Gerardo Pineda 22880

Laboratorio 1 – Parte 2

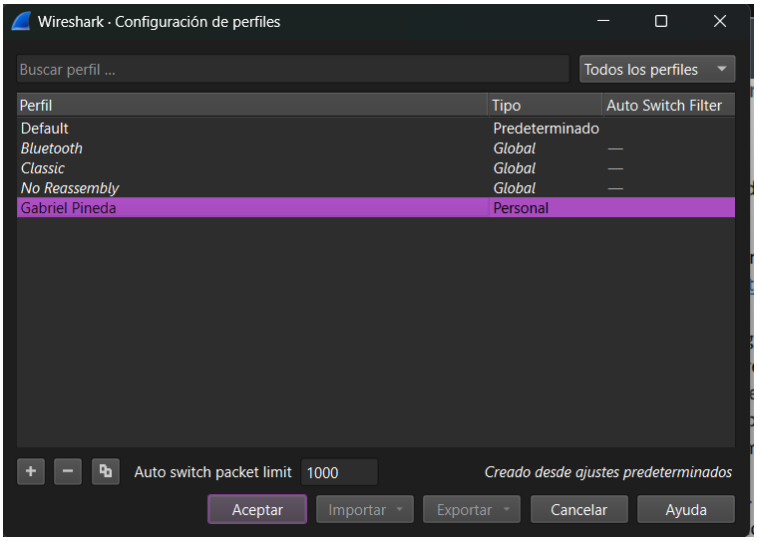
Introducción

El propósito de este laboratorio fue familiarizarse con la herramienta Wireshark mediante la personalización del entorno, la configuración de interfaces de red y la captura y análisis de paquetes reales. A través de distintas actividades prácticas, se buscó reforzar los conceptos teóricos sobre redes y protocolos, observando de forma directa cómo se transmite la información en una red local.

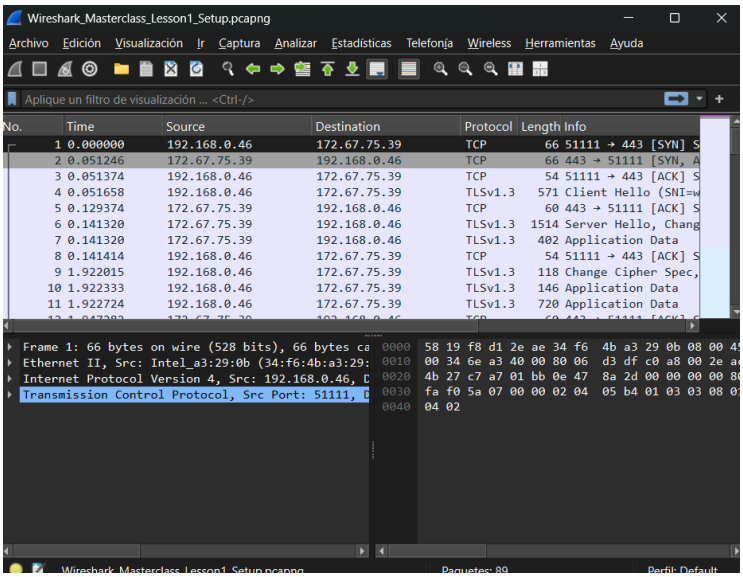
Capturas y evidencias

1.1personalización de entorno

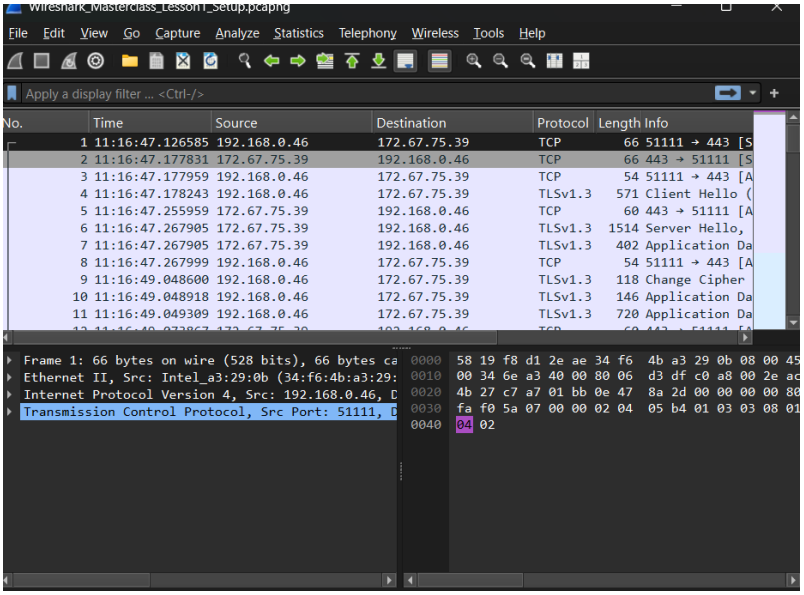
1.
2.



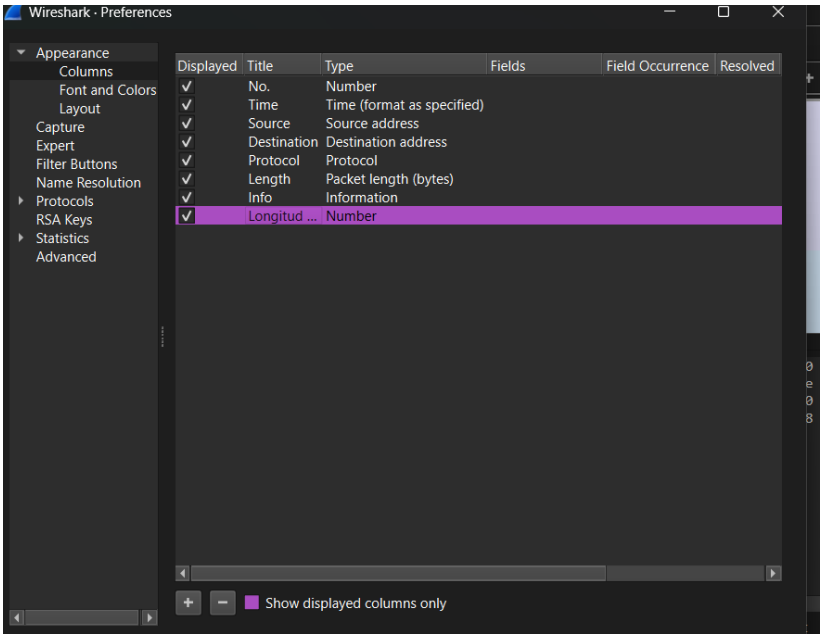
3.
4.


Wireshark_Masterclass_Lesson1_Setup.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.46 172.67.75.39 TCP 66 51111 → 443 [SYN] S
2 0.051246 172.67.75.39 192.168.0.46 TCP 66 443 → 51111 [SYN, A
3 0.051374 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] S
4 0.051658 192.168.0.46 172.67.75.39 TLSv1.3 571 Client Hello (SNI=w
5 0.129374 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] S
6 0.141320 172.67.75.39 192.168.0.46 TLSv1.3 1514 Server Hello, Chang
7 0.141320 172.67.75.39 192.168.0.46 TLSv1.3 402 Application Data
8 0.141414 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] S
9 1.922015 192.168.0.46 172.67.75.39 TLSv1.3 118 Change Cipher Spec,
10 1.922333 192.168.0.46 172.67.75.39 TLSv1.3 146 Application Data
11 1.922724 192.168.0.46 172.67.75.39 TLSv1.3 720 Application Data
Frame 1: 66 bytes on wire (528 bits), 66 bytes ca
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:
Internet Protocol Version 4, Src: 192.168.0.46, D
Transmission Control Protocol, Src Port: 51111, D
0000 58 19 f8 d1 2e ae 34 f6 4b a3 29 0b 08 00 45
0010 00 34 6e a3 40 00 80 06 d3 df c0 a8 00 2e ac
0020 4b 27 c7 a7 01 bb 0e 47 8a 2d 00 00 00 00 80
0030 fa f0 5a 07 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02
Wireshark_Masterclass_Lesson1_Setup.pcapng
Paquetes: 89
Perfil: Default

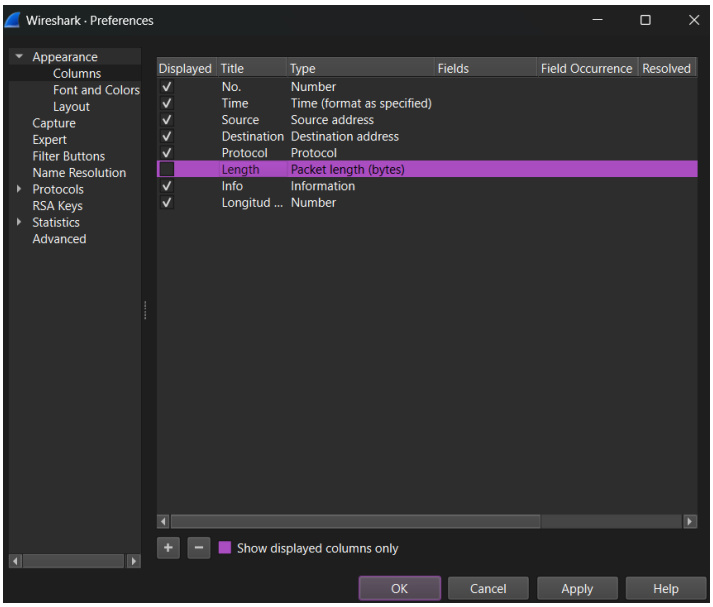
5.


Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 11:16:47.126585 192.168.0.46 172.67.75.39 TCP 66 51111 → 443 [S
2 11:16:47.177831 172.67.75.39 192.168.0.46 TCP 66 443 → 51111 [S
3 11:16:47.177959 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [A
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 [A
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 Da
8 11:16:47.267999 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [A
9 11:16:49.048600 192.168.0.46 172.67.75.39 TLSv1.3 118 Change Cipher
10 11:16:49.048918 192.168.0.46 172.67.75.39 TLSv1.3 146 Application Da
11 11:16:49.049309 192.168.0.46 172.67.75.39 TLSv1.3 720 Application Da
Frame 1: 66 bytes on wire (528 bits), 66 bytes ca
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:
Internet Protocol Version 4, Src: 192.168.0.46, D
Transmission Control Protocol, Src Port: 51111, D
0000 58 19 f8 d1 2e ae 34 f6 4b a3 29 0b 08 00 45
0010 00 34 6e a3 40 00 80 06 d3 df c0 a8 00 2e ac
0020 4b 27 c7 a7 01 bb 0e 47 8a 2d 00 00 00 00 80
0030 fa f0 5a 07 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02

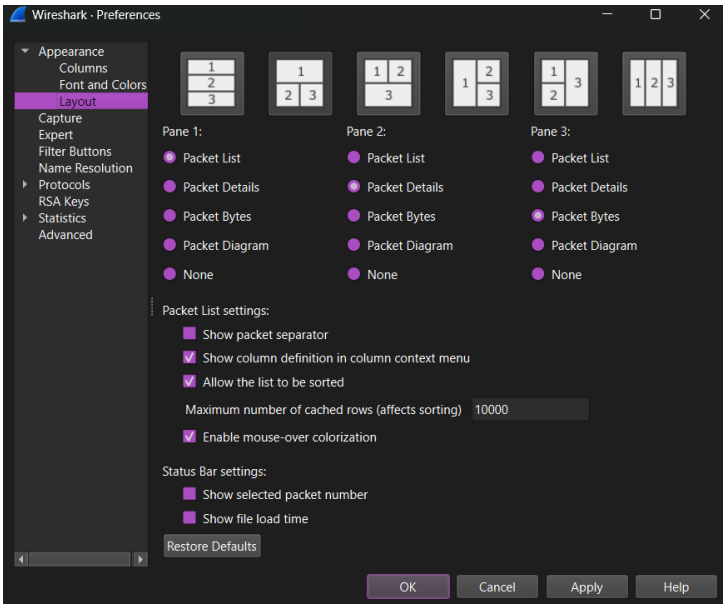
6.



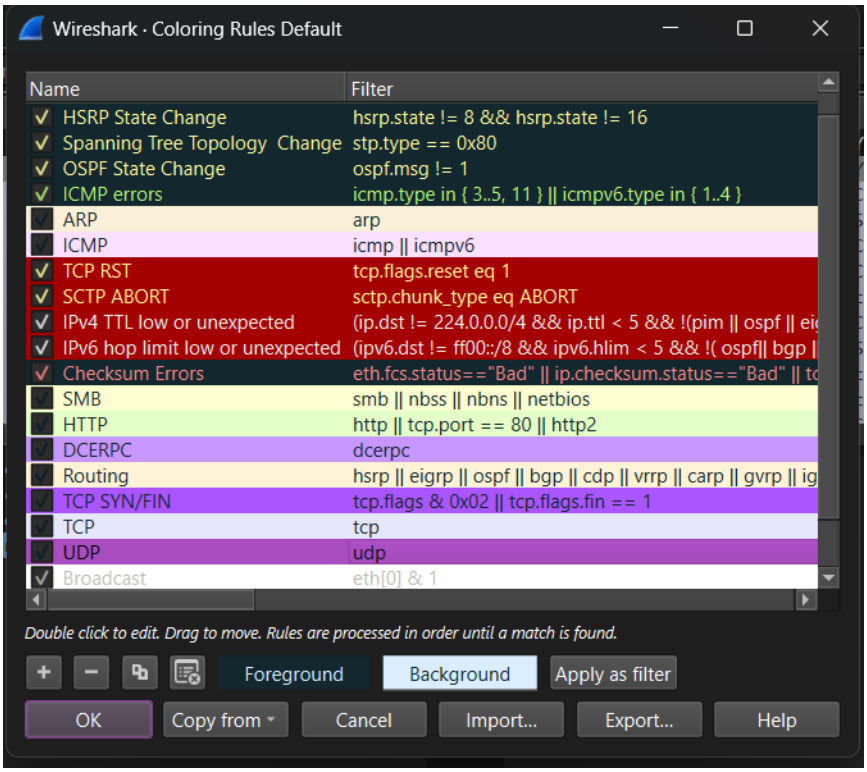
7.



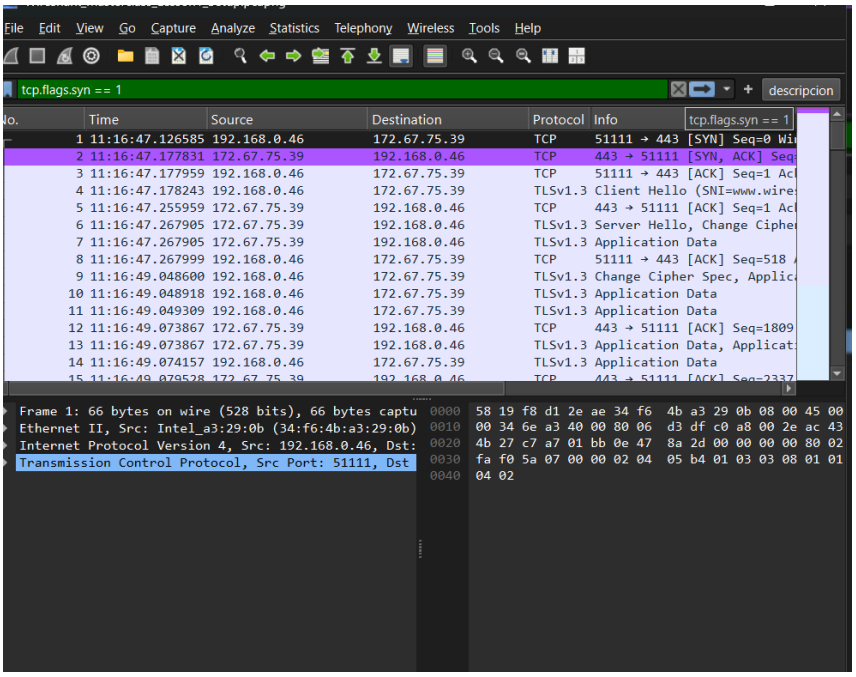
8. Elegí el layout 2



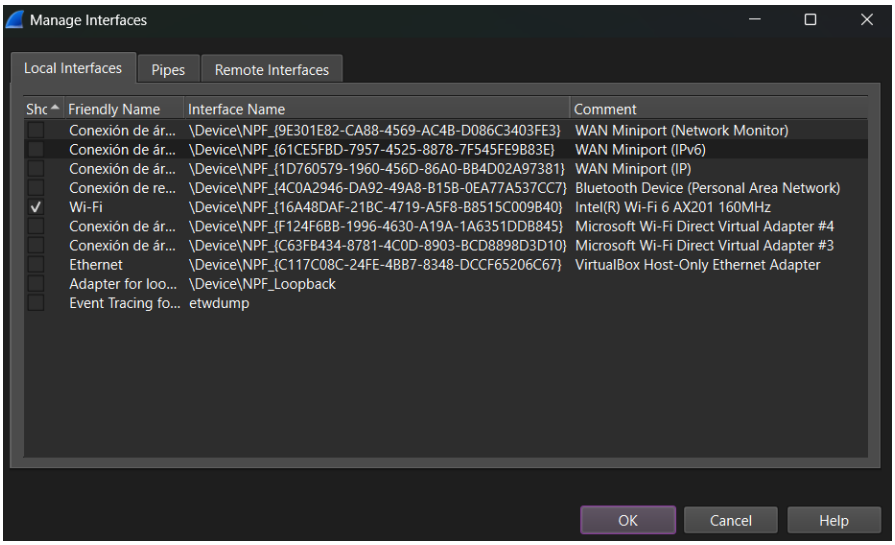
9.

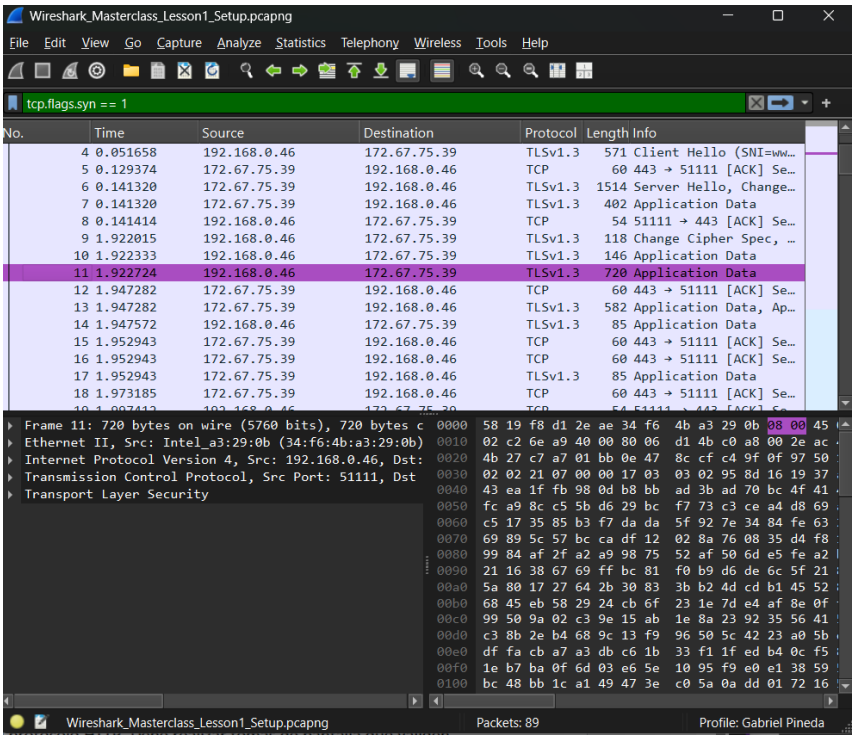


10. El botón se llama descripción (ahí esta a la derecha)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1
descripcion
No. Time Source Destination Protocol Info
1 11:16:47.126585 192.168.0.46 172.67.75.39 TCP 51111 → 443 [SYN] Seq=0
2 11:16:47.177831 172.67.75.39 192.168.0.46 TCP 443 → 51111 [SYN, ACK]
3 11:16:47.177959 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK]
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 [ACK]
6 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 Server Hello, Change Cipher
7 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
8 11:16:47.267999 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK]
9 11:16:49.048600 192.168.0.46 172.67.75.39 TLSv1.3 Change Cipher Spec, Application Data
10 11:16:49.048918 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
11 11:16:49.049309 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
12 11:16:49.073867 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK]
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
Frame 1: 66 bytes on wire (528 bits), 66 bytes captu
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Internet Protocol Version 4, Src: 192.168.0.46, Dst:
Transmission Control Protocol, Src Port: 51111, Dst
0000 58 19 f8 d1 2e ae 34 f6 4b a3 29 0b 08 00 45 00
0010 00 34 6e a3 40 00 80 06 d3 df c0 a8 00 2e ac 43
0020 4b 27 c7 a7 01 bb 0e 47 8a 2d 00 00 00 00 80 02
0030 fa f0 5a 07 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02

11.


Manage Interfaces
Local Interfaces
Pipes
Remote Interfaces
Shc
Friendly Name
Interface Name
Comment
Conexión de ár... \Device\NPF_{9E301E82-CA88-4569-AC4B-D086C3403FE3} WAN Miniport (Network Monitor)
Conexión de ár... \Device\NPF_{61CE5FBD-7957-4525-8878-7F545FE9B83E} WAN Miniport (IPv6)
Conexión de ár... \Device\NPF_{1D760579-1960-456D-86A0-BB4D02A97381} WAN Miniport (IP)
Conexión de re... \Device\NPF_{4C0A2946-DA92-49A8-B15B-0EA77A537CC7} Bluetooth Device (Personal Area Network)
Wi-Fi \Device\NPF_{16A48DAF-21BC-4719-A5F8-B8515C009B40} Intel(R) Wi-Fi 6 AX201 160MHz
Conexión de ár... \Device\NPF_{F124F6BB-1996-4630-A19A-1A6351DDB845} Microsoft Wi-Fi Direct Virtual Adapter #4
Conexión de ár... \Device\NPF_{C63FB434-8781-4C0D-8903-BCD8898D3D10} Microsoft Wi-Fi Direct Virtual Adapter #3
Ethernet \Device\NPF_{C117C08C-24FE-4BB7-8348-DCCF65206C67} VirtualBox Host-Only Ethernet Adapter
Adapter for loo... \Device\NPF_Loopback
Event Tracing fo... etwdump
OK
Cancel
Help



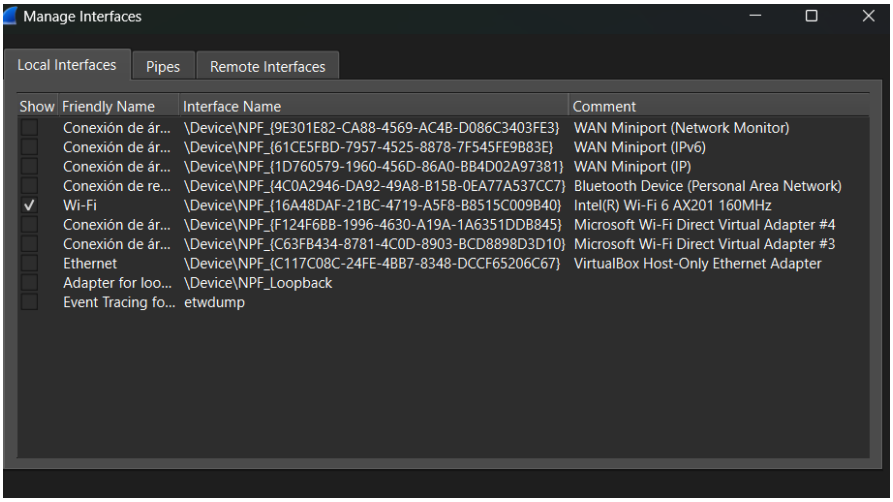
1.2Configuración de la captura de paquetes

```
C:\Users\Gerax>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::31d6:52af:b053:85a9%18
   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* 3:

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

Adaptador de LAN inalámbrica Conexión de área local* 4:

   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:c800:4191:7f6b:ae2f:d79d:9bce:5bb9
   Dirección IPv6 temporal. . . . . . . . . . : 2803:c800:4191:7f6b:3c7b:af47:5347:8032
   Vínculo: dirección IPv6 local. . . : fe80::b85c:d464:2fe4:c9c7%6
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.171.121
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::ac87:d6ff:fe5f:548e%6
                                               192.168.171.38

Adaptador de Ethernet Conexión de red Bluetooth:

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

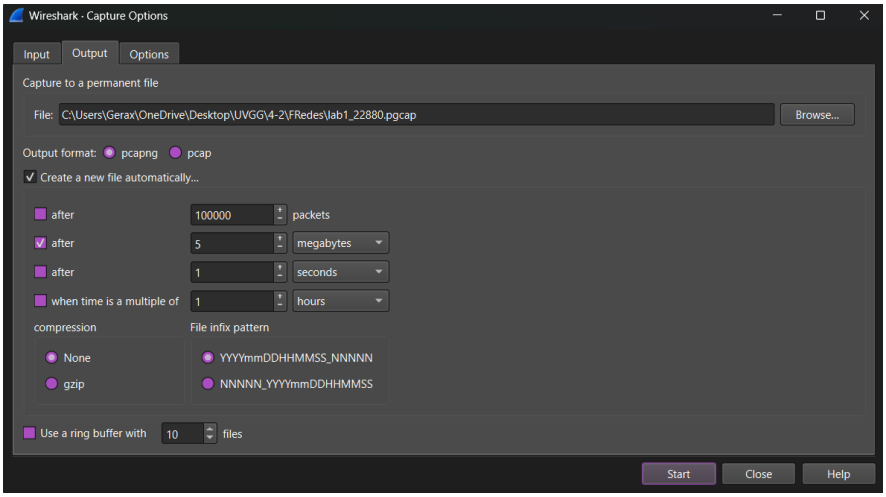
Detalle y explique lo observado

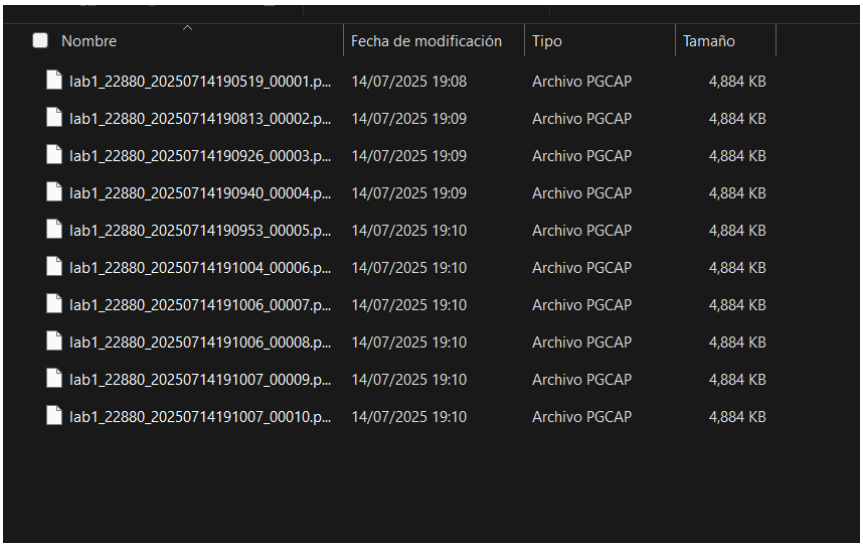
Al crear ejecutar el comando esta muestra información sobre cada adaptador de red activo. Aquí se muestra la dirección Ipv4 y una dirección pv6 de enlace local, pero tiene puertas de enlace configuradas, lo que se usa para conexiones internas. Se muestra que el adaptador LAN inalámbrico de wifi si está en uso y tiene configuradas varias direcciones ip. también muestra el adaptador de blutooth también esta desconectado, por lo que no muestra configuraciones activas.

2.


Manage Interfaces
Local Interfaces
Pipes
Remote Interfaces
Show
Friendly Name
Interface Name
Comment
Conexión de ár... \Device\NPF_{9E301E82-CA88-4569-AC4B-D086C3403FE3} WAN Miniport (Network Monitor)
Conexión de ár... \Device\NPF_{61CE5FBD-7957-4525-8878-7F545FE9B83E} WAN Miniport (IPv6)
Conexión de ár... \Device\NPF_{1D760579-1960-456D-86A0-BB4D02A97381} WAN Miniport (IP)
Conexión de re... \Device\NPF_{4C0A2946-DA92-49A8-B15B-0EA77A537CC7} Bluetooth Device (Personal Area Network)
Wi-Fi \Device\NPF_{16A48DAF-21BC-4719-A5F8-B8515C009B40} Intel(R) Wi-Fi 6 AX201 160MHz
Conexión de ár... \Device\NPF_{F124F6BB-1996-4630-A19A-1A6351DDB845} Microsoft Wi-Fi Direct Virtual Adapter #4
Conexión de ár... \Device\NPF_{C63FB434-8781-4C0D-8903-BCD8898D3D10} Microsoft Wi-Fi Direct Virtual Adapter #3
Ethernet \Device\NPF_{C117C08C-24FE-4BB7-8348-DCCF65206C67} VirtualBox Host-Only Ethernet Adapter
Adapter for loo... \Device\NPF_Loopback
Event Tracing fo... etwdump

3.


Wireshark · Capture Options
Input
Output
Options
Capture to a permanent file
File: C:\Users\Gerax\OneDrive\Desktop\UVGG\4-2\FRedes\lab1_22880.pgcap
Browse...
Output format: pcapng pcap
Create a new file automatically...
after 100000 packets
after 5 megabytes
after 1 seconds
when time is a multiple of 1 hours
compression
File infix pattern
None
gzip
YYYYmmDDHHMMSS_NNNNN
NNNNN_YYYYmmDDHHMMSS
Use a ring buffer with 10 files
Start
Close
Help


Nombre
Fecha de modificación
Tipo
Tamaño
lab1_22880_20250714190519_00001.p... 14/07/2025 19:08 Archivo PGCAP 4,884 KB
lab1_22880_20250714190813_00002.p... 14/07/2025 19:09 Archivo PGCAP 4,884 KB
lab1_22880_20250714190926_00003.p... 14/07/2025 19:09 Archivo PGCAP 4,884 KB
lab1_22880_20250714190940_00004.p... 14/07/2025 19:09 Archivo PGCAP 4,884 KB
lab1_22880_20250714190953_00005.p... 14/07/2025 19:10 Archivo PGCAP 4,884 KB
lab1_22880_20250714191004_00006.p... 14/07/2025 19:10 Archivo PGCAP 4,884 KB
lab1_22880_20250714191006_00007.p... 14/07/2025 19:10 Archivo PGCAP 4,884 KB
lab1_22880_20250714191006_00008.p... 14/07/2025 19:10 Archivo PGCAP 4,884 KB
lab1_22880_20250714191007_00009.p... 14/07/2025 19:10 Archivo PGCAP 4,884 KB
lab1_22880_20250714191007_00010.p... 14/07/2025 19:10 Archivo PGCAP 4,884 KB

1.3

¿Qué versión de HTTP está ejecutando su navegador?

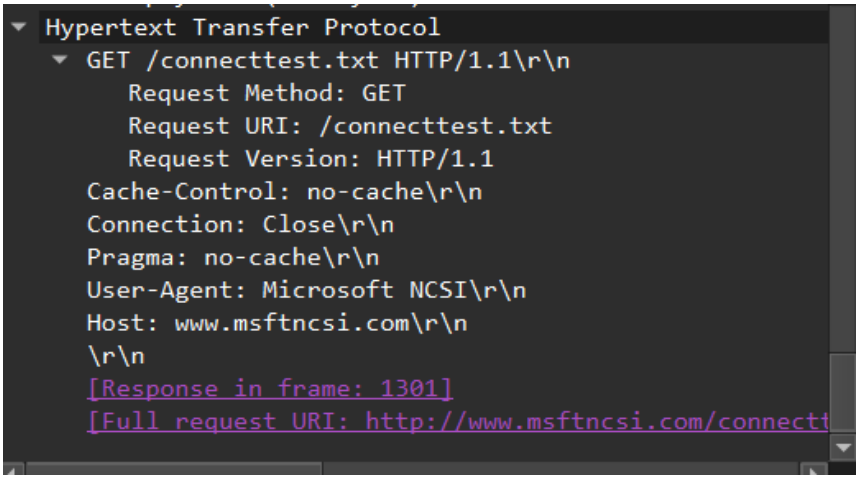
Http/1.1

¿Qué versión de HTTP está ejecutando el servidor?

Http/1.1

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

No tengo lenguajes



¿Cuántos bytes de contenido fueron devueltos por el servidor?

22 bytes

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.

El primero lugar en el que conviene escuchar los paquetes es el cliente, capturar el trafico desde el permite observar el tiempo de resolución de DNS, la latencia de conexión, los retrasos de protocolo http/https. No, no es conveniente, este puede afecta el rendimiento, representar un riesgo de seguridad y dificultad el análisis si el servidor atiende múltiples usuarios al mismo tiempo.

Discusión

Durante el laboratorio se hicieron varias actividades para familiarizarse con el eterno Wireshark. En la primera parte se realizaron instrucciones varias como cambiar de color, personalizar la interfaz y programar el entorno de captura de interfaces virtuales.

Durante la segunda parte del laboratorio se realizo una captura de paquetes con un ring buffer, primero se solicitaba realizar el comando ipconfig que devuelve la información sobre los adaptadores de red. Además, se realizaron 10 archivos de captura de la interfaz de wifi generados por el tráfico del internet. Por último, se realizó otra captura de paquetes, pero esta vez desde una pagina web especifica donde se solicito un archivo a ser descargado.

Se logro aprender sobre el software Wireshark, logrando interactuar de forma adecuada con el entorno y configurando adecuadamente paso a paso. Creando un perfil especifico para el entorno. Creando archivos de captura de la red, donde se guardan específicamente ciertas acciones hechas.

Durante el laboratorio se encontraron varias dificultades, como que el buscador Edge por defecto busca https por lo tanto fue un reto lograr descargar el archivo. Otro reto para tomar en cuenta fue la configuración de la captura de la interfaz de wifi. Debido a que estos salían de vez en cuando y era de pura suerte lograr configurarlo de forma adecuada. Además, algunas instrucciones estaban ambiguas o incompletas lo que hacía que algunos pasos fueran inciertos.

Comentarios

En lo personal, este laboratorio no me gusto considero que algunos pasos a seguir eran ambiguos o a creatividad de nosotros para entender dónde estaban ciertas cosas. Adicionalmente agregaría un primer paso que es configurar en ingles el sistema porque en español son muy distintas algunas cosas. La parte de http hay que aclarar de mejor forma como se hace porque es muy al azar la forma en la que función y NO función en cualquier navegador. En mi computadora solo tengo Edge porque no me interesa instalar otro, pero este fue un reto intentar obtener esto.

Conclusiones

- Se logro comprender el funcionamiento de Wireshark
- La práctica permitió reforzar conocimientos teóricos del tráfico de la red
- El análisis de protocolo como Http permitió ver en detalle como se realizaban las transferencias en la web

Referencias

Walton, A. (2018, 13 abril). ¿Qué es y cómo usar el comando IPCONFIG en Windows? | Blog Redes. *CCNA desde Cero*. https://ccnadesdecero.es/usar-comando-ipconfig-windows/