Reporte

Nombre: Carlos Alberto Valladares Guerra

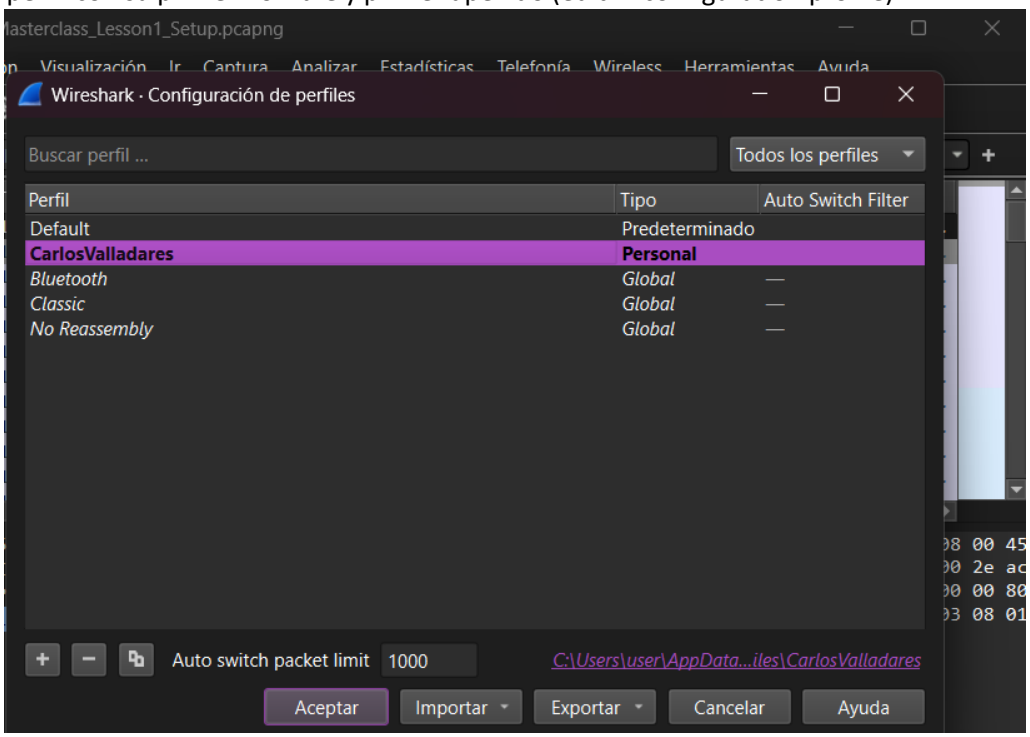
Carné: 221164

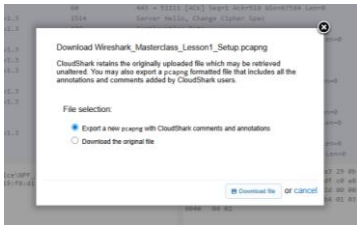
Segunda parte: Introducción a Wireshark

Se debe descargar e instalar el software de Wireshark. Es probable que para ejecutarlo pida permisos de administrador (sudo, click + run as admin, etc.).

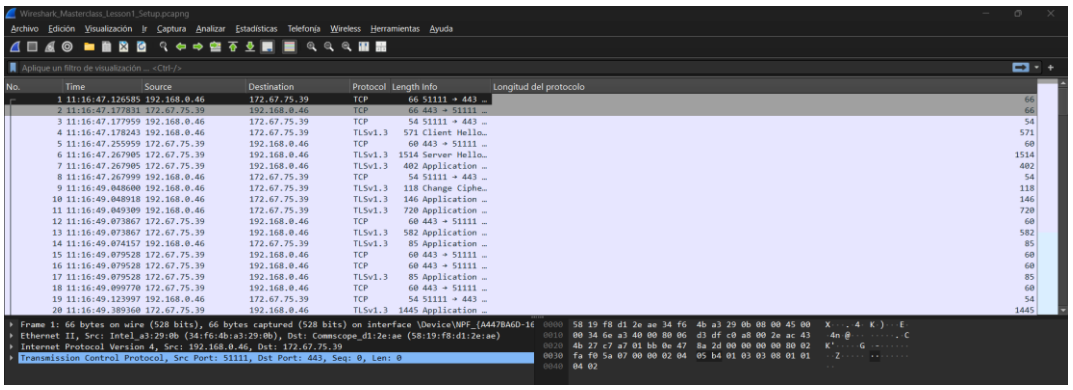
1.1 Personalización del entorno

En la primera parte se realizará la personalización del entorno de Wireshark, de modo que se adapte a nuestras preferencias de uso.

1. Inicie Wireshark
2. Cree un perfil con su primer nombre y primer apellido (edit -> configuration profile)
   a. 

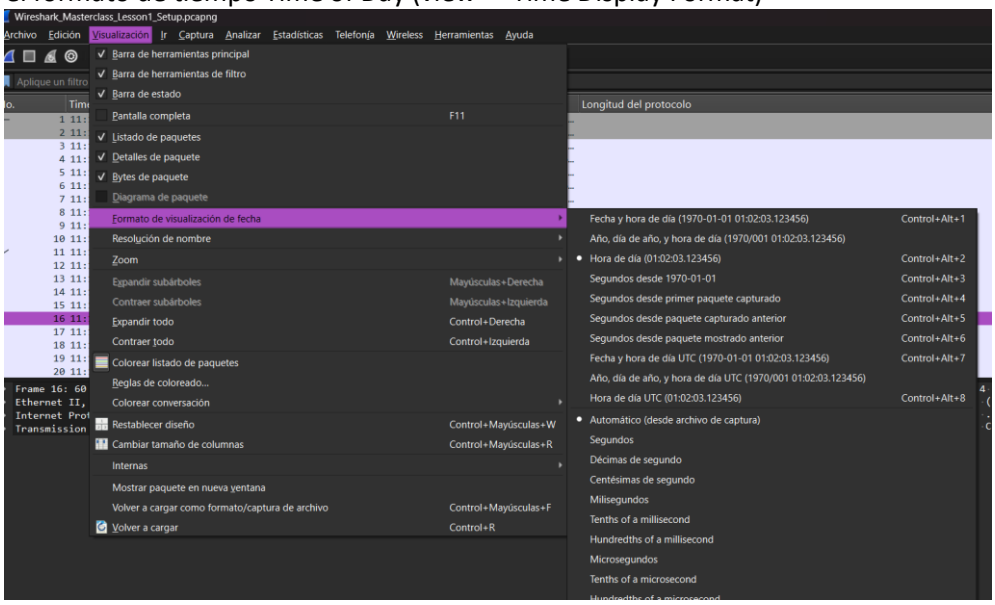
3. Descargue el archivo https://www.cloudshark.org/captures/e6fb36096dbb (Export -> Download)
   a. 
4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.

a.



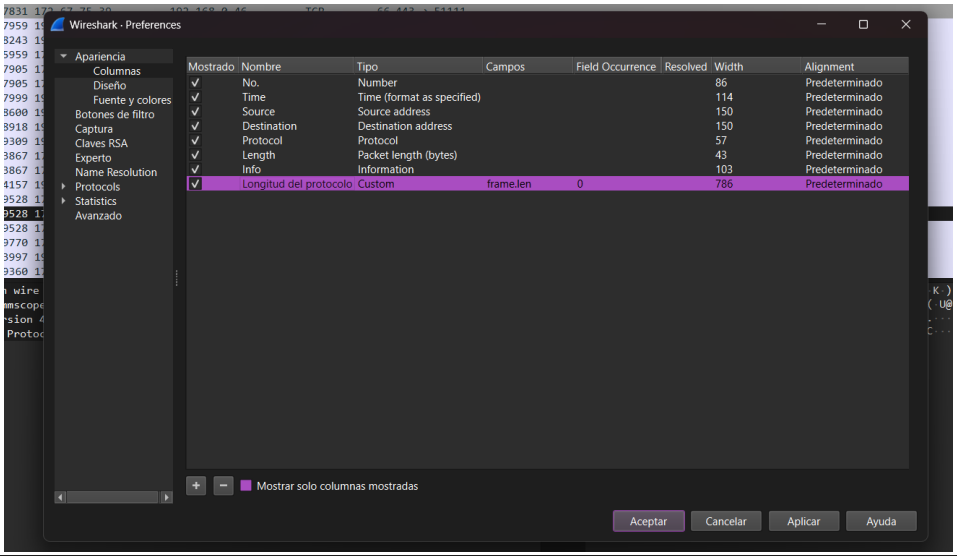
5. Aplique el formato de tiempo Time of Day (view -> Time Display Format)

a.



6. Agregue una columna con la longitud del protocolo (preferences -> column -> +)

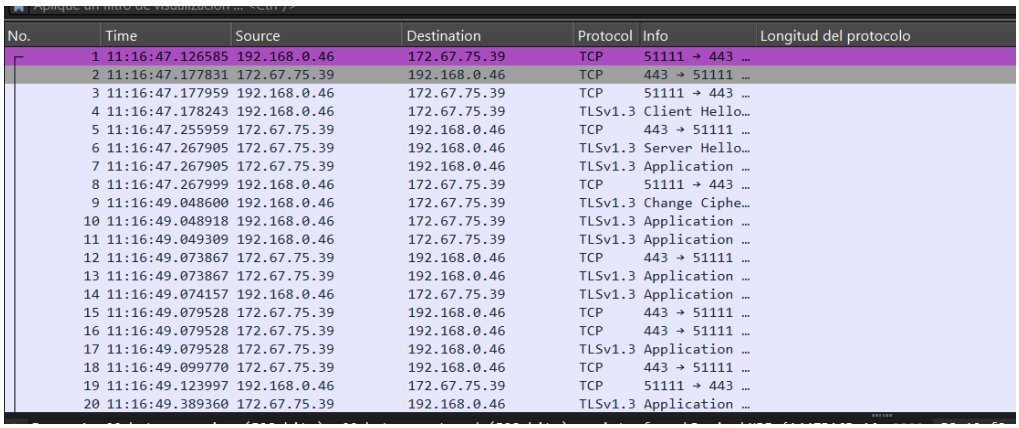
a.



No.	Time	Source	Destination	Protocol	Length Info	Longitud del protocolo
1	11:16:47.126585	192.168.0.46	172.67.75.39	TCP	66 51111 → 443 …	
2	11:16:47.177831	172.67.75.39	192.168.0.46	TCP	66 443 → 51111 …	
3	11:16:47.177959	192.168.0.46	172.67.75.39	TCP	54 51111 → 443 …	
4	11:16:47.178243	192.168.0.46	172.67.75.39	TLSv1.3	571 Client Hello…	
5	11:16:47.255959	172.67.75.39	192.168.0.46	TCP	60 443 → 51111 …	
6	11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	1514 Server Hello…	
7	11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	402 Application …	
8	11:16:47.267999	192.168.0.46	172.67.75.39	TCP	54 51111 → 443 …	
9	11:16:49.048600	192.168.0.46	172.67.75.39	TLSv1.3	118 Change Ciphe…	
10	11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1.3	146 Application …	
11	11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1.3	720 Application …	
12	11:16:49.073867	172.67.75.39	192.168.0.46	TCP	60 443 → 51111 …	
13	11:16:49.073867	172.67.75.39	192.168.0.46	TLSv1.3	582 Application …	
14	11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1.3	85 Application …	
15	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60 443 → 51111 …	
16	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60 443 → 51111 …	
17	11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1.3	85 Application …	
18	11:16:49.099770	172.67.75.39	192.168.0.46	TCP	60 443 → 51111 …	
19	11:16:49.123997	192.168.0.46	172.67.75.39	TCP	54 51111 → 443 …	
20	11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1.3	1445 Application …	

7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)

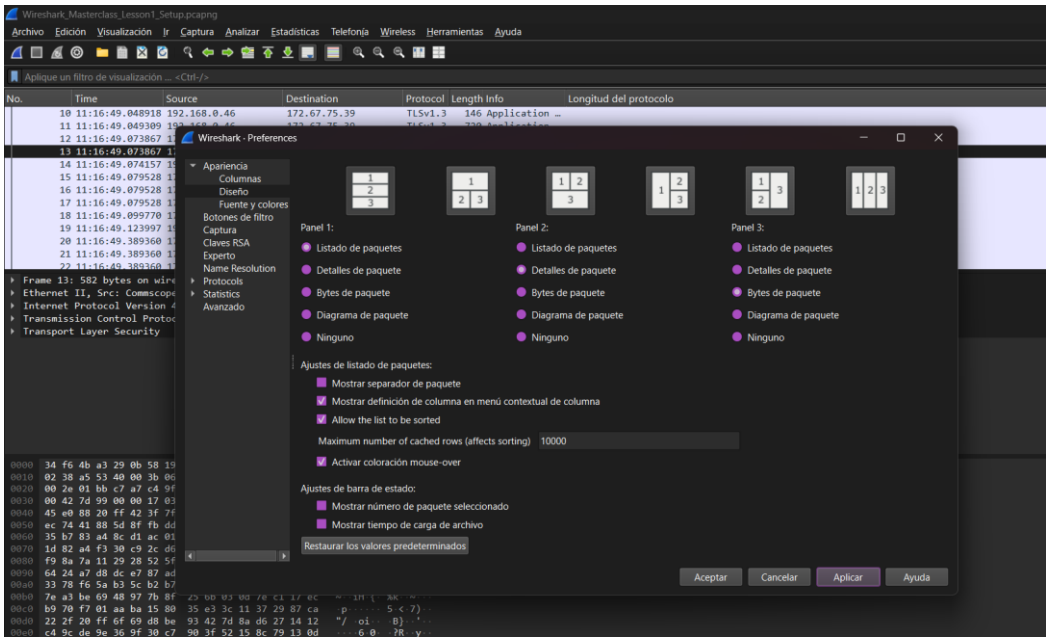
a.



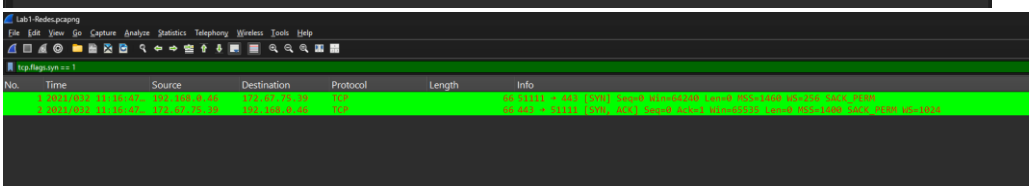
No.	Time	Source	Destination	Protocol	Info	Longitud del protocolo
1	11:16:47.126585	192.168.0.46	172.67.75.39	TCP	51111 → 443 …	
2	11:16:47.177831	172.67.75.39	192.168.0.46	TCP	443 → 51111 …	
3	11:16:47.177959	192.168.0.46	172.67.75.39	TCP	51111 → 443 …	
4	11:16:47.178243	192.168.0.46	172.67.75.39	TLSv1.3	Client Hello…	
5	11:16:47.255959	172.67.75.39	192.168.0.46	TCP	443 → 51111 …	
6	11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	Server Hello…	
7	11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	Application …	
8	11:16:47.267999	192.168.0.46	172.67.75.39	TCP	51111 → 443 …	
9	11:16:49.048600	192.168.0.46	172.67.75.39	TLSv1.3	Change Ciphe…	
10	11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1.3	Application …	
11	11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1.3	Application …	
12	11:16:49.073867	172.67.75.39	192.168.0.46	TCP	443 → 51111 …	
13	11:16:49.073867	172.67.75.39	192.168.0.46	TLSv1.3	Application …	
14	11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1.3	Application …	
15	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	443 → 51111 …	
16	11:16:49.079528	172.67.75.39	192.168.0.46	TCP	443 → 51111 …	
17	11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1.3	Application …	
18	11:16:49.099770	172.67.75.39	192.168.0.46	TCP	443 → 51111 …	
19	11:16:49.123997	192.168.0.46	172.67.75.39	TCP	51111 → 443 …	
20	11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1.3	Application …	

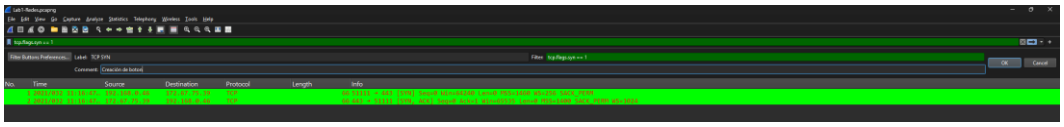
8. Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout)

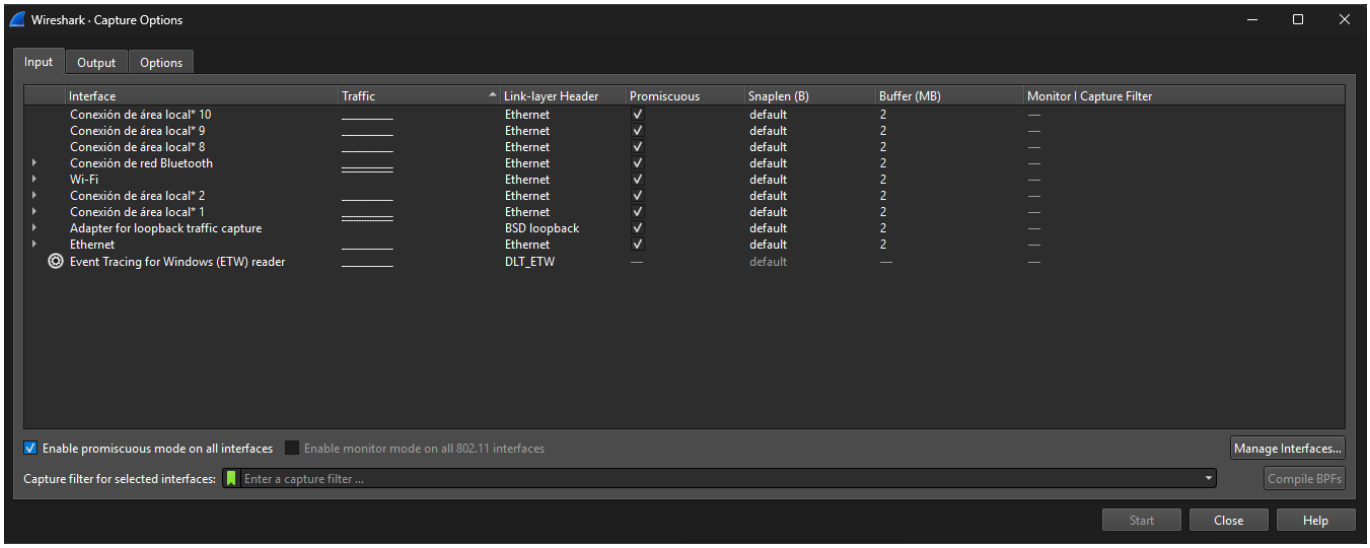
a.



9. Aplique una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia. (View -> coloring rules -> +)



10. Cree un botón que aplique un filtro para paquetes TCP con la bandera SYN igual a 1. (esquina superior derecha -> +)
    a. 
11. Oculte las interfaces virtuales (en caso aplique: capture -> options)
    a.



Se debe realizar tomas de pantalla que muestren el entorno final personalizado, el nombre del perfil y el uso de las regla de color y botón del filtro, así como la lista simplificada de las interfaces de captura.

1.2 Configuración de la captura de paquetes

En la segunda parte, se realizará una captura de paquetes con un ring buffer.

1. 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.

a.

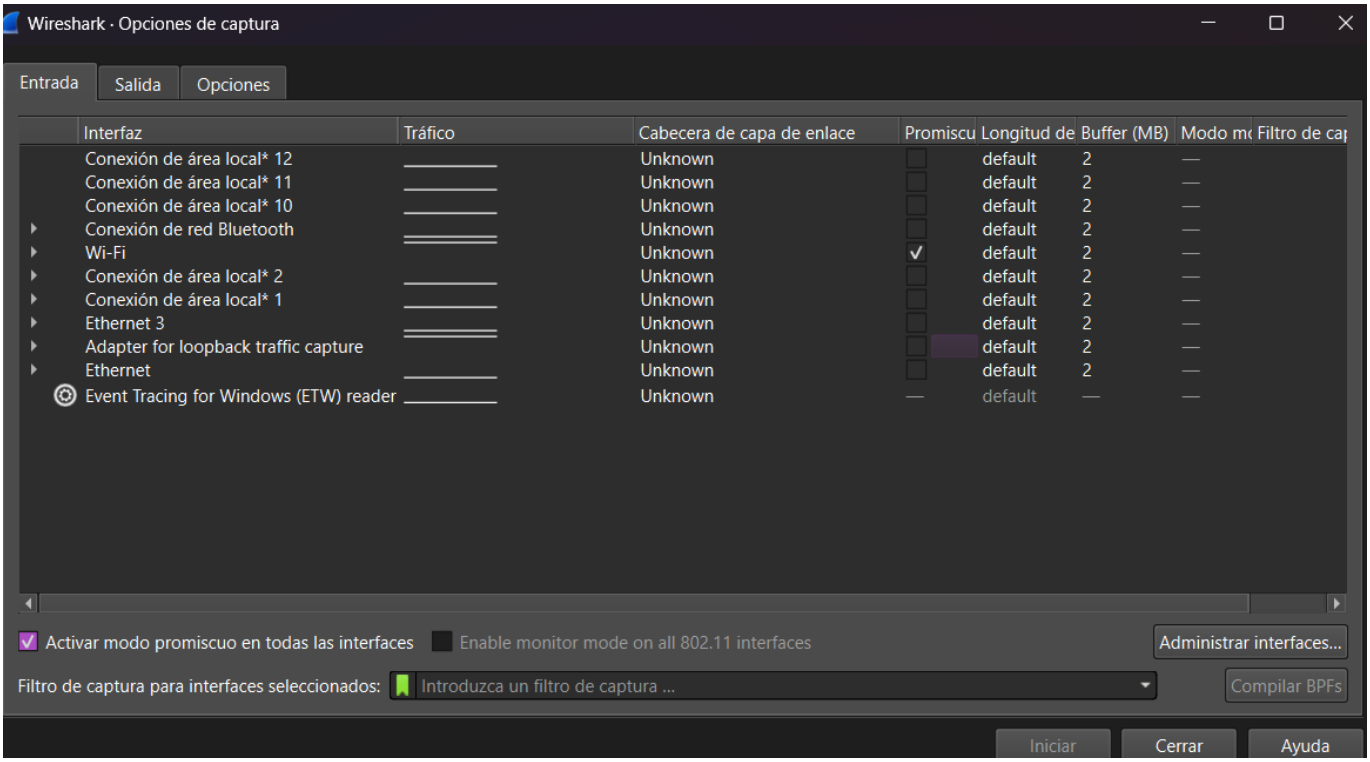
```
C:\Users\user>ipconfig/all

Configuración IP de Windows

   Nombre de host. . . . . . . . . . : CarloL
   Sufijo DNS principal  . . . . . . :
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . . : no
   Proxy WINS habilitado . . . . . . : no

Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Dirección física. . . . . . . . . . . . . . : D4-5D-64-69-00-1B
   DHCP habilitado . . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . . : sí

Adaptador de Ethernet Ethernet 3:

   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Dirección física. . . . . . . . . . . . . . : 0A-00-27-00-00-0F
   DHCP habilitado . . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . . : sí
   Vínculo: dirección IPv6 local. . . . : fe80::6ef1:8a8e:925:9deb%15(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . . : 192.168.56.1(Preferido)
   Máscara de subred . . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
   IAID DHCPv6 . . . . . . . . . . . . . . . . : 805961767
   DUID de cliente DHCPv6. . . . . . . . . . . : 00-01-00-01-27-18-AE-B9-D4-5D-64-69-00-1B
   NetBIOS sobre TCP/IP. . . . . . . . . . . . : habilitado

Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Dirección física. . . . . . . . . . . . . . : E0-D4-E8-BF-43-A3
   DHCP habilitado . . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . . : sí

Adaptador de LAN inalámbrica Conexión de área local* 2:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Dirección física. . . . . . . . . . . . . . : E2-D4-E8-BF-43-A2
   DHCP habilitado . . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Dirección física. . . . . . . . . . . . . . : E0-D4-E8-BF-43-A2
   DHCP habilitado . . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . . : sí
   Dirección IPv6 . . . . . . . . . . . . : 2803:d100:9910:1915:cf70:2a0d:8e64:873f(Preferido)
   Dirección IPv6 temporal. . . . . . . . : 2803:d100:9910:1915:a979:1d1d:4e9b:1ed7(Preferido)
   Vínculo: dirección IPv6 local. . . . : fe80::cd6e:4445:ac5b:c44b%22(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . . : 192.168.0.14(Preferido)
   Máscara de subred . . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . . : martes, 15 de julio de 2025 19:05:43
   La concesión expira . . . . . . . . . . . . : martes, 15 de julio de 2025 20:05:43
   Puerta de enlace predeterminada . . . . . : fe80::fa63:d9ff:fe9a:e074%22
                                               192.168.0.1
   Servidor DHCP . . . . . . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . . . . . . : 216061160
   DUID de cliente DHCPv6. . . . . . . . . . . : 00-01-00-01-27-18-AE-B9-D4-5D-64-69-00-1B
   Servidores DNS. . . . . . . . . . . . . . . : 2803:c800:0:7b::2
                                               10.240.80.242
                                               10.240.80.254
                                               2803:c800:0:7b::2
   NetBIOS sobre TCP/IP. . . . . . . . . . . . : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Dirección física. . . . . . . . . . . . . . : E0-D4-E8-BF-43-A6
   DHCP habilitado . . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . . : sí

C:\Users\user>
```

b.

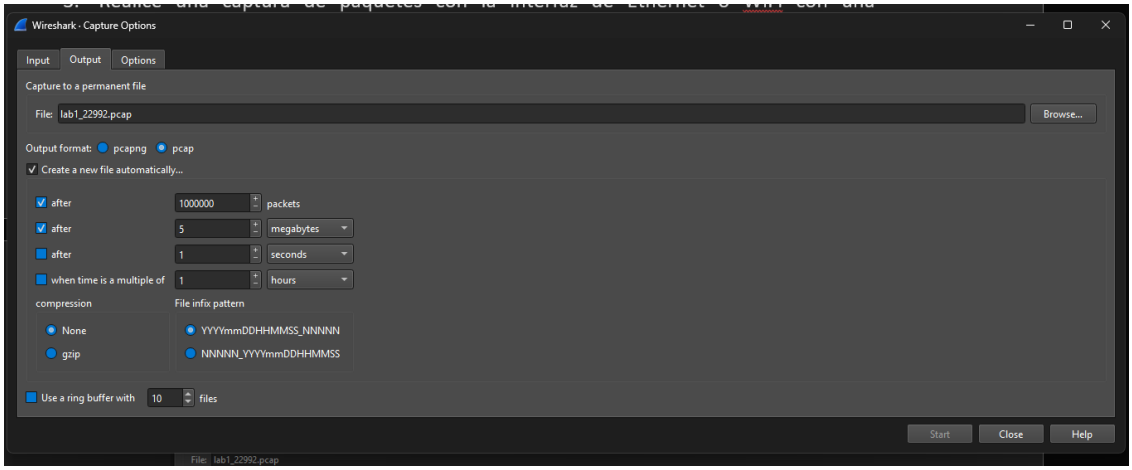
```
C:\Users\user>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 3:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::6ef1:8a0e:925:9deb%15
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . : 2803:d100:9910:1915:cf70:2a0d:8e64:873f
   Dirección IPv6 temporal. . . . . . . : 2803:d100:9910:1915:a979:1d1d:4e9b:1ed7
   Vínculo: dirección IPv6 local. . . : fe80::cd6e:4445:ac5b:c44b%22
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.14
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::fa63:d9ff:fe9a:e074%22
                                       192.168.0.1

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

C:\Users\user>
```

c. **Interfaz seleccionada**: Wi-Fi – Intel(R) Wireless-AC 9560 160MHz
IPv4: 192.168.0.14 – dirección asignada dinámicamente por el router doméstico mediante DHCP.
Máscara: 255.255.255.0 – red de clase C (/24), permite hasta 254 dispositivos conectados (192.168.0.1 a 192.168.0.254).
Puerta de enlace: 192.168.0.1 – dirección IP del router que permite salir a internet.
DHCP: 192.168.0.1 – el mismo router actúa como servidor de DHCP y asigna automáticamente IPs.
MAC: E0-D4-E8-BF-43-A2 – dirección física (única) de la tarjeta Wi-Fi.
Estado: Conectada y activa; será la interfaz usada para generar tráfico real durante la captura.
Otras interfaces: Ethernet, adaptadores VirtualBox, Bluetooth y Wi-Fi Direct están desconectadas o son virtuales, por lo que fueron **deshabilitadas en Wireshark** para evitar ruido innecesario durante la captura.

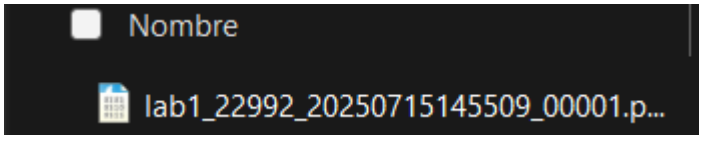
2. Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.



3. 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)

a. 

Se debe realizar tomas de pantalla de la configuración o comandos para la creación del ring buffer, así como los archivos generados.



1.3 Análisis de paquetes

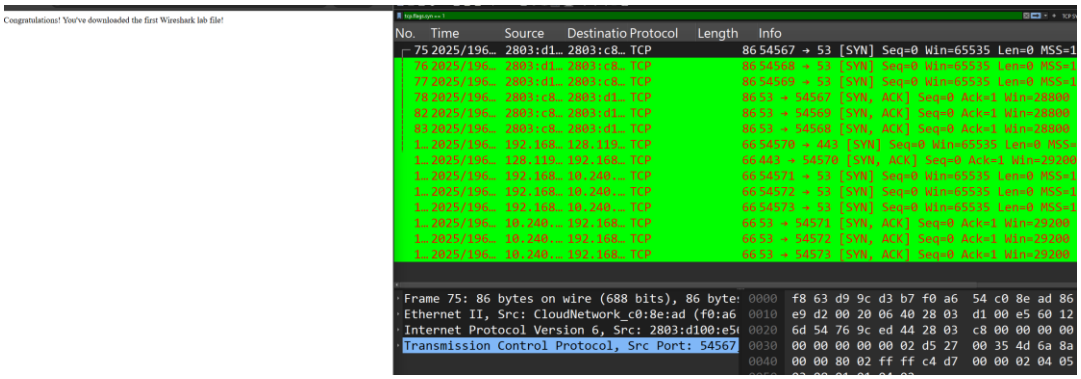
En la tercera parte se analizará el protocolo HTTP. Debe realizar tomas de pantalla que validen sus respuestas.

1. 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

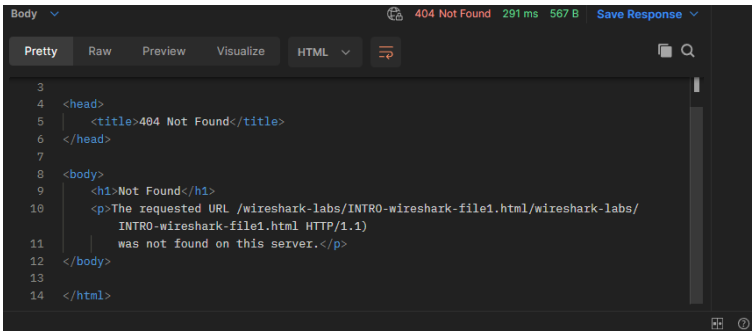
a.

2. 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).



a.

3. Responda las siguientes preguntas:
   a. ¿Qué versión de HTTP está ejecutando su navegador?
      - HTTP/1.1
      -



   b. ¿Qué versión de HTTP está ejecutando el servidor?
      - HTTP/1.1 200 OK
   c. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?
      - En la cabecera Accept-Language se indica que el navegador acepta los siguientes idiomas:
        - en-Us, en, es
   d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
      - El servidor devolvió 393 bytes de contenido
   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.

      Si se presentan problemas de rendimiento, lo más recomendable es capturar el tráfico en puntos estratégicos de la red, como el router, un switch configurado con port mirroring o un firewall, ya que permiten observar la comunicación completa entre el cliente y el servidor.

      Instalar Wireshark directamente en el servidor no es aconsejable, ya que podría afectar su rendimiento, introducir riesgos de seguridad y vulnerar políticas administrativas. Lo ideal es monitorear desde un dispositivo independiente o desde un nodo con acceso a todo el tráfico relevante sin comprometer ningún sistema de producción.

Discusión sobre la actividad

Este laboratorio me permitió explorar tanto la personalización de la interfaz de Wireshark como el análisis práctico del tráfico de red. En la primera parte, configuré un perfil propio, añadí columnas personalizadas como

frame.len, cambié el diseño de los paneles y establecí reglas de color para identificar fácilmente paquetes TCP con bandera SYN activa. Estas configuraciones facilitaron una interpretación más visual y ágil del tráfico.

En la segunda parte, realicé una captura real del protocolo HTTP al visitar un sitio específico. Pude identificar cabeceras como Accept-Language, la versión del protocolo utilizada, y el tamaño del contenido en la respuesta del servidor. También aprendí a configurar el ring buffer, herramienta que permite realizar capturas prolongadas dividiendo automáticamente los archivos, evitando así problemas de almacenamiento.

Conclusiones

- Aprendí a configurar Wireshark de manera personalizada para facilitar el análisis visual de los paquetes.
- Logré capturar tráfico real HTTP, identificar elementos clave de las solicitudes y respuestas, y analizar cómo fluye la información entre el cliente y el servidor.
- Comprendí por qué es preferible monitorear desde puntos de red intermedios en lugar de instalar Wireshark directamente en un servidor.
- El uso del buffer cíclico (ring buffer) demostró ser esencial para sesiones largas de captura sin saturar el disco.
