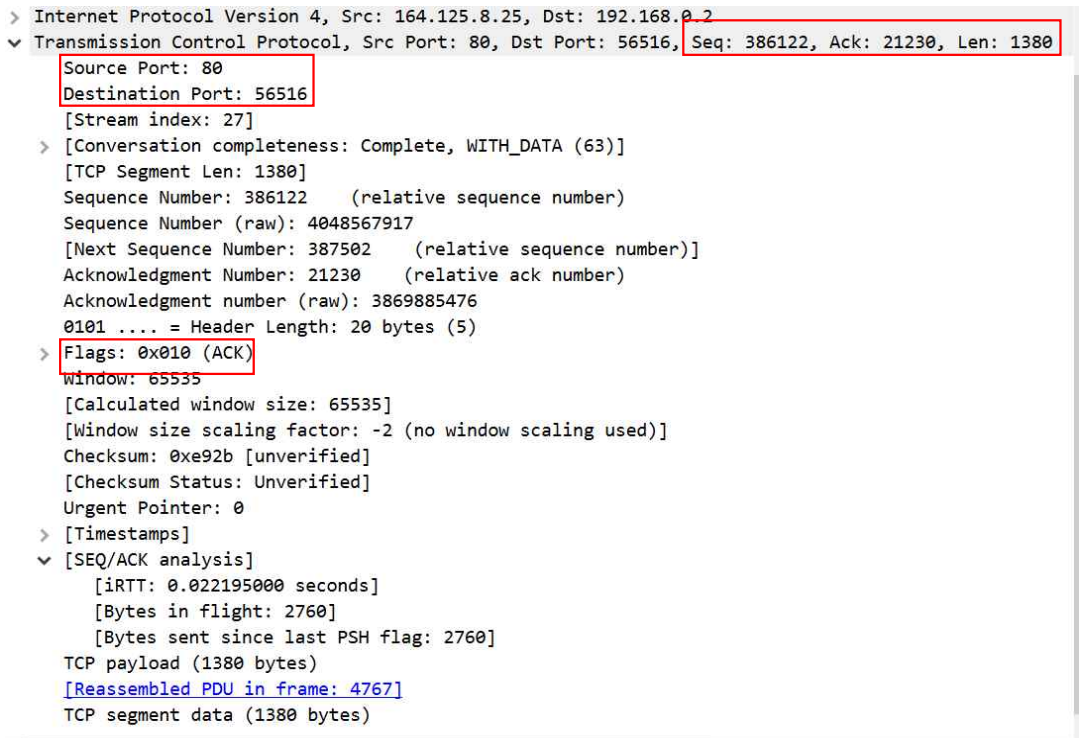


그림 19 - 캡처된 세 번째 패킷

세 번째 패킷 역시 1380의 길이로 80번 포트에서 56516 포트로 전송된다. seq는 384742에서 데이터의 크기인 전의 크기인 1380이 더해진 386122이다. ack는 21230으로 ACK요청을 한다. Window크기는 65535이다.

- 그래프

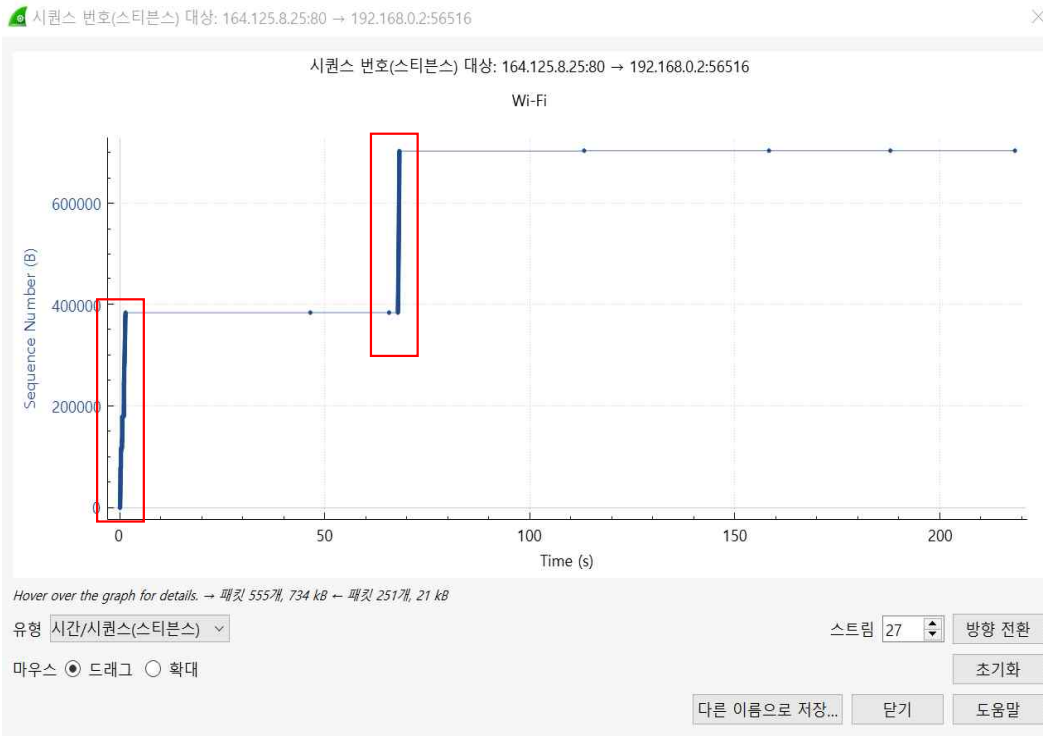


그림 20 - seq/time 스티븐스 그래프

80번(HTTP) 포트에서 56516 포트로 TCP연결을 할 때 보내는 SEQ NUM이 점점 증가한다는 것은 보내는 데이터가 올라간다고 볼 수 있다. TCP slow start가 일어나고 있으며, 설정되어있는 threshold에 도달한다면 0부터 다시 SEQ NUM이 초기화되고 다시 시작한다고 예측된다.

2. DHCP

2-1. DHCP메시지의 Transport layer protocol의 종류와 사용 이유.

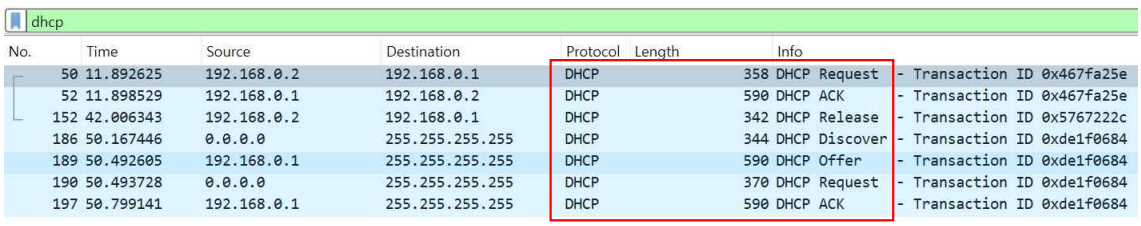
DHCP 메시지는 일반적으로 Transport Layer Protocol의 종류 중 하나인 UDP 패킷 내에 캡슐화된다.

UDP는 신뢰성이 떨어지고 3-way connection을 하지 않아 즉각적인 반응이 더 중요한 애플리케이션에 사용. DHCP는 오버헤드 없이 메시지를 전송하는 더 빠르고 효율적인 방법을 제공하기 때문에 TCP보다는 UDP를 선호한다.

DHCP는 주로 서버 통신에 UDP 포트 67을 사용하고 클라이언트 통신에 UDP 포트 68을 사용합니다. DHCP에서 UDP를 사용하면 IP 주소 및 관련 구성 정보를 동적으로 할당하기 위해 클라이언트와 서버 간의 빠르고 간단한 통신이 가능하다.

2-2. DHCP메시지

ipconfig /renew -> ipconfig /release 이후 패킷 캡처


dhcp

No.	Time	Source	Destination	Protocol	Length	Info
50	11.892625	192.168.0.2	192.168.0.1	DHCP	358	DHCP Request - Transaction ID 0x467fa25e
52	11.898529	192.168.0.1	192.168.0.2	DHCP	590	DHCP ACK - Transaction ID 0x467fa25e
152	42.006343	192.168.0.2	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0x5767222c
186	50.167446	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xde1f0684
189	50.492605	192.168.0.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0xde1f0684
190	50.493728	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xde1f0684
197	50.799141	192.168.0.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0xde1f0684

그림 21 - 명령어 이후 캡처한 패킷

[DHCP - Discover]

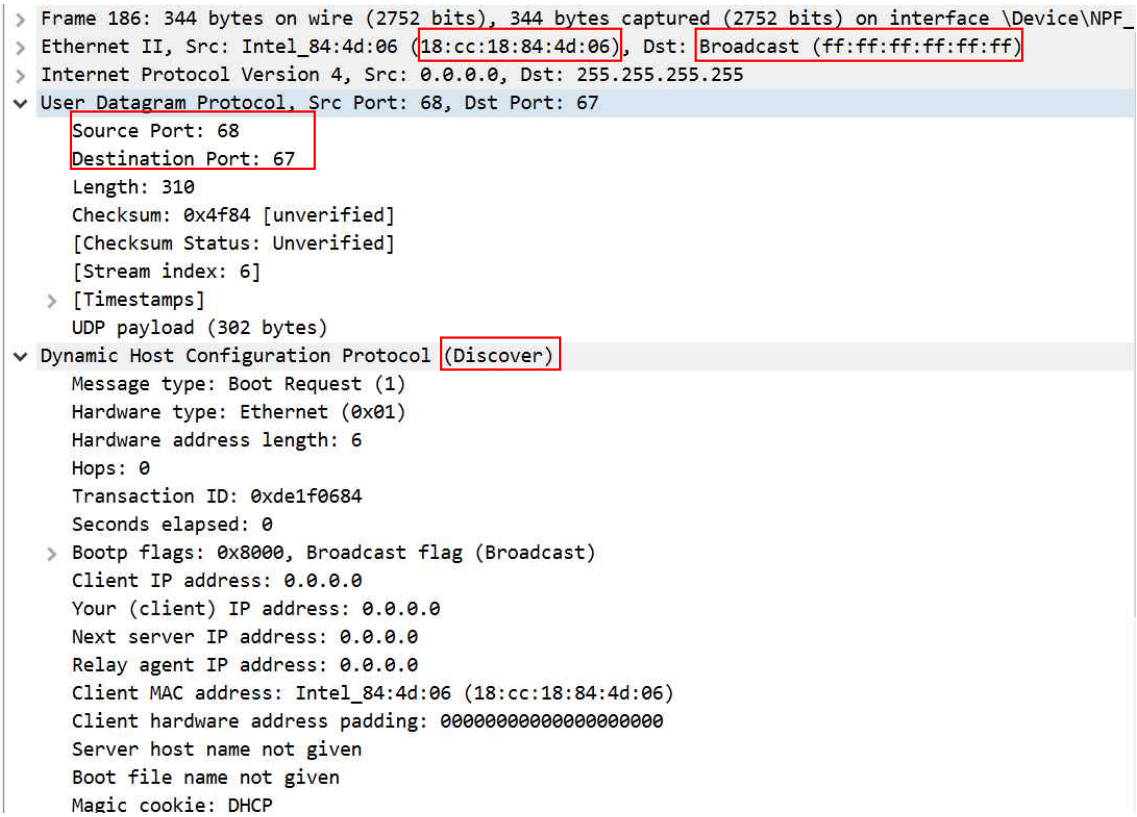


그림 22 - DHCP - DISCOVER 패킷 분석

DHCP Discover는 클라이언트가 네트워크에서 IP를 할당받기 위해 DHCP 서버에 연결하기 위해 Broadcast형식으로 UDP형식으로 67번 포트로 전송한다.

그림 23 - DHCP - DISCOVER 옵션

필드 값은
SubNet Mast : 서브넷 마스크, Router : 사용 가능한 라우터 리스트, DNS : 사용 가능한 DNS서버 리스트, Hostname : 호스트 이름, Request IP address : 요청된 IP 주소, IP address Lease Time : DHCP가 IP 주소 대여해주는 시간, DHCP Message Length : 메시지 식별자, Parameter List : 클라이언트 요청 매개변수, Hops: DHCP 서버에 오기위해 통과하는 네트워크 수, DHCP Message Type : DHCP 메시지 타입 정의, Vendor Class Identifier : 벤더 클래스 식별자, End : DHCP 옵션의 끝을 알림 등이 있다.

[DHCP - Offer]

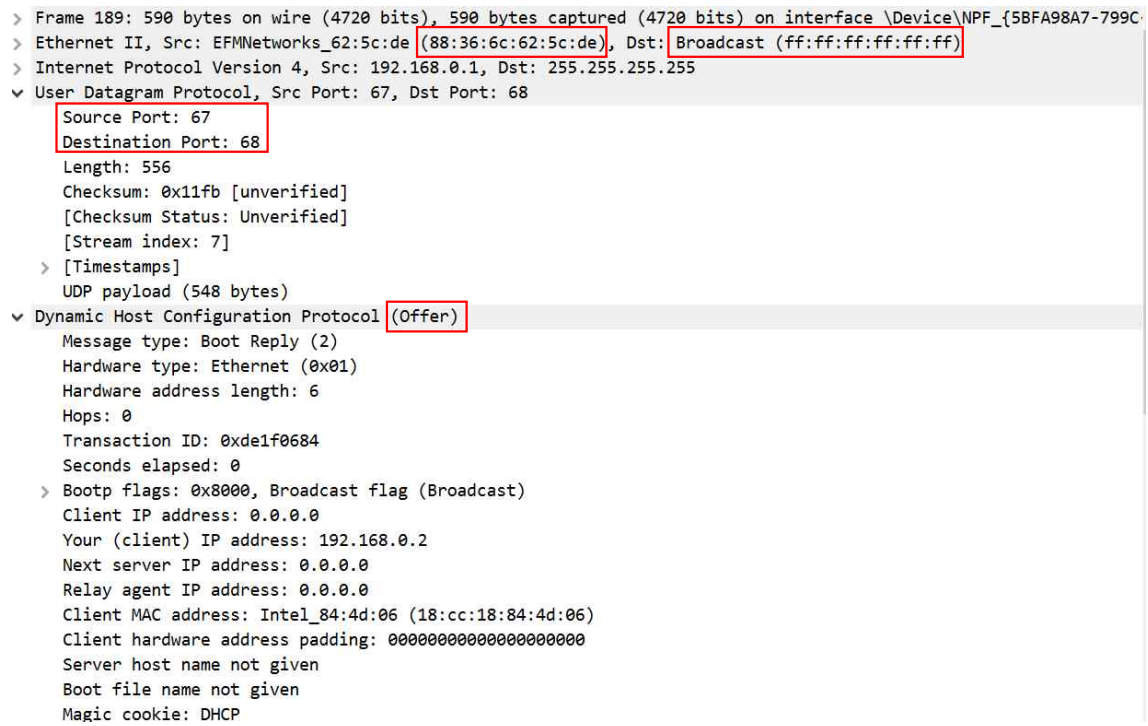


그림 24 - DHCP - OFFER 패킷 분석

DHCP Offer는 네트워크에서 Discover의 응답으로 클라이언트에게 IP를 할당을 시도한다.

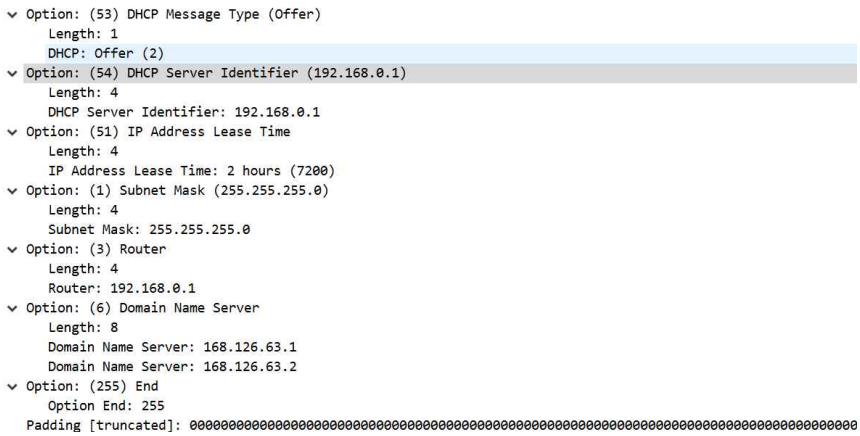


그림 25 - DHCP - OFFER 옵션

[DHCP - Request]

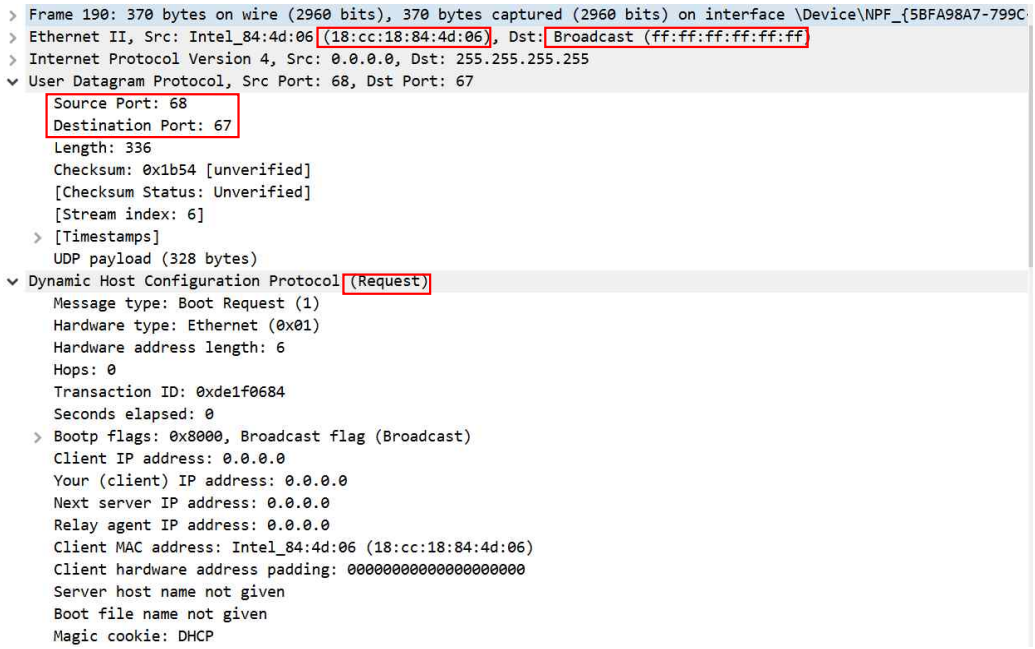


그림 26 - DHCP - REQUEST 패킷 분석

DHCP Request 패킷은 서버로부터 IP로 제공받고 Client가 IP를 사용한다는 응답을 보냅니다.

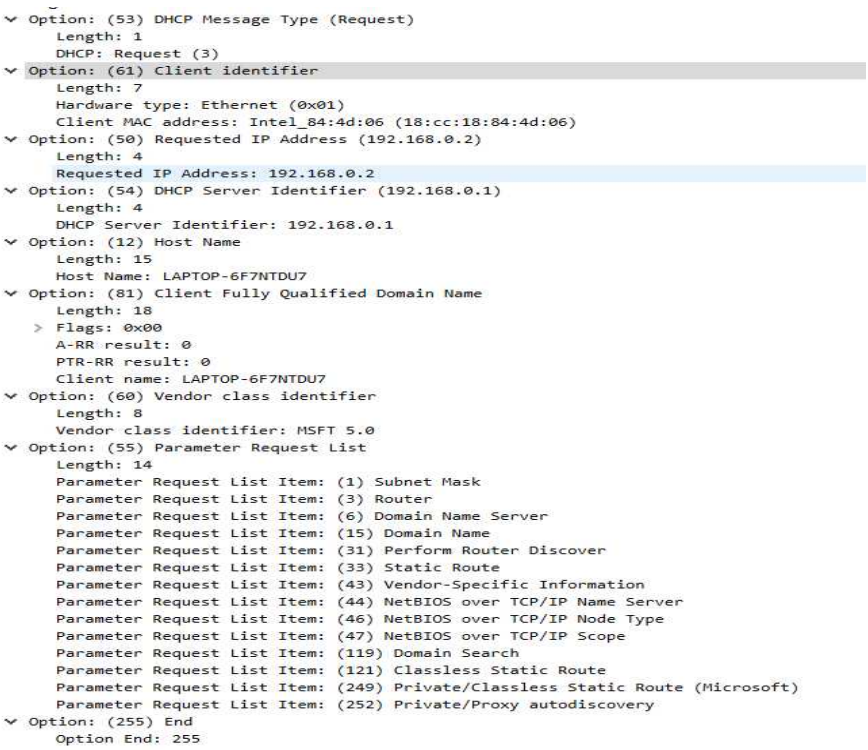


그림 27 - DHCP - REQUEST 옵션

[DHCP - ACK]

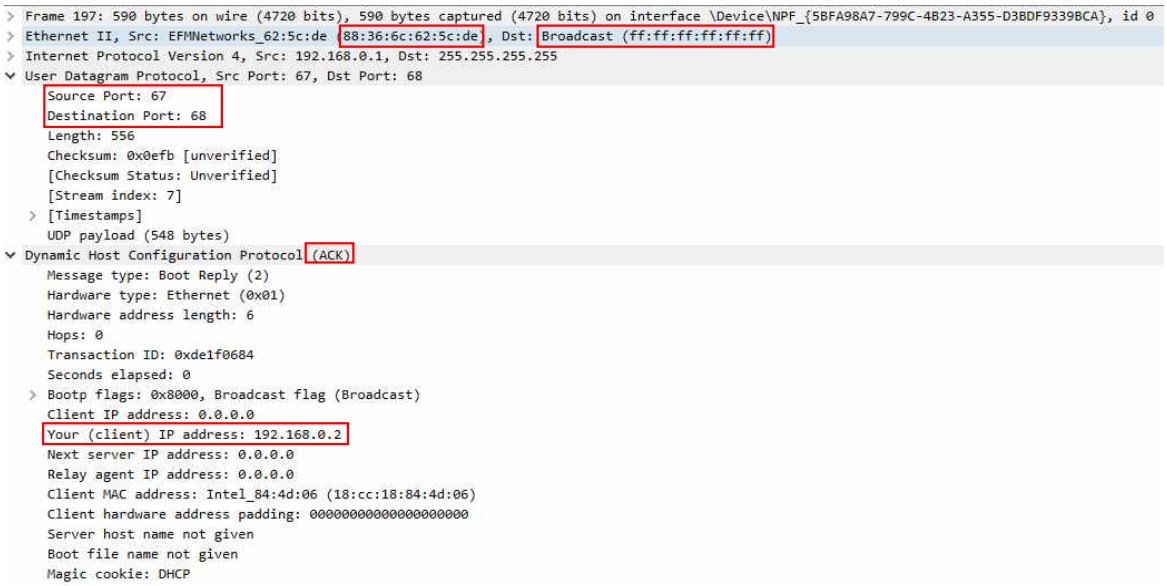


그림 28 - DHCP - ACK 패킷 분석

DHCP 통신의 최종 과정으로 서버가 IP를 최종으로 할당하는 과정으로, 0.0.0.0이었던 IP주소가 192.168.0.2의 IP주소로 할당받아진 것을 확인 할 수있다.

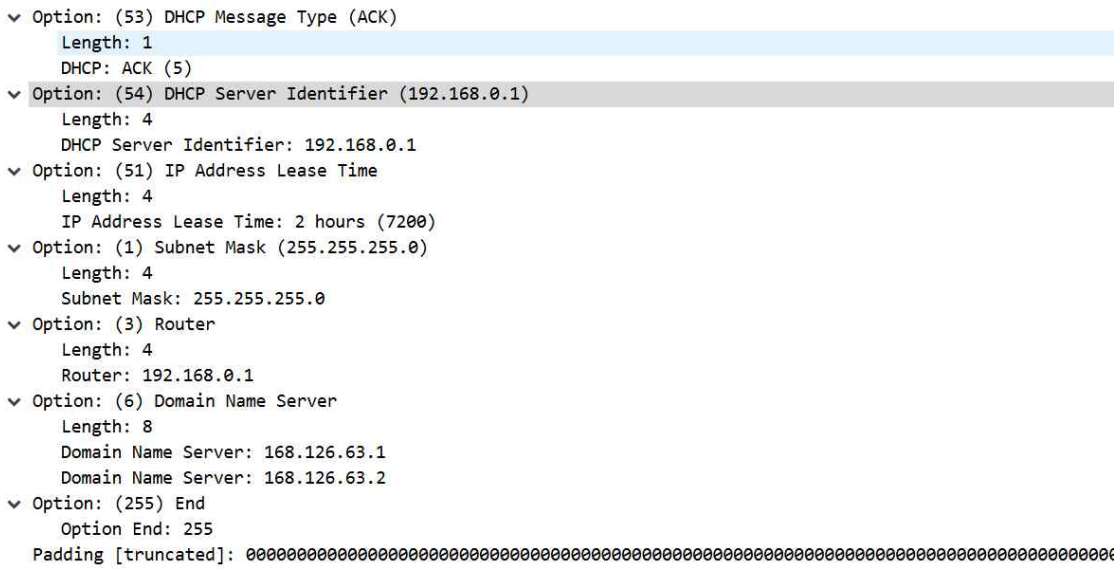


그림 29 - DHCP - ACK 옵션

[DHCP - Release]

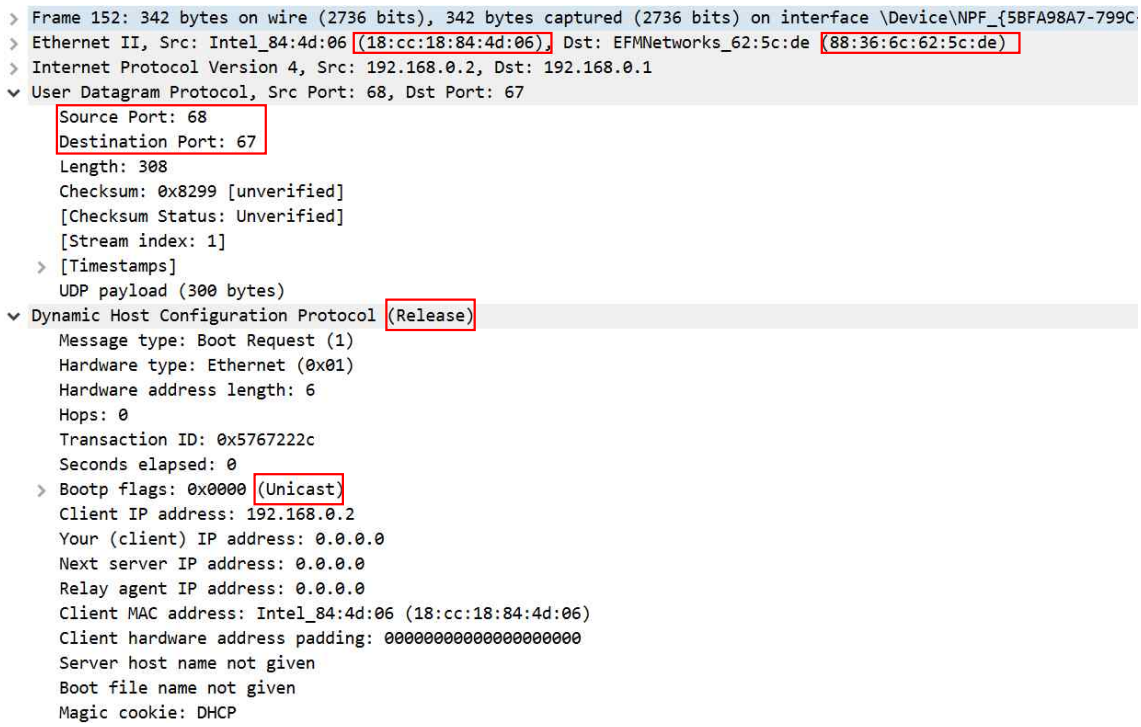


그림 30 - DHCP - Release 패킷 분석

IP의 임대시간 종료나, release 명령어로 IP가 갱신되며, Discover과 달리 DHCP 서버에게 UNICAST 형식으로 보내진다.

그림 31 - DHCP - Release 옵션

3. ARP

arp -a -> arp -d *를 관리자 권한으로 실행 후

3-1. ARP reqest, ARP reply 패킷을 분석

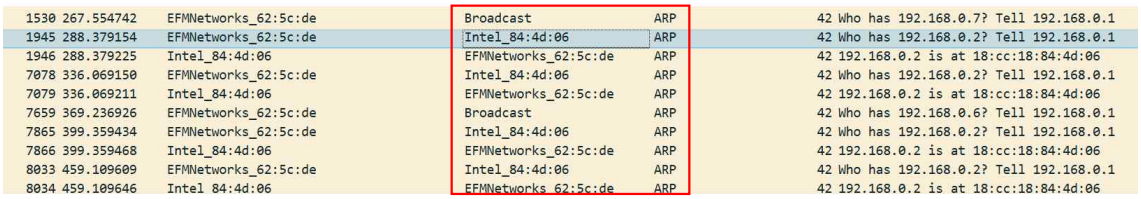


그림 32 - 캡처된 ARP 메시지 패킷

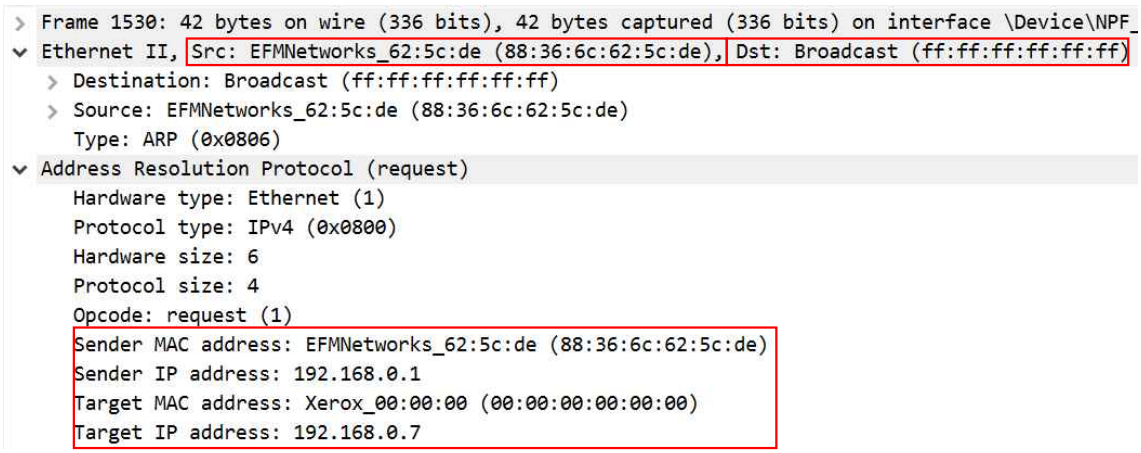


그림 33 - ARP Request 패킷 분석

ARP Request 요청은 원하는 IP주소(192.168.0.7)와 상응하는 MAC주소를 알기 위해 사용. Target MAC 주소를 알지 못하므로, 0으로 채워져있다.

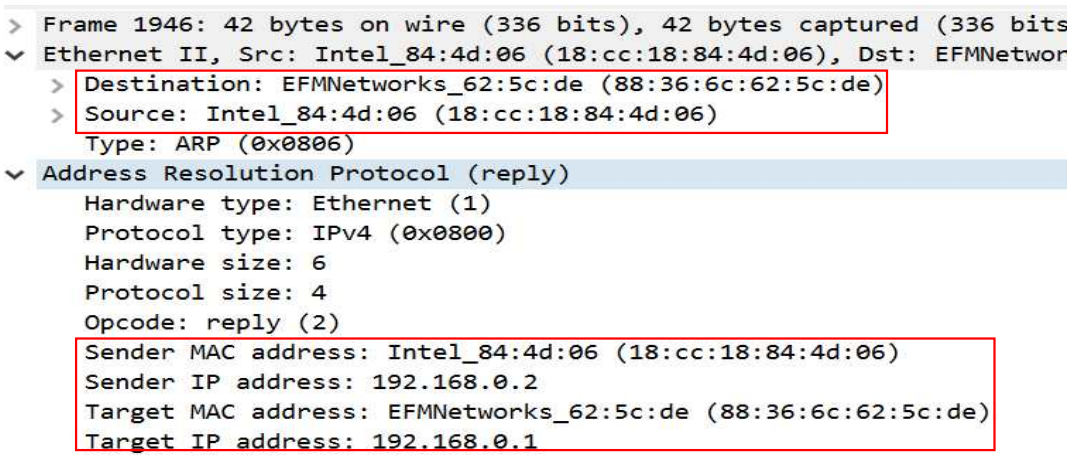


그림 34 - ARP Reply 패킷 분석

ARP Reply 요청으로 원하는 IP주소(192.168.0.7)와 상응하는 MAC주소(88:36:6c:62:5c:de)를 ARP Request 했던 IP주소(192.168.0.1)로 돌려준다.

3-2. HTTP request의 src,dest MAC주소 제시 후 장치가 무엇인지 제시.

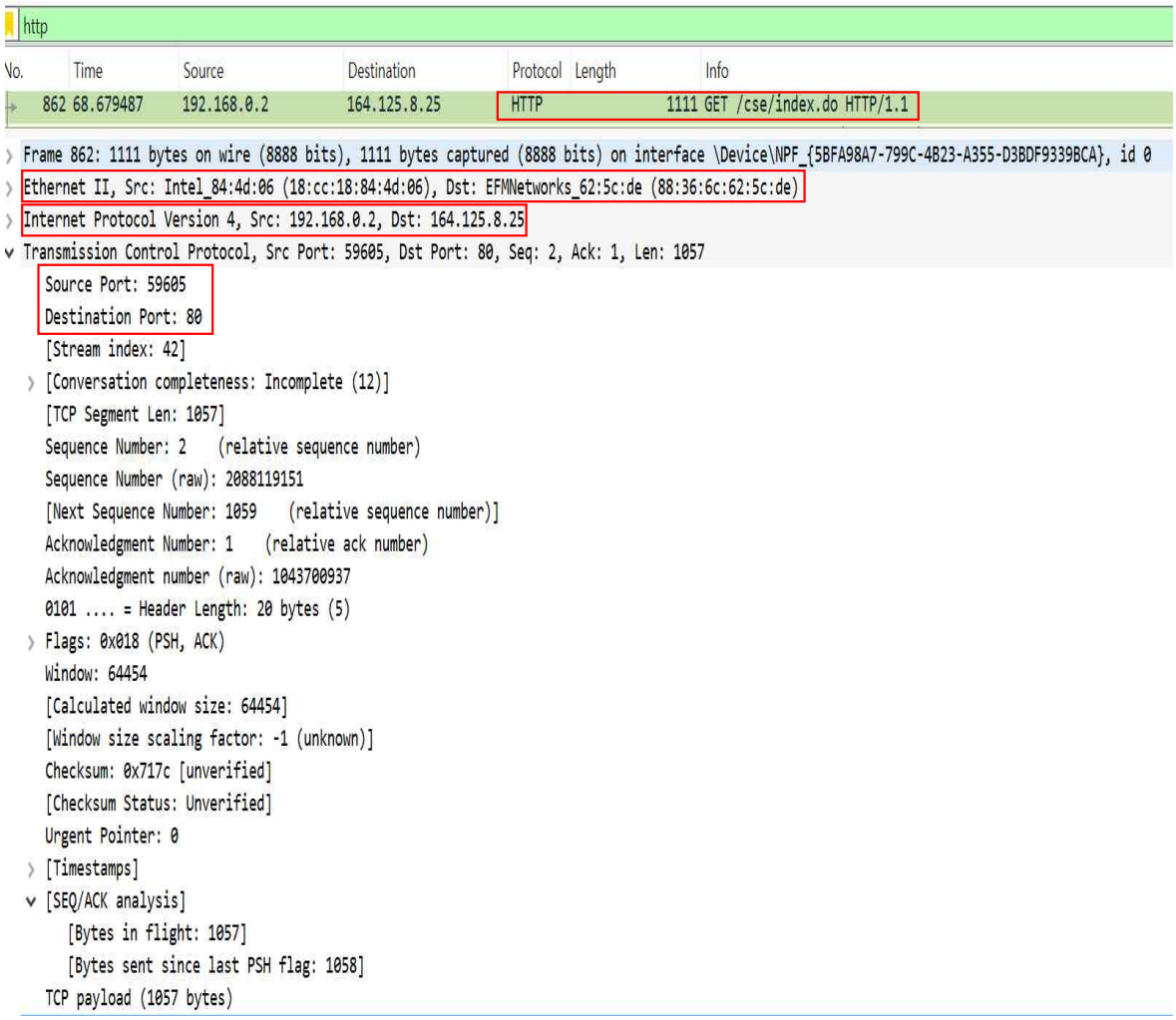


그림 35 - HTTP 접속 후 분석

HTTP (80번 포트)로 부산대 정컴 홈페이지에 접속하였다. 이더넷 부분을 보면 src MAC (18:cc:18:84:4d:06) 노트북의 고유한 MAC 주소에서 ARP Reply로 받은 dest MAC 주소인 (88:36:6c:62:5c:de) 즉, 부산대 정컴 홈페이지의 고유한 MAC으로 접속이 일어난다.

3-3. HTTP GET 메시지에서 “G”이전까지 총 bytes 제시, link layer(이더넷) header가 차지하는 크기는?

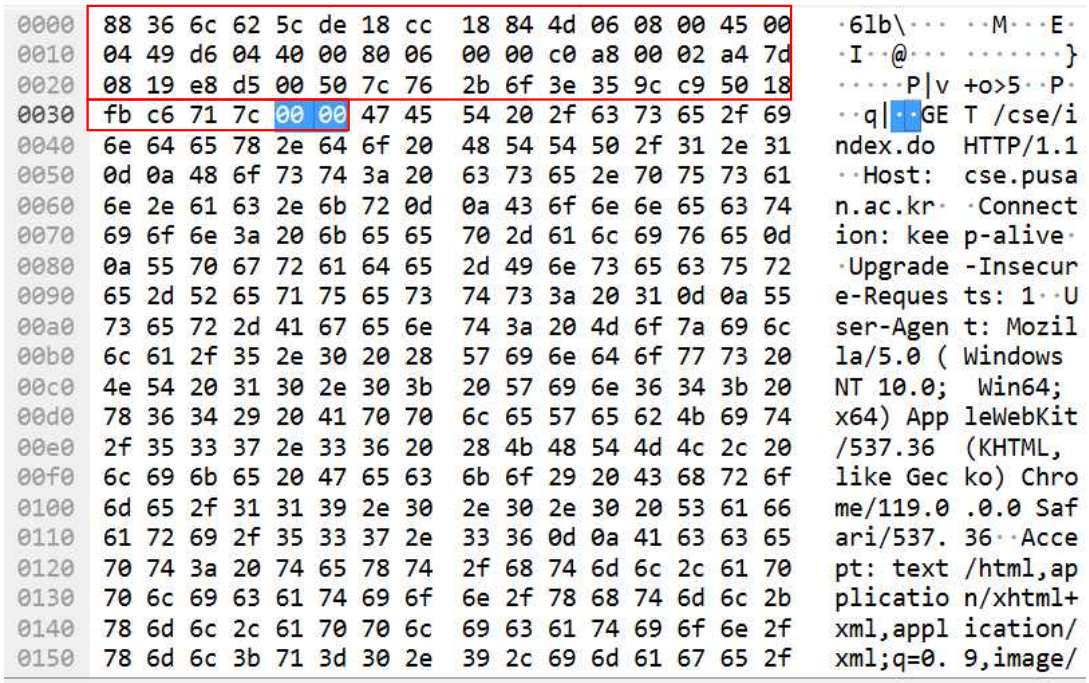


그림 36 - ‘G’ 이전까지의 총 BYTE

한 블록에 1바이트인 패킷데이터가 54개 있는 부분부터 ‘G’ 이전이므로 1bytes * 54 = 54로 54 bytes 이다.

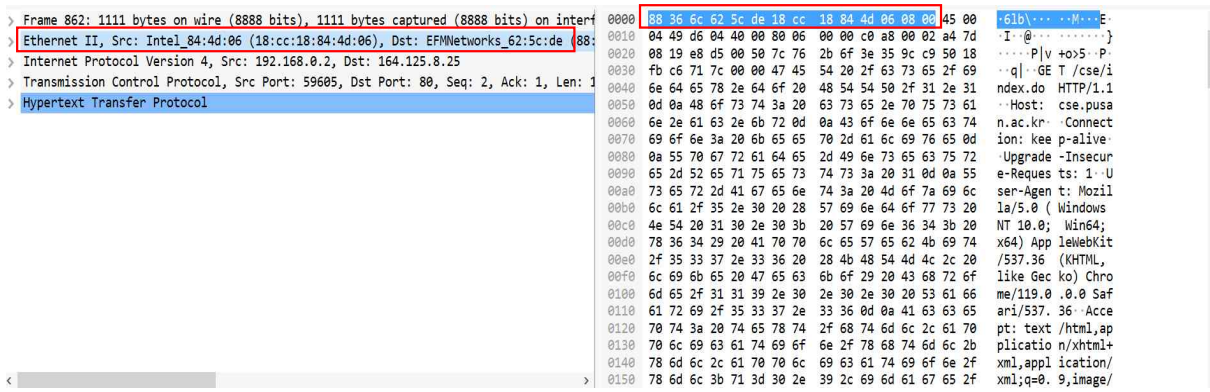


그림 37 - Link Layer frame header 크기

이 중에서 이더넷을 클릭했을 때, 나오는 1 bytes * 14 = 14로 14 bytes가 Link Layer Frame Header 크기이다.