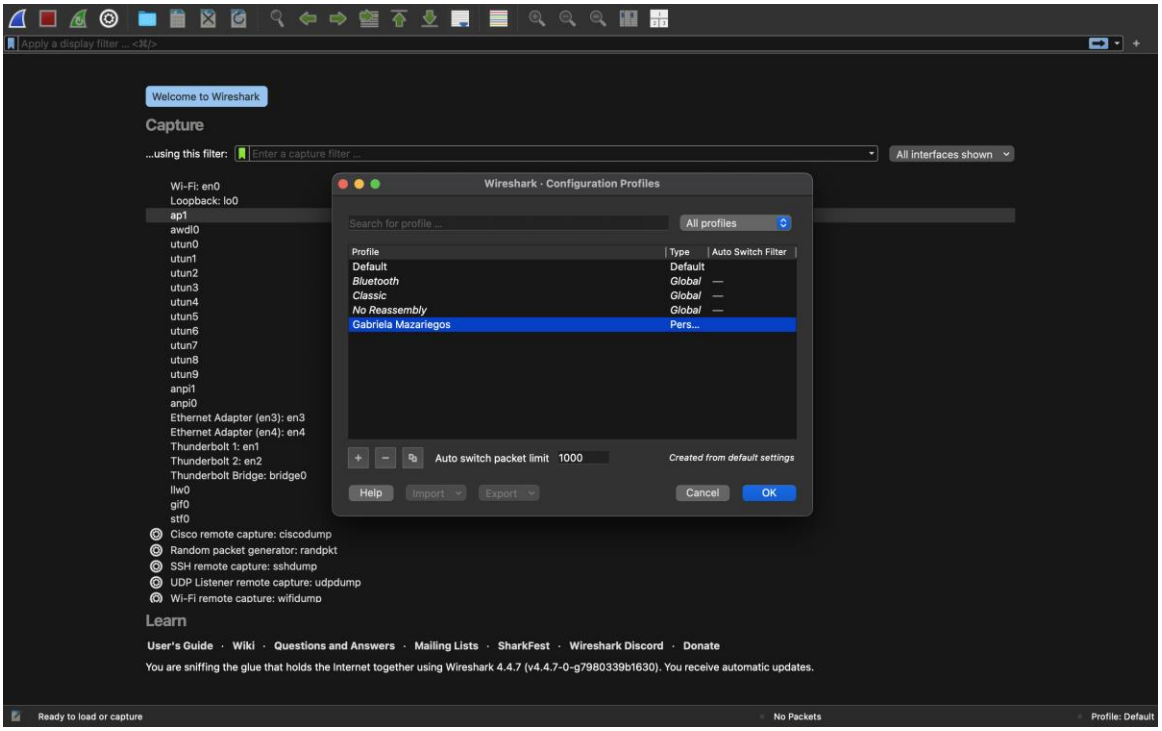
Laboratorio 1 – Individual

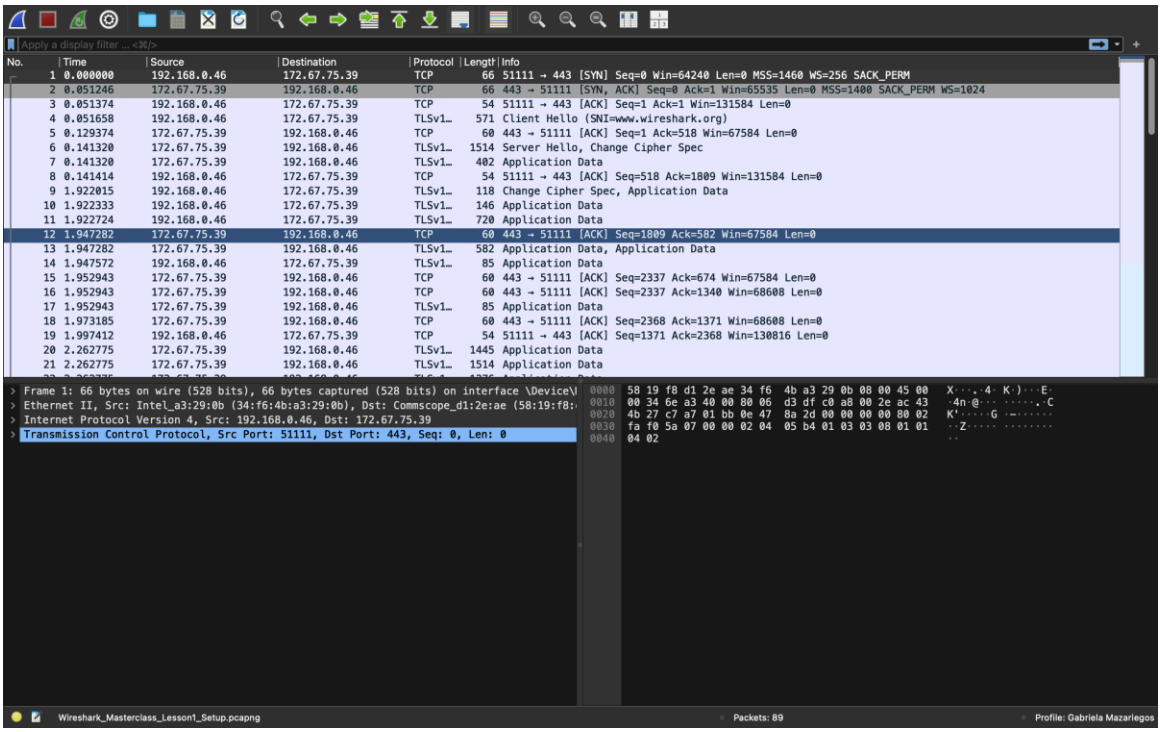
Nancy Mazariegos – 22513

1.1 Personalización del entorno

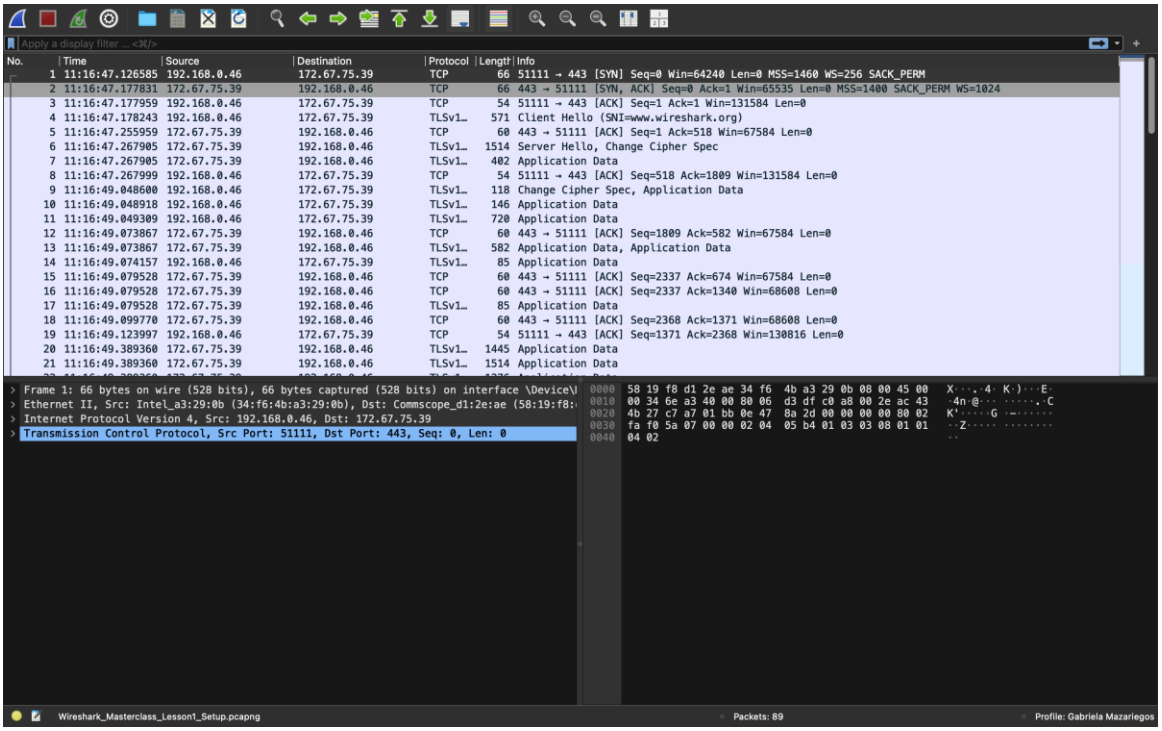
- Creación de usuario:



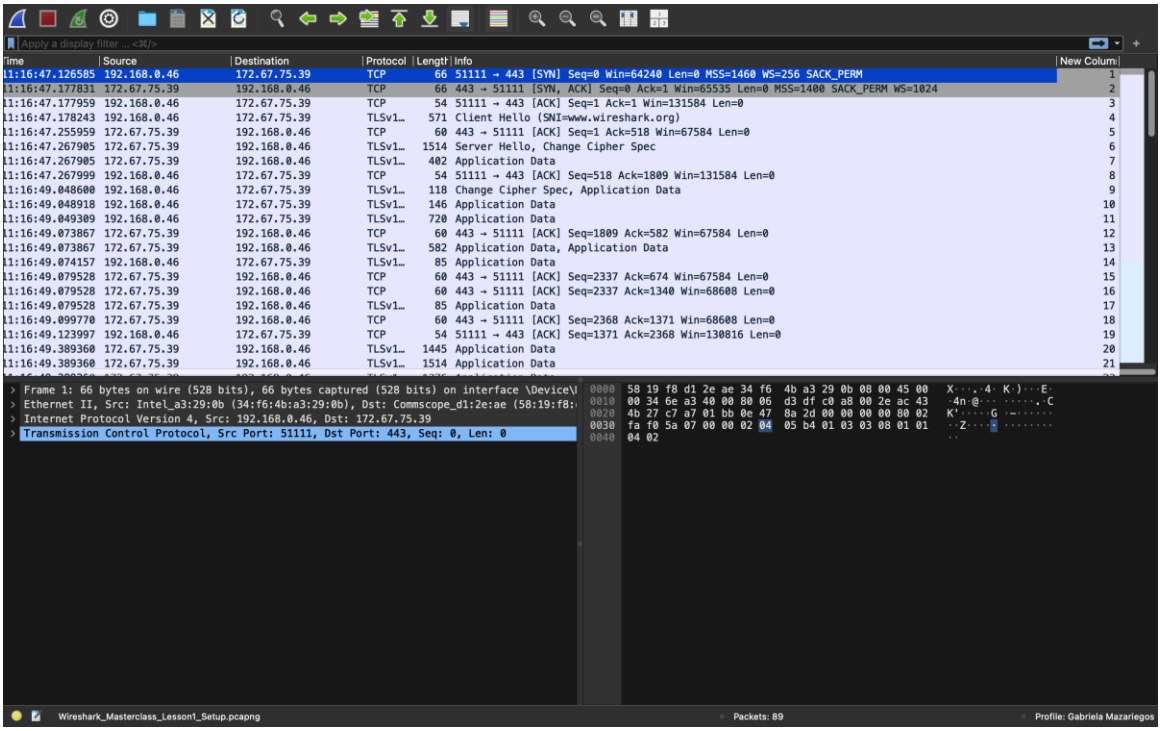
- Abrir archivo descargado:



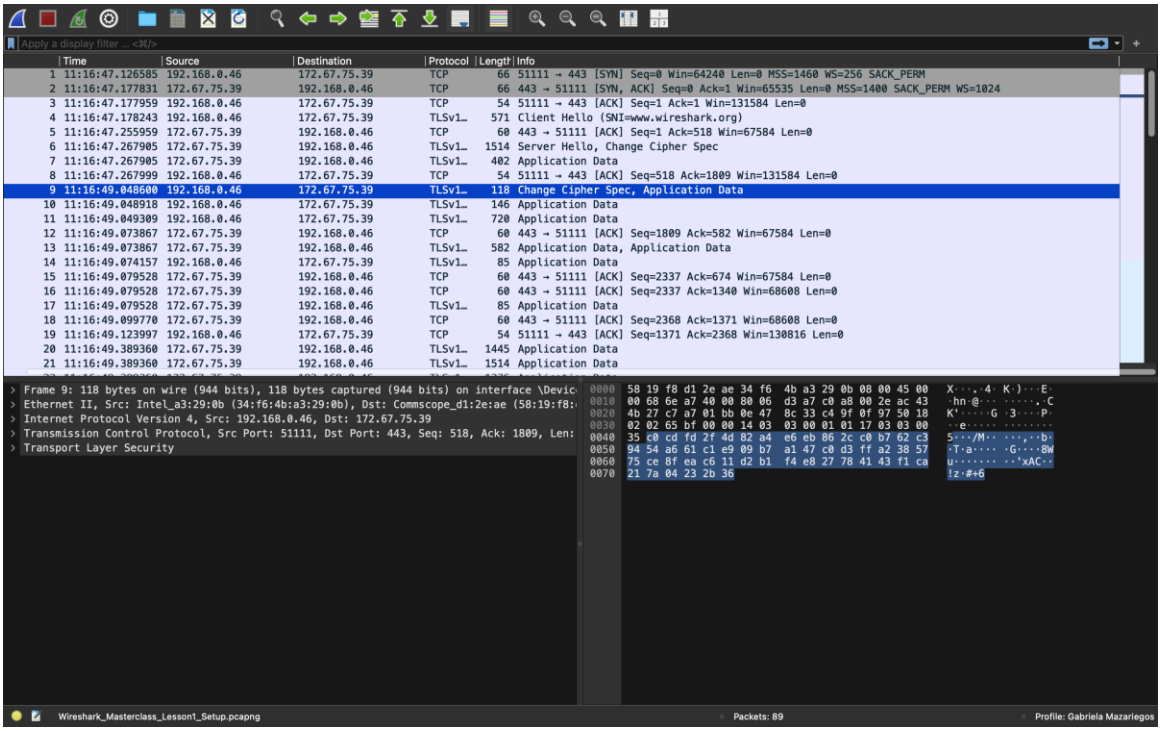
- Formato Time of Day:



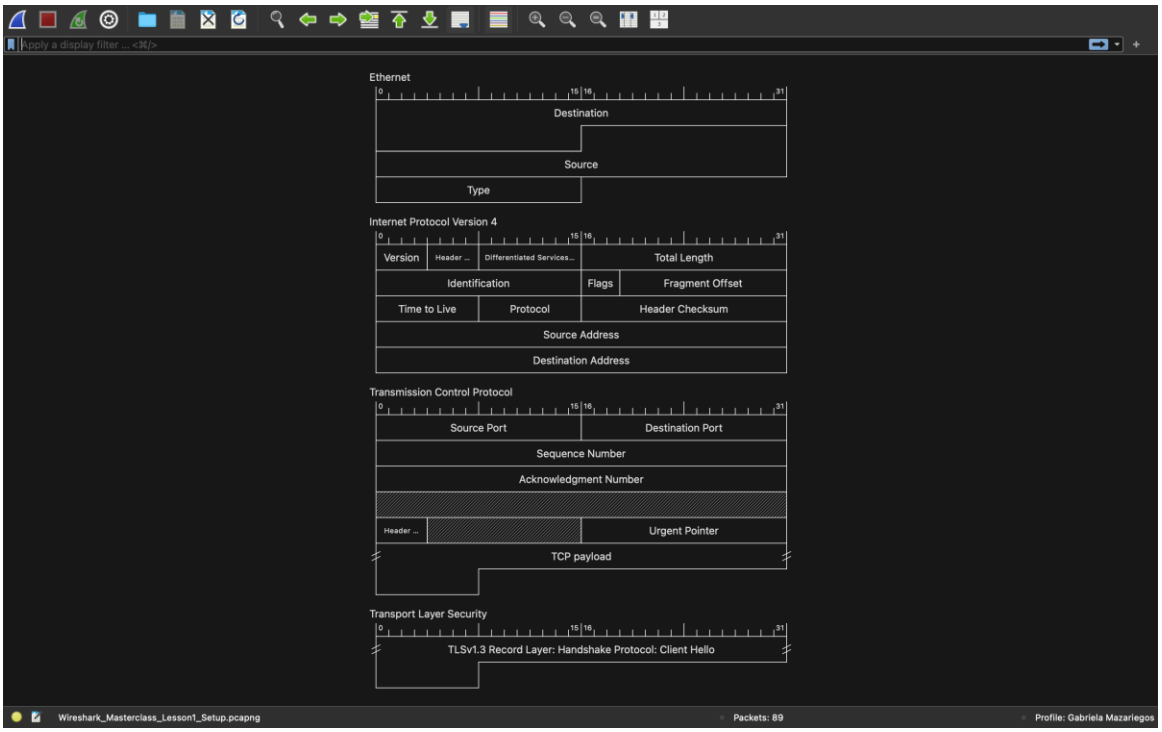
- Agregar columna:



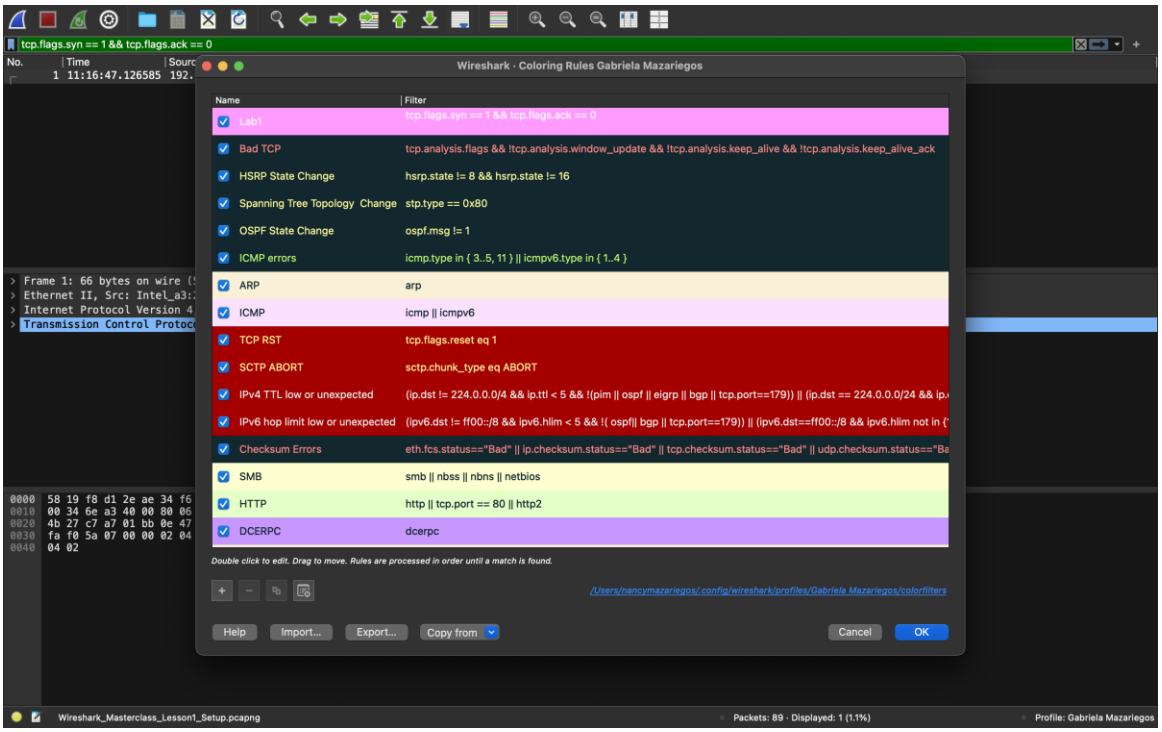
- Eliminar/ocultar columna:



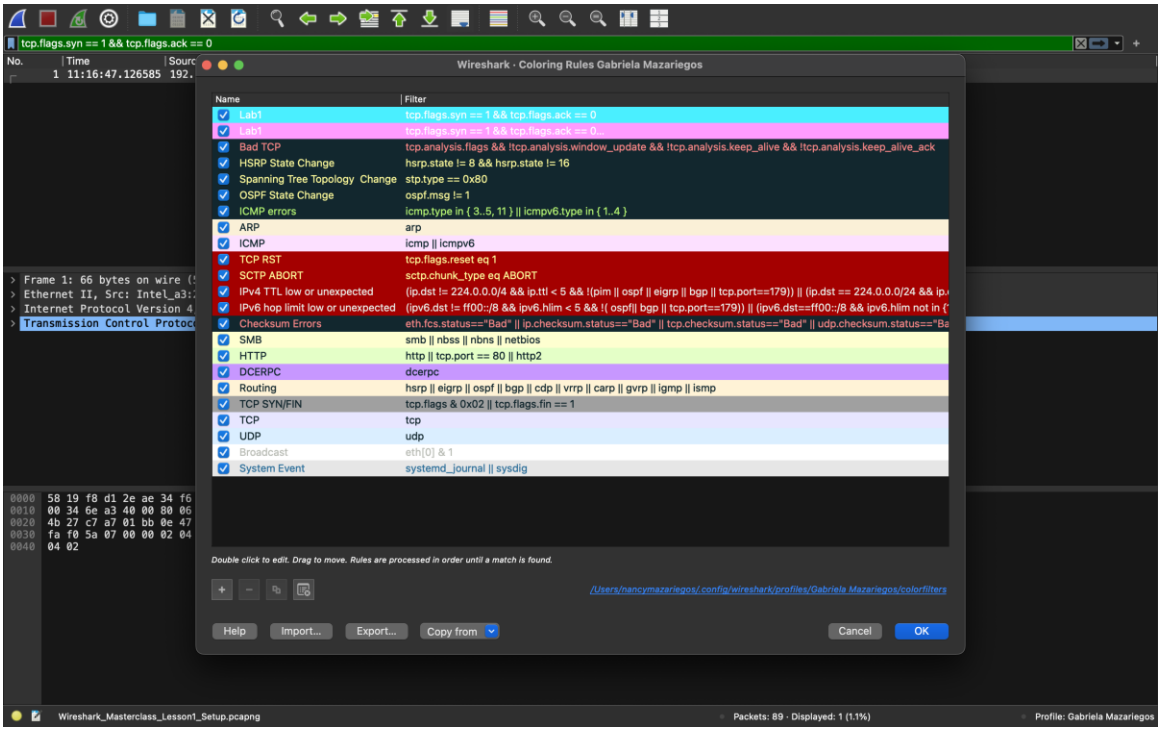
- Esquema de paneles aplicado:



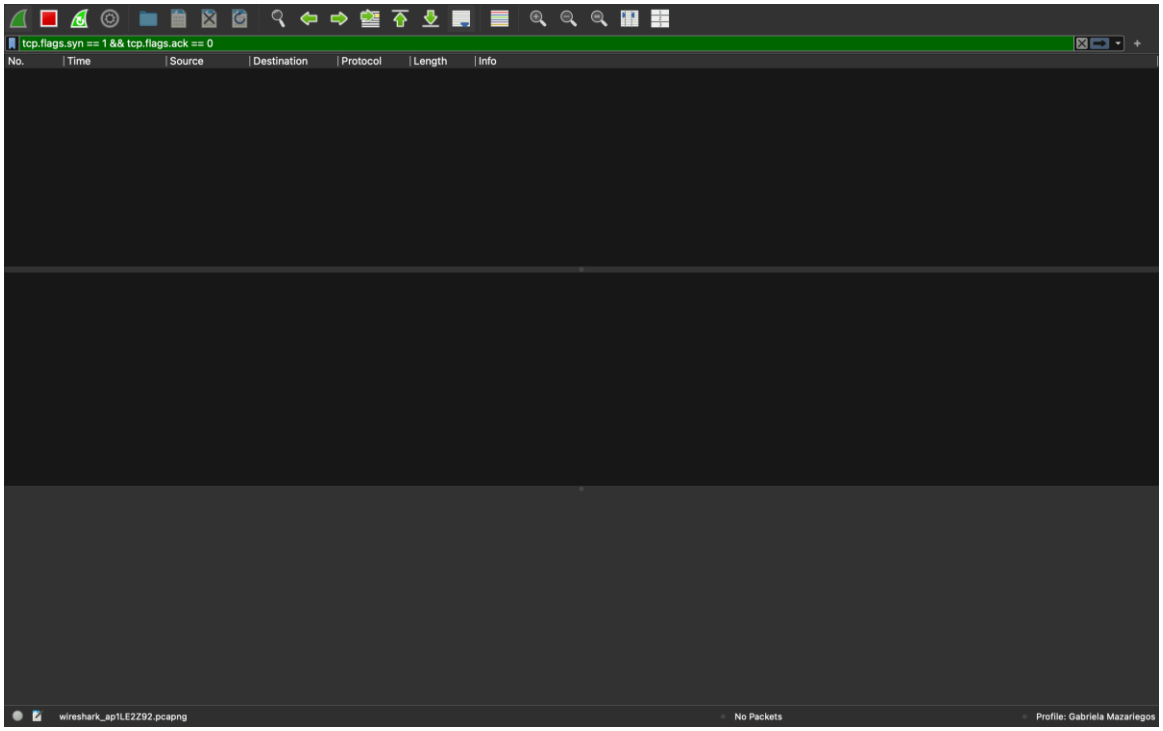
- Regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia:



- Botón que aplica un filtro para paquetes TCP con la bandera SYN igual a 1:

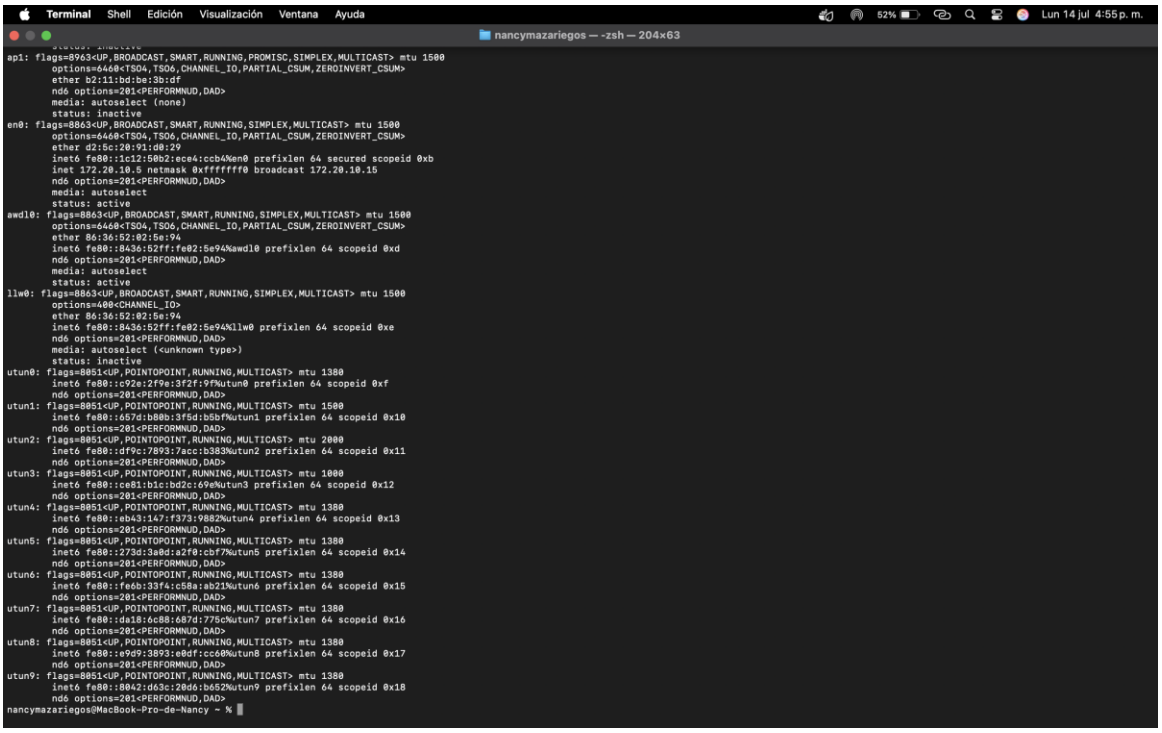


- Oculte las interfaces virtuales (en caso aplique: capture -> options):



1.2 Configuración de la captura de paquetes

- Abra una terminal y ejecute el comando ifconfig/ipconfig (dependiendo de su OS). Detalle y explique lo observado, investigue (i.e.: 'man ifconfig', documentación) de ser necesario.



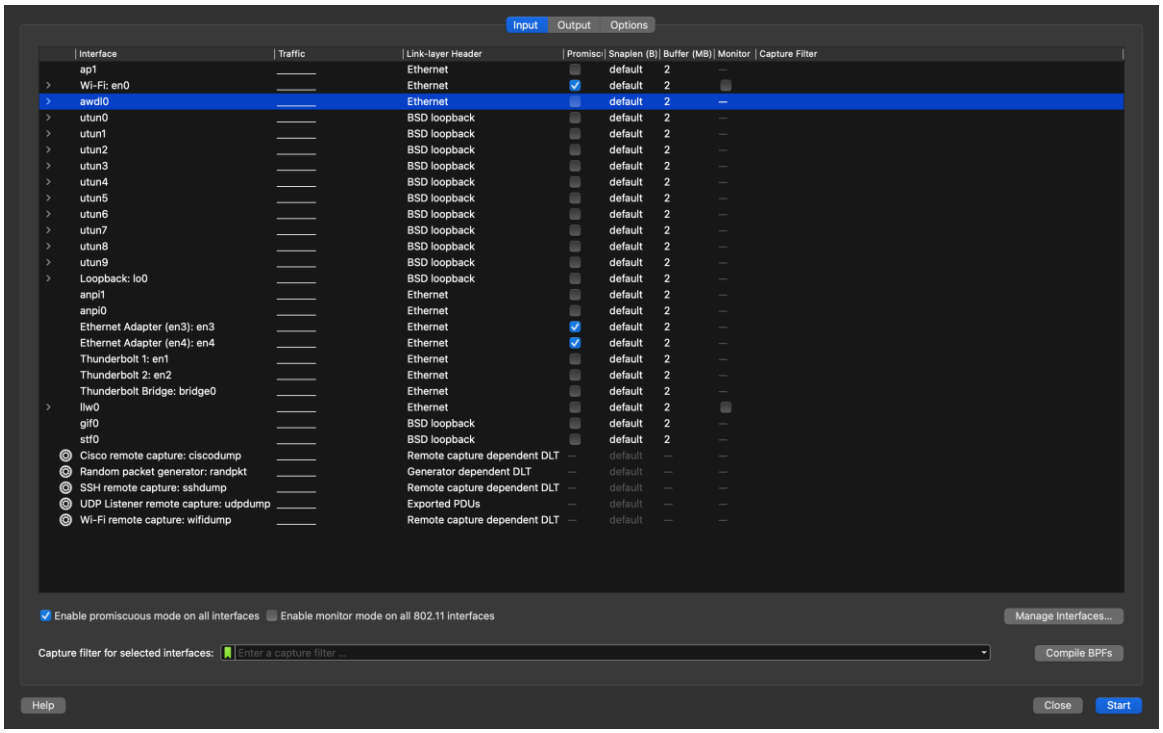
En la terminal se pudo ver lo siquiente

  - Loopback: Es una interfaz virtual usada para que la computadora se comunique consigo misma. Tiene la dirección `127.0.0.1` y siempre está activa.
  - Interfaz principal activa (Wi-Fi): Es la interfaz que está conectada a Internet. Tiene una dirección IP local `172.20.10.5`, está activa y es de tipo Wi-Fi. También se muestra su dirección MAC.
  - awdl0 y llw0: Son interfaces relacionadas con funciones de Apple como AirDrop. Aunque están activas y tienen dirección IPv6, no se usan para tráfico web común.
  - utun0 a utun9: Son interfaces virtuales utilizadas para túneles o conexiones VPN. Están activas pero no tienen dirección IP IPv4, por lo que no se usan para navegación normal.
  - anpi0, anpi1, en1, en2, en3, en4, bridge0: Son interfaces físicas o virtuales que no están activas. No tienen dirección IP y no están en uso actualmente.

  Básicamente, la interfaz que se está usando para la conexión a Internet es `en0`, ya que tiene una IP asignada, está activa y tiene dirección MAC. Las demás interfaces como utunX, gif0, stf0, y anpiX no están activas o no se usan para tráfico regular, por lo que pueden ignorarse o

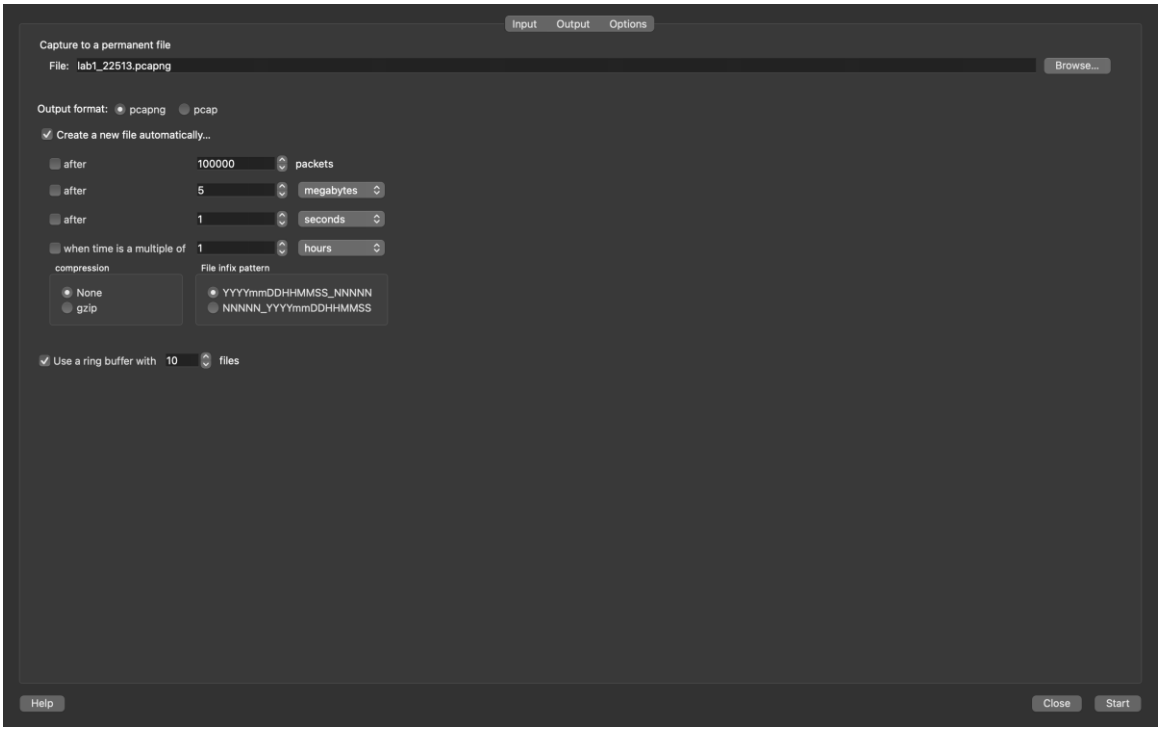
desactivarse en Wireshark.

- Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.



- Realice una captura de paquetes con la interfaz de Ethernet o WiFi con una configuración de ring buffer, con un tamaño de 5 MB por archivo y un número máximo de 10 archivos (puede hacerlo por medio de la interfaz de usuario o por medio de comandos) Genere tráfico para que los archivos se creen. Defina el nombre de los archivos de la siguiente forma: lab1_carnet.pgcap (options ->

capture -> output):

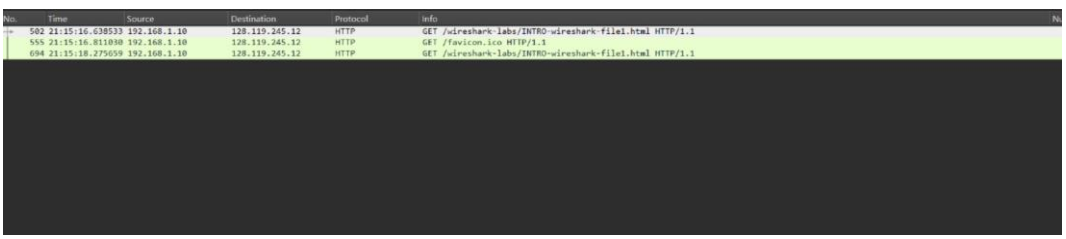


1.3 Análisis de paquetes

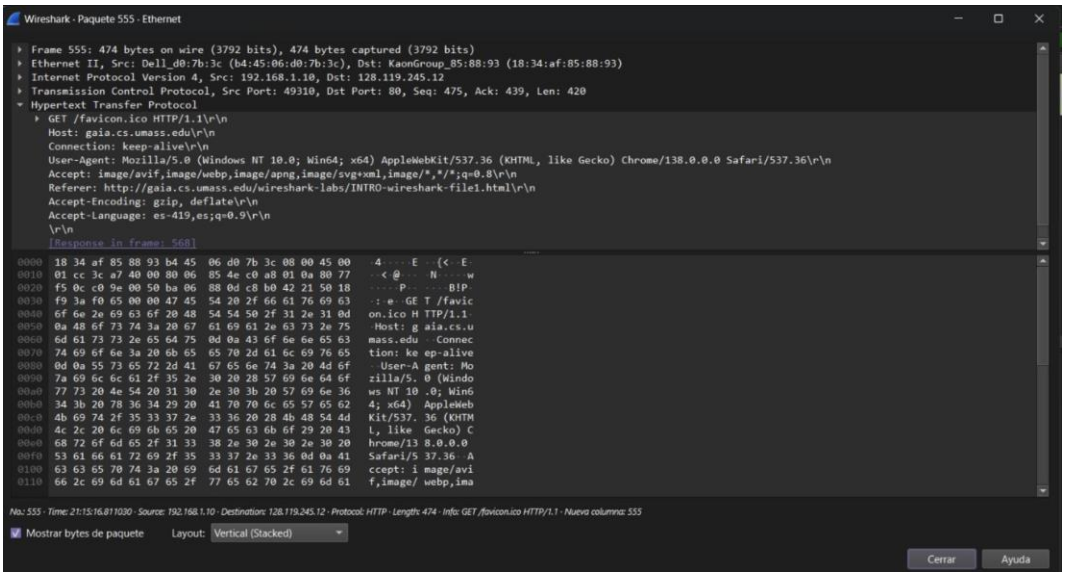
- Abra su navegador, inicie una captura de paquetes en Wireshark (sin filtro) en la interfaz y acceda a la siguiente direccion: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

- Detenga la captura de paquetes (si desea realizar una nueva captura de la página deberá borrar el caché de su navegador, de lo contrario no se realizará la captura del protocolo HTTP).

- Responda las siguientes preguntas:
    - a. ¿Qué versión de HTTP está ejecutando su navegador?
      La versión que utiliza el navegador es HTTP/1.1.
    - b. ¿Qué versión de HTTP está ejecutando el servidor?
      El servidor también responde con HTTP/1.1.



- c. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?
  El navegador prioriza el español, pero también acepta inglés si no hay versiones en español.



- d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
  Fueron 85 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
  Conviene escuchar en el cliente, en el router y, si es posible, en el servidor.
  Instalar Wireshark en el servidor puede ser útil para analizar si hay errores o lentitud en las respuestas, pero solo si se tiene permiso y no afecta su rendimiento. Si el servidor fuese crítico, es mejor analizar desde otro punto de la red.

Discusión

En esta actividad usamos Wireshark para capturar paquetes de red. Primero, aplicamos filtros y colores para reconocer fácilmente ciertos paquetes, como los que tienen la bandera SYN. Esto nos ayudó a entender mejor el tipo de tráfico que pasa por la red.

Después, configuramos la captura con una opción llamada ring buffer, que guarda archivos de 5 MB y hasta 10 archivos en total. Elegimos la interfaz correcta (en0) para asegurar que se capturara el tráfico real. Luego, generamos tráfico desde el navegador para ver cómo se hacen las solicitudes HTTP y analizamos un paquete paso a paso.

Comentarios

- Fue interesante descubrir cuántas interfaces virtuales existen en el sistema y cómo afectan la captura si no se filtran correctamente.
- Configurar el ring buffer fue algo complejo a pesar de que se hace desde la interfaz gráfica, pero esta permite un control útil sobre el almacenamiento.

Conclusiones

- Es importante elegir bien la interfaz para capturar solo el tráfico que sirve porque si no se hace un desastre y no se logra entender bien.
- Los filtros y colores ayudan a identificar rápido los paquetes importantes.
- El ring buffer permite guardar muchas capturas sin llenar el espacio para solo utilizar lo que se considera necesario.

Referencias

- Wireshark User Guide: https://www.wireshark.org/docs/wsug_html_chunked/
- Manual de ifconfig en macOS: ejecutado con man ifconfig
- Documentación oficial del protocolo HTTP: https://developer.mozilla.org/en-US/docs/Web/HTTP