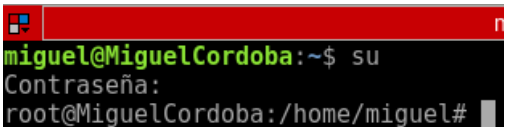
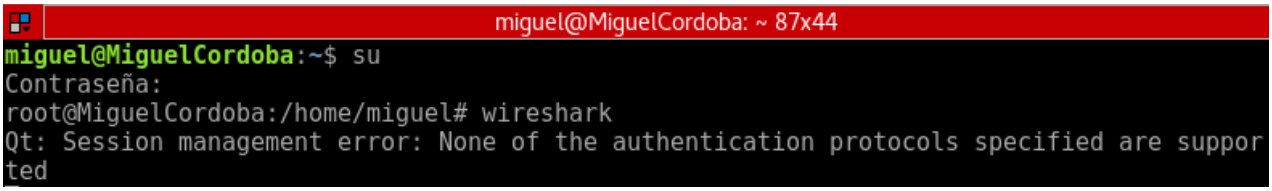
# CAPTURA DE TRAFICO CON WIRESHARK

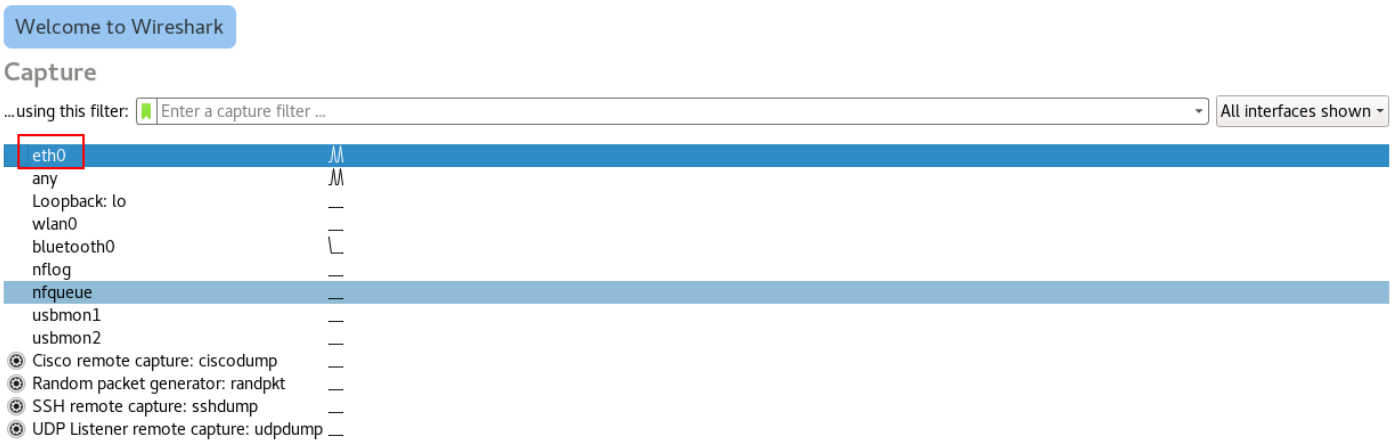
Para capturar tráfico con **Wireshark** tenemos que ponernos como superusuario en la terminal.




Una vez logueado como superusuario ponemos **Wireshark** en la terminal para poder capturar tráfico en nuestra interfaz.

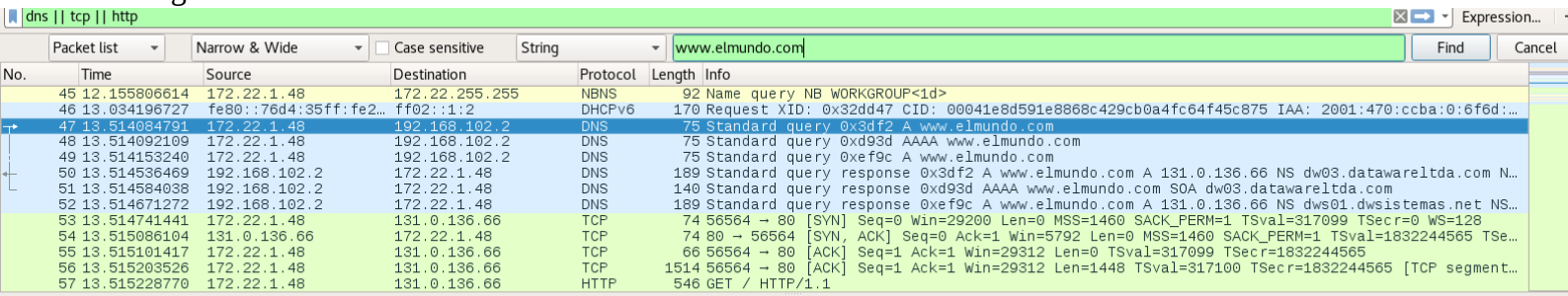



Una vez iniciado el **Wireshark** nos da la opción de seleccionar la interfaz por la que queremos capturar el tráfico. En este caso seleccionaremos **eth0**.




Para capturar el tráfico primero debemos poner el **Wireshark** en escucha y luego acceder a la web de la que deseemos obtener la información.

Con este icono (parte superior izquierda) iniciamos la escucha y posteriormente en el navegador introducimos la URL.
Por defecto nos saldrá mucha información en una captura de tráfico por lo que lo filtramos de la siguiente manera.




En el primer filtrado le indicamos que solo queremos ver **dns || tcp || http** y en el segundo filtrado le he indicado el nombre **www.elmundo.com**.

A continuación pasare a desglosar la información de la captura.

1. 6 paquetes de **DNS**.
2. 4 paquetes **TCP**.
3. 1 paquete de **HTTP**.

Cuando el servidor recibe el mensaje 10, con la petición de la página de inicio, ¿cómo sabe cuál es el sitio web del que debe enviar la página principal?