**SEGURIDAD INFORMÁTICA**

**PRÁCTICA I (PARTE I)**

Los objetivos de esta práctica son los siguientes:

**I. DEMONIOS EN LINUX**

1. Estudiar los servicios (demonios) en Linux y el proceso de conexión cliente-servidor.
2. Instalar, arrancar y administrar dos tipos de demonios en Linux:
   1. Los demonios dependientes y gestionados por el súper demonio de red o súper servidor. Es este súper demonio el que escucha y arranca los demonios al llegar una petición al puerto correspondiente.
   2. Se elegirá para este caso el demonio telnetd, que deberá arrancarse mediante el súper demonio de red Inetd.
   3. Los demonios *standalone*, llamados así porque funcionan de forma independiente del súper demonio de red. En este caso tendremos el Open SSH y el Proftpd

**II. USO DEL WIRESHARK COMO SNIFFER**

1. Uso de un sniffer como el Wireshark para:
   1. Identificar los paquetes del Three-way handshake
   2. Identificar las características más importantes de los paquetes enviados: direcciones IP origen y destino, flags, número de secuencia y número ack (Leer artículo de la revista Hackxcrack “1-port\_scanning\_hxc.pdf”, pags. 59-61).
2. Capturar los paquetes con el nombre de usuario y contraseña en una sesión ftp y telnet (no cifrada) y en una sesión ssh y sftp (cifrada) para ver sus datos, en este caso los usuarios y contraseñas:
   1. En texto claro en telnet y en ftp
   2. Cifradas mediante claves pública y privada en SSH (ya explicaremos este método de cifrado en el curso más adelante)

**III. USO DE NMAP PARA ESCANEAR PUERTOS**

1. Aprender a usar nmap para escanear puertos
2. Entender los diferentes tipos de escaneo que hay y el uso de los distintos flags en los paquetes TCP/IP

**ACTIVIDADES**

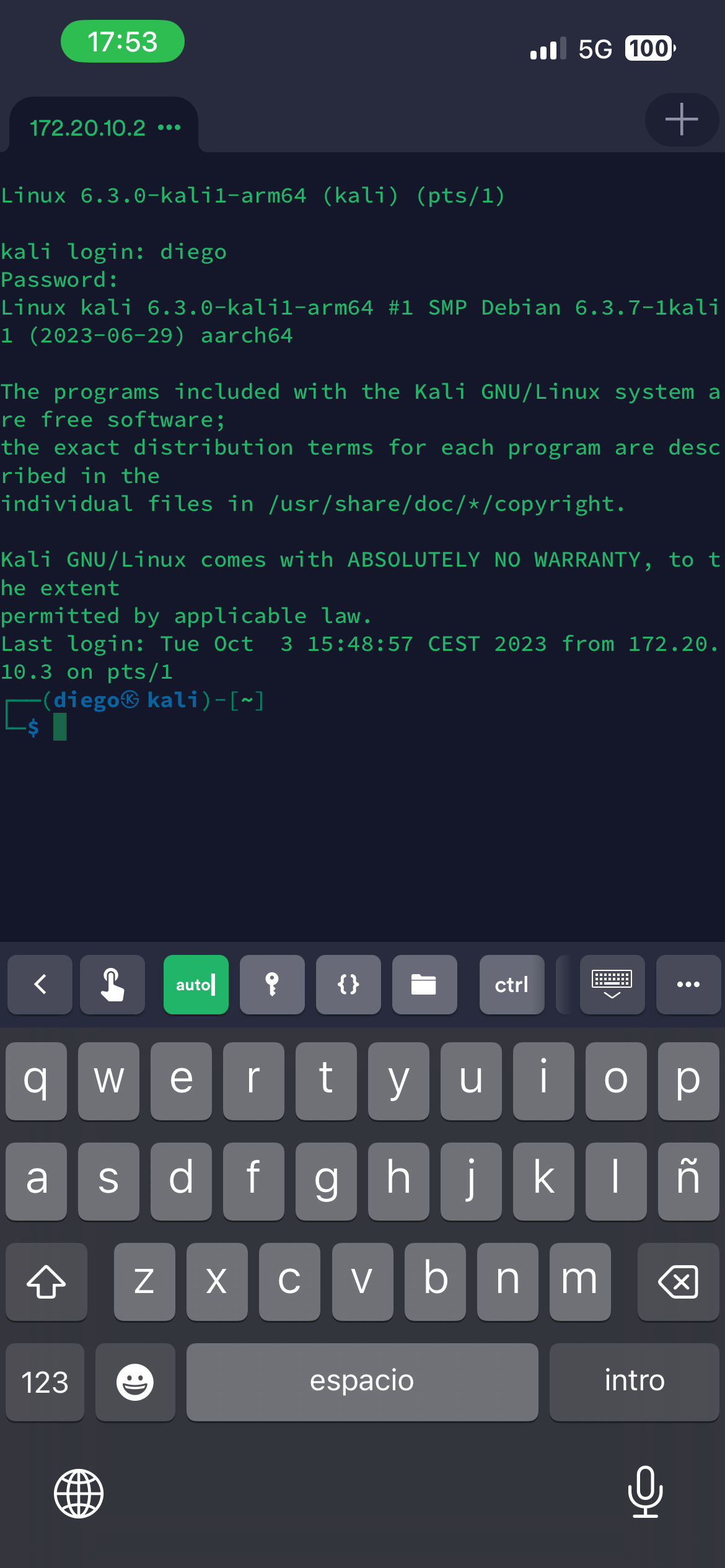
**PARTE 1: Instalar servidor Telnet**

1. **Instalar un servidor telnet en Linux.**
   1. ¿Cómo funciona y cómo se instala?
      1. Lo lanza el súper demonio de red llamado **inetd.**
      2. Este súper demonio se instala con la orden **sudo apt install openbsd-inetd**
      3. Después se instala el demonio servidor telnet con la orden **sudo apt install telnetd**
   2. Arrancar el servidor telnet (que en realidad es arrancar el súper demonio de red) con la orden **sudo /etc/init.d/openbsd-inetd start**
   3. ¿Cómo puedo saber si está arrancado o no?
      1. Mediante la orden systemctl **sudo systemctl status openbsd-inetd.service**
      2. Mirando los procesos que están ejecutándose en el sistema mediante la orden **ps aux | grep inetd**
      3. Mediante nmap

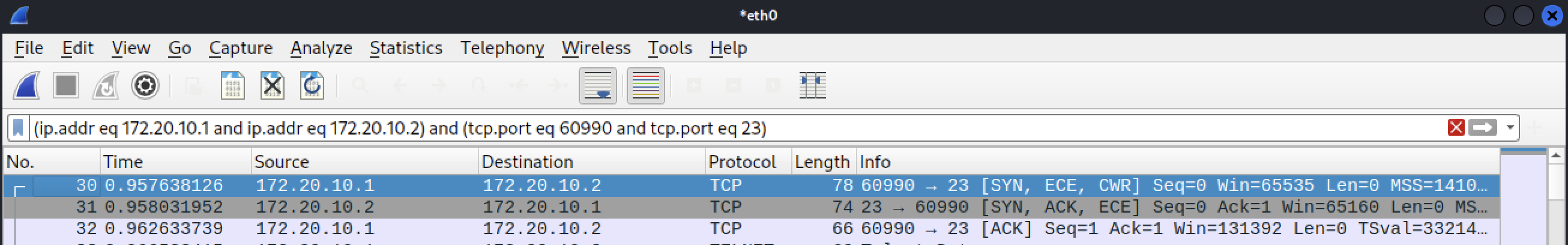


* + 1. Mediante cualquier otro método alternativo **telnet (ip del Kali) desde el cliente (Windows o mac)**
  1. ¿Qué puerto utiliza este servidor? **23**

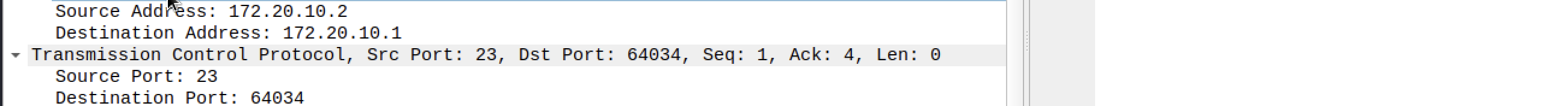
1. **Instalar un cliente telnet en móvil, por ejemplo Termius, en iOS o en Android (también podríamos conectarnos mediante el CMD en Windows, aunque en este caso hay que habilitarlo previamente porque está deshabilitado por defecto).** 
   1. Conectarse desde el móvil al servidor telnet



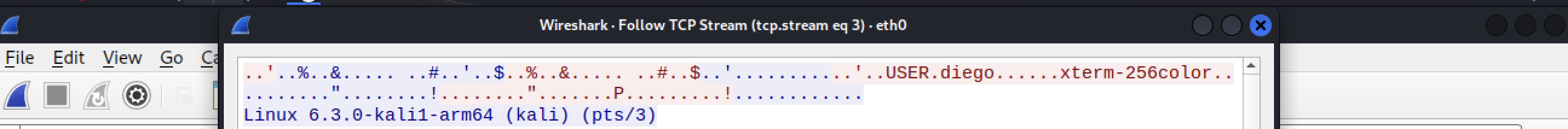
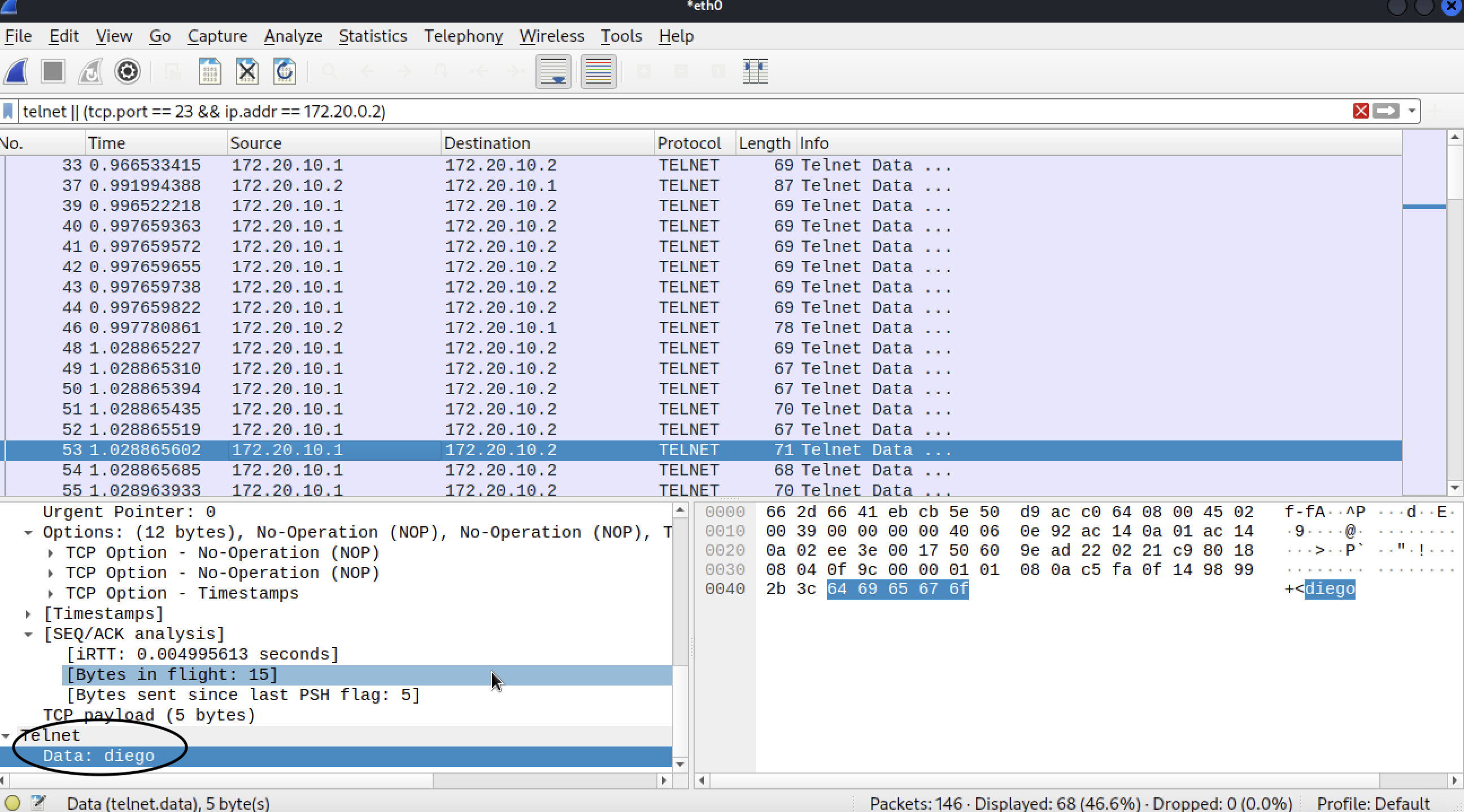
1. **Monitorización con un sniffer**
   1. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:
      1. Three-way handshake – Tres paquetes con los que se establece la conexión cliente-servidor



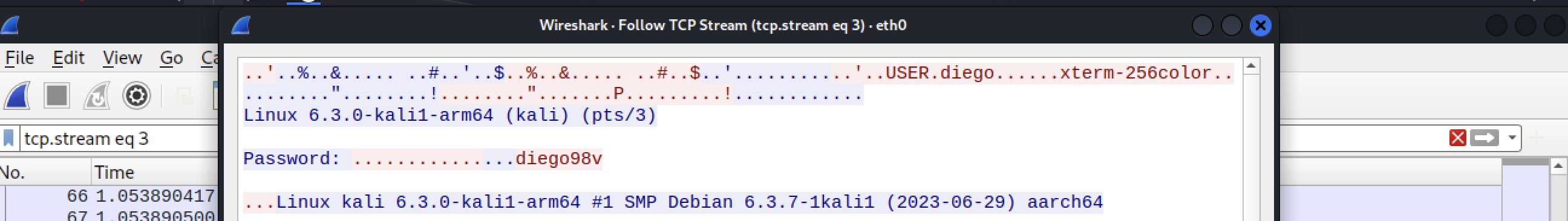
* + 1. Donde aparezcan los puertos del cliente y el servidor, junto con sus direcciones IP.



* + 1. USUARIO Y CONTRASEÑA
       1. **Usuario:**

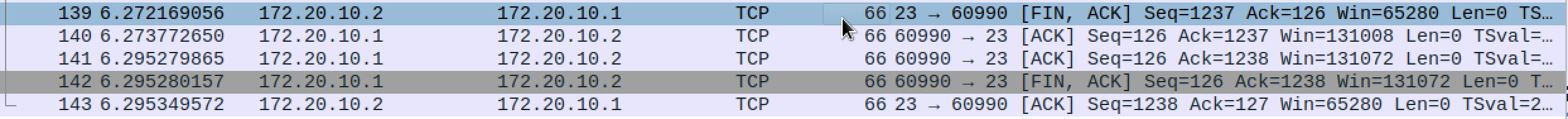


* + - 1. **Contraseña**



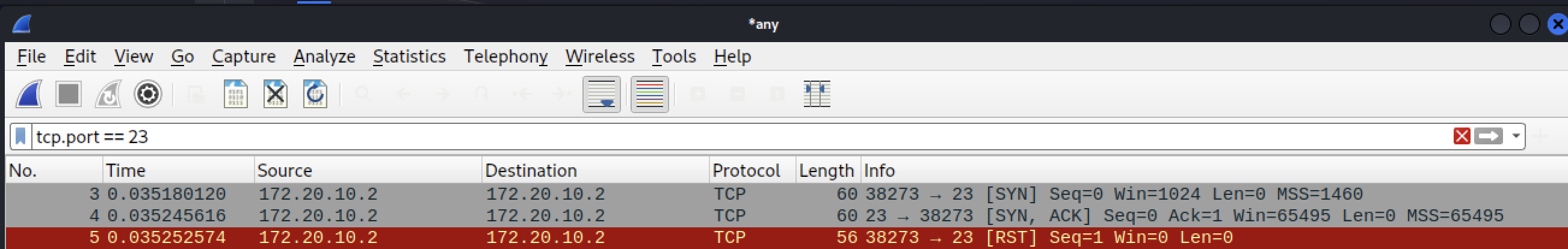
**La contraseña aparece como una letra por cada paquete, lo que hemos hecho es ir al primer paquete y darle a la opción Follow TCP Stream para poder mostrar la contraseña por completo**

* + 1. Capturar los paquetes con los que se cierra la conexión

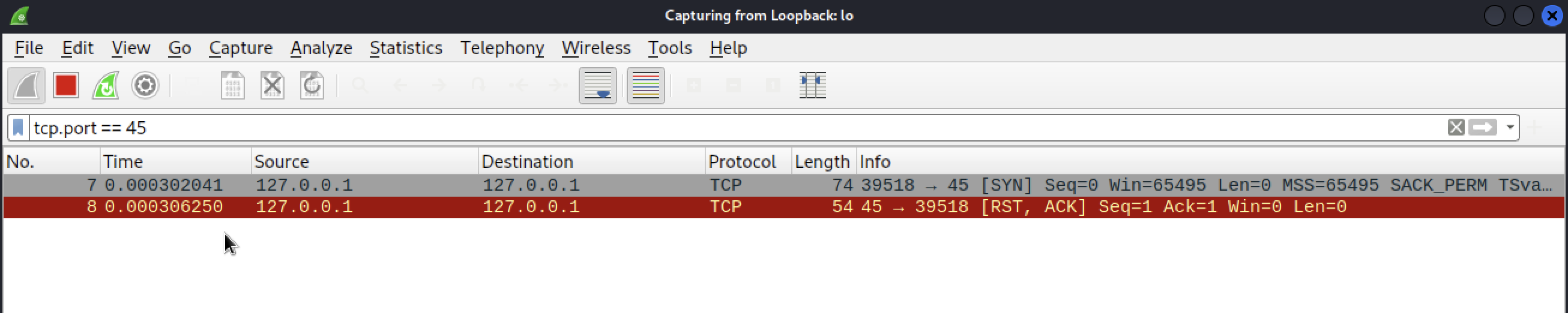


**NOTA: No serán válidas capturas que no estén bien filtradas de forma que se puedan encontrar de forma más o menos sencilla esos paquetes. Destacar esos paquetes con un trazo rojo ayuda, pero eso no es un filtro de Wireshark.**

1. **Escaneo de los puertos mediante nmap** 
   1. Hacer un escaneo **HALF SCAN** al servidor telnet mediante nmap
   2. Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:
      1. Un escaneo filtrado con éxito (a un puerto abierto)



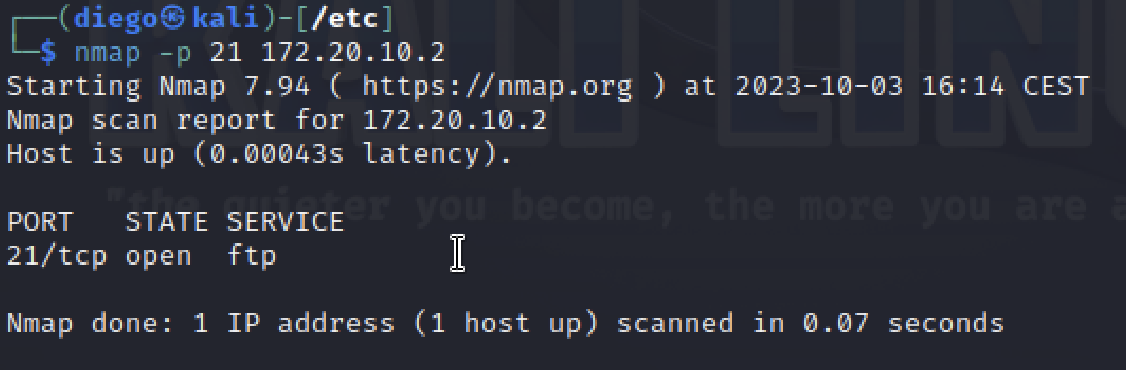
* + 1. Un escaneo filtrado a un puerto cerrado



**NOTA: El resultado de estos pantallazos deben reflejar las diapositivas que hay en la teoría donde se explica este tipo de escaneo.**

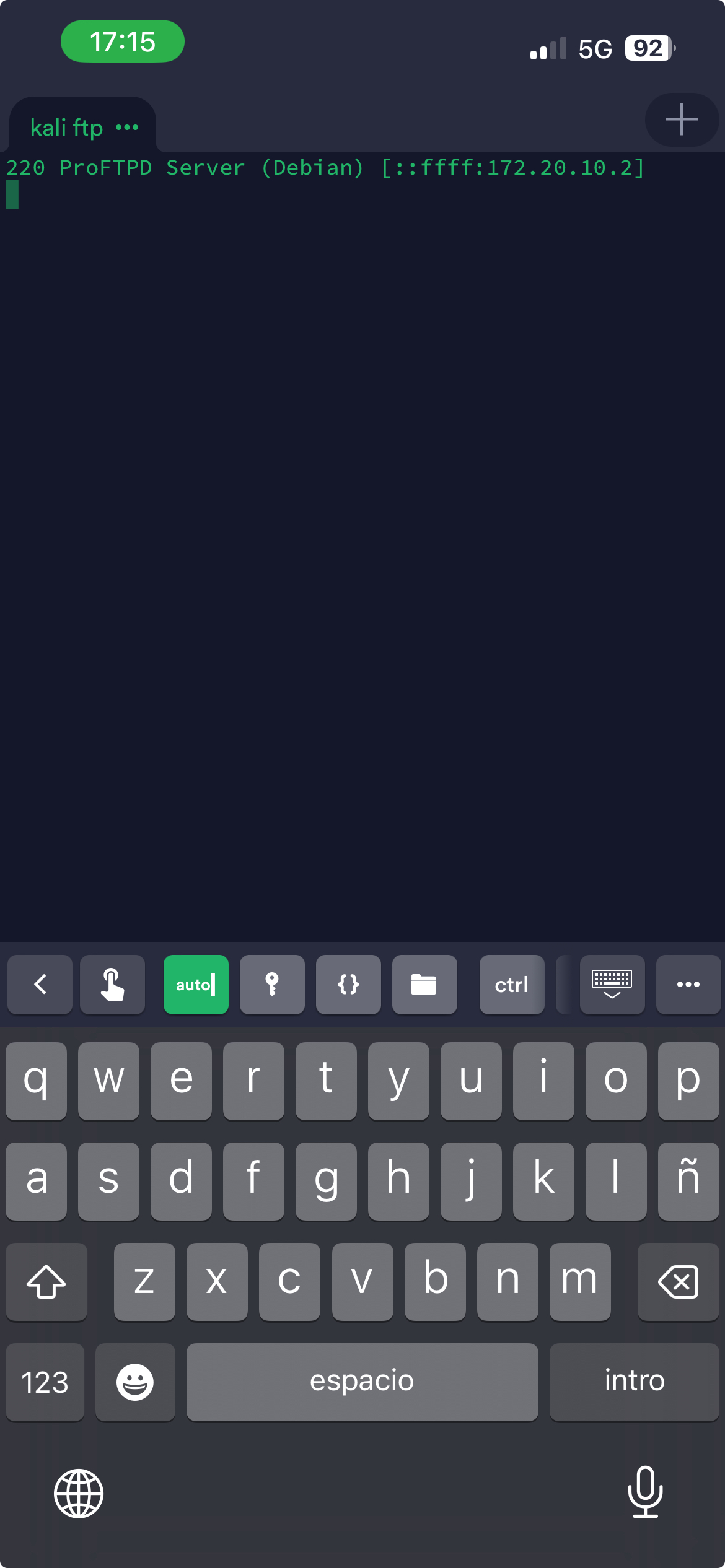
**PARTE 2: PROFTPD**

1. **Repetir los pasos 1 al 4 para el servidor Proftpd y conectarse al servidor desde el móvil (mediante la app FTP Manager o cualquier cliente gratuito). También nos podríamos conectar desde el CMD de Windows.**
2. **Instalar un servidor ftp en Linux.**
   1. ¿Cómo funciona y cómo se instala?
      1. Lo lanza el súper demonio de red llamado **inetd.**
      2. Este súper demonio se instala con la orden **sudo apt install openbsd-inetd**
      3. Después se instala el demonio servidor FTP con la orden **sudo apt install proftpd-core**
   2. Arrancar el servidor FTP (que en realidad es arrancar el súper demonio de red) con la orden **sudo /etc/init.d/proftpd restart**
   3. ¿Cómo puedo saber si está arrancado o no?
      1. Mediante la orden systemctl **sudo systemctl status proftpd**
      2. Mirando los procesos que están ejecutándose en el sistema mediante la orden **ps aux | grep ftp**
      3. Mediante nmap

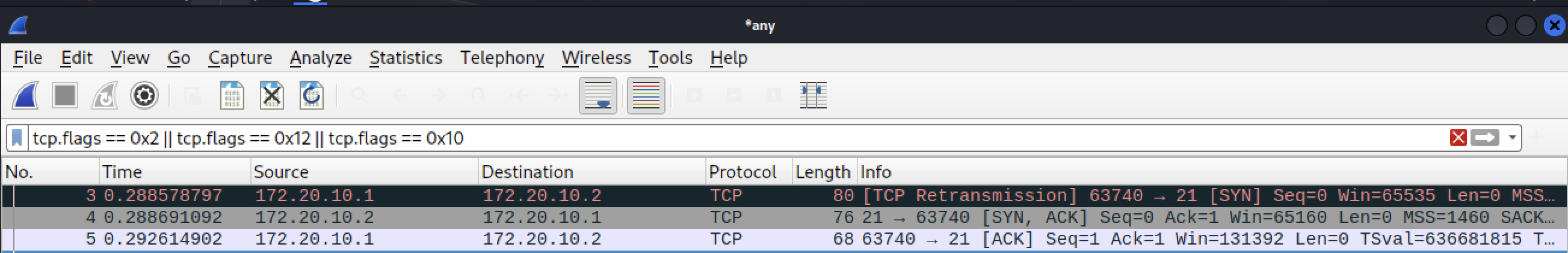


* + 1. Mediante cualquier otro método alternativo **desde el terminal mac: ftp (ip del Kali linx)**
  1. ¿Qué puerto utiliza este servidor? **21**

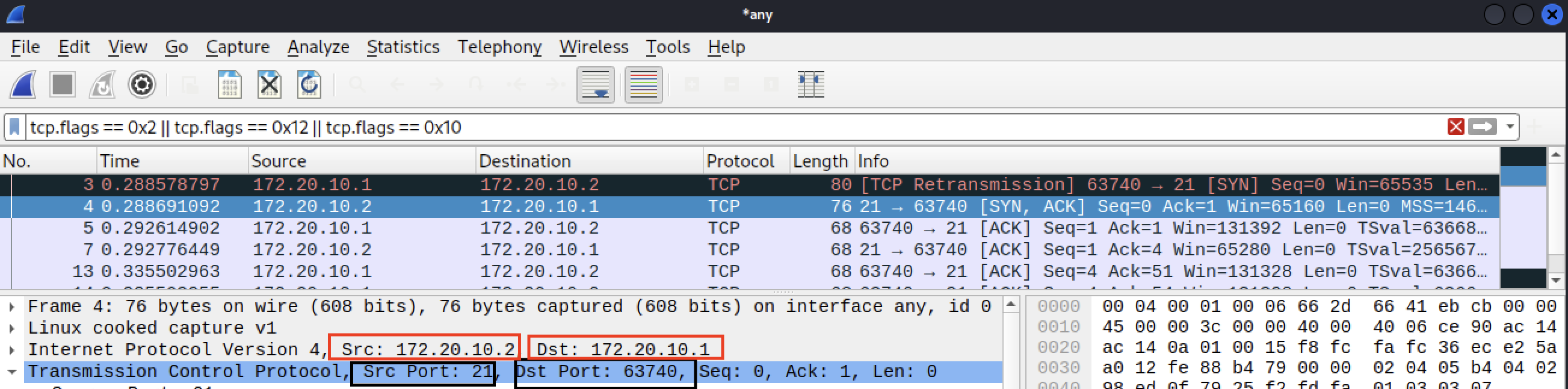
1. **Instalar un cliente ftp en móvil, por ejemplo Termius, en iOS o en Android (también podríamos conectarnos mediante el CMD en Windows, aunque en este caso hay que habilitarlo previamente porque está deshabilitado por defecto).** 
   1. Conectarse desde el móvil al servidor FTP



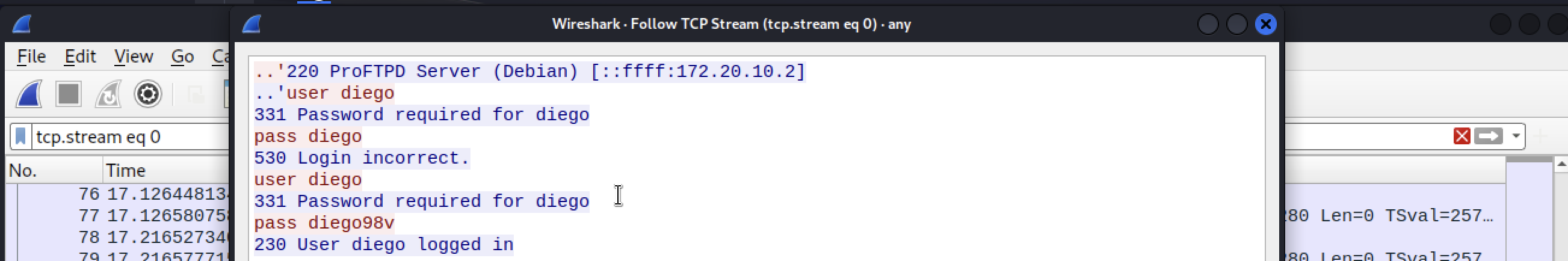
1. **Monitorización con un sniffer**
   1. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:
      1. Three-way handshake – Tres paquetes con los que se establece la conexión cliente-servidor



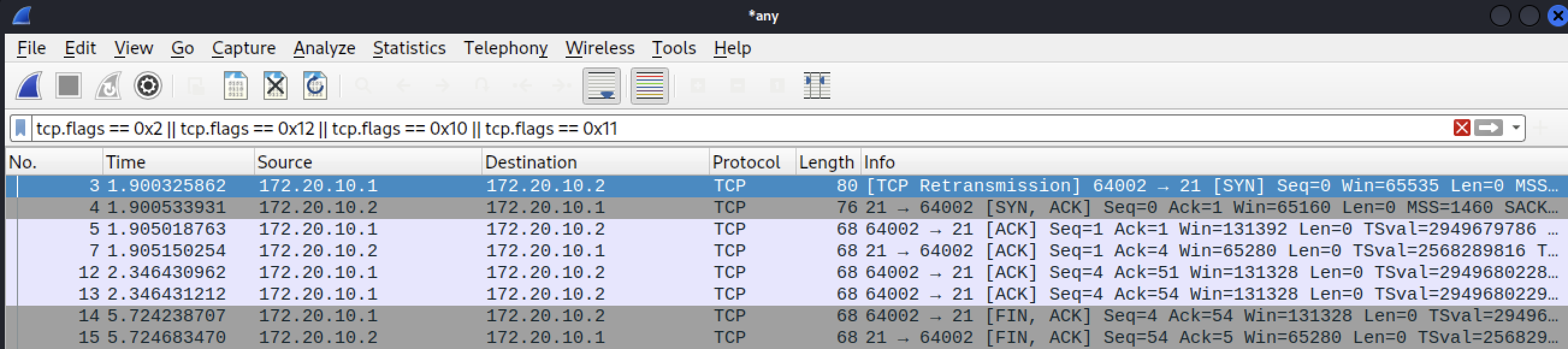
* + 1. donde aparezcan los puertos del cliente y el servidor, junto con sus direcciones IP.



* + 1. USUARIO Y CONTRASEÑA

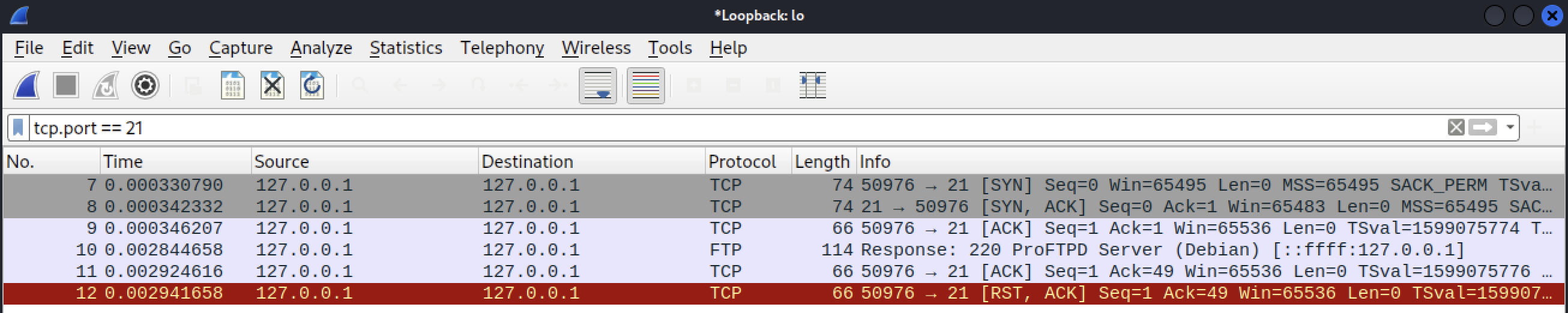


* + 1. Capturar los paquetes con los que se cierra la conexión

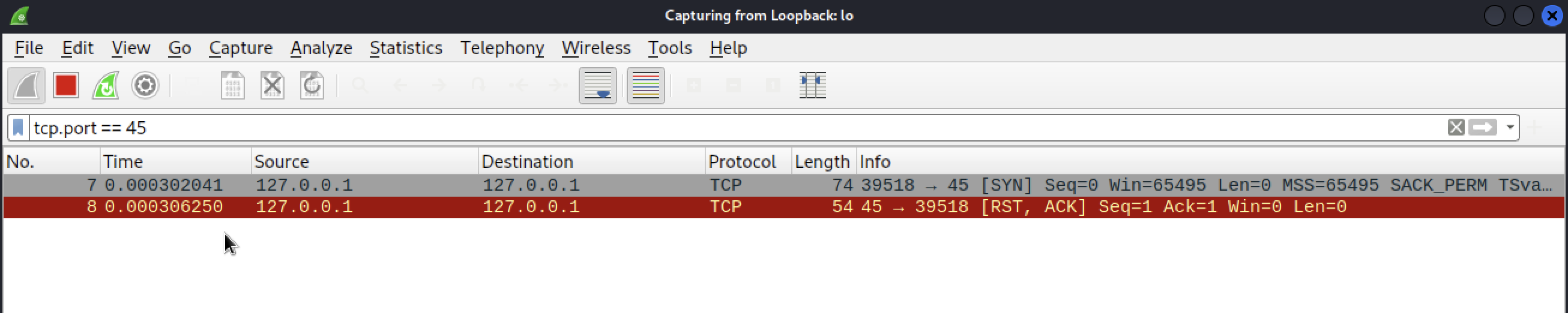


**NOTA: No serán válidas capturas que no estén bien filtradas de forma que se puedan encontrar de forma más o menos sencilla esos paquetes. Destacar esos paquetes con un trazo rojo ayuda, pero eso no es un filtro de Wireshark.**

1. **Escaneo de los puertos mediante nmap**
   1. Hacer un escaneo **FULL SCAN** al servidor ftp mediante nmap
   2. Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:
      1. Un escaneo filtrado con éxito (a un puerto abierto)



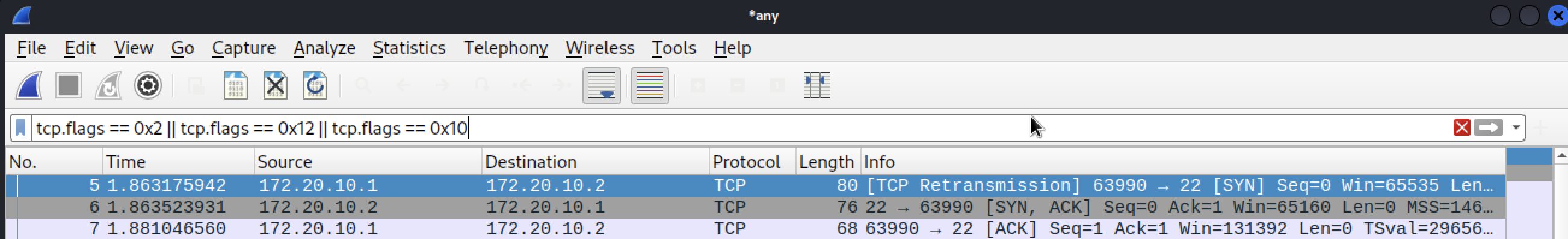
* + 1. Un escaneo filtrado a un puerto cerrado



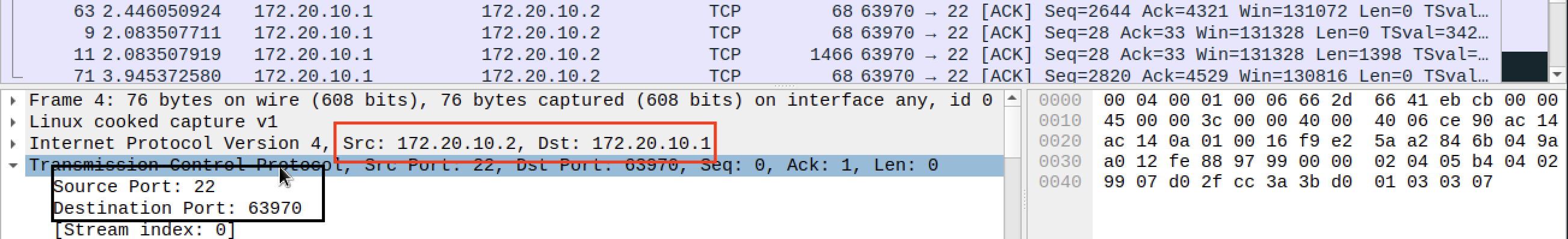
**NOTA: La única diferencia es que hay que hacer un escaneo HALF SCAN para el servidor TELNET y ver los paquetes (en especial los flags que están activados) que se mandan en este caso.**

**PARTE 3: SSH**

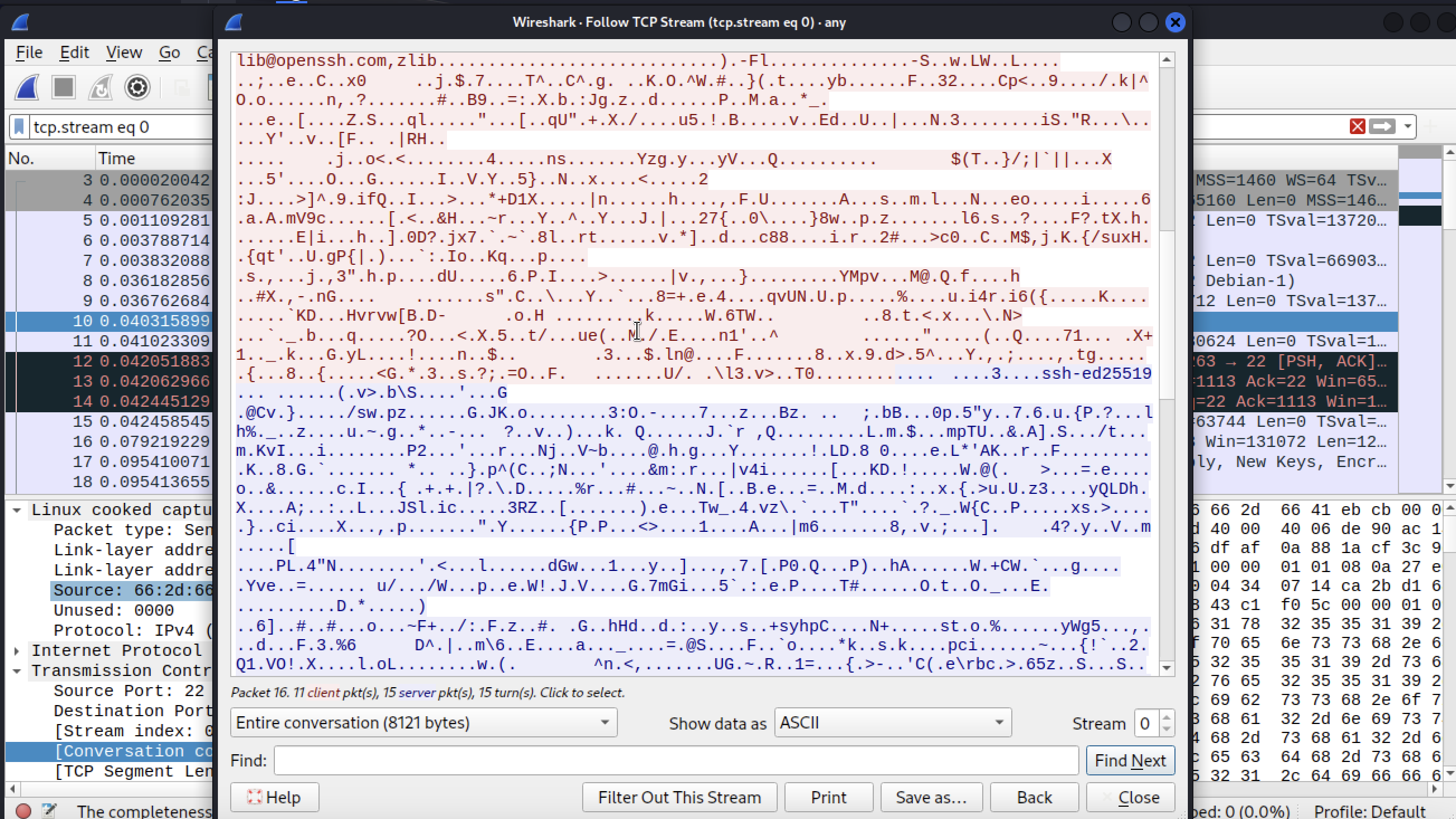
1. **Realizar el paso 3 (captura del Three-way handsake, fin de conexión y usuario y contraseña) para el servidor Open SSH, con sus correspondientes pantallazos.**
2. **Monitorización con un sniffer (SSH)**
   1. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:
      1. Three-way handshake – Tres paquetes con los que se establece la conexión cliente-servidor



* + 1. donde aparezcan los puertos del cliente y el servidor, junto con sus direcciones IP.

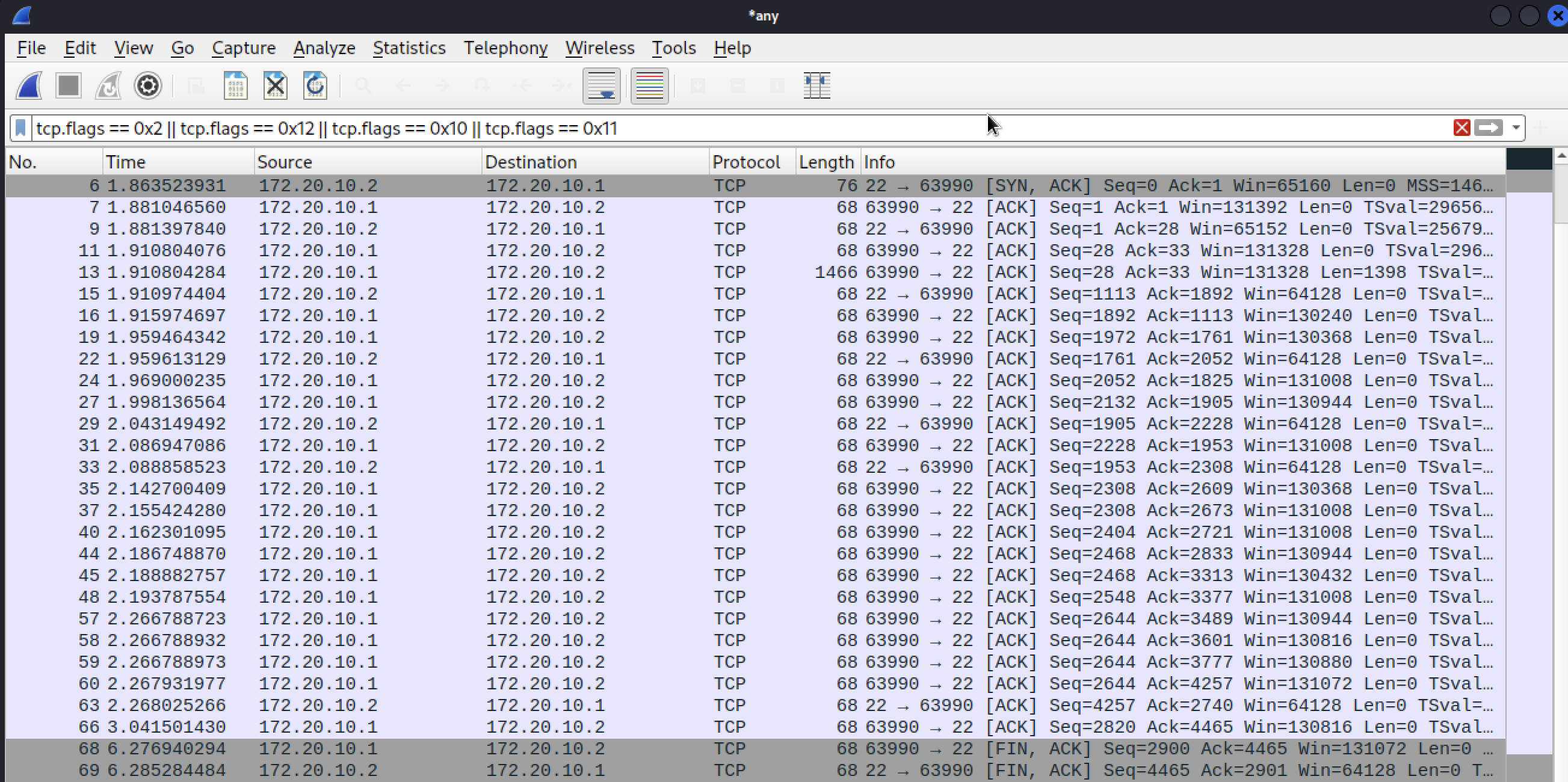


* + 1. USUARIO Y CONTRASEÑA



Podemos observar que el paquete está completamente cifrado, lo que significa que ni la contraseña ni el nombre de usuario son visibles.

* + 1. Capturar los paquetes con los que se cierra la conexión



1. Contesta a las siguientes preguntas:
   1. Explica en pocas líneas qué es el servicio SSH y para qué sirve

**SSH es como un candado digital para tu conexión a internet. Se usa para mantener seguras las comunicaciones entre dispositivos, como tu computadora y un servidor remoto. Esto es útil para administrar sistemas a distancia y transferir archivos de forma segura. SSH protege tus datos cifrándolos y garantiza que solo las personas autorizadas puedan acceder a ellos.**

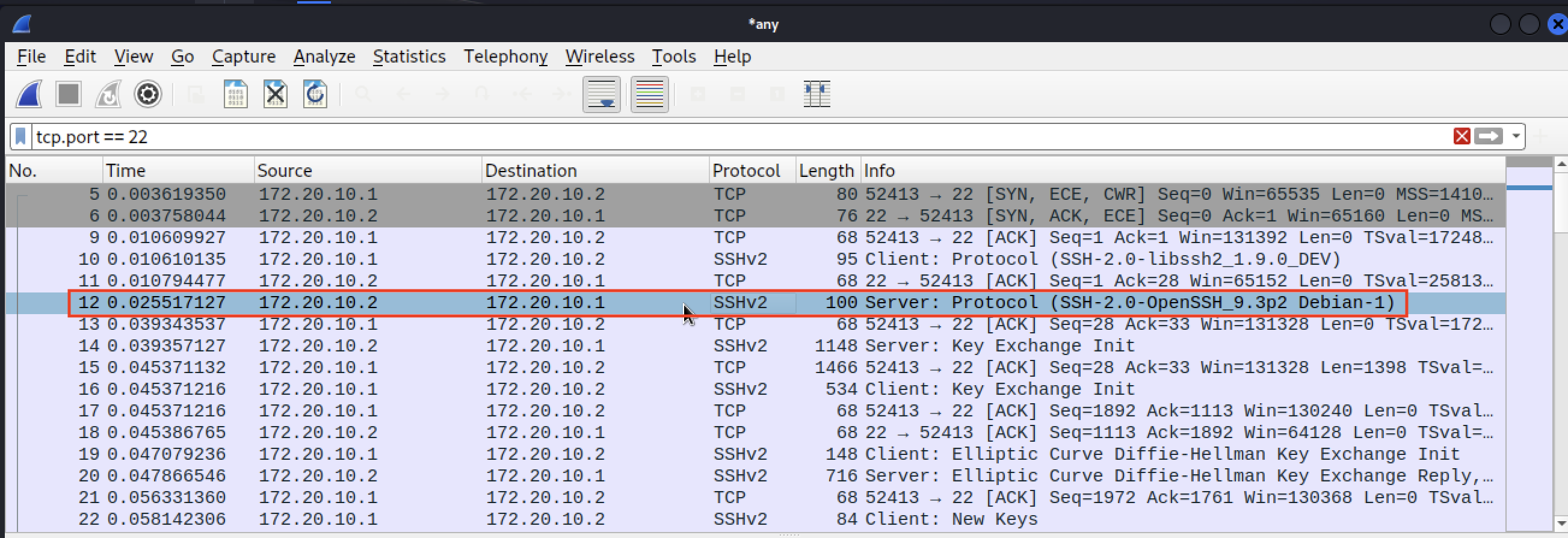
* 1. ¿Qué puerto utiliza el servidor? ¿Qué puerto has utilizado tú como cliente?

**Usa el puerto 22. Nosotros hemos usado como cliente el puerto 63990**

* 1. ¿Cómo es su autenticación y cómo viajan los datos que se intercambian entre el cliente y el servidor? Explica en unas pocas líneas y con tus palabras qué método utilizamos para autenticarnos y qué algoritmo de cifrado de utiliza para ello.

**SSH usa un sistema de llaves: una privada en tu dispositivo y una pública en el servidor. Cuando te conectas, el servidor pide una firma digital con tu llave privada para asegurarse de que eres quien dices ser. Luego, se cifran los datos con algoritmos como AES, y las claves se intercambian con algoritmos como RSA o DSA para mantener todo seguro.**

* 1. ¿Has podido ver la contraseña en Wireshark? ¿Qué paquetes son los que definen la autenticación? Señálalos en tu captura.



**No se puede ver la contraseña en Wireshark por lo que hemos explicado en los apartados anteriores, está cifrada de forma segura. Los paquetes que definen la autenticación son los paquetes con protocolo SSHv2.**

* 1. ¿Hay un servicio análogo para el servicio ftp basado en SSH?

**Sí, está el SFTP, que es como un hermano seguro del FTP. En lugar de enviar datos en texto plano, utiliza SSH para cifrar todo: tus credenciales y los archivos que transfieres. Es la forma más segura de mover archivos por la red y se usa mucho para proteger la transferencia de datos.**

**IMPORTANTE: Si se detecta que este último punto está copiado la práctica será calificada con un 0. Tenéis que leerlo, entenderlo y explicarlo con vuestras palabras.**

**INSTRUCCIONES**

* Entrega:
  + **Un archivo PDF** a partir de este documento de Word modificado con las respuestas escritas (las que están señaladas en rojo) y los pantallazos pedidos.
* Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo. **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**
* El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
* Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.
* **La fecha límite de entrega será el miércoles 11 de octubre a las 23 horas.**
* No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.