

Universidad del Valle de Guatemala

Facultad de ingeniería

Redes

Catedrático: Jorge Yass



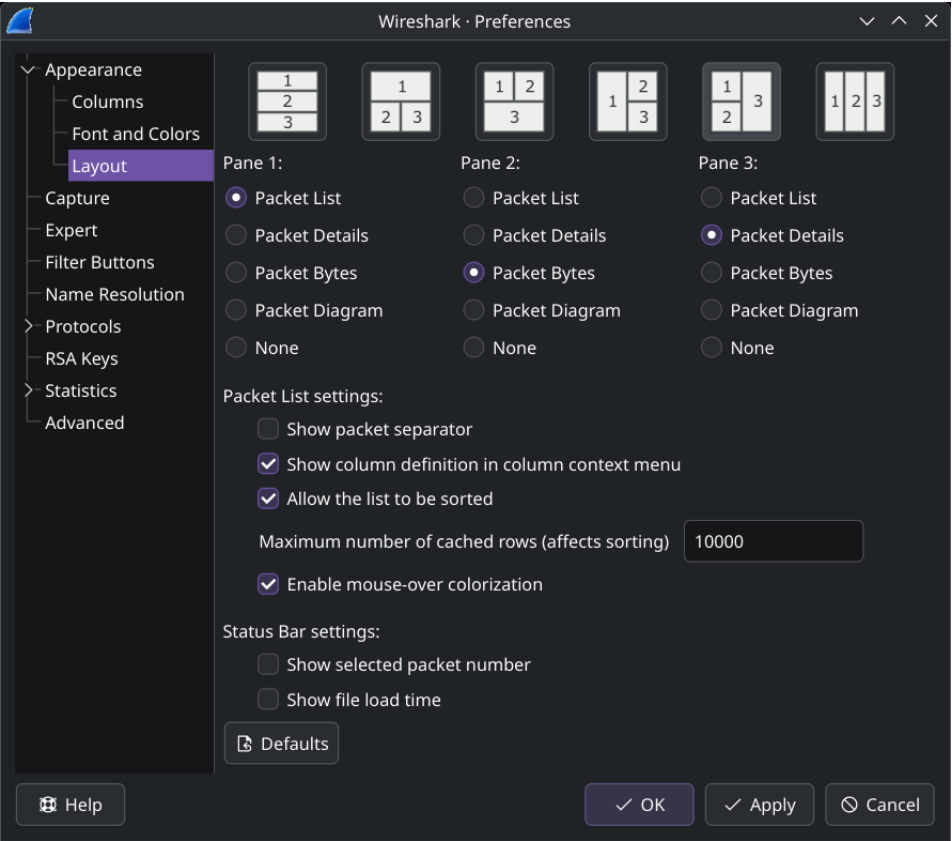
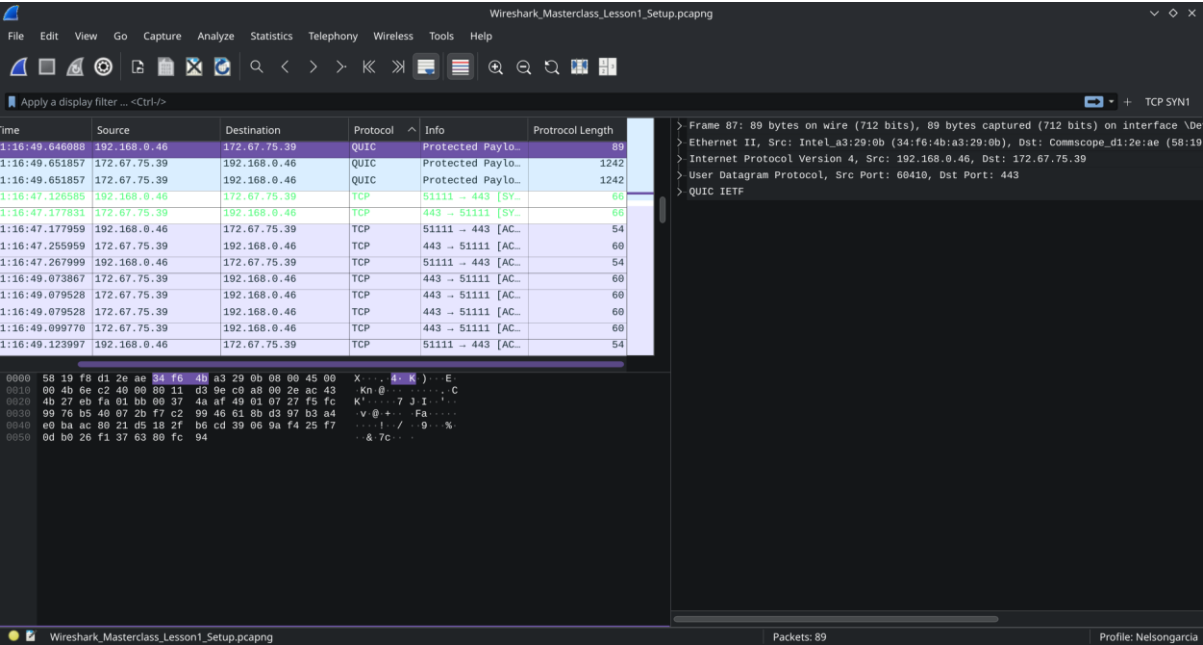
Laboratorio #1 - Esquemas de comunicación e Introducción a Wireshark

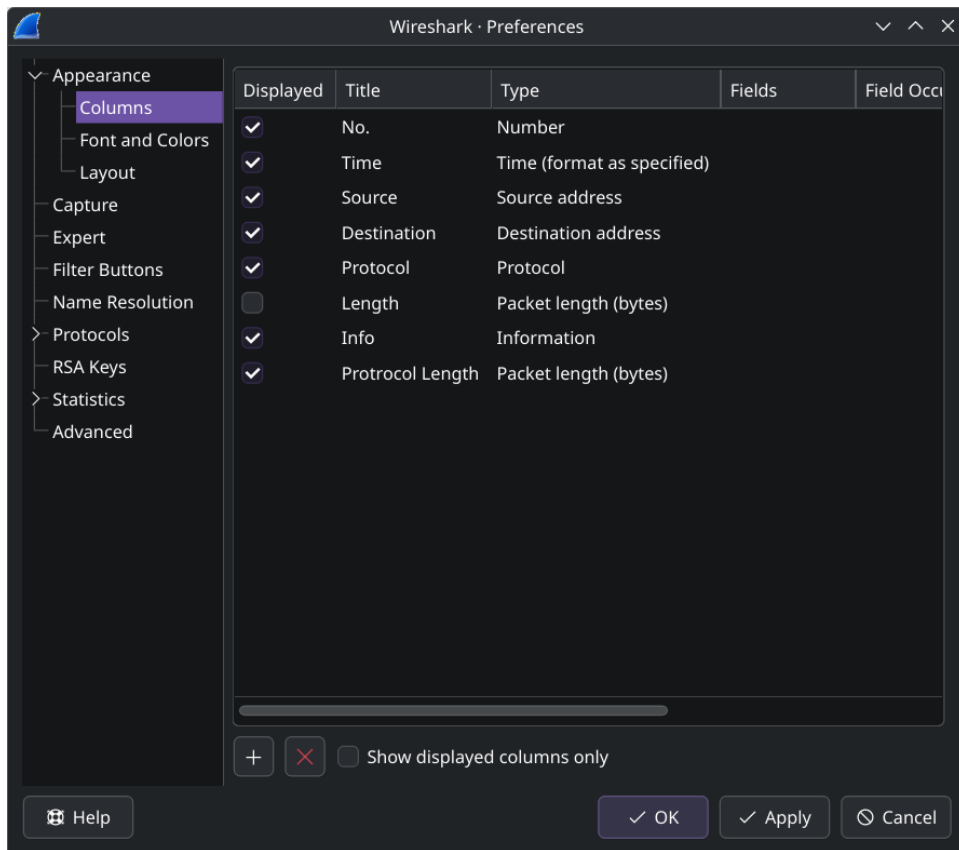
Nelson Eduardo García Bravatti 22434

Guatemala, julio de 2025

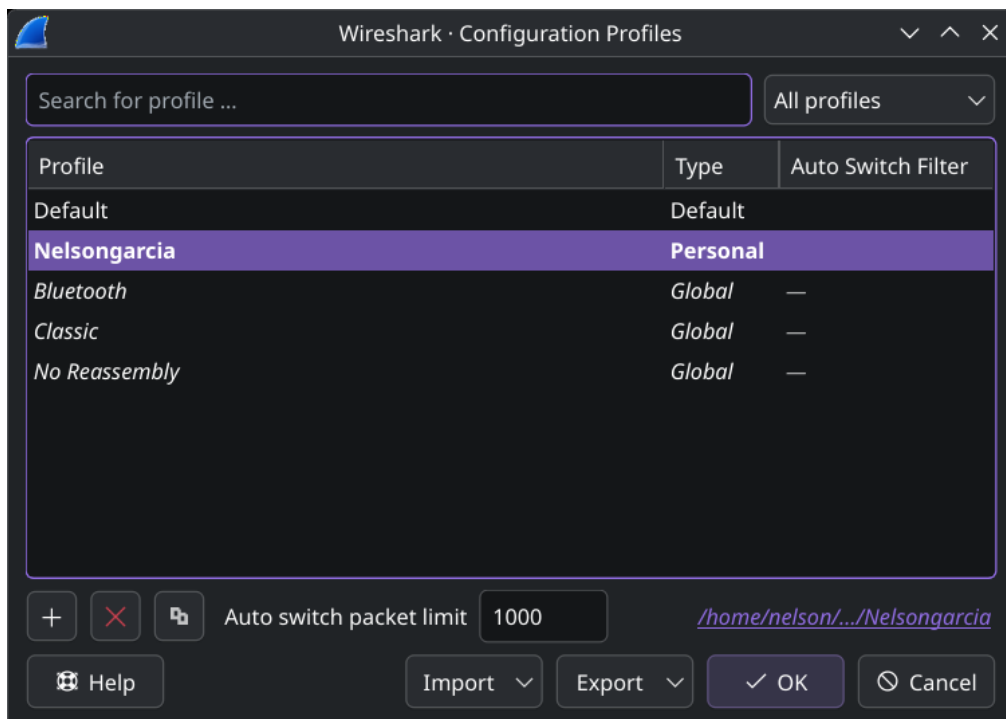
1.1 Personalización del entorno:

Entorno final:

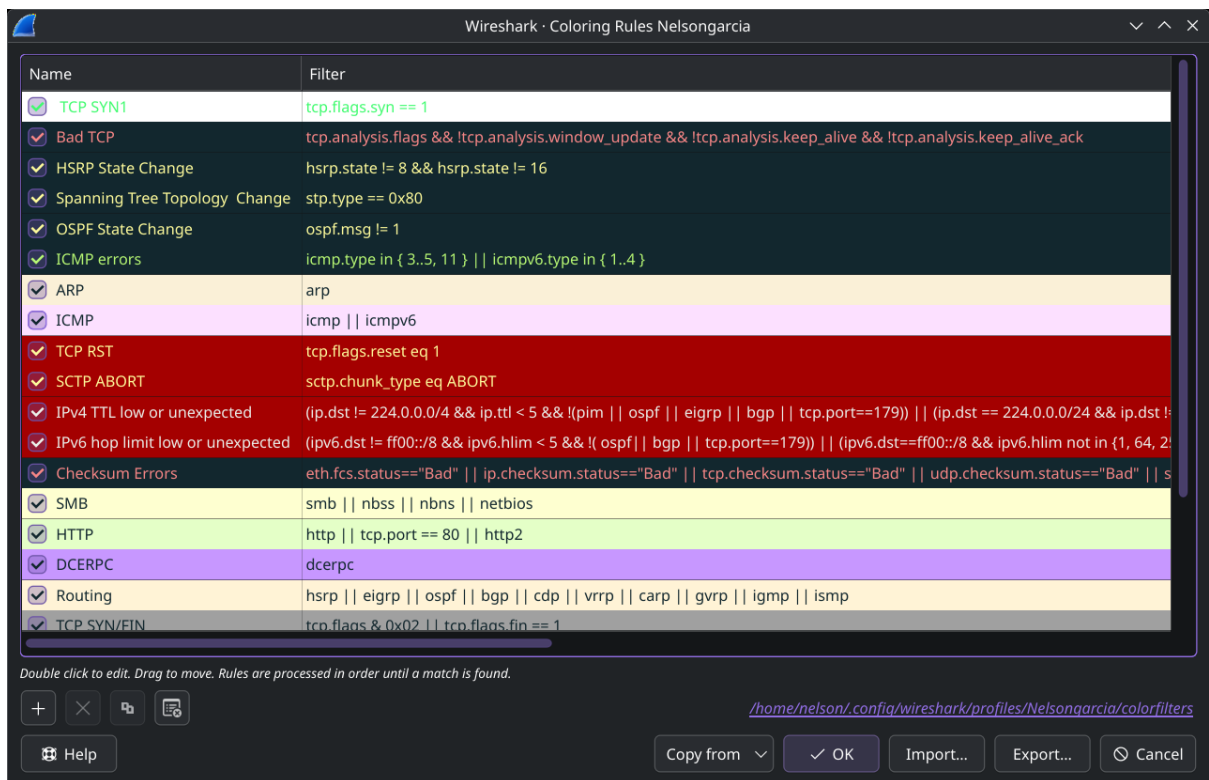




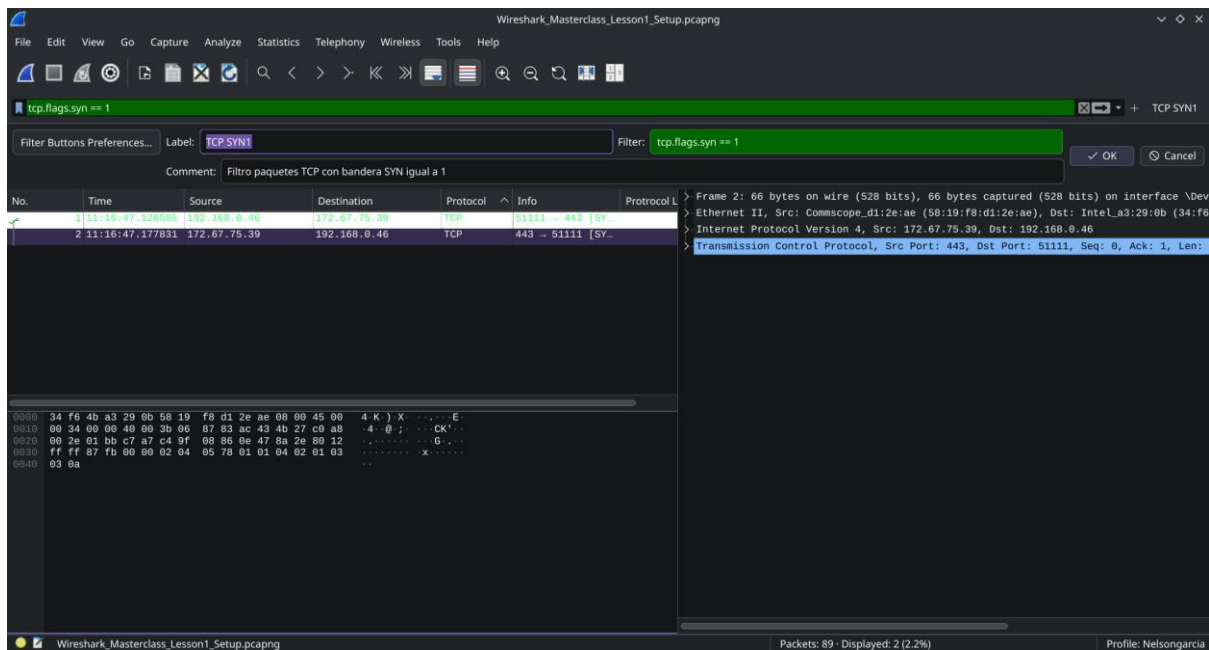
Perfil:



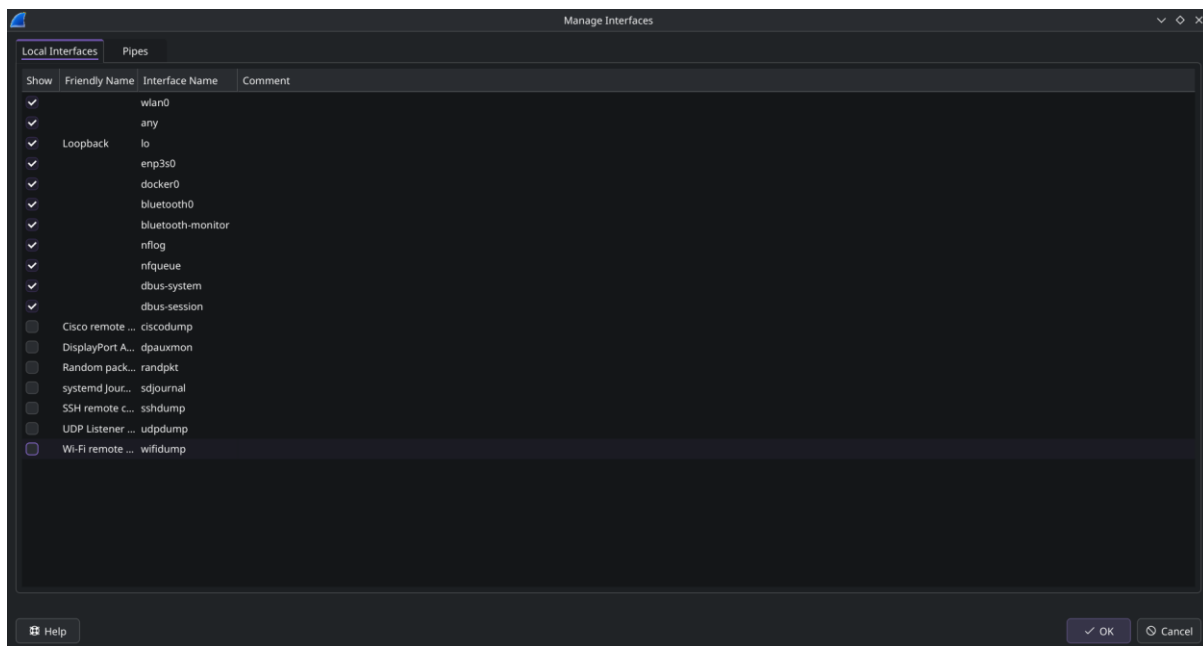
Regla de color:



Botón de filtro:

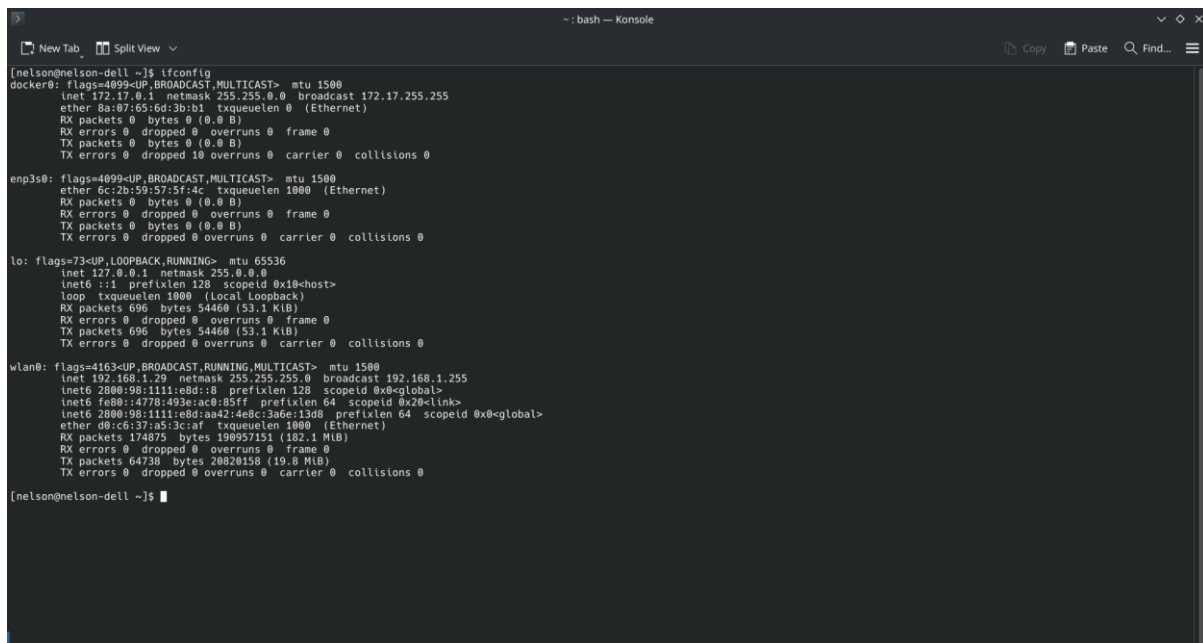


Lista simplificada de interfaces:



1.2 Configuración de la captura de paquetes:

1.

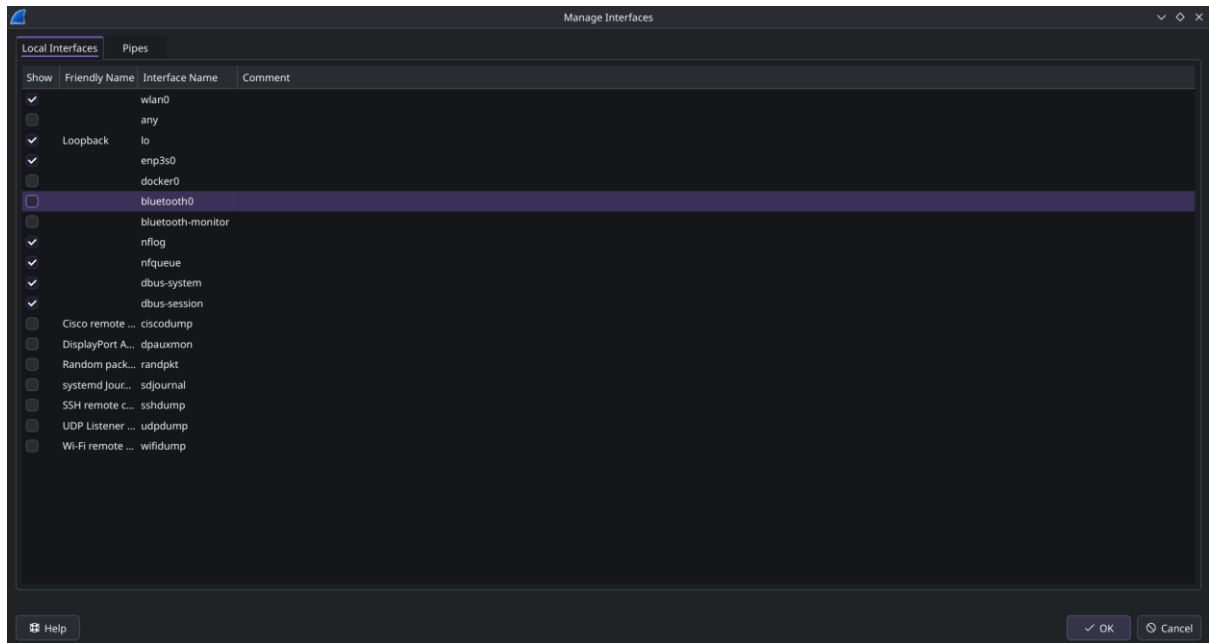


R// El comando `ifconfig` (interface configuration) se usa para ver la configuración de las interfaces de red, lo que hace es mostrarte información como:

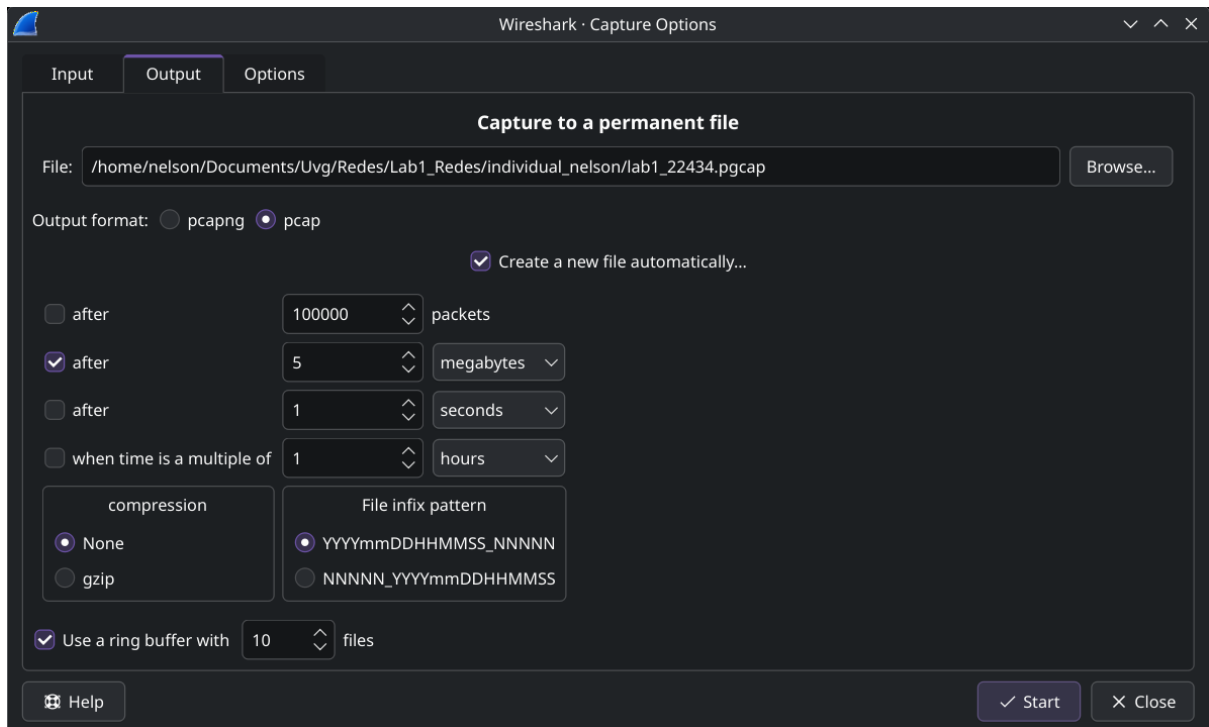
- Nombre de la interfaz de red (por ejemplo: `docker0`, `enp3s0`, `lo`, `wlan0`; en mi caso)
- Estado (UP/DOWN), si está activa o no
- Dirección IP asignada (IPv4 e IPv6)
- Máscara de red y dirección de broadcast
- Dirección MAC (ether)

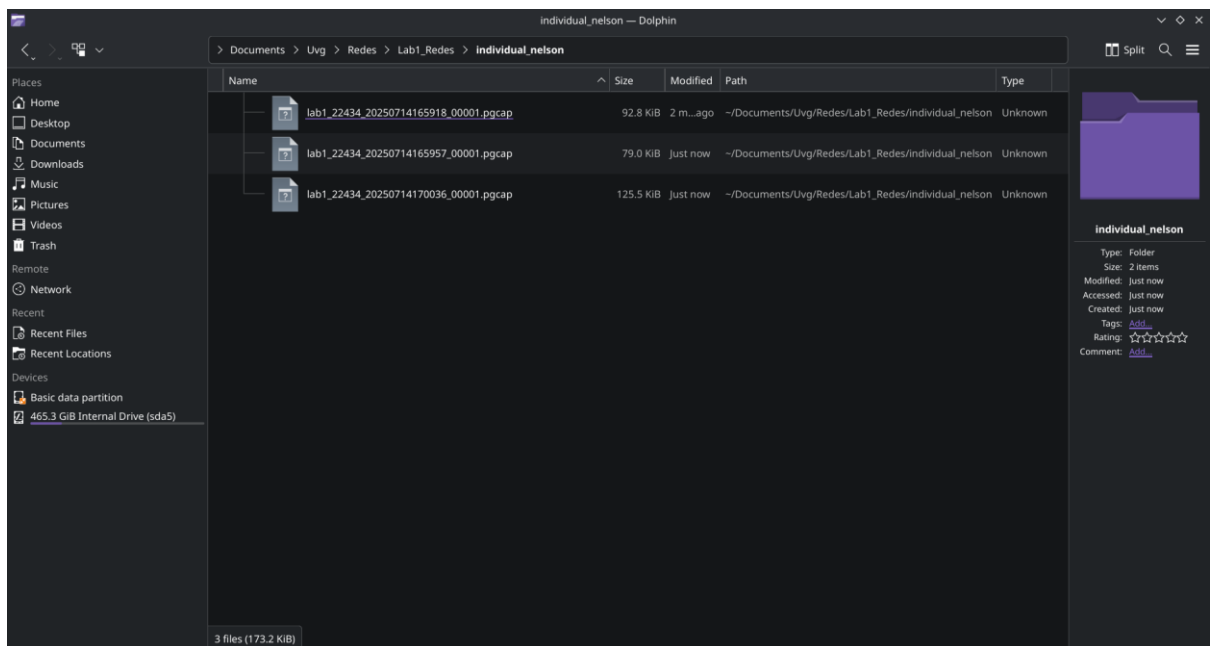
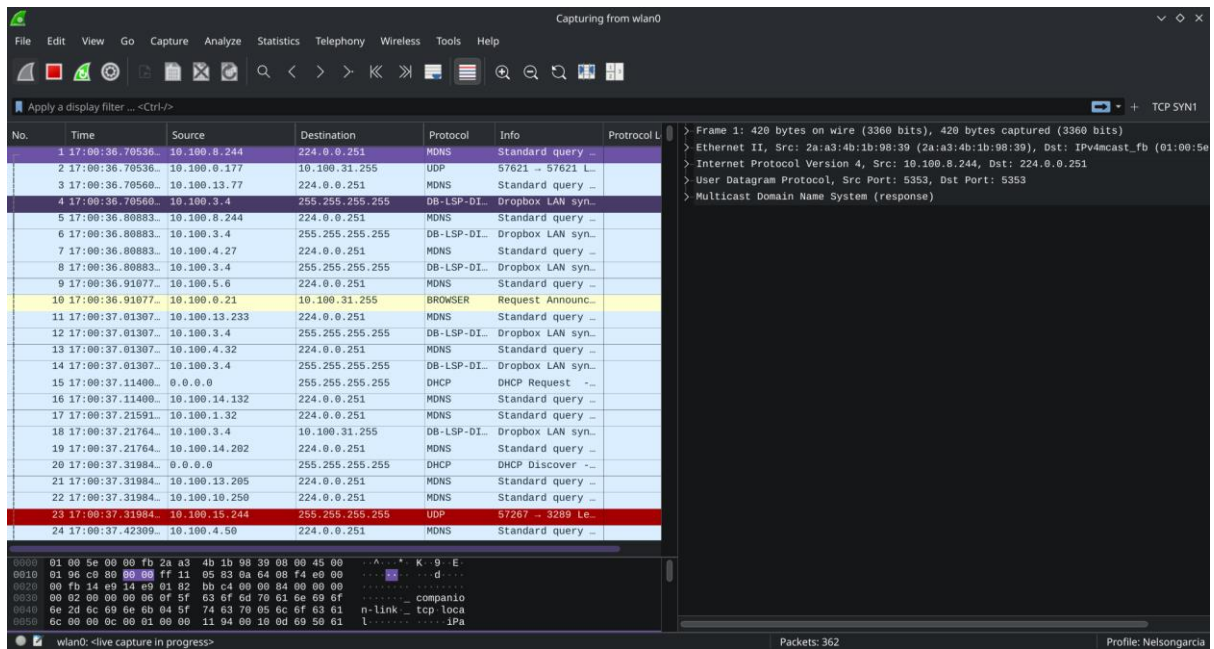
- Cantidad de paquetes transmitidos y recibidos
- Errores y colisiones

2.



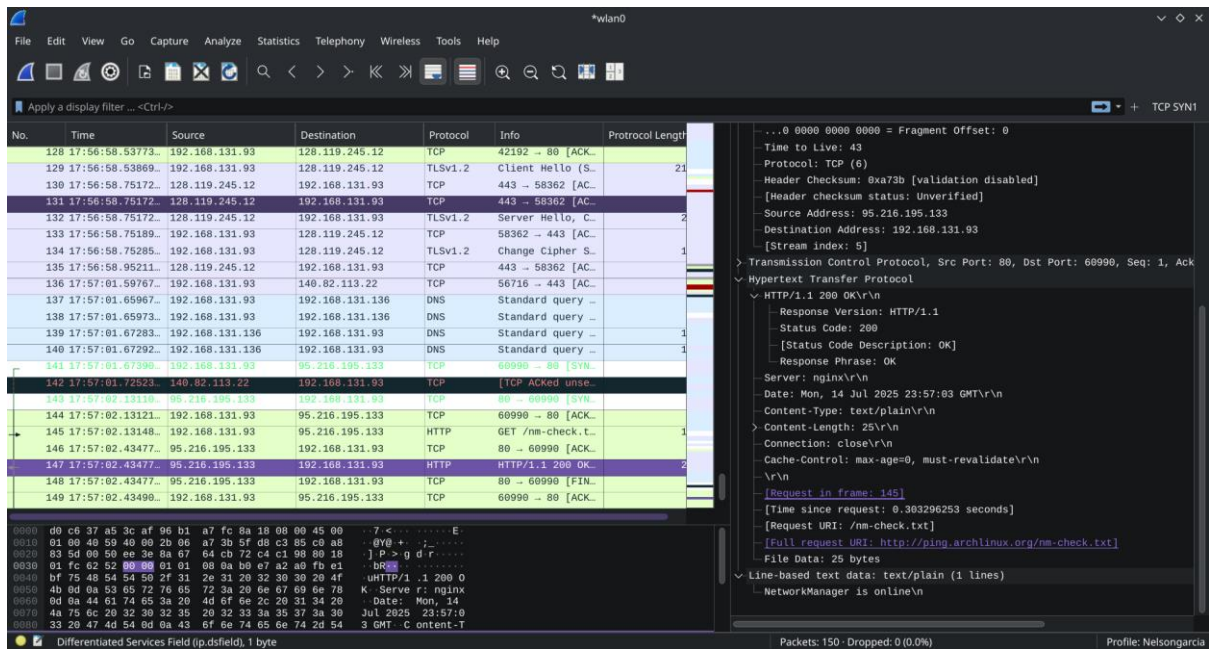
3.





1.3 Análisis de paquetes:

3.



a. ¿Qué versión de HTTP está ejecutando su navegador?

R// 1.1

b. ¿Qué versión de HTTP está ejecutando el servidor?

R// 1.1

c. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?

R// No lo menciona.

d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?

R// 25 bytes.

e. En el caso que haya un problema de rendimiento mientras se descarga la página, ¿en que elementos de la red convendría “escuchar” los paquetes? ¿Es conveniente instalar Wireshark en el servidor? Justifique.

R// Si hay un problema de rendimiento al descargar la página, convendría “escuchar” en el punto más cercano al cliente, como su propia computadora o el router de salida de la red local. Esto permite observar si el problema está en la conexión del cliente, en la entrega del contenido, o en la latencia de la red. No es conveniente instalar Wireshark en el servidor porque:

- El problema podría estar fuera del servidor (en la red intermedia o en el cliente).
- Monitorear desde el servidor solo mostrará el tráfico que llega o sale del servidor, y no revelará problemas de tránsito o recepción del cliente.
- Además, puede afectar la seguridad o el rendimiento del servidor.

Discusión/Comentarios:

El laboratorio me pareció interesante, la verdad creo que nunca había utilizado algún software que viera el tráfico en la red o algo parecido. Al momento de trabajar en la parte 1.2 tuve problemas porque me salía un pop-up diciendo que Wireshark no podía acceder al archivo .pgcap para guardar los paquetes de la captura, tuve que darle acceso a Wireshark con unos comandos en la terminal (`sudo setcap 'CAP_NET_RAW,CAP_NET_ADMIN+eip' /usr/bin/dumpcap`) para que pudiera realizar el guardado de los paquetes correctamente. Luego de eso ya no tuve problemas, más que todo costó en la parte 1.3 encontrar el protocolo HTTP en Wireshark, si tuve que probar varias veces hasta que ya apareció, terminé utilizando otro navegador al que uso normalmente para no tener que borrar la caché y perder datos como mis sesiones en diferentes sitios web. Me gustó la modalidad guiada del laboratorio, ya que, pues seguramente muchos no conocen cómo utilizar estas herramientas y es bueno para familiarizarse con lo demás que haremos en el curso.

Conclusiones:

- Wireshark es una herramienta para el análisis de redes, que permite visualizar y estudiar el tráfico de datos en tiempo real. Este laboratorio facilitó la familiarización con su entorno, funciones de personalización y captura de paquetes.
- La identificación y solución de problemas durante la práctica reforzó el aprendizaje autónomo. Enfrentar inconvenientes como la falta de permisos o la ausencia del tráfico HTTP ayudó a desarrollar habilidades de troubleshooting fundamentales para el trabajo con redes.
- Finalmente, la modalidad guiada del laboratorio fue clave para introducirse en el análisis de paquetes. Permitió conocer funciones básicas y avanzadas de Wireshark, sentando bases sólidas para futuras prácticas más complejas dentro del curso.

Bibliografía:

Leonardo, J. (2024, 9 enero). Comando ifconfig de Linux. EXTASSIS NETwork Tutoriales. <https://extassisnetwork.com/tutoriales/comando-ifconfig-de-linux/>