정보보호학개론

네트워크 패킷 분석

Team_Safe Zone

CONTENTS

01

팀원 소개

02

분석 도구

03

Wireshark 실습

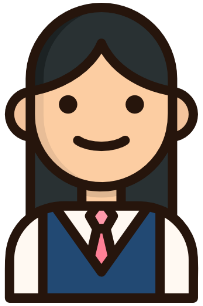
04

Hping3 실습

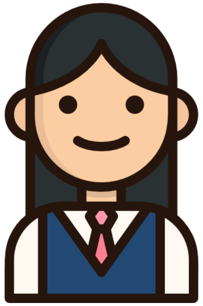
Team_Safe Zone

팀원 소개

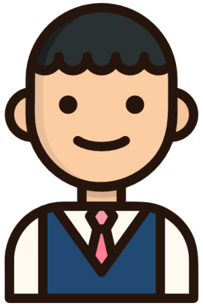
01 팀원 소개



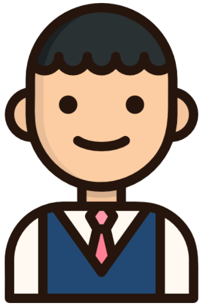
최유미
자료조사



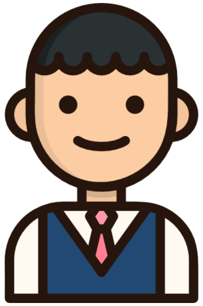
조윤서
자료조사



김윤호
발표



강민혁
자료조사



어영민
PPT 제작

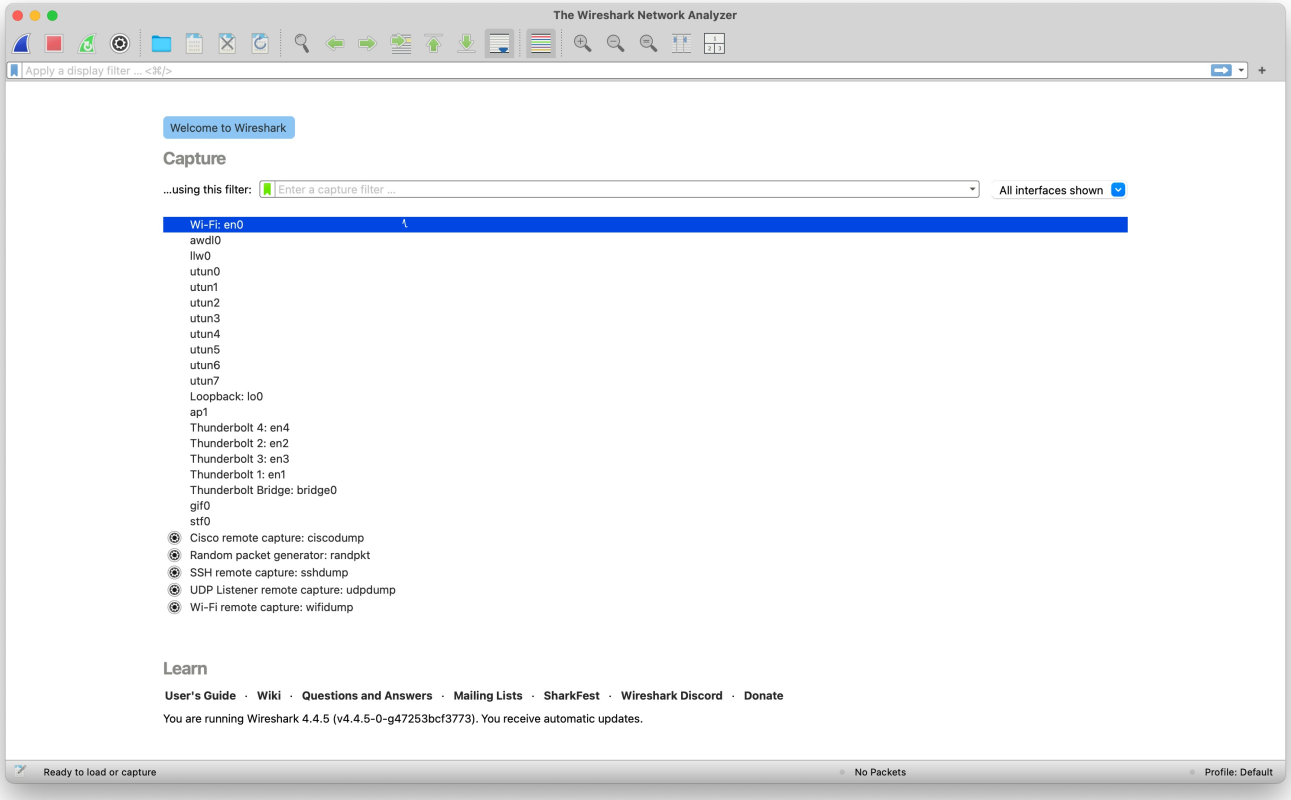
네트워크 패킷 분석

분석 도구

02

분석 도구

Wireshark, hping3



The Wireshark Network Analyzer

Apply a display filter ... <⌘/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi: en0
awdl0
llw0
utun0
utun1
utun2
utun3
utun4
utun5
utun6
utun7
Loopback: lo0
ap1
Thunderbolt 4: en4
Thunderbolt 2: en2
Thunderbolt 3: en3
Thunderbolt 1: en1
Thunderbolt Bridge: bridge0
gif0
stf0
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

Learn

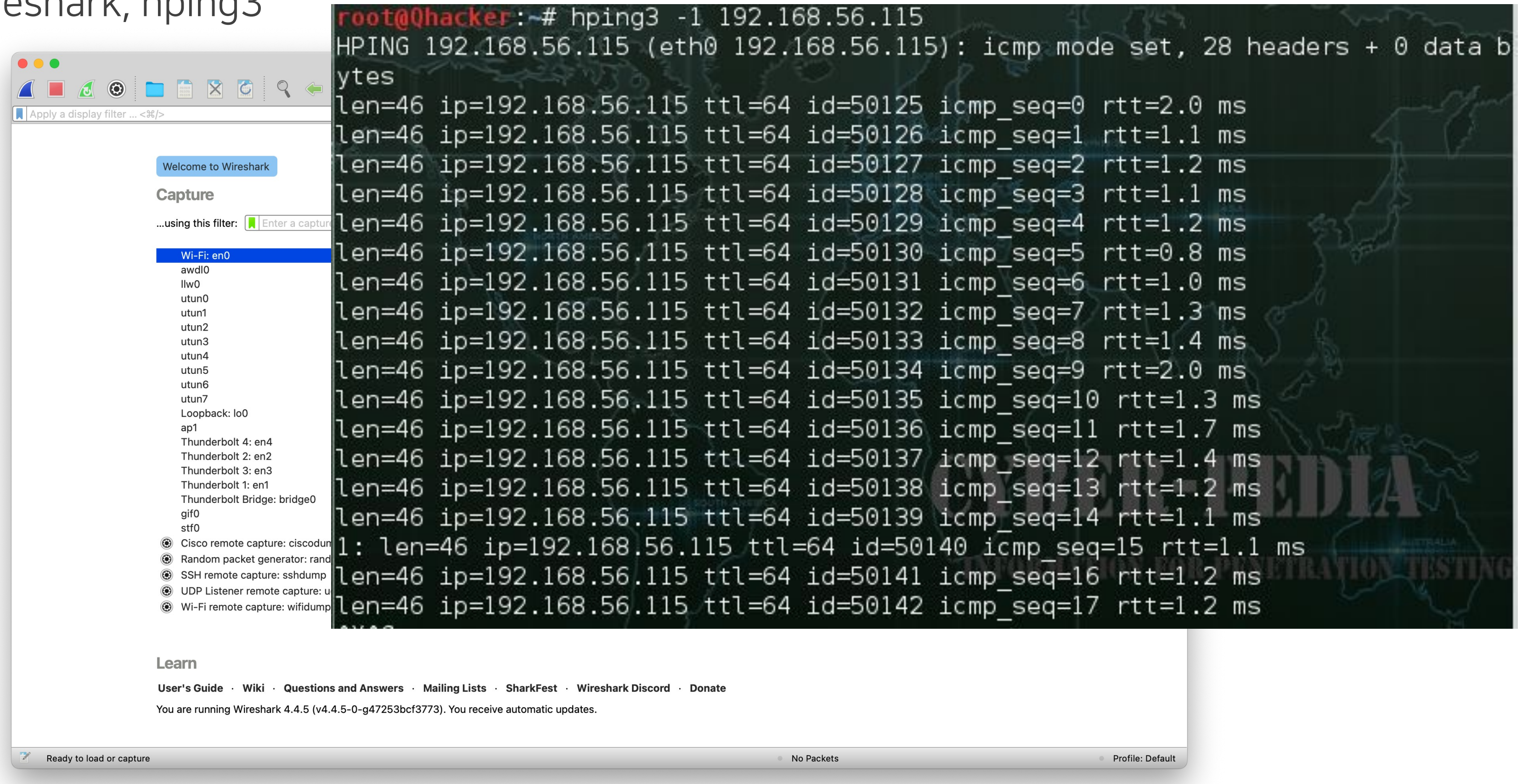
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.5 (v4.4.5-0-g47253bcf3773). You receive automatic updates.

Ready to load or capture No Packets Profile: Default

02 분석 도구

Wireshark, hping3



```
root@Qhacker:~# hping3 -1 192.168.56.115
HPING 192.168.56.115 (eth0 192.168.56.115): icmp mode set, 28 headers + 0 data b
ytes
len=46 ip=192.168.56.115 ttl=64 id=50125 icmp_seq=0 rtt=2.0 ms
len=46 ip=192.168.56.115 ttl=64 id=50126 icmp_seq=1 rtt=1.1 ms
len=46 ip=192.168.56.115 ttl=64 id=50127 icmp_seq=2 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50128 icmp_seq=3 rtt=1.1 ms
len=46 ip=192.168.56.115 ttl=64 id=50129 icmp_seq=4 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50130 icmp_seq=5 rtt=0.8 ms
len=46 ip=192.168.56.115 ttl=64 id=50131 icmp_seq=6 rtt=1.0 ms
len=46 ip=192.168.56.115 ttl=64 id=50132 icmp_seq=7 rtt=1.3 ms
len=46 ip=192.168.56.115 ttl=64 id=50133 icmp_seq=8 rtt=1.4 ms
len=46 ip=192.168.56.115 ttl=64 id=50134 icmp_seq=9 rtt=2.0 ms
len=46 ip=192.168.56.115 ttl=64 id=50135 icmp_seq=10 rtt=1.3 ms
len=46 ip=192.168.56.115 ttl=64 id=50136 icmp_seq=11 rtt=1.7 ms
len=46 ip=192.168.56.115 ttl=64 id=50137 icmp_seq=12 rtt=1.4 ms
len=46 ip=192.168.56.115 ttl=64 id=50138 icmp_seq=13 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50139 icmp_seq=14 rtt=1.1 ms
1: len=46 ip=192.168.56.115 ttl=64 id=50140 icmp_seq=15 rtt=1.1 ms
len=46 ip=192.168.56.115 ttl=64 id=50141 icmp_seq=16 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50142 icmp_seq=17 rtt=1.2 ms
```

Capture

...using this filter: Enter a captur

- Wi-Fi: en0
- awdl0
- llw0
- utun0
- utun1
- utun2
- utun3
- utun4
- utun5
- utun6
- utun7
- Loopback: lo0
- ap1
- Thunderbolt 4: en4
- Thunderbolt 2: en2
- Thunderbolt 3: en3
- Thunderbolt 1: en1
- Thunderbolt Bridge: bridge0
- gif0
- stf0
- ⦿ Cisco remote capture: ciscodum
- ⦿ Random packet generator: rand
- ⦿ SSH remote capture: sshdump
- ⦿ UDP Listener remote capture: u
- ⦿ Wi-Fi remote capture: wifidump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

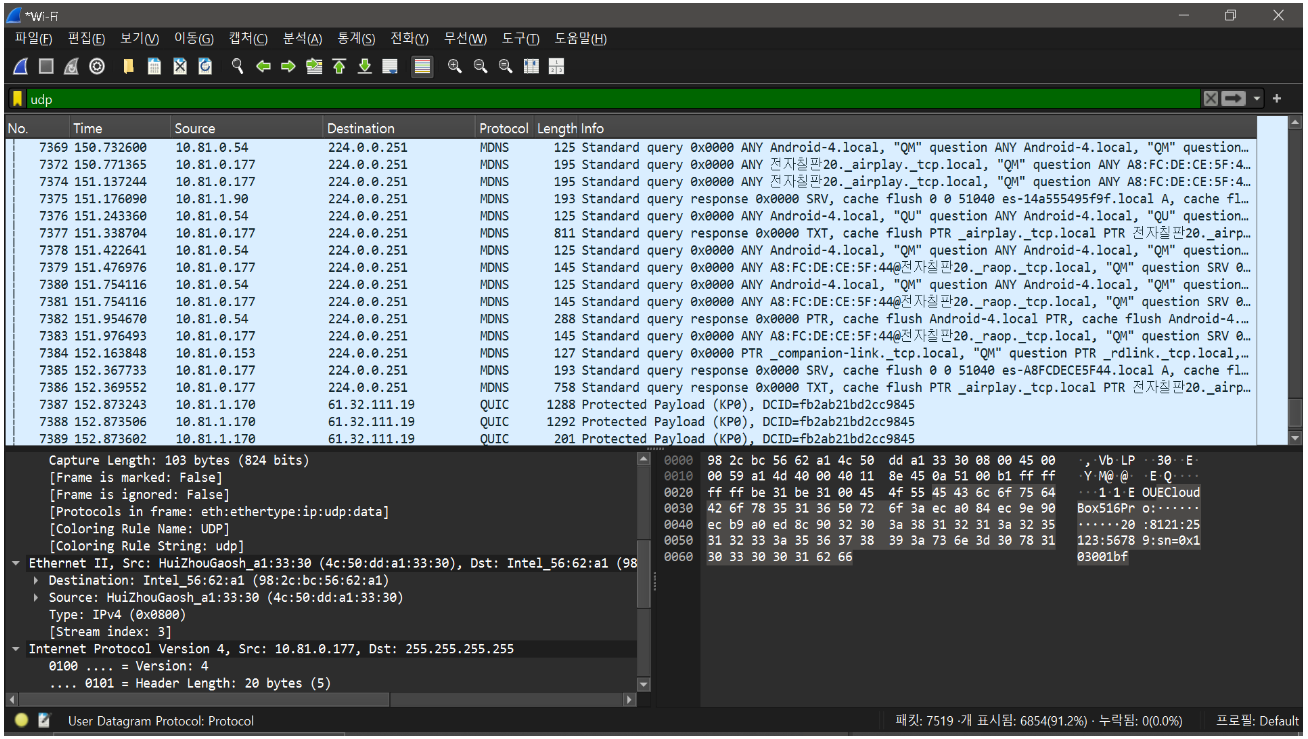
You are running Wireshark 4.4.5 (v4.4.5-0-g47253bcf3773). You receive automatic updates.

실습

Wireshark

03 wireshark

Wi-fi 패킷 분석


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)
udp

```
No.     Time        Source        Destination   Protocol Length Info
   7369 150.732600  10.81.0.54    224.0.0.251   MDNS      125 Standard query 0x0000 ANY Android-4.local, "QM" question ANY Android-4.local, "QM" question…
   7372 150.771365  10.81.0.177   224.0.0.251   MDNS      195 Standard query 0x0000 ANY 전자칠판20._airplay._tcp.local, "QM" question ANY A8:FC:DE:CE:5F:4…
   7374 151.137244  10.81.0.177   224.0.0.251   MDNS      195 Standard query 0x0000 ANY 전자칠판20._airplay._tcp.local, "QM" question ANY A8:FC:DE:CE:5F:4…
   7375 151.176090  10.81.1.90    224.0.0.251   MDNS      193 Standard query response 0x0000 SRV, cache flush 0 0 51040 es-14a555495f9f.local A, cache fl…
   7376 151.243360  10.81.0.54    224.0.0.251   MDNS      125 Standard query 0x0000 ANY Android-4.local, "QU" question ANY Android-4.local, "QU" question…
   7377 151.338704  10.81.0.177   224.0.0.251   MDNS      811 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR 전자칠판20._airp…
   7378 151.422641  10.81.0.54    224.0.0.251   MDNS      125 Standard query 0x0000 ANY Android-4.local, "QM" question ANY Android-4.local, "QM" question…
   7379 151.476976  10.81.0.177   224.0.0.251   MDNS      145 Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전자칠판20._raop._tcp.local, "QM" question SRV 0…
   7380 151.754116  10.81.0.54    224.0.0.251   MDNS      125 Standard query 0x0000 ANY Android-4.local, "QM" question ANY Android-4.local, "QM" question…
   7381 151.754116  10.81.0.177   224.0.0.251   MDNS      145 Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전자칠판20._raop._tcp.local, "QM" question SRV 0…
   7382 151.954670  10.81.0.54    224.0.0.251   MDNS      288 Standard query response 0x0000 PTR, cache flush Android-4.local PTR, cache flush Android-4.…
   7383 151.976493  10.81.0.177   224.0.0.251   MDNS      145 Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전자칠판20._raop._tcp.local, "QM" question SRV 0…
   7384 152.163848  10.81.0.153   224.0.0.251   MDNS      127 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local,…
   7385 152.367733  10.81.0.177   224.0.0.251   MDNS      193 Standard query response 0x0000 SRV, cache flush 0 0 51040 es-A8FCDECE5F44.local A, cache fl…
   7386 152.369552  10.81.0.177   224.0.0.251   MDNS      758 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR 전자칠판20._airp…
   7387 152.873243  10.81.1.170   61.32.111.19  QUIC     1288 Protected Payload (KP0), DCID=fb2ab21bd2cc9845
   7388 152.873506  10.81.1.170   61.32.111.19  QUIC     1292 Protected Payload (KP0), DCID=fb2ab21bd2cc9845
   7389 152.873602  10.81.1.170   61.32.111.19  QUIC      201 Protected Payload (KP0), DCID=fb2ab21bd2cc9845
```

```
    Capture Length: 103 bytes (824 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  Ethernet II, Src: HuiZhouGaosh_a1:33:30 (4c:50:dd:a1:33:30), Dst: Intel_56:62:a1 (98
    Destination: Intel_56:62:a1 (98:2c:bc:56:62:a1)
    Source: HuiZhouGaosh_a1:33:30 (4c:50:dd:a1:33:30)
    Type: IPv4 (0x0800)
    [Stream index: 3]
  Internet Protocol Version 4, Src: 10.81.0.177, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

```
0000  98 2c bc 56 62 a1 4c 50  dd a1 33 30 08 00 45 00   ·,·Vb·LP ··30··E·
0010  00 59 a1 4d 40 00 40 11  8e 45 0a 51 00 b1 ff ff   ·Y·M@·@· ·E·Q····
0020  ff ff be 31 be 31 00 45  4f 55 45 43 6c 6f 75 64   ···1·1·E OUECloud
0030  42 6f 78 35 31 36 50 72  6f 3a ec a0 84 ec 9e 90   Box516Pr o:······
0040  ec b9 a0 ed 8c 90 32 30  3a 38 31 32 31 3a 32 35   ······20 :8121:25
0050  31 32 33 3a 35 36 37 38  39 3a 73 6e 3d 30 78 31   123:5678 9:sn=0x1
0060  30 33 30 30 31 62 66                               03001bf
```

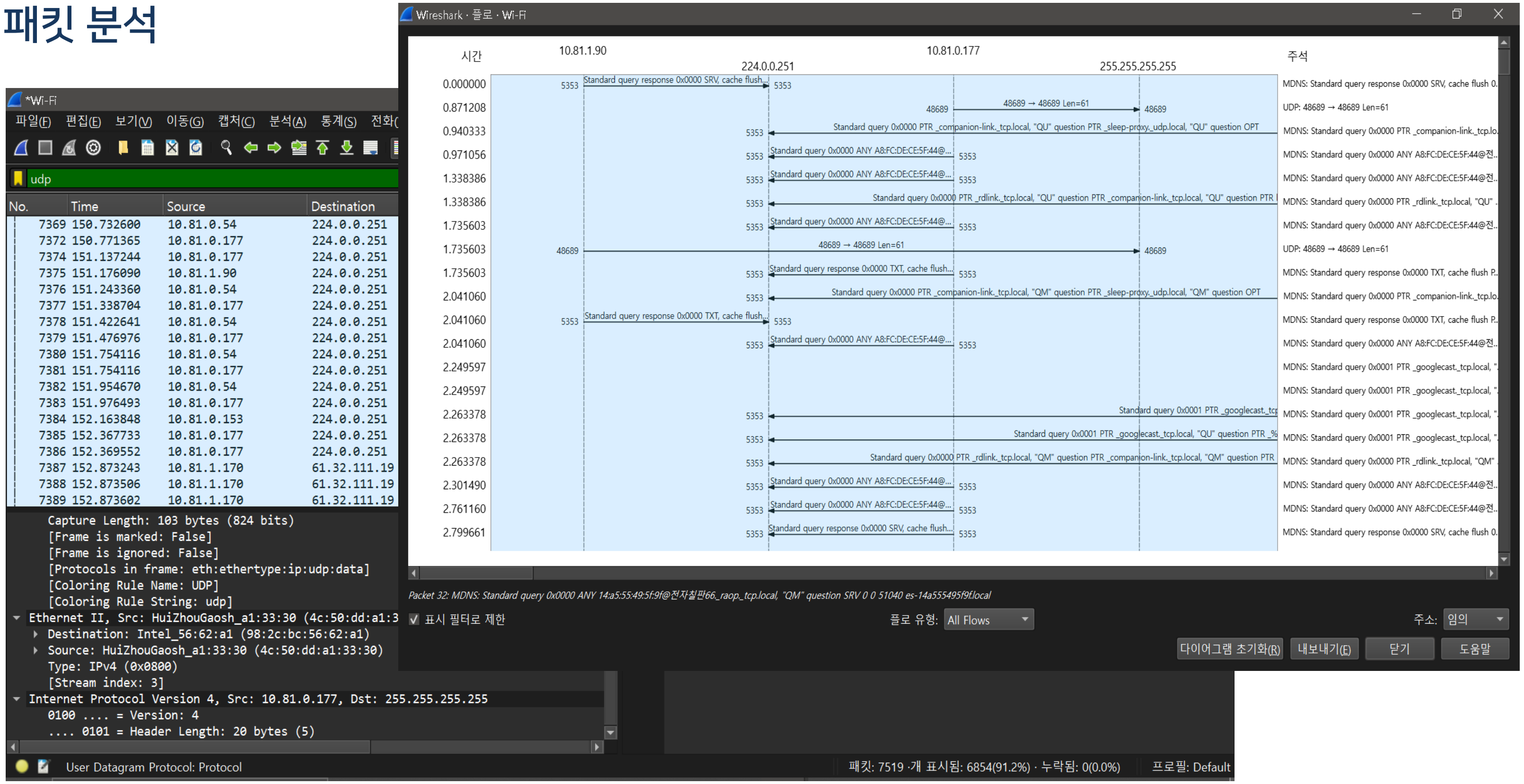
User Datagram Protocol: Protocol

패킷: 7519 ·개 표시됨: 6854(91.2%) · 누락됨: 0(0.0%)

프로필: Default

03 wireshark

Wi-fi 패킷 분석


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(
udp
Wireshark · 플로 · Wi-Fi
10.81.1.90
224.0.0.251
10.81.0.177
255.255.255.255
Standard query response 0x0000 SRV, cache flush...
48689 → 48689 Len=61
Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _sleep-proxy._udp.local, "QU" question OPT
Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@...
Standard query 0x0000 PTR _rdlink._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question PTR
Standard query response 0x0000 TXT, cache flush...
Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _sleep-proxy._udp.local, "QM" question OPT
Standard query 0x0001 PTR _googlecast._tcp
Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _%
Standard query 0x0000 PTR _rdlink._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question PTR
5353
48689
☑ 표시 필터로 제한
플로 유형: All Flows
주소: 임의
다이어그램 초기화(R)
내보내기(E)
닫기
도움말

```
No.    Time          Source         Destination
  7369 150.732600    10.81.0.54     224.0.0.251
  7372 150.771365    10.81.0.177    224.0.0.251
  7374 151.137244    10.81.0.177    224.0.0.251
  7375 151.176090    10.81.1.90     224.0.0.251
  7376 151.243360    10.81.0.54     224.0.0.251
  7377 151.338704    10.81.0.177    224.0.0.251
  7378 151.422641    10.81.0.54     224.0.0.251
  7379 151.476976    10.81.0.177    224.0.0.251
  7380 151.754116    10.81.0.54     224.0.0.251
  7381 151.754116    10.81.0.177    224.0.0.251
  7382 151.954670    10.81.0.54     224.0.0.251
  7383 151.976493    10.81.0.177    224.0.0.251
  7384 152.163848    10.81.0.153    224.0.0.251
  7385 152.367733    10.81.0.177    224.0.0.251
  7386 152.369552    10.81.0.177    224.0.0.251
  7387 152.873243    10.81.1.170    61.32.111.19
  7388 152.873506    10.81.1.170    61.32.111.19
  7389 152.873602    10.81.1.170    61.32.111.19
```

```
    Capture Length: 103 bytes (824 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▾ Ethernet II, Src: HuiZhouGaosh_a1:33:30 (4c:50:dd:a1:3
  ▸ Destination: Intel_56:62:a1 (98:2c:bc:56:62:a1)
  ▸ Source: HuiZhouGaosh_a1:33:30 (4c:50:dd:a1:33:30)
    Type: IPv4 (0x0800)
    [Stream index: 3]
▾ Internet Protocol Version 4, Src: 10.81.0.177, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

User Datagram Protocol: Protocol

패킷: 7519 ·개 표시됨: 6854(91.2%) · 누락됨: 0(0.0%) 프로필: Default

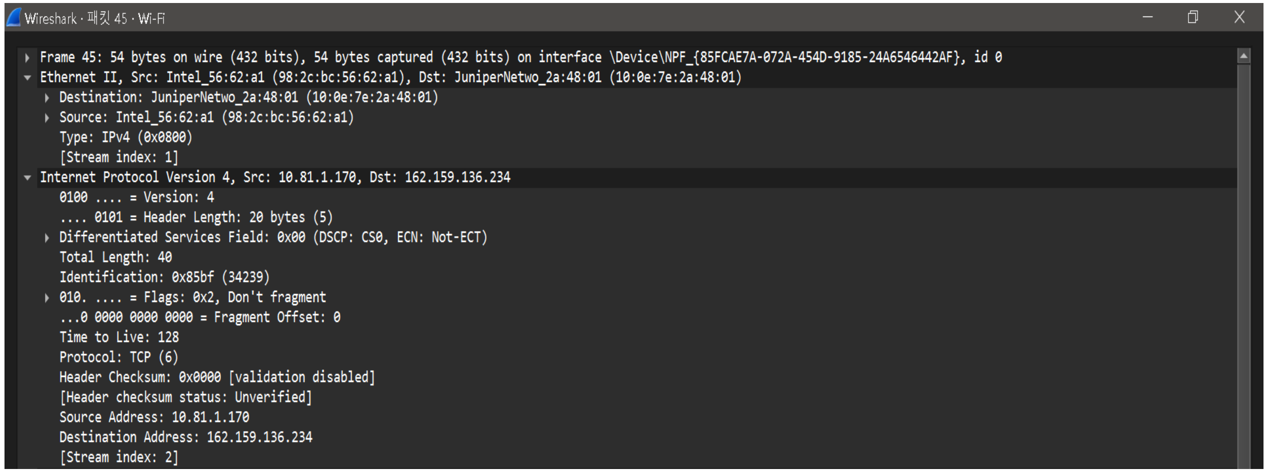
시간	주석
0.000000	MDNS: Standard query response 0x0000 SRV, cache flush 0.
0.871208	UDP: 48689 → 48689 Len=61
0.940333	MDNS: Standard query 0x0000 PTR _companion-link._tcp.lo
0.971056	MDNS: Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전..
1.338386	MDNS: Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전..
1.338386	MDNS: Standard query 0x0000 PTR _rdlink._tcp.local, "QU" .
1.735603	MDNS: Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전..
1.735603	UDP: 48689 → 48689 Len=61
1.735603	MDNS: Standard query response 0x0000 TXT, cache flush P..
2.041060	MDNS: Standard query 0x0000 PTR _companion-link._tcp.lo
2.041060	MDNS: Standard query response 0x0000 TXT, cache flush P..
2.041060	MDNS: Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전..
2.249597	MDNS: Standard query 0x0001 PTR _googlecast._tcp.local, ".
2.249597	MDNS: Standard query 0x0001 PTR _googlecast._tcp.local, ".
2.263378	MDNS: Standard query 0x0001 PTR _googlecast._tcp.local, ".
2.263378	MDNS: Standard query 0x0001 PTR _googlecast._tcp.local, ".
2.263378	MDNS: Standard query 0x0000 PTR _rdlink._tcp.local, "QM" .
2.301490	MDNS: Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전..
2.761160	MDNS: Standard query 0x0000 ANY A8:FC:DE:CE:5F:44@전..
2.799661	MDNS: Standard query response 0x0000 SRV, cache flush 0.

Packet 32: MDNS: Standard query 0x0000 ANY 14:a5:55:49:5f:9f@전자칠판66._raop._tcp.local, "QM" question SRV 0 0 51040 es-14a555495f9f.local

03

wireshark

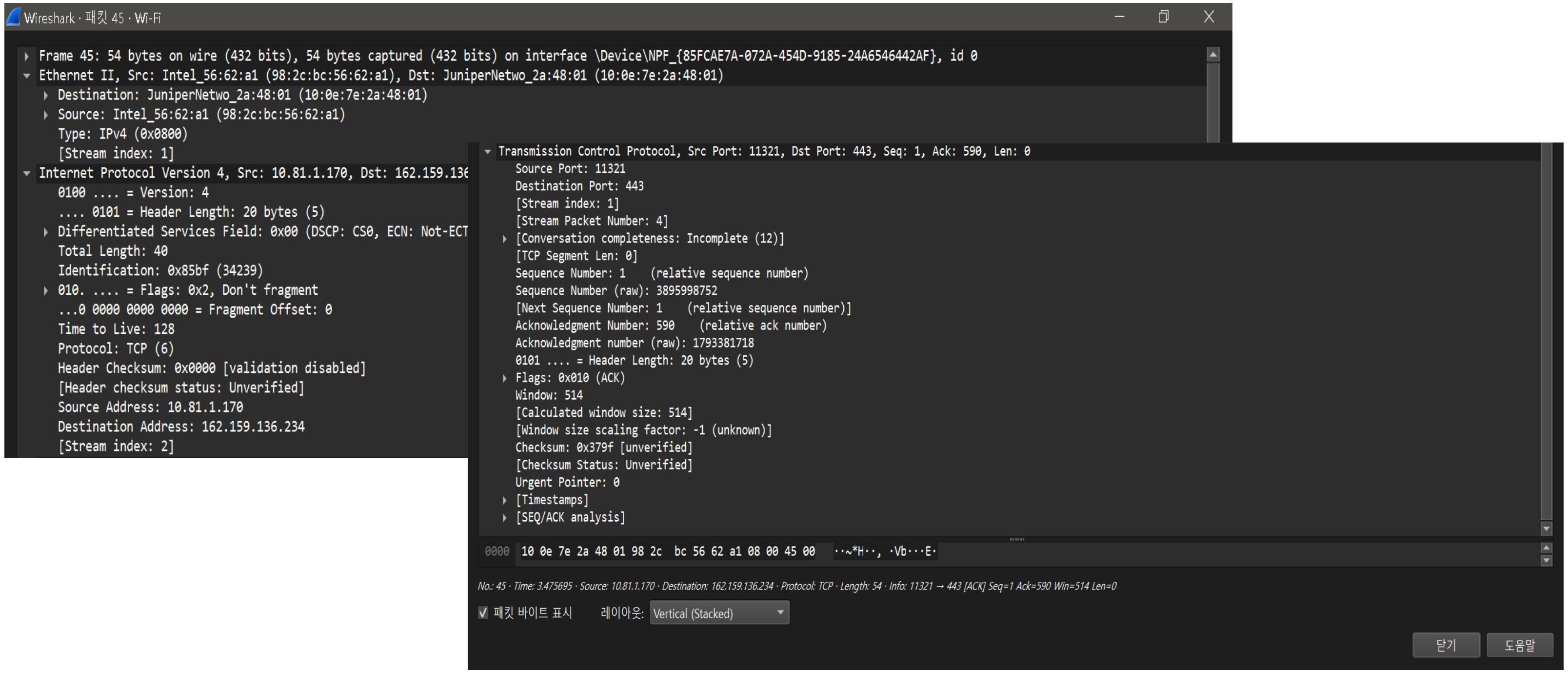
TCP



```
Frame 45: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{85FCAE7A-072A-454D-9185-24A6546442AF}, id 0
Ethernet II, Src: Intel_56:62:a1 (98:2c:bc:56:62:a1), Dst: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  Destination: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  Source: Intel_56:62:a1 (98:2c:bc:56:62:a1)
  Type: IPv4 (0x0800)
  [Stream index: 1]
Internet Protocol Version 4, Src: 10.81.1.170, Dst: 162.159.136.234
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x85bf (34239)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.81.1.170
  Destination Address: 162.159.136.234
  [Stream index: 2]
```

03 wireshark

TCP



```
▸ Frame 45: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{85FCAE7A-072A-454D-9185-24A6546442AF}, id 0
▾ Ethernet II, Src: Intel_56:62:a1 (98:2c:bc:56:62:a1), Dst: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  ▸ Destination: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  ▸ Source: Intel_56:62:a1 (98:2c:bc:56:62:a1)
    Type: IPv4 (0x0800)
    [Stream index: 1]
▾ Internet Protocol Version 4, Src: 10.81.1.170, Dst: 162.159.136
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT
    Total Length: 40
    Identification: 0x85bf (34239)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.81.1.170
    Destination Address: 162.159.136.234
    [Stream index: 2]
```

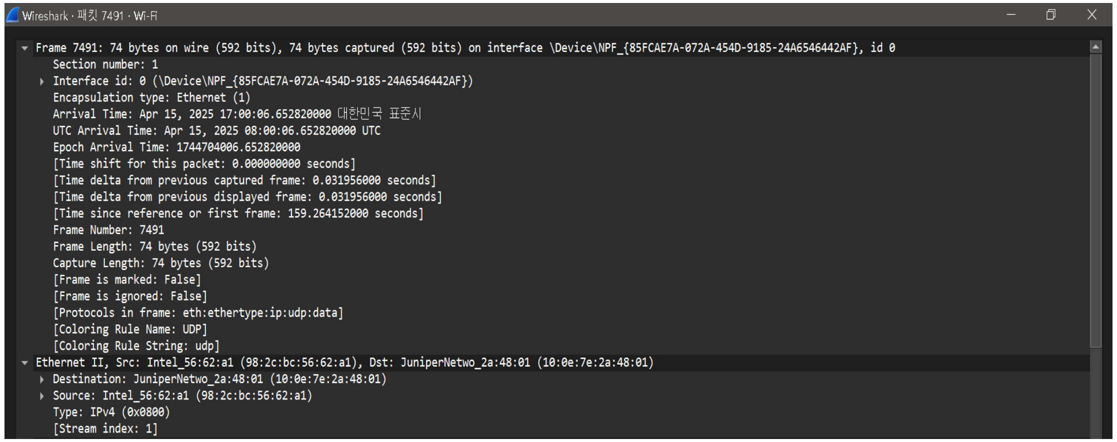
```
▾ Transmission Control Protocol, Src Port: 11321, Dst Port: 443, Seq: 1, Ack: 590, Len: 0
    Source Port: 11321
    Destination Port: 443
    [Stream index: 1]
    [Stream Packet Number: 4]
  ▸ [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3895998752
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 590    (relative ack number)
    Acknowledgment number (raw): 1793381718
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 514
    [Calculated window size: 514]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x379f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]

0000  10 0e 7e 2a 48 01 98 2c  bc 56 62 a1 08 00 45 00   ··~*H··, ·Vb···E·
```

No.: 45 · Time: 3.475695 · Source: 10.81.1.170 · Destination: 162.159.136.234 · Protocol: TCP · Length: 54 · Info: 11321 → 443 [ACK] Seq=1 Ack=590 Win=514 Len=0

☑ 패킷 바이트 표시 레이아웃: Vertical (Stacked)

03 wireshark

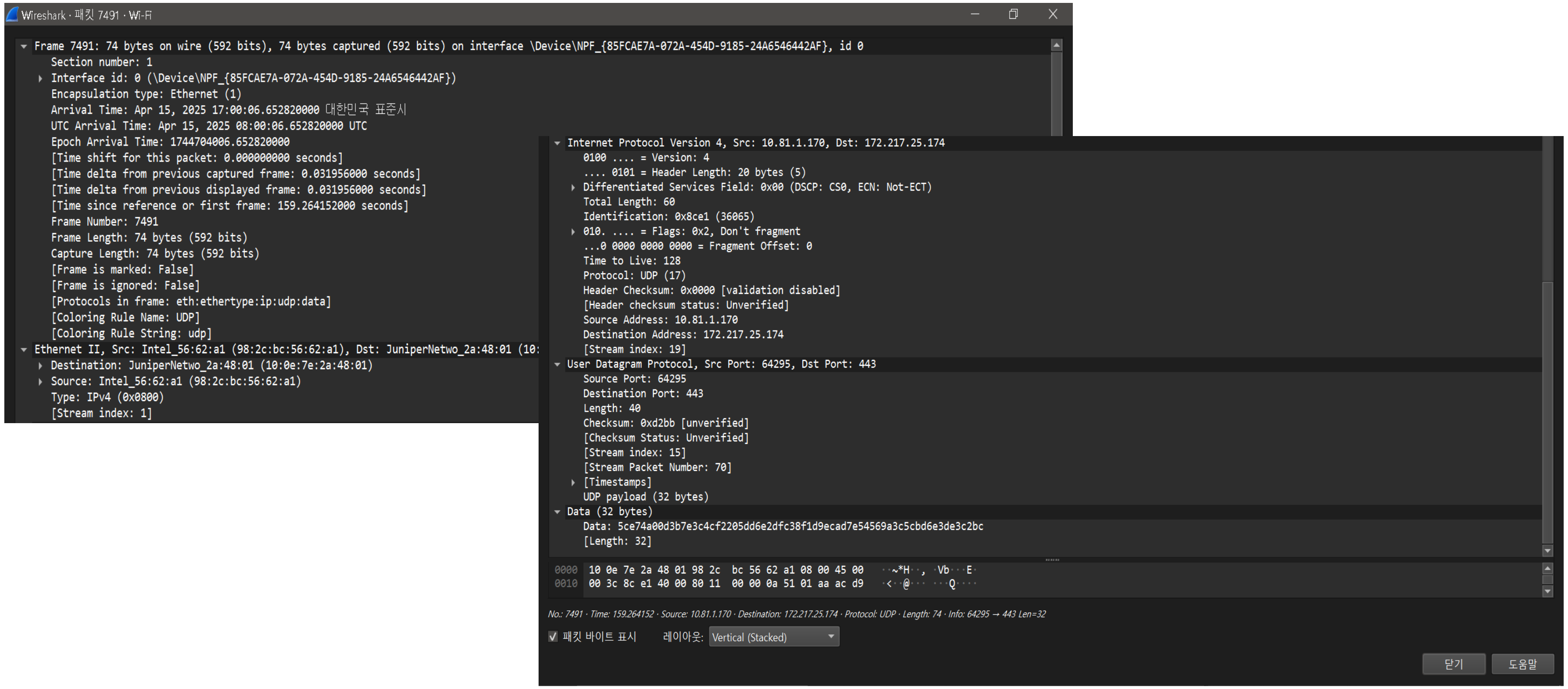
UDP



```
▾ Frame 7491: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{85FCAE7A-072A-454D-9185-24A6546442AF}, id 0
    Section number: 1
  ▸ Interface id: 0 (\Device\NPF_{85FCAE7A-072A-454D-9185-24A6546442AF})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 15, 2025 17:00:06.652820000 대한민국 표준시
    UTC Arrival Time: Apr 15, 2025 08:00:06.652820000 UTC
    Epoch Arrival Time: 1744704006.652820000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.031956000 seconds]
    [Time delta from previous displayed frame: 0.031956000 seconds]
    [Time since reference or first frame: 159.264152000 seconds]
    Frame Number: 7491
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▾ Ethernet II, Src: Intel_56:62:a1 (98:2c:bc:56:62:a1), Dst: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  ▸ Destination: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  ▸ Source: Intel_56:62:a1 (98:2c:bc:56:62:a1)
    Type: IPv4 (0x0800)
    [Stream index: 1]
```

03 wireshark

UDP



```
▾ Frame 7491: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{85FCAE7A-072A-454D-9185-24A6546442AF}, id 0
    Section number: 1
  ▸ Interface id: 0 (\Device\NPF_{85FCAE7A-072A-454D-9185-24A6546442AF})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 15, 2025 17:00:06.652820000 대한민국 표준시
    UTC Arrival Time: Apr 15, 2025 08:00:06.652820000 UTC
    Epoch Arrival Time: 1744704006.652820000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.031956000 seconds]
    [Time delta from previous displayed frame: 0.031956000 seconds]
    [Time since reference or first frame: 159.264152000 seconds]
    Frame Number: 7491
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▾ Ethernet II, Src: Intel_56:62:a1 (98:2c:bc:56:62:a1), Dst: JuniperNetwo_2a:48:01 (10:
  ▸ Destination: JuniperNetwo_2a:48:01 (10:0e:7e:2a:48:01)
  ▸ Source: Intel_56:62:a1 (98:2c:bc:56:62:a1)
    Type: IPv4 (0x0800)
    [Stream index: 1]
```

```
▾ Internet Protocol Version 4, Src: 10.81.1.170, Dst: 172.217.25.174
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8ce1 (36065)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.81.1.170
    Destination Address: 172.217.25.174
    [Stream index: 19]
▾ User Datagram Protocol, Src Port: 64295, Dst Port: 443
    Source Port: 64295
    Destination Port: 443
    Length: 40
    Checksum: 0xd2bb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
    [Stream Packet Number: 70]
  ▸ [Timestamps]
    UDP payload (32 bytes)
▾ Data (32 bytes)
    Data: 5ce74a00d3b7e3c4cf2205dd6e2dfc38f1d9ecad7e54569a3c5cbd6e3de3c2bc
    [Length: 32]

0000  10 0e 7e 2a 48 01 98 2c  bc 56 62 a1 08 00 45 00   ··~*H··, ·Vb···E·
0010  00 3c 8c e1 40 00 80 11  00 00 0a 51 01 aa ac d9   ·<··@··· ···Q····

No.: 7491 · Time: 159.264152 · Source: 10.81.1.170 · Destination: 172.217.25.174 · Protocol: UDP · Length: 74 · Info: 64295 → 443 Len=32
```

☑ 패킷 바이트 표시   레이아웃: Vertical (Stacked)

TCP, UDP 비교

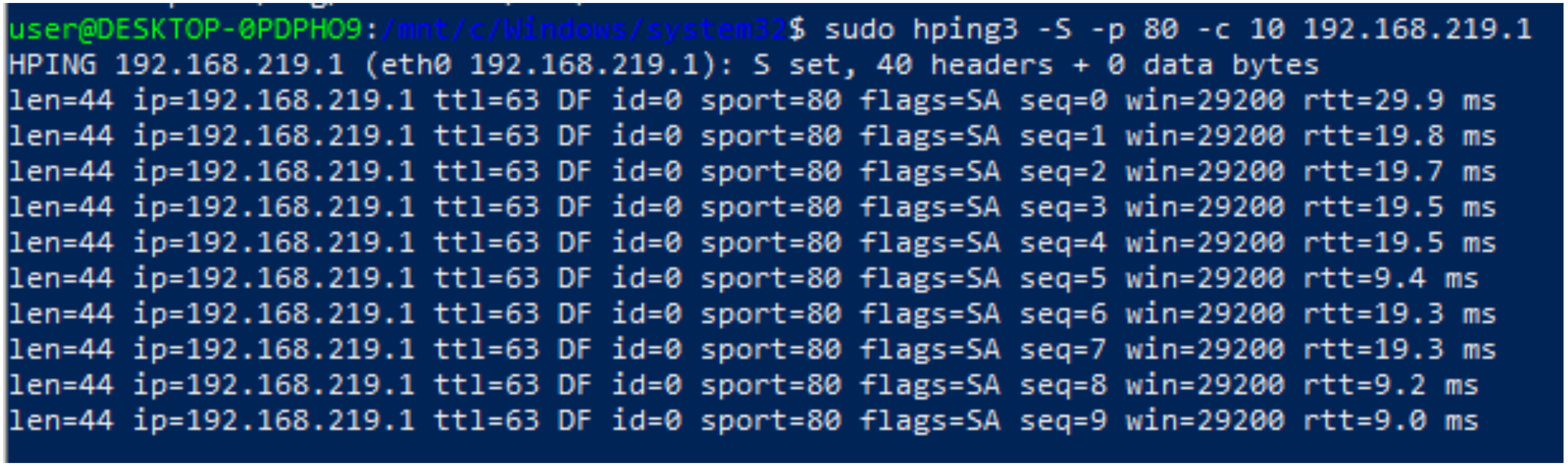
구분	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
연결 방식	연결형 (Connection-oriented)	비연결형 (Connectionless)
연결 설정	3-way Handshake 필요	연결 설정 없음
신뢰성	신뢰성 보장 (순서, 손실, 중복 처리)	신뢰성 없음 (순서, 손실, 중복 처리 X)
오류/흐름/혼잡 제어	있음	없음
데이터 단위	바이트 스트림 (경계 없음)	데이터그램 (경계 명확)
속도	느림 (오버헤드 큼)	빠름 (오버헤드 작음)
통신 방식	1:1 (Unicast)	1:1, 1:다수 (Broadcast), 다:다 (Multicast)
헤더 크기	최소 20바이트 (복잡)	8바이트 (단순)
사용 예시	웹(HTTP/HTTPS), 이메일, 파일 전송 등	실시간 스트리밍, VoIP, 온라인 게임 등

실습

hping3

03 hping3

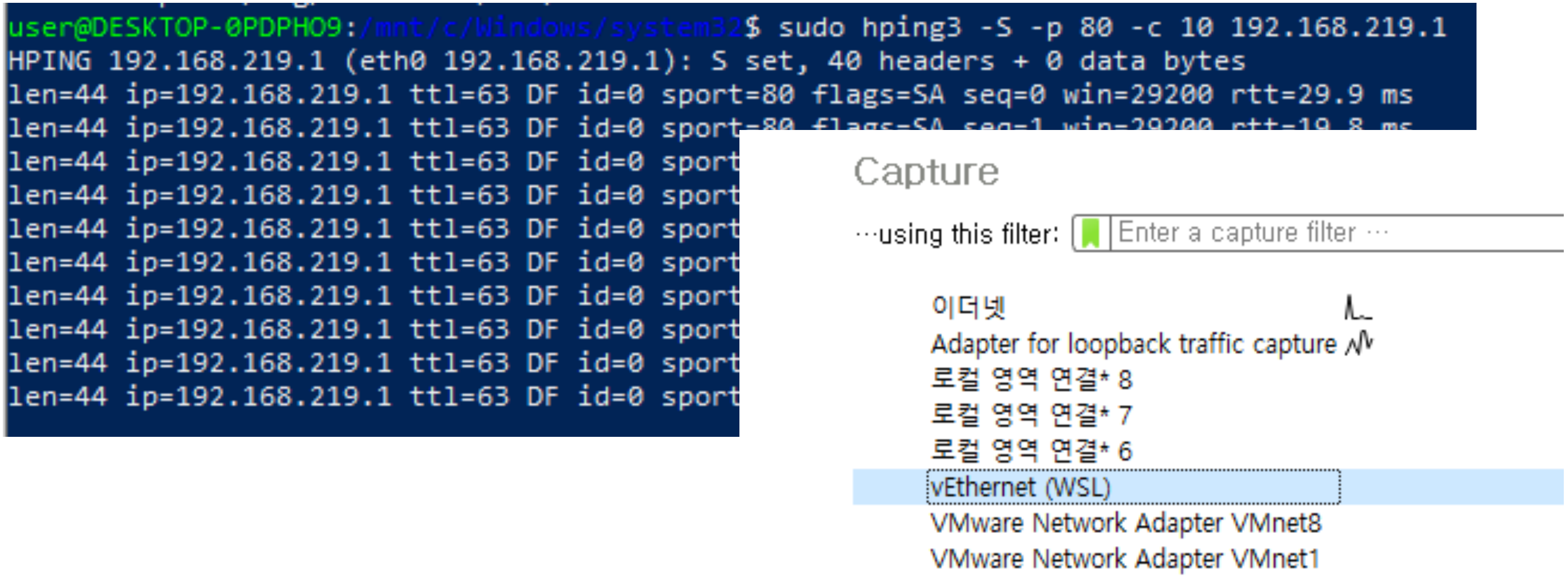
Hping3 패킷 생성



```
user@DESKTOP-0PDPHO9:/mnt/c/Windows/system32$ sudo hping3 -S -p 80 -c 10 192.168.219.1
HPING 192.168.219.1 (eth0 192.168.219.1): S set, 40 headers + 0 data bytes
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=29.9 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=19.8 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt=19.7 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=3 win=29200 rtt=19.5 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=4 win=29200 rtt=19.5 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=5 win=29200 rtt=9.4 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=6 win=29200 rtt=19.3 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=7 win=29200 rtt=19.3 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=8 win=29200 rtt=9.2 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=9 win=29200 rtt=9.0 ms
```

03 hping3

Wireshark로 관측



```
user@DESKTOP-0PDPHO9:/mnt/c/Windows/system32$ sudo hping3 -S -p 80 -c 10 192.168.219.1
HPING 192.168.219.1 (eth0 192.168.219.1): S set, 40 headers + 0 data bytes
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=29.9 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=19.8 ms
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
len=44 ip=192.168.219.1 ttl=63 DF id=0 sport
```

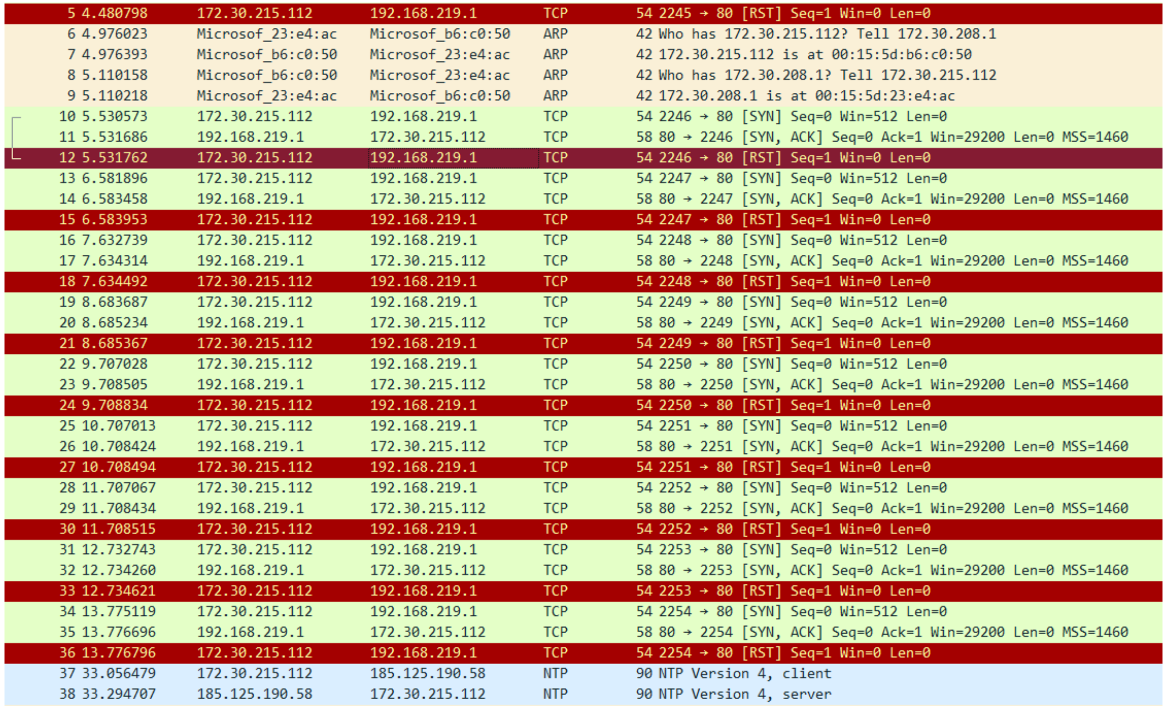
Capture

…using this filter: Enter a capture filter …

이더넷
Adapter for loopback traffic capture
로컬 영역 연결* 8
로컬 영역 연결* 7
로컬 영역 연결* 6
vEthernet (WSL)
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1

03 hping3

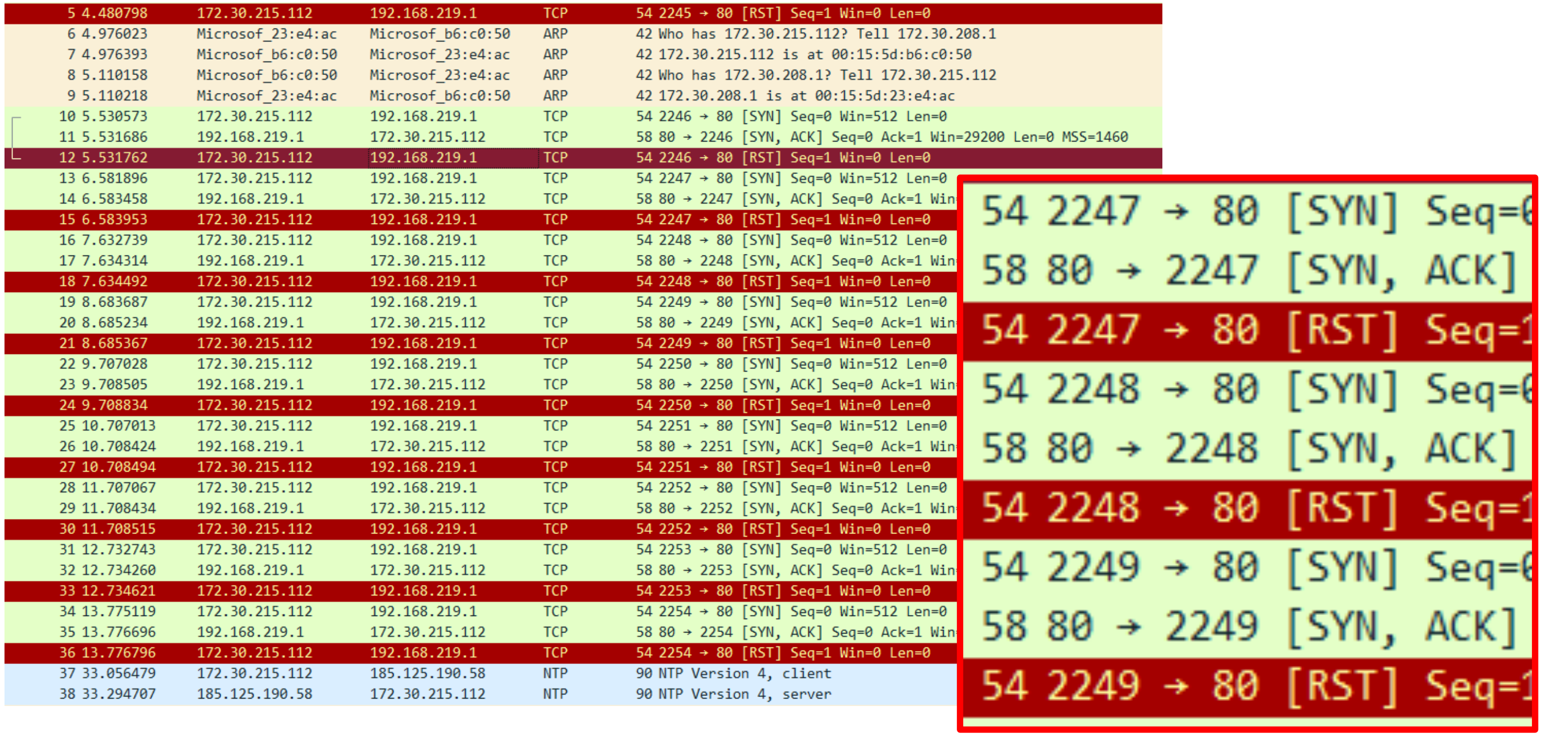
캡처 확인



```
  5 4.480798   172.30.215.112   192.168.219.1    TCP   54 2245 → 80 [RST] Seq=1 Win=0 Len=0
  6 4.976023   Microsof_23:e4:ac Microsof_b6:c0:50 ARP  42 Who has 172.30.215.112? Tell 172.30.208.1
  7 4.976393   Microsof_b6:c0:50 Microsof_23:e4:ac ARP  42 172.30.215.112 is at 00:15:5d:b6:c0:50
  8 5.110158   Microsof_b6:c0:50 Microsof_23:e4:ac ARP  42 Who has 172.30.208.1? Tell 172.30.215.112
  9 5.110218   Microsof_23:e4:ac Microsof_b6:c0:50 ARP  42 172.30.208.1 is at 00:15:5d:23:e4:ac
 10 5.530573   172.30.215.112   192.168.219.1    TCP   54 2246 → 80 [SYN] Seq=0 Win=512 Len=0
 11 5.531686   192.168.219.1    172.30.215.112   TCP   58 80 → 2246 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 12 5.531762   172.30.215.112   192.168.219.1    TCP   54 2246 → 80 [RST] Seq=1 Win=0 Len=0
 13 6.581896   172.30.215.112   192.168.219.1    TCP   54 2247 → 80 [SYN] Seq=0 Win=512 Len=0
 14 6.583458   192.168.219.1    172.30.215.112   TCP   58 80 → 2247 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 15 6.583953   172.30.215.112   192.168.219.1    TCP   54 2247 → 80 [RST] Seq=1 Win=0 Len=0
 16 7.632739   172.30.215.112   192.168.219.1    TCP   54 2248 → 80 [SYN] Seq=0 Win=512 Len=0
 17 7.634314   192.168.219.1    172.30.215.112   TCP   58 80 → 2248 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 18 7.634492   172.30.215.112   192.168.219.1    TCP   54 2248 → 80 [RST] Seq=1 Win=0 Len=0
 19 8.683687   172.30.215.112   192.168.219.1    TCP   54 2249 → 80 [SYN] Seq=0 Win=512 Len=0
 20 8.685234   192.168.219.1    172.30.215.112   TCP   58 80 → 2249 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 21 8.685367   172.30.215.112   192.168.219.1    TCP   54 2249 → 80 [RST] Seq=1 Win=0 Len=0
 22 9.707028   172.30.215.112   192.168.219.1    TCP   54 2250 → 80 [SYN] Seq=0 Win=512 Len=0
 23 9.708505   192.168.219.1    172.30.215.112   TCP   58 80 → 2250 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 24 9.708834   172.30.215.112   192.168.219.1    TCP   54 2250 → 80 [RST] Seq=1 Win=0 Len=0
 25 10.707013  172.30.215.112   192.168.219.1    TCP   54 2251 → 80 [SYN] Seq=0 Win=512 Len=0
 26 10.708424  192.168.219.1    172.30.215.112   TCP   58 80 → 2251 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 27 10.708494  172.30.215.112   192.168.219.1    TCP   54 2251 → 80 [RST] Seq=1 Win=0 Len=0
 28 11.707067  172.30.215.112   192.168.219.1    TCP   54 2252 → 80 [SYN] Seq=0 Win=512 Len=0
 29 11.708434  192.168.219.1    172.30.215.112   TCP   58 80 → 2252 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 30 11.708515  172.30.215.112   192.168.219.1    TCP   54 2252 → 80 [RST] Seq=1 Win=0 Len=0
 31 12.732743  172.30.215.112   192.168.219.1    TCP   54 2253 → 80 [SYN] Seq=0 Win=512 Len=0
 32 12.734260  192.168.219.1    172.30.215.112   TCP   58 80 → 2253 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 33 12.734621  172.30.215.112   192.168.219.1    TCP   54 2253 → 80 [RST] Seq=1 Win=0 Len=0
 34 13.775119  172.30.215.112   192.168.219.1    TCP   54 2254 → 80 [SYN] Seq=0 Win=512 Len=0
 35 13.776696  192.168.219.1    172.30.215.112   TCP   58 80 → 2254 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 36 13.776796  172.30.215.112   192.168.219.1    TCP   54 2254 → 80 [RST] Seq=1 Win=0 Len=0
 37 33.056479  172.30.215.112   185.125.190.58   NTP   90 NTP Version 4, client
 38 33.294707  185.125.190.58   172.30.215.112   NTP   90 NTP Version 4, server
```

03 hping3

캡쳐 확인

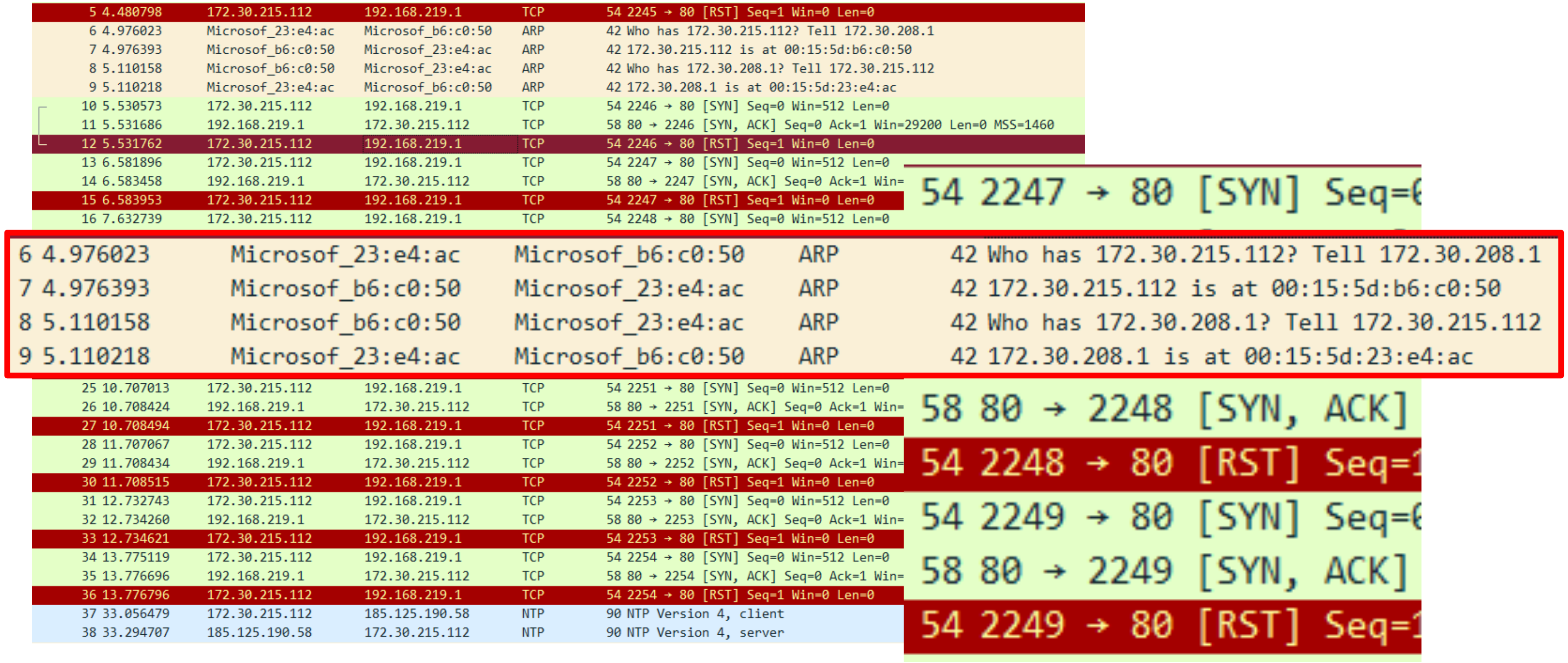


```
 5 4.480798   172.30.215.112     192.168.219.1      TCP   54 2245 → 80 [RST] Seq=1 Win=0 Len=0
 6 4.976023   Microsof_23:e4:ac  Microsof_b6:c0:50  ARP   42 Who has 172.30.215.112? Tell 172.30.208.1
 7 4.976393   Microsof_b6:c0:50  Microsof_23:e4:ac  ARP   42 172.30.215.112 is at 00:15:5d:b6:c0:50
 8 5.110158   Microsof_b6:c0:50  Microsof_23:e4:ac  ARP   42 Who has 172.30.208.1? Tell 172.30.215.112
 9 5.110218   Microsof_23:e4:ac  Microsof_b6:c0:50  ARP   42 172.30.208.1 is at 00:15:5d:23:e4:ac
10 5.530573   172.30.215.112     192.168.219.1      TCP   54 2246 → 80 [SYN] Seq=0 Win=512 Len=0
11 5.531686   192.168.219.1      172.30.215.112     TCP   58 80 → 2246 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12 5.531762   172.30.215.112     192.168.219.1      TCP   54 2246 → 80 [RST] Seq=1 Win=0 Len=0
13 6.581896   172.30.215.112     192.168.219.1      TCP   54 2247 → 80 [SYN] Seq=0 Win=512 Len=0
14 6.583458   192.168.219.1      172.30.215.112     TCP   58 80 → 2247 [SYN, ACK] Seq=0 Ack=1 Win
15 6.583953   172.30.215.112     192.168.219.1      TCP   54 2247 → 80 [RST] Seq=1 Win=0 Len=0
16 7.632739   172.30.215.112     192.168.219.1      TCP   54 2248 → 80 [SYN] Seq=0 Win=512 Len=0
17 7.634314   192.168.219.1      172.30.215.112     TCP   58 80 → 2248 [SYN, ACK] Seq=0 Ack=1 Win
18 7.634492   172.30.215.112     192.168.219.1      TCP   54 2248 → 80 [RST] Seq=1 Win=0 Len=0
19 8.683687   172.30.215.112     192.168.219.1      TCP   54 2249 → 80 [SYN] Seq=0 Win=512 Len=0
20 8.685234   192.168.219.1      172.30.215.112     TCP   58 80 → 2249 [SYN, ACK] Seq=0 Ack=1 Win
21 8.685367   172.30.215.112     192.168.219.1      TCP   54 2249 → 80 [RST] Seq=1 Win=0 Len=0
22 9.707028   172.30.215.112     192.168.219.1      TCP   54 2250 → 80 [SYN] Seq=0 Win=512 Len=0
23 9.708505   192.168.219.1      172.30.215.112     TCP   58 80 → 2250 [SYN, ACK] Seq=0 Ack=1 Win
24 9.708834   172.30.215.112     192.168.219.1      TCP   54 2250 → 80 [RST] Seq=1 Win=0 Len=0
25 10.707013  172.30.215.112     192.168.219.1      TCP   54 2251 → 80 [SYN] Seq=0 Win=512 Len=0
26 10.708424  192.168.219.1      172.30.215.112     TCP   58 80 → 2251 [SYN, ACK] Seq=0 Ack=1 Win
27 10.708494  172.30.215.112     192.168.219.1      TCP   54 2251 → 80 [RST] Seq=1 Win=0 Len=0
28 11.707067  172.30.215.112     192.168.219.1      TCP   54 2252 → 80 [SYN] Seq=0 Win=512 Len=0
29 11.708434  192.168.219.1      172.30.215.112     TCP   58 80 → 2252 [SYN, ACK] Seq=0 Ack=1 Win
30 11.708515  172.30.215.112     192.168.219.1      TCP   54 2252 → 80 [RST] Seq=1 Win=0 Len=0
31 12.732743  172.30.215.112     192.168.219.1      TCP   54 2253 → 80 [SYN] Seq=0 Win=512 Len=0
32 12.734260  192.168.219.1      172.30.215.112     TCP   58 80 → 2253 [SYN, ACK] Seq=0 Ack=1 Win
33 12.734621  172.30.215.112     192.168.219.1      TCP   54 2253 → 80 [RST] Seq=1 Win=0 Len=0
34 13.775119  172.30.215.112     192.168.219.1      TCP   54 2254 → 80 [SYN] Seq=0 Win=512 Len=0
35 13.776696  192.168.219.1      172.30.215.112     TCP   58 80 → 2254 [SYN, ACK] Seq=0 Ack=1 Win
36 13.776796  172.30.215.112     192.168.219.1      TCP   54 2254 → 80 [RST] Seq=1 Win=0 Len=0
37 33.056479  172.30.215.112     185.125.190.58     NTP   90 NTP Version 4, client
38 33.294707  185.125.190.58     172.30.215.112     NTP   90 NTP Version 4, server
```

```
54 2247 → 80 [SYN] Seq=0
58 80 → 2247 [SYN, ACK]
54 2247 → 80 [RST] Seq=1
54 2248 → 80 [SYN] Seq=0
58 80 → 2248 [SYN, ACK]
54 2248 → 80 [RST] Seq=1
54 2249 → 80 [SYN] Seq=0
58 80 → 2249 [SYN, ACK]
54 2249 → 80 [RST] Seq=1
```

03 hping3

캡처 확인



```
 5 4.480798    172.30.215.112     192.168.219.1      TCP    54 2245 → 80 [RST] Seq=1 Win=0 Len=0
 6 4.976023    Microsof_23:e4:ac  Microsof_b6:c0:50  ARP    42 Who has 172.30.215.112? Tell 172.30.208.1
 7 4.976393    Microsof_b6:c0:50  Microsof_23:e4:ac  ARP    42 172.30.215.112 is at 00:15:5d:b6:c0:50
 8 5.110158    Microsof_b6:c0:50  Microsof_23:e4:ac  ARP    42 Who has 172.30.208.1? Tell 172.30.215.112
 9 5.110218    Microsof_23:e4:ac  Microsof_b6:c0:50  ARP    42 172.30.208.1 is at 00:15:5d:23:e4:ac
10 5.530573    172.30.215.112     192.168.219.1      TCP    54 2246 → 80 [SYN] Seq=0 Win=512 Len=0
11 5.531686    192.168.219.1      172.30.215.112     TCP    58 80 → 2246 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12 5.531762    172.30.215.112     192.168.219.1      TCP    54 2246 → 80 [RST] Seq=1 Win=0 Len=0
13 6.581896    172.30.215.112     192.168.219.1      TCP    54 2247 → 80 [SYN] Seq=0 Win=512 Len=0
14 6.583458    192.168.219.1      172.30.215.112     TCP    58 80 → 2247 [SYN, ACK] Seq=0 Ack=1 Win=
15 6.583953    172.30.215.112     192.168.219.1      TCP    54 2247 → 80 [RST] Seq=1 Win=0 Len=0
16 7.632739    172.30.215.112     192.168.219.1      TCP    54 2248 → 80 [SYN] Seq=0 Win=512 Len=0
25 10.707013   172.30.215.112     192.168.219.1      TCP    54 2251 → 80 [SYN] Seq=0 Win=512 Len=0
26 10.708424   192.168.219.1      172.30.215.112     TCP    58 80 → 2251 [SYN, ACK] Seq=0 Ack=1 Win=
27 10.708494   172.30.215.112     192.168.219.1      TCP    54 2251 → 80 [RST] Seq=1 Win=0 Len=0
28 11.707067   172.30.215.112     192.168.219.1      TCP    54 2252 → 80 [SYN] Seq=0 Win=512 Len=0
29 11.708434   192.168.219.1      172.30.215.112     TCP    58 80 → 2252 [SYN, ACK] Seq=0 Ack=1 Win=
30 11.708515   172.30.215.112     192.168.219.1      TCP    54 2252 → 80 [RST] Seq=1 Win=0 Len=0
31 12.732743   172.30.215.112     192.168.219.1      TCP    54 2253 → 80 [SYN] Seq=0 Win=512 Len=0
32 12.734260   192.168.219.1      172.30.215.112     TCP    58 80 → 2253 [SYN, ACK] Seq=0 Ack=1 Win=
33 12.734621   172.30.215.112     192.168.219.1      TCP    54 2253 → 80 [RST] Seq=1 Win=0 Len=0
34 13.775119   172.30.215.112     192.168.219.1      TCP    54 2254 → 80 [SYN] Seq=0 Win=512 Len=0
35 13.776696   192.168.219.1      172.30.215.112     TCP    58 80 → 2254 [SYN, ACK] Seq=0 Ack=1 Win=
36 13.776796   172.30.215.112     192.168.219.1      TCP    54 2254 → 80 [RST] Seq=1 Win=0 Len=0
37 33.056479   172.30.215.112     185.125.190.58     NTP    90 NTP Version 4, client
38 33.294707   185.125.190.58     172.30.215.112     NTP    90 NTP Version 4, server
```

```
6 4.976023    Microsof_23:e4:ac   Microsof_b6:c0:50   ARP    42 Who has 172.30.215.112? Tell 172.30.208.1
7 4.976393    Microsof_b6:c0:50   Microsof_23:e4:ac   ARP    42 172.30.215.112 is at 00:15:5d:b6:c0:50
8 5.110158    Microsof_b6:c0:50   Microsof_23:e4:ac   ARP    42 Who has 172.30.208.1? Tell 172.30.215.112
9 5.110218    Microsof_23:e4:ac   Microsof_b6:c0:50   ARP    42 172.30.208.1 is at 00:15:5d:23:e4:ac
```

```
54 2247 → 80 [SYN] Seq=
58 80 → 2248 [SYN, ACK]
54 2248 → 80 [RST] Seq=
54 2249 → 80 [SYN] Seq=
58 80 → 2249 [SYN, ACK]
54 2249 → 80 [RST] Seq=
```

정보보호학개론

THANK YOU

Team_Safe Zone