**Parte Individual Laboratorio**

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.

A screenshot of a computer

AI-generated content may be incorrect.

(abajo a la derecha se ve mi perfil)

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

A screenshot of a computer

AI-generated content may be incorrect.

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

A computer screen shot of a computer

AI-generated content may be incorrect.

7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna) 8A screenshot of a computer

AI-generated content may be incorrect.

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

A screenshot of a computer

AI-generated content may be incorrect.

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 screenshot of a computer

AI-generated content may be incorrect.

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

A screenshot of a computer

AI-generated content may be incorrect.

Parte 1.2

Descripción del ipconfig /all

La salida del comando ipconfig en mi computadora revela que el equipo, identificado como DESKTOP-LCA4PCQ y ejecutando Windows 10 versión 19045.6093, opera en modo híbrido sin enrutamiento IP ni proxy WINS. Entre los adaptadores detectados se incluyen:

* VirtualBox Host-Only Ethernet Adapter, con IPv4 X.X.X.X/24 y sin puerta de enlace, usado para las redes internas de las máquinas virtuales.
* Dos Microsoft Wi-Fi Direct Virtual Adapter en estado “medios desconectados”, que no participan en el tráfico habitual.
* El adaptador físico Intel(R) Wi-Fi 6 AX201 160MHz, configurado por DHCP con IPv4 X.X.X.X/24, puerta de enlace X.X.X.X y DNS X.X.X.X, que es el único que se conecta a Internet.
* Un adaptador Bluetooth Device (Personal Area Network) desconectado.
* El adaptador vEthernet (WSL) de Hyper-V, con IPv4 X.X.X.X/20 y sin puerta de enlace, empleado internamente por el Subsistema de Linux en Windows.

A screenshot of a computer program

AI-generated content may be incorrect.

Desmarcar todo

A screenshot of a computer

AI-generated content may be incorrect.

Capturas hechas

A black screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Parte 1.3**

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).



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

3. Responda las siguientes preguntas:

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

Al inspeccionar la primera petición GET en Wireshark (p. ej. la línea con

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

se ve que el navegador está usando HTTP/1.1.

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

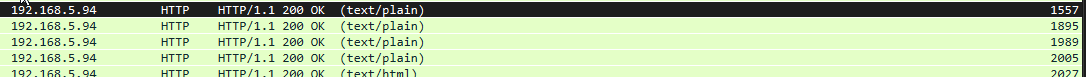
En la respuesta correspondiente ( HTTP/1.1 200 OK), el servidor también responde con HTTP/1.1.

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

Accept-Language: es-ES,es;q=0.9,en;q=0.8

lo que indica que el navegador prefiere Español de España, luego Español genérico y después Inglés.

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



En la respuesta al GET /wireshark-labs/INTRO-wireshark-file1.html (donde el Content-Type es text/html), la columna Length de Wireshark muestra 2027 bytes. Por lo tanto, el servidor devolvió 2027 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.

* Puntos de captura recomendados

1. En el cliente (tu máquina): para medir la experiencia de usuario real.
2. En un puerto espejo (SPAN) del switch o enrutador que une cliente y servidor: así capturas todo el tráfico sin interferir en ninguno de los extremos.

* Instalar Wireshark en el servidor
  + No es recomendable en un entorno de producción, porque:
    - Consume CPU y disco justo donde debe atender peticiones.
    - Puede interferir con el rendimiento de la aplicación.
    - Existe riesgo de exponer datos sensibles.
  + Es mejor usar una sonda dedicada o un puerto espejo para hacer la captura de forma pasiva.