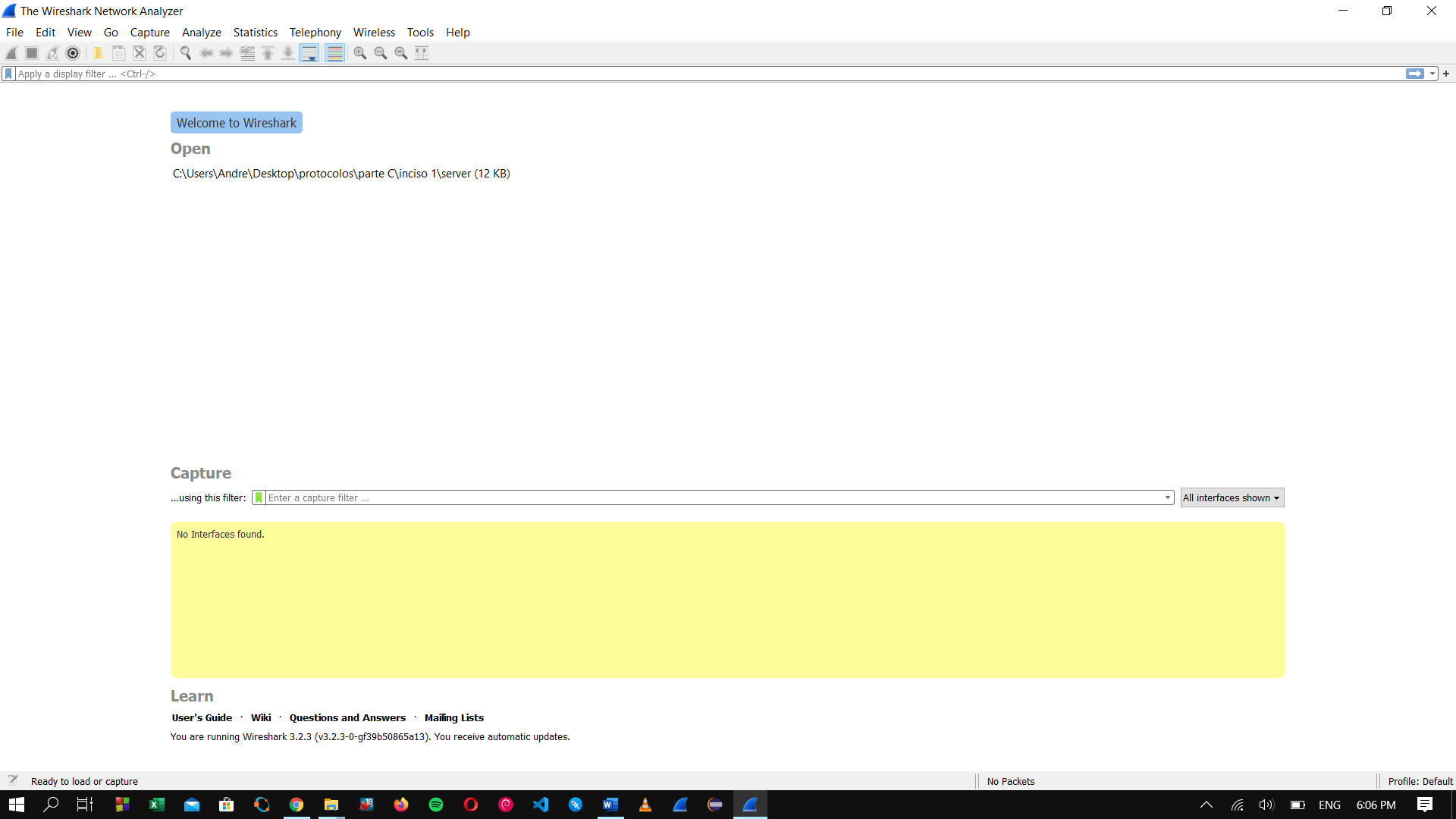
# ***Wireshark informe***

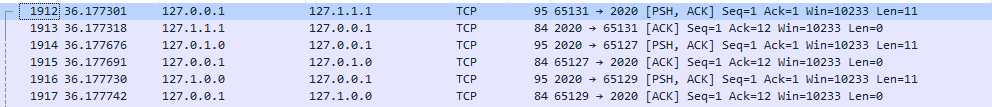
Para poder capturar los paquetes por Wireshark, lo que se hace primero fue ejecutar el ***programa\_servidor\_cliente\_udp.c*** en la carpeta el cual tiene asignado el ***puerto 2020***, luego de ello abrir 3 clientes telnet o mas podría haber sido, usando ***telnet localhost 2020***. La imagen de la carpeta es ilustrativa únicamente. Las conexiones fueron realizadas con las siguientes direcciones, aunque podríamos haber usado otras:

1. 127.0.1.0
2. 127.1.0.0
3. 127.1.1.1

Desde la **dirección 127.1.1.1** se decidió mandar unos 2 mensajes (distanciados temporalmente) y luego casi instantáneamente se pudo ver que ese mensaje enviado desde la **dirección 127.1.1.1** era visible en los otros dos clientes telnet, que mencionamos anteriormente(**127.0.1.0 y 127.1.0.0**). Para poder ver estos paquetes en WIRESHARK se utilizó el filter y se escribió lo siguiente ***tcp.port == 2020***, que se encuentra en la parte superior del programa:



El mensaje que primero se envió fue un “mensaje 1”, y los paquetes que se pudieron observar fueron los siguientes:

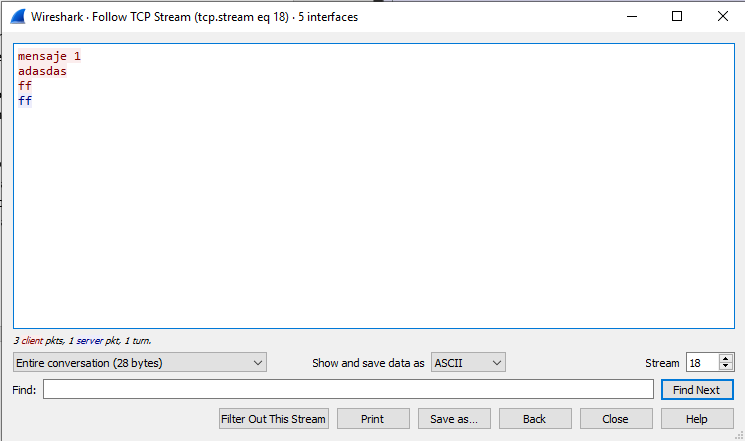


Ahora podremos realizar algún análisis de los paquetes:

1. El paquete salió con destino a localhost partiendo desde la maquina con dirección 127.1.1.1 hacia 127.0.0.1. Los flags que llevo fueron PSH (permite a la aplicación que envía comenzar a enviar la información, aunque el buffer no esté lleno) y el ACK. El segundo paquete contiene el flag de ACK y va en dirección inversa para asegurar la confirmación.
2. El paquete tercero de la mano con el cuatro. Este tercer paquete va desde otra de las terminales conectadas a telnet hacia la 127.0.0.1 y esta le devuelve un ACK de confirmación de recepción del paquete.
3. Los paquete quinto y paquete sexto consisten también en el par de flags PSH y ACK con su respectiva confirmación, pero acá entra en juego el ultimo cliente que es el 127.1.0.0.

En el programa de Wireshark, podemos ver cómo los paquetes llegan a cada una de las terminales y algunas de las partes del paquete que son visibles con Wireshark, lo que demuestra que lo que visualmente se ve es verdad, es decir, que el mensaje lo pueden ver todos los clientes.

En ***esta captura de paquetes*** podemos también empezar a comprender como funciona telnet. Este es un protocolo que va procesando un pedido a la vez y no es como un servidor concurrente que procesa varios clientes a la vez, estamos trabajando con un servidor de concurrencia aparente. La forma en la que telnet funciona puede ser relacionada con cómo un servidor iterativo funciona, procesando de a un cliente por vez. En los paquetes podemos también ver que pudimos encontrarlos en la categoría de TCP, lo que confirma que telnet es un protocolo TCP/IP. Haciendo pensar que atiende a todos los clientes al mismo tiempo pero realmente los atiende de a uno, lo que ocurre es que lo realiza en tiempos muy cortos que uno no se da cuenta ello. Cuando analizamos paquetes en Wireshark, telnet es sin duda un protocolo muy inseguro. Debido a que si vamos a la ***opción follow*** y luego ***“TCP Stream”,*** se ve lo que se envió. Si usaramos telnet se usa para almacenar password o datos importantes, resultaría bastante fácil para cualquier persona que intercepte el paquete y lo pueda analizar con una herramienta simple como el Wireshark podría en peligro nuestros datos importantes.



**En esta captura se pueden ver todos los chats que hubo entre los usuarios pero el mensaje 1 fue el primero que se mandó.**