

WIRESHARK

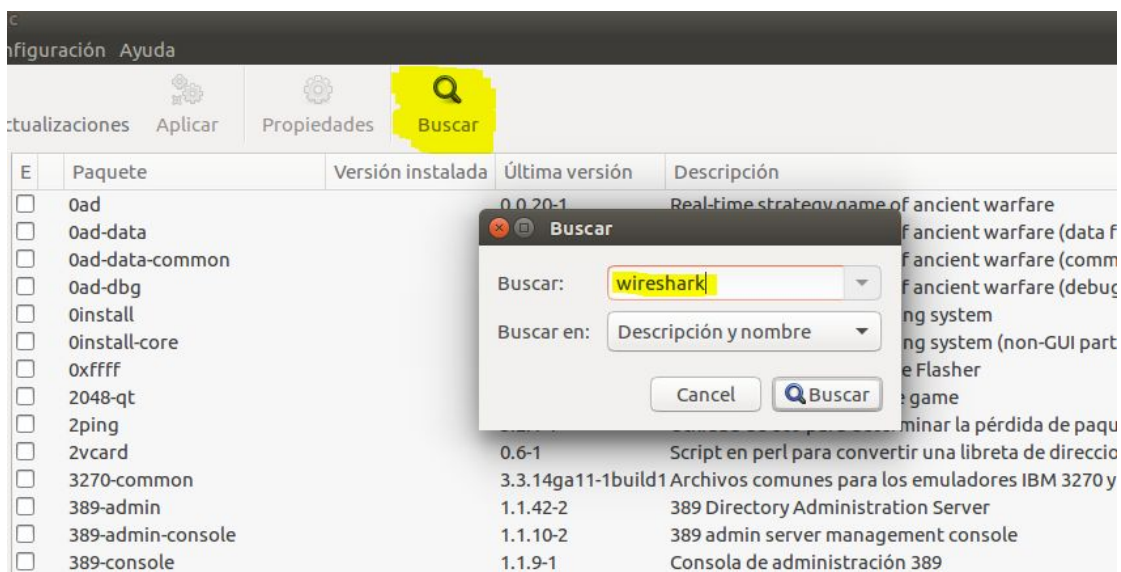
¿Como descargarlo?

Para descargarlo primero deberemos de instalar synaptic

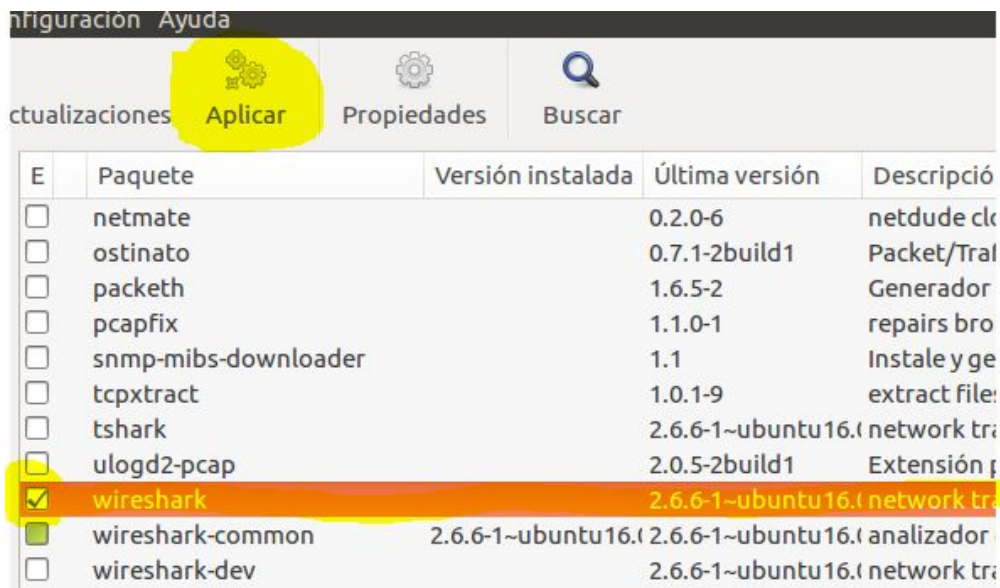
```
$ apt-get install synaptic
```

```
$ synaptic
```

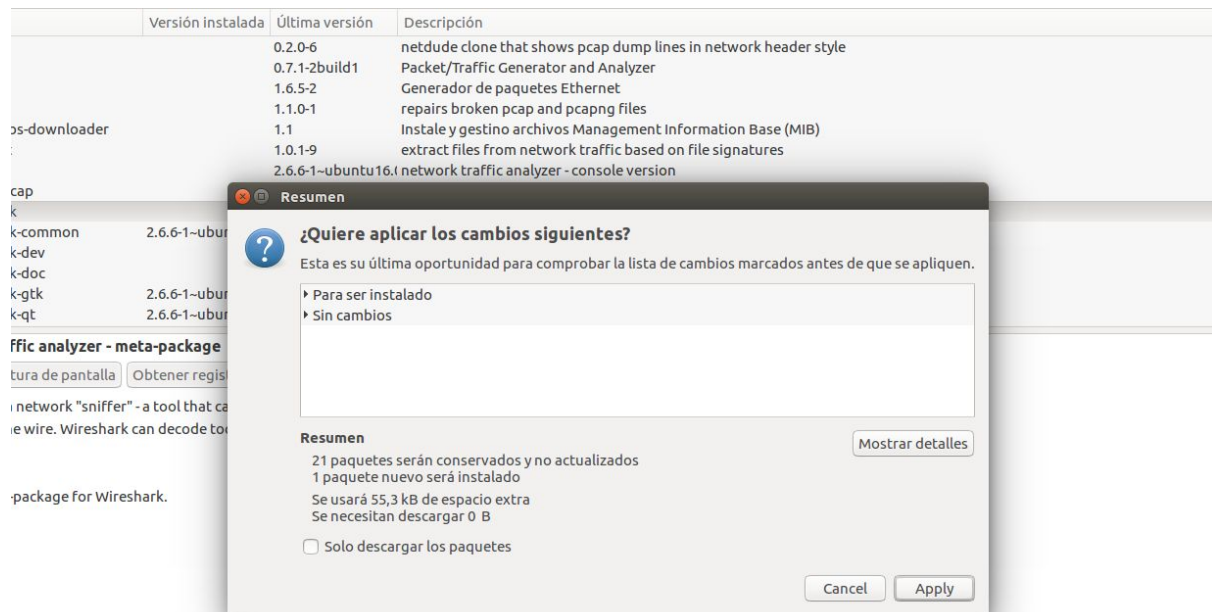
Una vez dentro pinchamos en la lupa y escribimos "Wireshark".



Le damos en la ventana pequeña a buscar y tendremos que buscar el paquete de wireshark:



El checkbox estará desmarcado. Lo marcamos y le damos al engranaje de “Aplicar”.

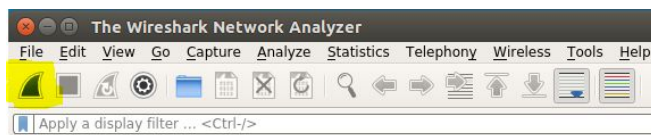


Nos sale esta ventana y le damos en aplicar.

Una vez instalado, como necesita permisos de root, para arrancarlo lo deberemos hacer desde la terminal:

```
$ sudo wireshark
```

Ya arrancado, haciendo doble click en la interfaz de red que queramos y la aleta pasará a color rojo. Esto quiere decir que ya está “escuchando”.



Welcome to Wireshark

Capture

...using this filter:

enp0s3	
any	
Loopback: lo	
docker0	
nflog	
nfqueue	
usbmon1	
usbmon2	
<input checked="" type="radio"/> Cisco remote capture: ciscodump	
<input checked="" type="radio"/> Random packet generator: randpkt	
<input checked="" type="radio"/> SSH remote capture: sshdump	
<input checked="" type="radio"/> UDP Listener remote capture: udpdump	