Inicialmente instalamos wireshark. La versión Wireshark-gtk será la que utilizaremos para la captura de paquetes en Windows. En Windows las versiones 3.x por algún motivo no termina de ejecutarse bien

wlanpi@wlanpi:~$ sudo apt-update

wlanpi@wlanpi:~$ sudo apt install wireshark

wlanpi@wlanpi:~$ sudo apt install wireshark-gtk

Permitimos que los usuarios no administradores puedan hacer captura de paquetes.



Si esta pantalla no aparece al terminar la instalación la podemos ejecutar con:

wlanpi@wlanpi:~$ sudo dpkg-reconfigure wireshark-common

Ejecutamos los siguientes comandos para proporcionar permisos adicionales al usuario actual. Se no se ejecuta algunas interfaces no aparecen para poder tomar capturas.

wlanpi@wlanpi:~$ sudo groupadd wireshark

wlanpi@wlanpi:~$ sudo gpasswd -a $USER wireshark

sudo chgrp wireshark /usr/bin/dumpcap

Instalamos los paquetes para poder ejecutar programas basados en ventanas.

wlanpi@wlanpi:~$ sudo apt install xorg

wlanpi@wlanpi:~$ sudo apt install x11-apps

Desde Linux podemos ya hacer capturas para ello abrimos una terminal y ejecutamos:

┌──(josepi㉿kali)-[~]

└─$ ssh -l Usuario -X ip\_de\_la\_wlanpi

Para sistemas Windows hemos de hacer un paso adicional y hemos de instalar el programa xming. Lo podemos descargar desde la siguiente dirección:

<https://sourceforge.net/projects/xming/>

Una vez instalado ejecutamos el programa XLaunch y lo dejamos de la siguiente manera

 







Realizado este paso ejecutamos Xming



La aplicación se queda corriendo en segundo plano



Una vez hecho esto podemos hacer la conexión ssh con la wlanpi utilizando por ejemplo putty



Hemos de habilitar la opción X11.



Para poner la interfaz en modo monitor ejecutamos:

wlanpi@wlanpi:~$ sudo ip link set wlan0 down

wlanpi@wlanpi:~$ sudo iwconfig wlan0 mode monitor/managed

wlanpi@wlanpi:~$ sudo ip link set wlan0 up