**WIRESHARK FİLTRELEME KOMUTLARI**

|  |  |
| --- | --- |
| Belli bir adrese ait trafik | host <IP adresi> ya da host [www.example.com](http://www.example.com) |
| Belli bir IP bloğuna ait trafik | net <IP/blok> ya da net <IP/blok> or mask <mask değeri> |
| Kaynak adrese göre filtreleme | src net <IP/blok> ya da ip.src==<IP/blok> |
| Hedef adrese göre filtreleme | dst net <IP/blok> |
| Port numarasına göre filtreleme | port <port numarası> ya da <protokol adı>.port eq <port numarası> |
| Belli bir porttan gelmeyen trafikler için | host <www.example.com> and not (port <port numarası>) |
| Belli bir port aralığındaki trafik | tcp portrange <başlangıç - bitiş> |
| MAC adresine göre filtreleme | ether dst <mac adresi> ya da not ether dst <mac adresi> |
| Broadcast ve multicast olmayan trafik | not broadcast and not multicast |
| URL’de geçenlere göre filtreleme | http.request.uri contains ”kelime” ya da http contains "sayfa adı" |
| Dosya tipine göre filtreleme | http.content\_type contains “dosya tipi” ya da http contains “dosya tipi” |
| Dönen cevap kodlarına göre filtreleme | http.response.code == <kod numarası> |
| HTTP metotlara göre filtreleme | http.request.method == "metot adı (get-post vs)" |
| Yapılan istekleri görme | arp.opcode==1 |
| Dönen cevapları görme | arp.opcode==2 |
| Açık portları görme | tcp.flags.syn==1 and tcp.flags.ack==1 |
| Kapalı portları görme | tcp.flags.reset==1 and tcp.flags.ack==1 |
| İsteklerde kullanılan parametreleri görme | http.request.uri.query.parameter contains “parametre (mesela login)” |
| Kullanılan tarayıcı bilgisi | http.user\_agent |