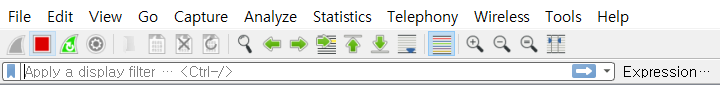
Filter rules of Wireshark

필터링 방법

1. 명령어 입력
2. Expression에서 선택



1.명령어 입력 캡쳐 필터

* 패킷이 캡쳐 될 때 지정
* 버클리 패킷 필터

한정자

1. Type : 식별자. Host, net, port

2. Dir: 전송 방향 . src, dst

3. Proto: 특정한 프로토콜. Ether, broadcast, ip, tcp, udp, icmp, http, ftp

논리 연산자

1. 논리합 연산자 : AND (&&)
2. 논리곱 연산자 : OR ( || )
3. 논리 부정 연산자 : NOT ( ! )
4. Expression에서 선택하는 표시 필터

-캡처 후 원하지 않는 패킷을 숨기거나 원하는 패킷을 표시하기 위해 사용

비교연산자

==: 같다

!=: 같지 않다

>: 보다 더 크다

<: 보다 더 작다

>=: 크거나 같다

<=: 작거나 같다

논리 연산자

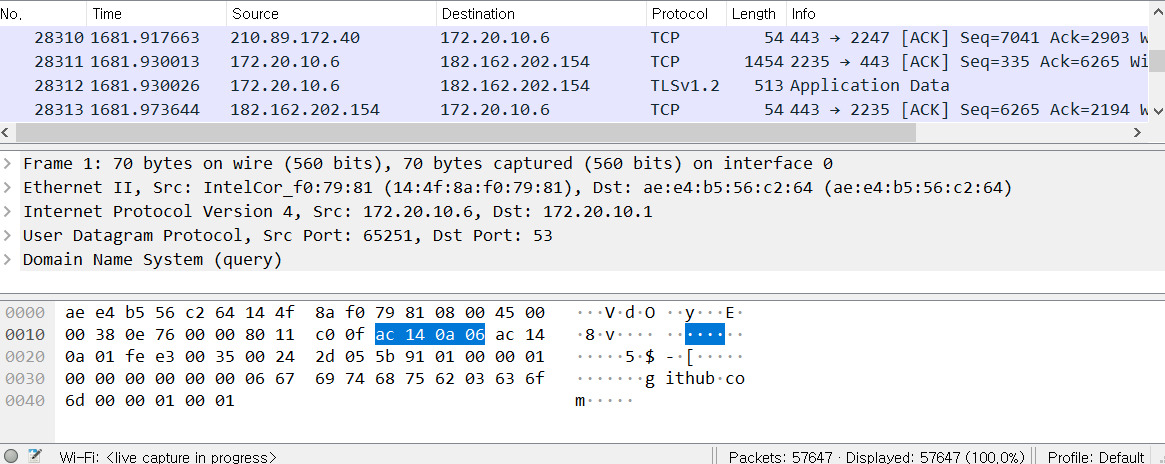
And: 모든 조건이 참일 때

Or: 하나만 참일 때

Xor: 하나와 오직하나의 조건이 참이 될 때

Not: 조건들 중 어느것도 참이 아닐 때

Filter 사용 예



Ip.addr == 172.20.10.6

:출발지나 목적지의 ip가 172.20.10.6인 경우에 출력

ip.addr == 172.20.10.6 && ip.addr == 182.162.202.154

:두개의 정의된 ip주소 모두 출력

Tcp.port == 4000

:출발지나 목적지의 포트가 4000인 tcp 패킷을 출력

http.request

:모든 http get 요청 패킷을 출력

Tcp contains traffic

:’traffic’이라는 단어를 포함하는 tcp 패킷을 출력