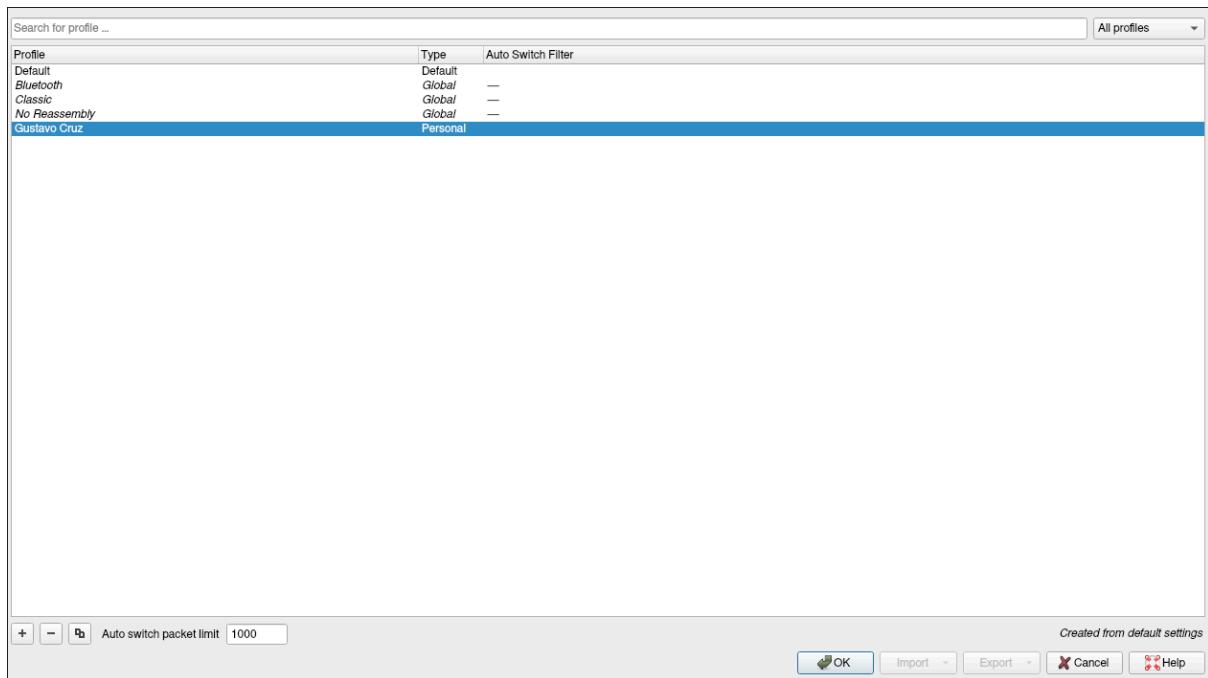


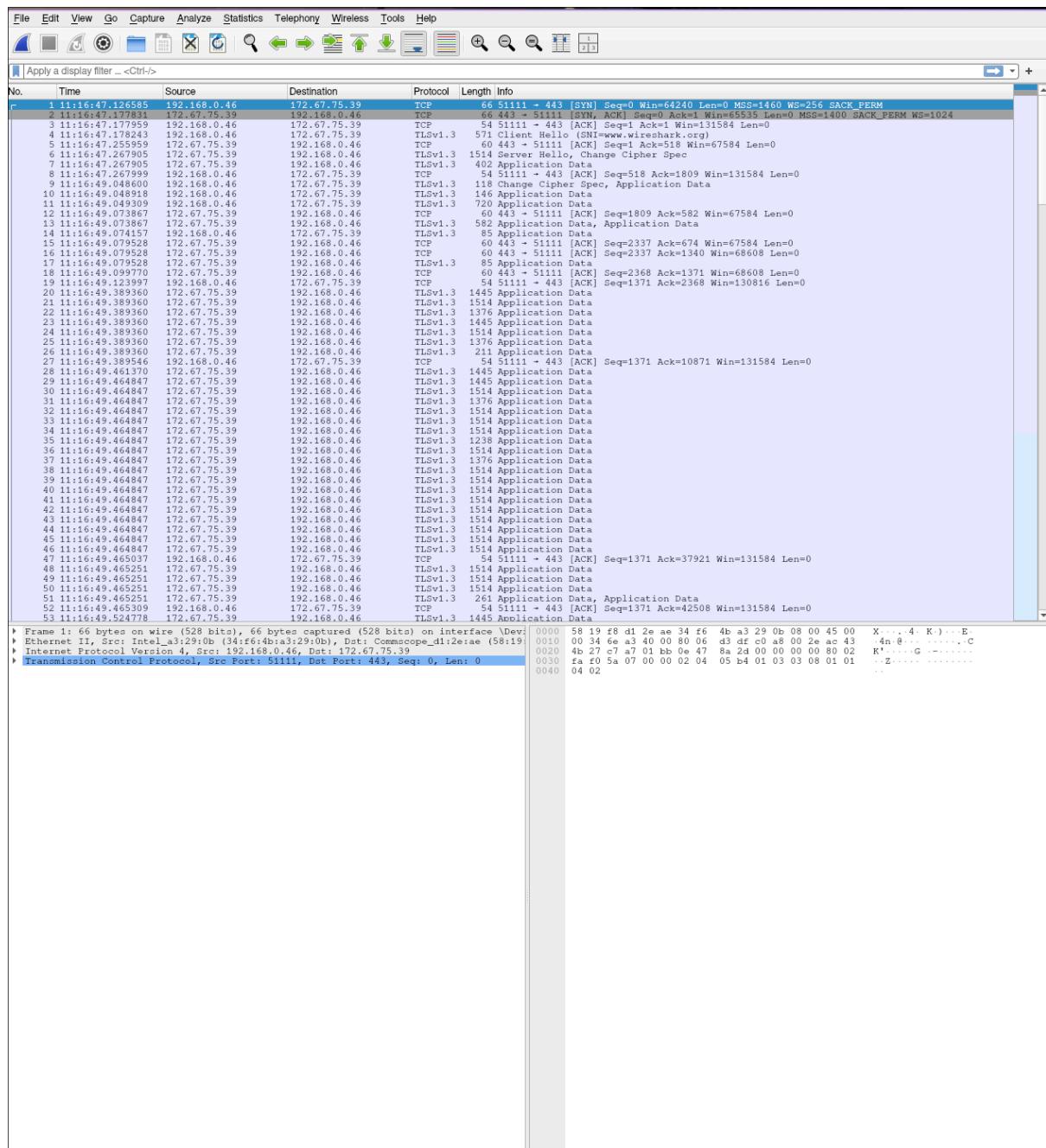
Universidad del Valle de Guatemala
Redes
Jorge Yass

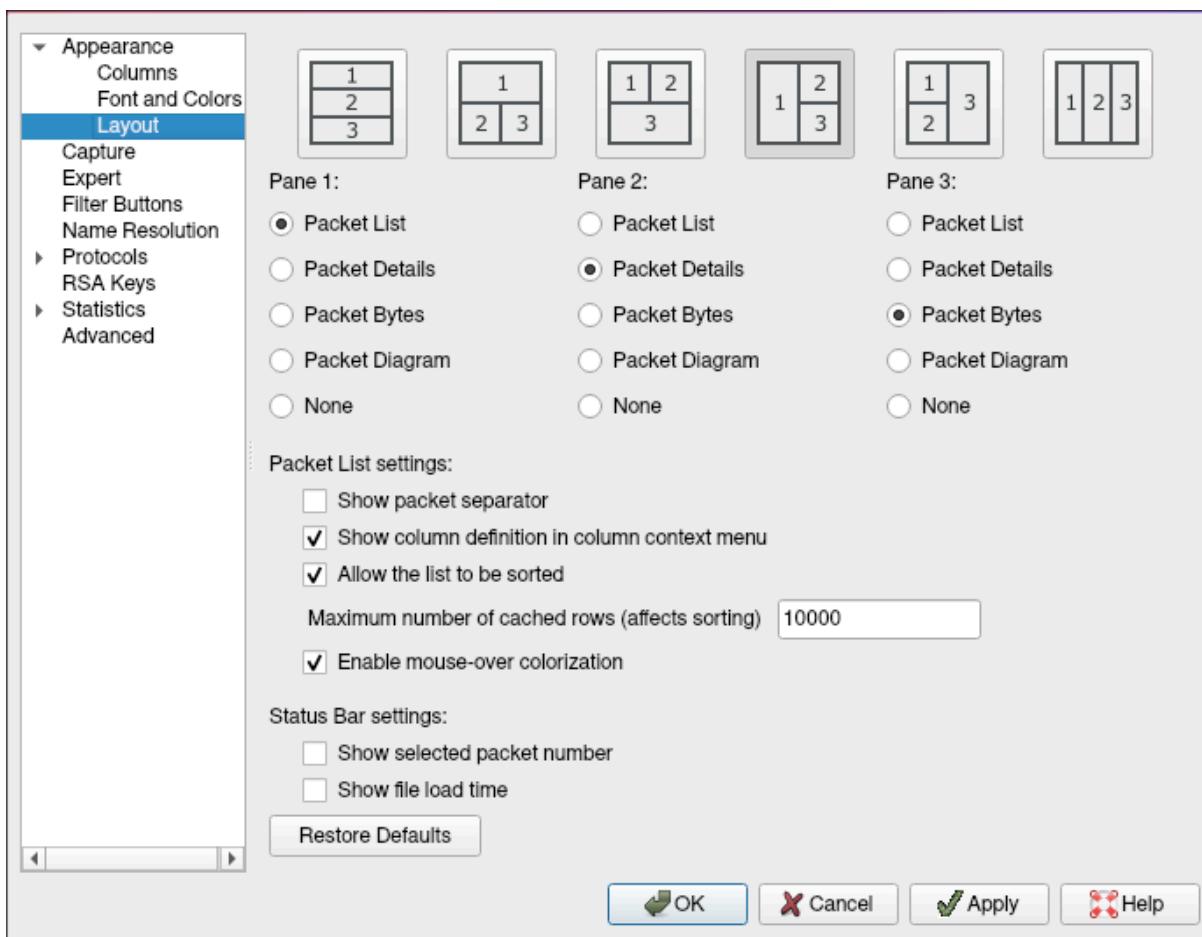
Laboratorio 1

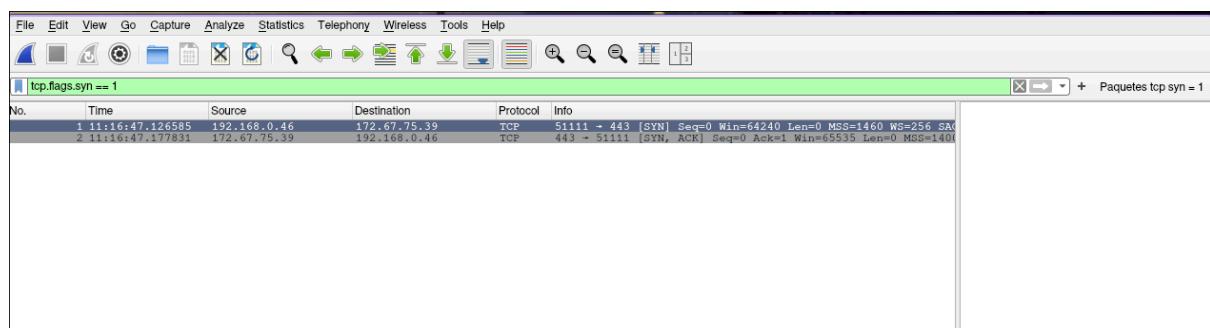
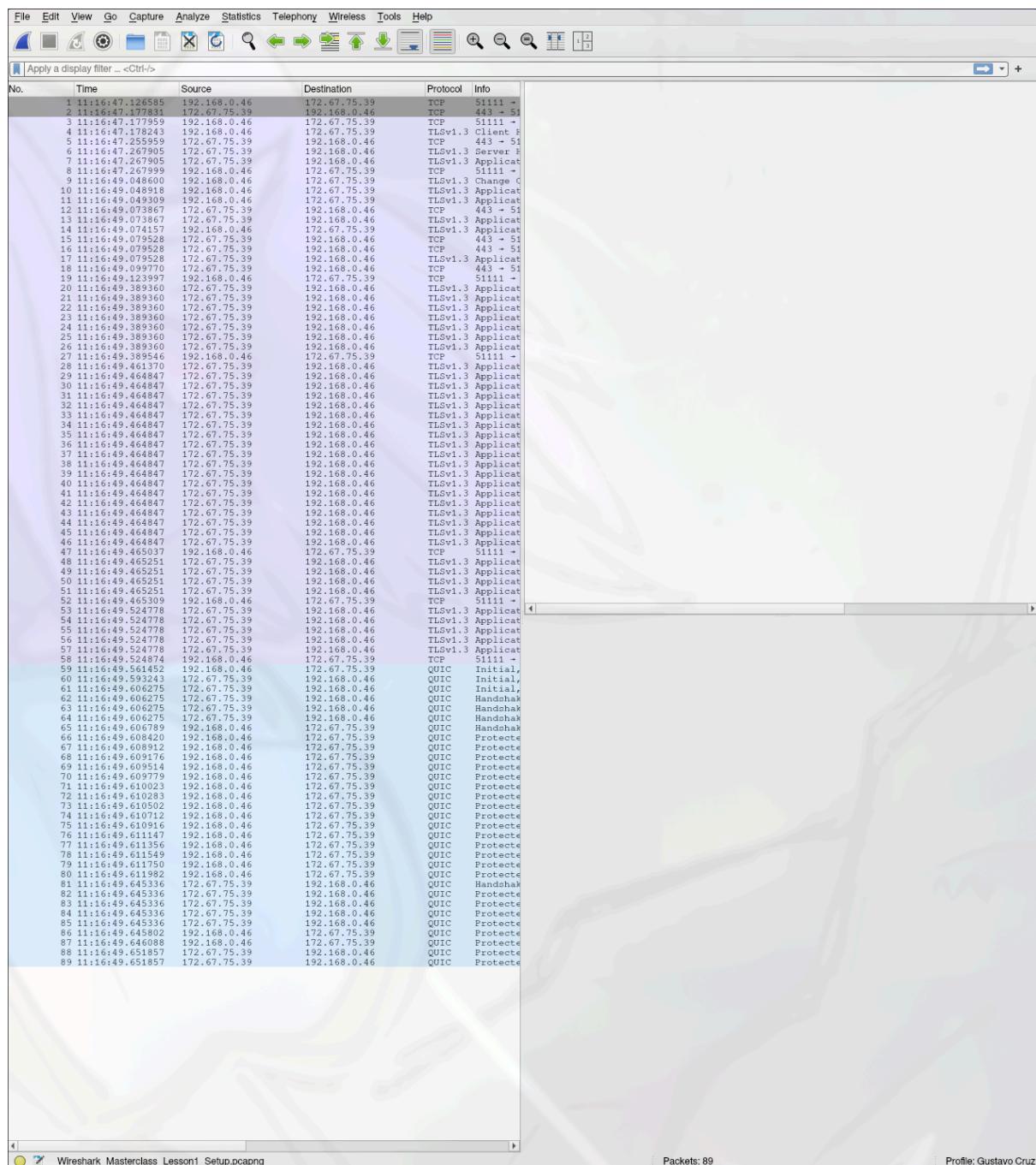
Gustavo Adolfo Cruz Bardales
22779

1.1 Personalización de entorno









1.2

1.

```
> ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp7s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 58:11:22:4e:00:6a brd ff:ff:ff:ff:ff:ff
    altname enx5811224e006a
        inet 192.168.1.88/24 metric 100 brd 192.168.1.255 scope global dynamic enp7s0
            valid_lft 80642sec preferred_lft 80642sec
        inet6 2800:98:1116:221f:5a11:22ff:fe4e:6a/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 431837sec preferred_lft 431837sec
        inet6 fe80::5a11:22ff:fe4e:6a/64 scope link proto kernel_ll
            valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether ec:2e:98:16:99:67 brd ff:ff:ff:ff:ff:ff
```

Comentarios

En mi caso, tengo 3 redes, una lo que es el localhost, otra red llamada enp7s0 y esa es mi tarjeta de red por cable, que es la utilizada mientras hago el lab con ipv4: 192.168.1.88 que es la que ha dado mi router con configuración DHCP para mi computadora.. También está wlan0 que es tarjeta inalámbrica pero en este momento no está conectada y como se puede ver tampoco tiene su dirección ip por eso.

2.

3. No entendí como utilizar la GUI debido a que me daba errores, por lo que use la ArchWiki para usar wireshark por medio de la consola, y realice las pruebas haciendo ping a archlinux.org y guardando la información en un lab1_22779.pcapng

```
> sudo dumpcap -i 1 \
-b filesize:5120 \
-b files:10 \
-w /tmp/lab1_22779.pcapng
Capturing on 'enp7s0'
File: /tmp/lab1_22779_00001_20250713184425.pcapng
Packets: 3369 File: /tmp/lab1_22779_00002_20250713184811.pcapng
Packets: 5663
```

```
> sudo dumpcap -i 1 \
-b filesize:5120 \
-b files:10 \
-w /tmp/lab1_22779.pcap

Capturing on 'enp7s0'
File: /tmp/lab1_22779_00001_20250713184014.pcap
Packets captured: 862
Packets received/dropped on interface 'enp7s0': 862/0 (100.0%)
> sudo dumpcap -i 1 \
-b filesize:5120 \
-b files:10 \
-w /tmp/lab1_22779.pcapng

Capturing on 'enp7s0'
File: /tmp/lab1_22779_00001_20250713184115.pcapng
Packets: 146 [
```

```
ssdm-auth-1ddc6d3e-601f-4d70-aa-03-83139749fb58
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-bluetooth.service-VgRNju
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-dbus-broker.service-oXClI3
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-polkit.service-d60cGA
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-systemd-logind.service-U1ZVpP
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-upower.service-Js7G78
wireshark_enps0t1ZU92.pcapng
    ls
cab2b21a0-9ddc-4b6f-88fa-b16b030577d2.zip
lab1_22779_00001_20250713183843.pcap
ssdm-auth-0-qySLPU
ssdm-auth-1ddc6d3e-601f-4d70-aa-03-83139749fb58
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-bluetooth.service-VgRNju
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-dbus-broker.service-oXClI3
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-polkit.service-d60cGA
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-systemd-logind.service-U1ZVpP
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-upower.service-Js7G78
wireshark_enps0t1ZU92.pcapng
    rm lab1_22779_00001_20250713183843.pcap
rm: remove write-protected regular file 'lab1_22779_00001_20250713183843.pcap'?
y
rm: cannot remove 'lab1_22779_00001_20250713183843.pcap': Operation not permitted
    sudo rm lab1_22779_00001_20250713183843.pcap
[sudo] password for gustavo:
Sorry, try again.
[sudo] password for gustavo:
    ls
cab2b21a0-9ddc-4b6f-88fa-b16b030577d2.zip
lab1_22779_00001_20250713184014.pcap
ssdm-auth-0-qySLPU
ssdm-auth-1ddc6d3e-601f-4d70-aa-03-83139749fb58
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-bluetooth.service-VgRNju
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-dbus-broker.service-oXClI3
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-polkit.service-d60cGA
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-systemd-logind.service-U1ZVpP
systemd-private_98cfa093c69f049d7a15bb9b5851a3e27-upower.service-Js7G78
wireshark_enps0t1ZU92.pcapng
```

```

64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=135 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=136 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=137 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=138 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=139 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=140 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=141 ttl=46 time=182 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=142 ttl=46 time=179 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=143 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=144 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=145 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=146 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=147 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=148 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=149 ttl=46 time=179 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=150 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=151 ttl=46 time=178 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=152 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=153 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=154 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=155 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=156 ttl=46 time=174 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=157 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=158 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=159 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=160 ttl=46 time=174 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=161 ttl=46 time=183 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=162 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=163 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=164 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=165 ttl=46 time=176 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=166 ttl=46 time=177 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=167 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=168 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=169 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=170 ttl=46 time=175 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=171 ttl=46 time=178 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=172 ttl=46 time=174 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=173 ttl=46 time=174 ms
64 bytes from archlinux.org (2a01:4f9:c010:6b1f::1): icmp_seq=174 ttl=46 time=177 ms

```

```

❯ sudo dumpcap -i 1 \
-b filesize:5120 \
-b files:10 \
-w /tmp/lab1_22779.pcap

Capturing on 'enp5s0'
File: /tmp/lab1_22779_00001_20250713184014.pcap
Packets captured: 862
Packets received/dropped on interface 'enp5s0': 862/0 (pcap:0/dumpcap:0/flushed :/0/ps_ifdrop:0) (100.0%)
❯ sudo dumpcap -i 1 \
-b filesize:5120 \
-b files:10 \
-w /tmp/lab1_22779.pcapng
Capturing on 'enp5s0'
File: /tmp/lab1_22779_00001_20250713184115.pcapng
Packets: 7020

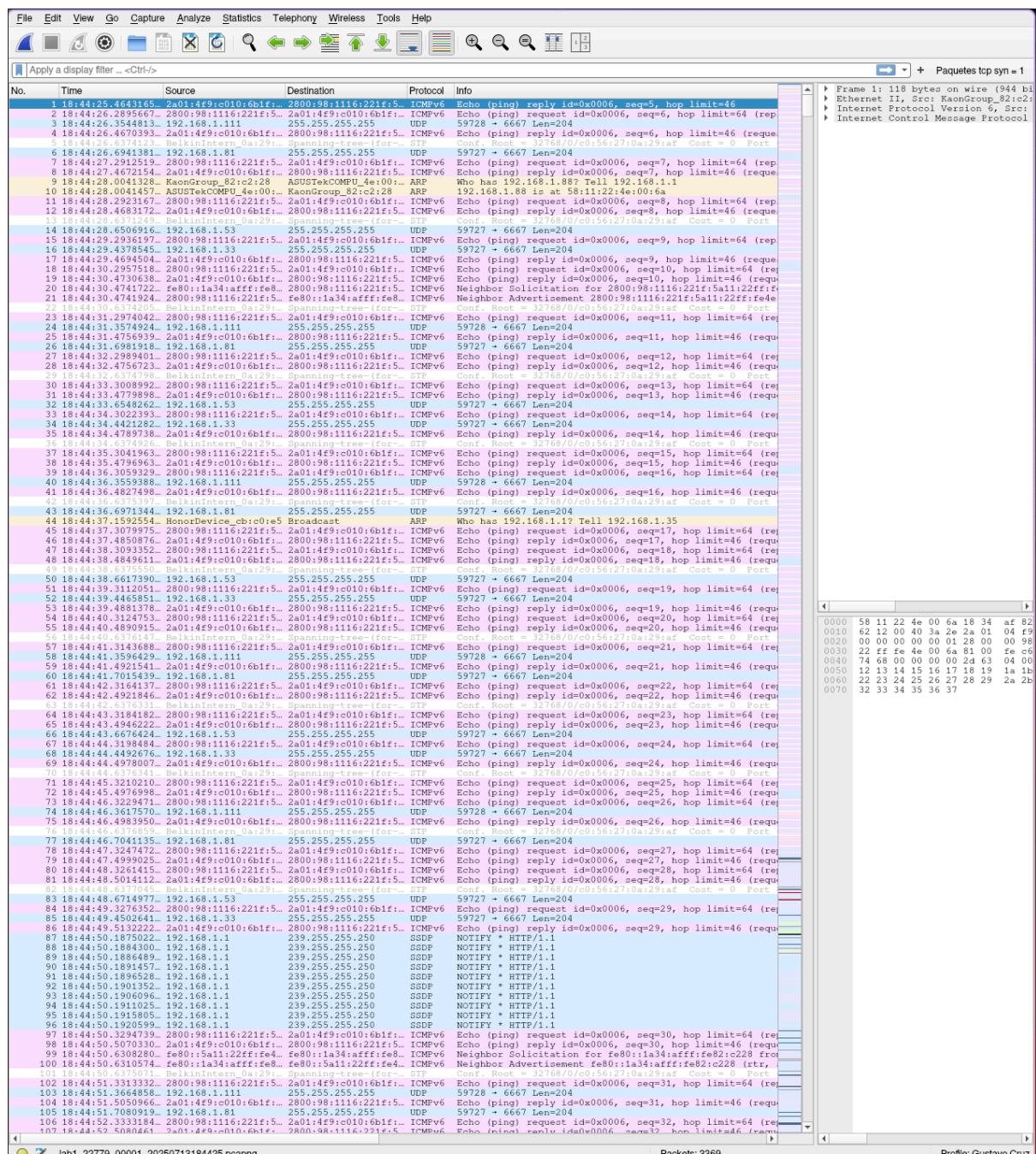
```

```

sddm-auth-1dc6de3-601f-4d70-aa03-83139749fb58
systemd-private-98cf039c69f049d7a158bb95851a3e27-bluetooth.service-VgRNju
systemd-private-98cf039c69f049d7a158bb95851a3e27-dbus-broker.service-0xCl3
systemd-private-98cf039c69f049d7a158bb95851a3e27-polkit.service-d60cGA
systemd-private-98cf039c69f049d7a158bb95851a3e27-systemd-logind.service-U1ZVpP
systemd-private-98cf039c69f049d7a158bb95851a3e27-upower.service-Js7G78
wireshark_enp7s0IZ1U92.pcapng
❯ ls
ca2b21a0-9ddc-4b6f-88fa-b16b030577d2.zip
lab1_22779_00001_20250713183843.pcap
sddm-0-qySLPU
sddm-auth-1dc6de3-601f-4d70-aa03-83139749fb58
systemd-private-98cf039c69f049d7a158bb95851a3e27-bluetooth.service-VgRNju
systemd-private-98cf039c69f049d7a158bb95851a3e27-dbus-broker.service-0xCl3
systemd-private-98cf039c69f049d7a158bb95851a3e27-polkit.service-d60cGA
systemd-private-98cf039c69f049d7a158bb95851a3e27-systemd-logind.service-U1ZVpP
systemd-private-98cf039c69f049d7a158bb95851a3e27-upower.service-Js7G78
wireshark_enp7s0IZ1U92.pcapng
❯ rm lab1_22779_00001_20250713183843.pcap
rm: remove write-protected regular file 'lab1_22779_00001_20250713183843.pcap'?
rm: cannot remove 'lab1_22779_00001_20250713183843.pcap': Operation not permitted
❯ sudo rm lab1_22779_00001_20250713183843.pcap
[sudo] password for gustavo:
Sorry, try again.
[sudo] password for gustavo:
❯ ls
ca2b21a0-9ddc-4b6f-88fa-b16b030577d2.zip
lab1_22779_00001_20250713184014.pcap
sddm-0-qySLPU
sddm-auth-1dc6de3-601f-4d70-aa03-83139749fb58
systemd-private-98cf039c69f049d7a158bb95851a3e27-bluetooth.service-VgRNju
systemd-private-98cf039c69f049d7a158bb95851a3e27-dbus-broker.service-0xCl3
systemd-private-98cf039c69f049d7a158bb95851a3e27-polkit.service-d60cGA
systemd-private-98cf039c69f049d7a158bb95851a3e27-systemd-logind.service-U1ZVpP
systemd-private-98cf039c69f049d7a158bb95851a3e27-upower.service-Js7G78
wireshark_enp7s0IZ1U92.pcapng

```

at 18:40:33



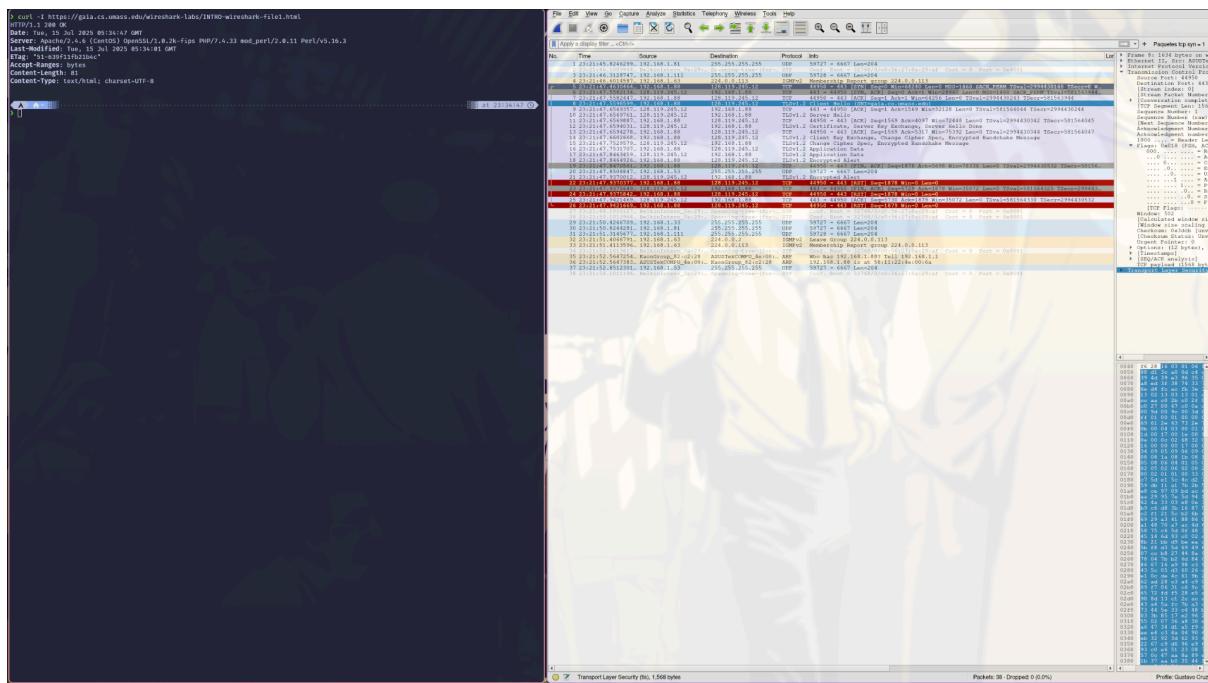
1.3

Comentarios

Para esta parte del laboratorio me fue imposible sacar las peticiones http. Se borro la cache del navegador antes de iniciar a grabar, luego se inició a grabar, se abrió el navegador e introdujo la dirección, sin embargo siempre que accedía me salía esto en wireshark, que eran peticiones cifradas en tls. Finalmente abrí una consola y cerré el navegador, repetí los pasos e hice un curl -I para asegurar que la petición realizada era HTTP y que mi navegador

(firefox) no convertía http a https. Sin embargo siempre seguía cifrado como la imagen, por lo que finalmente tomé los datos del servidor usando curl y abriendo otras pestañas http obtuve los datos de mi maquina. Con eso conteste las preguntas.

9 23:21:47.6569357...	128.119.245.12	192.168.1.88	TCP	443 - 44950 [ACK] Seq=1 Ack=1569 Win=32128 Len=0 TStamp=581564044 TSecr=2994430244
10 23:21:47.6569761...	128.119.245.12	192.168.1.88	TLSv1.2	Server Hello
11 23:21:47.6569886...	128.119.245.12	192.168.1.88	TCP	44950 - 44953 [ACK] Seq=1569 Ack=4097 Win=72448 Len=0 TStamp=2994430342 TSecr=581564045
12 23:21:47.6569831...	128.119.245.12	192.168.1.88	TLSv1.2	Certificate, Server Key Exchange, Server Hello Done
13 23:21:47.6594278...	192.168.1.88	128.119.245.12	TCP	44950 - 44953 [ACK] Seq=1569 Ack=4097 Win=72448 Len=0 TStamp=2994430342 TSecr=581564045
14 23:21:47.6602668...	192.168.1.88	128.119.245.12	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
15 23:21:47.7529579...	128.119.245.12	192.168.1.88	TLSv1.2	Change Cipher Spec, Encrypted Handshake Message
16 23:21:47.7531707...	192.168.1.88	128.119.245.12	TLSv1.2	Application Data
17 23:21:47.8463459...	128.119.245.12	192.168.1.88	TLSv1.2	Application Data
18 23:21:47.8464926...	192.168.1.88	128.119.245.12	TLSv1.2	Encrypted Alert



```
> curl -I https://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1 200 OK
Date: Tue, 15 Jul 2025 05:34:47 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Tue, 15 Jul 2025 05:34:01 GMT
ETag: "51-639f11fb21b4c"
Accept-Ranges: bytes
Content-Length: 81
Content-Type: text/html; charset=UTF-8
```

3. Responda las siguientes preguntas:

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

HTTP/1.1 200 OK

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?

Wireshark solo recibió la petición cifrada con tls y en mi curl no me da esta información por lo que me fue imposible obtener esta respuesta.

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

81

e. En el caso que haya un problema de rendimiento mientras se descarga la página,

¿en qué elementos de la red convendría “escuchar” los paquetes?

¿Es conveniente instalar Wireshark en el servidor? Justifique

Considero que si hay problemas de rendimiento mientras se descarga la página convendría primero escuchar los paquetes en el cliente, o asegurarse que no se deba a un bajón de rendimiento debido a que la banda del cliente está siendo bastante utilizada al momento de abrir la web y esto haga que se quede sin ancho de banda en ese momento. Además, considero que no sería buena idea instalar wireshark debido a que este guarda información, o puede guardar en lugares como directorios como tmp en los servidores, y un backdoor en el servidor con la info de los clientes/usuarios no sería buena idea.

Discusión y hallazgos

Utilice Linux para hacer el laboratorio, y utilice las herramientas oficiales de wireshark. Sin embargo, como mencionaba tuve complicaciones al usar o capturar la llamada al servidor pues me lo cifraba. Debido a esto tuve que buscar alternativas, y una que encontre en la Arch Wiki(la mejor wiki) fue usar curl -I desde la terminal para asegurar que fuera una llamada HTTP y que mi navegador por una configuración que permite Firefox, no convierta de HTTP a HTTPS, sin embargo el resultado en wireshark fue el mismo. Sin embargo, con curl -I, pude obtener algunas respuestas para contestar el último inciso.

Además, aprendí a usar wireshark-cli, las herramientas de wireshark para la consola, debido a complicaciones que tuve, pero logré solucionar más adelante.

Conclusiones

Considero que wireshark es una herramienta bastante potente, que puede no ser tan intuitiva de usar, pero al poderla modificar para que se adapte a mis gustos y preferencias, facilita el aprendizaje. En lo personal, me gustó más la herramienta de terminal, debido a que era más sencilla de utilizar (con cuatro comandos pude tomar la captura de los 10 paquetes).

La documentación de wireshark en la arch wiki está bastante completa y facilita utilizarlo.

Referencias

<https://wiki.archlinux.org/title/Wireshark>

<https://wiki.archlinux.org/title/CURL>