

过滤源ip、目的ip。在wireshark的过滤规则框Filter中输入过滤条件。如查找目的地址为192.168.101.8的包，`ip.dst==192.168.101.8`；查找源地址为1.1.1.1的包，`ip.src==1.1.1.1`；

端口过滤。如过滤80端口，在Filter中输入，`tcp.port==80`，这条规则是把源端口和目的端口为80的都过滤出来。使用`tcp.dstport==80`只过滤目的端口为80的，`tcp.srcport==80`只过滤源端口为80的包；

协议过滤比较简单，直接在Filter框中直接输入协议名即可，如过滤HTTP的协议；

http模式过滤。如过滤get包，`http.request.method=="GET"`，过滤post包，`http.request.method=="POST"`；

连接符and的使用。过滤两种条件时，使用and连接，如过滤ip为192.168.101.8并且为http协议的，`ip.src==192.168.101.8 and http`。