

TERM PROJECT



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



1-1. TCP https 3개의 웹 사이트 접속 후 패킷 분석

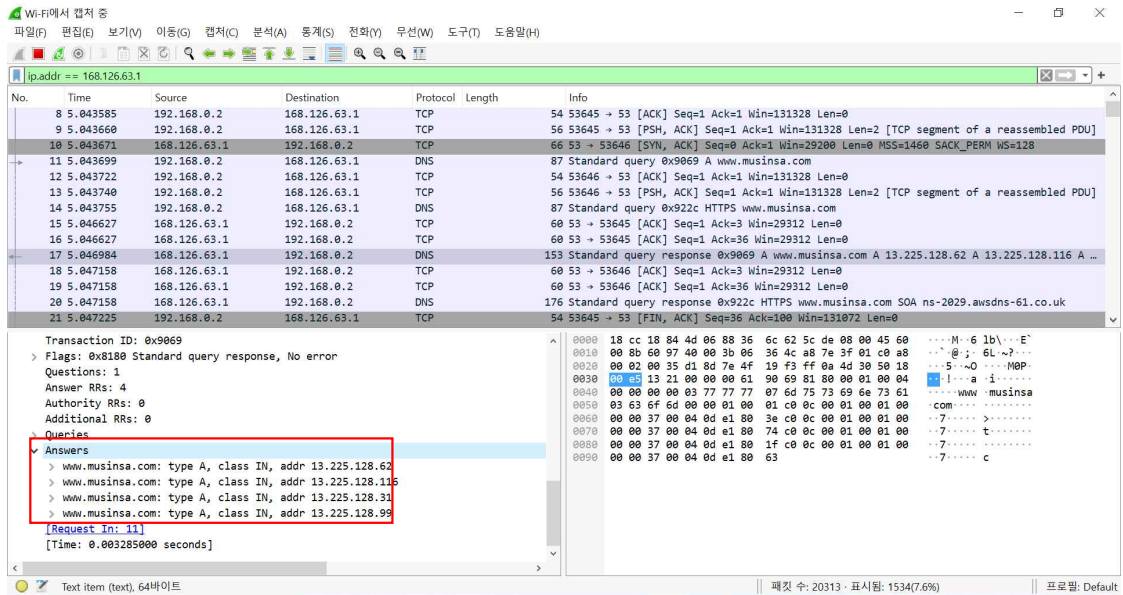


그림 1 - 무신사 웹 페이지의 DNS

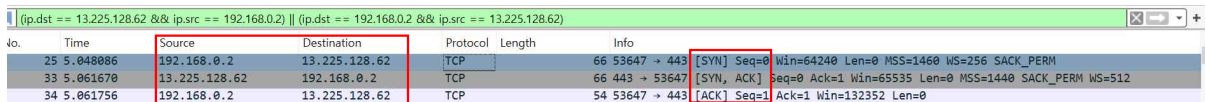


그림 2 - 무신사 웹 페이지의 3-way handshaking

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.

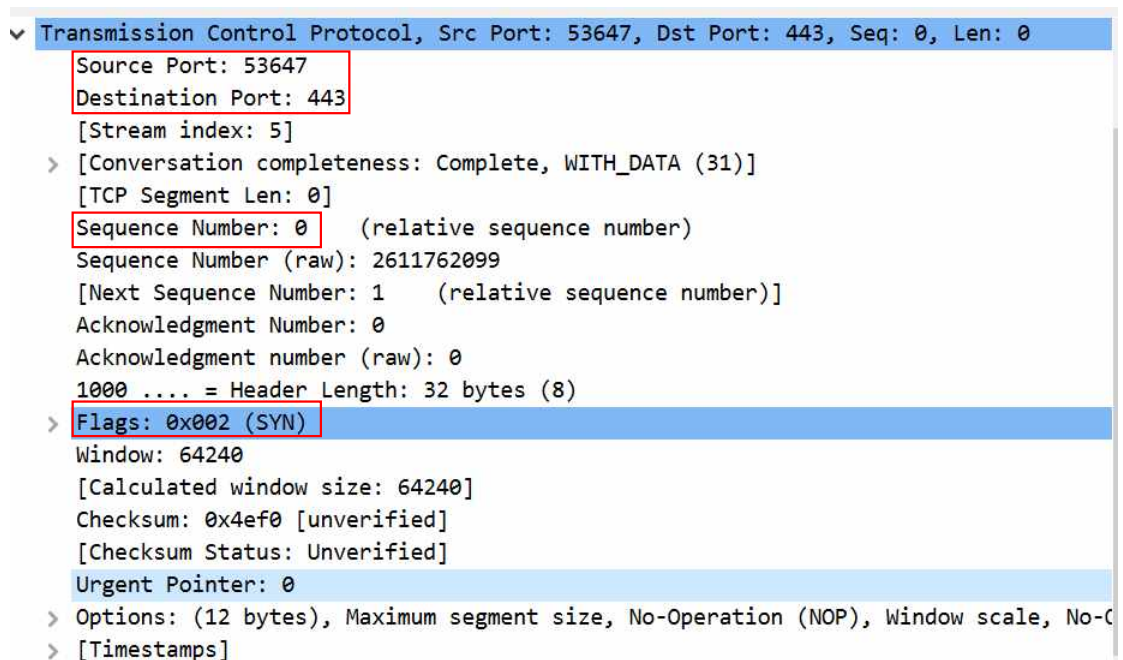


그림 3 - SYN 패킷 분석

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

```
> Frame 33: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devi
> Ethernet II, Src: EFMNetworks_62:5c:de (88:36:6c:62:5c:de), Dst: Intel_84:4d:06 (18:cc
> Internet Protocol Version 4, Src: 13.225.128.62, Dst: 192.168.0.2
v Transmission Control Protocol, Src Port: 443, Dst Port: 53647, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 53647
  [Stream index: 5]
  > [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 786974301
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2611762100
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0xe858 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP),
  > [Timestamps]
  v [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 25]
    [The RTT to ACK the segment was: 0.013584000 seconds]
    [iRTT: 0.013670000 seconds]
```

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.

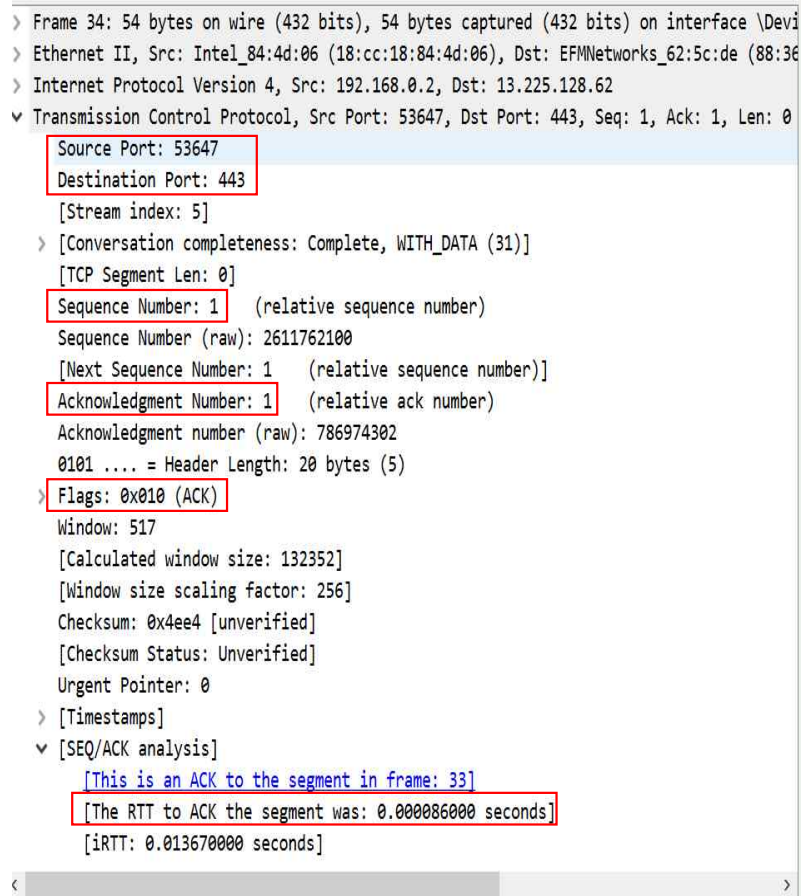


그림 5 - ACK 패킷 분석

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.

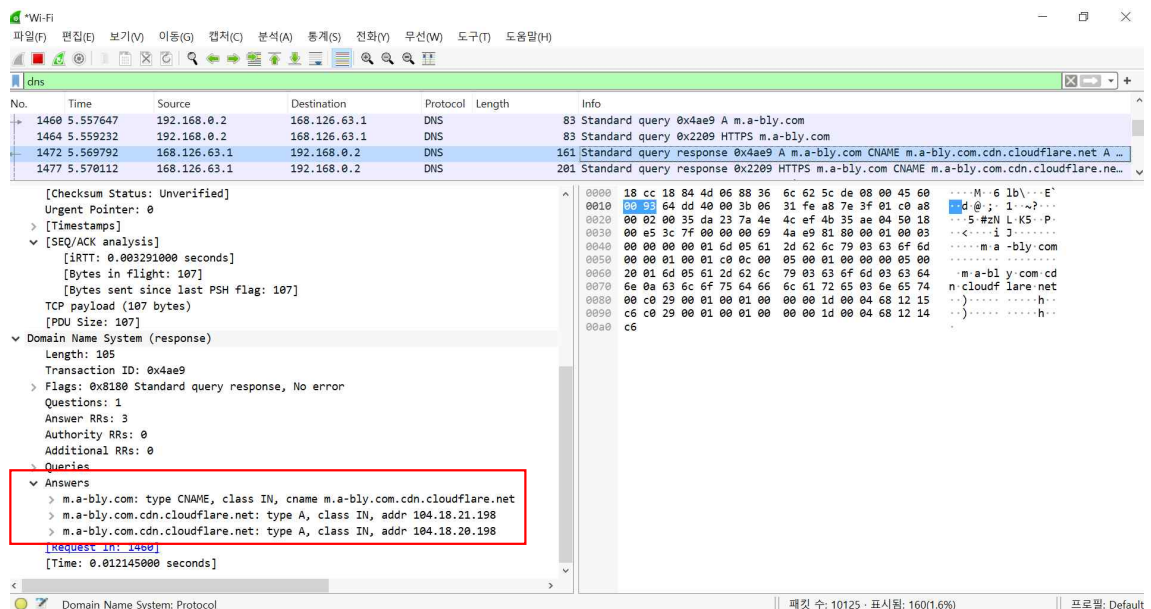


그림 6 - 에이블리 웹 사이트 DNS

No.	Time	Source	Destination	Protocol	Length	Info
1480	5.590660	192.168.0.2	104.18.21.198	TCP	66	55847 → 443 [SYN] Seq= Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1502	5.581533	104.18.21.198	192.168.0.2	TCP	66	443 → 55847 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=8192
1503	5.581589	192.168.0.2	104.18.21.198	TCP	54	55847 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
1512	5.607177	192.168.0.2	104.18.21.198	TLSv1.3		571 Client Hello (SNImm.a-bly.com)
1513	5.618777	104.18.21.198	192.168.0.2	TCP	60	443 → 55847 [ACK] Seq=1 Ack=518 Win=57344 Len=0
1514	5.620821	104.18.21.198	192.168.0.2	TLSv1.3		1514 Server Hello, Change Cipher Spec
1515	5.620821	104.18.21.198	192.168.0.2	TCP	1514	443 → 55847 [ACK] Seq=1461 Ack=518 Win=65536 Len=1460 [TCP segment of a reassembled ...]
1516	5.620867	192.168.0.2	104.18.21.198	TCP	54	55847 → 443 [ACK] Seq=518 Ack=2921 Win=131584 Len=0
1517	5.621339	104.18.21.198	192.168.0.2	TLSv1.3		1234 Application Data

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.

```
> Frame 1480: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \De
> Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: EFMNetworks_62:5c:de (88:3e
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 104.18.21.198
▼ Transmission Control Protocol, Src Port: 55847, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 55847
  Destination Port: 443
  [Stream index: 60]
  > [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2763081226
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x3ea9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Op
  > [Timestamps]
```

그림 8 - SYN 패킷 분석

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

```
▼ Transmission Control Protocol, Src Port: 443, Dst Port: 55847, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 55847
  [Stream index: 60]
  > [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 813167799
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2763081227
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x49f5 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP),
  > [Timestamps]
  ▼ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 1480]
    [The RTT to ACK the segment was: 0.010873000 seconds]
    [iRTT: 0.010929000 seconds]
```

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.

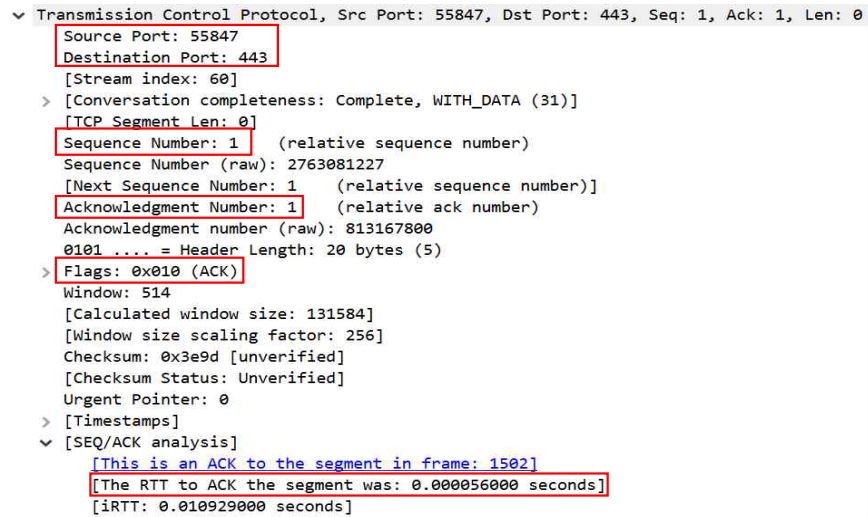


그림 10 - ACK 패킷 분석

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

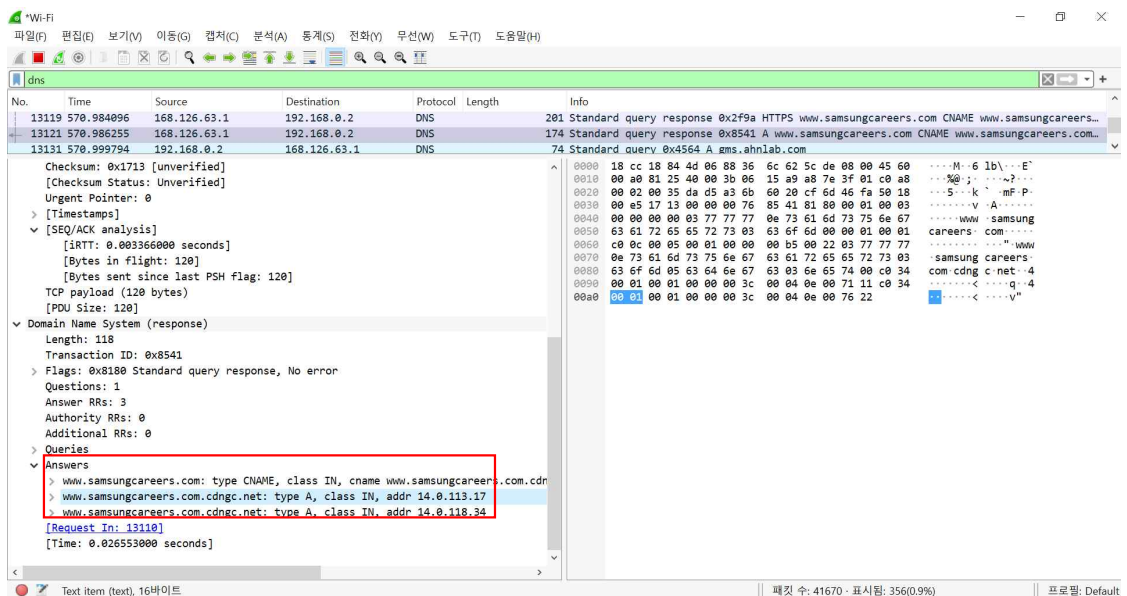


그림 11 - 삼성 커리어스 DNS

No.	Time	Source	Destination	Protocol	Length	Info
13125	570.986914	192.168.0.2	14.0.113.17	TCP	66	56023 → 443 [SYN] Seq= Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13128	570.998699	14.0.113.17	192.168.0.2	TCP	66	443 → 56023 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM WS=128
13129	570.998739	192.168.0.2	14.0.113.17	TCP	54	56023 → 443 [ACK] Seq= Ack=1 Win=131328 Len=0
13139	571.036999	192.168.0.2	14.0.113.17	TLSv1.2		596 Client Hello (SHA1=samsungcareers.com)
13140	571.046522	14.0.113.17	192.168.0.2	TCP	60	443 → 56023 [ACK] Seq=1 Ack=543 Win=48256 Len=0
13141	571.051520	14.0.113.17	192.168.0.2	TLSv1.2		1514 Server Hello
13142	571.051520	14.0.113.17	192.168.0.2	TCP		1514 443 → 56023 [ACK] Seq=1461 Ack=543 Win=48256 Len=1460 [TCP segment of a reassembled ...
13143	571.051520	14.0.113.17	192.168.0.2	TCP		1230 443 → 56023 [PSH, ACK] Seq=2921 Ack=543 Win=48256 Len=1176 [TCP segment of a reassem...
13144	571.051611	192.168.0.2	14.0.113.17	TCP	54	56023 → 443 [ACK] Seq=543 Ack=4097 Win=131328 Len=0
13145	571.054323	14.0.113.17	192.168.0.2	TLSv1.2		1078 Certificate, Server Key Exchange, Server Hello Done

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.

▼ Transmission Control Protocol, Src Port: 56023, Dst Port: 443, Seq: 0, Len: 0
Source Port: 56023
Destination Port: 443
[Stream index: 254]
> [Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 4069347026
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x3fe2 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Ope
> [Timestamps]

그림 13 - SYN 패킷 분석

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

```

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 56023, Seq: 0, Ack: 1, Len:
  Source Port: 443
  Destination Port: 56023
  [Stream index: 254]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1031557086
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4069347027
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window: 42340
  [Calculated window size: 42340]
  Checksum: 0xde92 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP)
  > [Timestamps]
  ▼ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 13125]
    [The RTT to ACK the segment was: 0.011785000 seconds]
    [iRTT: 0.011825000 seconds]

```

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.

```

▼ Transmission Control Protocol, Src Port: 56023, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 56023
  Destination Port: 443
  [Stream index: 254]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 4069347027
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1031557087
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
  Checksum: 0x3fd6 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  ▼ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 13128]
    [The RTT to ACK the segment was: 0.000040000 seconds]
    [iRTT: 0.011825000 seconds]

```

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

4436	107.547359	192.168.0.2	164.125.8.25	HTTP	1453 GET /bbs/cse/2605/865074/download.do HTTP/1.1
4437	107.576830	164.125.8.25	192.168.0.2	TCP	60 80 → 56516 [ACK] Seq=384742 Ack=21230 Win=65535 Len=0
4438	109.734409	164.125.8.25	192.168.0.2	TCP	1434 80 → 56516 [ACK] Seq=384742 Ack=21230 Win=65535 Len=1380 [TCP segment of a reassembl...
4439	109.734409	164.125.8.25	192.168.0.2	TCP	1434 80 → 56516 [ACK] Seq=386122 Ack=21230 Win=65535 Len=1380 [TCP segment of a reassembl...
4440	109.734409	164.125.8.25	192.168.0.2	TCP	1434 80 → 56516 [ACK] Seq=387502 Ack=21230 Win=65535 Len=1380 [TCP segment of a reassembl...
4441	109.734409	164.125.8.25	192.168.0.2	TCP	1434 80 → 56516 [ACK] Seq=388882 Ack=21230 Win=65535 Len=1380 [TCP segment of a reassembl...
4442	109.734409	164.125.8.25	192.168.0.2	TCP	1434 80 → 56516 [ACK] Seq=390262 Ack=21230 Win=65535 Len=1380 [TCP segment of a reassembl...
4443	109.734409	164.125.8.25	192.168.0.2	TCP	1434 80 → 56516 [ACK] Seq=391642 Ack=21230 Win=65535 Len=1380 [TCP segment of a reassembl...

그림 16 - 첨부파일 다운로드 후 캡처된 패킷

```

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 56516, Seq: 384742, Ack: 21230, Len: 0
  Source Port: 80
  Destination Port: 56516
  [Stream index: 27]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 384742 (relative sequence number)
  Sequence Number (raw): 4048566537
  [Next Sequence Number: 384742 (relative sequence number)]
  Acknowledgment Number: 21230 (relative ack number)
  Acknowledgment number (raw): 3869885476
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 65535
  [Calculated window size: 65535]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x9056 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  ▼ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 4436]
    [The RTT to ACK the segment was: 0.029471000 seconds]
    [iRTT: 0.022195000 seconds]

```

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.

```

v Transmission Control Protocol, Src Port: 80, Dst Port: 56516, Seq: 384742, Ack: 21230, Len: 1380
  Source Port: 80
  Destination Port: 56516
  [Stream index: 27]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 1380]
  Sequence Number: 384742 (relative sequence number)
  Sequence Number (raw): 4048566537
  [Next Sequence Number: 386122 (relative sequence number)]
  Acknowledgment Number: 21230 (relative ack number)
  Acknowledgment number (raw): 3869885476
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 65535
  [Calculated window size: 65535]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x0f69 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  v [SEQ/ACK analysis]
    [iRTT: 0.022195000 seconds]
    [Bytes in flight: 1380]
    [Bytes sent since last PSH flag: 1380]
    TCP payload (1380 bytes)
    [Reassembled PDU in frame: 4767]
    TCP segment data (1380 bytes)

```

그림 18 - 캡처된 두 번째 패킷

두 번째 패킷은 1380의 길이로 80번 포트에서 56516 포트로 전송된다. seq는 384742에서 데이터의 크기인 1380을 더한 386122이다. ack는 21230으로 ACK요청을 한다. Window크기는 65535이다.

```

> Internet Protocol Version 4, Src: 164.125.8.25, Dst: 192.168.0.2
v Transmission Control Protocol, Src Port: 80, Dst Port: 56516, Seq: 386122, Ack: 21230, Len: 1380
  Source Port: 80
  Destination Port: 56516
  [Stream index: 27]
  > [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 1380]
  Sequence Number: 386122 (relative sequence number)
  Sequence Number (raw): 4048567917
  [Next Sequence Number: 387502 (relative sequence number)]
  Acknowledgment Number: 21230 (relative ack number)
  Acknowledgment number (raw): 3869885476
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 65535
  [Calculated window size: 65535]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0xe92b [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  v [SEQ/ACK analysis]
    [iRTT: 0.022195000 seconds]
    [Bytes in flight: 2760]
    [Bytes sent since last PSH flag: 2760]
    TCP payload (1380 bytes)
    [Reassembled PDU in frame: 4767]
    TCP segment data (1380 bytes)

```

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

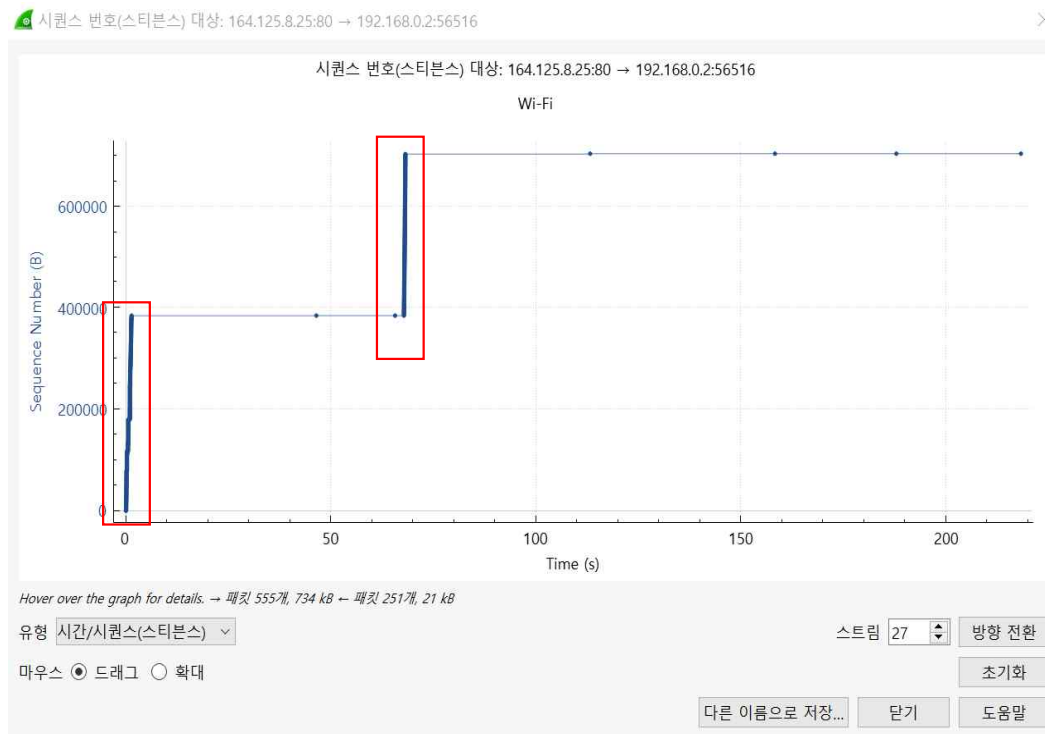


그림 20 - seq/time 스티븐스 그래프

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]

```

> Frame 186: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_
> Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 310
    Checksum: 0x4f84 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
    > [Timestamps]
    UDP payload (302 bytes)
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xde1f0684
    Seconds elapsed: 0
    > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP

```

그림 22 - DHCP - DISCOVER 패킷 분석

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

```

v Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
v Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
v Option: (50) Requested IP Address (192.168.0.2)
    Length: 4
    Requested IP Address: 192.168.0.2
v Option: (12) Host Name
    Length: 15
    Host Name: LAPTOP-6F7NTDU7
v Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
v Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
v Option: (255) End
    Option End: 255

```

그림 23 - DHCP - DISCOVER 옵션

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.

```
> Frame 189: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{58FA98A7-799C-4E6A-8000-000000000000}
> Ethernet II, Src: EFMNetworks_62:5c:de (88:36:6c:62:5c:de), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
√ User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 556
    Checksum: 0x11fb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
    > [Timestamps]
    UDP payload (548 bytes)
√ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xde1f0684
    Seconds elapsed: 0
    > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.2
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

DHCP Offer는 네트워크에서 Discover의 응답으로 클라이언트에게 IP를 할당을 시도한다.

그림 25 - DHCP - OFFER 옵션

[DHCP - Request]

```
> Frame 190: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{5BFA98A7-799C}
> Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 336
    Checksum: 0x1b54 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
    > [Timestamps]
    UDP payload (328 bytes)
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xde1f0684
    Seconds elapsed: 0
    > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

그림 26 - DHCP - REQUEST 패킷 분석

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

```
v Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
v Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
v Option: (50) Requested IP Address (192.168.0.2)
    Length: 4
    Requested IP Address: 192.168.0.2
v Option: (54) DHCP Server Identifier (192.168.0.1)
    Length: 4
    DHCP Server Identifier: 192.168.0.1
v Option: (12) Host Name
    Length: 15
    Host Name: LAPTOP-6F7NTDU7
v Option: (81) Client Fully Qualified Domain Name
    Length: 18
    > Flags: 0x00
    A-RR result: 0
    PTR-RR result: 0
    Client name: LAPTOP-6F7NTDU7
v Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
v Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
v Option: (255) End
    Option End: 255
```

그림 27 - DHCP - REQUEST 옵션

[DHCP - ACK]

```
> Frame 197: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{58FA98A7-799C-4823-A355-D3BDF9339BCA}, id 0
> Ethernet II, Src: EFMNetworks_62:5c:de:88:36:6c:62:5c:de, Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 556
    Checksum: 0x0efb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
    > [Timestamps]
        UDP payload (548 bytes)
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xdelf0684
    Seconds elapsed: 0
    > Bootp flags: 0x8000, Broadcast flag (Broadcast)
        Client IP address: 0.0.0.0
        Your (client) IP address: 192.168.0.2
        Next server IP address: 0.0.0.0
        Relay agent IP address: 0.0.0.0
        Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
        Client hardware address padding: 00000000000000000000
        Server host name not given
        Boot file name not given
        Magic cookie: DHCP
```

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 할당받았음을 확인할 수 있다.

[illegible]

그림 29 - DHCP - ACK 옵션

[DHCP - Release]

```
> Frame 152: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{5BFA98A7-799C-4E6A-8000-000000000000}
> Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: EFMNetworks_62:5c:de (88:36:6c:62:5c:de)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
  Source Port: 68
  Destination Port: 67
  Length: 308
  Checksum: 0x8299 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  UDP payload (300 bytes)
> Dynamic Host Configuration Protocol (Release)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x5767222c
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 192.168.0.2
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

그림 30 - DHCP - Release 패킷 분석

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

[illegible]

그림 31 - DHCP - Release 옵션

3. ARP

arp -a -> arp -d *를 관리자 권한으로 실행 후

3-1. ARP request, ARP reply 패킷을 분석

1530 267.554742	EFMNetworks_62:5c:de	Broadcast	ARP	42 Who has 192.168.0.7? Tell 192.168.0.1
1945 288.379154	EFMNetworks_62:5c:de	Intel_84:4d:06	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1
1946 288.379225	Intel_84:4d:06	EFMNetworks_62:5c:de	ARP	42 192.168.0.2 is at 18:cc:18:84:4d:06
7078 336.069150	EFMNetworks_62:5c:de	Intel_84:4d:06	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1
7079 336.069211	Intel_84:4d:06	EFMNetworks_62:5c:de	ARP	42 192.168.0.2 is at 18:cc:18:84:4d:06
7659 369.236926	EFMNetworks_62:5c:de	Broadcast	ARP	42 Who has 192.168.0.6? Tell 192.168.0.1
7865 399.359434	EFMNetworks_62:5c:de	Intel_84:4d:06	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1
7866 399.359468	Intel_84:4d:06	EFMNetworks_62:5c:de	ARP	42 192.168.0.2 is at 18:cc:18:84:4d:06
8033 459.109609	EFMNetworks_62:5c:de	Intel_84:4d:06	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1
8034 459.109646	Intel_84:4d:06	EFMNetworks_62:5c:de	ARP	42 192.168.0.2 is at 18:cc:18:84:4d:06

그림 32 - 캡처된 ARP 메시지 패킷

```
> Frame 1530: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_
▼ Ethernet II, Src: EFMNetworks_62:5c:de (88:36:6c:62:5c:de), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: EFMNetworks_62:5c:de (88:36:6c:62:5c:de)
  Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: EFMNetworks_62:5c:de (88:36:6c:62:5c:de)
  Sender IP address: 192.168.0.1
  Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.7
```

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.

```
> Frame 1946: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▼ Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: EFMNetworks_62:5c:de (88:36:6c:62:5c:de)
  > Destination: EFMNetworks_62:5c:de (88:36:6c:62:5c:de)
  > Source: Intel_84:4d:06 (18:cc:18:84:4d:06)
  Type: ARP (0x0806)
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Intel_84:4d:06 (18:cc:18:84:4d:06)
  Sender IP address: 192.168.0.2
  Target MAC address: EFMNetworks_62:5c:de (88:36:6c:62:5c:de)
  Target IP address: 192.168.0.1
```

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.

http						
No.	Time	Source	Destination	Protocol	Length	Info
862	68.679487	192.168.0.2	164.125.8.25	HTTP	1111	GET /cse/index.do HTTP/1.1
> Frame 862: 1111 bytes on wire (8888 bits), 1111 bytes captured (8888 bits) on interface \Device\NPF_{5BFA98A7-799C-4B23-A355-D3BDF9339BCA}, id 0 > Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: EFMNetworks_62:5c:de (88:36:6c:62:5c:de) > Internet Protocol Version 4, Src: 192.168.0.2, Dst: 164.125.8.25 > Transmission Control Protocol, Src Port: 59605, Dst Port: 80, Seq: 2, Ack: 1, Len: 1057 Source Port: 59605 Destination Port: 80 [Stream index: 42] > [Conversation completeness: Incomplete (12)] [TCP Segment Len: 1057] Sequence Number: 2 (relative sequence number) Sequence Number (raw): 2088119151 [Next Sequence Number: 1059 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 1043700937 0101 = Header Length: 20 bytes (5) > Flags: 0x018 (PSH, ACK) Window: 64454 [Calculated window size: 64454] [Window size scaling factor: -1 (unknown)] Checksum: 0x717c [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 > [Timestamps] > [SEQ/ACK analysis] [Bytes in flight: 1057] [Bytes sent since last PSH flag: 1058] TCP payload (1057 bytes)						

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?

0000	88 36 6c 62 5c de 18 cc 18 84 4d 06 08 00 45 00	·61b\... ·M...E·
0010	04 49 d6 04 40 00 80 06 00 00 c0 a8 00 02 a4 7d	·I·@... ·.....}
0020	08 19 e8 d5 00 50 7c 76 2b 6f 3e 35 9c c9 50 18	·...·P v +o>5·P·
0030	fb c6 71 7c 00 00 47 45 54 20 2f 63 73 65 2f 69	··q ·GE T /cse/i
0040	6e 64 65 78 2e 64 6f 20 48 54 54 50 2f 31 2e 31	ndex.do HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20 63 73 65 2e 70 75 73 61	··Host: cse.pusa
0060	6e 2e 61 63 2e 6b 72 0d 0a 43 6f 6e 6e 65 63 74	n.ac.kr· Connect
0070	69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d	ion: kee p-alive·
0080	0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72	·Upgrade -Insecur
0090	65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55	e-Reques ts: 1·U
00a0	73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c	ser-Agen t: Mozil
00b0	6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20	la/5.0 (Windows
00c0	4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20	NT 10.0; Win64;
00d0	78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74	x64) App leWebKit
00e0	2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20	/537.36 (KHTML,
00f0	6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f	like Gec ko) Chro
0100	6d 65 2f 31 31 39 2e 30 2e 30 2e 30 20 53 61 66	me/119.0 .0 Saf
0110	61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65	ari/537. 36·Acce
0120	70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70	pt: text /html,ap
0130	70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtmll+
0140	78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f	xml,application/
0150	78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f	xml;q=0. 9,image/

그림 36 - ‘G’ 이전까지의 총 BYTE

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

> Frame 862: 1111 bytes on wire (8888 bits), 1111 bytes captured (8888 bits) on interface 0	0000	88 36 6c 62 5c de 18 cc 18 84 4d 06 08 00 45 00	·61b\... ·M...E·
> Ethernet II, Src: Intel_84:4d:06 (18:cc:18:84:4d:06), Dst: EFMNetworks_62:5c:de (88:04:49:d6:04:40:00:80:06)	0010	04 49 d6 04 40 00 80 06 00 00 c0 a8 00 02 a4 7d	·I·@... ·.....}
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 164.125.8.25	0020	08 19 e8 d5 00 50 7c 76 2b 6f 3e 35 9c c9 50 18	·...·P v +o>5·P·
> Transmission Control Protocol, Src Port: 59605, Dst Port: 80, Seq: 2, Ack: 1, Len: 1	0030	fb c6 71 7c 00 00 47 45 54 20 2f 63 73 65 2f 69	··q ·GE T /cse/i
> Hypertext Transfer Protocol	0040	6e 64 65 78 2e 64 6f 20 48 54 54 50 2f 31 2e 31	ndex.do HTTP/1.1
	0050	0d 0a 48 6f 73 74 3a 20 63 73 65 2e 70 75 73 61	··Host: cse.pusa
	0060	6e 2e 61 63 2e 6b 72 0d 0a 43 6f 6e 6e 65 63 74	n.ac.kr· Connect
	0070	69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d	ion: kee p-alive·
	0080	0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72	·Upgrade -Insecur
	0090	65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55	e-Reques ts: 1·U
	00a0	73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c	ser-Agen t: Mozil
	00b0	6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20	la/5.0 (Windows
	00c0	4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20	NT 10.0; Win64;
	00d0	78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74	x64) App leWebKit
	00e0	2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20	/537.36 (KHTML,
	00f0	6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f	like Gec ko) Chro
	0100	6d 65 2f 31 31 39 2e 30 2e 30 2e 30 20 53 61 66	me/119.0 .0 Saf
	0110	61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65	ari/537. 36·Acce
	0120	70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70	pt: text /html,ap
	0130	70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtmll+
	0140	78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f	xml,application/
	0150	78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f	xml;q=0. 9,image/

그림 37 - Link Layer frame header 크기

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