

UNIVERSIDAD DEL VALLE DE GUATEMALA

Redes, sección 20

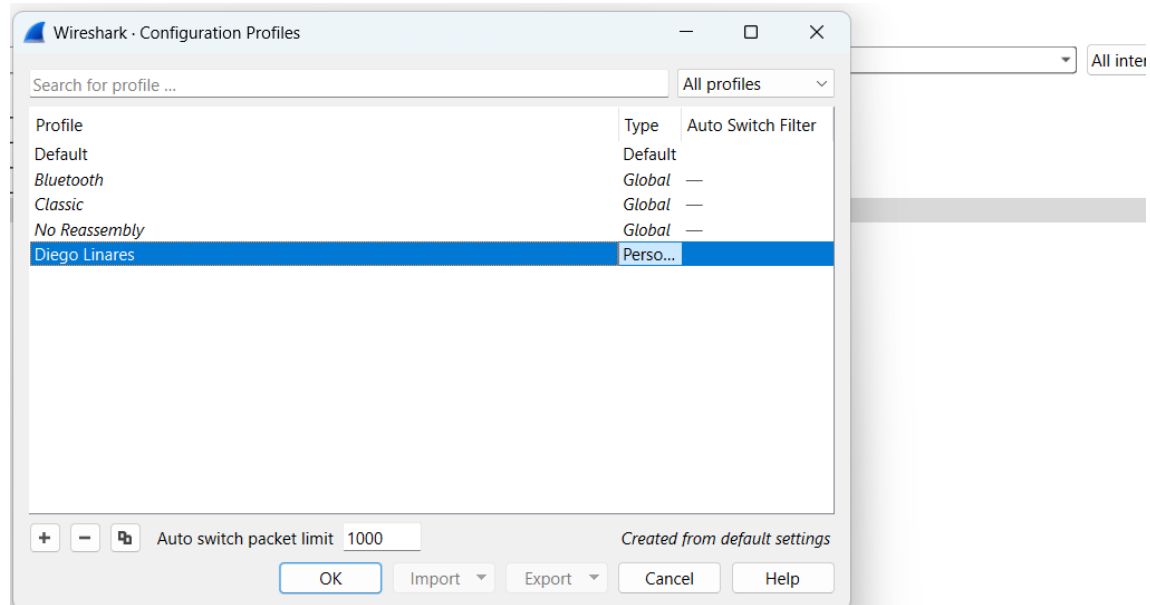


LAB # 1 parte individual

Diego Linares - 221256

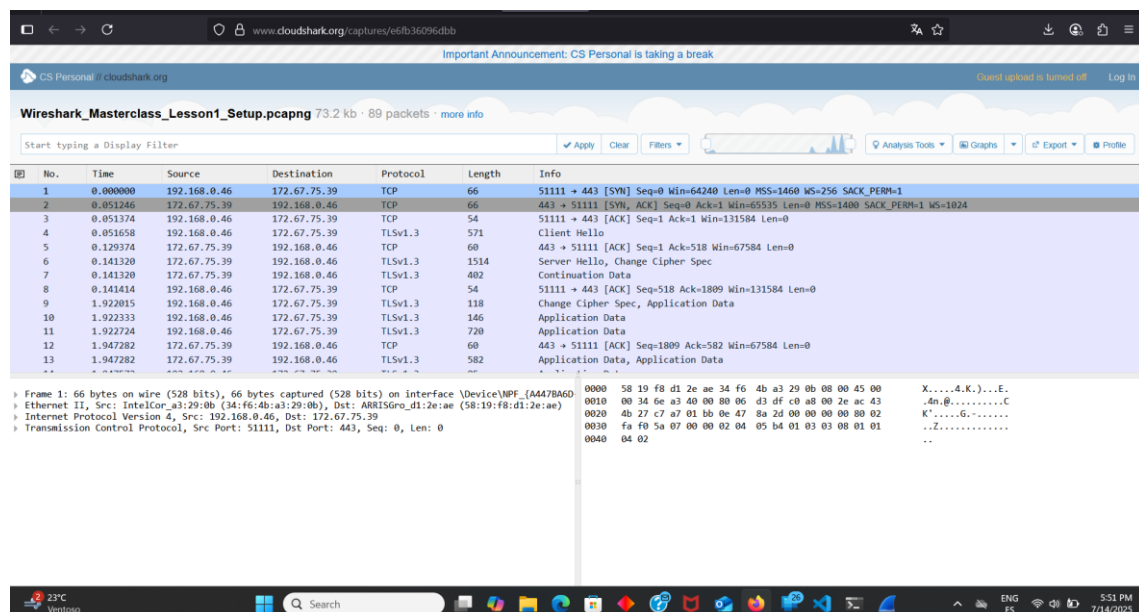
Guatemala, Julio 2025

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

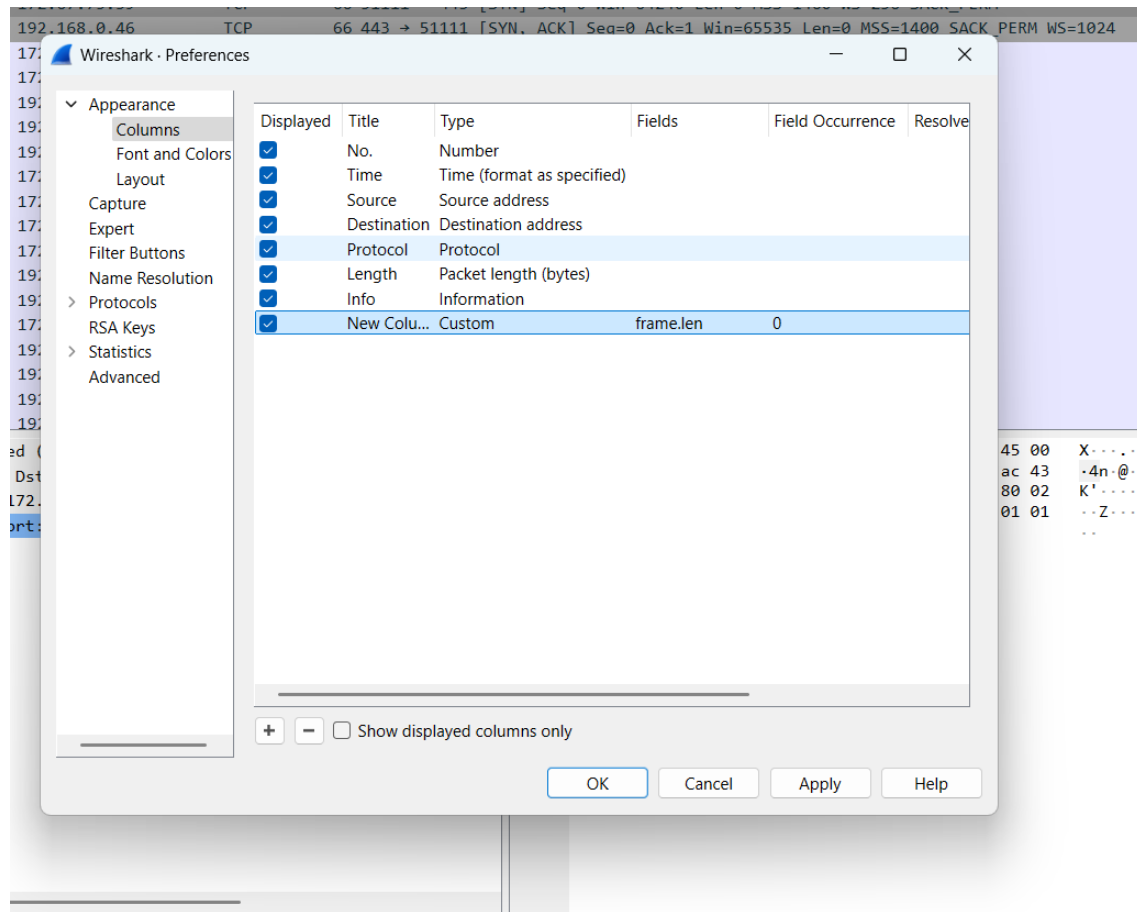


[Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

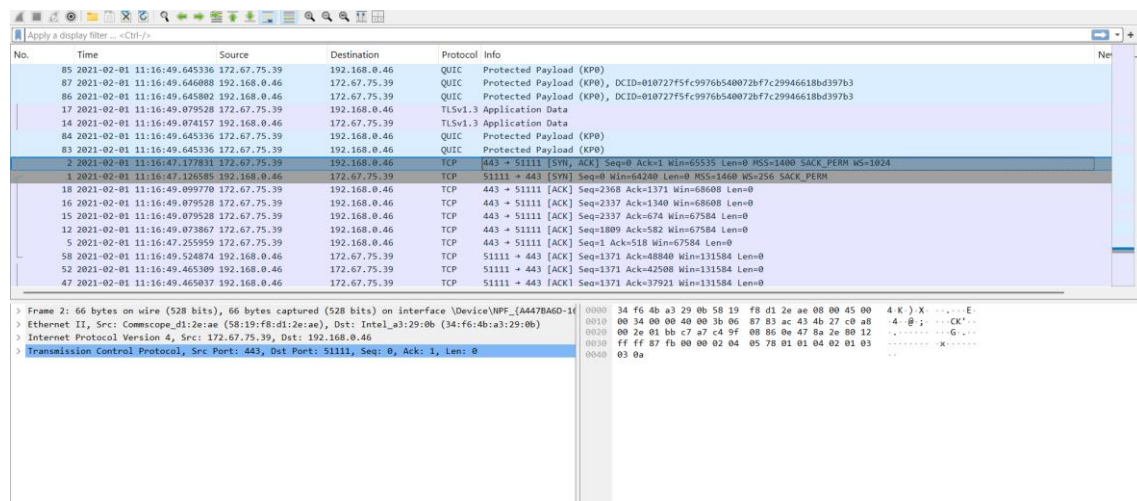
3. Descargue el archivo <https://www.cloudshark.org/captures/e6fb36096dbb>
(Export -> Download)



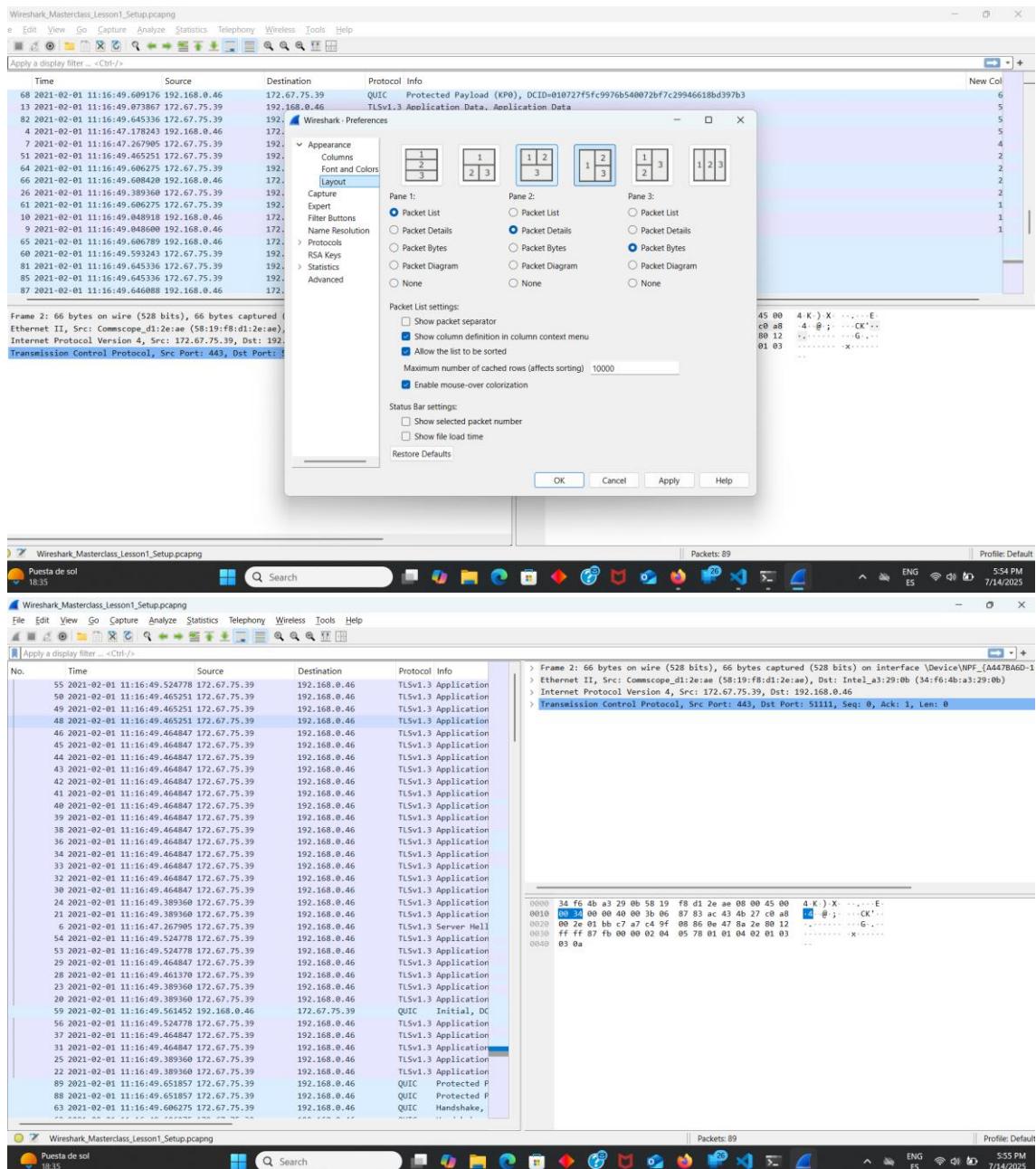
4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.



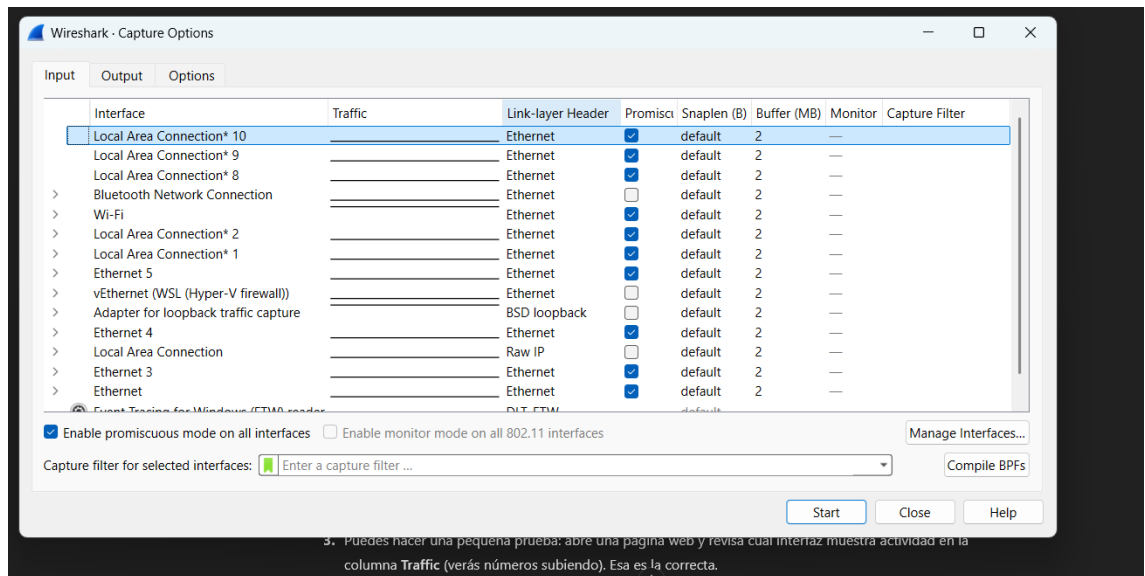
7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)



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 -> +)



- vEthernet (WSL Hyper-V firewall) → virtual
- Adapter for loopback traffic capture → virtual
- Bluetooth Network Connection → no aplica para red Ethernet/WiFi
- Raw IP, DLT_ETW, Local Area Connection sin número → probablemente virtual

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.

```
C:\Users\diego>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 3:

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

Unknown adapter Local Area Connection:

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

Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

    Connection-specific DNS Suffix  . :
    Link-Local IPv6 Address . . . . . : fe80::87cd:ac08:f935:f089%84
    IPv4 Address. . . . . : 172.30.0.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . :
    Link-Local IPv6 Address . . . . . : fe80::e685:5949:ac61:b2df%18
    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* 2:

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

Ethernet adapter Ethernet 4:

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



```

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter Ethernet 4:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2800:98:1124:146d:cc5d:9bd:2d64:a22f
    Temporary IPv6 Address. . . . . : 2800:98:1124:146d:212e:da74:d5b4:3f8f
    Link-local IPv6 Address . . . . . : fe80::bb37:18f3:e825:7fef%21
    IPv4 Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::52a5:dcff:fedc:a8a5%21
                                192.168.1.1

Ethernet adapter Bluetooth Network Connection:

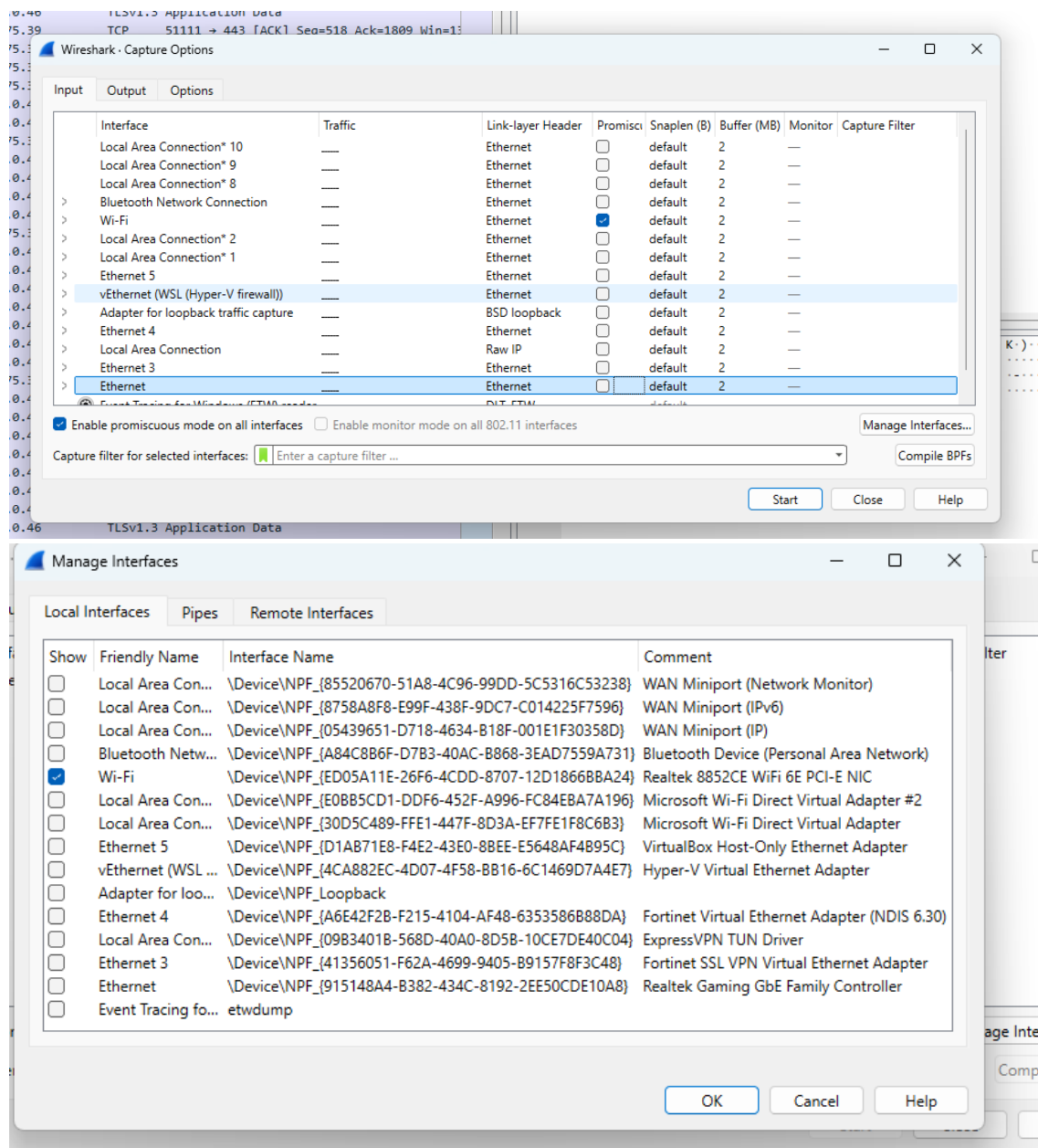
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\diego>

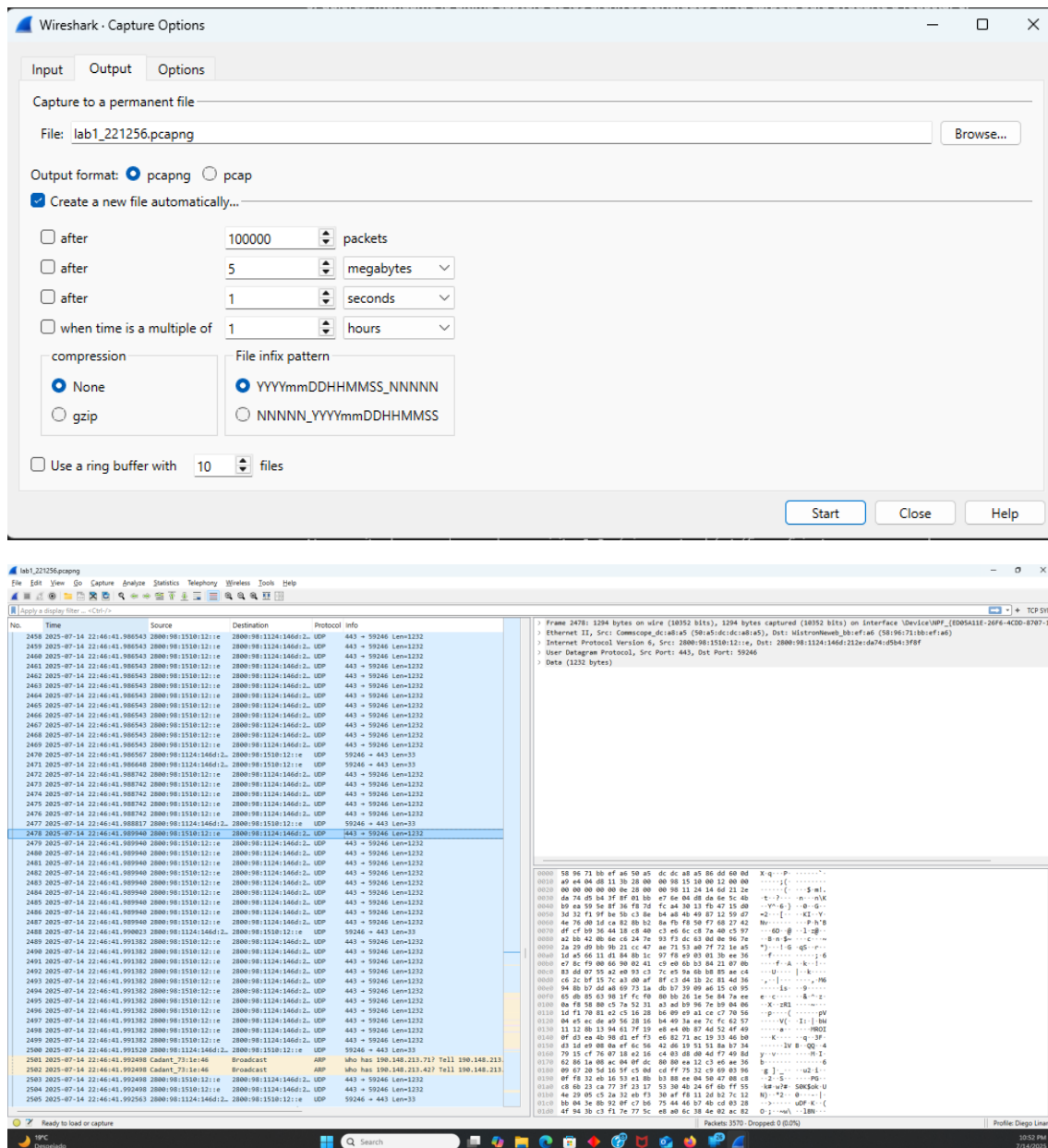
```

- **Ethernet adapters (varios)**
 Todos aparecen como Media disconnected → significa que ningún cable Ethernet físico está conectado ni activo.
- **vEthernet (WSL Hyper-V firewall)**
 Este es un adaptador virtual de Windows (para máquinas virtuales o subsistemas).
 IP: 172.30.0.1 (virtual, no se usa para Internet)
- **Ethernet adapter Ethernet 5**
 Otro adaptador virtual, probablemente para VirtualBox o Hyper-V.
 IP: 192.168.56.1 (virtual, no se usa para Internet)
- **Wi-Fi**
 Este sí está activo y conectado:
 IP: 192.168.1.7 (tu dirección local en la red Wi-Fi)
 Gateway: 192.168.1.1 (el router)

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)



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 dirección: <https://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:

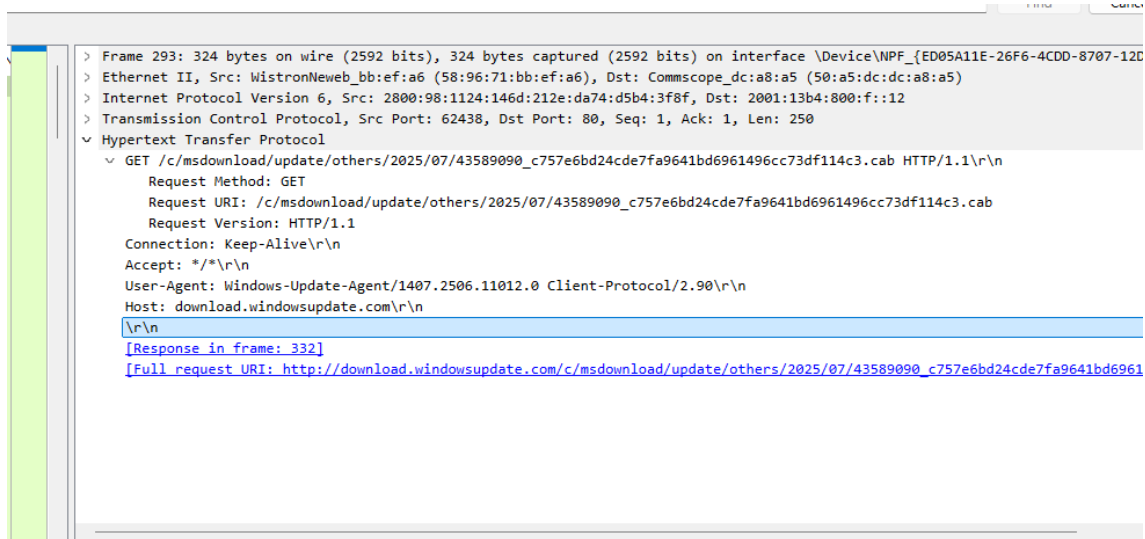
a. ¿Qué versión de HTTP está ejecutando su navegador?

El navegador usa la versión HTTP/1.1.

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

El servidor usa la versión HTTP/1.1.

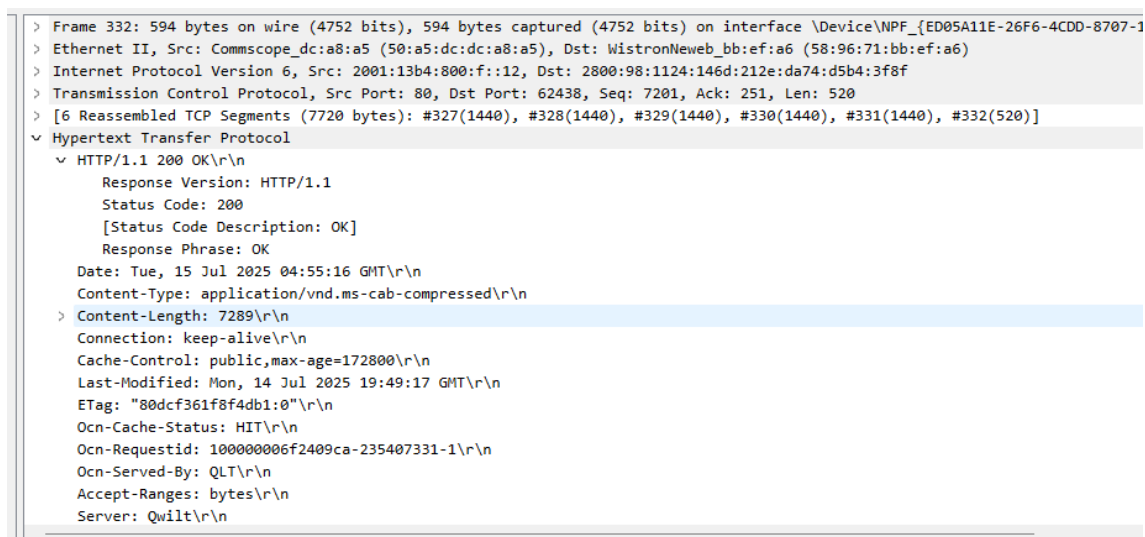
c. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?



```
> Frame 293: 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interface \Device\NPF_{ED05A11E-26F6-4CDD-8707-12C...}
> Ethernet II, Src: WistronNeweb_bb:ef:a6 (58:96:71:bb:ef:a6), Dst: Commscope_dc:a8:a5 (50:a5:dc:dc:a8:a5)
> Internet Protocol Version 6, Src: 2800:98:1124:146d:212e:da74:d5b4:3f8f, Dst: 2001:13b4:800:f::12
> Transmission Control Protocol, Src Port: 62438, Dst Port: 80, Seq: 1, Ack: 1, Len: 250
  Hypertext Transfer Protocol
    GET /c/msdownload/update/others/2025/07/43589090_c757e6bd24cde7fa9641bd6961496cc73df114c3.cab HTTP/1.1\r\n
      Request Method: GET
      Request URI: /c/msdownload/update/others/2025/07/43589090_c757e6bd24cde7fa9641bd6961496cc73df114c3.cab
      Request Version: HTTP/1.1
      Connection: Keep-Alive\r\n
      Accept: */*\r\n
      User-Agent: Windows-Update-Agent/1407.2506.11012.0 Client-Protocol/2.90\r\n
      Host: download.windowsupdate.com\r\n
    \r\n
    [Response in frame: 332]
    [Full request URI: http://download.windowsupdate.com/c/msdownload/update/others/2025/07/43589090_c757e6bd24cde7fa9641bd6961496cc73df114c3.cab]
```

En los paquetes HTTP capturados no se observa un encabezado Accept-Language, ya que el tráfico corresponde a solicitudes automáticas del servicio Windows Update, el cual no envía esa cabecera.

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



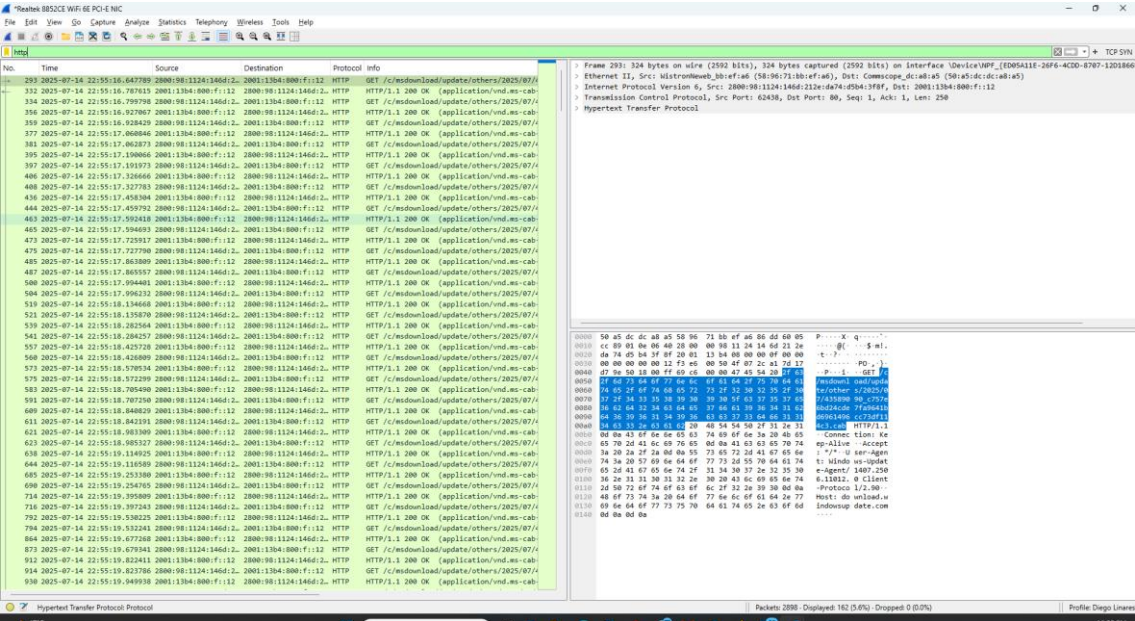
```
> Frame 332: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits) on interface \Device\NPF_{ED05A11E-26F6-4CDD-8707-12C...}
> Ethernet II, Src: Commscope_dc:a8:a5 (50:a5:dc:dc:a8:a5), Dst: WistronNeweb_bb:ef:a6 (58:96:71:bb:ef:a6)
> Internet Protocol Version 6, Src: 2001:13b4:800:f::12, Dst: 2800:98:1124:146d:212e:da74:d5b4:3f8f
> Transmission Control Protocol, Src Port: 80, Dst Port: 62438, Seq: 7201, Ack: 251, Len: 520
> [6 Reassembled TCP Segments (7720 bytes): #327(1440), #328(1440), #329(1440), #330(1440), #331(1440), #332(520)]
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Tue, 15 Jul 2025 04:55:16 GMT\r\n
      Content-Type: application/vnd.ms-cab-compressed\r\n
    Content-Length: 7289\r\n
      Connection: keep-alive\r\n
      Cache-Control: public,max-age=172800\r\n
      Last-Modified: Mon, 14 Jul 2025 19:49:17 GMT\r\n
      ETag: "80dcf361f8f4db1:0"\r\n
      Ocn-Cache-Status: HIT\r\n
      Ocn-Requestid: 100000006f2409ca-235407331-1\r\n
      Ocn-Served-By: QLT\r\n
      Accept-Ranges: bytes\r\n
      Server: Qwilt\r\n
```

7289

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 los paquetes en un punto de red cercano al servidor, como en el router o switch principal, ya que esto permite ver el tráfico completo sin afectar el rendimiento del servidor ni comprometer su seguridad. No es recomendable instalar Wireshark directamente en el servidor, ya que puede consumir recursos y afectar la estabilidad del servicio.



!!!Comentario personal de la actividad!!!

Este laboratorio me permitió familiarizarme con el uso de Wireshark y entender la importancia de analizar el tráfico de red de manera práctica. Aunque al principio me costó identificar la interfaz correcta y configurar los parámetros, logré capturar paquetes reales y comprender las cabeceras HTTP. Me resultó interesante ver cómo las herramientas de monitoreo permiten visualizar la comunicación entre cliente y servidor en tiempo real.

Discusión

Durante la práctica, fue evidente que seleccionar la interfaz correcta es fundamental para poder capturar tráfico válido, ya que muchas interfaces listadas son virtuales o no están activas. La configuración del ring buffer resultó útil para gestionar de manera eficiente el almacenamiento de las capturas, evitando ocupar demasiado espacio en disco. En el análisis HTTP, se pudo observar que no todos

los clientes envían las mismas cabeceras, como Accept-Language, y que en algunos casos el servidor no envía Content-Length debido al uso de técnicas como codificación por fragmentos. Esto resalta la diversidad de implementaciones en los protocolos y la importancia de interpretar correctamente la información disponible.

Conclusión

Con este laboratorio se comprobó la utilidad de Wireshark como herramienta de monitoreo y análisis de tráfico de red, facilitando la identificación de protocolos, cabeceras y tamaños de respuesta. También se evidenció la necesidad de configurar adecuadamente la captura y de comprender las características de cada interfaz de red. Finalmente, se logró comprender cómo la información capturada permite diagnosticar y evaluar el comportamiento de la red y de las aplicaciones que se comunican a través de ella, siendo un recurso clave para la administración de redes.