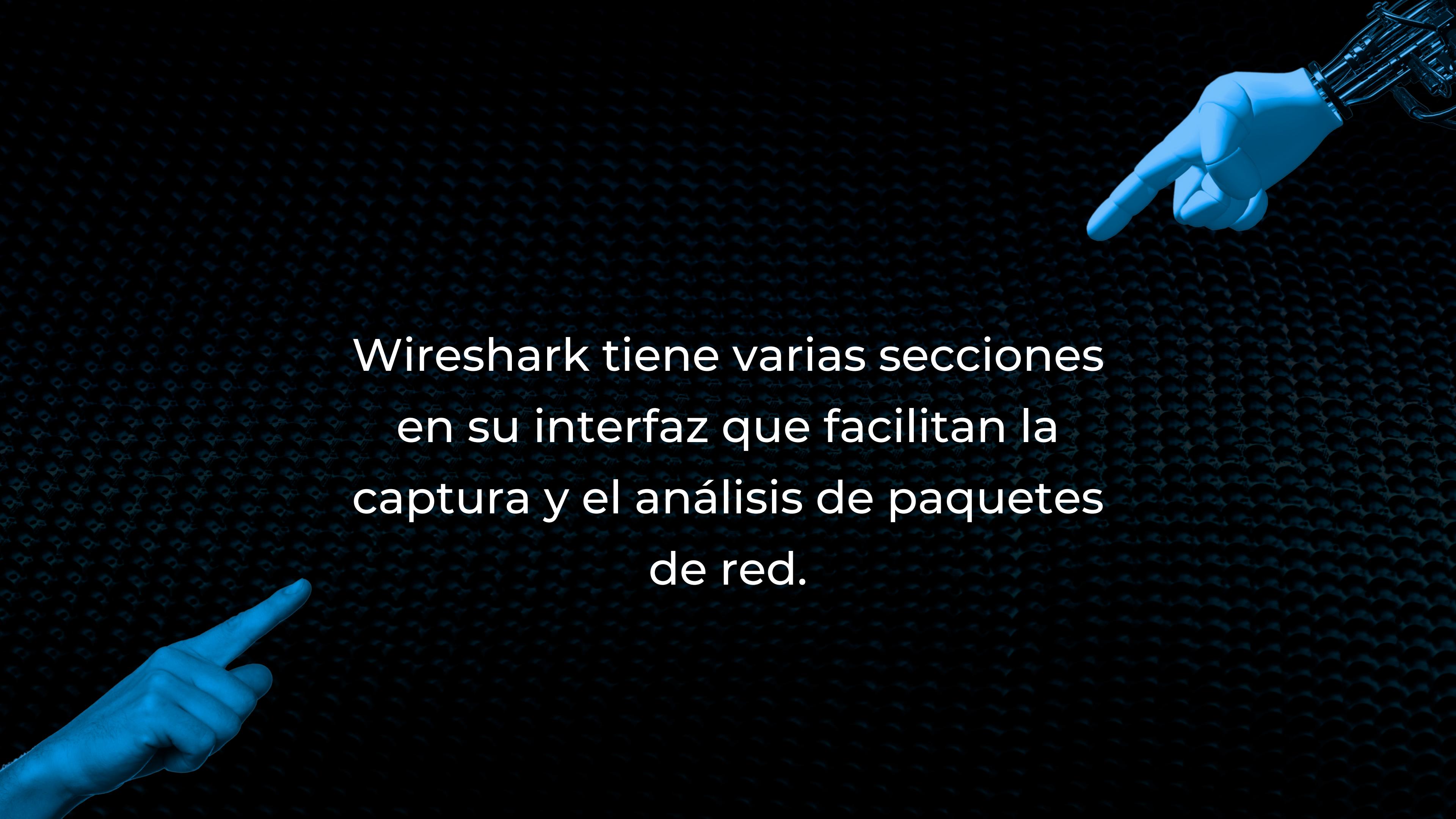




Sofia Gil-Camilo Castaño-Carolina Morales

PARTES DE LA INTERFAZ WIRESHARK



Wireshark tiene varias secciones
en su interfaz que facilitan la
captura y el análisis de paquetes
de red.

Partes de la interfaz

1

Barra de Menú:

Contiene opciones para abrir archivos, iniciar y detener la captura, y acceder a diferentes funciones y configuraciones.

2

Barra de Herramientas:

Proporciona accesos directos a funciones comunes, como iniciar/detener la captura, filtrar paquetes y configurar opciones.

3

Panel de Lista de Paquetes:

Muestra una lista de todos los paquetes capturados con detalles clave, como número de paquete, tiempo, origen, destino y protocolo.

4

Panel de Detalles del Paquete:

Ofrece información detallada sobre el paquete seleccionado en la lista, desglosando cada capa del protocolo.

5

Panel de Árbol de Protocolos:

Proporciona una vista jerárquica de los campos del paquete, facilitando el análisis detallado de cada protocolo.

6

Panel de Bytes de Datos:

Muestra la representación hexadecimal y ASCII de los datos contenidos en el paquete seleccionado.

Partes de la interfaz

6

Panel de Flujo:

Permite ver la conversación entre dos hosts a lo largo del tiempo, facilitando el seguimiento de interacciones específicas.

7

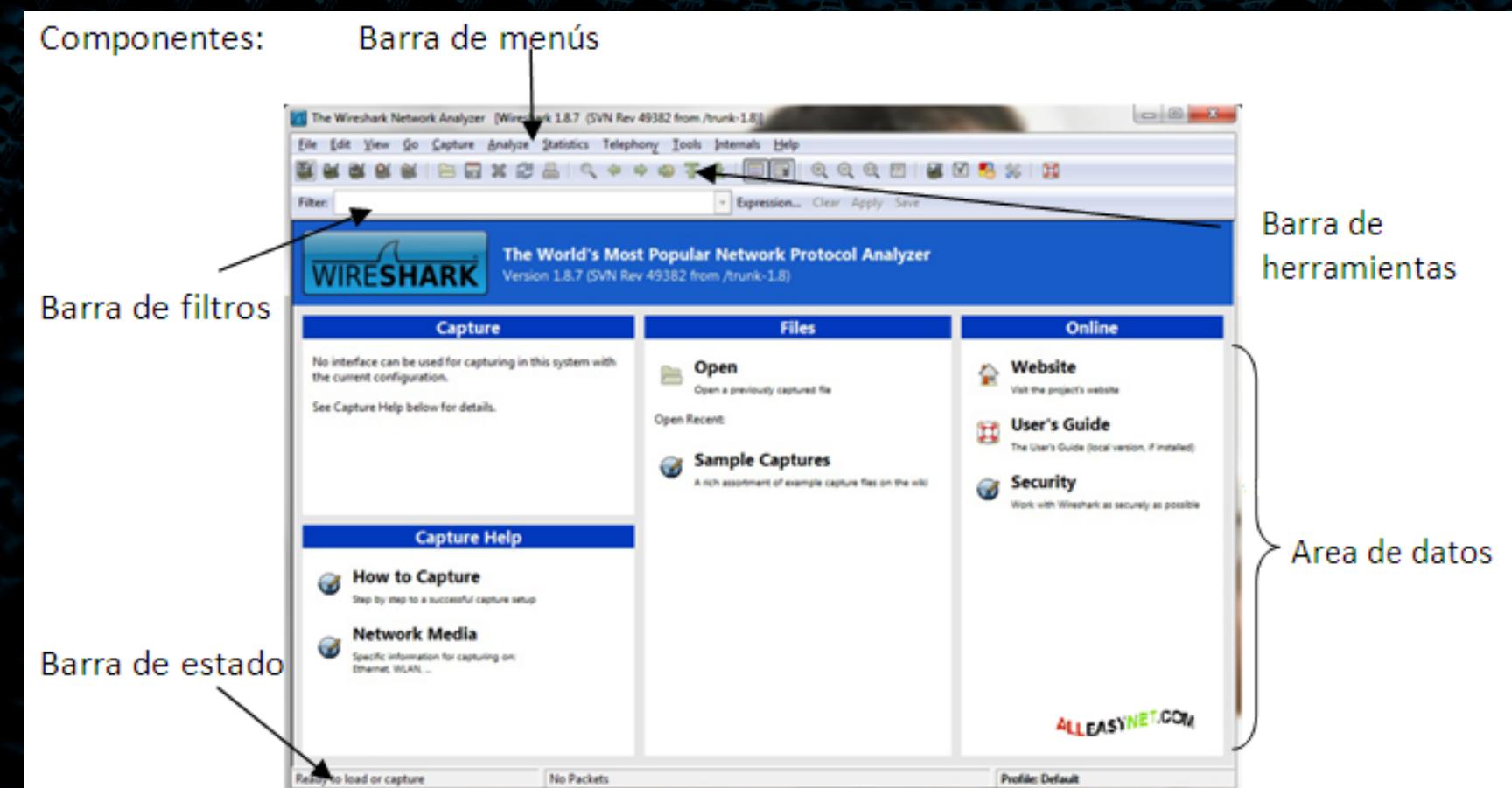
Filtros:

Permite aplicar filtros para mostrar solo los paquetes que cumplen con ciertos criterios, como direcciones IP o protocolos específicos.

8

Barra de Estado:

Proporciona información sobre la captura en curso, como el número de paquetes capturados y el ancho de banda utilizado.



Generar filtros

Filtrar por Dirección IP:

Para ver solo los paquetes que involucran una dirección IP específica, puedes usar el filtro: `ip.addr == <dirección IP>`.

Filtrar por Protocolo:

Puedes filtrar por un protocolo específico, por ejemplo, para ver solo los paquetes de protocolo TCP: `tcp`.

Filtrar por Puerto:

Si deseas ver solo paquetes que utilizan un puerto específico, puedes usar: `tcp.port == <número de puerto>` o `udp.port == <número de puerto>`.

Filtrar por Tipo de Tráfico:

Puedes filtrar por el tipo de tráfico, por ejemplo, para ver solo paquetes ICMP (ping): `icmp`.

Filtrar por Dirección MAC:

Para filtrar por una dirección MAC específica, puedes usar: `eth.addr == <dirección MAC>`. `icmp`.

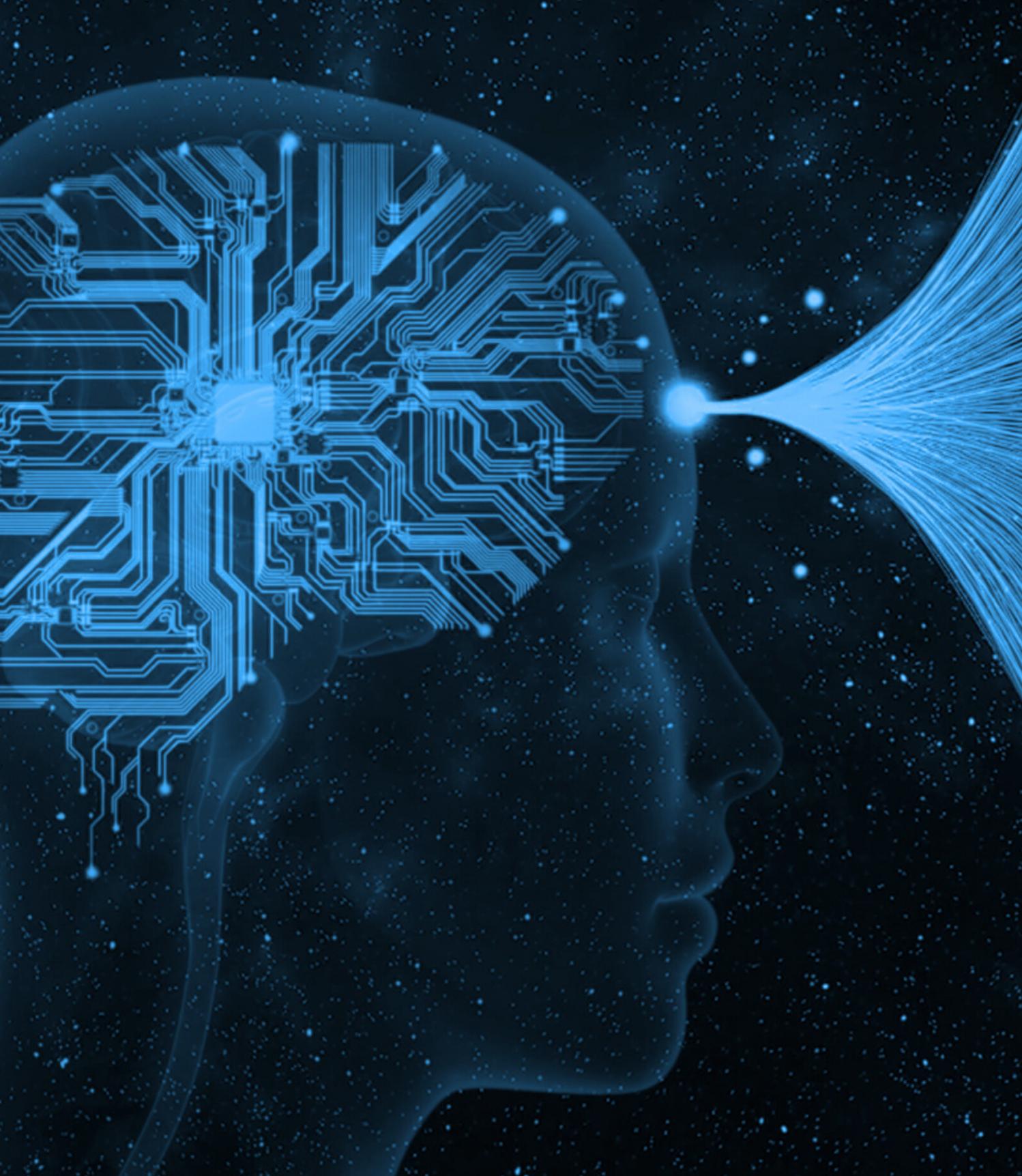
Filtrar por Nombre de Host:

Si quieres ver paquetes relacionados con un nombre de host específico, puedes utilizar el filtro `dns.resp.name == <nombre del host>`.

Filtrar por Longitud de Paquete:

Si estás interesado en paquetes de una longitud específica, puedes usar filtros como `frame.len == <longitud>`.





¿Para qué se usan los filtros?

Los filtros en Wireshark son herramientas poderosas que permiten enfocarse en paquetes de red específicos, lo que facilita el análisis y la resolución de problemas en una red.

Identificación de Problemas de Conexión:

- Si se experimentando problemas de conectividad con un servidor.

```
ip.addr == <dirección IP del servidor>
```

Análisis de Tráfico Web:

- Permite examinar las solicitudes y respuestas HTTP, identificar URLs específicas y analizar el contenido.



```
http
```

Detección de Ataques:

- Para identificar posibles ataques, como escaneo de puertos.

```
tcp.flags == 0x02 # Paquetes SYN (inicio de conexión)
```

Bibliografía



Sitio web

[Wireshark Official Website](#)

"Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide" de [Laura Chappell](#).