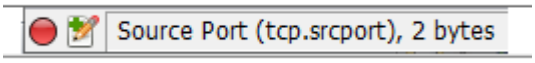
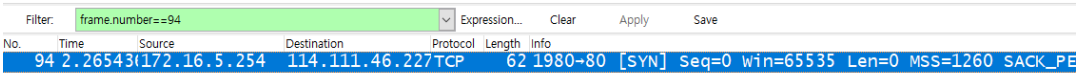
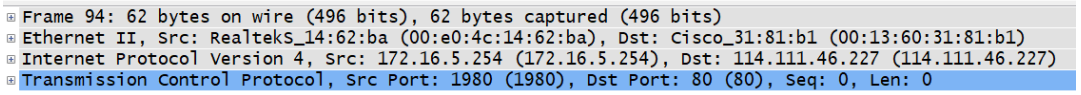
제5장 와이어샤크 필터

1. 와이어샤크 필터 명령어

- '5-1.와이어샤크 필터.pcap'파일 실행
- Filter : frame.number == 94
- TCP 프로토콜 클릭 → 'Source Port' 클릭 → 좌측 하단에 필터 명령어가 ( ) 안에 출력됨.







1) 필터 명령어

- 각각의 헤더를 클릭하여 다음 필터 명령어들을 확인한다.

항목	필터 명령어
출발지 TCP 포트	tcp.srcport
목적지 TCP 포트	tcp.dstport
출발지 UDP 포트	udp.srcport
목적지 UDP 포트	udp.dstport
출발지 IP 주소	ip.src
목적지 IP 주소	ip.dst
출발지 MAC 주소	eth.src
목적지 MAC 주소	eth.dst
TCP Syn	tcp.flags.syn
TCP Ack	tcp.flags.ack

2) 필터 관련 기호

항목	내용
&&	and
||	or
==	eq
!	not
( )	여러 개의 필터를 클래스로 구성

3) 필터 예제

TCP / UDP 관련 필터

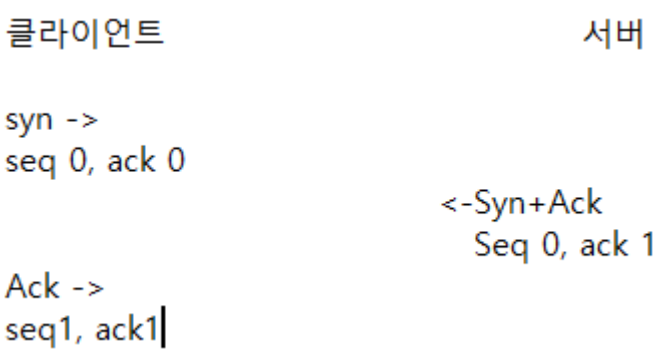
```
tcp.srcport == 80 or tcp.dstport == 80
tcp.port == 80

tcp.flags.syn == 1
tcp.flags == 0x02        // tcp.flags == 2

tcp.flags.syn == 1 and tcp.flags.ack == 1
tcp.flags == 0x12        // tcp.flags == 18

tcp.flags.ack==1
tcp.flags == 0x10        // tcp.flags == 16

tcp.seq == 1
tcp.ack == 1
tcp.seq == 1 and tcp.ack == 1

udp.srcport == 53 or udp.dstport == 53
udp.port == 53
```

IP 관련 필터

```
ip.src == 172.16.5.254
ip.dst == 172.16.5.254

ip.src == 172.16.5.254 or ip.dst == 172.16.5.254
ip.addr == 172.16.5.254

ip.src == 172.16.5.254 && tcp
ip.src == 172.16.5.254 && tcp.srcport == 1980
ip.src == 172.16.5.254 && tcp.dstport == 80

ip.src == 172.16.5.254 && udp
ip.src == 172.16.5.254 && udp.dstport eq 53

ip.src == 172.16.5.254 && ip.dst == 114.111.46.227 && tcp.flags == 0x02
ip.src == 114.111.46.227 && ip.dst == 172.16.5.254 && tcp.flags == 0x12
```

1. 첫번째 씽크
2. 두번째 싱크

```
ip.src == 172.16.5.254 && ip.dst == 114.111.46.227 && tcp.flags == 0x10
ip.src == 172.16.5.254 && ip.dst == 114.111.46.227 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1
```



p.src == 172.16.5.254 && ip.dst == 114.111.46.227 && tcp.flags == 0x10\

- flag중에 ack가 다 나오게

ip.src == 172.16.5.254 && ip.dst == 114.111.46.227 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1

- 3-way handshaking 중 3번째 ack만 나오게

3) ! 관련 필터

```
!arp              // not arp
ip.addr == 172.16.5.254 && !tcp && !udp
!ip && !ipv6
```

- 2번째 : 출발지 IP가 5.254 이고 TCP, UDP 를 뺀 아이피를 뽑아라

4) ICMP 관련 필터

```
icmp
icmp.type == 8
icmp.type eq 0
```

5) Ethernet 관련 필터

```
eth
eth.src == 00:00:0c:92:ab:2c
eth.dst == 00:e0:4c:14:62:ba
eth.src eq 00:00:0c:92:ab:2c or eth.dst eq 00:13:60:31:81:b1
eth.src eq 00:00:0c:92:ab:2c and eth.dst eq 00:e0:4c:14:62:ba
eth.dst eq ff:ff:ff:ff:ff:ff
```

- eth : 이더넷 프로토콜 쓰는애들 다 나옴
- 맨아래: 브로드캐스트 (목적지)

6) ARP 관련 필터

```
arp
arp.opcode == 1              // arp.opcode == 2
arp.src.proto_ipv4 == 172.16.5.254
arp.src.hw_mac == 00:e0:4c:14:62:ba
arp.src.proto_ipv4 == 172.16.5.254 && arp.src.hw_mac == 00:e0:4c:14:62:ba
```

- opcode가 2번이면 응답이다.
- Target MacAdress 가 없으면 요청

7) HTTP 관련 필터

http http.host eq lm3.cafe.naver.com	http.request.method == GET http.request.method matches "(?i)get"

- 대소문자를 가림
- 구분없이 하려면 matches “(?i)”

<u>와이어샤크 필터 예제:</u>

2) '192.168.1.201' TCP 3-Way 핸드 쉐이킹 & HTTP(TCP 80) 내용 필터

PC	서버
192.168.1.254	192.168.1.201
70:85:C2:0A:E8:F6	
Syn(0x02) ->	
seq 0	
	<- Syn+Ack(0x12)
	seq 0, ack 1
Ack(0x10) ->	
seq 1, ack 1	

TCP 3-way handshaking:

1. ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x02 && tcp.seq == 0

2. ip.src == 192.168.1.201 and ip.dst == 192.168.1.254 && tcp.srcport == 80 && tcp.flags == 0x12 && tcp.seq == 0 && tcp.ack == 1

3. ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1

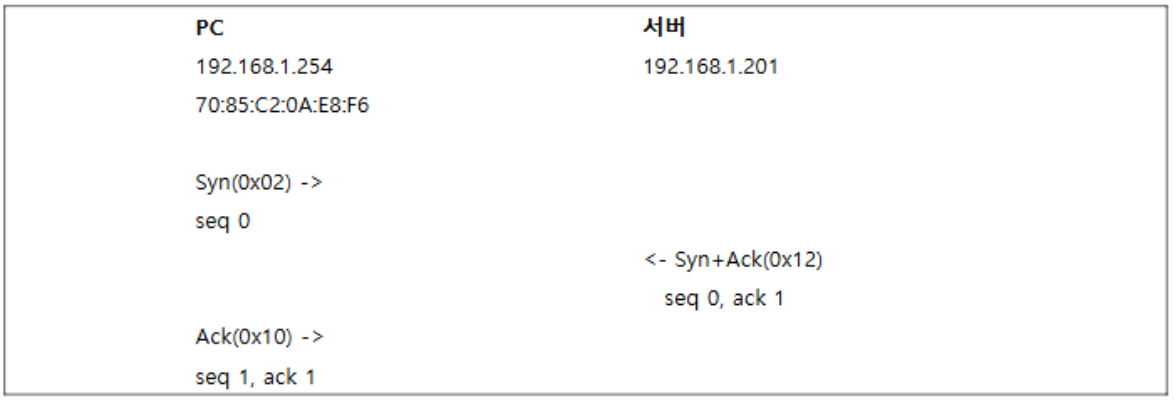
HTTP(TCP 80):

1. (ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && http) or (ip.src == 192.168.1.201 and ip.dst == 192.168.1.254 && http)

Answer:

(ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x02 && tcp.seq == 0) or (ip.src == 192.168.1.201 and ip.dst == 192.168.1.254 && tcp.srcport == 80 && tcp.flags == 0x12 && tcp.seq == 0 && tcp.ack == 1) or (ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1) or (ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && http) or (ip.src == 192.168.1.201 and ip.dst == 192.168.1.254 && http)

3) '192.168.1.201' TCP 3-Way 핸드 쉐이킹 및 FTP(TCP 21) 내용 필터



Answer: (포트번호 80 → 21, http → FTP)

(ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && tcp.dstport == 21 && tcp.flags == 0x02 && tcp.seq == 0) or (ip.src == 192.168.1.201 and ip.dst == 192.168.1.254 && tcp.srcport == 21 && tcp.flags == 0x12 && tcp.seq == 0 && tcp.ack == 1) or (ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && tcp.dstport == 21 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1) or (ip.src == 192.168.1.254 and ip.dst == 192.168.1.201 && ftp) or (ip.src == 192.168.1.201 and ip.dst == 192.168.1.254 && ftp)

2. 와이어샤크 필터 예제

- '5-2.와이어샤크 필터 예제.pcap' 파일을 와이어샤크로 오픈한다.

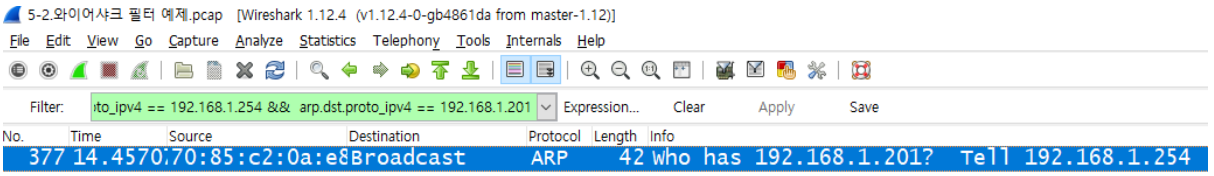
PC	서버
192.168.1.254	192.168.1.201
70:85:C2:0A:E8:F6	

1) '192.168.1.201' ARP 요청 및 응답 내용 필터

request(1) or response(2) : arp.opcode == N
sender mac : arp.src.hw_mac
sender IP : arp.src.proto_ipv4
target mac : arp.dst.hw_mac
target IP : arp.dst.proto_ipv4

- ARP 요청 메세지

arp.opcode == 1 && arp.src.hw_mac == 70:85:c2:0a:e8:f6 && arp.src.proto_ipv4 == 192.168.1.254 && arp.dst.proto_ipv4 == 192.168.1.201

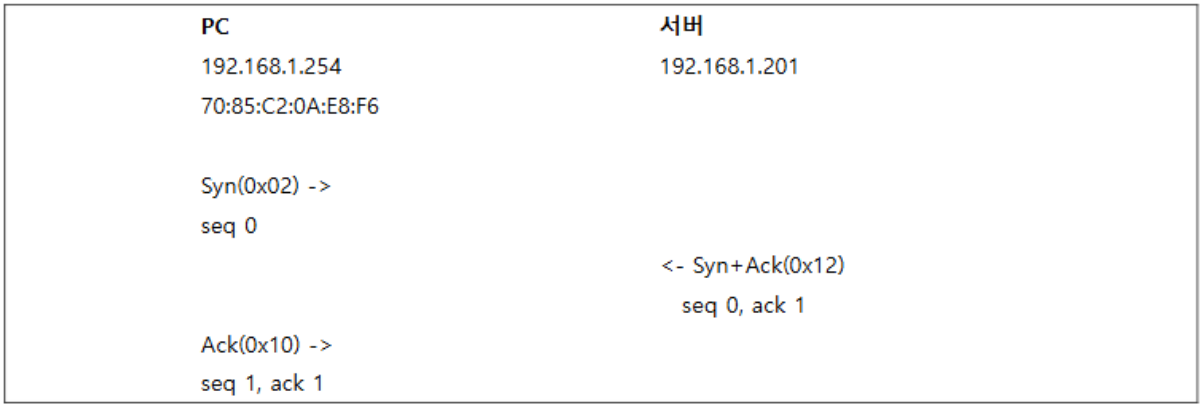


- ARP 응답 메세지

arp.opcode == 2 && arp.src.proto_ipv4 == 192.168.1.201 && arp.dst.proto_ipv4 == 192.168.1.201

정답:
(arp.opcode == 1 && arp.src.hw_mac == 70:85:c2:0a:e8:f6 && arp.src.proto_ipv4 == 192.168.1.254 && arp.dst.proto_ipv4 == 192.168.1.201) or (arp.opcode == 2 && arp.src.proto_ipv4 == 192.168.1.201 && arp.dst.proto_ipv4 == 192.168.1.201)

2) '192.168.1.201' TCP 3-Way 핸드 쉐이킹 & HTTP(TCP 80) 내용 필터




```
ip.src == 192.168.1.254 && ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x02 && tcp.seq == 0

ip.src == 192.168.1.201 && ip.dst == 192.168.1.254 && tcp.srcport == 80 && tcp.flags == 0x12 && tcp.seq == 0 && tcp.ack == 1

ip.src == 192.168.1.254 && ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1
```

답:

```
(ip.src == 192.168.1.254 && ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x02 && tcp.seq == 0) or (ip.src == 192.168.1.201 && ip.dst == 192.168.1.254 && tcp.srcport == 80 && tcp.flags == 0x12 && tcp.seq == 0 && tcp.ack == 1) or (ip.src == 192.168.1.254 && ip.dst == 192.168.1.201 && tcp.dstport == 80 && tcp.flags == 0x10 && tcp.seq == 1 && tcp.ack == 1)
```

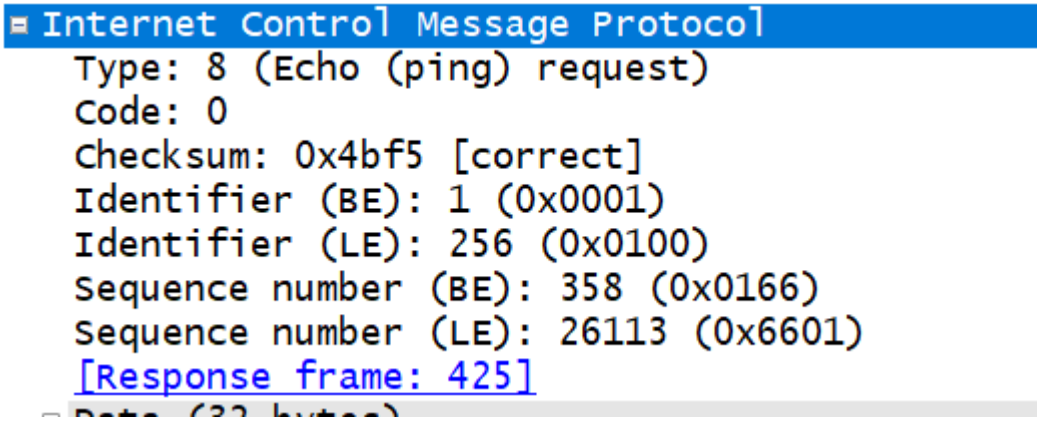
== eq
&& and
|| or
! not

5) '192.168.1.201' ICMP Echo-Request, ICMP Echo-Reply 내용 필터

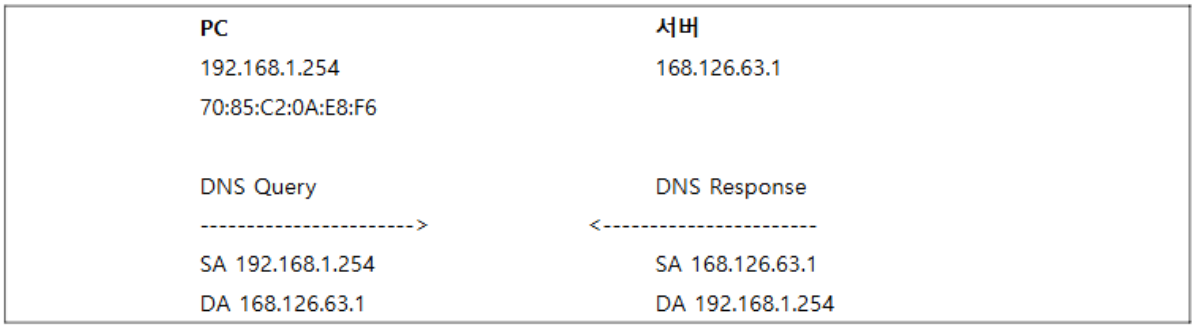
PC		서버
192.168.1.254		192.168.1.201
70:85:C2:0A:E8:F6		
ICMP Echo-Request		ICMP Echo-Reply
---------->		<----------
SA 192.168.1.254		SA 192.168.1.201
DA 192.168.1.201		DA 192.168.1.254

요청 8
응답 0
목적지 못간다 3

CODE 3: 목적지까지 도착했는데 포트가 닫혀있다.



6) PC 에서 '168.126.63.1'으로 'www.naver.com'에 대한 DNS 요청 및 응답 내용 필터



요청:

```
dns.qry.name
dns.resp.name

ip.src == 192.168.1.254 && ip.dst == 168.126.63.1 && dns.qry.name == www.naver.com
```

응답:

```
ip.src == 168.126.63.1 && ip.dst == 192.168.1.254 && dns.resp.name == www.naver.com
```

정답:

```
(ip.src == 192.168.1.254 && ip.dst == 168.126.63.1 && dns.qry.name == www.naver.com) or (ip.src == 168.126.63.1 && ip.dst == 192.168.1.254 && dns.resp.name == www.naver.com)
```