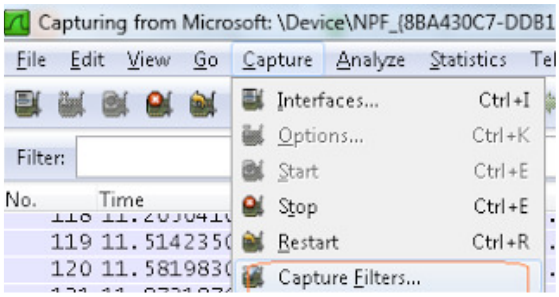
Wireshark. Filtros de Captura

Wireshark. Filtros de Captura y de Visualización

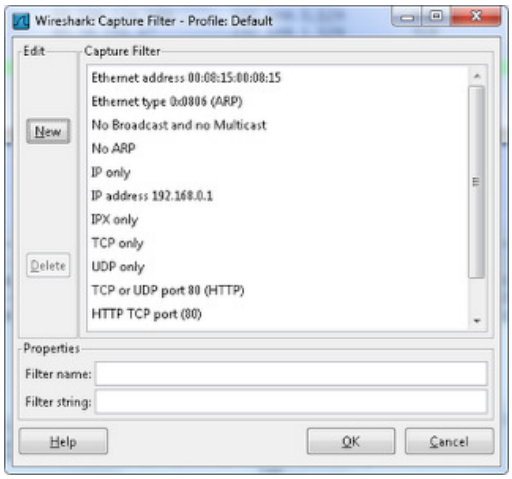
Los filtros de captura (Capture Filter) son los que se establecen para mostrar solo los paquetes de cumplan los requisitos indicados en el filtro. Si no establecemos ninguno, Wireshark capturará todo el tráfico y lo presentará en la pantalla principal. Aún así podrémos establecer filtros de visualización (display filter) para que nos muestre solo el trafíco deseado.

Los filtros de visualización (Display Filer) establecen un criterio de filtro sobre las paquetes capturados y que estamos visualizando en la pantalla principal de Wireshark. Estos filtros son mas flexibles y pontentes.

Para visualizar la ventana de Filtros de captura, vamos a Capture > Options:



Desde la ventana de Capture Filters podemos introducir un filtro en la caja de texto.



Sintaxis de los filtros y ejemplos de filtros de captura

Combinación de Filtros

Podemos combinar las primitivas de los filtros de la siguiente forma:

Negación: ! ó not
Unión o Concatenación: && ó and
Alternancia:|| ó or

Vamos ahora a los filtros:

Básico:

arp - Para capturar tráfico del Address Resolution Protocol

icmp - Para capturar tráfico icmp, por ejemplo captura de paquetes de ping

ip - Captura todo el tráfico IP

ipx - Capturar tráfico ipx, este comando puede ser util para determinar si este protocolo esta corriendo en la red (algo que ya no es nada comun en estos días).

netbeui - Capturar tráfico de NetBIOS extendede user interface

stp - Capturar tráfico de spanning tree protocol (a veces es útil usar la forma no stp para evitar este tráfico que pudiera no ser relevante para el análisis)

tcp - Captura todo el tráfico tcp

udp - Captura todo el tráfico udp

Filtros basados en hosts

host “host2 Filtrar por host
src host “host” Capturar por host origen
dst host “host” Capturar por host destino

Ejemplos:

host 192.168.1.20 Captura todos los paquetes con origen y destino 192.168.1.20
src host 192.168.1.1 Captura todos los paquetes con origen en host 192.1681.1
dst host 192.168.1.1 Captura todos los paquetes con destino en host 192.168.1.1
dst host SERVER-1 Captura todos los paquetes con destino en host SERVER-1
host www.google.com Captura todos los paquetes con origen y distino www.google.com

Filtros basados en puertos

port “port”
Captura todos los paquetes con puerto origen y destino port

src port “port”
Captura todos los paquetes con puerto origen port

dst port “port”
Captura todos los paquetes con puerto destino port

not port “port”
Captura todos los paquetes excepto origen y destino puerto port

not port “port” and not port “port1”
Captura todos los paquetes excepto origen y destino puertos port y port1

Ejemplos:

port 21
Captura todos los paquetes con puerto origen y destino 21
src port 21
Captura todos los paquetes con puerto origen 21
not port 21 and not port 80
Captura todos los paquetes excepto origen y destino puertos 21 y 80
portrange 1-1024
Captura todos los paquetes con puerto origen y destino en un rango de puertos 1 a 1024
dst portrange 1-1024 Captura todos los paquetes con puerto destino en un rango de puertos 1 a 1024

Filtros basados en protocolos Ethernet/IP

ip Captura todo el trafico IP
ip proto \tcp Captura todos los segmentos TCP
ether proto \ip Captura todo el trafico IP
ip proto \arp Captura todo el trafico ARP

Filtros basados en red

net net Captura todo el trafico con origen y destino red net
dst net net Captura todo el trafico con destino red net
src net net Captura todo el trafico con origen red net

Ejemplos:

net 192.168.1.0 Captura todo el trafico con origen y destino subred 1.0
net 192.168.1.0/24 Captura todo el trafico para la subred 1.0 mascara 255.0
dst net 192.168.2.0 Captura todo el trafico con destino para la subred 2.0
net 192.168.2.0 and port 21 Captura todo el trafico origen y destibo puerto 21 en subred 2.0
broadcast Captura solo el trafico broadcast
not broadcast and not multicast Captura todo el trafico excepto el broadcast y el multicast

Filtros de visualización

Comparando filtros:

Igual a: eq ó ==
No igual: ne ó !=
Mayor que:gt ó >
Menor que: lt ó < Mayor o igual: ge ó >=
Menor o igual: le ó <=

Combinando filtros:

Negación: ! ó not
Unión o Concatenación: && ó and
Alternancia:|| ó or

Otro operadores:

Contains: Realizamos una busqueda por la cadena contains

Todos estos filtros los debemos poner en la pantalla principal de Wireshark en la caja de texto Filter.

Filtros de visualización

ip.addr == 192.168.1.40 Visualizar tráfico por host 192.168.1.40
ip.addr != 192.168.1.25 Visualizar todo el tráfico excepto host 192.168.1.25
ip.dst == 192.168.1.30 Visualizar por host origen 192.168.1.30
ip.src == 192.168.1.30 Visualizar por host destino 192.168.1.30
ip Visualiza todo el tráfico IP
tcp.port ==143 Visualiza todo el tráfico origen y destino puerto 143
ip.addr == 192.168.1.30 and tcp.port == 143 Visualiza todo el tráfico origen y destino puerto 143 relativo al gost 192.168.1.30
http contains “http://www.google.com“ Visualiza los paquetes que contienen www.google.com en el contenido en protocolo http.
frame contains “@gmail.com” Visualizamos todos los correos con origen y destino al dominio gmail.com
icmp[0:1] == 08 Filtro avanzado con el que visualizamos todo el tráfico icmp de tipo echo request
ip.ttl == 1 Visualiza todo los paquetes IP cuyo campo TTL sea igual a 1
tcp.windows_size != 0 Visualizar todos los paquetes cuyos campo Tamaño de Ventana del segmento TCP sea distinto de 0
ip.tos == x Visualiza todo los paquetes IP cuyo campo TOS sea igual a x
ip.flags.df == x Visualiza todo los paquetes IP cuyo campo DF sea igual a x
udp.port == 53 Visualiza todo el trafico UDP puerto 53
tcp contains “google.com” Visualizamos segmentos TCP conteniendo la cadena google.com