UVG UNIVERSIDAD DEL VALLE DE GUATEMALA	Universidad del Valle de Guatemala Facultad de Ingeniería Departamento de Ciencias de la Computación CC3067 - Redes	**Laboratorio #1 – Esquemas de comunicación e Introducción a Wireshark** Semestre II - 2025

Reporte

Nombre: Brandon Reyes Morales

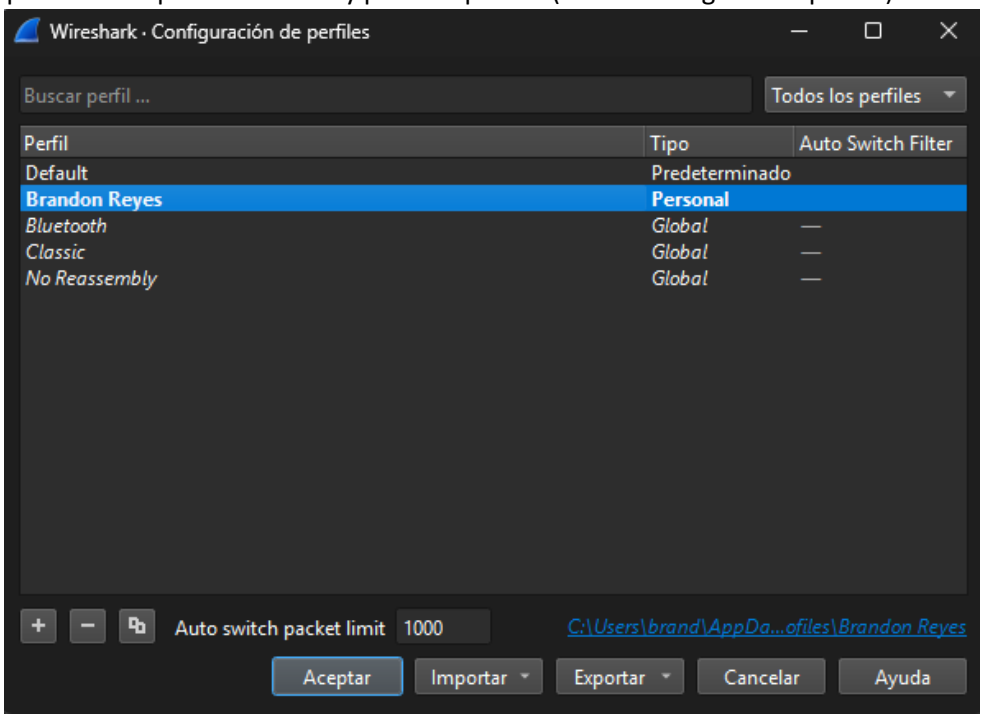
Carné: 22992

Segunda parte: Introducción a Wireshark

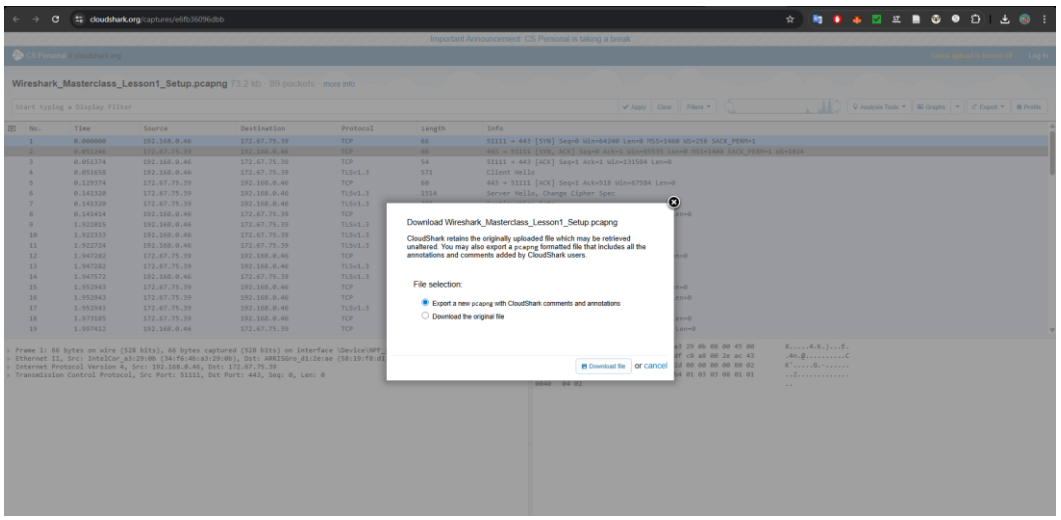
Se debe descargar e instalar el software de Wireshark. Es probable que para ejecutarlo pida permisos de administrador (sudo, click + run as admin, etc.).

1.1 Personalización del entorno

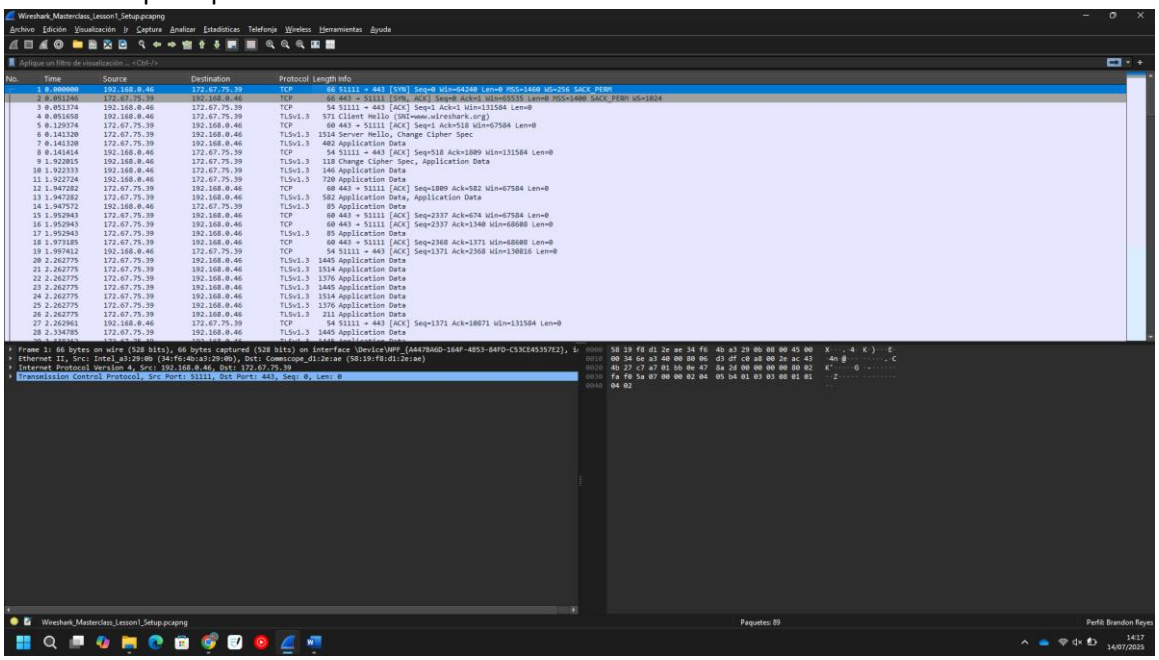
En la primera parte se realizará la personalización del entorno de Wireshark, de modo que se adapte a nuestras preferencias de uso.

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

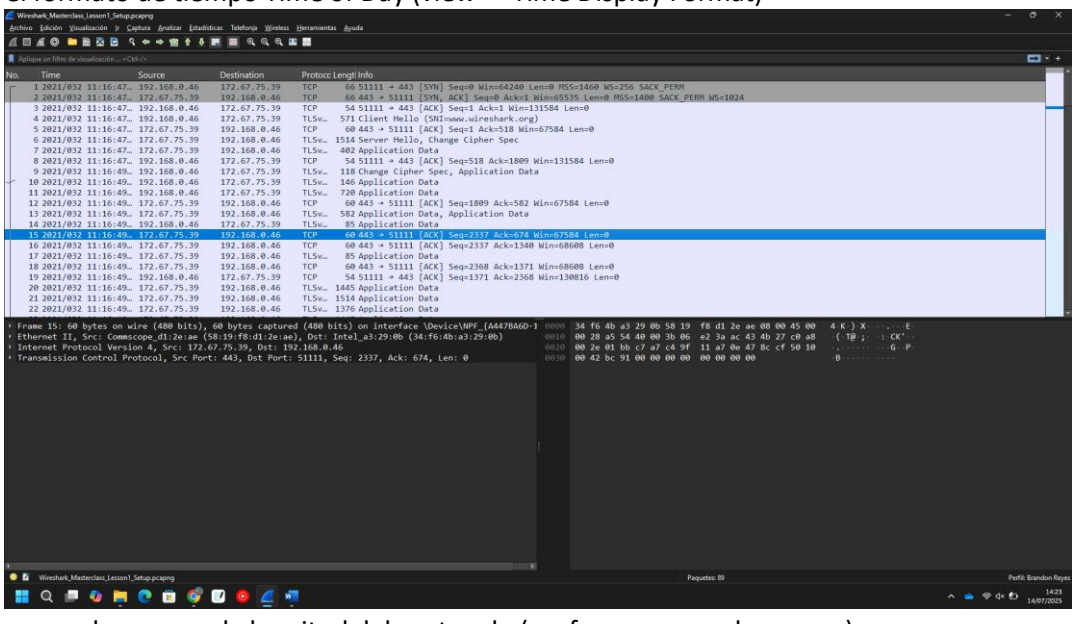
3. Descargue el archivo https://www.cloudshark.org/captures/e6fb36096dbb (Export -> Download)

a. 

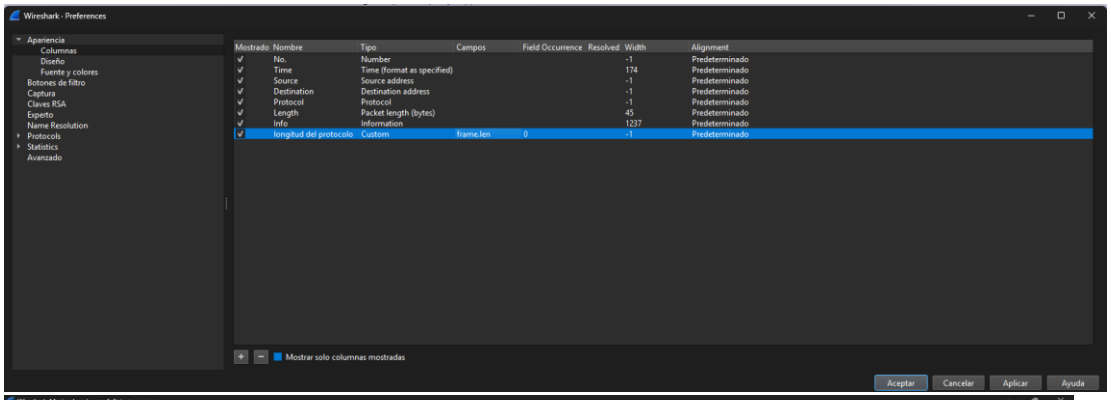
4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.

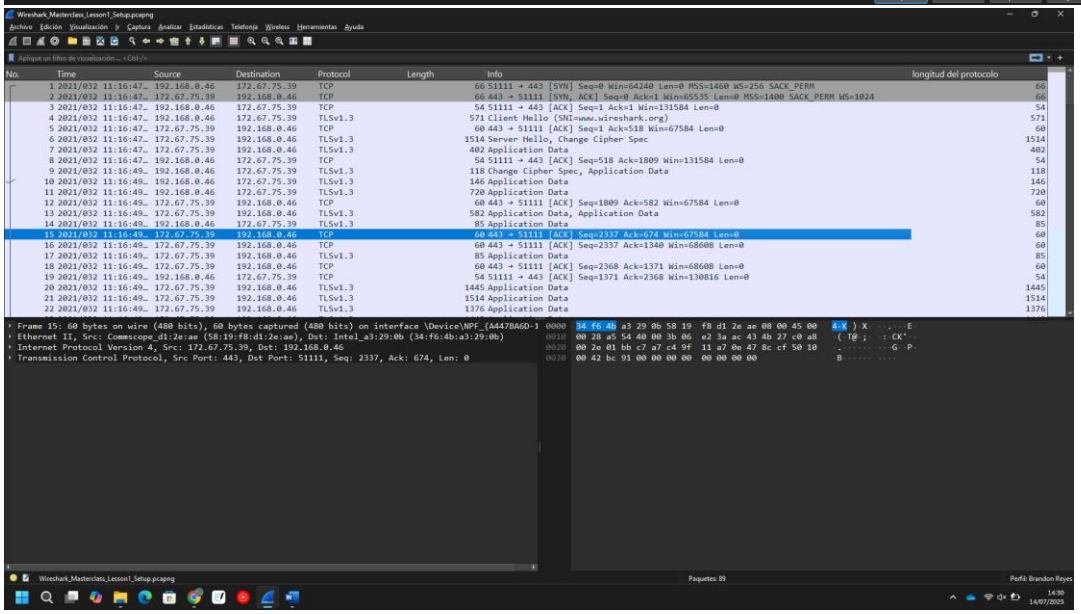
a. 

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

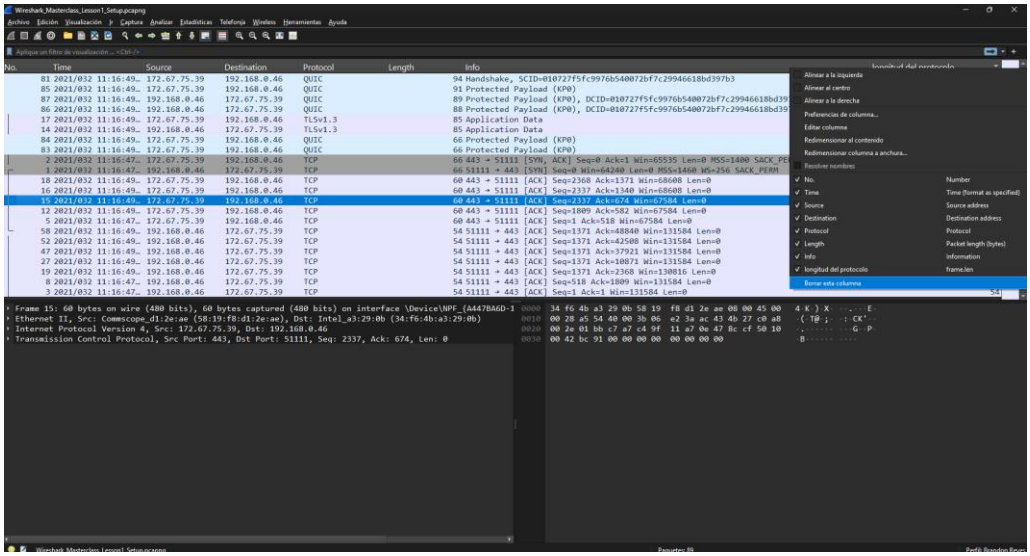
a. 

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

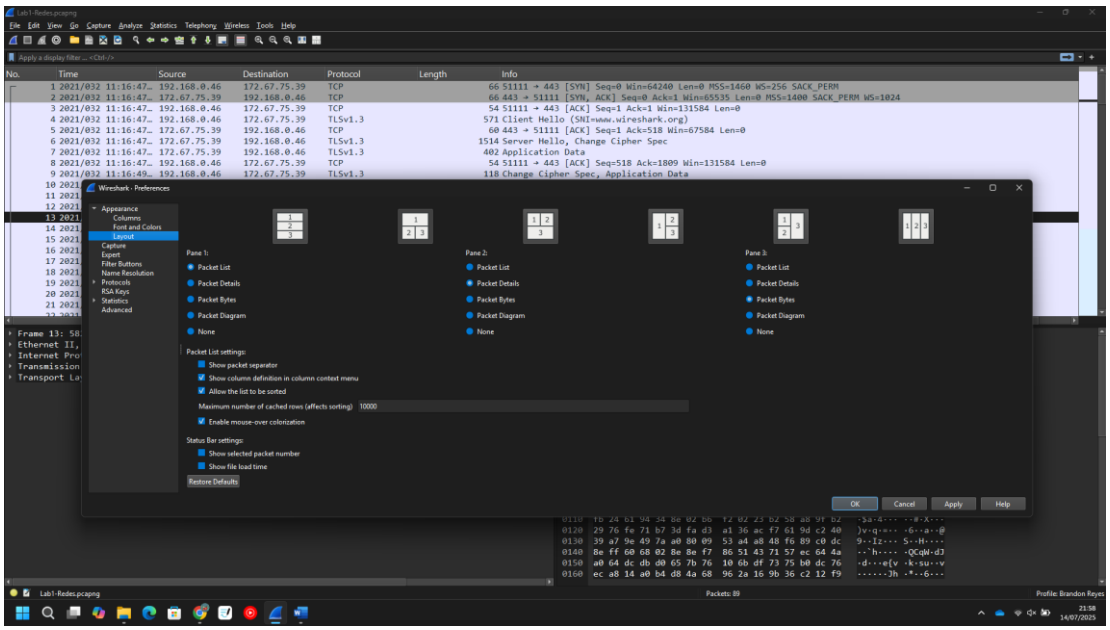
a. 

b. 

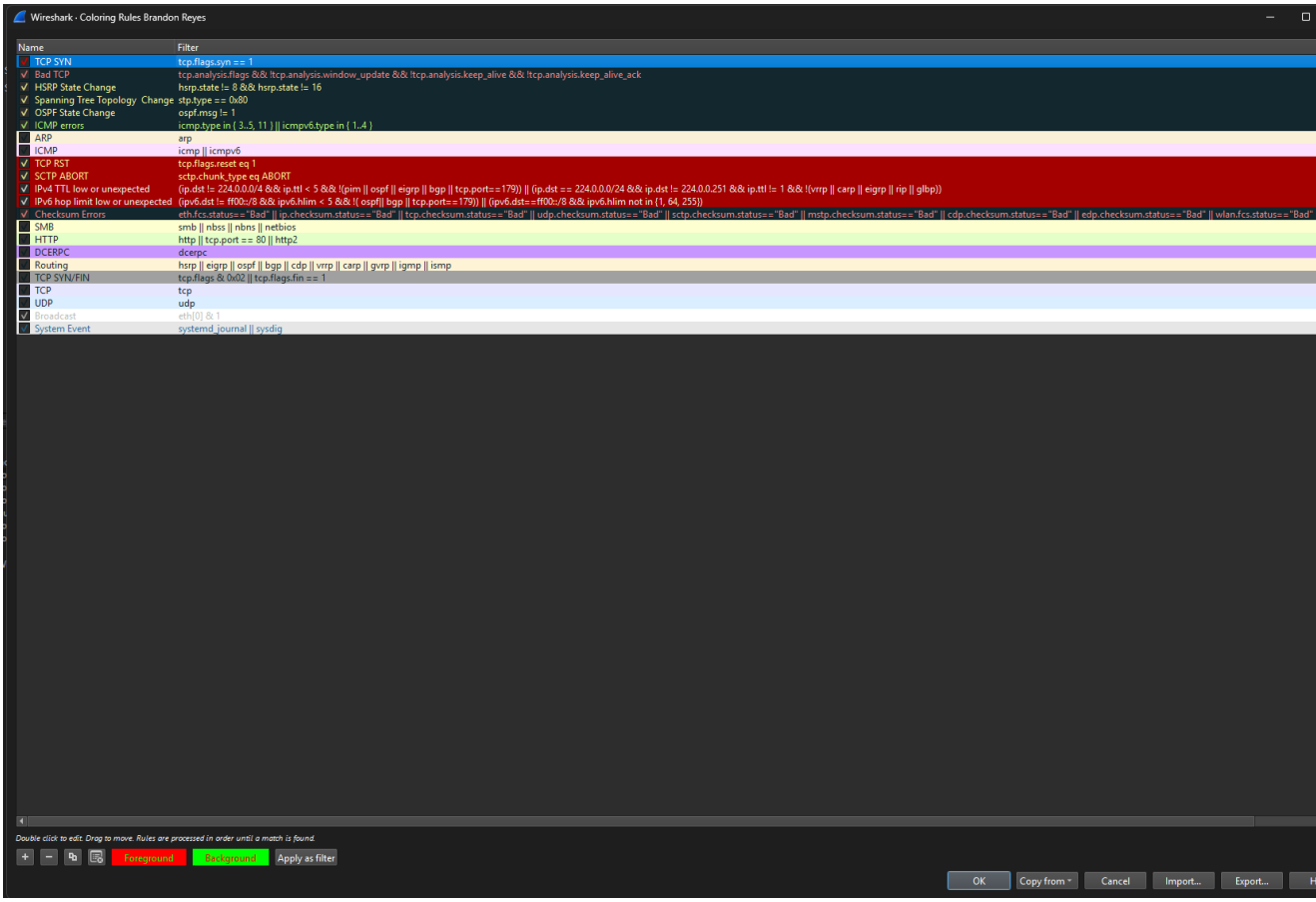
7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)

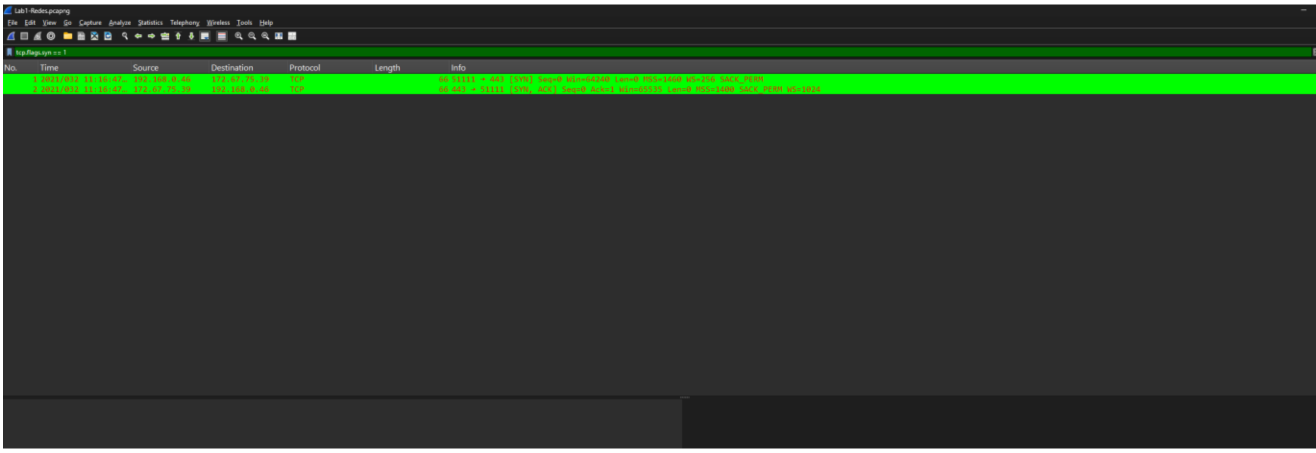
a. 

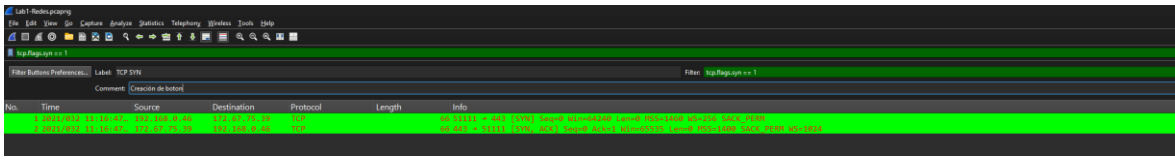
8. Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout)

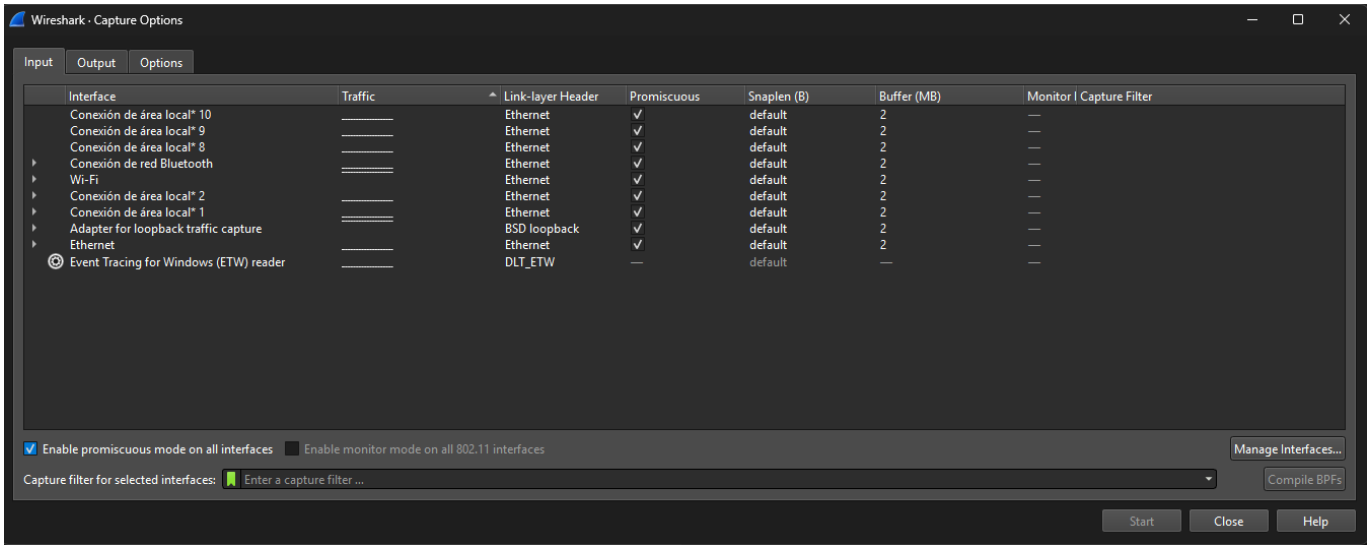
a. 

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 -> +)




Lab1-Redes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1
No. Time Source Destination Protocol Length Info
1 2021/032 11:16:47… 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 2021/032 11:16:47… 172.67.75.39 192.168.0.46 TCP 66 443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=1024

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\brand>ipconfig/all

Configuración IP de Windows

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

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
   Dirección física. . . . . . . . . . . . . : F2-A6-54-C0-AE-8D
   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 #2
   Dirección física. . . . . . . . . . . . . : F2-A6-54-C0-BE-9D
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Dirección física. . . . . . . . . . . . . : F0-A6-54-C0-8E-AD
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . : 2803:d100:e560:1290:98ae:2d11:5da5:bf19(Preferido)
   Dirección IPv6 temporal. . . . . . . . . : 2803:d100:e560:1290:49ea:6d54:769c:ed44(Preferido)
   Vínculo: dirección IPv6 local. . . . . : fe80::d341:8b41:2dc8:52e4%22(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.9(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : martes, 15 de julio de 2025 12:32:36
   La concesión expira . . . . . . . . . . . : martes, 15 de julio de 2025 15:02:35
   Puerta de enlace predeterminada . . . . . : fe80::fa63:d9ff:fe9c:d3b7%22
                                               192.168.0.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 183543380
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2B-6F-03-D4-04-BF-1B-49-AC-3C
   Servidores DNS. . . . . . . . . . . . . . : 2803:c800:0:7a::2
                                               10.240.80.254
                                               10.240.80.234
                                               2803:c800:0:7a::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. . . . . . . . . . . . . : F0-A6-54-C0-8E-AE
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí

Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Dirección física. . . . . . . . . . . . . : 04-BF-1B-49-AC-3C
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
```

```
C:\Users\brand>ipconfig

Configuración IP de Windows


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:e560:1290:98ae:2d11:5da5:bf19
   Dirección IPv6 temporal. . . . . . . : 2803:d100:e560:1290:49ea:6d54:769c:ed44
   Vínculo: dirección IPv6 local. . . . : fe80::d341:8b41:2dc8:52e4%22
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.9
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::fa63:d9ff:fe9c:d3b7%22
                                       192.168.0.1

Adaptador de Ethernet Conexión de red Bluetooth:

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

Adaptador de Ethernet Ethernet:

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

C:\Users\brand>
```

b.

c. Interfaz seleccionada: Wi-Fi – MediaTek Wi-Fi 6 MT7921

d. IPv4 192.168.0.9 – dirección asignada dinámicamente por el router doméstico.

e. Máscara 255.255.255.0 – red /24; permite 254 hosts (192.168.0.1-254).

f. Puerta de enlace 192.168.0.1 – IP del router; dirige el tráfico a Internet.

g. DHCP 192.168.0.1 – mismo router actúa como servidor DHCP.

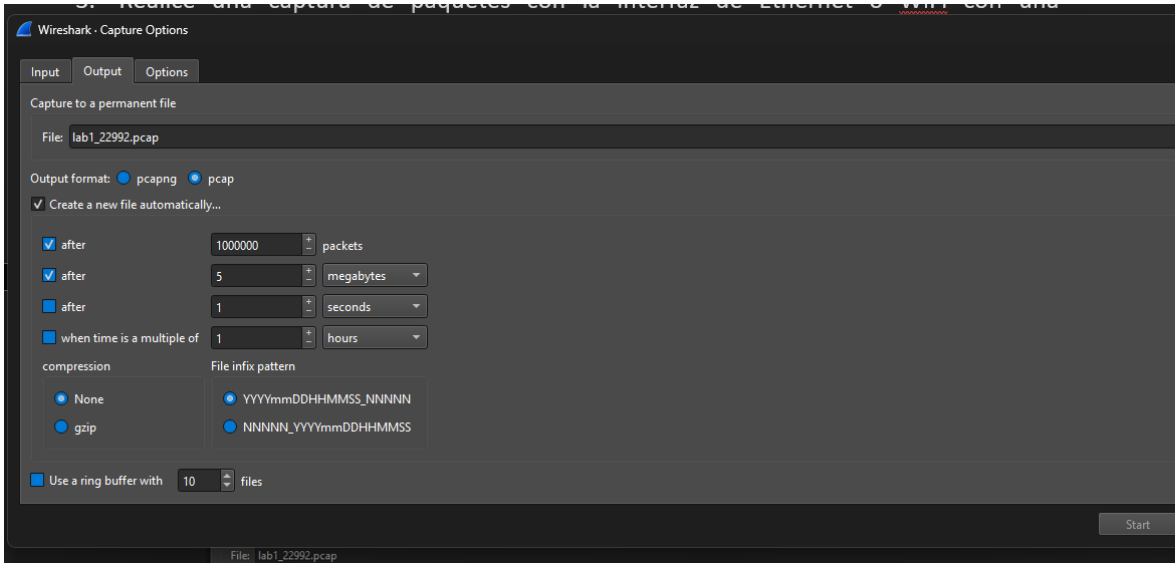
h. MAC F0-A6-54-C0-8E-AD – identificador único de la tarjeta Wi-Fi.

i. Estado: conectada; será la interfaz desde la que generaré y capturaré tráfico real.

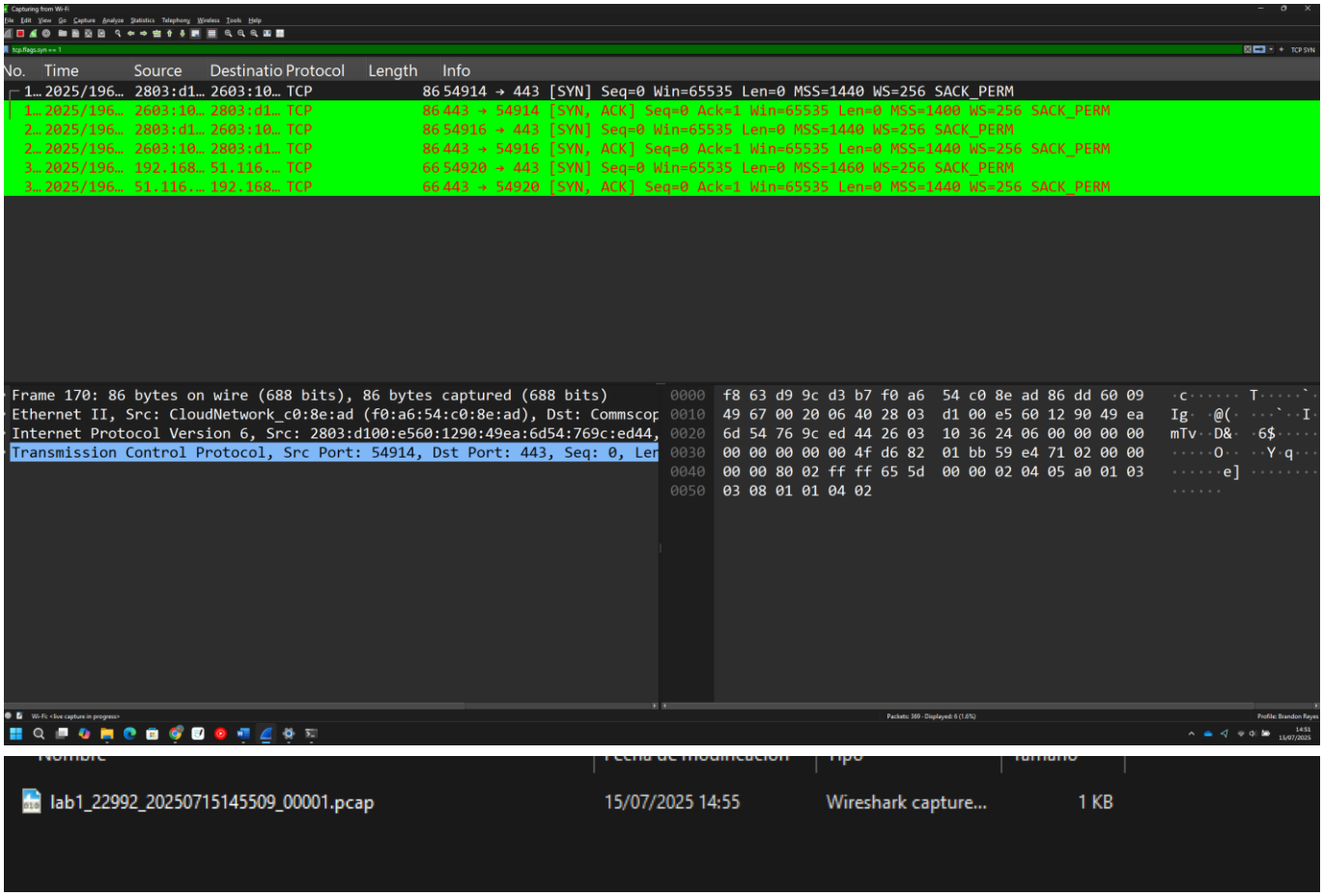
j. Las demás interfaces (Ethernet, Bluetooth, Virtual Adapters) están desconectadas o son virtuales, por lo que fueron deshabilitadas en Wireshark para evitar ruido en la captura.

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



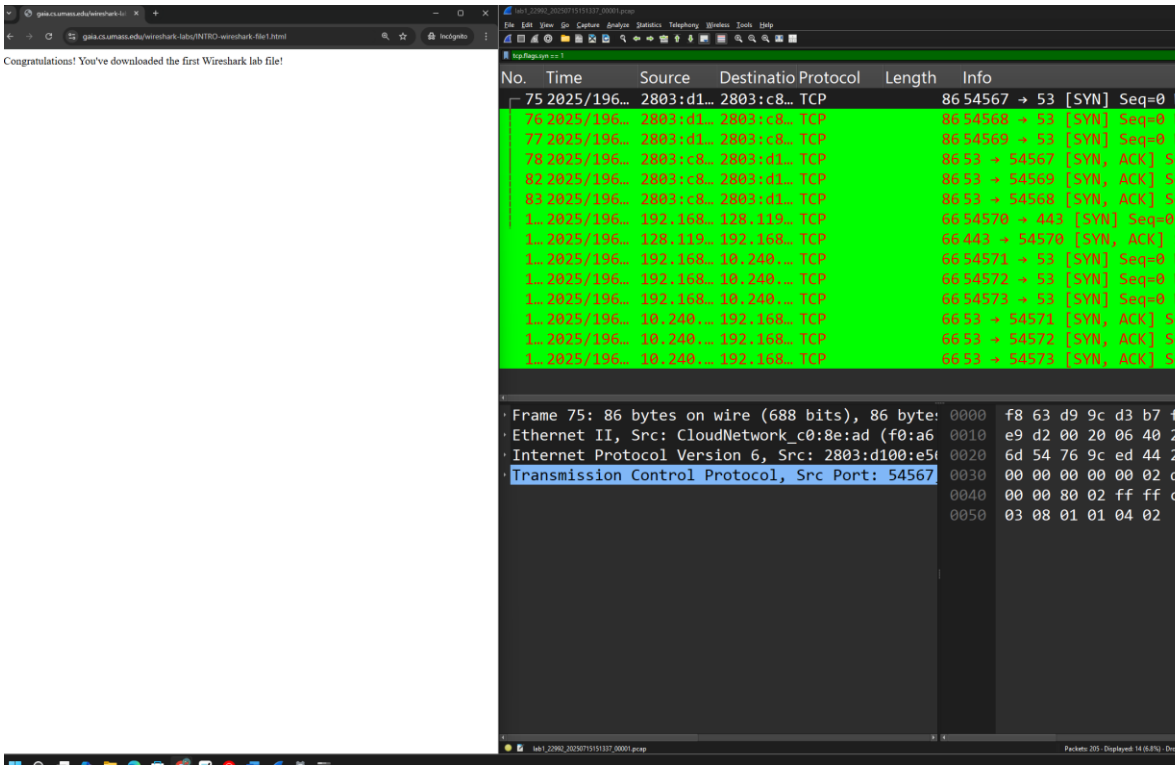
1.3 Análisis de paquetes

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

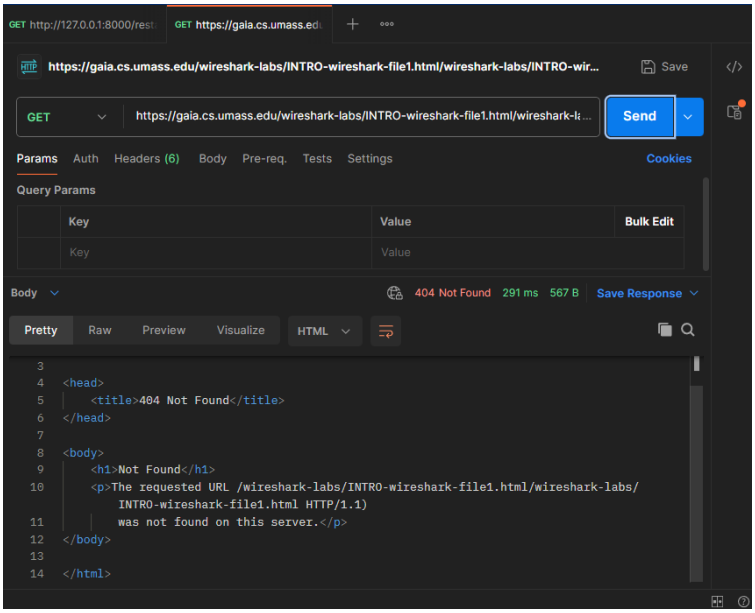
1. Abra su navegador, inicie una captura de paquetes en Wireshark (sin filtro) en la interfaz y acceda a la siguiente direccion: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

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, según el campo Content-Length en el paquete de respuesta HTTP.

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.

   En caso de presentarse problemas de rendimiento al descargar una página, lo ideal es capturar los paquetes en puntos clave de la red como un switch con port mirroring, un firewall o un router, ya que estos permiten observar todo el tráfico entre cliente y servidor. No es recomendable instalar Wireshark directamente en el servidor de producción, pues puede afectar su rendimiento, comprometer la seguridad y violar políticas de TI.

Discusión sobre la actividad

Durante este laboratorio exploré dos aspectos esenciales: la configuración personalizada de Wireshark y el análisis de tráfico HTTP. En la primera parte, aprendí a crear perfiles, columnas personalizadas (frame.len), esquemas de paneles y filtros de color para destacar paquetes SYN TCP, lo cual mejoró mucho la visualización y comprensión del tráfico. En la segunda parte, capturé tráfico real visitando un sitio de laboratorio; identifiqué la versión HTTP (1.1) en ambas direcciones, revisé encabezados como Accept-Language y el Content-Length, y comprendí cómo se intercambia la información entre cliente y servidor. El uso del modo ring buffer me permitió gestionar automáticamente archivos de captura sin llenar el disco, lo cual me pareció muy útil para sesiones prolongadas.

Comentarios:

- Wireshark demostró ser una herramienta robusta y completa. Su interfaz facilita el aprendizaje, aunque requiere tiempo y paciencia para encontrar opciones rebuscadas.

- El rendimiento puede verse afectado en equipos con mucha carga de tráfico si se captura sin filtros, y la interfaz podría resultar compleja para principiantes.

Conclusiones

- En la parte práctica, pude capturar y analizar las solicitudes y respuestas HTTP, identificando correctamente versiones, idiomas aceptados y tamaño del contenido.
- Además, comprendí las implicaciones de monitoreo de red, especialmente por qué no es conveniente instalar Wireshark en servidores de producción y cómo usarlo responsablemente desde puntos de captura adecuados.

Referencias utilizadas

- Ryufath Soepeno, Wireshark: An Effective Tool for Network Analysis, ResearchGate – utilidad en seguridad y análisis de protocolosm https://www.researchgate.net/publication/374675769_Wireshark_An_Effective_Tool_for_Network_Analysis?utm_source=chatgpt.com
- Sanchit Gurukul, Advantages, Disadvantages, and Use Cases, resumen de ventajas y limitaciones de Wireshark https://sanchitgurukul.com/exploring-wireshark-tool/?utm_source=chatgpt.com
- What is Wireshark? Applications, Features & How It Works, KnowledgeHut – impacto en el rendimiento y desventajas https://www.knowledgehut.com/blog/security/what-is-wireshark?utm_source=chatgpt.com