A continuación, se describe cómo instalar Wireshark en un contenedor Docker basado en Ubuntu:

**Pasos:**

1. **Crea un archivo Dockerfile** Este archivo definirá cómo se configura el contenedor.
2. # Usa una imagen base de Ubuntu
3. FROM ubuntu:latest
4. # Actualiza el sistema e instala Wireshark
5. RUN apt-get update && apt-get install -y \
6. wireshark \
7. tshark \
8. && apt-get clean
9. # Configura Wireshark para ejecutarse sin GUI (modo terminal)
10. ENV DEBIAN\_FRONTEND=noninteractive
11. # Crea un punto de entrada para utilizar Wireshark
12. ENTRYPOINT ["/usr/bin/tshark"]
13. **Construye la imagen de Docker** Utiliza el Dockerfile para construir la imagen:
14. docker build -t wireshark-docker .
15. **Ejecuta el contenedor con privilegios** Para capturar paquetes, Wireshark requiere acceso a las interfaces de red, lo que significa que debes ejecutar el contenedor con privilegios elevados.
16. docker run --rm -it --network="host" --cap-add=NET\_ADMIN --cap-add=NET\_RAW wireshark-docker
    * --network="host": Permite que el contenedor use la red del host.
    * --cap-add=NET\_ADMIN y --cap-add=NET\_RAW: Permiten capturar tráfico de red.
17. **Ejecuta Wireshark en el contenedor** Una vez dentro del contenedor, puedes usar tshark, la versión en línea de comandos de Wireshark:
18. tshark -i eth0

Sustituye eth0 con la interfaz de red que deseas monitorear.

**Notas adicionales:**

* **Acceso GUI**: Wireshark es una herramienta gráfica, pero dentro de Docker puede ser más práctico usar tshark.
* **Permisos**: Si necesitas GUI, necesitarás configurar un servidor X o usar una herramienta como VNC para redirigir la salida gráfica.
* **Uso responsable**: Asegúrate de usar esta herramienta solo en redes donde tengas permiso de monitoreo.