Análisis de red con Wireshark. Filtros de captura y visualización.

Wireshark contempla dos tipos de Filtros. **Filtros de captura y Filtros 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.

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

Filtros de Visualización (Display Filter)

Los filtros de visualización establecen un criterio de filtro sobre los paquetes que estamos capturando y que estamos visualizando en la pantalla principal de Wireshark. Al aplicar el filtro en la pantalla principal de Wireshark aparecerá solo el tráfico filtrado a través del filtro 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**

Otros operadores.

- Contains: Realizamos una búsqueda por la cadena contains

Ejemplos de filtros:

Filtros de visualización

Ejemplos

Sintaxis	Significado
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 destino192.168.1.30
ip.src == 192.168.1.30	Visualizar por host origen 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 host 192.168.1.30
http contains “https://www.todofp.es/“	Visualiza el tráfico origen y destino https://www.todofp.es/. Visualiza los paquetes que contienen https://www.todofp.es/ en el contenido en protocolo http.
frame contains “@miempresa.es»	Visualizamos todos los correos con origen y destino al dominio ***miempresa.es***, incluyendo **usuarios, pass**, etc
icmp[0:1] == 08	Filtro avanzado con el que visualizamos 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	Visualizar todos los paquetes cuyos campos Tamaño de Ventana del segmento TCP sea distinto de 0
ip.tos == x	Visualiza todos los paquetes IP cuyo campo TOS sea igual a x
ip.flags.df == x	Visualiza todos los paquetes IP cuyo campo DF sea igual a x
udp.port == 53	Visualiza todo el tráfico UDP puerto 53
tcp contains “todofp.es»	Visualizamos segmentos TCP conteniendo la cadena todofp.es