

1. Instalar wireshark:

```
sudo apt install wireshark
```

2. Instalar telnet:

```
sudo apt-get install openbsd-inetd
```

```
sudo apt-get install telnetd
```

3. Abrir el fichero de configuracion de telnet.

```
sudo vim /etc/inetd.conf
```

4. Verificar que la linea resaltada no este comentada.

```
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet superserver configuration database
#
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard          stream  tcp    nowait  root    internal
#discard          dgram   udp     wait    root    internal
#daytime          stream  tcp     nowait  root    internal
#time             stream  tcp     nowait  root    internal

#:STANDARD: These are standard services.
telnet            stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd

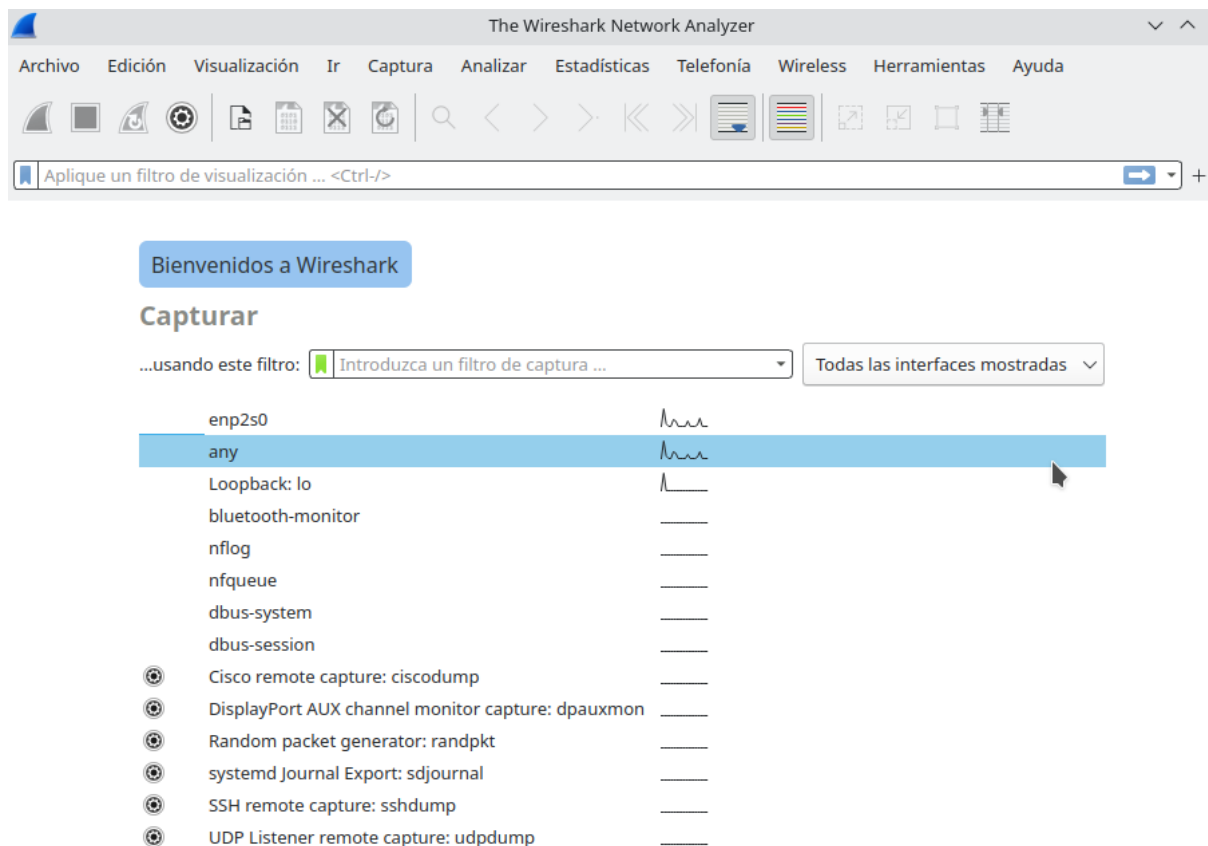
#:BSD: Shell, login, exec and talk are BSD protocols.
#
#:MAIL: Mail, news and uucp services.
#
#:INFO: Info services
#
#:BOOT: TFTP service is provided primarily for booting.  Most sites
#       run this only on machines acting as "boot servers."
#
#:RPC: RPC based services
#
#:HAM-RADIO: amateur-radio services
#
#:OTHER: Other services
```

5. Abrir wireshark en modo administrador.

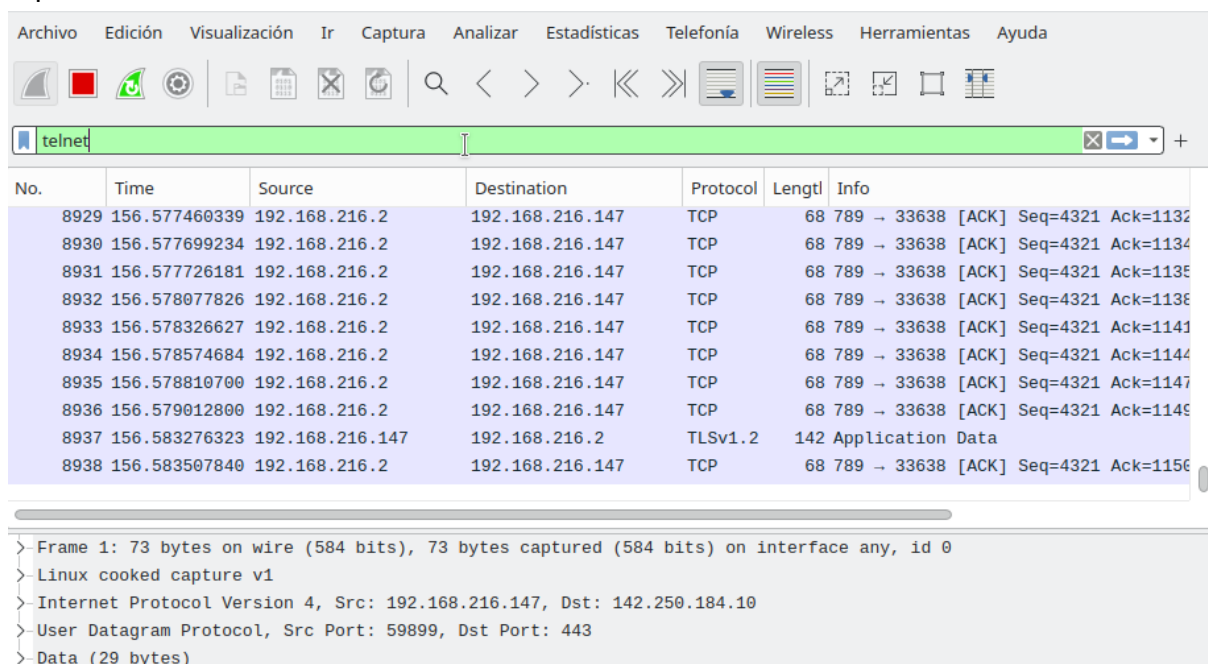
```
sudo wireshark
```

6. Ver el trafico de datos de la red.

Dar doble click izquierdo en el apartado de “any”.



7. Filtrar “telnet” para cuando nos conectemos al otro ordenador poder capturar el paquete específico.



8. Conectarnos a la ip deseada.

```
telnet [ip a la que deseamos conectarnos]
```

9. Loguearse a un usuario de la maquina a la que te conectaste.

```
Trying 192.168.216.122...
Connected to 192.168.216.122.
Escape character is '^]'.
Ubuntu 22.04.3 LTS
E216-10 login: alum
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

25 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Mon Sep 18 13:46:27 WEST 2023 from 192.168.216.207 on pts/7
```

10. Nada mas conectarte entrar en wireshark y parar de capturar paquetes.

-Se pausa pulsando el cuadrado rojo.

Wireshark interface showing a packet capture of a telnet session. The packet list shows several TCP and TELNET packets between 192.168.216.147 and 192.168.216.122. The packet details pane shows the structure of a frame: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data.

No.	Time	Source	Destination	Protocol	Length	Info
23960	445.060006770	192.168.216.147	192.168.216.122	TCP	68	40178 → 23 [ACK] Seq=135 Ack=7
23961	445.275100467	192.168.216.122	192.168.216.147	TELNET	76	Telnet Data ...
23962	445.275144828	192.168.216.147	192.168.216.122	TCP	68	40178 → 23 [ACK] Seq=135 Ack=7
23963	445.275281912	192.168.216.122	192.168.216.147	TELNET	130	Telnet Data ...
23964	445.275293256	192.168.216.147	192.168.216.122	TCP	68	40178 → 23 [ACK] Seq=135 Ack=7
23965	445.633917886	ASUSTekC_7e:f0:af	192.168.216.122	ARP	62	Who has 192.168.216.132? Tell
23966	446.075852721	192.168.216.147	142.250.185.1	TCP	68	[TCP Keep-Alive] 53714 → 443 [
23967	446.075864450	192.168.216.147	142.250.185.1	TCP	68	[TCP Keep-Alive] 53692 → 443 [
23968	446.101945228	142.250.185.1	192.168.216.147	TCP	68	[TCP Keep-Alive ACK] 443 → 537
23969	446.103002932	142.250.185.1	192.168.216.147	TCP	68	[TCP Keep-Alive ACK] 443 → 536

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.216.147, Dst: 142.250.184.10
User Datagram Protocol, Src Port: 59899, Dst Port: 443
Data (29 bytes)

11. Click derecho encima de cualquier paquete con el protocolo telnet.

Seguir>Flujo TCP

Te saltara un fichero con toda la infomacion del paquete en la que encontraras el usuario y la contraseña.

```
untu 22.04.3 LTS  
E216-09 login: aalluumm  
.  
Password: csas1234
```