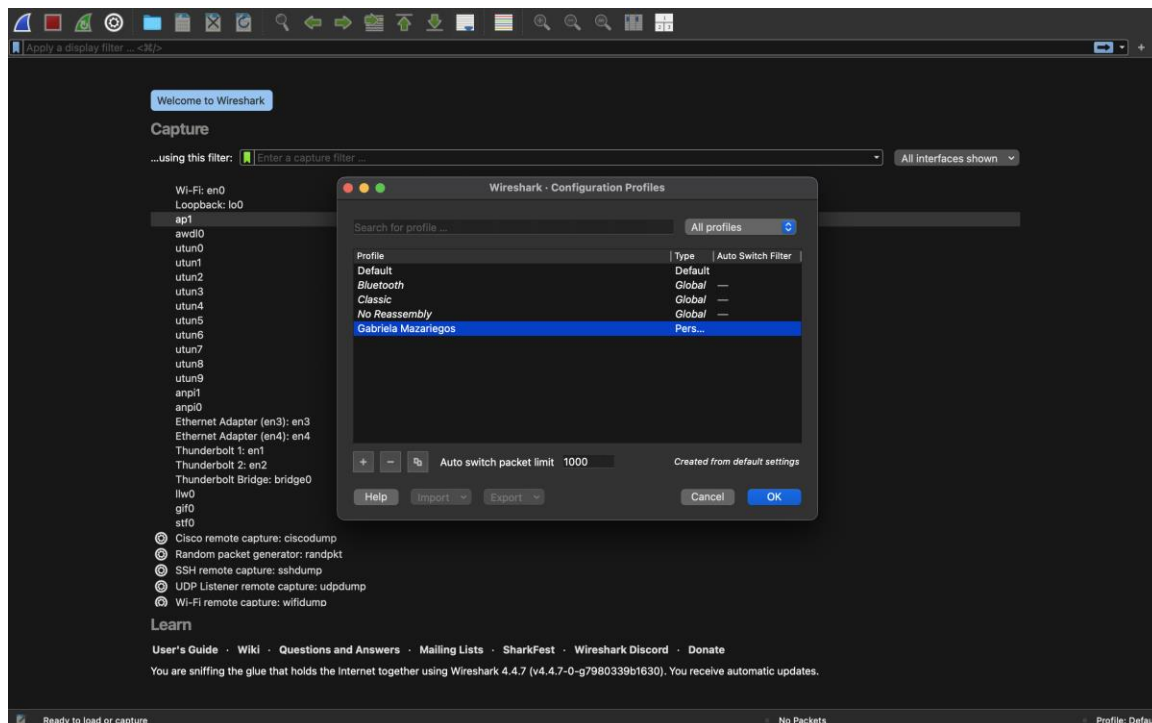




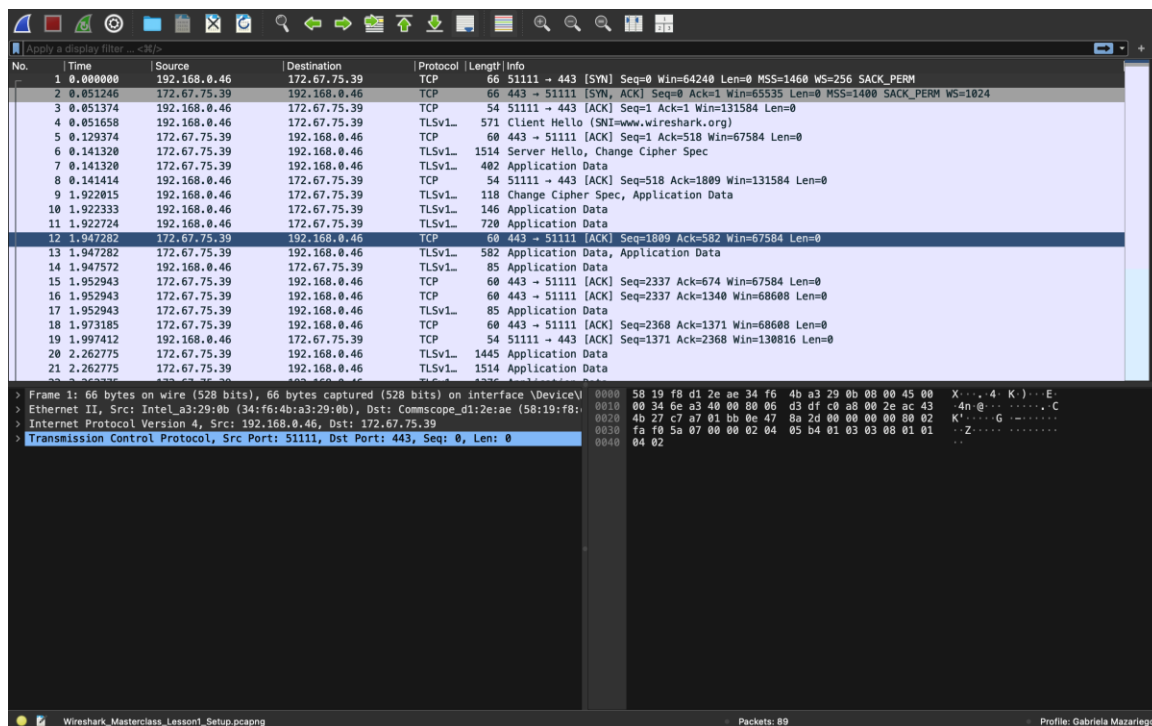
## Laboratorio 1 – Individual

## 1.1 Personalización del entorno

- Creación de usuario:



- Abrir archivo descargado:



- Formato Time of Day:

No.	Time	Source	Destination	Protocol	Length	Info
1	11:16:47.126585	192.168.0.46	172.67.75.39	TCP	66	51111 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	11:16:47.177831	192.168.0.46	172.67.75.39	TCP	66	443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=1024
3	11:16:47.177959	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
4	11:16:47.178243	192.168.0.46	172.67.75.39	TLSv1	571	Client Hello (SNI=www.wireshark.org)
5	11:16:47.255959	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=1 Ack=518 Win=67584 Len=0
6	11:16:47.267985	172.67.75.39	192.168.0.46	TLSv1	1514	Server Hello, Change Cipher Spec
7	11:16:47.267985	172.67.75.39	192.168.0.46	TLSv1	402	Application Data
8	11:16:47.267999	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=518 Ack=1809 Win=131584 Len=0
9	11:16:49.048600	192.168.0.46	172.67.75.39	TLSv1	118	Change Cipher Spec, Application Data
10	11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1	146	Application Data
11	11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1	720	Application Data
12	11:16:49.073867	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=1809 Ack=582 Win=67584 Len=0
13	11:16:49.073867	172.67.75.39	192.168.0.46	TLSv1	582	Application Data, Application Data
14	11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1	85	Application Data
15	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=2337 Ack=674 Win=67584 Len=0
16	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=2337 Ack=1340 Win=68608 Len=0
17	11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1	85	Application Data
18	11:16:49.099770	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=2368 Ack=1371 Win=68608 Len=0
19	11:16:49.123997	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=1371 Ack=2368 Win=130816 Len=0
20	11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1	1445	Application Data
21	11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1	1514	Application Data

- Agregar columna:

No.	Time	Source	Destination	Protocol	Length	Info	New Column
1	11:16:47.126585	192.168.0.46	172.67.75.39	TCP	66	51111 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	1
2	11:16:47.177831	192.168.0.46	172.67.75.39	TCP	66	443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=1024	2
3	11:16:47.177959	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0	3
4	11:16:47.178243	192.168.0.46	172.67.75.39	TLSv1	571	Client Hello (SNI=www.wireshark.org)	4
5	11:16:47.255959	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=1 Ack=518 Win=67584 Len=0	5
6	11:16:47.267985	172.67.75.39	192.168.0.46	TLSv1	1514	Server Hello, Change Cipher Spec	6
7	11:16:47.267985	172.67.75.39	192.168.0.46	TLSv1	402	Application Data	7
8	11:16:47.267999	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=518 Ack=1809 Win=131584 Len=0	8
9	11:16:49.048600	192.168.0.46	172.67.75.39	TLSv1	118	Change Cipher Spec, Application Data	9
10	11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1	146	Application Data	10
11	11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1	720	Application Data	11
12	11:16:49.073867	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=1809 Ack=582 Win=67584 Len=0	12
13	11:16:49.073867	172.67.75.39	192.168.0.46	TLSv1	582	Application Data, Application Data	13
14	11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1	85	Application Data	14
15	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=2337 Ack=674 Win=67584 Len=0	15
16	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=2337 Ack=1340 Win=68608 Len=0	16
17	11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1	85	Application Data	17
18	11:16:49.099770	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=2368 Ack=1371 Win=68608 Len=0	18
19	11:16:49.123997	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=1371 Ack=2368 Win=130816 Len=0	19
20	11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1	1445	Application Data	20
21	11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1	1514	Application Data	21

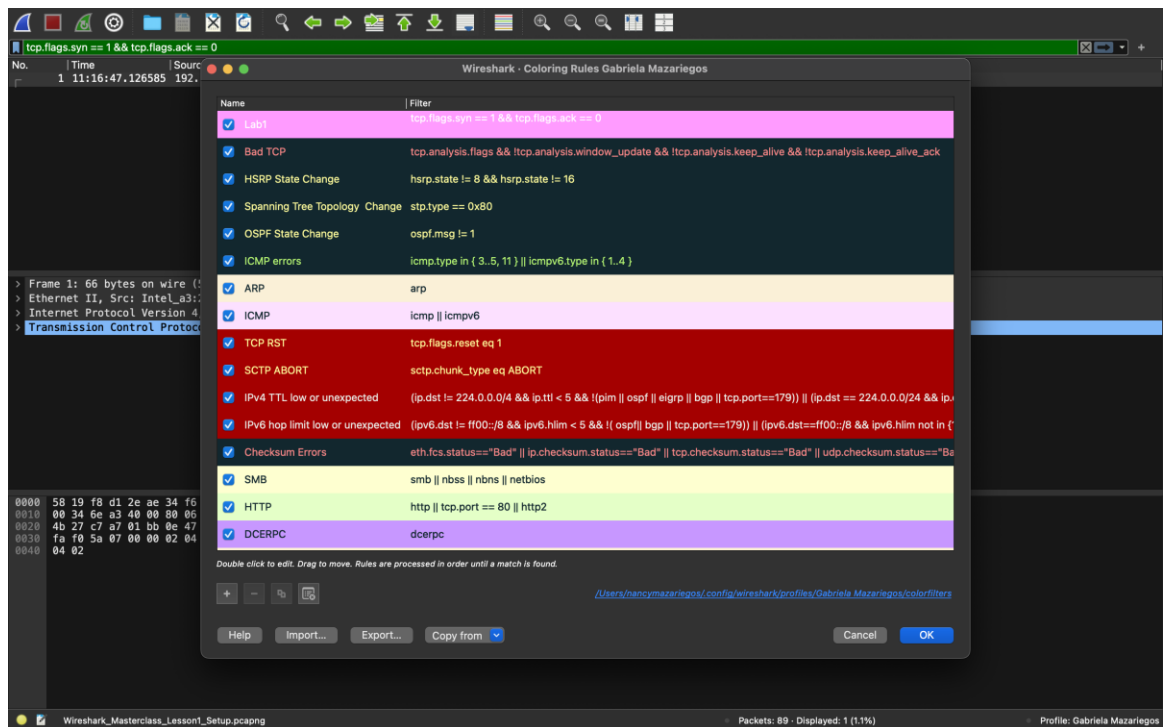
- Eliminar/ocultar columna:

The screenshot shows the Wireshark interface with a packet capture list on the left and a detailed view of a selected packet (Frame 9) on the right. The packet list shows a series of TCP and TLSv1.3 packets between 192.168.0.46 and 172.67.75.39. The detailed view shows the structure of the selected packet, which is a TLSv1.3 Change Cipher Spec, Application Data. The packet is 118 bytes long. The detailed view shows the packet structure, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and the TLSv1.3 Record Layer. The packet is captured on interface eth0, and the source is 192.168.0.46, destination is 172.67.75.39. The packet is a TCP Reset (RST) with sequence number 51111 and port 443.

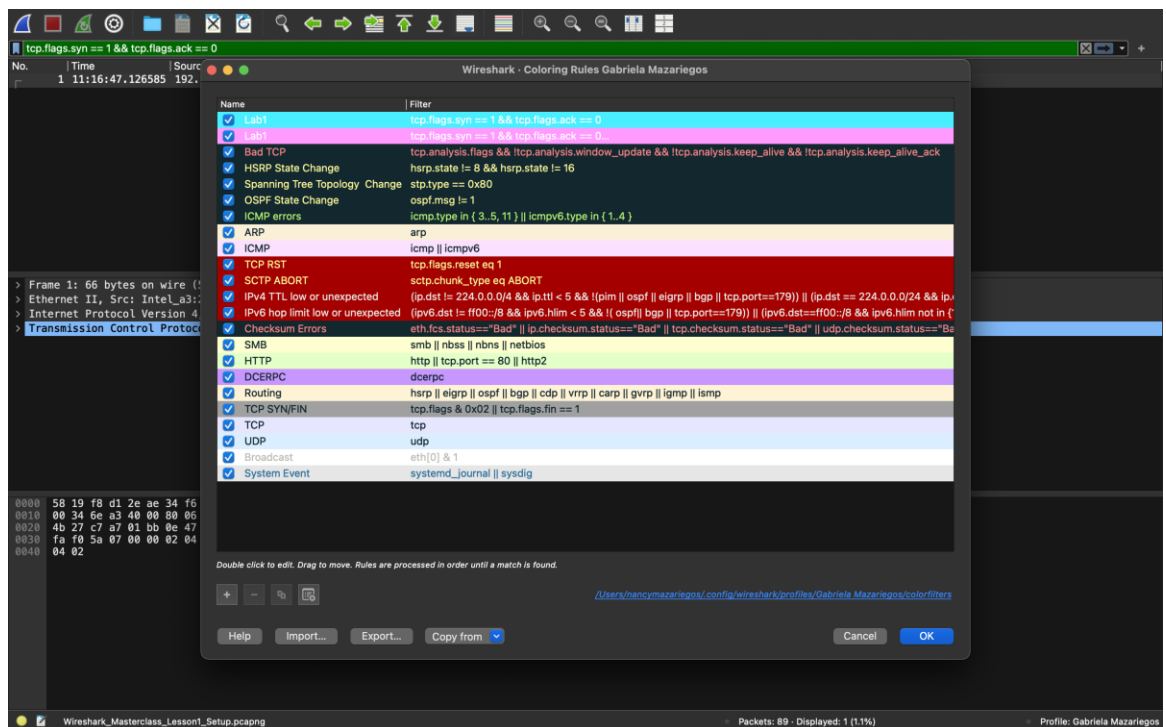
- Esquema de paneles aplicado:

The screenshot shows the Wireshark interface with a packet capture list on the left and a packet diagram on the right. The packet list shows a series of TCP and TLSv1.3 packets between 192.168.0.46 and 172.67.75.39. The packet diagram shows the structure of the selected packet, which is a TLSv1.3 Record Layer. The diagram shows the packet structure, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and the TLSv1.3 Record Layer. The packet is captured on interface eth0, and the source is 192.168.0.46, destination is 172.67.75.39. The packet is a TCP Reset (RST) with sequence number 51111 and port 443.

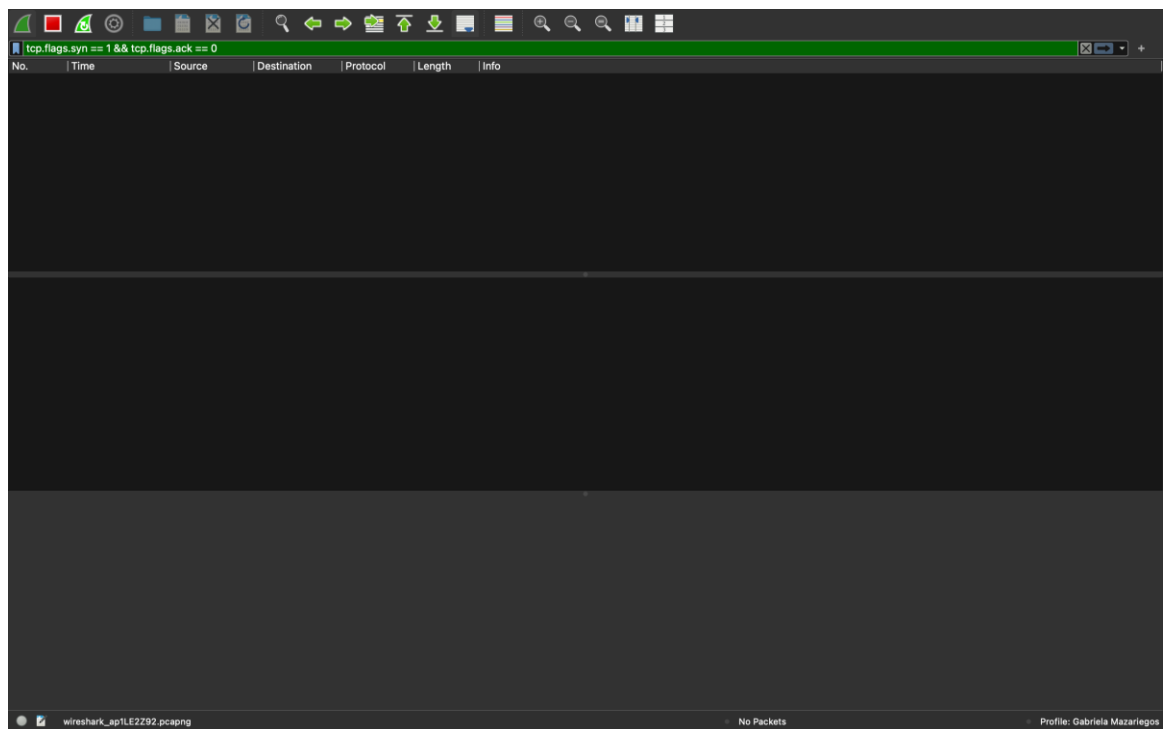
- Regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia:



- 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.

```

nancymazariegos ~ - ssh - 204x63
nancymazariegos@MacBook-Pro-de-Nancy: ~ % ifconfig

ap1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=640<TSO4,TSO6,CHANNEL_ID,PARTIAL_CSUM,ZEROINVERT_CSUM>
    ether 02:11:bd:b6:3b:df
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (none)
    status: inactive

en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=640<TSO4,TSO6,CHANNEL_ID,PARTIAL_CSUM,ZEROINVERT_CSUM>
    ether d2:5c:20:91:d0:29
    inet6 fe80::1c12:58b2:ec64:c0b8%en0 prefixlen 64 scoped 0xb
    inet 172.20.10.5 netmask 0xffffff00 broadcast 172.20.10.15
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

awdl0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=640<TSO4,TSO6,CHANNEL_ID,PARTIAL_CSUM,ZEROINVERT_CSUM>
    ether 86:36:1521:a2:1a:94
    inet6 fe80::8436:52ff:fe82:5e94%awdl0 prefixlen 64 scoped 0xd
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=408<CHANNEL_ID>
    ether 86:36:1521:a2:1a:94
    inet6 fe80::8436:52ff:fe82:5e94%llw0 prefixlen 64 scoped 0xe
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (<unknown type>)
    status: inactive

utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::c02e:2f9e:3f2f:9f%utun0 prefixlen 64 scoped 0xf
    nd6 options=201<PERFORMNUD,DAD>

utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::657d:b8b0:3f5d:b55f%utun1 prefixlen 64 scoped 0x10
    nd6 options=201<PERFORMNUD,DAD>

utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::df9c:7893:7acc:b383%utun2 prefixlen 64 scoped 0x11
    nd6 options=201<PERFORMNUD,DAD>

utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
    inet6 fe80::ce81:b1c:bd2c:69e%utun3 prefixlen 64 scoped 0x12
    nd6 options=201<PERFORMNUD,DAD>

utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
    inet6 fe80::0b43:147:f373:9882%utun4 prefixlen 64 scoped 0x13
    nd6 options=201<PERFORMNUD,DAD>

utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
    inet6 fe80::273d:3a8d:a2f0:cbf7%utun5 prefixlen 64 scoped 0x14
    nd6 options=201<PERFORMNUD,DAD>

utun6: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
    inet6 fe80::f6ab:33fa:c58a:ab21%utun6 prefixlen 64 scoped 0x15
    nd6 options=201<PERFORMNUD,DAD>

utun7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
    inet6 fe80::da18:6c8b:a5d:77%utun7 prefixlen 64 scoped 0x16
    nd6 options=201<PERFORMNUD,DAD>

utun8: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
    inet6 fe80::e6f9:3893:e6ff:cc0b%utun8 prefixlen 64 scoped 0x17
    nd6 options=201<PERFORMNUD,DAD>

utun9: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
    inet6 fe80::8042:d63b:2066:b452%utun9 prefixlen 64 scoped 0x18
    nd6 options=201<PERFORMNUD,DAD>

nancymazariegos@MacBook-Pro-de-Nancy: ~ %

```

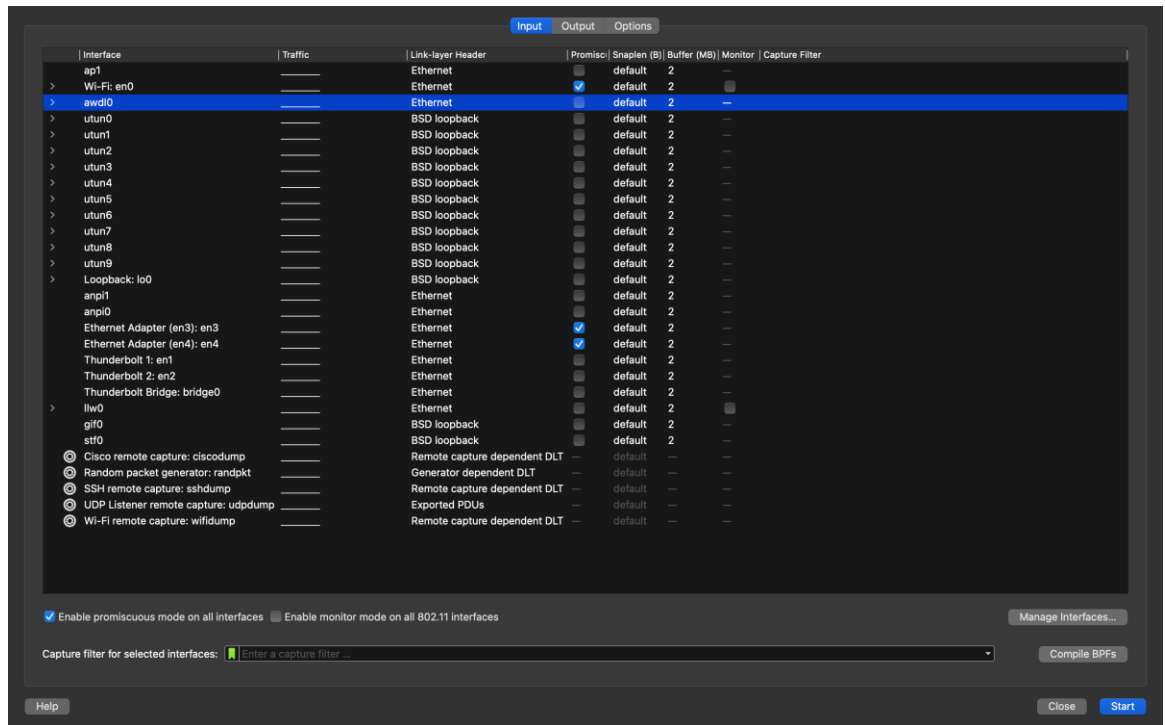
En la terminal se pudo ver lo siguiente

- 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.

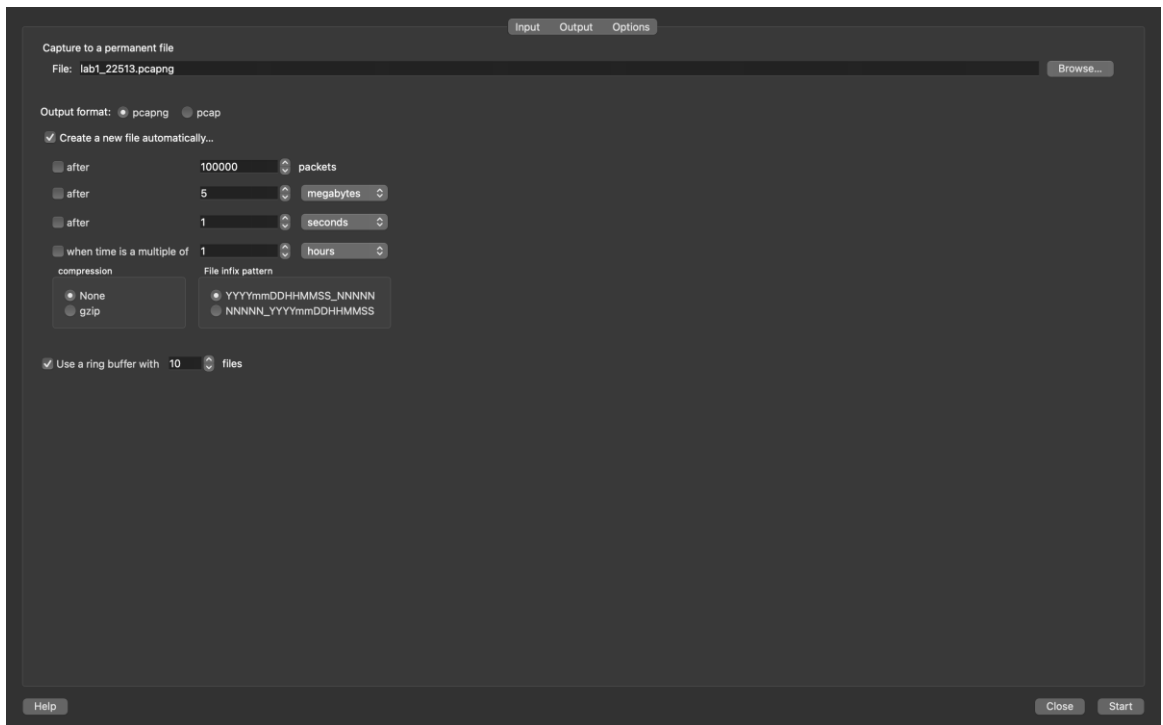
- Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.



- 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):



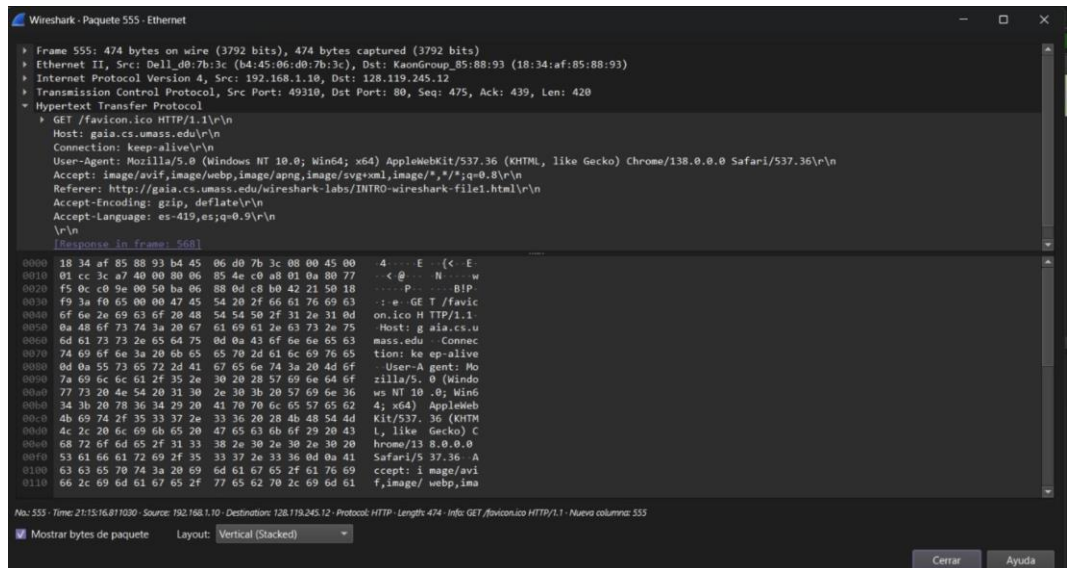
### 1.3 Análisis de paquetes

- 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.*

No.	Time	Source	Destination	Protocol	Info
502	21:15:16.638533	192.168.1.10	128.119.245.12	HTTP	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
515	21:15:16.811890	192.168.1.10	128.119.245.12	HTTP	GET /favicon.ico HTTP/1.1
694	21:15:18.275059	192.168.1.10	128.119.245.12	HTTP	GET /wireshark-labs/INTRO-wireshark-file1.html 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/](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>