Filter rules of Wireshark

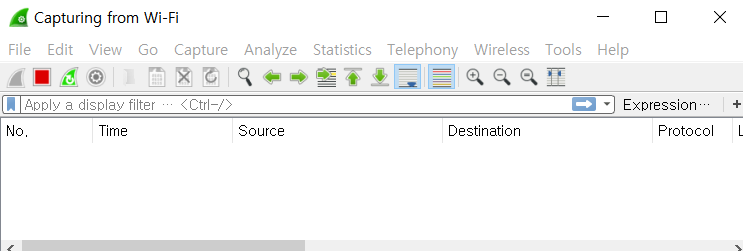
Member\_2\_Jung\_Suzie

필터링 방법

1, 명령어 입력

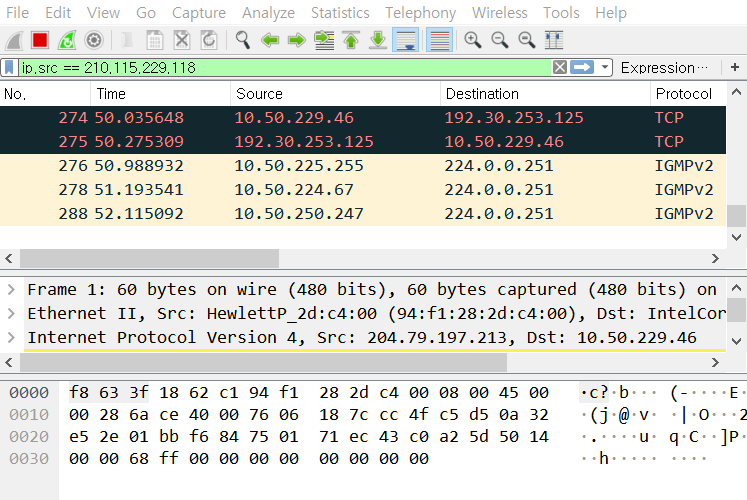
2. Expression에서 명령어선택

1. 명령어 입력 Apply a display filter 안에 명령어 입력



ip.addr == 210.115.229.118 //출발지나 목적지의 ip주소가 210.115.229.118인 패킷들만 보여준다.

ip.src == 210.115.229.118 //출발지의 ip가 210.115.229.118인 패킷만 보여준다.



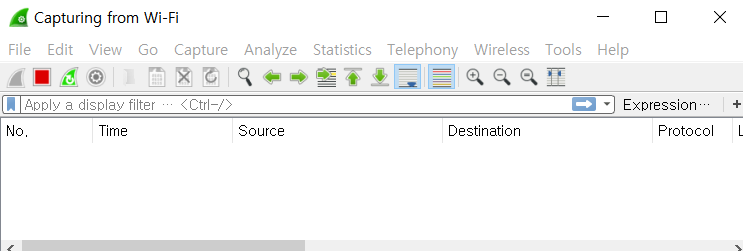
ip.dst==210.115.229.118 or ip.dst==127.0.1.1 //목적지의 ip가 127.0.0.1 이거나 127.0.1.1

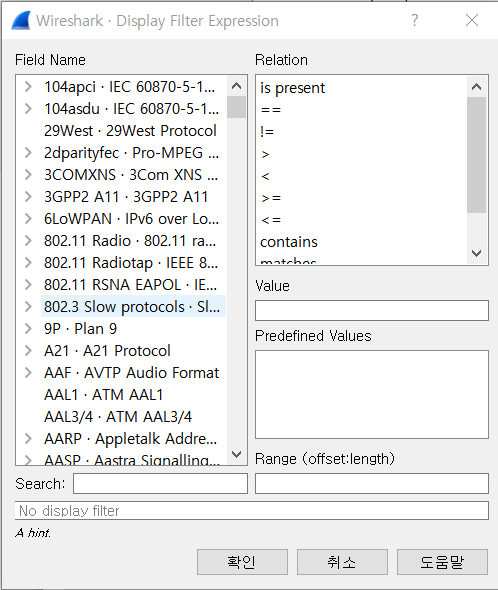
tcp.port==80 //출발지나 목적지의 tcp포트가 80인 것만 보여줌

tcp.srcport==980 //출발지의 tcp포트가 980인것만 보여줌

tcp.srcport==80 && tcp.dstport==980 //출발지의 포트가 80이고 목적지의 포트가 980인 패킷만 보여줌

2. Expression에서 명령어선택





**Expression 버튼을 클릭 후**

**Protocol. String1. String2 Comparison operator Value Logical Operations Other expression**

**각 프로토콜의 하위 프로토콜의 하위 프로토콜 카테고리를 보기 위해서, 프로토콜을 선택한 뒤 “+” 표시를 클릭**