

Estudiante: Adrian Peñaloza Ortega

DOC: 1005060452

Redes

Universidad de Pamplona

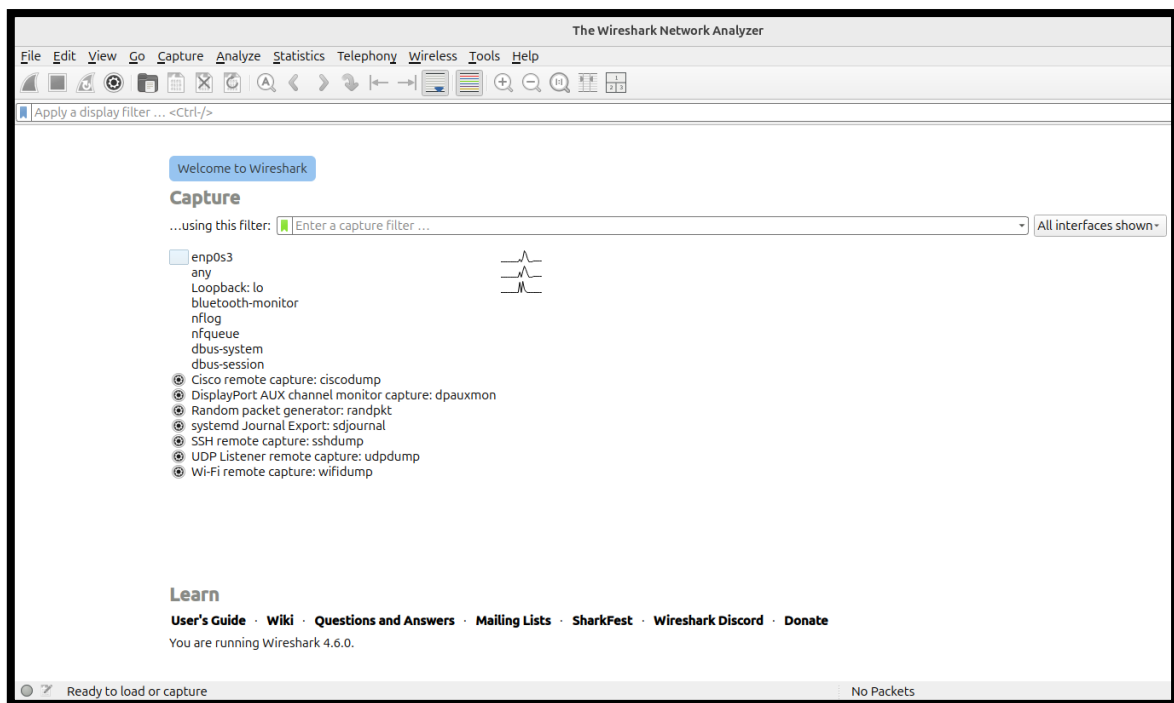
Pamplona - Colombia

2025



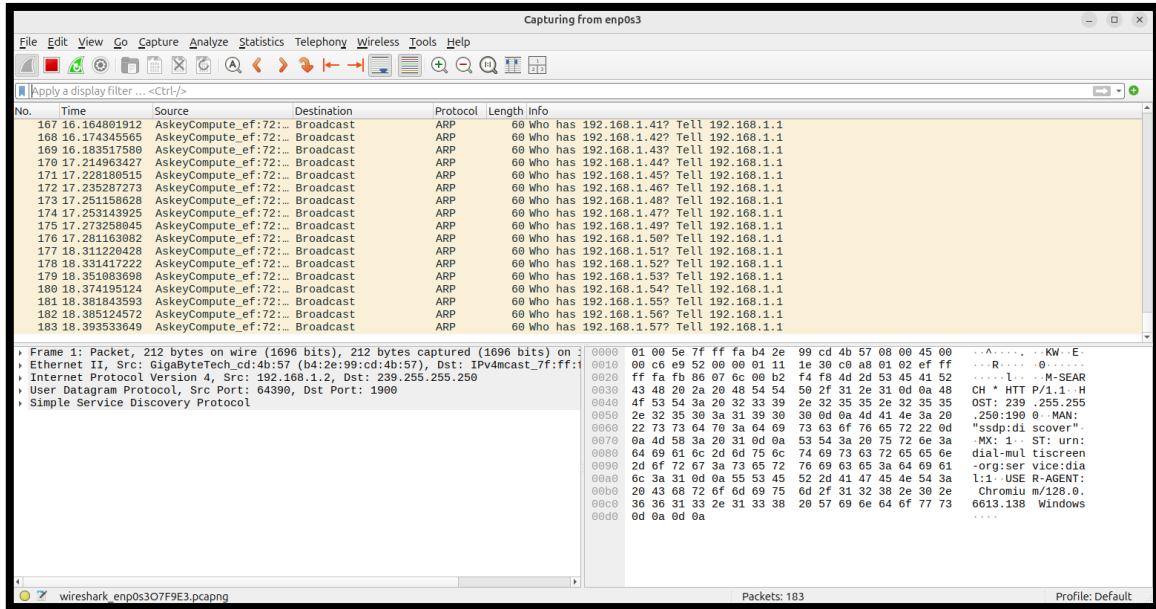
Punto 3: Documento wireshark con captura de mensajes intercambiados entre cliente y servidor de la captura remota.

Paso 1: Abrimos wireshark.



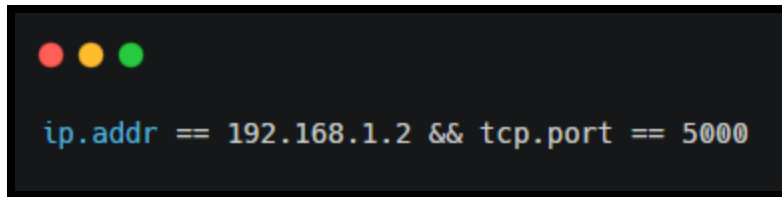
Paso 2: seleccionamos interface de captura, en este caso enp0s3 (el que tiene la ip de la red local **192.168.1.2** en este caso).

nos aparece un montón de paquetes:



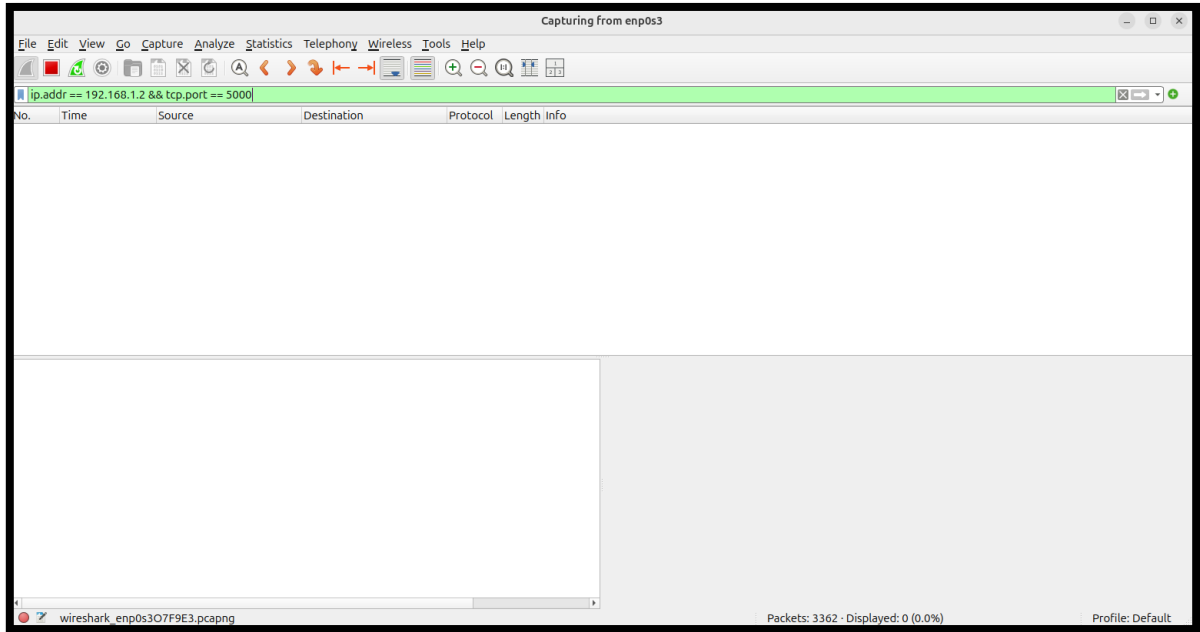
Paso 3: aplicar filtro para quedarnos con lo que nos interesa (la practica).

Aplicamos el siguiente filtro



este filtro tomara solo la ip del cliente (**192.168.1.2**) donde este como emisor o receptor y también que solo tome el puerto 5000, es la puerta de lo que desarrollamos (puerto usado en la práctica).





Aparece en blanco porque aun no hemos enviado paquetes, enviemos uno:

Paso 4: enviar paquete

Vamos a Windows y en la terminal ejecutamos el script **client.py** y especificamos la ip del servidor **192.168.1.6**

```
PS C:\Users\adrianspeedcode> py client.py 192.168.1.6
```

Y nos pedirá que escribamos la información (numero1, numero2, y operador)

```
PS C:\Users\adrianspeedcode> py client.py 192.168.1.6
Primer número: 1927
Segundo número: 1974
Operación (+, -, *, /): -
Resultado: -47
PS C:\Users\adrianspeedcode>
```

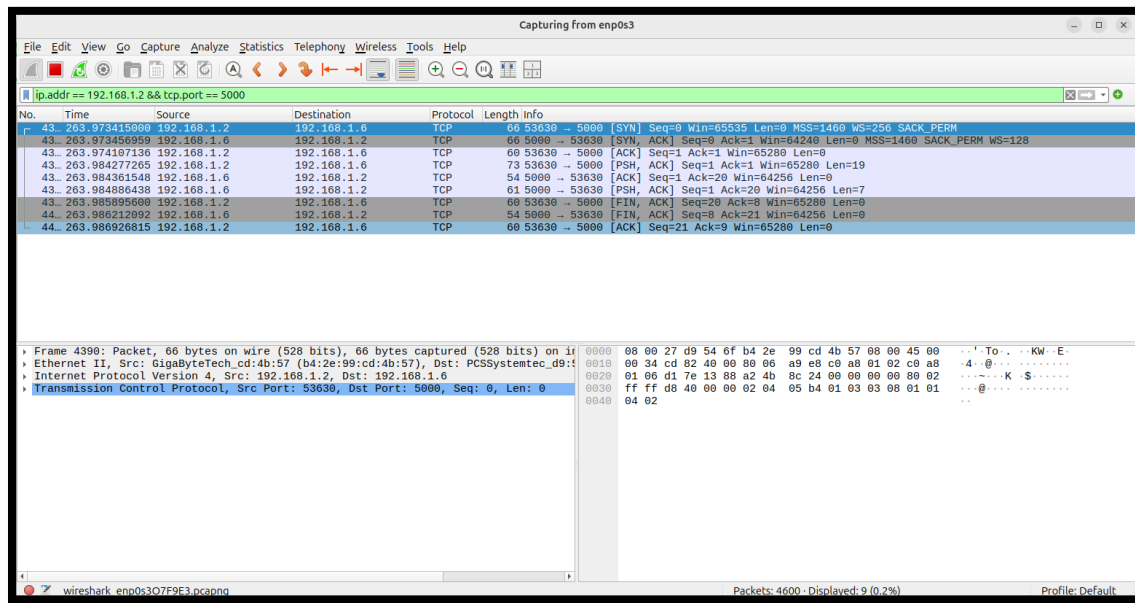
El paquete fue enviado, y nos respondió con el resultado de operar.

Paso 6: también podemos ver lo que esta respondiendo el servidor

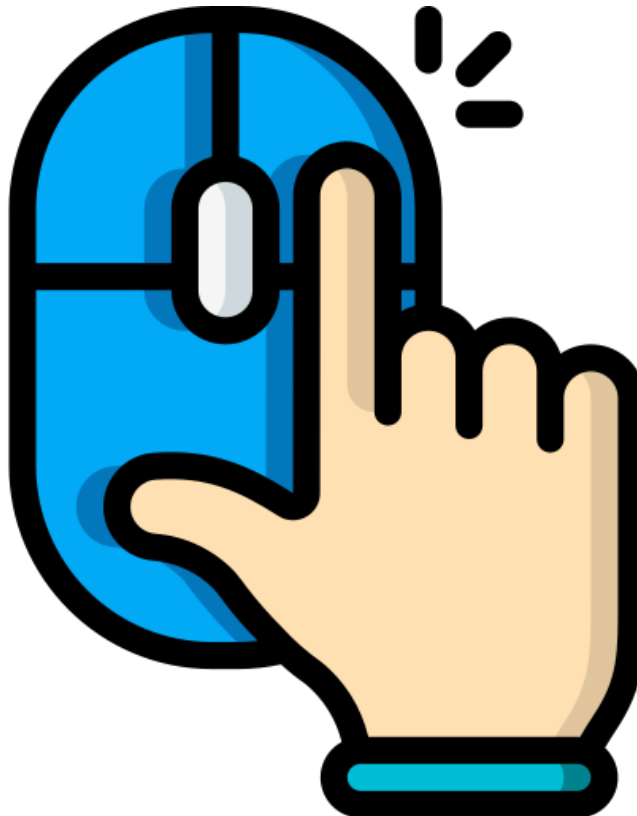
```
[ACCEPT] ('192.168.1.2', 53630)
[RX ('192.168.1.2', 53630)] OP - 1927.0 1974.0
[TX ('192.168.1.2', 53630)] OK -47
```

Paso 5: Verificar que wireshark capturo paquetes.

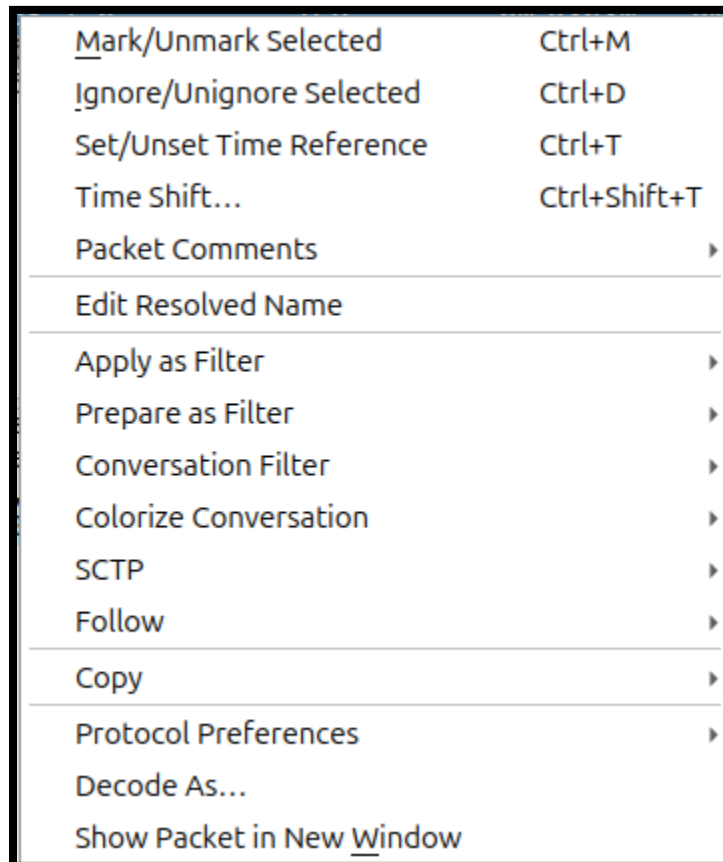
Volvemos a wireshark y vemos que efectivamente se capturaron los paquetes.



Paso 6: Verificar que el contenido que mandamos antes se puede observar selecciona cualquiera de los paquetes, y dale click derecho



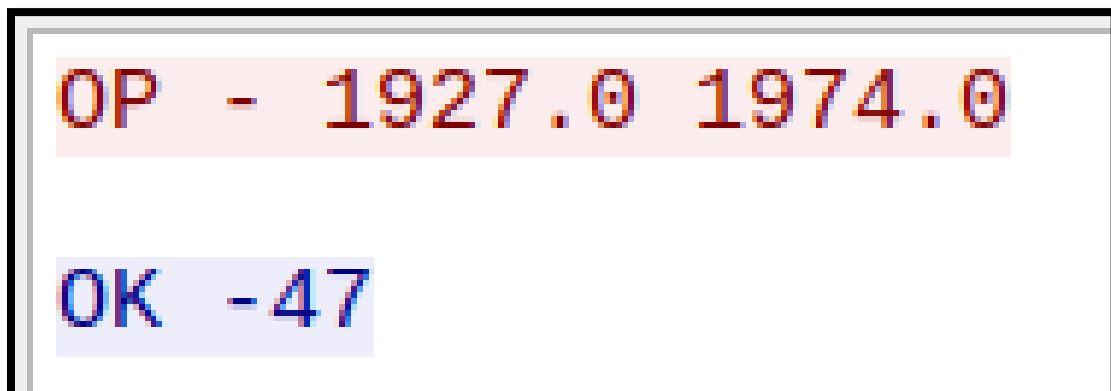
aparecerán estas opciones:



selecciono follow Y tcp stream



Aparecerá la informacion real que enviamos desde el cliente



Wireshark · Follow TCP Stream (tcp.stream eq 33) · enp0s3

OP - 1927.0 1974.0
OK -47

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (26 bytes)

Show as ASCII

No delta times

Stream 33

Find:

☐ Case sensitive

Find Next

Help

Filter Out This Stream

Print

Save as...

Back

Close