

UNIVERSIDAD DEL VALLE DE GUATEMALA

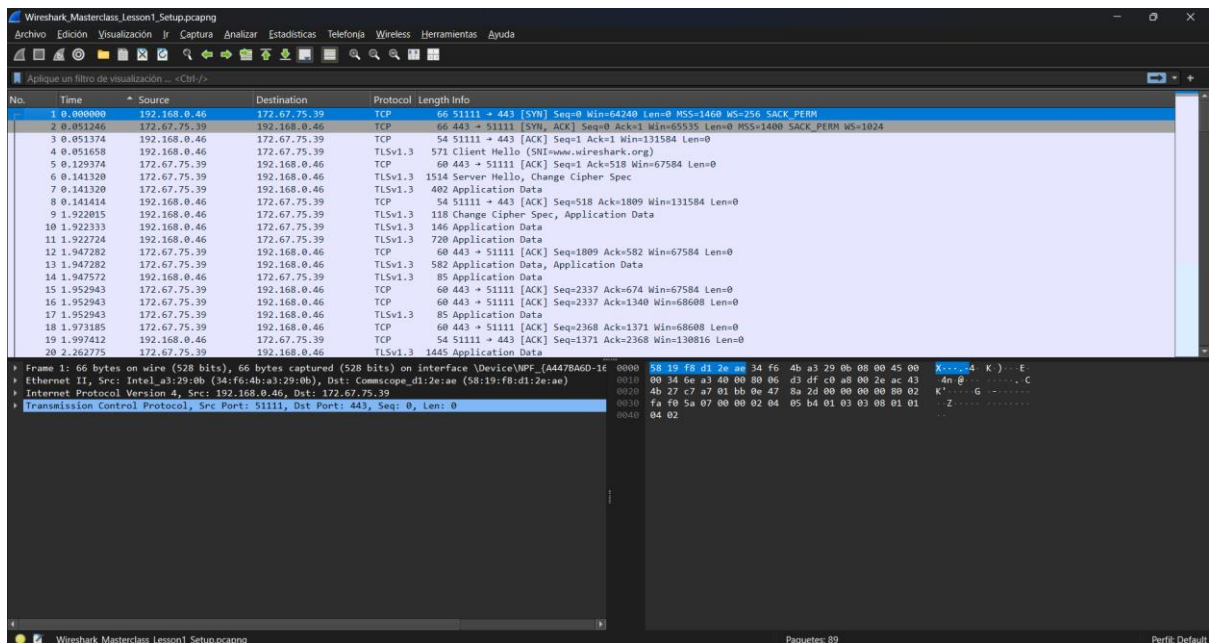
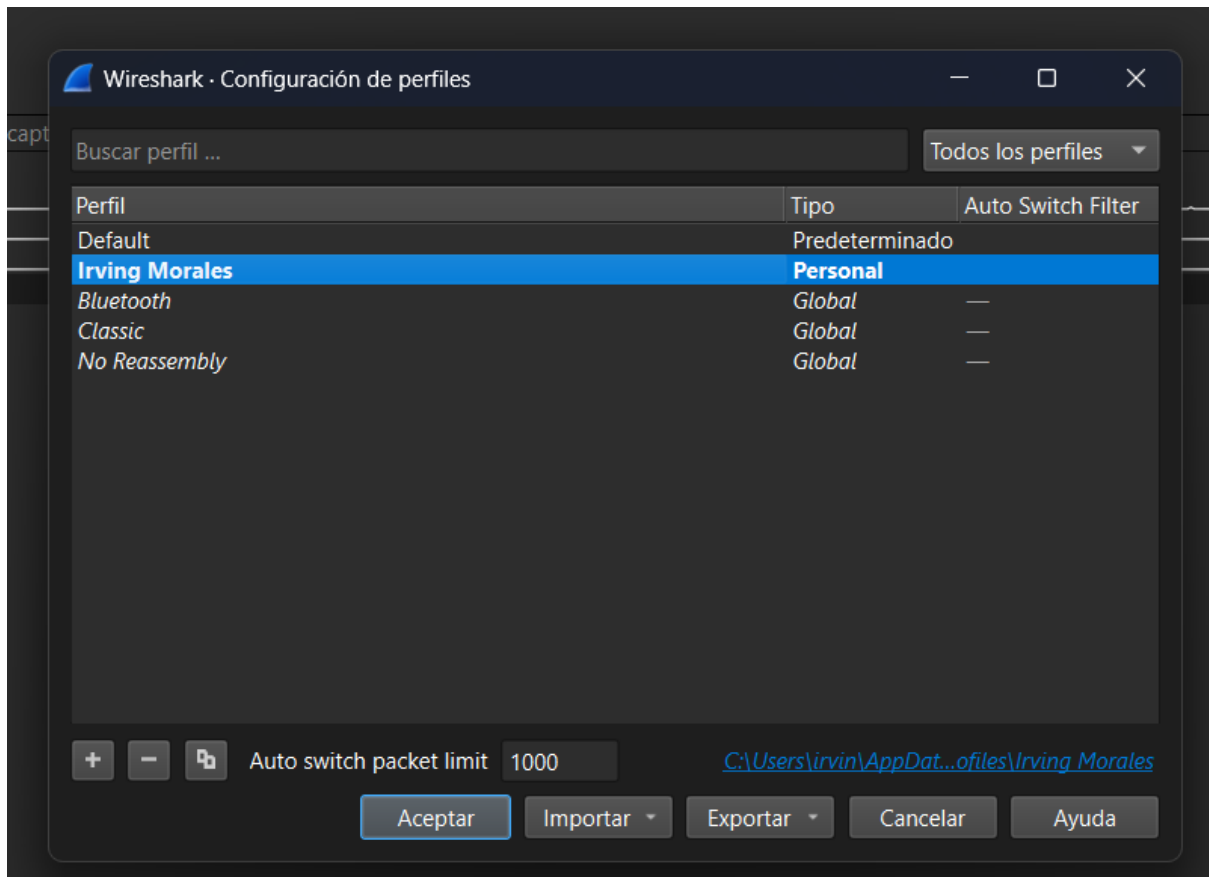
Facultad de Ingeniería

Data Science – Lynette García

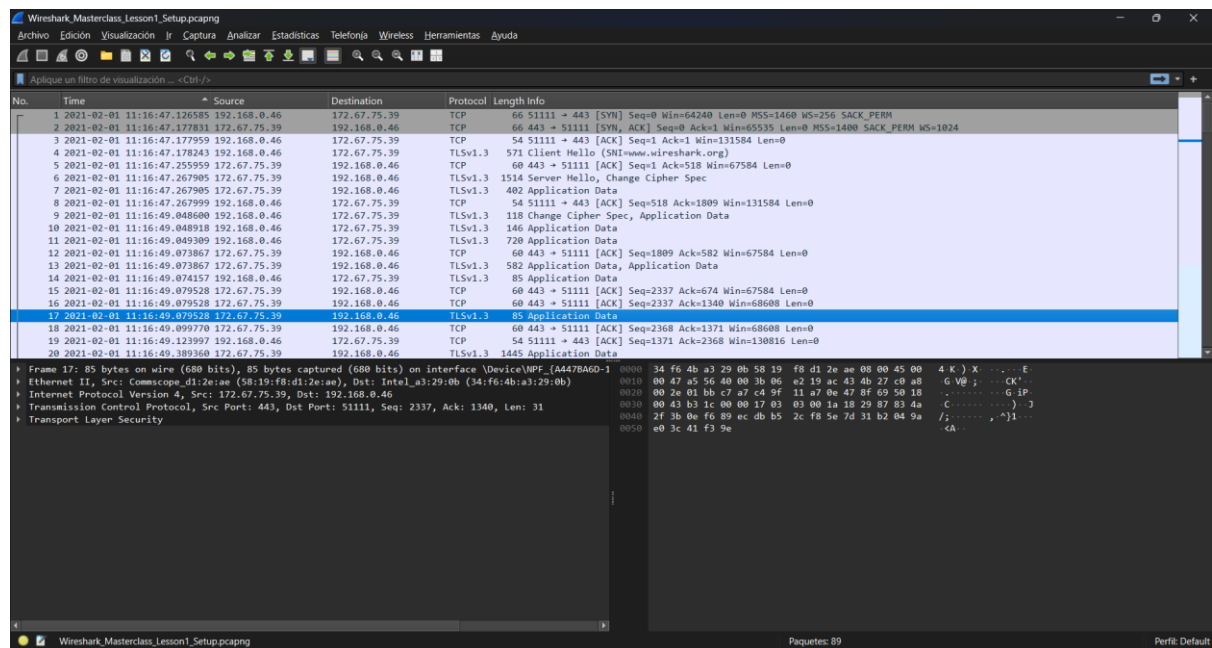


Laboratorio 1

Irving Fabricio Morales Acosta, 22788



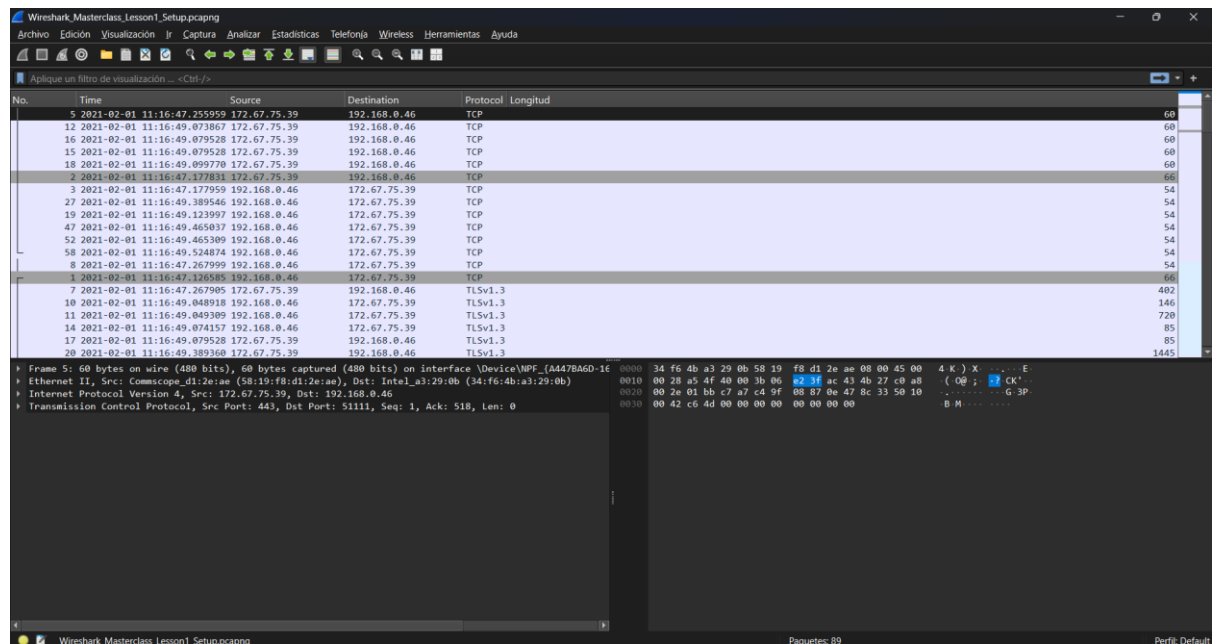
formato de tiempo Time of Day



No.	Time	Source	Destination	Protocol	Length	Info
1	2021-02-01 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	2021-02-01 11:16:47.177959	192.168.0.46	172.67.75.39	TCP	66	443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=1024
3	2021-02-01 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	2021-02-01 11:16:47.178243	192.168.0.46	172.67.75.39	TLSv1.3	571	Client Hello (SNI=www.wireshark.org)
5	2021-02-01 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	2021-02-01 11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	1514	Server Hello, Change Cipher Spec
7	2021-02-01 11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	482	Application Data
8	2021-02-01 11:16:47.267999	192.168.0.46	172.67.75.39	TCP	54	51111 → 443 [ACK] Seq=518 Ack=1009 Win=131584 Len=0
9	2021-02-01 11:16:49.048600	192.168.0.46	172.67.75.39	TLSv1.3	118	Change Cipher Spec, Application Data
10	2021-02-01 11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1.3	146	Application Data
11	2021-02-01 11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1.3	720	Application Data
12	2021-02-01 11:16:49.073867	172.67.75.39	192.168.0.46	TCP	60	443 → 51111 [ACK] Seq=1009 Ack=582 Win=67584 Len=0
13	2021-02-01 11:16:49.073867	172.67.75.39	192.168.0.46	TLSv1.3	582	Application Data, Application Data
14	2021-02-01 11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1.3	85	Application Data
15	2021-02-01 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	2021-02-01 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	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1.3	85	Application Data
18	2021-02-01 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	2021-02-01 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	2021-02-01 11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1.3	1445	Application Data

Frame 17: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF... (A447BAG0-1) on interface Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Ethernet II, Src: Comscope_d12e:ae (58:19:f8:d12e:ae), Dst: Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Internet Protocol Version 4, Src: 172.67.75.39, Dst: 192.168.0.46
Transmission Control Protocol, Src Port: 443, Dst Port: 51111, Seq: 2337, Ack: 1340, Len: 31
Transport Layer Security

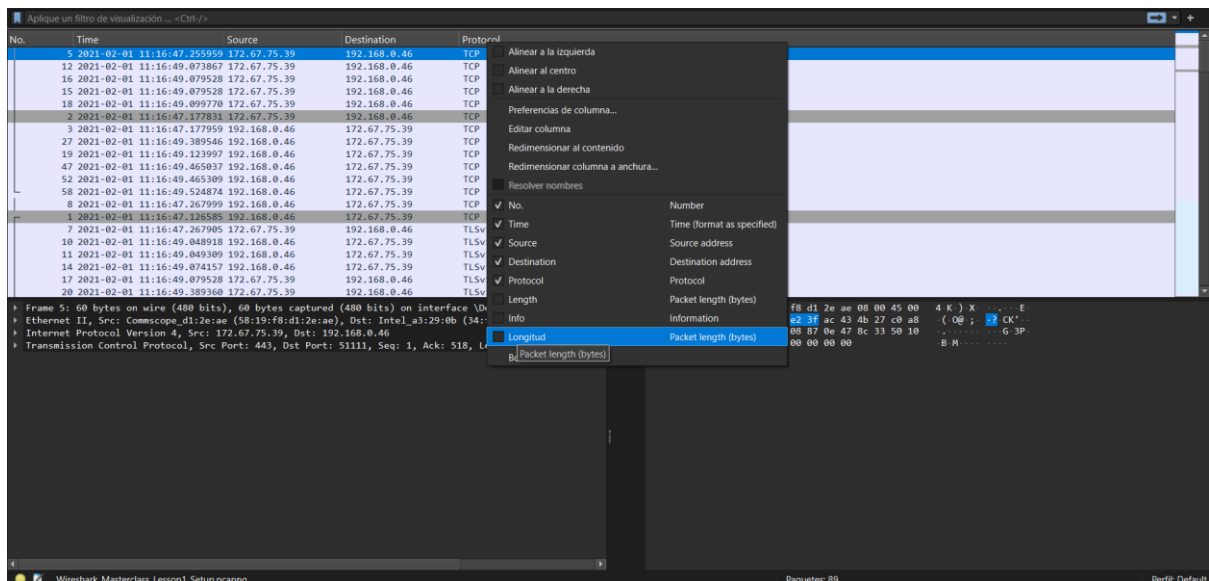
Agregue una columna con la longitud del protocolo (preferences -> column -> +)



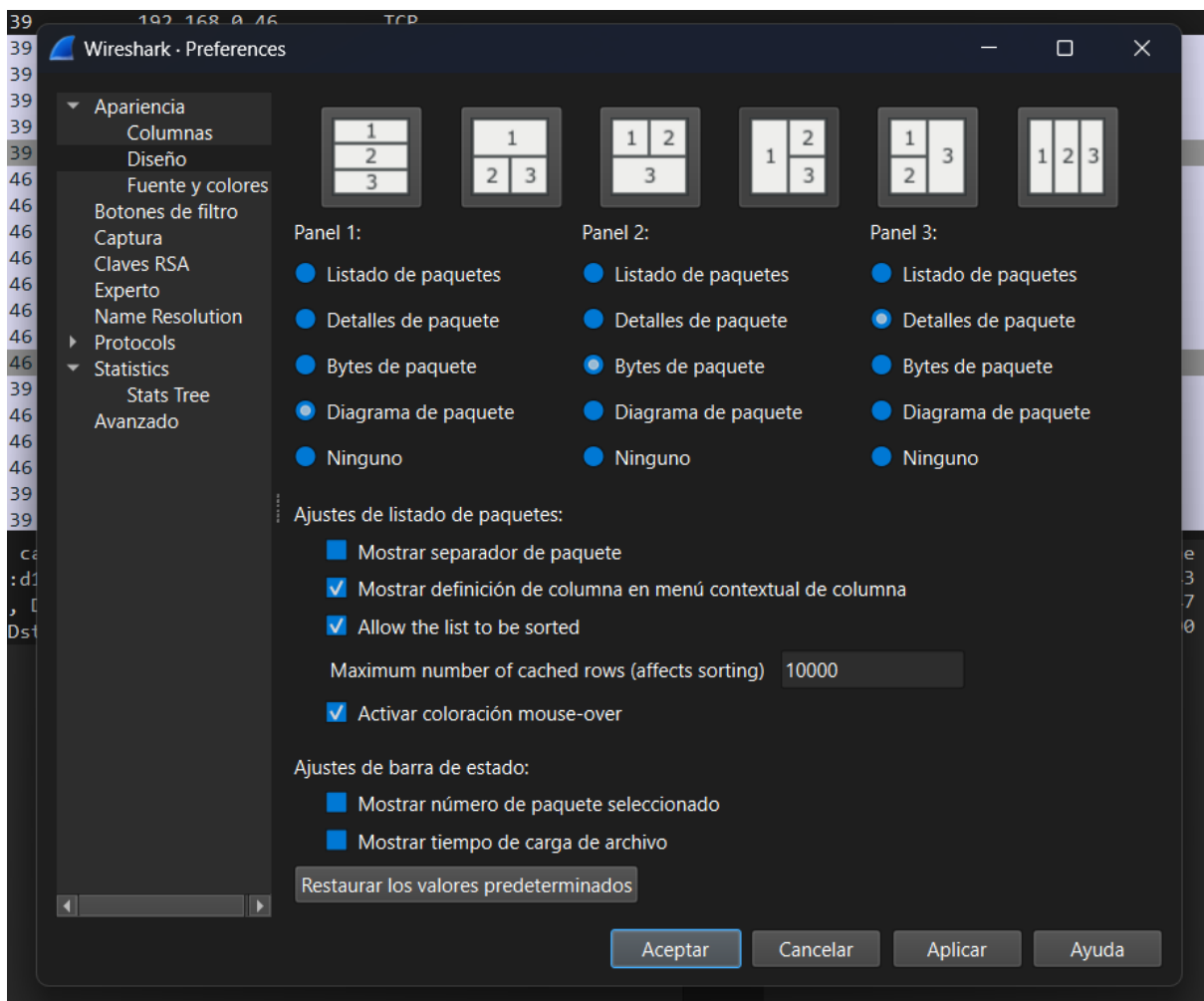
No.	Time	Source	Destination	Protocol	Longitud
5	2021-02-01 11:16:47.255959	172.67.75.39	192.168.0.46	TCP	60
12	2021-02-01 11:16:49.073867	172.67.75.39	192.168.0.46	TCP	60
16	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60
15	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TCP	60
18	2021-02-01 11:16:49.099770	172.67.75.39	192.168.0.46	TCP	60
3	2021-02-01 11:16:47.177959	192.168.0.46	172.67.75.39	TCP	54
27	2021-02-01 11:16:49.389546	192.168.0.46	172.67.75.39	TCP	54
19	2021-02-01 11:16:49.123997	192.168.0.46	172.67.75.39	TCP	54
47	2021-02-01 11:16:49.465837	192.168.0.46	172.67.75.39	TCP	54
52	2021-02-01 11:16:49.465309	192.168.0.46	172.67.75.39	TCP	54
58	2021-02-01 11:16:49.524874	192.168.0.46	172.67.75.39	TCP	54
8	2021-02-01 11:16:47.267999	192.168.0.46	172.67.75.39	TCP	54
1	2021-02-01 11:16:47.126585	192.168.0.46	172.67.75.39	TCP	66
7	2021-02-01 11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3	402
10	2021-02-01 11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1.3	146
11	2021-02-01 11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1.3	720
14	2021-02-01 11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1.3	85
17	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1.3	85
20	2021-02-01 11:16:49.389360	172.67.75.39	192.168.0.46	TLSv1.3	1445

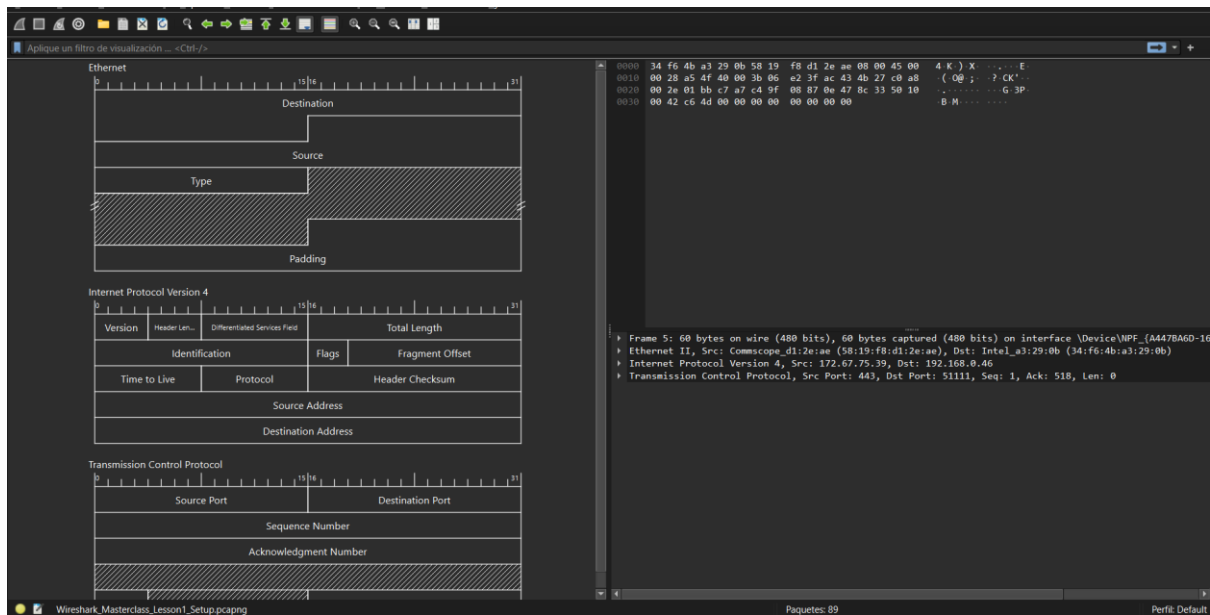
Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF... (A447BAG0-1) on interface Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Ethernet II, Src: Comscope_d12e:ae (58:19:f8:d12e:ae), Dst: Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Internet Protocol Version 4, Src: 172.67.75.39, Dst: 192.168.0.46
Transmission Control Protocol, Src Port: 443, Dst Port: 51111, Seq: 1, Ack: 518, Len: 0

Elimine u oculte la columna Longitud (quise eliminar otras)

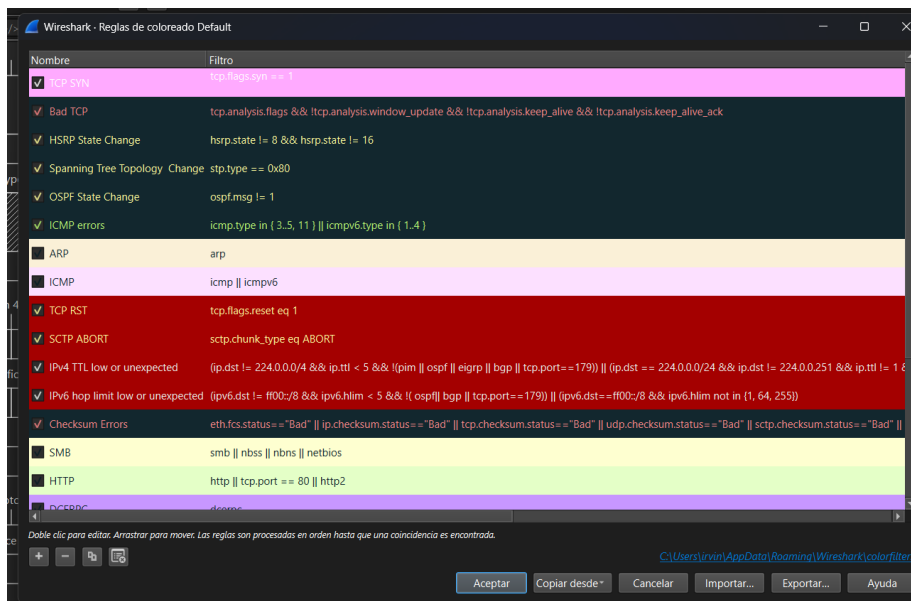


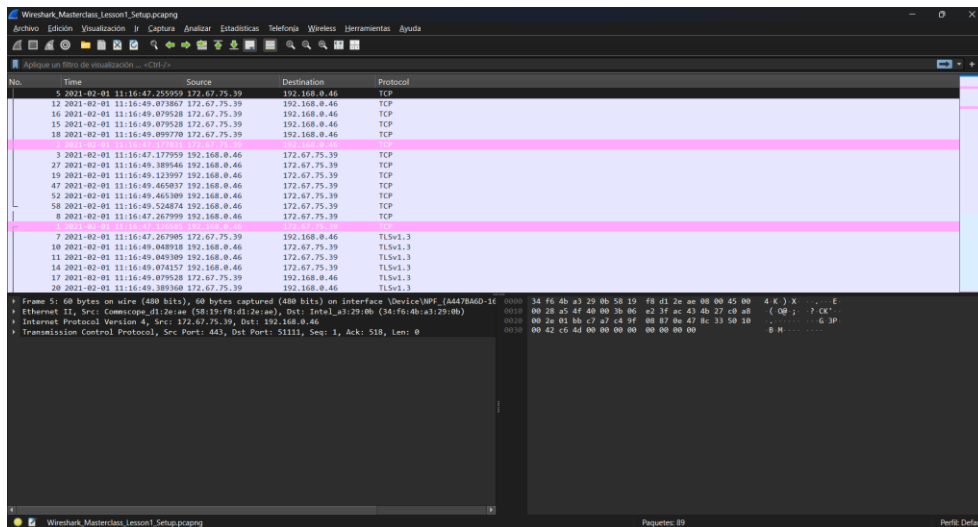
Aplice un esquema de paneles que sea de su preferencia



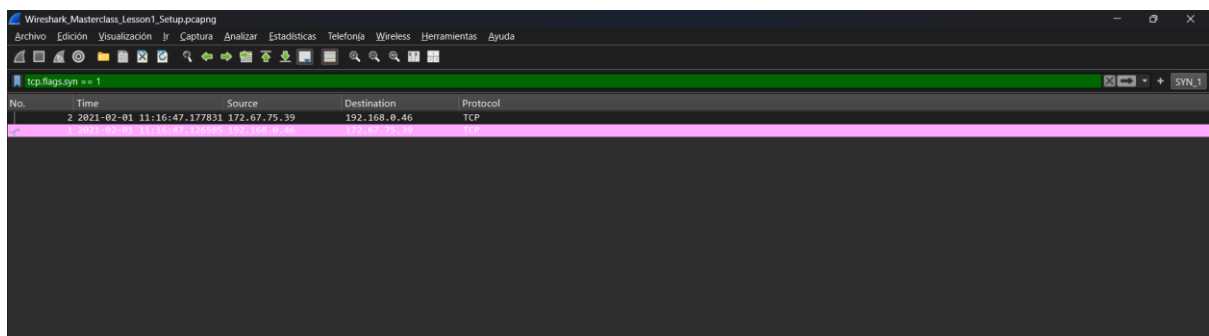


Aplice una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia.

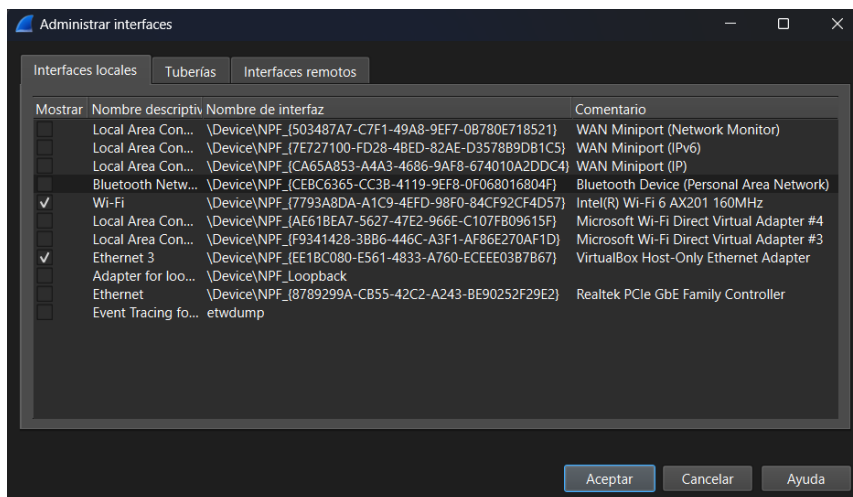




Cree un botón que aplique un filtro para paquetes TCP con la bandera SYN igual a 1.



Oculte las interfaces virtuales



No.	Time	Source	Destination	Protocol
5	2021-02-01 11:16:47.255959	172.67.75.39	192.168.0.46	TCP
12	2021-02-01 11:16:49.073867	172.67.75.39	192.168.0.46	TCP
16	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TCP
15	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TCP
18	2021-02-01 11:16:49.089270	172.67.75.39	192.168.0.46	TCP
2	2021-02-01 11:16:47.177831	172.67.75.39	192.168.0.46	TCP
3	2021-02-01 11:16:47.177959	192.168.0.46	172.67.75.39	TCP
27	2021-02-01 11:16:49.389546	192.168.0.46	172.67.75.39	TCP
19	2021-02-01 11:16:49.123997	192.168.0.46	172.67.75.39	TCP
47	2021-02-01 11:16:49.465037	192.168.0.46	172.67.75.39	TCP
52	2021-02-01 11:16:49.465309	192.168.0.46	172.67.75.39	TCP
58	2021-02-01 11:16:49.524874	192.168.0.46	172.67.75.39	TCP
8	2021-02-01 11:16:47.267999	192.168.0.46	172.67.75.39	TCP
7	2021-02-01 11:16:47.267905	172.67.75.39	192.168.0.46	TLSv1.3
10	2021-02-01 11:16:49.048918	192.168.0.46	172.67.75.39	TLSv1.3
11	2021-02-01 11:16:49.049309	192.168.0.46	172.67.75.39	TLSv1.3
14	2021-02-01 11:16:49.074157	192.168.0.46	172.67.75.39	TLSv1.3
17	2021-02-01 11:16:49.079528	172.67.75.39	192.168.0.46	TLSv1.3
20	2021-02-01 11:16:49.389368	172.67.75.39	192.168.0.46	TLSv1.3

* From 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface DeviceNPF_{A417BADD-1E...}
 * Ethernet II, Src: ComScope_e1:2a:ae:58:10:f6(d1:2a:ae), Dst: Intel_a3:29:0b:34:f6:4b(a3:29:0b)
 * Internet Protocol Version 4, Src: 172.67.75.39, Dst: 192.168.0.46
 * Transmission Control Protocol, Src Port: 443, Dst Port: 51111, Seq: 0, Ack: 1, Len: 0

Configuración de la captura de paquetes

Abra una terminal y ejecute el comando `ifconfig/ipconfig` (dependiendo de su OS).

Detalle y explique lo observado

```

C:\Users\lirvin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . :
    Link-Local IPv6 Address . . . . . : fe80::ada9:16e4:63ff:27d2%20
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : lan
    Link-Local IPv6 Address . . . . . : fe80::9c8d:ec9:9ac:db4d%7
    IPv4 Address. . . . . : 192.168.86.29
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.86.1

Ethernet adapter Bluetooth Network Connection:

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

El comando `ipconfig` muestra la configuración de red de todas las interfaces.

El Ethernet adaptar Ethernet hace referencia a que no está conectado a través del cable físico de Ethernet (eso se ve con el texto que dice “Media disconnected”).

El Ethernet adapter Ethernet 2, suele ser un adaptador virtual y dentro de ellos encontramos:

- IPv4: 192.168.56.1 es una subred privada
- Subnet Mask: 255.255.255.0 significa que permite 256 direcciones
- Default Gateway: (empty) significa que no enruta hacia otras redes
- Link-local IPv6 Address: es la dirección automática para comunicación local en la red

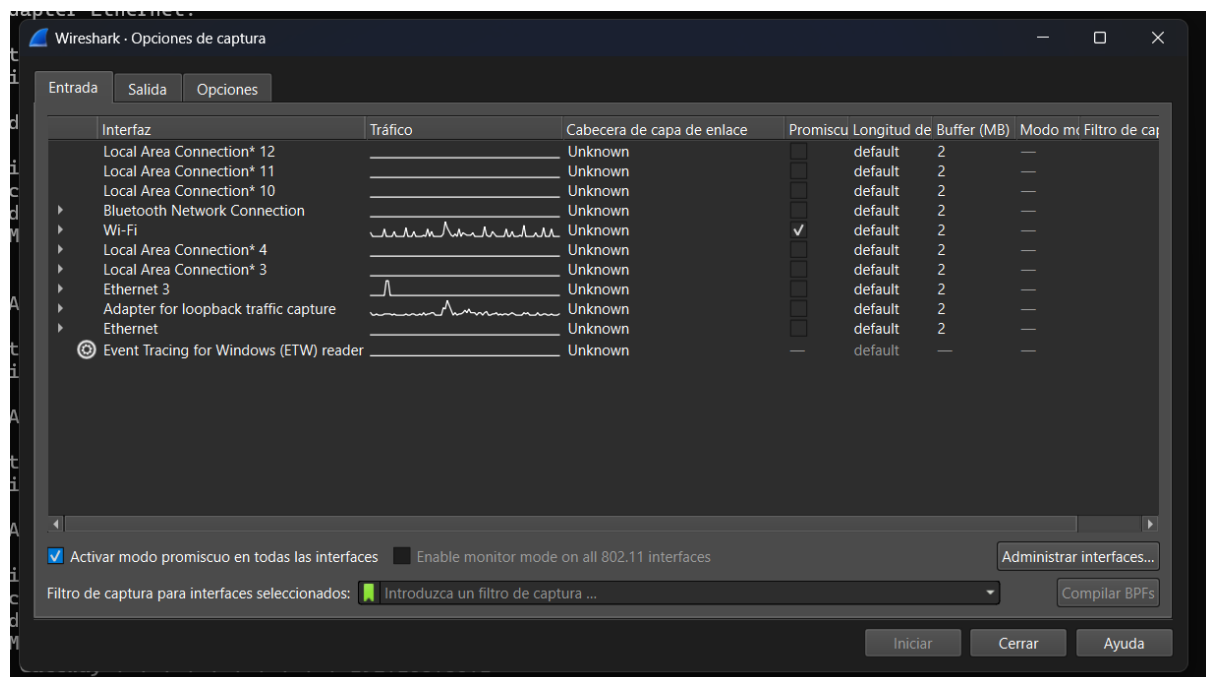
Con Wireless LAN adapter Local Area Connection 3 podemos saber que el Adaptador Wi-Fi virtual o configurado pero **desconectado**. Al igual que el Wireless LAN adapter Local Area Connection 4, que es otro adaptador Wi-fi que está desconectado

Uno de los más importantes es el Wireless LAN adapter Wifi, el cuál es el adaptador Wi-fi y conectado a la red.

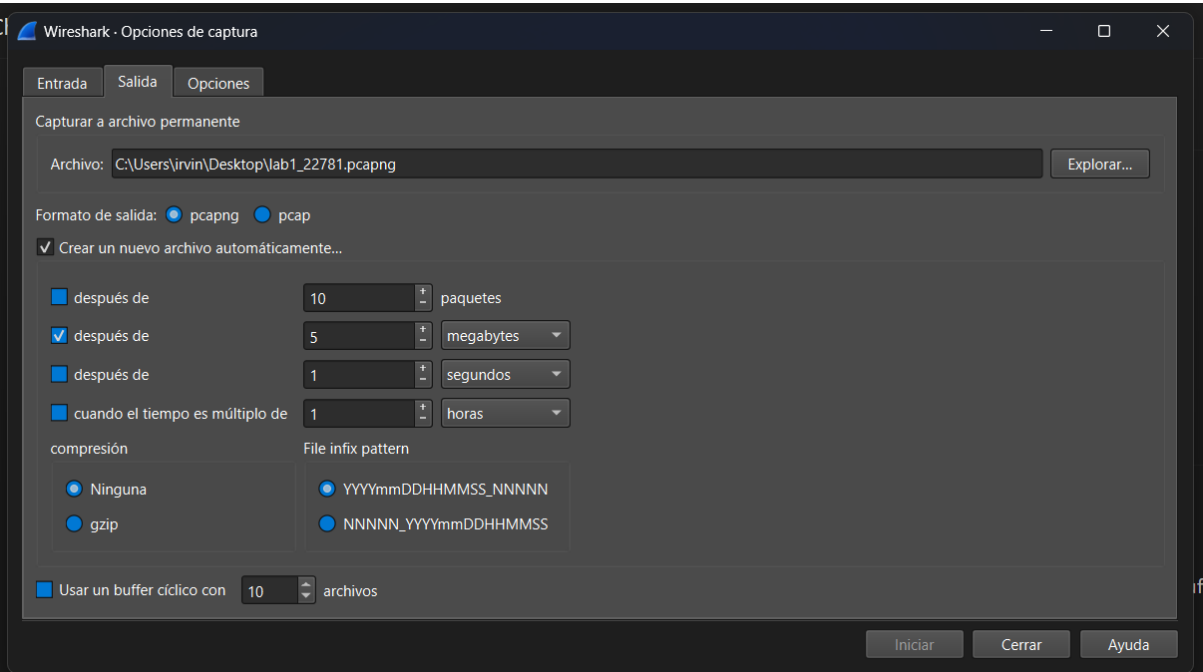
- DNS Suffix: lan es el nombre de la red local
- IPv6 link-local: dirección automática para comunicación local
- Ipv4: es la dirección IP que asigna el router de la red Wi-fi
- Subnet mask: 255.255.255.0 es una subred de 256 direcciones
- Default Gateway: 192.168.86.1 es la dirección del router

Por último, el Ethernet Bluetooth Network Connection es el adaptador de red para conexiones Bluetooth y según lo mostrado está desconectado.

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



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)



lab1_22781_20250713183312_00001	13/07/2025 06:33 p. m.	Wireshark capture ...	4,884 KB
lab1_22781_20250713183321_00002	13/07/2025 06:33 p. m.	Wireshark capture ...	4,885 KB
lab1_22781_20250713183322_00003	13/07/2025 06:33 p. m.	Wireshark capture ...	4,884 KB
lab1_22781_20250713183328_00004	13/07/2025 06:33 p. m.	Wireshark capture ...	4,883 KB
lab1_22781_20250713183334_00005	13/07/2025 06:33 p. m.	Wireshark capture ...	4,883 KB
lab1_22781_20250713183343_00006	13/07/2025 06:33 p. m.	Wireshark capture ...	4,901 KB
lab1_22781_20250713183348_00007	13/07/2025 06:33 p. m.	Wireshark capture ...	4,885 KB
lab1_22781_20250713183359_00008	13/07/2025 06:34 p. m.	Wireshark capture ...	4,883 KB
lab1_22781_20250713183404_00009	13/07/2025 06:34 p. m.	Wireshark capture ...	4,884 KB
lab1_22781_20250713183410_00010	13/07/2025 06:34 p. m.	Wireshark capture ...	4,884 KB
lab1_22781_20250713183419_00011	13/07/2025 06:34 p. m.	Wireshark capture ...	4,885 KB
lab1_22781_20250713183423_00012	13/07/2025 06:34 p. m.	Wireshark capture ...	4,884 KB
lab1_22781_20250713183427_00013	13/07/2025 06:34 p. m.	Wireshark capture ...	4,883 KB

lab1_22781_20250713183338.0001.pcapng

Archivo Edición Visualización F Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... «Ctrl+F»

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
2	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
3	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
4	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
5	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
6	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
7	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
8	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
9	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
10	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
11	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
12	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
13	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466 Encrypted Data	
14	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
15	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
16	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
17	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
18	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
19	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	
20	0.000000	200.12.61.216	192.168.86.29	SSLv2	1466	

Frame 1: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Device\NPF_{7795...} (04:ec:d8:62:45:b2) (04:ec:d8:62:45:b2)

Ethernet II, Src: Google_Adaptiva (1c:f2:9a:ad:a5:ea), Dst: Intel_62:45:b2 (04:ec:d8:62:45:b2)

Internet Protocol Version 4, Src: 200.12.61.216, Dst: 192.168.86.29

Transmission Control Protocol, Src Port: 443, Dst Port: 55585, Seq: 1, Ack: 1, Len: 1412

Transport Layer Security

lab1_22781_20250713183332.0000.pcapng

Archivo Edición Visualización F Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... «Ctrl+F»

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.18.33.206	192.168.86.29	TLSv1.2	924	Encrypted Data (SSL Record)
2	0.000000	104.18.33.206	192.168.86.29	TLSv1.2	186	Application Data
3	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=927 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
4	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=2359 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
5	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=3751 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
6	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=5163 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
7	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=6575 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
8	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=7987 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
9	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=9399 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
10	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=10811 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
11	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=12223 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
12	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=13635 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
13	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=15047 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 14]
14	0.000000	104.18.33.206	192.168.86.29	TLSv1.2	920	Application Data
15	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=17333 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 20]
16	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=18745 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 20]
17	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=20157 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 20]
18	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=21569 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 20]
19	0.000000	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=22981 Ack=1 Win=17 Len=1412 [TCP PDU reassembled in 20]
20	0.000000	104.18.33.206	192.168.86.29	TLSv1.2	1750	Application Data

Frame 1: 928 bytes on wire (7424 bits), 928 bytes captured (7424 bits) on interface \Device\NPF_{7795...} (04:ec:d8:62:45:b2) (04:ec:d8:62:45:b2)

Ethernet II, Src: Google_Adaptiva (1c:f2:9a:ad:a5:ea), Dst: Intel_62:45:b2 (04:ec:d8:62:45:b2)

Internet Protocol Version 4, Src: 104.18.33.206, Dst: 192.168.86.29

Transmission Control Protocol, Src Port: 443, Dst Port: 55464, Seq: 1, Ack: 1, Len: 874

Transport Layer Security

lab1_22781_20250713183321.0000.pcapng

Archivo Edición Visualización F Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... «Ctrl+F»

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.18.33.206	192.168.86.29	TLSv1.2	85	Application Data
2	0.000000	192.168.86.29	104.18.33.206	TCP	54	55464 → 443 [ACK] Seq=459 Ack=32 Win=255 Len=0
3	0.000000	104.18.33.206	192.168.86.29	TCP	60	443 → 55464 [ACK] Seq=32 Ack=459 Win=17 Len=0
4	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	227	Application Data
5	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1445	Application Data
6	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1445	Application Data
7	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1466	Application Data
8	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1424	Application Data
9	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1466	Application Data
10	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1466	Application Data
11	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	1403	Application Data
12	0.000559	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=9942 Ack=459 Win=17 Len=1412 [TCP PDU reassembled in 15]
13	0.000559	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=11354 Ack=459 Win=17 Len=1412 [TCP PDU reassembled in 15]
14	0.000559	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=12766 Ack=459 Win=17 Len=1412 [TCP PDU reassembled in 15]
15	0.000559	104.18.33.206	192.168.86.29	TLSv1.2	69	Application Data
16	0.000627	192.168.86.29	104.18.33.206	TCP	54	55464 → 443 [ACK] Seq=459 Ack=14193 Win=255 Len=0
17	0.000519	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=14193 Ack=459 Win=17 Len=1412 [TCP PDU reassembled in 20]
18	0.000519	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=15605 Ack=459 Win=17 Len=1412 [TCP PDU reassembled in 20]
19	0.000519	104.18.33.206	192.168.86.29	TCP	1466	443 → 55464 [ACK] Seq=17017 Ack=459 Win=17 Len=1412 [TCP PDU reassembled in 20]
20	0.000519	104.18.33.206	192.168.86.29	TLSv1.2	69	Application Data

Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{7795...} (04:ec:d8:62:45:b2) (04:ec:d8:62:45:b2)

Ethernet II, Src: Intel_62:45:b2 (04:ec:d8:62:45:b2), Dst: Google_Adaptiva (1c:f2:9a:ad:a5:ea)

Internet Protocol Version 4, Src: 104.18.33.206, Dst: 192.168.86.29

Transmission Control Protocol, Src Port: 443, Dst Port: 55464, Seq: 1, Ack: 1, Len: 31

Transport Layer Security

lab1_22781_20250713183332.0000.pcapng

Archivo Edición Visualización F Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... «Ctrl+F»

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.86.29	104.18.32.47	TLSv1.2	93	Application Data
2	0.000074	192.168.86.29	172.64.155.209	TLSv1.2	93	Application Data
3	0.005261	172.64.155.209	192.168.86.29	TLSv1.2	93	Application Data
4	0.005261	104.18.32.47	192.168.86.29	TCP	60	443 → 55190 [ACK] Seq=1 Ack=40 Win=159 Len=0
5	0.005261	104.18.32.47	192.168.86.29	TLSv1.2	93	Application Data
6	0.046842	192.168.86.29	172.64.155.209	TCP	54	55426 → 443 [ACK] Seq=40 Ack=40 Win=255 Len=0
7	0.046842	192.168.86.29	104.18.32.47	TCP	54	55190 → 443 [ACK] Seq=40 Ack=40 Win=510 Len=0
8	0.502942	192.168.86.29	200.12.61.216	TLSv1.2	956	Application Data
9	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=1 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
10	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=1413 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
11	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=2825 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
12	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=4237 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
13	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=5649 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
14	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=7061 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
15	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=8473 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
16	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=9885 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
17	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=11297 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
18	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=12709 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
19	0.512720	200.12.61.216	192.168.86.29	TCP	1466	443 → 55364 [ACK] Seq=14121 Ack=903 Win=2024 Len=1412 [TCP PDU reassembled in 20]
20	0.512720	200.12.61.216	192.168.86.29	TLSv1.2	928	Application Data

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{7795...} (04:ec:d8:62:45:b2) (04:ec:d8:62:45:b2)

Ethernet II, Src: Intel_62:45:b2 (04:ec:d8:62:45:b2), Dst: Google_Adaptiva (1c:f2:9a:ad:a5:ea)

Internet Protocol Version 4, Src: 192.168.86.29, Dst: 104.18.32.47

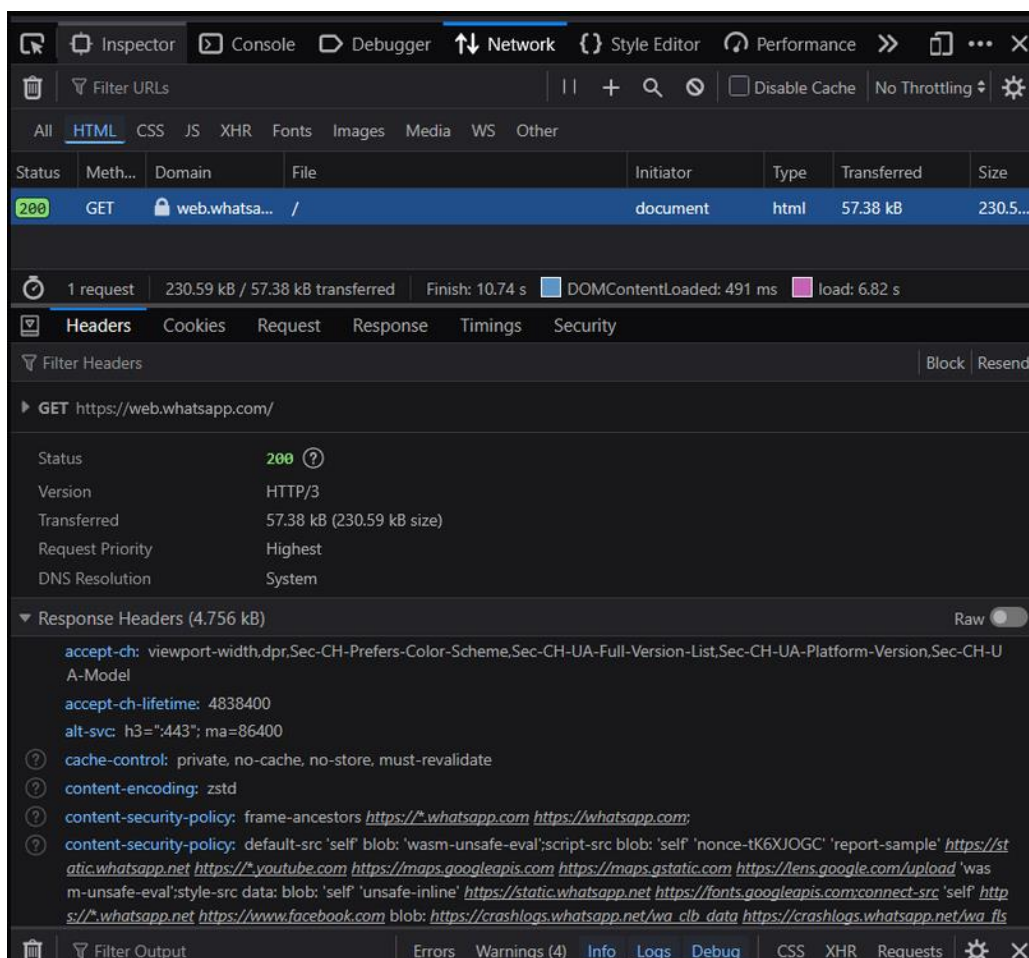
Transmission Control Protocol, Src Port: 55190, Dst Port: 443, Seq: 1, Ack: 1, Len: 39

Transport Layer Security

1.3 Análisis de paquetes



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

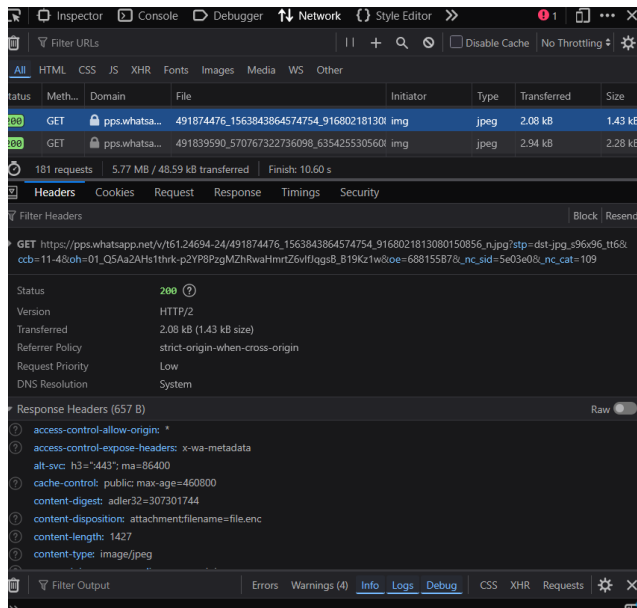


Como tal no es posible observar la versión HTTP del navegador a través de la imagen capturada con wireshark, sino solo Tráfico TLSv1.2 y TLSv1.3, Handshake de TLS y

Datos de aplicación cifrados. Esto se debe a que cuando el navegador usa HTTPS, la solicitudes y respuestas HTTP se cifran con TLS, por lo que Wireshark solo muestra los registros TLS.

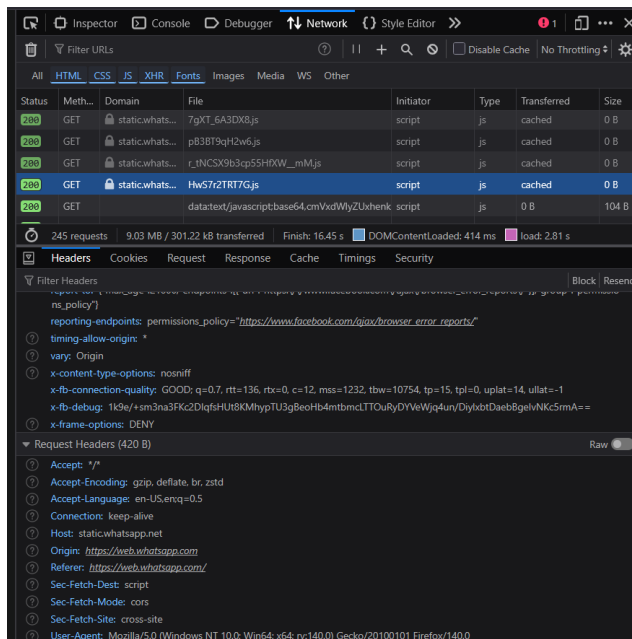
Alternativamente al revisar desde las devtools del navegador se puede saber que está usando HTTP/3.

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



Al igual que la pregunta anterior, se puede saber que versión de HTTP está usando el servidor porque están cifrados y Wireshark solo muestra el tráfico TLS. Pero según las devtools, el servidor está usando la versión HTTP/2

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



contenido en inglés de EE.UU. (en-US) con preferencia principal, y en inglés general (en) con menor prioridad (q=0.5).

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

No se puede saber con exactitud, depende de la request.

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

Lo más conveniente sería capturar paquetes tanto en el lado del cliente como en puntos intermedios de la red, de ser posible, en el servidor. En el cliente se puede observar la latencia elevada o pérdida de paquetes; en la red intermedia se pueden identificar cuellos de botella; en el servidor se pueden observar los tiempo de respuesta de la aplicación, aceptación de conexiones y rendimiento de las respuestas.

Acerca de si es conveniente instalar Wireshark en el servidor, lo es si es posible y seguro, pues permitiría analizar en detalle la llegada de solicitudes y las respuesta. Empero es prudente considerar que realizar esta captura podría también causar un impacto en el rendimiento.