FILTROS DE WIRESHARK

operadores lógicos:

• Igual a: **eq** (o **==)**

• No igual: **ne** (o **!=)**

• Mayor que:**gt** (o **>)**

• Menor que: **lt (**o **<)**

• Mayor o igual: **ge** (o **>=)**

• Menor o igual: **le** (o **<=)**

• Negación: **!** (o **not)**

• Unión o Concatenación: **&&** (o **and)**

• Alternancia: **||** (u **or)**

• Si en un texto del paquete aparece una cadena: **contains "cadena"**

Ejemplos de filtros

Ejemplos de filtros: Sintaxis	**Significado**
ip.addr == 192.168.1.70	Visualiza tráfico en el que participe el host 192.168.1.70
ip.addr != 192.168.31.80	Visualiza todo el tráfico excepto en el que participe el host 192.168.31.80
ip.dst == 170.168.1.30	Visualiza tráfico con IP destino170.168.1.30
ip.src == 7.168.1.30	Visualiza tráfico con IP origen 7.168.1.30
ip	Visualiza todo el tráfico IP
tcp.port ==45	Visualiza todo el tráfico cuyo origen o destino sea el puerto 45
ip.addr == 192.168.1.30 and tcp.port == 143	Visualiza todo el tráfico en el que participe el host 192.168.1.30 y cuyo origen o destino sea el puerto 143
http contains "http://www.uma.es"	Visualiza los paquetes que contienen http://www.uma.es en el contenido en protocolo de nivel de aplicación http.
icmp[0:1] == 08	Filtro avanzado con el que se visualiza todo el tráfico icmp de tipo echo request

ip.ttl == 1	Visualiza todos los paquetes IP cuyo campo TTL sea igual a 1
tcp.windows_size != 0	Visualiza todos los paquetes cuyo campo Tamaño de Ventana del segmento TCP sea distinto de 0
ip.flags.df == x	Visualiza todo los paquetes IP cuyo campo DF (don't fragment o prohibido fragmentar) sea igual a x
udp.port == 53	Visualiza todo el trafico UDP cuyo origen o destino sea el puerto 53

Relación de todos los filtros

: https://wiki.wireshark.org/DisplayFilters

Link de filtros según el protocolo

Ethernet:
https://www.wireshark.org/docs/dfref/e/eth.html
ARP:
https://www.wireshark.org/docs/dfref/a/arp.html
IP:
https://www.wireshark.org/docs/dfref/i/ip.html
ICMP:
https://www.wireshark.org/docs/dfref/i/icmp.html
TCP:
https://www.wireshark.org/docs/dfref/t/tcp.html
UDP:
https://www.wireshark.org/docs/dfref/u/udp.html