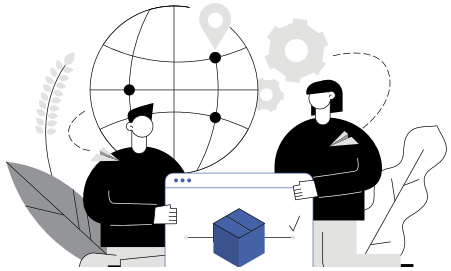


Wireshark cheat sheet

Herramienta gratuita para el análisis de protocolos de red.
Permite analizar en detalle todo el tráfico entrante y saliente en un equipo.

1. Filtros de visualización en Wireshark

- Modos de captura de Wireshark

a. Modo promiscuo

Establece la interfaz para capturar todos los paquetes en un segmento de red al que está asociado.

b. Modo monitor

Configura la interfaz inalámbrica para capturar todo el tráfico que puede recibir (sólo Unix/Linux).

- Tipos de filtro

a. Filtro de captura

Filtra paquetes durante la captura.

b. Filtro de visualización

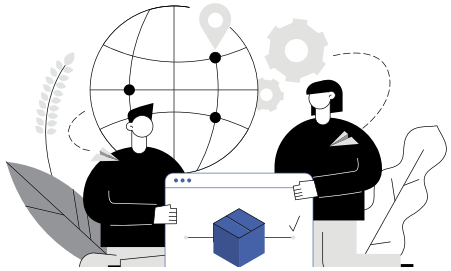
Oculta paquetes de una pantalla de captura.

- Sintaxis del filtro de captura

Ejemplo	Protocolo	Dirección	Hosts	Valor	Operador lógico	Expresión
204.163.20.3	tcp	src	192.168.1.1	80	and	tcp dst

- Sintaxis del filtro de visualización

Sintaxis	Protocolo	Cadena1	Cadena2	Operador comparación	Operador lógico	Expresión
[redacted]	http	dest	ip	==	and	tcp port



2. Protocolos - Valores

- **ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp , udp**

3. Filtrado de paquetes (Filtros de visualización)

Operador	Descripción	Ejemplo
eq o ==	Igual	ip.dest == 192.168.1.1
ne o !=	No es igual	ip.dest != 192.168.1.1
gt o >	Mayor que	frame.len > 10
lt o <	Menor que	frame.len <10
ge o >=	Mayor que o igual	frame.len >= 10
le o <=	Menor que o igual	frame.len <= 10

4. Misceláneo

- **Operador slice**
  [...] - Rango de valores

  Ejemplo:
  eth.src[1-2] == 00:83
- **Operador de Membresía**
  {} - En

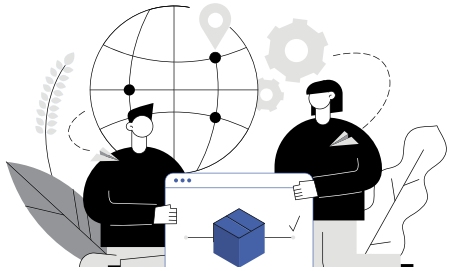
  Ejemplo:
  tcp.port in {80, 443, 8080}
- **Iniciar/Detener captura**
  CTRL+E

5. Operadores lógicos

Operador	Descripción	Ejemplo
And o &&	And lógico	Se deben cumplir todas las condiciones
Or o ||	Or lógico	Una o todas las condiciones se deben cumplir
Xor o ^^	Xor lógico	Sólo una de las condiciones se debe cumplir
Not o !	Negación	No es igual a
[n] [...]	Operador de subcadena	Filtrar una palabra o texto específico

6. Columnas predeterminadas en una salida de captura de paquetes

- **No**
  Número de trama desde el principio de la captura de paquetes
- **Time**
  Segundos desde el primer fotograma
- **Source (src)**
  Dirección de origen, comúnmente una dirección IPv4, IPv6 o Ethernet
- **Destination (dst)**
  Dirección de destino
- **Protocol**
  Protocolo utilizado en la trama Ethernet, el paquete IP o el segmento TCP
- **Length**
  Longitud de la trama en bytes

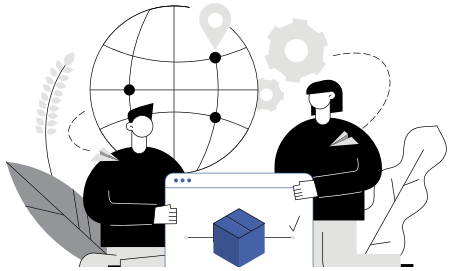


7. Métodos abreviados de teclado: ventana principal

- **Espacio o Shift+Espacio**
  Moverse entre los elementos de la pantalla, por ejemplo, desde las barras de herramientas hasta la lista de paquetes y el detalle del paquete.
- **Alt+→ o Option+→**
  Pasar al siguiente paquete en el historial de selección.
- **↓**
  Ir al siguiente paquete o elemento de detalle.
- **→**
  En el detalle del paquete, abre el elemento de árbol seleccionado.
- **↑**
  Ir al paquete o elemento de detalle anterior.
- **Shift+→**
  En el detalle del paquete, abre el elemento de árbol seleccionado y todos sus subárboles.
- **Ctrl+↓ o F8**
  Ir al siguiente paquete, incluso si la lista de paquetes no está enfocada.
- **Ctrl+→**
  En el detalle del paquete, abre todos los elementos del árbol.
- **Ctrl+↑ o F7**
  Ir al paquete anterior, incluso si la lista de paquetes no está enfocada.
- **Ctrl+←**
  En el detalle del paquete, cierra todos los elementos del árbol.
- **Ctrl+**
  Ir al siguiente paquete de la conversación (TCP, UDP o IP).
- **Backspace (retroceso)**
  En el detalle del paquete, salta al nodo primario.
- **Ctrl+,**
  Desplazarse al paquete anterior de la conversación (TCP, UDP o IP).
- **Return o Enter**
  En el detalle del paquete, alterna el elemento de árbol seleccionado.

8. Comandos de filtrado comunes

- **Filtro Wireshark por IP**
  ip.addr == 10.20.70.1
- **Filtrar por IP de destino**
  ip.dest == 10.20.70.1
- **Filtrar por IP de origen**
  ip.src == 10.20.70.1
- **Filtrar por rango de IP**
  ip.addr >= 10.20.70.1 and ip.addr <= 10.20.70.100
- **Filtrar por múltiples IPs**
  ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100
- **Filtrar/Excluir dirección IP**
  !(ip.addr == 10.20.100.1)
- **Filtrar subred IP**
  ip.addr == 10.10.50.1/24
- **Filtrar por varias subredes IP especificadas**
  ip.addr == 10.10.50.1/24 and ip.addr == 10.10.51.1/24
- **Filtrar por protocolo**
  Dns, http,ftp, ssh, arp, telnet, icmp
- **Filtrar por puerto (TCP)**
  tcp.port == 25
- **Filtrar por puerto de destino (TCP)**
  tcp.dstport == 23
- **Filtrar por dirección IP y puerto**
  ip.addr == 10.200.80.1 and Tcp.port == 25
- **Filtrar por URL**
  http.host == "host name"
- **Filtrar por timestamp**
  frame.time >= "June 02, 2019 18:04:00"
- **Filtro SYN flag**
  tcp.flags.syn == 1
  tcp.flags.syn == 1 and tcp.flags.ack == 0
- **Filtro wireshark Beacon**
  wlan.fc.type_subtype = 0x08
- **Filtro broadcast Wireshark**
  eth.dst == ff:ff:ff:ff:ff:ff
- **Filtro Multicast**
  (eth.dst[0] & 1)
- **Filtro de nombre de host**
  ip.host = hostname
- **Filtro de direcciones MAC**
  eth.addr == 00:70:f4:23:18:c4
- **Filtro de indicador RST**
  tcp.flags.reset == 1



9. Elementos principales de la barra de herramientas

Icono de la barra de herramientas	Elemento de la barra de herramientas	Elemento del menú	Descripción
	Empezar	Capture → Start	Utiliza las mismas opciones de captura de paquetes que la sesión anterior o utiliza valores predeter-minados si no se ha establecido ninguna opción
	Parar	Capture → Stop	Detiene la captura actualmente activa
	Reanudar	Capture → Restart	Reinicia la sesión de captura activa
	Opciones...	Capture → Options...	Abre el cuadro de diálogo "Opciones de captura"
	Abrir...	File → Open...	Abre el cuadro de diálogo "Archivo abierto" para cargar una captura para su visualización
	Guardar como...	File → Save As...	Guardar archivo de captura actual
	Cerrar	File → Close	Cerrar archivo de captura actual
	Recargar	View → Reload	Recarga el archivo de captura actual
	Buscar paquete...	Edit → Find Packet...	Buscar paquetes en función de diferentes criterios
	Volver	Go → Go Back	Volver al historial de paquetes
	Adelantarse	Go → Go Forward	Saltar hacia adelante en el historial de paquetes
	Ir a Paquete...	Go → Go to Packet...	Ir a un paquete específico
	Ir al primer paquete	Goe → First Packet	Saltar al primer paquete del archivo de captura
	Ir al último paquete	Go → Last Packet	Saltar al último paquete del archivo de captura
	Desplazamiento automático en Live Capture	View → Auto Scroll in Live Capture	Lista de paquetes de desplaza-miento automático durante la captura en vivo
	Colorear	View → Colorize	Colorear la lista de paquetes (o no)
	Acercar	View → Zoom In	Ampliar los datos del paquete (aumente el tamaño de la fuente)
	Alejar	View → Zoom Out	Alejar los datos del paquete (disminuir el tamaño de la fuente)
	Tamaño normal	View → Normal Size	Volver a establecer el nivel de zoom en 100%
	Cambiar el tamaño de las columnas	View → Resize Columns	Cambiar el tamaño de las columnas, para que el contenido se ajuste al ancho