Angela Garcia, 22869

Laboratorio 1 - Parte 2

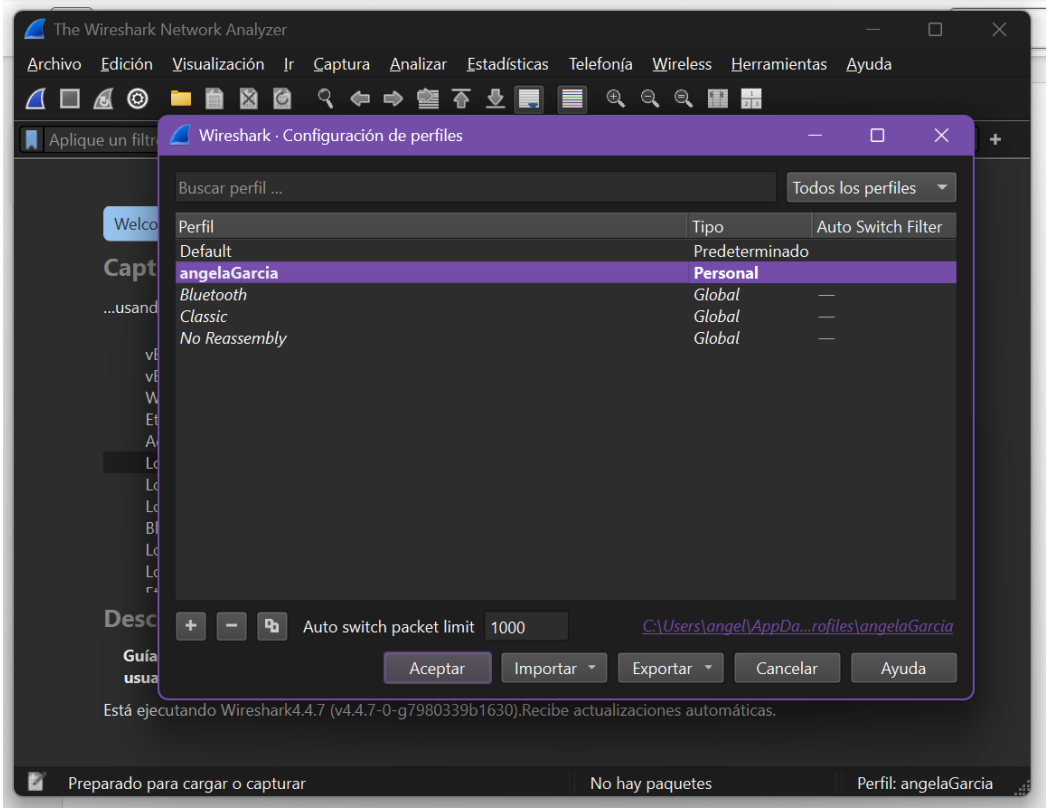
Introducción

Wireshark es una herramienta que permite analizar y capturar el tráfico en la red creada por Gerald Combs. Su principal uso es para saber que es lo que está pasando en la red: desde como detectar problemas de conexión, ver paquetes de datos que se envían y reciben, monitorear redes, generar estadísticas acerca del tráfico de la red, exportar datos, análisis de protocolos, aplicación de filtros en el tráfico.

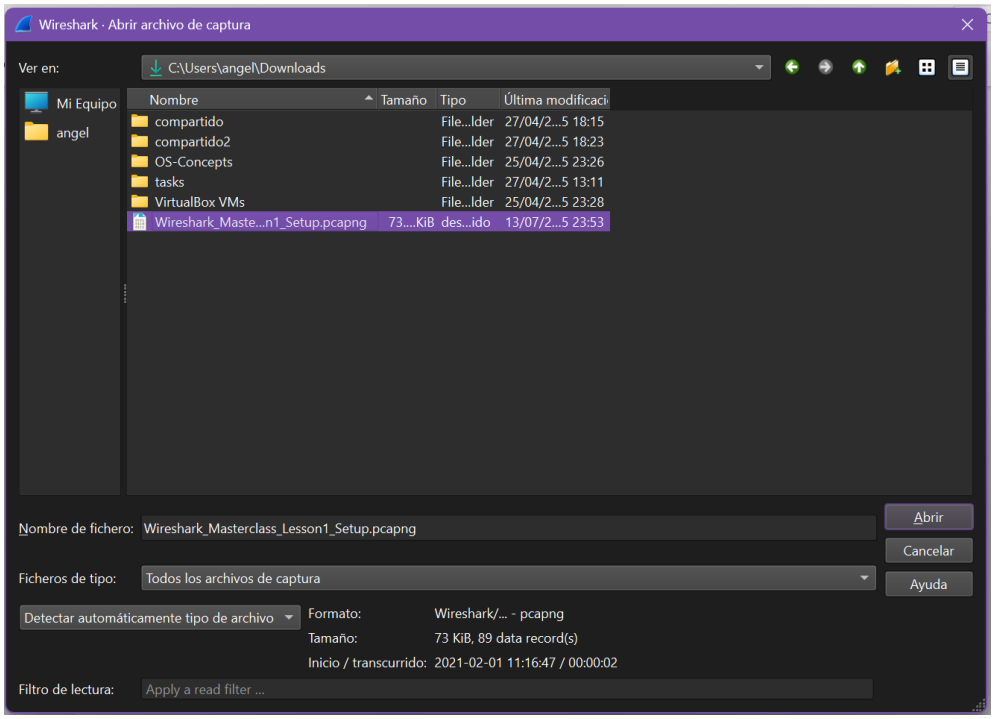
Capturas y evidencia

1.1 Personalización del entorno

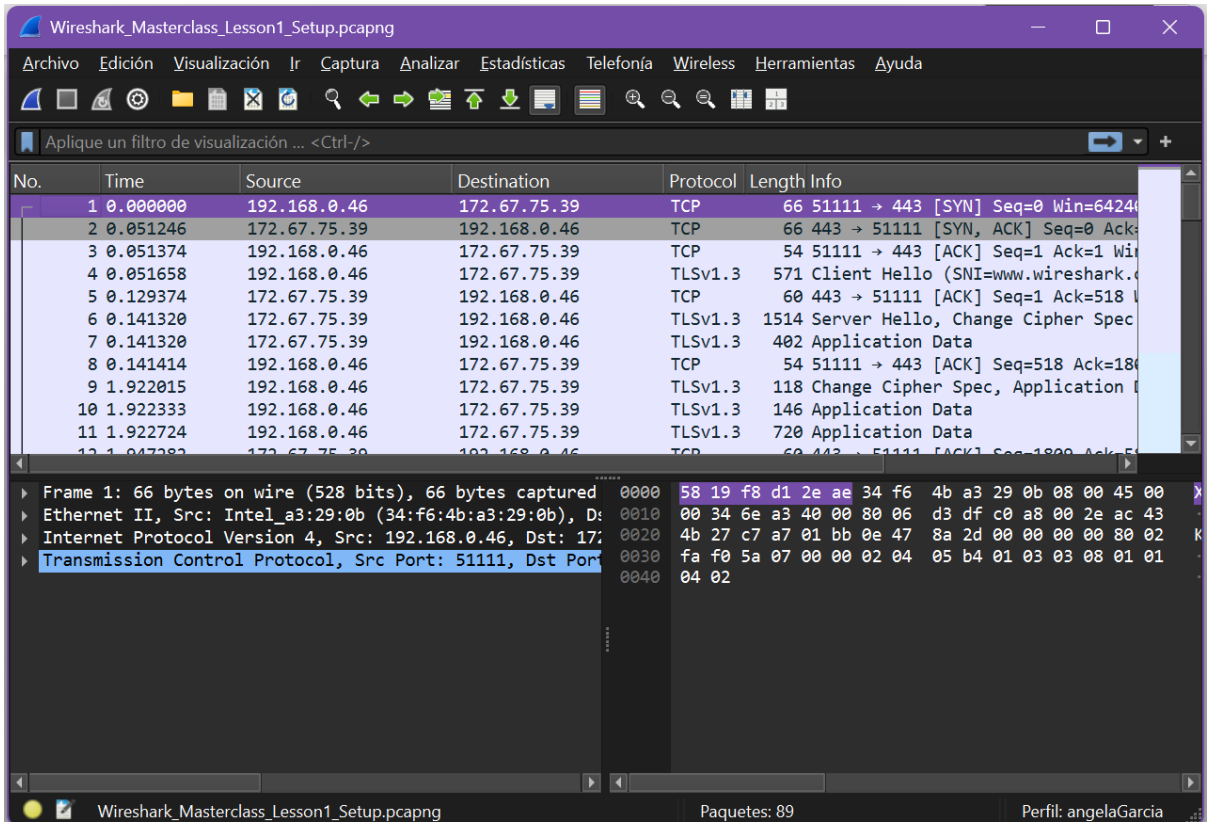
2.



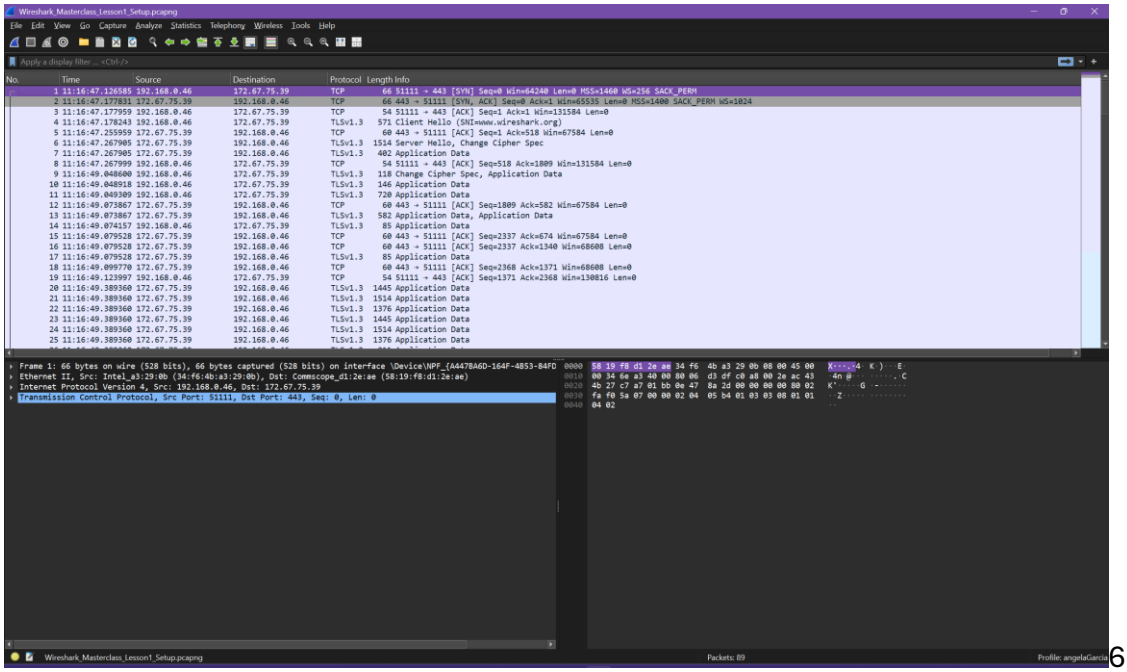
3.


Wireshark · Abrir archivo de captura
Ver en:
C:\Users\angel\Downloads
Mi Equipo
angel
Nombre
Tamaño
Tipo
Última modificaci
compartido
File...lder
27/04/2...5 18:15
compartido2
File...lder
27/04/2...5 18:23
OS-Concepts
File...lder
25/04/2...5 23:26
tasks
File...lder
27/04/2...5 13:11
VirtualBox VMs
File...lder
25/04/2...5 23:28
Wireshark_Maste...n1_Setup.pcapng
73....KiB
des...ido
13/07/2...5 23:53
Nombre de fichero:
Wireshark_Masterclass_Lesson1_Setup.pcapng
Abrir
Cancelar
Ficheros de tipo:
Todos los archivos de captura
Ayuda
Detectar automáticamente tipo de archivo
Formato:
Wireshark/... - pcapng
Tamaño:
73 KiB, 89 data record(s)
Inicio / transcurrido:
2021-02-01 11:16:47 / 00:00:02
Filtro de lectura:
Apply a read filter ...

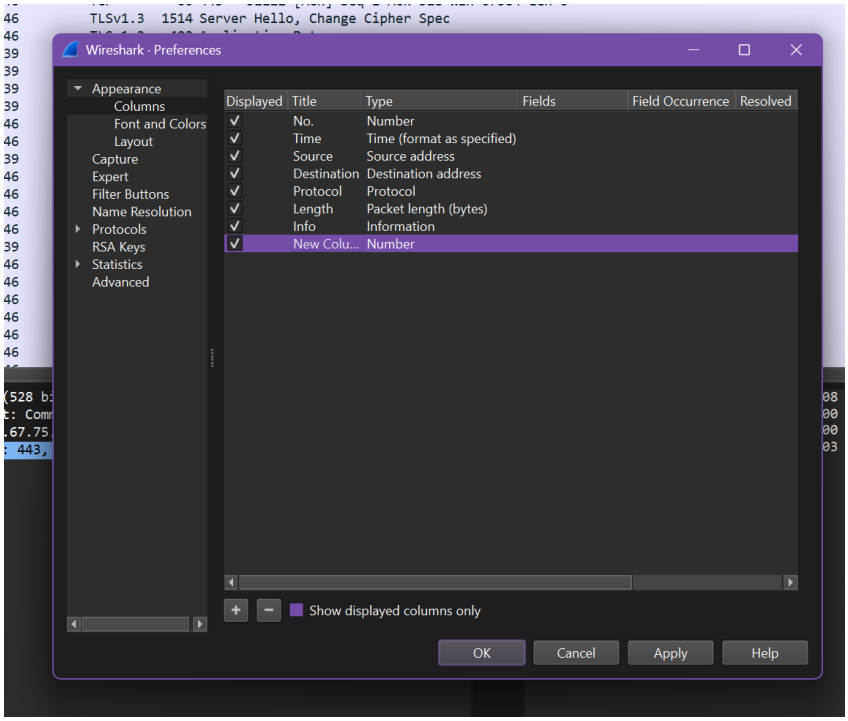
4.


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] Seq=0 Win=64240
2 0.051246 172.67.75.39 192.168.0.46 TCP 66 443 → 51111 [SYN, ACK] Seq=0 Ack=
3 0.051374 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=1 Ack=1 Wi
4 0.051658 192.168.0.46 172.67.75.39 TLSv1.3 571 Client Hello (SNI=www.wireshark.
5 0.129374 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=1 Ack=518
6 0.141320 172.67.75.39 192.168.0.46 TLSv1.3 1514 Server Hello, Change Cipher Spec
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] Seq=518 Ack=18
9 1.922015 192.168.0.46 172.67.75.39 TLSv1.3 118 Change Cipher Spec, Application
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 captured
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b), Ds
Internet Protocol Version 4, Src: 192.168.0.46, Dst: 17
Transmission Control Protocol, Src Port: 51111, Dst Port
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
Wireshark_Masterclass_Lesson1_Setup.pcapng
Paquetes: 89
Perfil: angelaGarcia

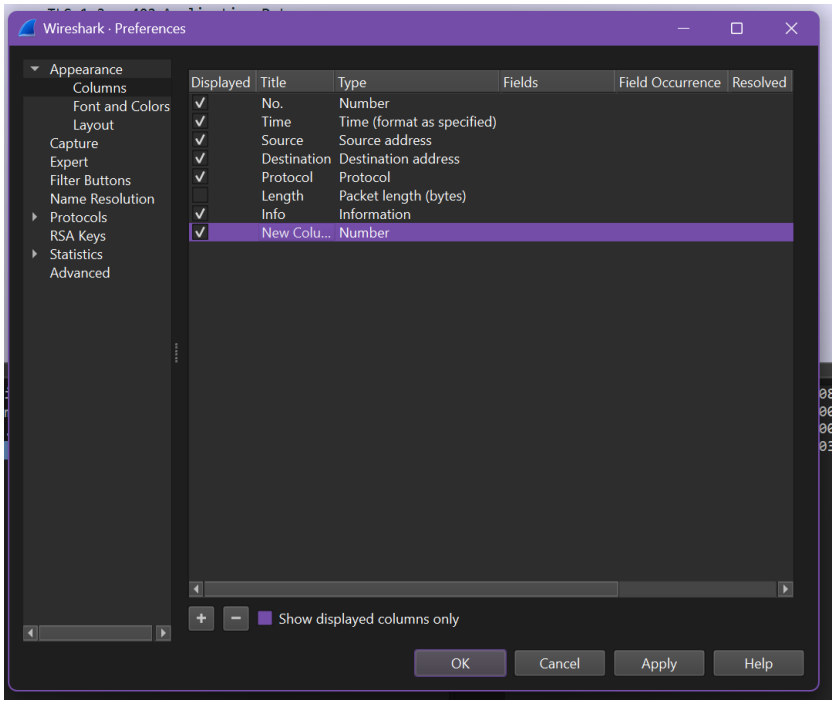
5.


Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 11:16:47.126585 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 11:16:47.177831 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
3 11:16:47.177959 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
4 11:16:47.178243 192.168.0.46 172.67.75.39 TLSv1.3 571 Client Hello (SNI=www.wireshark.org)
5 11:16:47.255959 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=1 Ack=518 Win=67584 Len=0
6 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 1514 Server Hello, Change Cipher Spec
7 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 402 Application Data
8 11:16:47.267999 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=518 Ack=1809 Win=131584 Len=0
9 11:16:49.048600 192.168.0.46 172.67.75.39 TLSv1.3 118 Change Cipher Spec, Application Data
10 11:16:49.048918 192.168.0.46 172.67.75.39 TLSv1.3 146 Application Data
11 11:16:49.049309 192.168.0.46 172.67.75.39 TLSv1.3 720 Application Data
12 11:16:49.073867 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=1809 Ack=582 Win=67584 Len=0
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 582 Application Data, Application Data
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 85 Application Data
15 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=2337 Ack=674 Win=67584 Len=0
16 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=2337 Ack=1340 Win=68608 Len=0
17 11:16:49.079528 172.67.75.39 192.168.0.46 TLSv1.3 85 Application Data
18 11:16:49.099770 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=2368 Ack=1371 Win=68608 Len=0
19 11:16:49.123997 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=1371 Ack=2368 Win=130816 Len=0
20 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1445 Application Data
21 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1514 Application Data
22 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1376 Application Data
23 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1445 Application Data
24 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1514 Application Data
25 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1376 Application Data
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A447BA6D-164F-4853-84FD
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b), Dst: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae)
Internet Protocol Version 4, Src: 192.168.0.46, Dst: 172.67.75.39
Transmission Control Protocol, Src Port: 51111, Dst Port: 443, Seq: 0, Len: 0
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 0a 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
Wireshark_Masterclass_Lesson1_Setup.pcapng
Packets: 89
Profile: angelaGarcia

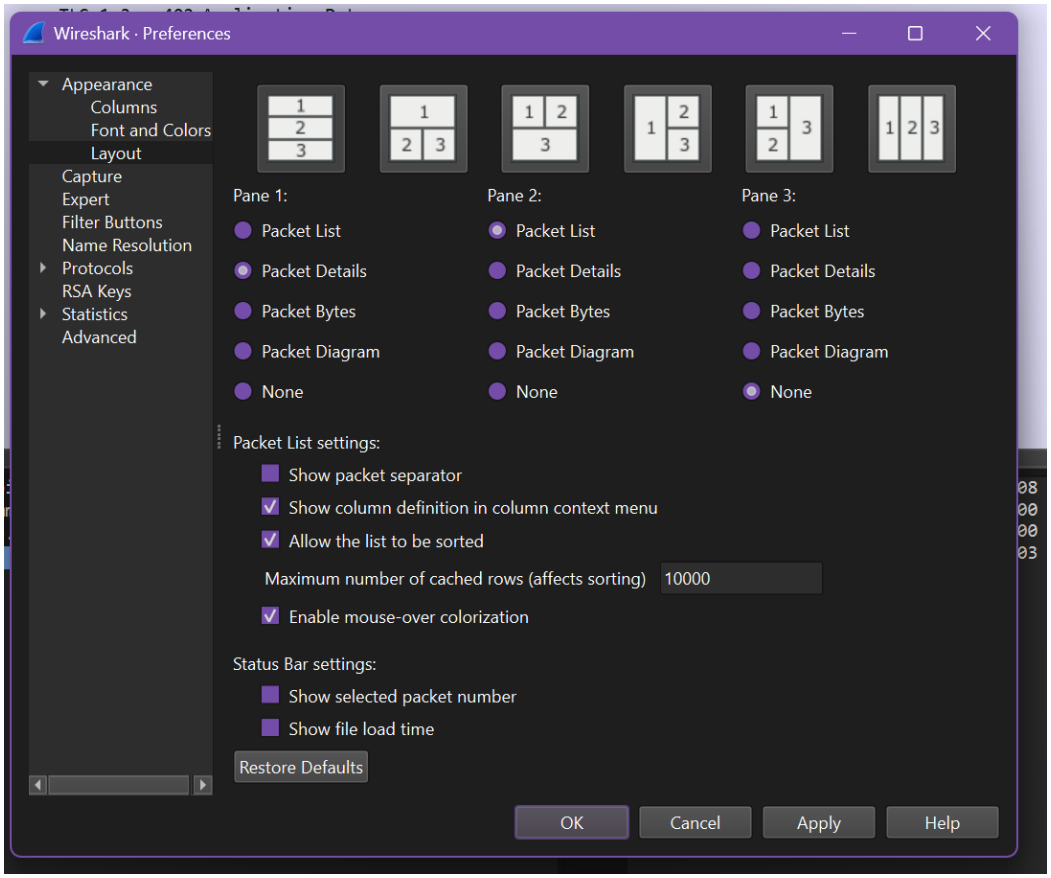
6.


TLSv1.3 1514 Server Hello, Change Cipher Spec
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Displayed Title Type Fields Field Occurrence Resolved
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
New Colu... Number
Show displayed columns only
OK
Cancel
Apply
Help

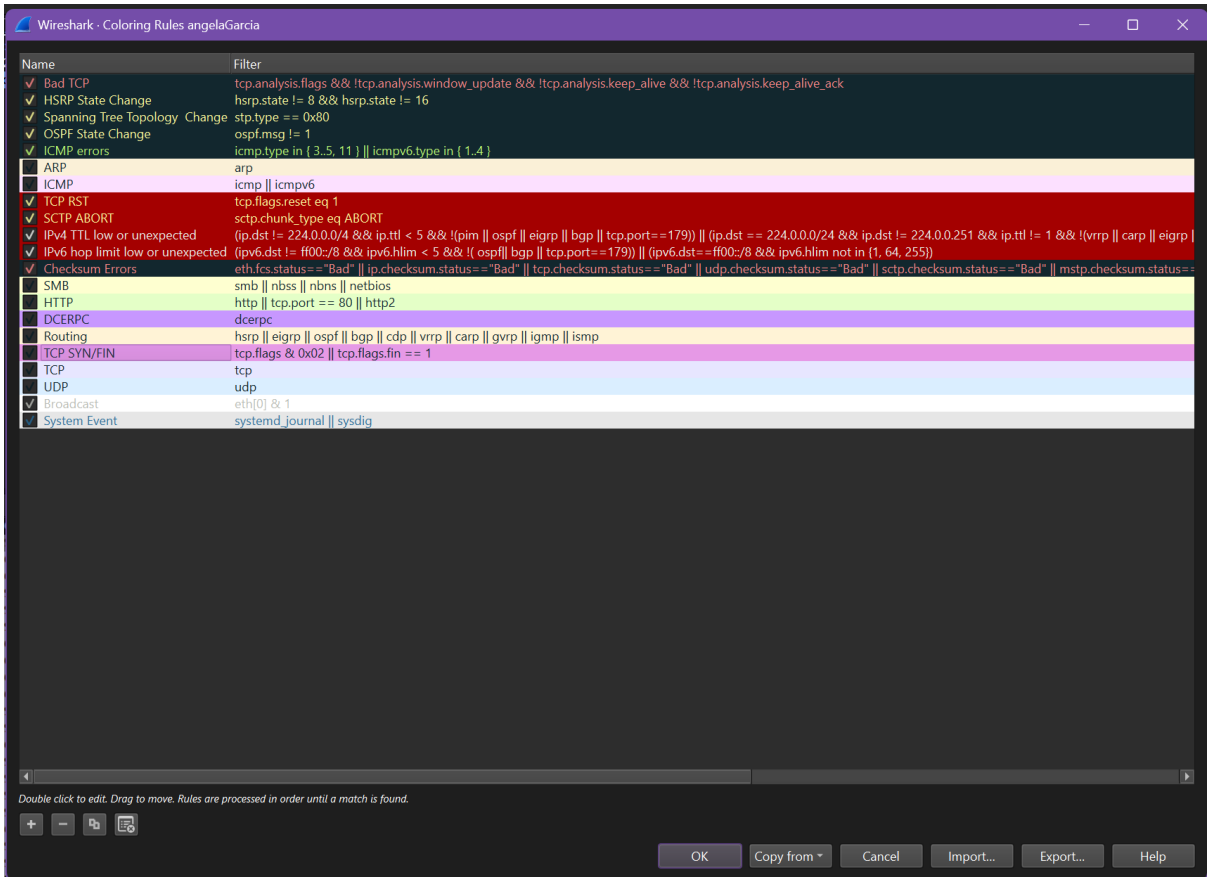
7.

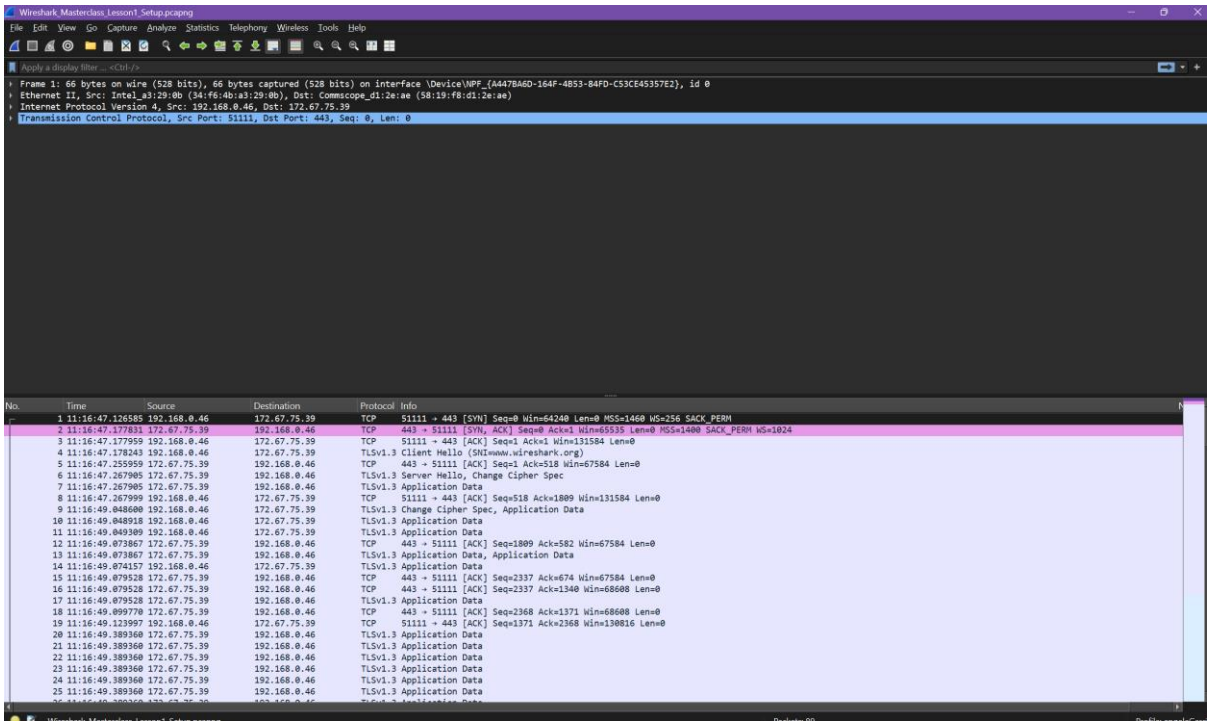

Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Displayed
Title
Type
Fields
Field Occurrence
Resolved
No.
Number
Time
Time (format as specified)
Source
Source address
Destination
Destination address
Protocol
Protocol
Length
Packet length (bytes)
Info
Information
New Colu...
Number
Show displayed columns only
OK
Cancel
Apply
Help

8.

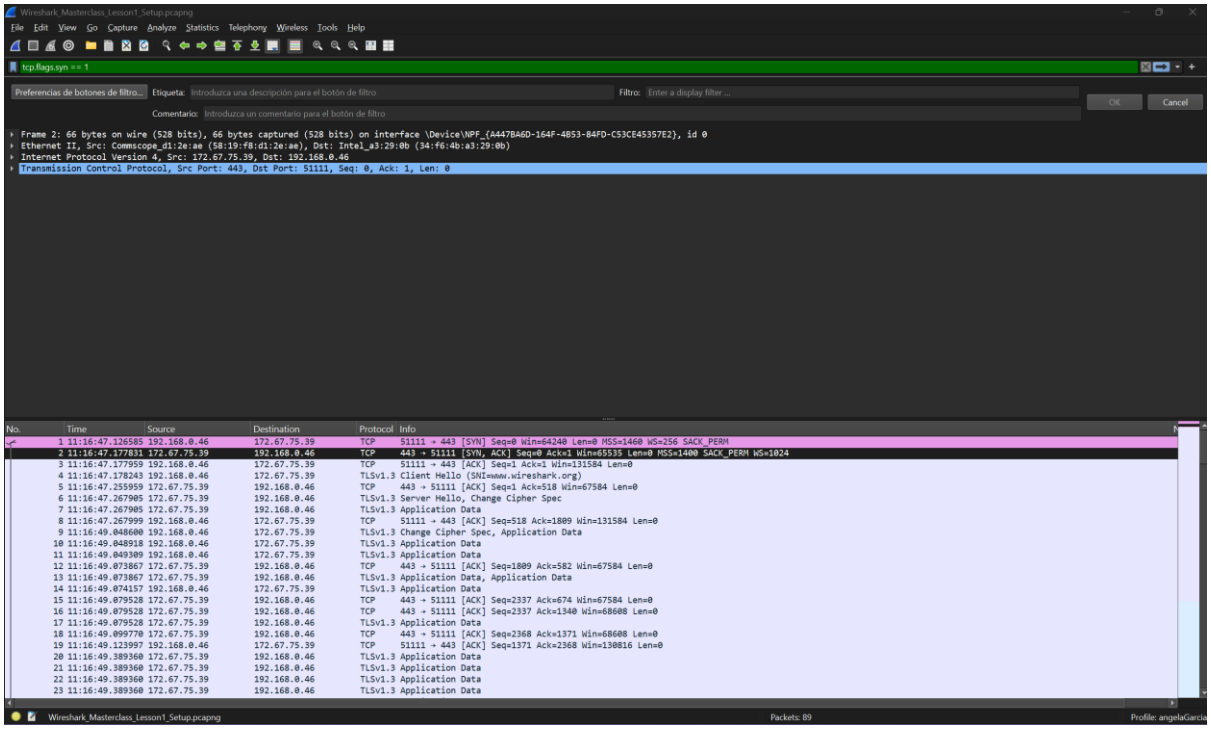

Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Pane 1:
Pane 2:
Pane 3:
Packet List
Packet Details
Packet Bytes
Packet Diagram
None
Packet List settings:
Show packet separator
Show column definition in column context menu
Allow the list to be sorted
Maximum number of cached rows (affects sorting)
10000
Enable mouse-over colorization
Status Bar settings:
Show selected packet number
Show file load time
Restore Defaults
OK
Cancel
Apply
Help

9.

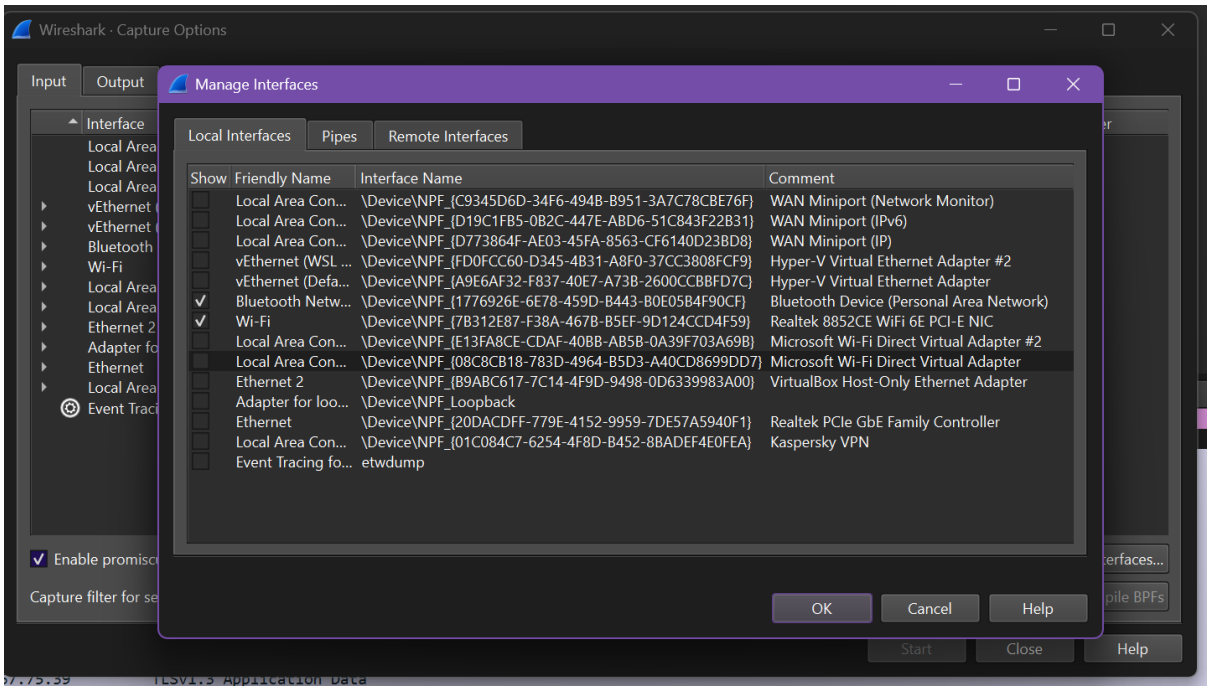

Wireshark · Coloring Rules angelaGarcia
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
IPv4 TTL low or unexpected
(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp || eigrp
IPv6 hop limit low or unexpected
(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp.checksum.status==
SMB
smb || nbss || nbns || netbios
HTTP
http || tcp.port == 80 || http2
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
System Event
systemd_journal || sysdig
Double click to edit. Drag to move. Rules are processed in order until a match is found.
OK
Copy from
Cancel
Import...
Export...
Help


Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A447BA6D-164F-4B53-84FD-C53CE45357E2}, id 0
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b), Dst: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae)
Internet Protocol Version 4, Src: 192.168.0.46, Dst: 172.67.75.39
Transmission Control Protocol, Src Port: 51111, Dst Port: 443, Seq: 0, Len: 0
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 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2 11:16:47.177831 172.67.75.39 192.168.0.46 TCP 443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=1024
3 11:16:47.177959 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
4 11:16:47.178243 192.168.0.46 172.67.75.39 TLSv1.3 Client Hello (SNI=www.wireshark.org)
5 11:16:47.255959 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=1 Ack=518 Win=67584 Len=0
6 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 Server Hello, Change Cipher Spec
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] Seq=518 Ack=1809 Win=131584 Len=0
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] Seq=1809 Ack=582 Win=67584 Len=0
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 Application Data, Application Data
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
15 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=2337 Ack=674 Win=67584 Len=0
16 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=2337 Ack=1340 Win=68608 Len=0
17 11:16:49.079528 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
18 11:16:49.099770 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=2368 Ack=1371 Win=68608 Len=0
19 11:16:49.123997 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=1371 Ack=2368 Win=130816 Len=0
20 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
21 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
22 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
23 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
24 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
25 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data

10.

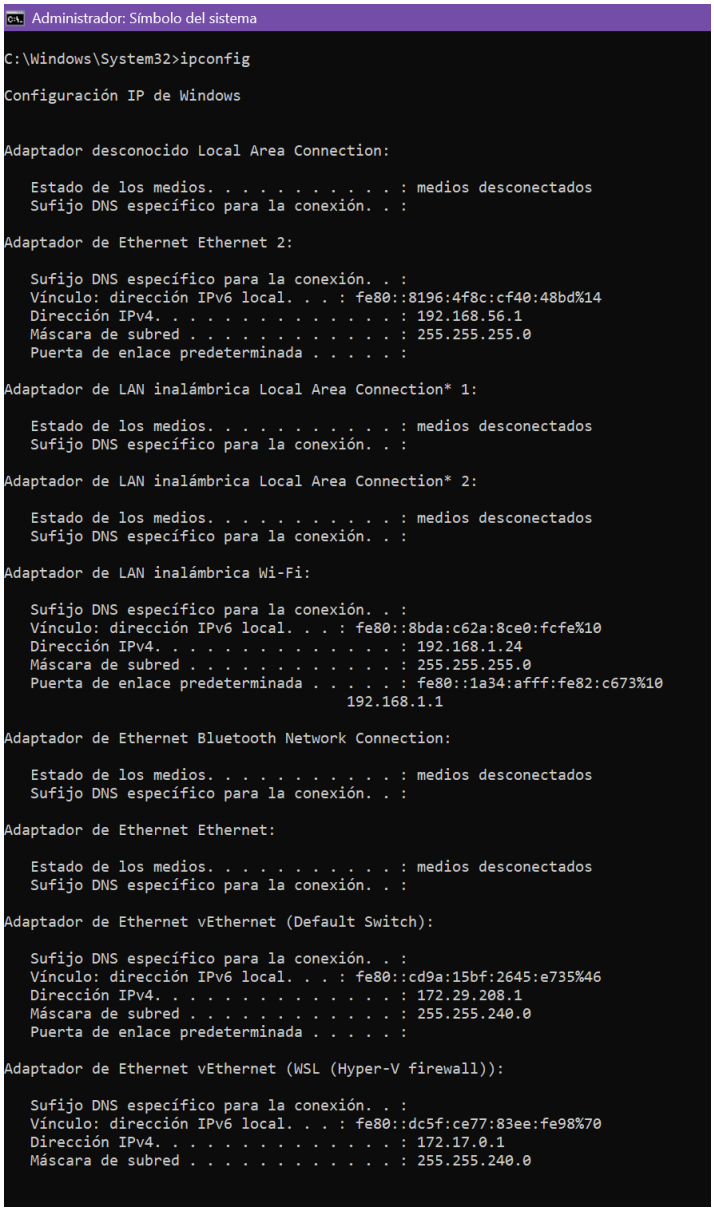


11.



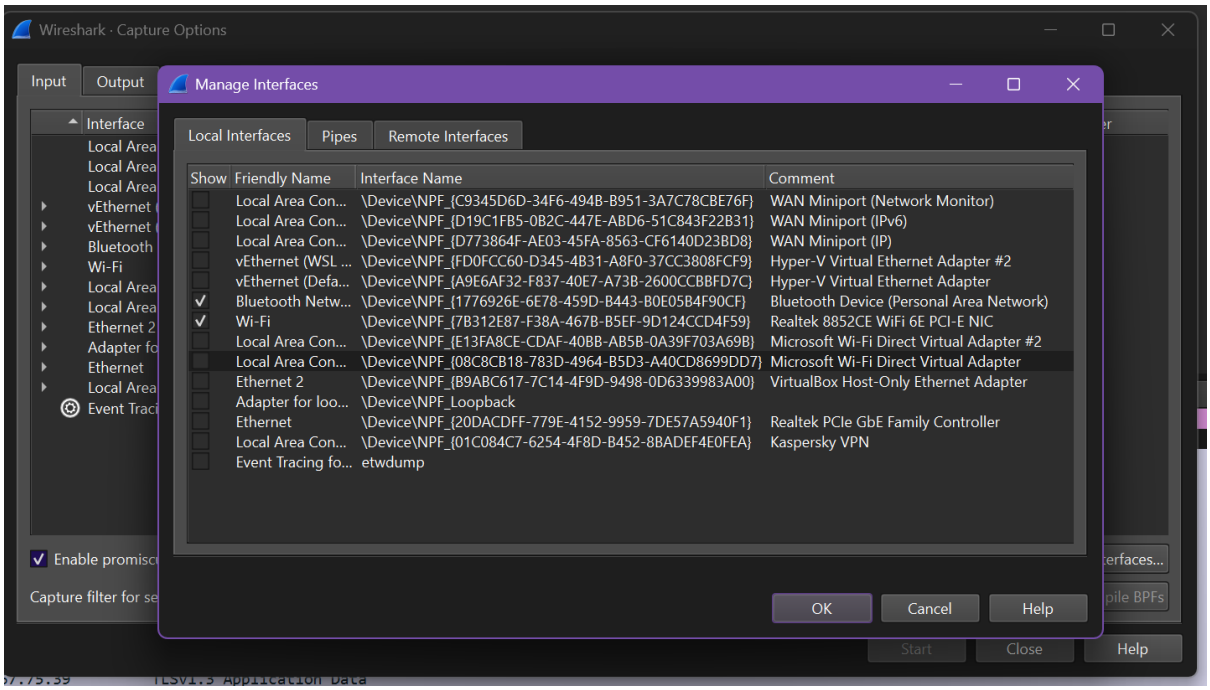
1.2 Configuración de la captura de paquetes

1.

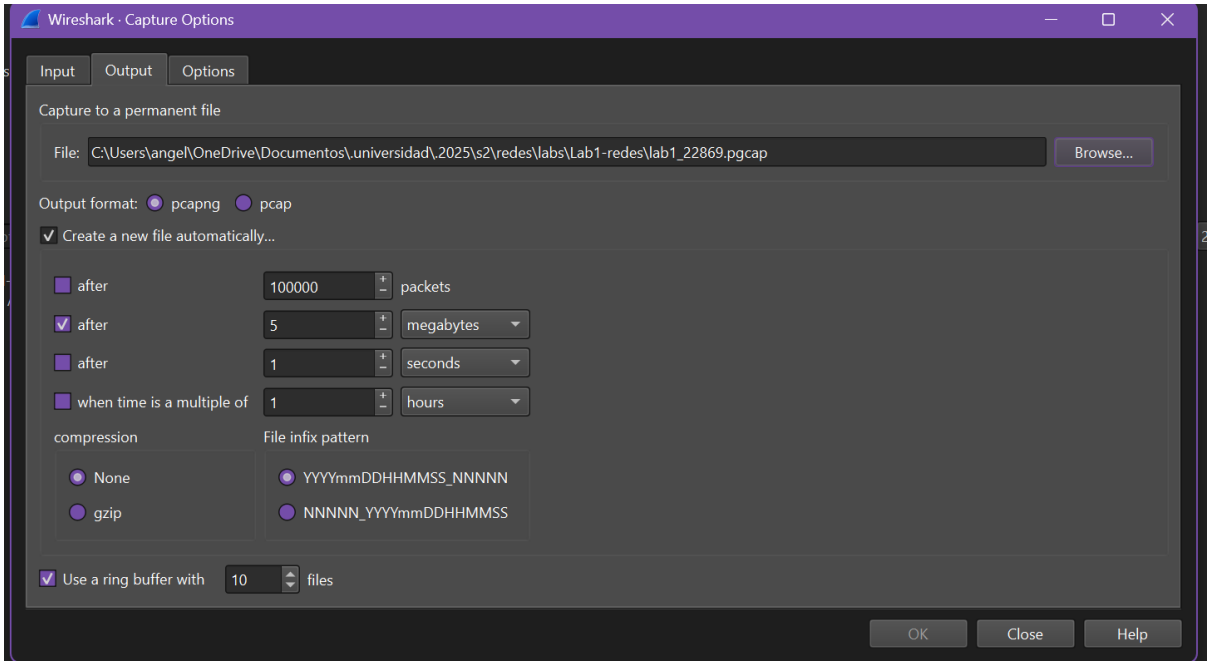


Al ejecutar el comando de ipconfig, se pueden ver las diferentes interfaces de red, que son físicas y virtuales. La que se usa para la conexión a internet es la del adaptador LAN inalámbrico wi-fi, con la dirección IPv4 de 192.168.1.24 y tiene una máscara de subred de 255.255.255.0 y la puerta de enlace predeterminada es 192.168.1.1. También, hay otras interfaces con direcciones IP como Ethernet, vEthernet y WSL, pero esas interfaces no disponen de puerta de enlace y no están conectadas a internet. Y por último, hay adaptadores con el estado “medios desconectados” como Local Area Connection, Bluetooth y Ethernet, que no tienen actividad de red. Estaban desconectados para capturar los paquetes adecuados y descartando los que no generen tráfico relevante.

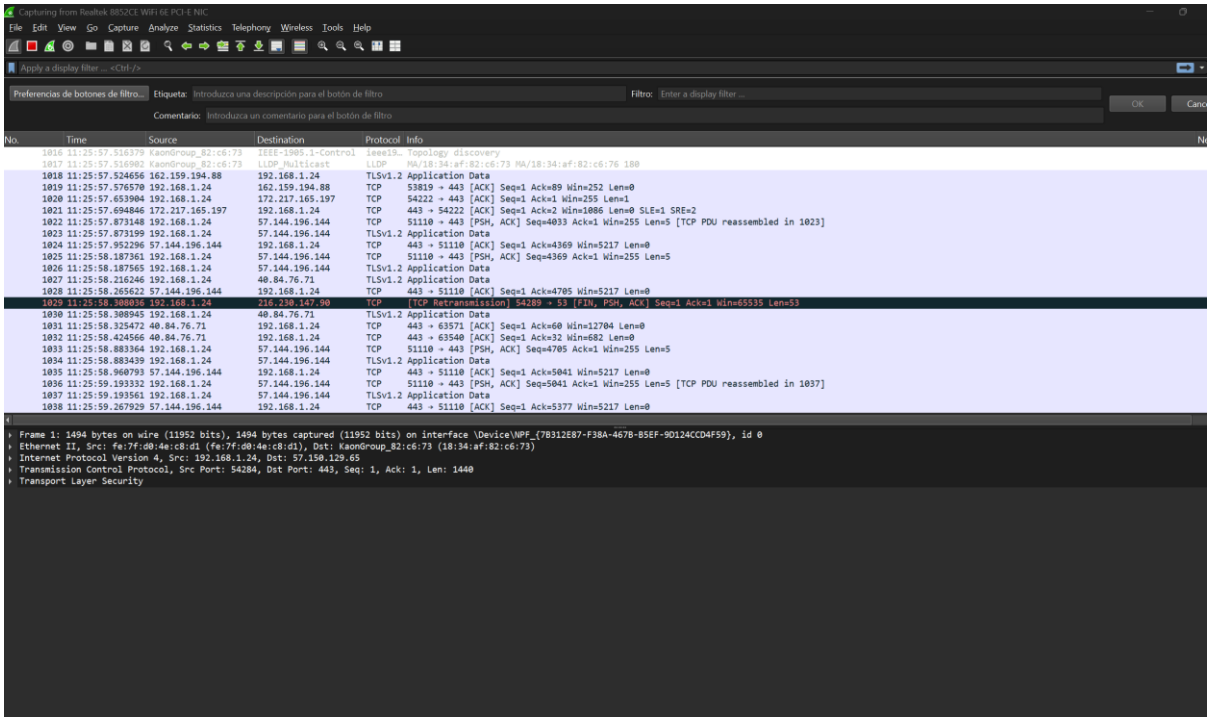
2.

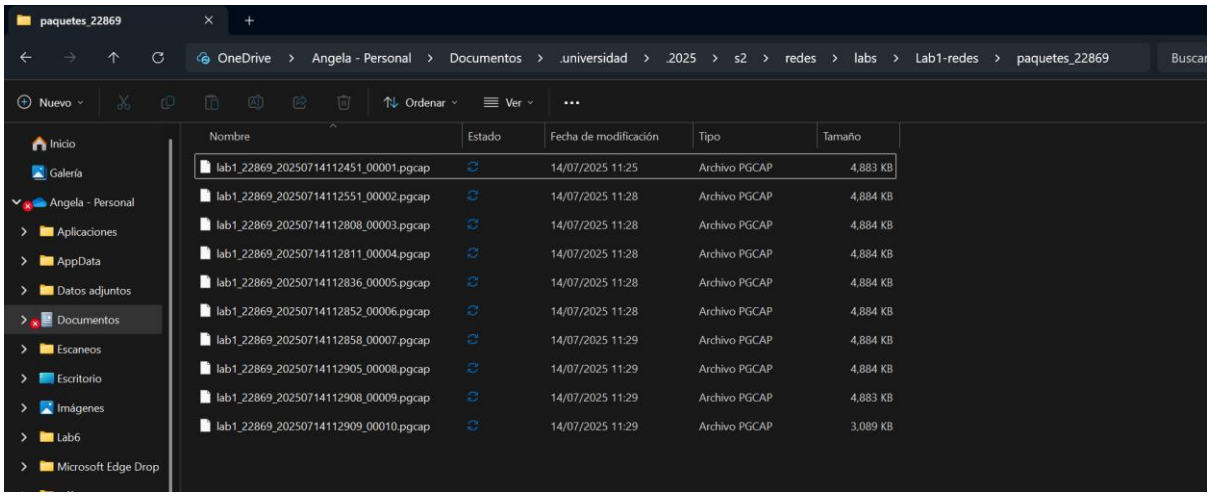

Wireshark · Capture Options
Input
Output
Interface
Manage Interfaces
Local Interfaces
Pipes
Remote Interfaces
Show Friendly Name Interface Name Comment
Local Area Con... \Device\NPF_{C9345D6D-34F6-494B-B951-3A7C78CBE76F} WAN Miniport (Network Monitor)
Local Area Con... \Device\NPF_{D19C1FB5-0B2C-447E-ABD6-51C843F22B31} WAN Miniport (IPv6)
Local Area Con... \Device\NPF_{D773864F-AE03-45FA-8563-CF6140D23BD8} WAN Miniport (IP)
vEthernet (WSL ... \Device\NPF_{FD0FCC60-D345-4B31-A8F0-37CC3808FCF9} Hyper-V Virtual Ethernet Adapter #2
vEthernet (Defa... \Device\NPF_{A9E6AF32-F837-40E7-A73B-2600CCBBFD7C} Hyper-V Virtual Ethernet Adapter
Bluetooth Netw... \Device\NPF_{1776926E-6E78-459D-B443-B0E05B4F90CF} Bluetooth Device (Personal Area Network)
Wi-Fi \Device\NPF_{7B312E87-F38A-467B-B5EF-9D124CCD4F59} Realtek 8852CE WiFi 6E PCI-E NIC
Local Area Con... \Device\NPF_{E13FA8CE-CDAF-40BB-AB5B-0A39F703A69B} Microsoft Wi-Fi Direct Virtual Adapter #2
Local Area Con... \Device\NPF_{08C8CB18-783D-4964-B5D3-A40CD8699DD7} Microsoft Wi-Fi Direct Virtual Adapter
Ethernet 2 \Device\NPF_{B9ABC617-7C14-4F9D-9498-0D6339983A00} VirtualBox Host-Only Ethernet Adapter
Adapter for loo... \Device\NPF_Loopback
Ethernet \Device\NPF_{20DACDFF-779E-4152-9959-7DE57A5940F1} Realtek PCIe GbE Family Controller
Local Area Con... \Device\NPF_{01C084C7-6254-4F8D-B452-8BADEF4E0FEA} Kaspersky VPN
Event Tracing fo... etwdump
OK
Cancel
Help
Start
Close
Help

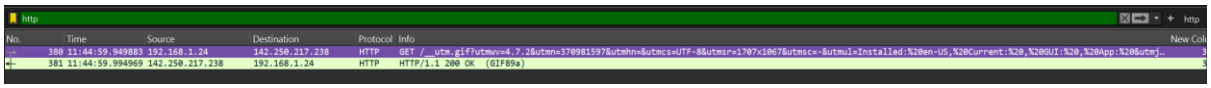
3.


Wireshark · Capture Options
Input
Output
Options
Capture to a permanent file
File: C:\Users\angel\OneDrive\Documentos\.universidad\.2025\s2\redes\labs\Lab1-redes\lab1_22869.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
None
gzip
File infix pattern
YYYYmmDDHHMMSS_NNNNN
NNNNN_YYYYmmDDHHMMSS
Use a ring buffer with 10 files
OK
Close
Help

1.3 Análisis del paquetes







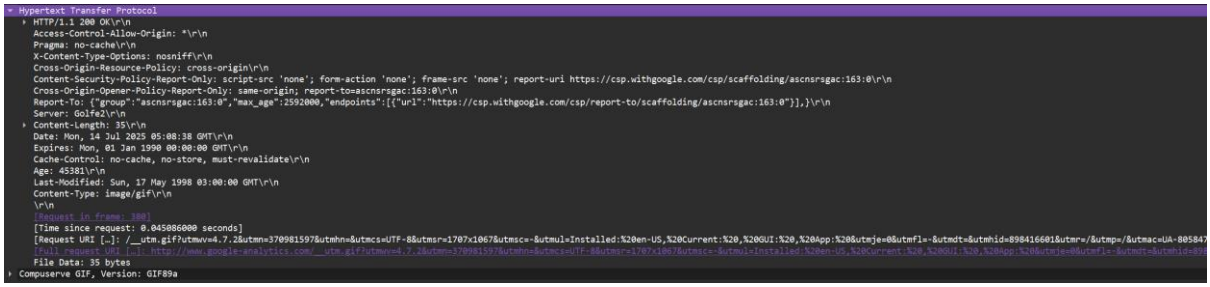
Lo copiado del texto al aplicar el filtro:

380 11:44:59.949883 192.168.1.24 142.250.217.238 HTTP GET /__utm.gif?utmwv=4.7.2&utmn=370981597&utmhn=&utmcs=UTF-8&utmsr=1707x1067&utmsc=-&utmul=Installed:%20en-US,%20Current:%20,%20GUI:%20,%20App:%20&utmje=0&utmfl=-&utmdt=&utmhid=898416601&utmr=/&utmp=/&utmac=UA-80584726-1&utmcc=__utma%3D0.1609550158.1749663655.1752443641.1752504357.26%3B%2B__utmz%3D0.1752504357.1.1.utmcsr%3D%28direct%29%7Cutmccn%3D%7Cutmc

md%3D%3B&utme=5%28GamesManager%2ABeta%20Game%20Started%2AChrome%29%28%29&gaq=1&utmt=event HTTP/1.1 380

381 11:44:59.994969 142.250.217.238 192.168.1.24 HTTP HTTP/1.1 200 OK (GIF89a) 381

Número de bytes:



Respuesta a las preguntas mencionadas

a. **¿Qué versión de HTTP está ejecutando su navegador?**
    a. La versión que está usando es HTTP/1.1 200
b. **¿Qué versión de HTTP está ejecutando el servidor?**
    a. La versión que está usando el servidor es HTTP/1.1
c. **¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?**
    a. **Los lenguajes que acepta son:**
        i. Español para América Latina
        ii. Español
        iii. Inglés España
        iv. Inglés general
        v. Inglés británico
        vi. Inglés estadounidense
        vii. Español México
d. **¿Cuántos bytes de contenido fueron devueltos por el servidor?**
    a. 35 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.**
    a. En el caso de que haya un problema de rendimiento mientras se descarga la página, sería mejor primero capturar el tráfico en el lado del cliente, para detectar problemas como pérdida de paquetes, retrasos o otros problemas. Y si no se encuentran problemas en el cliente, se debería de capturar el tráfico en el servidor o en algún punto intermedio

como un router o firewall. No es tan recomendable Wireshark porque consume varios recursos y por riesgos de seguridad.

Discusión

En este laboratorio se realizó la personalización de entorno, configuración de la captura de paquetes y el análisis de paquetes en Wireshark, con los objetivos de familiarizarse con el entorno, fortalecer la teoría sobre paquetes a través del análisis de paquetes reales, por último, conocer los propósitos y usos de un analizador de paquetes.

En la primera parte, acerca de familiarizarse con el entorno, se realizó varias actividades como el crear un perfil, cambiar configuraciones como: cambiar el del formato del tiempo, agregar y ocultar columnas, aplicar esquemas, cambiar colores para un protocolo en específico, crear filtros y se descargó un archivo con transmisiones capturadas.

La segunda parte es sobre la configuración de la captura de paquetes, en donde con ipconfig muestra todos los valores acerca de la configuración de red TCP/IP actuales y lo que realiza es actualiza la configuración del protocolo de configuración dinámica del host y del sistema de nombre de dominio. En el segundo paso se desactivaron todas las interfaces virtuales y las que no apliquen, con el objetivo de que solo se capturen los paquetes adecuados y descartar los que no generan tráfico relevante. En esta parte se observan las diferentes interfaces de red que son las físicas y virtuales. Lo que se puede destacar de esta parte es que la que se usa para la conexión a internet es la del adaptador LAN inalámbrico wi-fi, con la dirección IPv4 de 192.168.1.24 y tiene una máscara de subred de 255.255.255.0 y la puerta de enlace predeterminada es 192.168.1.1.

Y en la tercera parte, que es de análisis de paquetes, se analizó los resultados del protocolo HTTP, que dio como resultado que la versión que está usando el navegador es HTTP/1.1 200, al igual que por parte del servidor usa la misma versión. Acerca de los lenguajes que usa son varios, siendo el principal el Español para América. Mientras, los bytes devueltos por el servidor fueron 35 bytes, esto es debido a que el recurso solicitado es un gif de rastreo y este no es una imagen normal, sino que un pixel de rastreo transparente de 1x1 píxel y este es bastante pequeño.

Se cumplieron los objetivos de esta práctica, ya que se familiarizó con el entorno de la herramienta Wireshark y se fortaleció la teoría sobre paquetes a través del análisis de paquetes reales, para tener un mayor entendimientos teóricos de redes.

Comentario personal

Los primeros pasos en la guía considero que son bastante buenos para llegar a familiarizarse. Sin embargo, al llegar al paso 11 de ocultar las interfaces virtuales y seguir las opciones que dice, aunque estén cerca las opciones para ocultar las interfaces, si me perdí y no sabía donde es que era, por lo tanto, tuve que tomar de ayuda de chatgpt para lograr completar este paso. Por otra parte, en la configuración de captura de paquetes, es bastante confusa la parte de realizar una captura de paquetes, ya que cuando lo trate de hacer no me daba la opción de "ok", pero era porque me faltaba seleccionar after en lo de tamaño de 5MB y seleccionar wi-fi,. En lo personal, considero que para este tipo de configuraciones, es más fácil ver una captura de pantalla o una lista de que es lo que se tiene que tener. Y por último, otro desafío que encontré es la parte en la que se tiene que saber qué versión de HTTP está ejecutando el navegador, porque no me salía nada al detener el proceso en Wireshark, entonces lo tuve que volver a correr.

Referencias

- Dr369. (2023, septiembre 18). ¿Qué es Wireshark y para qué? *Informática y Tecnología Digital*. https://informatecdigital.com/que-es-wireshark-y-para-que/
- meaghanlewis. (s. f.). *Ipconfig*. Recuperado 14 de julio de 2025, de https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/ipconfig
- *¿Qué es Wireshark y cómo se utiliza? - Infoteknico*. (2024, junio 8). https://www.infoteknico.com/que-es-wireshark-y-como-se-utiliza/