



Carrera: Ing. Sistemas de información

Materia: Redes de datos

Profesor: Ing. Juan Antonio González

Docente Laboratorio: Ing. Carlos José Alberto Carrizo



Alumna:



Apellido y Nombre	legajo
Enriquez, Sylvina	-----

Curso: 2025

## CONSIGNA TRABAJO PRÁCTICO 4

**Tema: Capa transporte. TCP/UDP, DNS, TELNET.**

Herramientas a utilizar: PC con Windows, aplicación Wireshark

## 1. Desde una PC con Windows:

- Abrir la aplicación Wireshark e iniciar el monitoreo sobre la placa de red con el modo promiscuo desactivado.
- Investigar y utilizar el comando *telnet* para verificar si el servidor web que hostea la facultad tiene abierto el puerto 80 o 443.
- Una vez ejecutada la verificación detener el monitoreo de Wireshark.

a) Buscar, en Wireshark, los paquetes de inicio de conexión TCP. Documentarlos.

b) Determinar el puerto origen y destino de la conexión. Documentarlo.

c) Seleccionar el primer paquete de conexión TCP y haga un seguimiento del Stream TCP. Para tal efecto seleccione el paquete, haga click al botón derecho y seleccione la opción "Follow - TCP Stream".

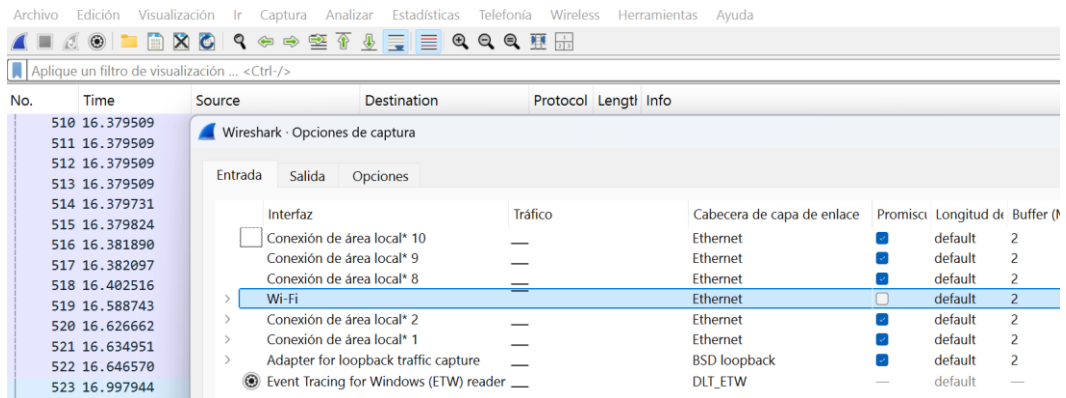
Analizar y comentar la salida visualizada. Si el transporte utilizado por el servicio es UDP, ¿cómo se puede verificar de forma remota si el puerto está abierto?

## Desarrollo del trabajo práctico 4

### Capa de transporte

Desde una PC con Windows:

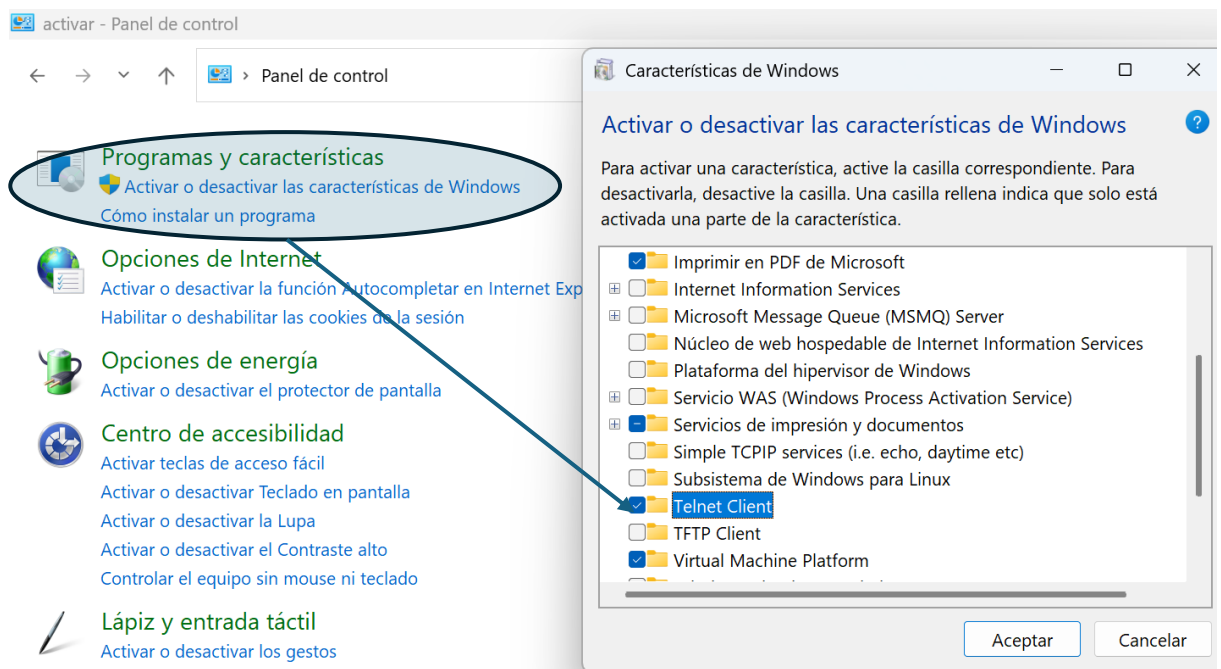
- Abrir la aplicación Wireshark e iniciar el monitoreo sobre la placa de red con el modo promiscuo desactivado.



- Investigar y utilizar el comando *telnet* para verificar si el servidor web que hostea la facultad tiene abierto el puerto 80 o 443.

```
C:\Users\sylvi>telnet www.frd.utn.edu.ar
"telnet" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
```

El comando *telnet* no se encontraba instalado, por lo que se procedió a activar esta opción desde el *Panel de control*:

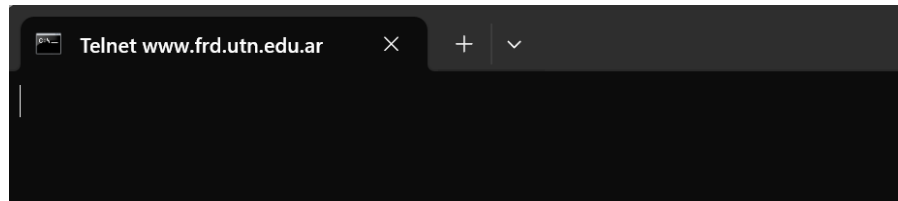


Una vez activada la característica de *telnet*, se ejecuta el comando *telnet www.frd.utn.edu.ar*

```
C:\Users\sylvi>telnet www.frd.utn.edu.ar
Conectándose a www.frd.utn.edu.ar...No se puede abrir la conexión al host, en puerto 23: Error en la conexión
```

No hubo conexión porque es necesario indicar el puerto 80 o 443, caso contrario, busca el puerto 23, que es el puerto que busca por defecto.

```
C:\Users\sylvia>telnet www.frd.utn.edu.ar 443
```



Se realiza la comunicación. El puerto 443 es un puerto que se utiliza en el protocolo https, por lo que está esperando una página web. Para interrumpir la conexión (o que muestre alguna contestación por pantalla) se procede a realizar algunos “enters” o espacios:

```
Símbolo del sistema
HTTP/1.1 400 Bad Request
Server: openresty
Date: Sun, 25 May 2025 01:23:35 GMT
Content-Type: text/html
Content-Length: 154
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>openresty</center>
</body>
</html>

Se ha perdido la conexión con el host.

C:\Users\sylvia>
```

- Una vez ejecutada la verificación detener el monitoreo de Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1199	62.056180	2a03:2880:f010:17:f...	2800:810:49c:8f9c:5...	TLSv1.2	112	Application Data
1200	62.104104	2800:810:49c:8f9c:5...	2a03:2880:f010:17:f...	TCP	74	51613 → 443 [ACK] Seq=161 Ack=191 Win=253 Len=0
1201	62.104171	2800:810:49c:8f9c:5...	2a03:2880:f010:c:fa...	TCP	74	51572 → 443 [ACK] Seq=4487 Ack=205 Win=252 Len=0
1202	62.959000	2800:810:49c:8f9c:5...	2a03:2880:f010:17:f...	TLSv1.2	106	Application Data
1203	62.978682	192.168.0.1	192.168.0.255	UDP	115	9431 → 9431 Len=73

- a) Buscar, en Wireshark, los paquetes de inicio de conexión TCP. Documentarlos.

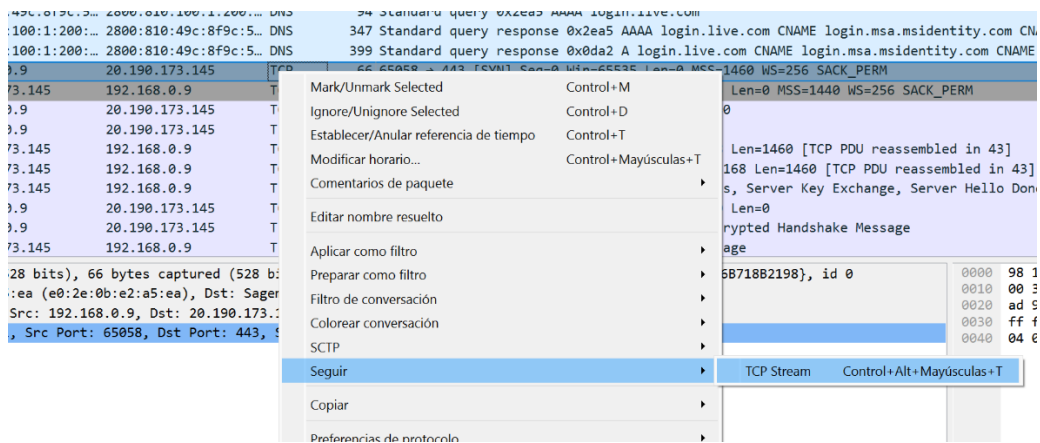
No.	Time	Source	Destination	Protocol	Length	Info
34	9.476096	2800:810:49c:8f9c:5...	2800:810:100:1:200:...	DNS	94	Standard query 0x2ea5 AAAA login.live.com
35	9.499145	2800:810:100:1:200:...	2800:810:49c:8f9c:5...	DNS	347	Standard query response 0x2ea5 AAAA login.live.com CNAME login.msa.msidentity.com CNAME ww...
36	9.499145	2800:810:100:1:200:...	2800:810:49c:8f9c:5...	DNS	399	Standard query response 0x0da2 A login.live.com CNAME login.msa.msidentity.com CNAME www.t...
37	9.502529	192.168.0.9	20.190.173.145	TCP	66	65058 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
38	9.553459	20.190.173.145	192.168.0.9	TCP	66	443 → 65058 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
39	9.553620	192.168.0.9	20.190.173.145	TCP	54	65058 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
40	9.557188	192.168.0.9	20.190.173.145	TLSv1.2	518	Client Hello (SNI=login.live.com)
41	9.615807	20.190.173.145	192.168.0.9	TCP	1514	443 → 65058 [ACK] Seq=1 Ack=465 Win=12583168 Len=1460 [TCP PDU reassembled in 43]
42	9.615807	20.190.173.145	192.168.0.9	TCP	1514	443 → 65058 [ACK] Seq=1461 Ack=465 Win=12583168 Len=1460 [TCP PDU reassembled in 43]
43	9.615807	20.190.173.145	192.168.0.9	TLSv1.2	1091	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done

b) Determinar el puerto origen y destino de la conexión. Documentarlo.

...	DNS	399	Standard query resp
	TCP	66	65058 → 443 [SYN] S
	TCP	66	443 → 65058 [SYN, A
	TCP	54	65058 → 443 [ACK] S

- Puerto origen: 65058
- Puerto destino: 443

c) Seleccionar el primer paquete de conexión TCP y haga un seguimiento del Stream TCP. Para tal efecto seleccione el paquete, haga click al botón derecho y seleccione la opción “Follow - TCP Stream”.



*Analizar y comentar la salida visualizada.*

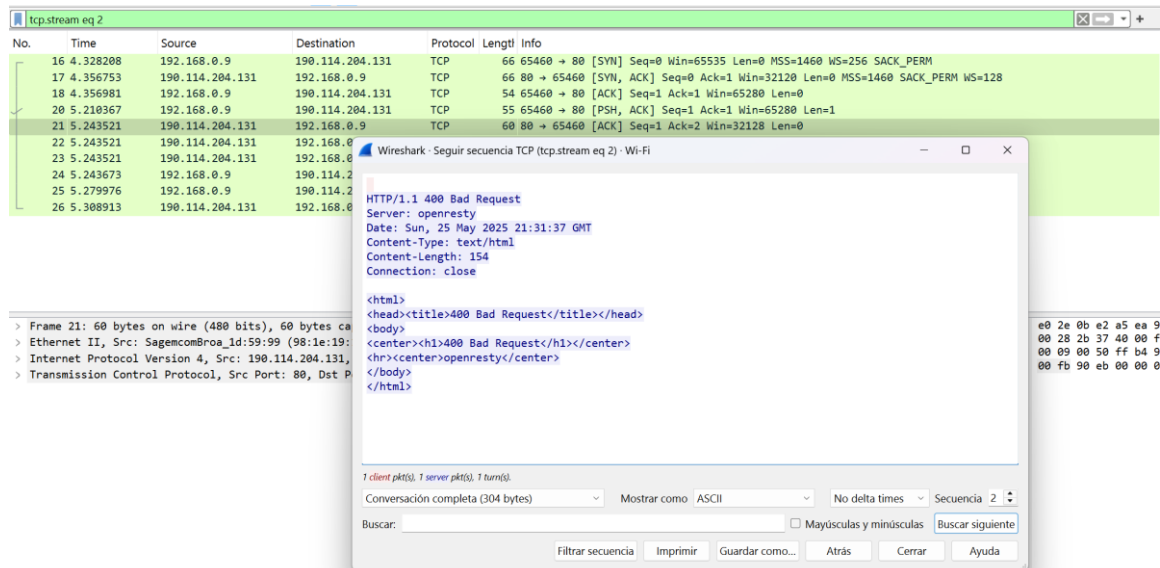
La pantalla obtenida no muestra los datos como los que se mostraron en la clase. Lo hice con varios elementos.

Debería aparecer información del servidor, usuario y contraseña, pero no se distingue en el texto obtenido.

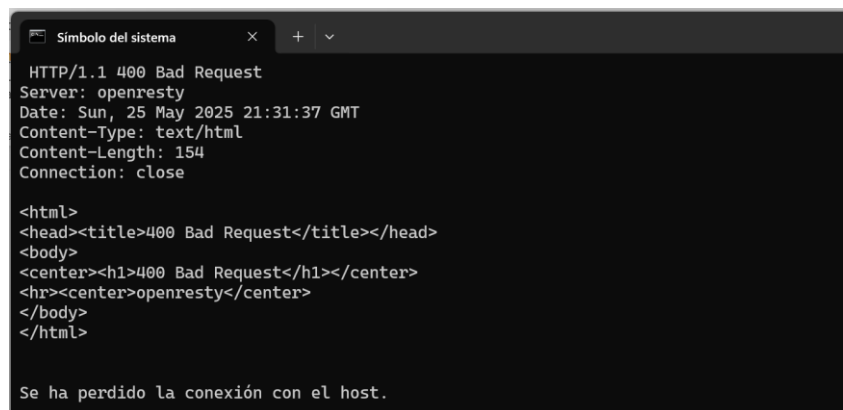
Si el transporte utilizado por el servicio es UDP, ¿cómo se puede verificar de forma remota si el puerto está abierto?

Para verificar, de forma remota, si un puerto está abierto cuando se utiliza es con protocolo UDP, se puede enviar un paquete UDP al puerto buscado y esperar una respuesta. Si se recibe respuesta, esto indica que el puerto está abierto.

Las capturas anteriores fueron realizadas ejecutando el programa Wireshark en modo administrador. Al salir del programa y no entrar en modo administrador pude realizar un seguimiento y me dio una captura distinta:



Lo que se observa en el cuadro es la misma información que se obtuvo al cortar la comunicación con el puerto 443 del sitio [www.frd.utn.edu.ar](http://www.frd.utn.edu.ar):



## Conclusiones

En este trabajo práctico de laboratorio se continuó con el uso del programa Wireshark y analizamos cómo hallar cómo encontrar algunos movimientos según el protocolo. Un ejemplo de esto fue detectar la conexión al puerto 443 a través de las líneas 37, 38 y 39 del análisis de Wireshark, en donde se observa que están:

- [SYN]
- [SYN, ACK]
- [ACK]

que indican la conexión con el puerto 443 de la dirección buscada.