Sofia Garcia - 22210

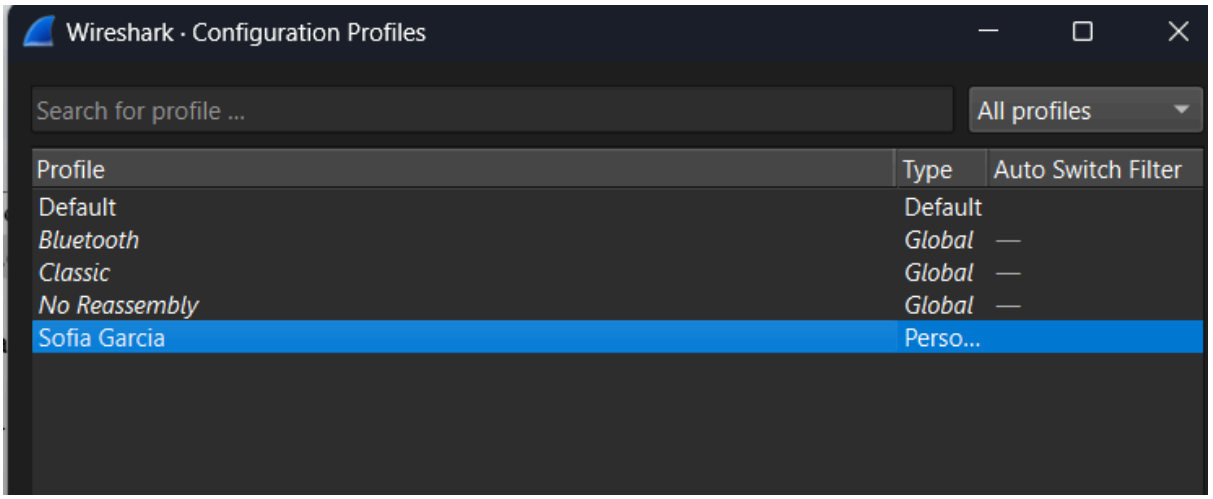
Segunda parte: Introducción a Wireshark

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

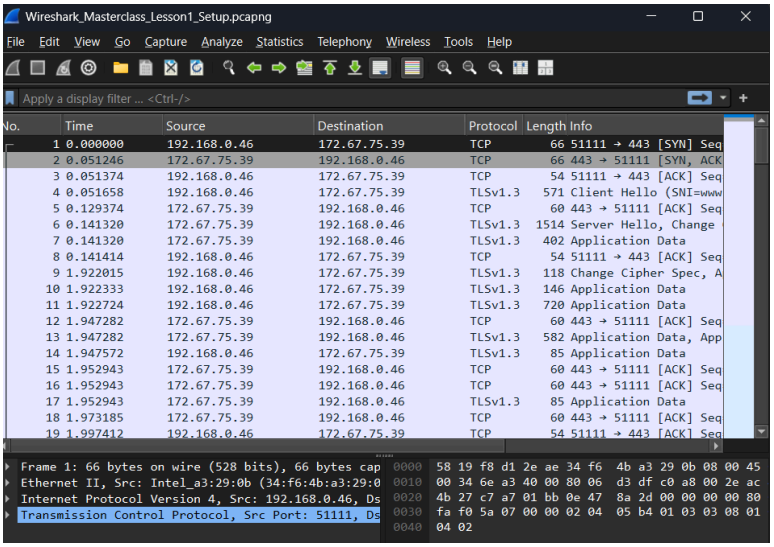
1.1 Personalización del entorno

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)

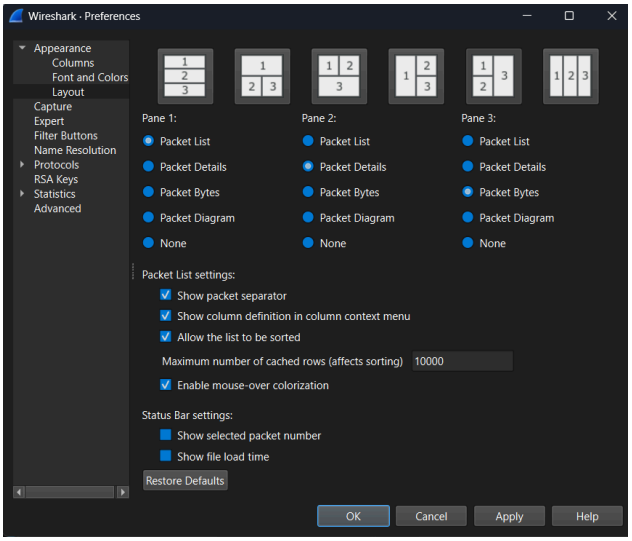


3. Descargue el archivo https://www.cloudshark.org/captures/e6fb36096dbb (Export -> Download)
4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.

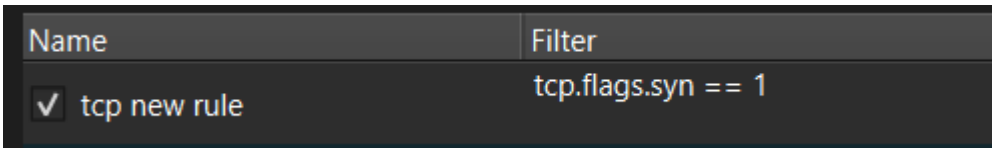


5. Aplique el formato de tiempo Time of Day (view -> Time Display Format)
6. Agregue una columna con la longitud del protocolo (preferences -> column -> +)
7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)

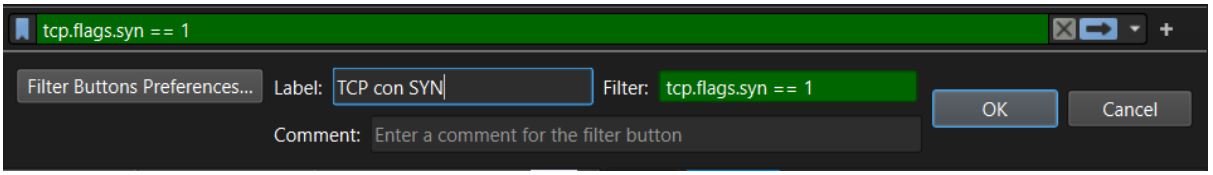
8. Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout)



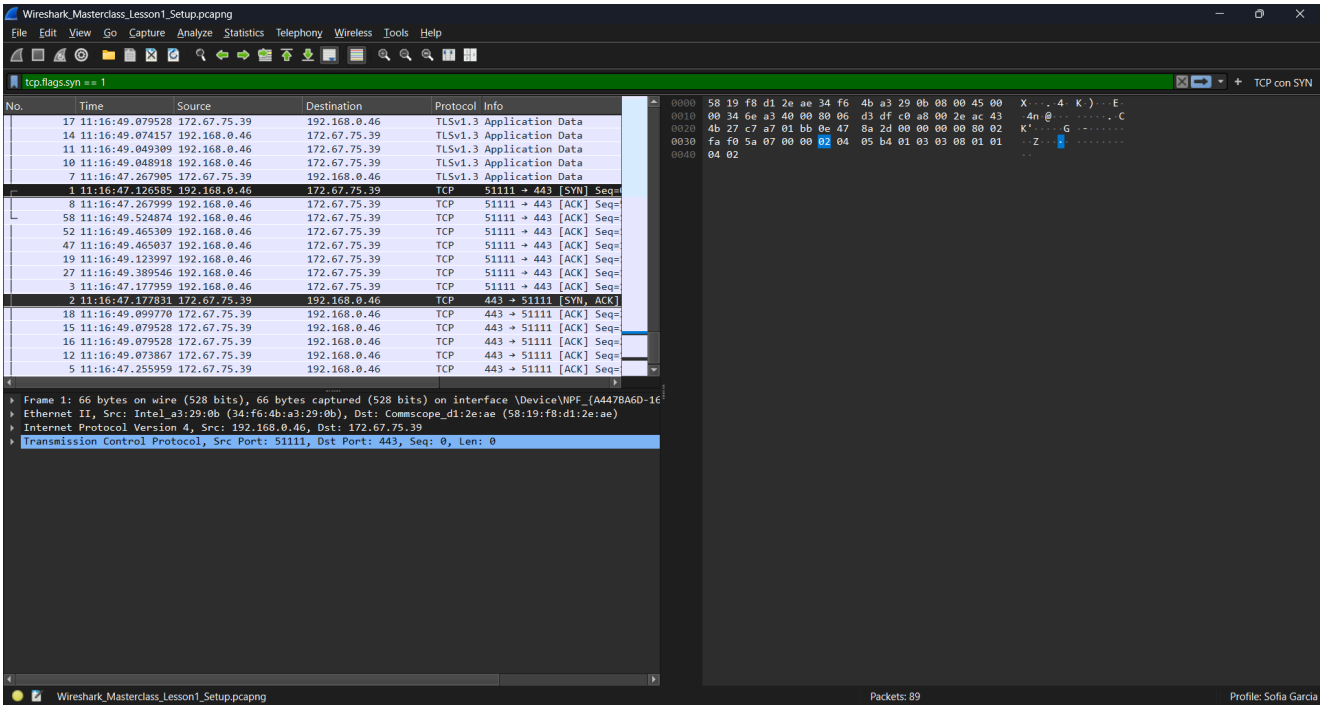
9. Aplique una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia. (View -> coloring rules -> +)



10. Cree un botón que aplique un filtro para paquetes TCP con la bandera SYN igual a 1. (esquina superior derecha -> +)



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

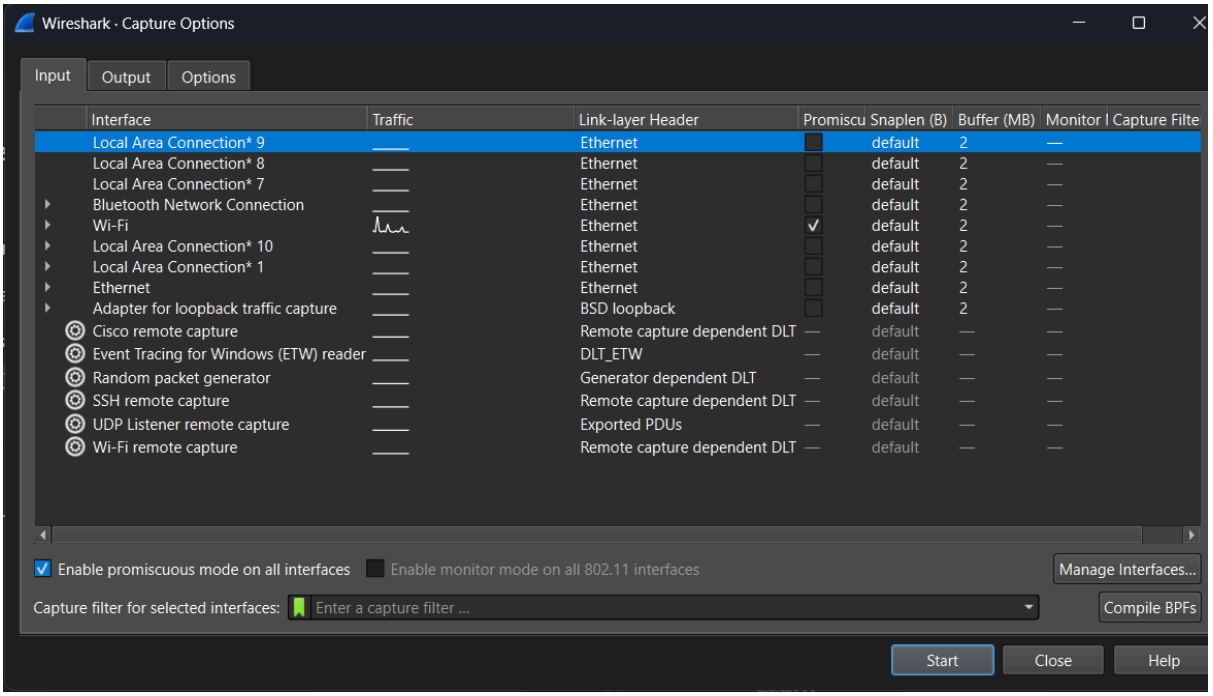
1. Abra una terminal y ejecute el comando ifconfig/ipconfig (dependiendo de su OS). Detalle y explique lo observado, investigue (i.e.: 'man ifconfig', documentación) de ser necesario.

```
PS C:\Users\sofia> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d824:3016:77f0:af79%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2800:98:110f:10d5::5
   IPv6 Address. . . . . . . . . . . : 2800:98:110f:10d5:eb41:24e8:3668:5f8f
   Temporary IPv6 Address. . . . . . : 2800:98:110f:10d5:d8b7:f41c:ad97:fe40
   Link-local IPv6 Address . . . . . : fe80::6872:4515:be69:ee75%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8601:12ff:fed3:1de9%3
                                       192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Al ejecutar el comando ipconfig, pude ver la configuración de red de mi equipo. Identifiqué varios adaptadores, pero sólo el adaptador Wi-Fi está activo, con dirección IPv4 192.168.1.9 y puerta de enlace 192.168.1.1, lo que indica que es el adaptador con acceso a internet.

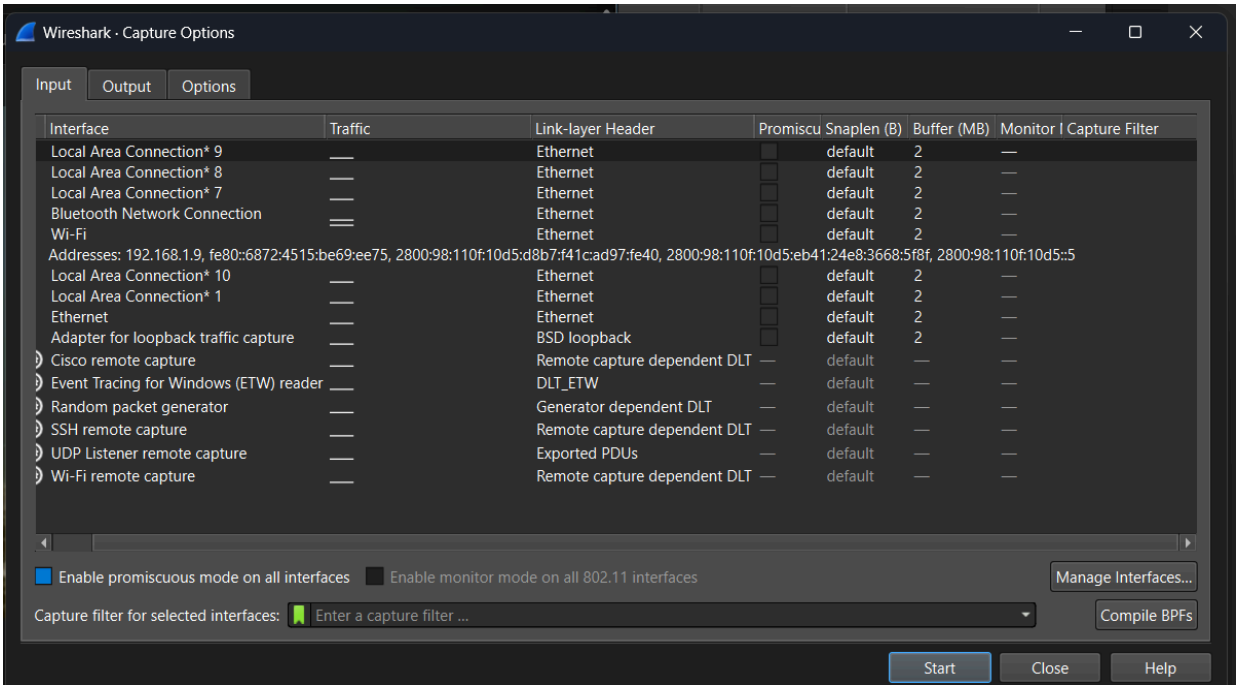
Los demás adaptadores (Ethernet, Bluetooth y conexiones de área local) están desconectados, por lo que no están siendo utilizados actualmente.

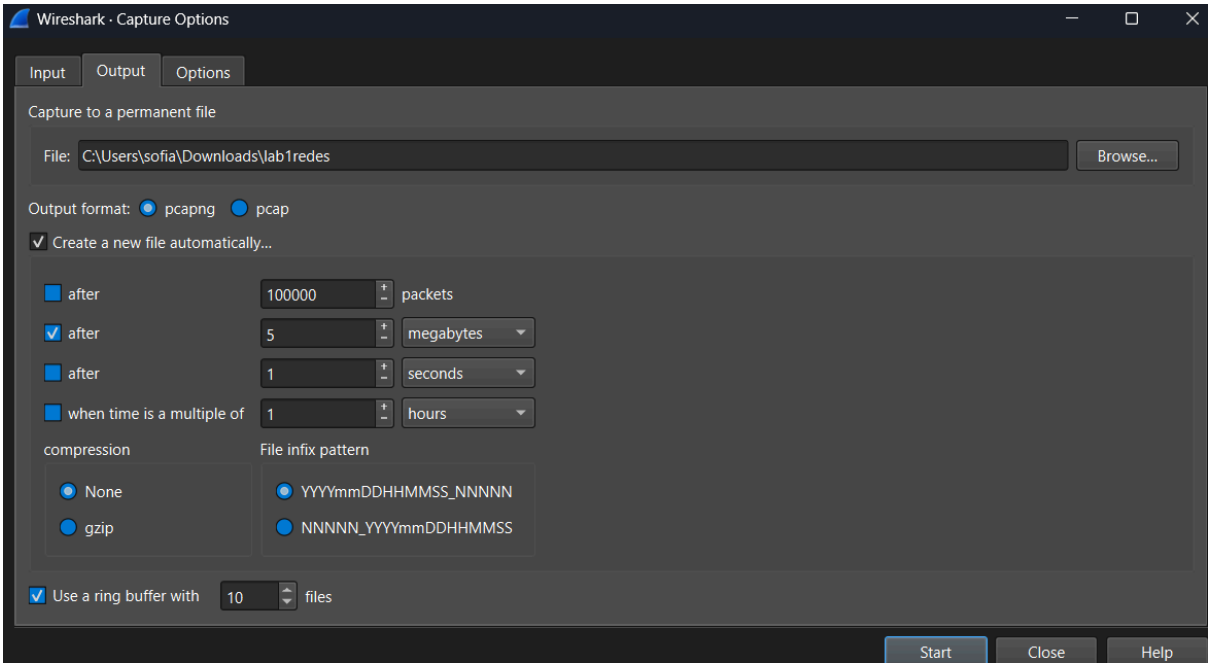
2. Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.

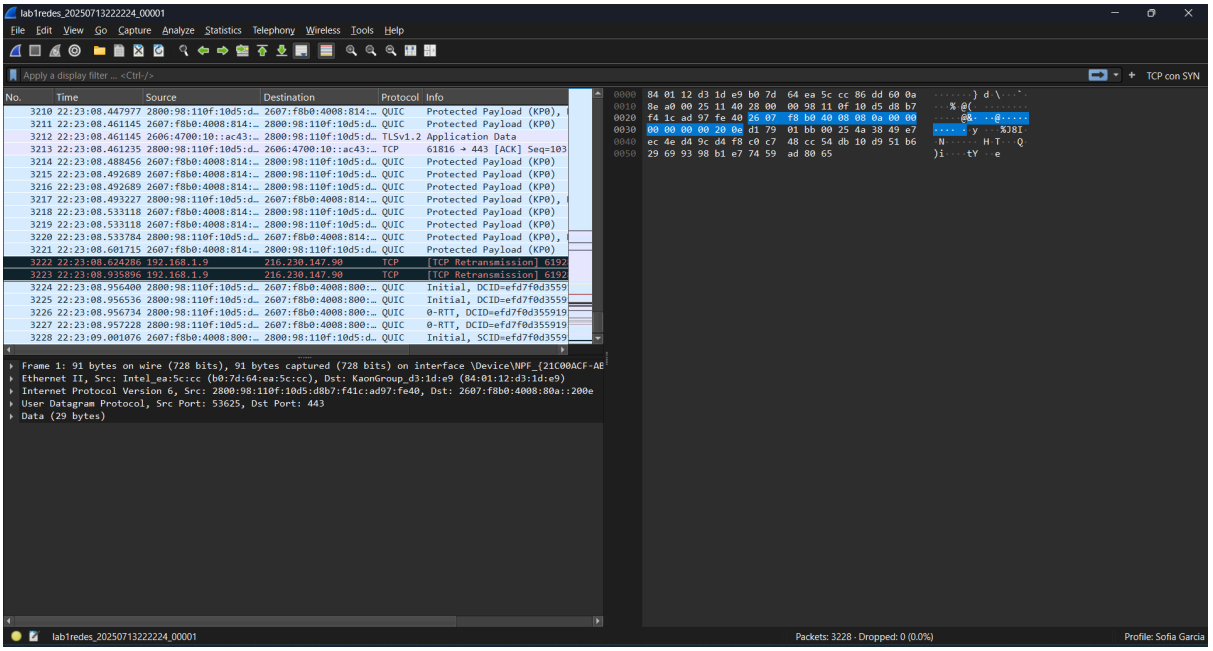


3. Realice una captura de paquetes con la interfaz de Ethernet o WiFi con una configuración de ring buffer, con un tamaño de 5 MB por archivo y un número máximo de 10 archivos (puede hacerlo por medio de la interfaz de usuario o por medio de comandos) Genere tráfico para que los archivos se creen. Defina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

Sofia Garcia - 22210





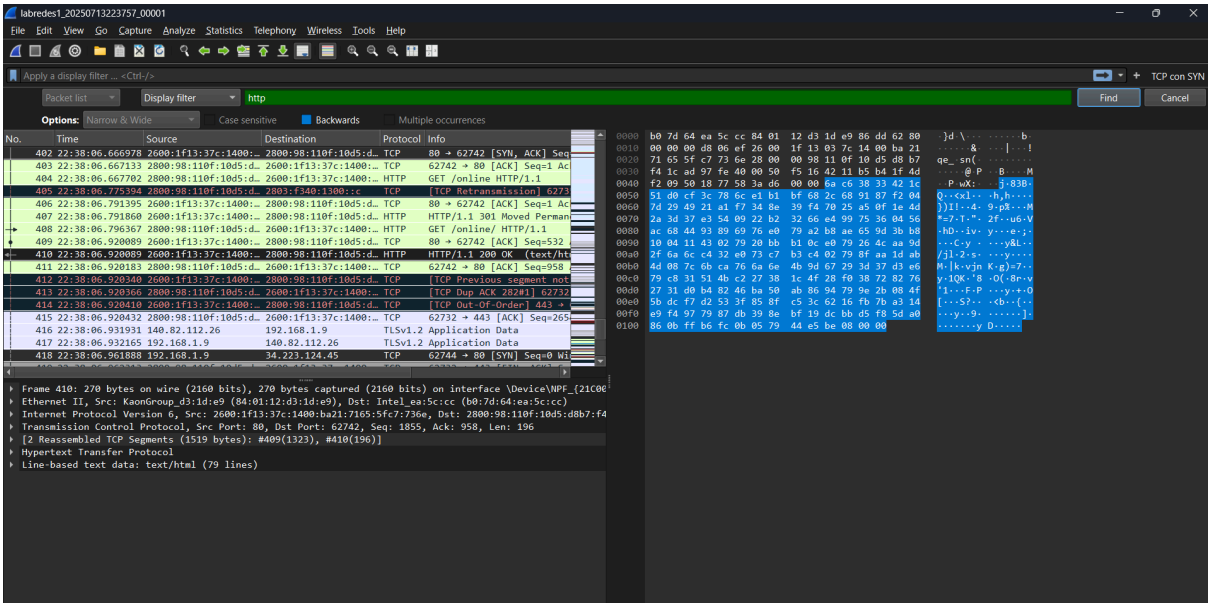


1.3 Análisis de paquetes

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

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).



3. Responda las siguientes preguntas:

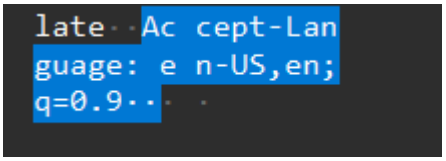
a. ¿Qué versión de HTTP está ejecutando su navegador?

HTTP/1.1

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

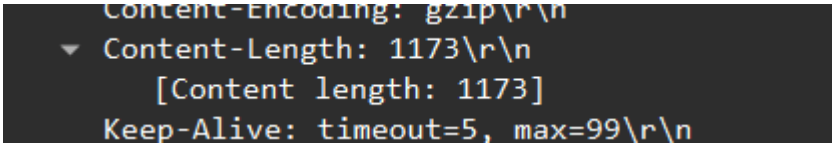
HTTP/1.1

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



en-US, en

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



1173 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.

Es mejor capturar paquetes en el punto más cercano al cliente afectado, como su computadora o router. Esto permite diagnosticar si el problema es local, del proveedor de internet, o de la conexión al servidor.

No es recomendable instalar Wireshark en el servidor, ya que podría afectar su rendimiento o representar un riesgo de seguridad. En entornos de producción, se utilizan herramientas especializadas para monitoreo de red.