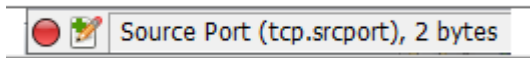


제5장 와이어샤크 필터

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.



Filter:	frame.number==94	Expression...	Clear	Apply	Save	
No.	Time	Source	Destination	Protocol	Length	Info
94	2.265431	172.16.5.254	114.111.46.227	TCP	62	1980→80 [SYN] Seq=0 win=65535 Len=0 MSS=1260 SACK_PE

Frame 94: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: RealtekS_14:62:ba (00:e0:4c:14:62:ba), Dst: Cisco_31:81:b1 (00:13:60:31:81:b1)
Internet Protocol Version 4, Src: 172.16.5.254 (172.16.5.254), Dst: 114.111.46.227 (114.111.46.227)
Transmission Control Protocol, Src Port: 1980 (1980), Dst Port: 80 (80), Seq: 0, Len: 0

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 싱크
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
```

클라이언트

서버

syn ->
seq 0, ack 0

<-Syn+Ack
Seq 0, ack 1

Ack ->
seq1, ack1

ip.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 2면 응답이다.
- Target MacAddress 가 없으면 요청

7) HTTP 관련 필터

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

- 대소문자를 가림
- 구분없이 하려면 matches "(?i)"

와이어샤크 필터 예제:

2) '192.168.1.201' TCP 3-Way 핸드 셰이킹 & 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

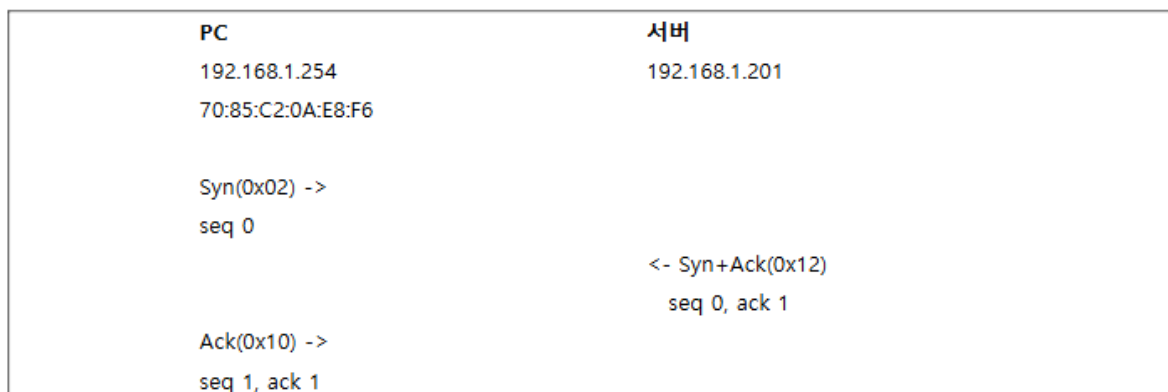
HTTP(TCP 80):

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 셰이킹 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)
```