Filtros de Wireshark Cheat Sheet

by ouyearedes via cheatography.com/165146/cs/34582/

Operadores lógicos

Igual a	eq	==
Diferente a	ne	!=
Mayor que	gt	>
Menor que	it	<
AND	and	&&
OR	or	||
NOT	not	!
Incluye	contains	

Características del Frame

frame.time_delta	Tiempo desde el último paquete
frame.time_epoch	Segundos desde UNIX time
frame.time	Tiempo de llegada
frame.len	Tamaño del paquete

Fitrar por protocolo

dns
http
ftp
ssh
telnet
icmp

Direcciones IP

ip.adrr==	Todo el tráfico de esa IP
ip.src==	Solamente cuando es el origen
ip.dst	Solamente cuando es el destino
!ip.addr	No mostrar paquetes de esta IP
ip.addr== 0.0.0.0/0 and ip.addr==	Tráfico entre dos subnet

Filtrar por puerto

Todos los paquetes	tcp.port==	udp.port==
Solo cuando el puerto es fuente	tcp.src-cport==	udp.src-cport==
Solo cuando el puerto es destino	tcp.ds-tport==	udp.ds-tport==

Protocolo TCP

tcp.ack	Numero de acknowledge
tcp.analysis.ack_rtt	Tiempo de recibido contra tiempo de acknowledge
tcp.checksum	Checksum del paquete
tcp.flags	Banderas TCP

Referencias

Display Filter Reference Wireshark.org	https://www.wireshark.org/docs/dfref/
Wireshark Display Filter Cheat Sheet	https://www.cellstream.com/-resources/2013-09-10-11-55--21/cellstream-public-documents/wireshark-related/83-wireshark-display-filter-cheat-sheet/file
My Wireshark Display Filters Cheat Sheet	https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c
The Best Wireshark Filters	https://www.alphr.com/best--wireshark-filters/

By **ouyearedes**

cheatography.com/ouyearedes/

Not published yet.
Last updated 12th October, 2022.
Page 1 of 1.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com