UT01: Adopción de pautas de seguridad informática – 7) – Monitorización de Tráfico en Redes.

Nombre: Francisco Jesús García – Uceda Díaz - Albo

Curso: 2º ASIR.

Índice

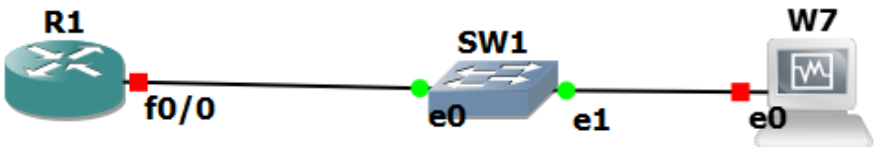
Introducción

En esta práctica aprenderemos a realizar una monitorización del tráfico en redes usando distintos protocolos. Veremos y aprenderemos sobre SYSLOG, SNMP Y NETFLOW. Usaremos otros programas para monitorizar la red distinta a Wireshark.

7. MONITORIZACIÓN DEL TRÁFICO EN REDES:

a) Descarga e instala software que monitorice y supervise el tráfico de la red y realiza filtrado de servicios de red: Syslog, SNMP y NetFlow. para monitorizar sólo el tráfico deseado. – diferente de Wireshark-.

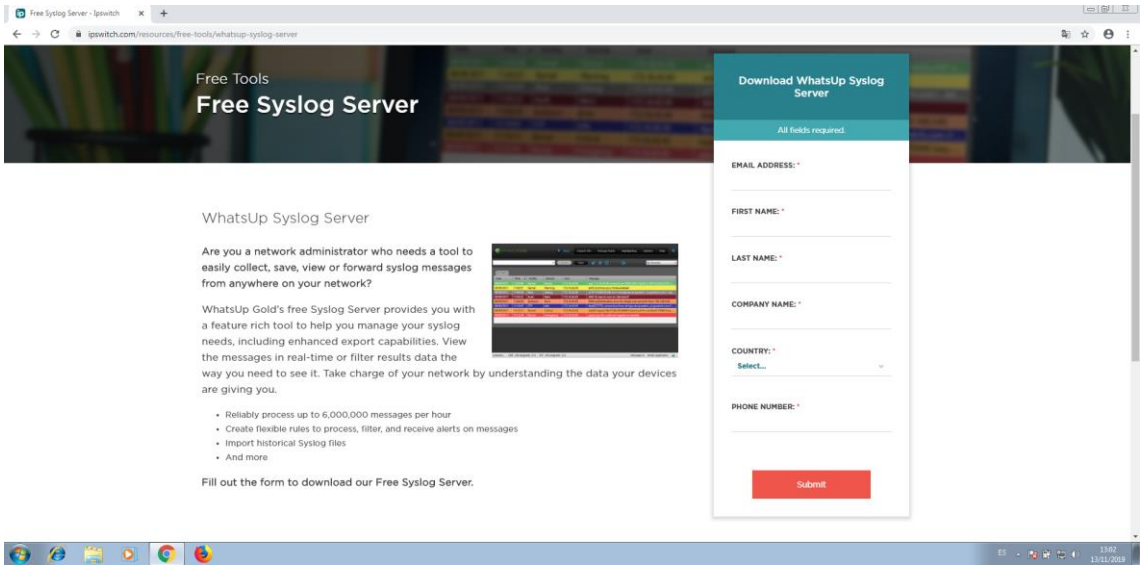
- Escenario



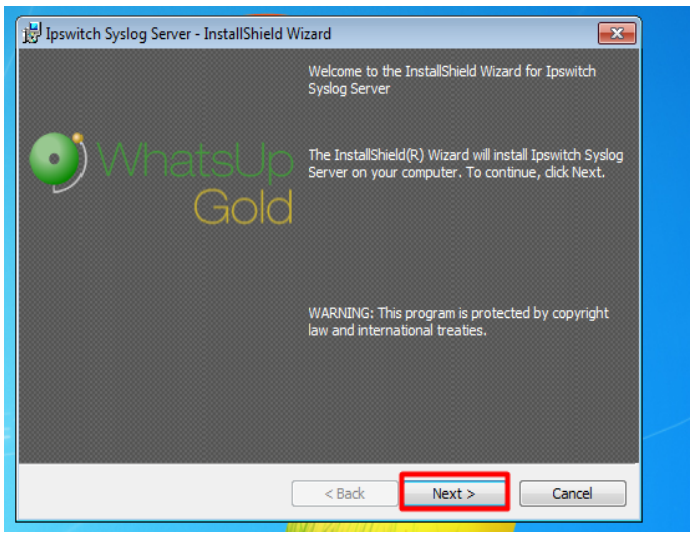
- SYSLOG

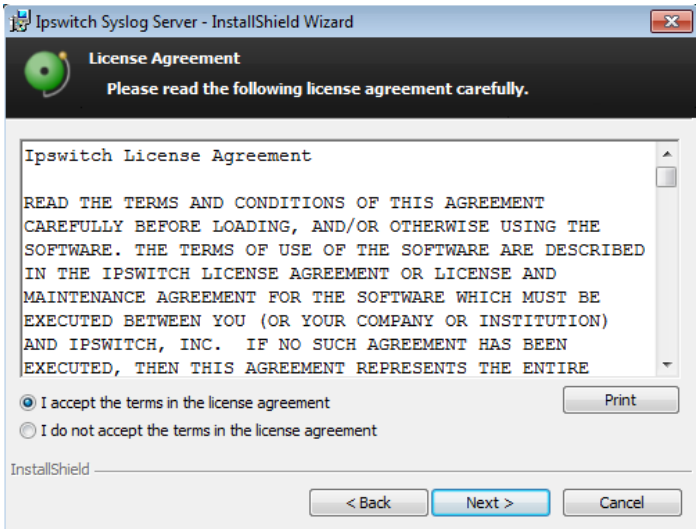
SYSLOG es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por SYSLOG se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

Descargaremos el software necesario, en mi caso usare WhatsUp Syslog en su versión gratuita. Podemos descargarlo pulsando aquí.

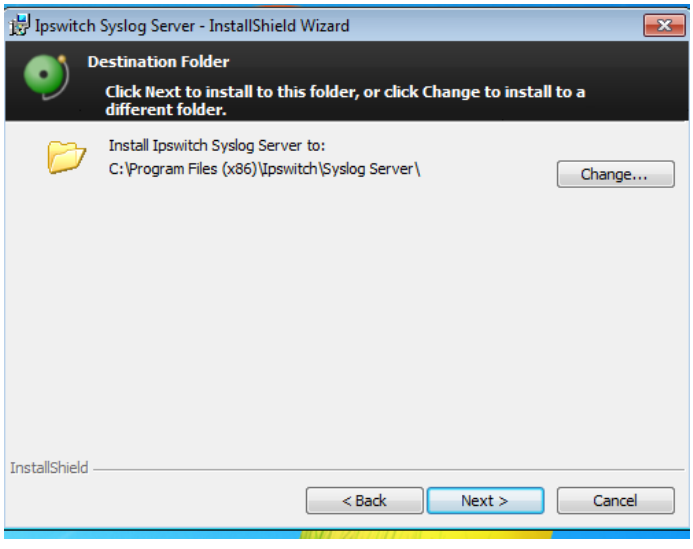


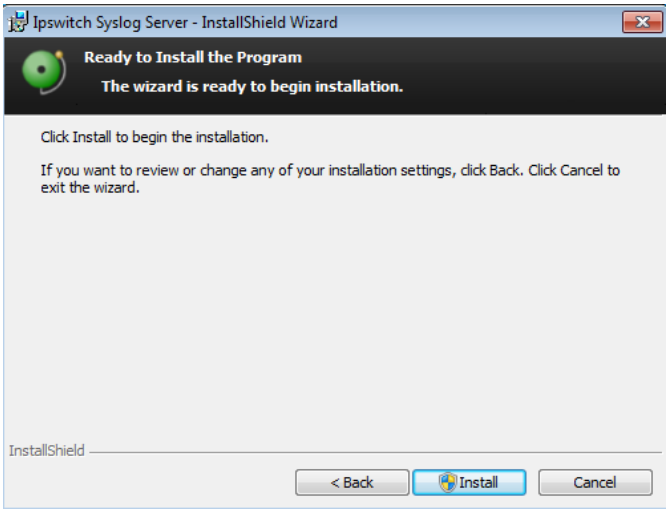
Lo descargamos e instalamos. Rellenaremos nuestros datos para poder descargarlo.



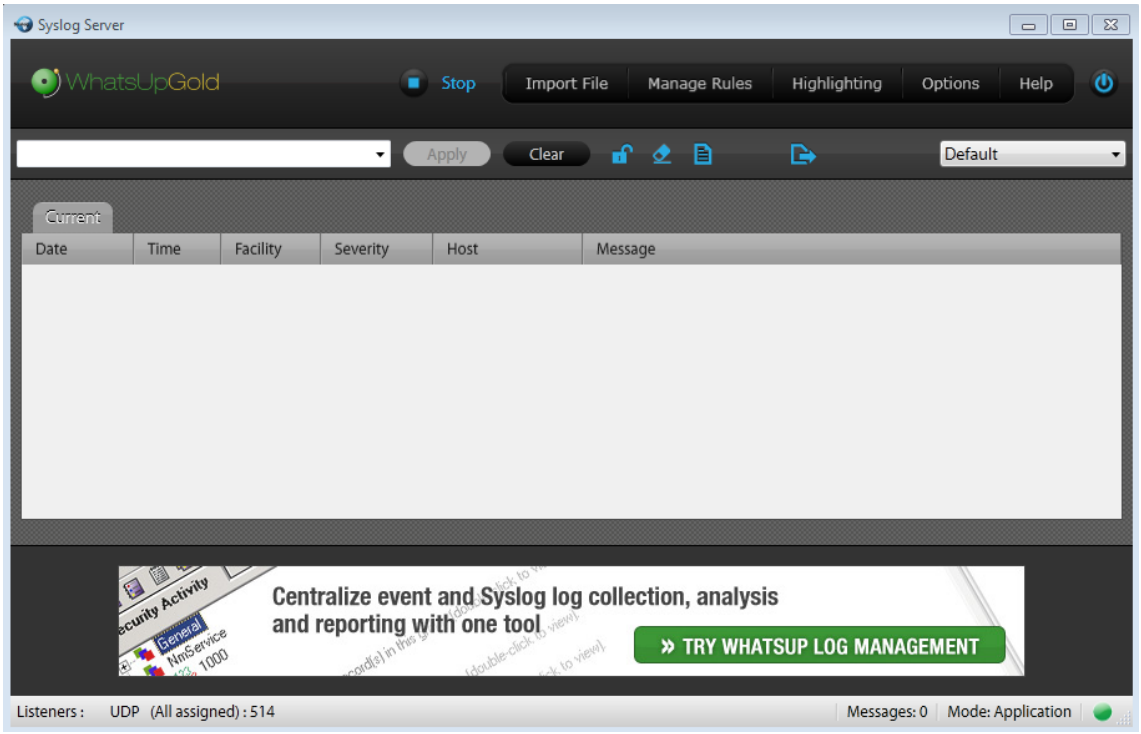


Escogemos la ruta de instalación e instalamos.





Una vez instalado lo ejecutamos.



Configuramos el router:

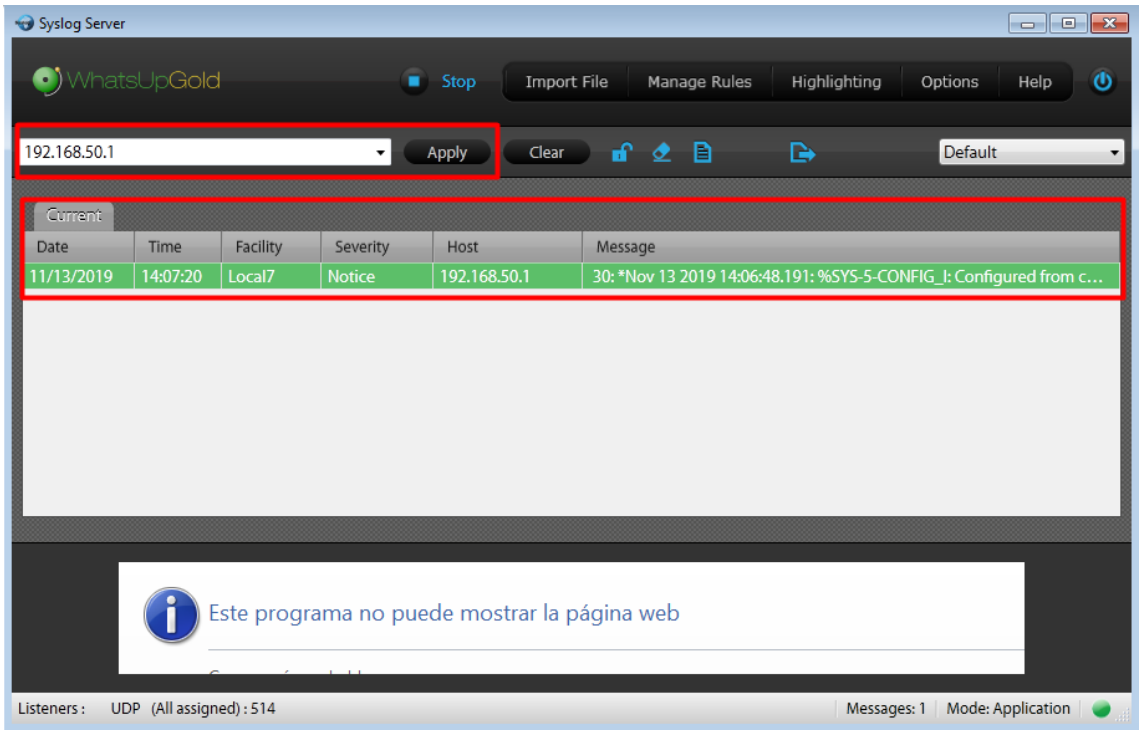
```
int f0/0
ip address 192.168.50.1 255.255.255.0
no shutdown
logging host 192.168.50.10
service timestaps log datetime msec *
```

(*): Este comando se utiliza para, que los mensajes que almacena el servidor Syslog, tengan la fecha, hora (con minutos y segundos).

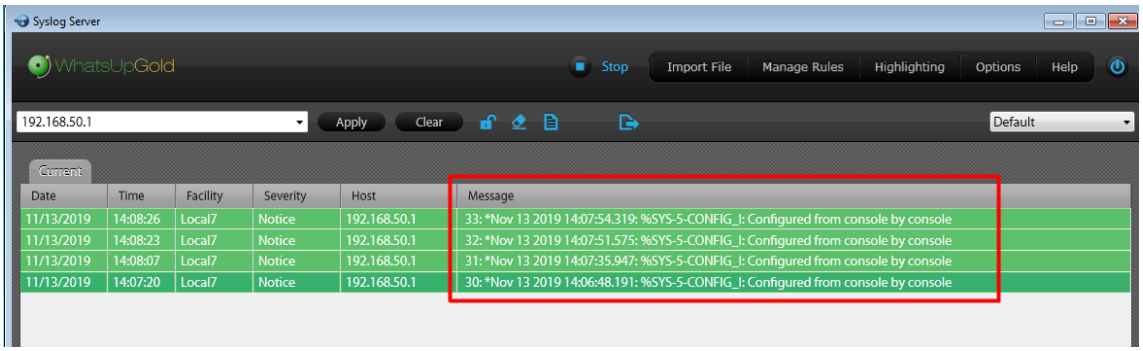
```
R1-franciscojesus(config)#int f0/0
R1-franciscojesus(config-if)#ip address 192.168.50.1 255.255.255.0
R1-franciscojesus(config-if)#no shutdown
R1-franciscojesus(config-if)#
```

```
R1-franciscojesus(config)#service timestamps log datetime msec year
R1-franciscojesus(config)#logging host 192.168.50.10
R1-franciscojesus(config)#
```

Ahora en el programa del Syslog ponemos la IP del router y damos en *Apply*. Veremos como empiezan a llegar los mensajes Syslog del router al servidor Syslog.



En mi caso entro y salgo del *conf t* a *enable* en repetidas ocasiones para generar más mensajes Syslog y que el router los envíe al servidor Syslog.



Ya tenemos el servidor Syslog configurado, ahora vemos el siguiente.

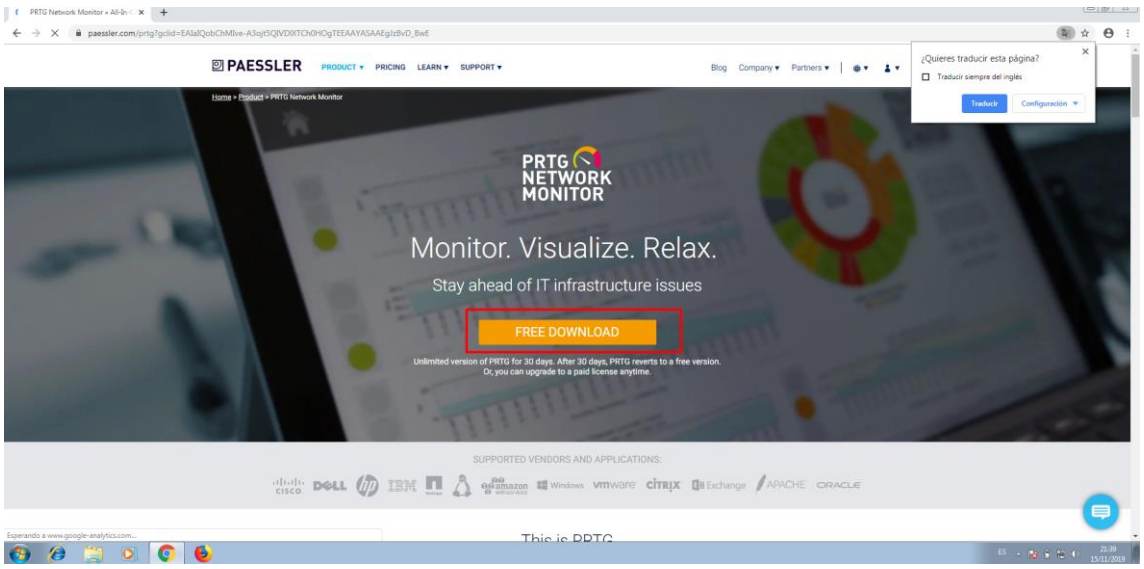
- SNMP

El Protocolo simple de administración de red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

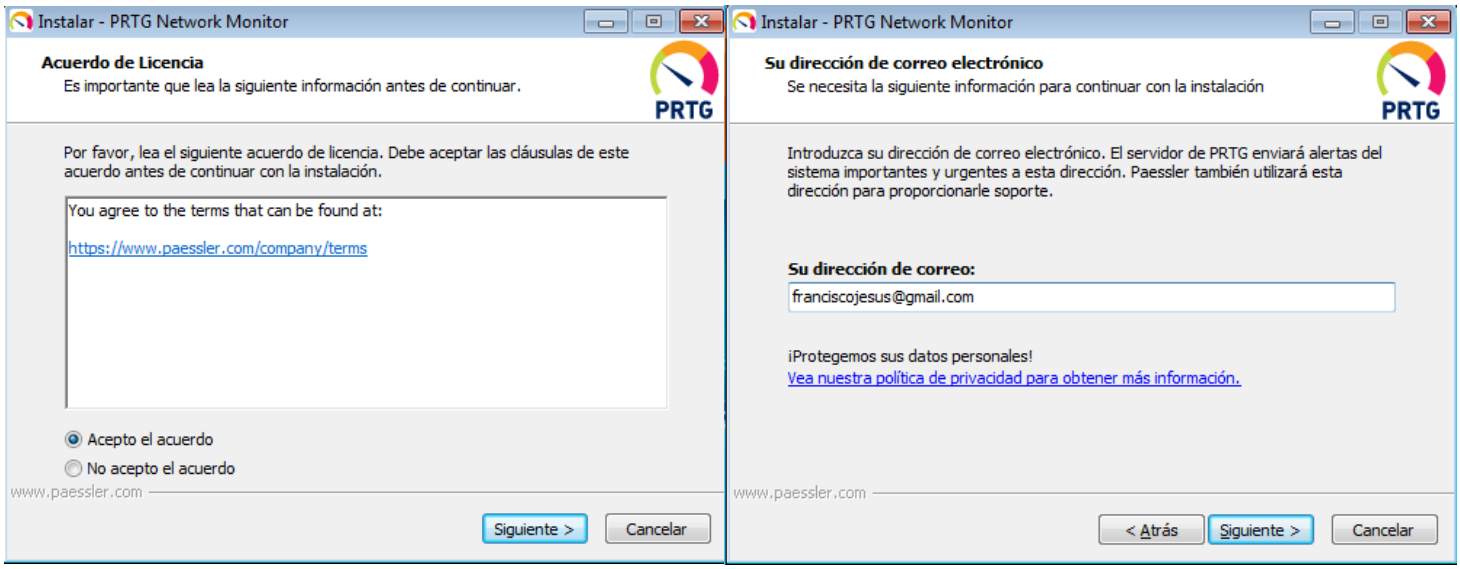
Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

En mi caso para esta práctica usare el escenario anterior, pero con otro router nuevo. El programa utilizado será PRTG. Puedes descargarlo desde aquí.

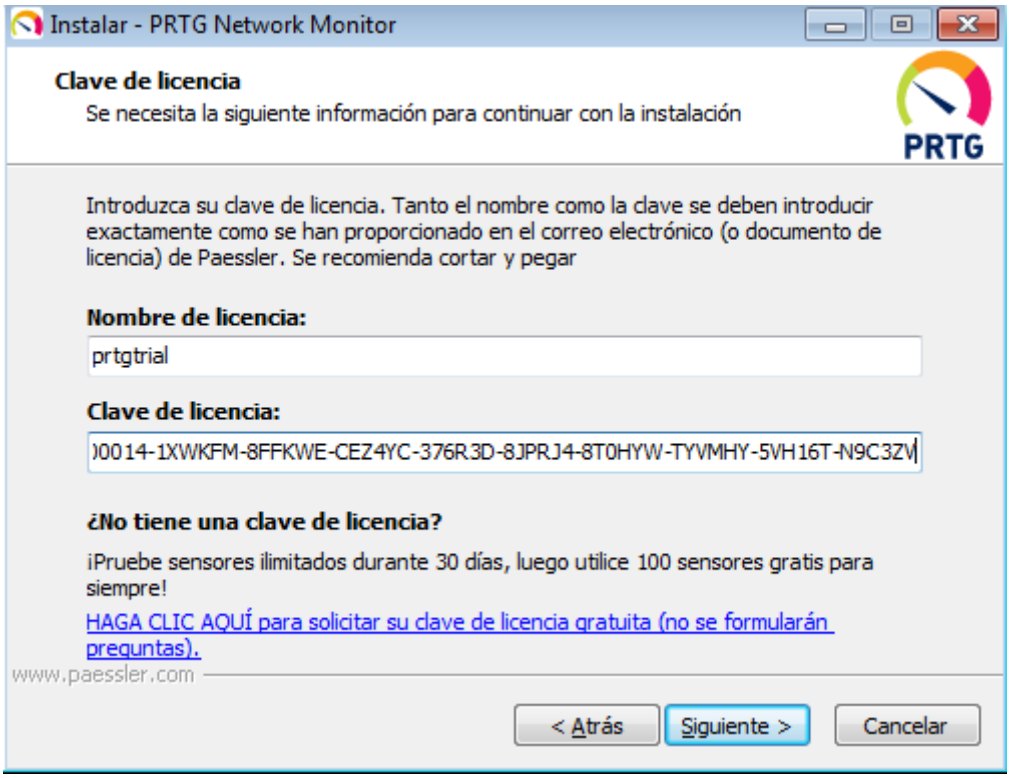
PRTG Network Monitor es un software de monitoreo de red. Puede monitorear y clasificar las condiciones del sistema, como el uso del ancho de banda o el tiempo de actividad, y recopilar estadísticas de varios hosts como conmutadores, enrutadores, servidores y otros dispositivos y aplicaciones.



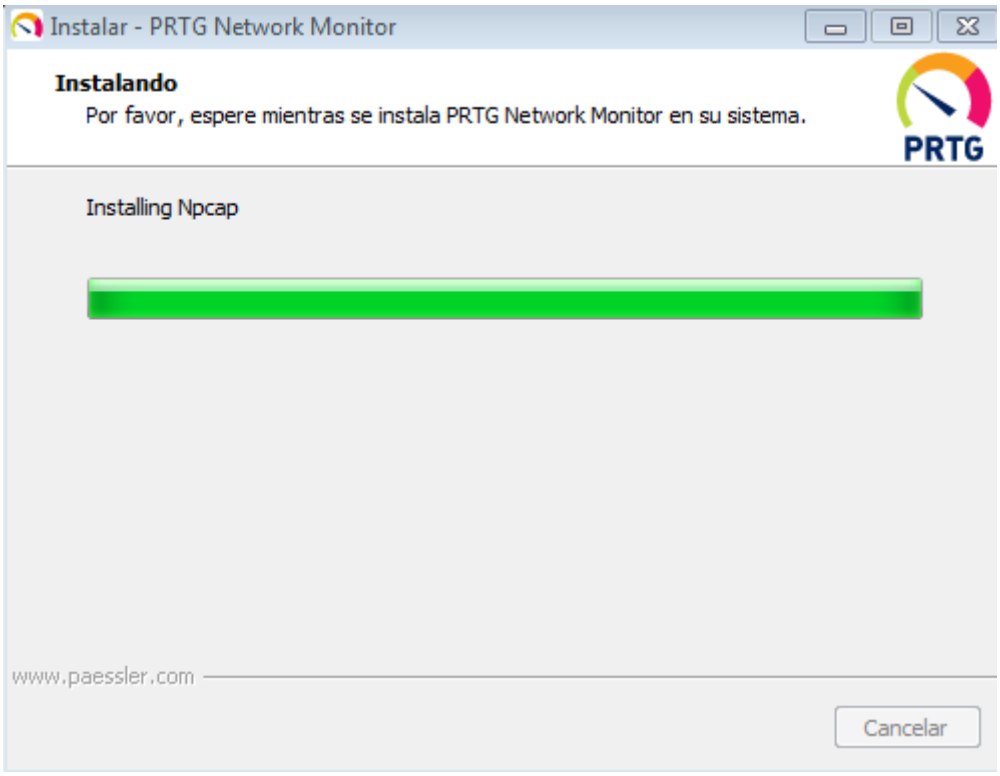
Lo descargamos e instalamos. Aceptamos los términos y condiciones e introducimos nuestro correo.



Introducimos el nombre de licencia y clave de licencia que nos enviaron.



Esperamos a que se instale.



Configuramos el router para que se muestre como un usuario SNMP.

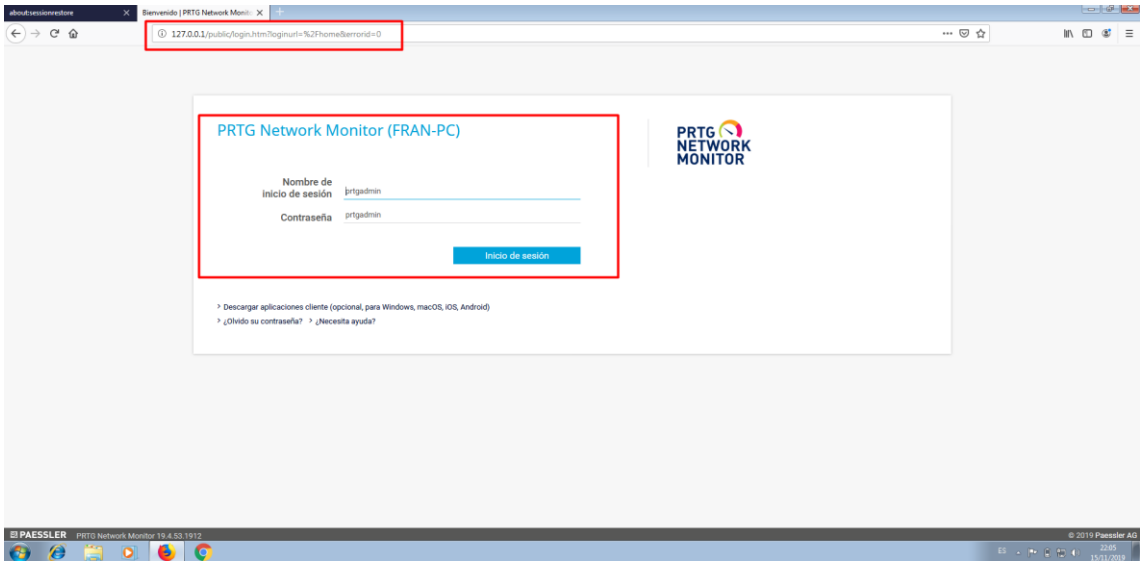
```
configure terminal

snmp-server community  p2 ro

snmp-server community  p2 rw
```

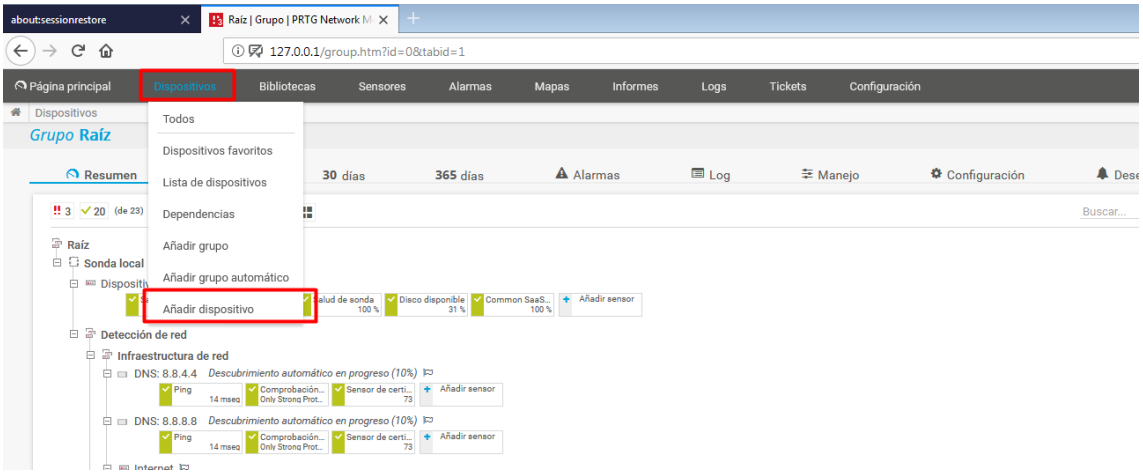
```
franciscojesus-snmp(config)#int f0/0
franciscojesus-snmp(config-if)#ip address 192.168.50.1 255.255.255.0
franciscojesus-snmp(config-if)#ex
franciscojesus-snmp(config)#snmp-server community  p2 rw
```

Ahora accederemos al PTRG vía web.

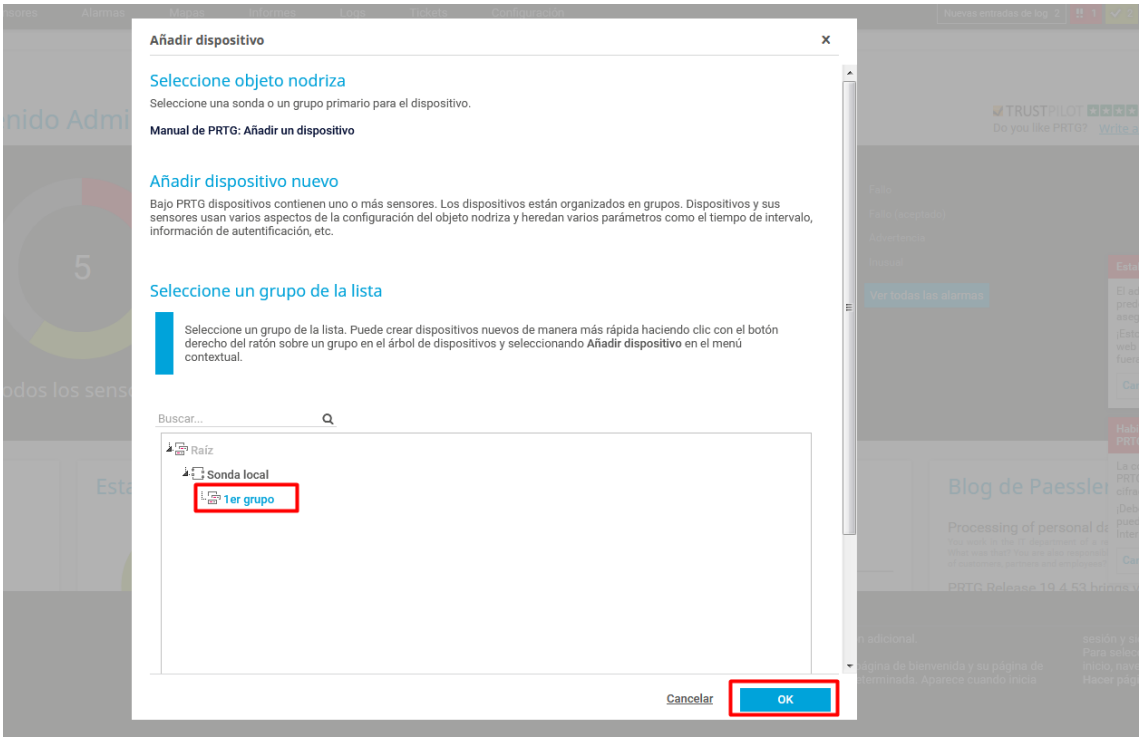


Podemos ver un informe general de PTRG

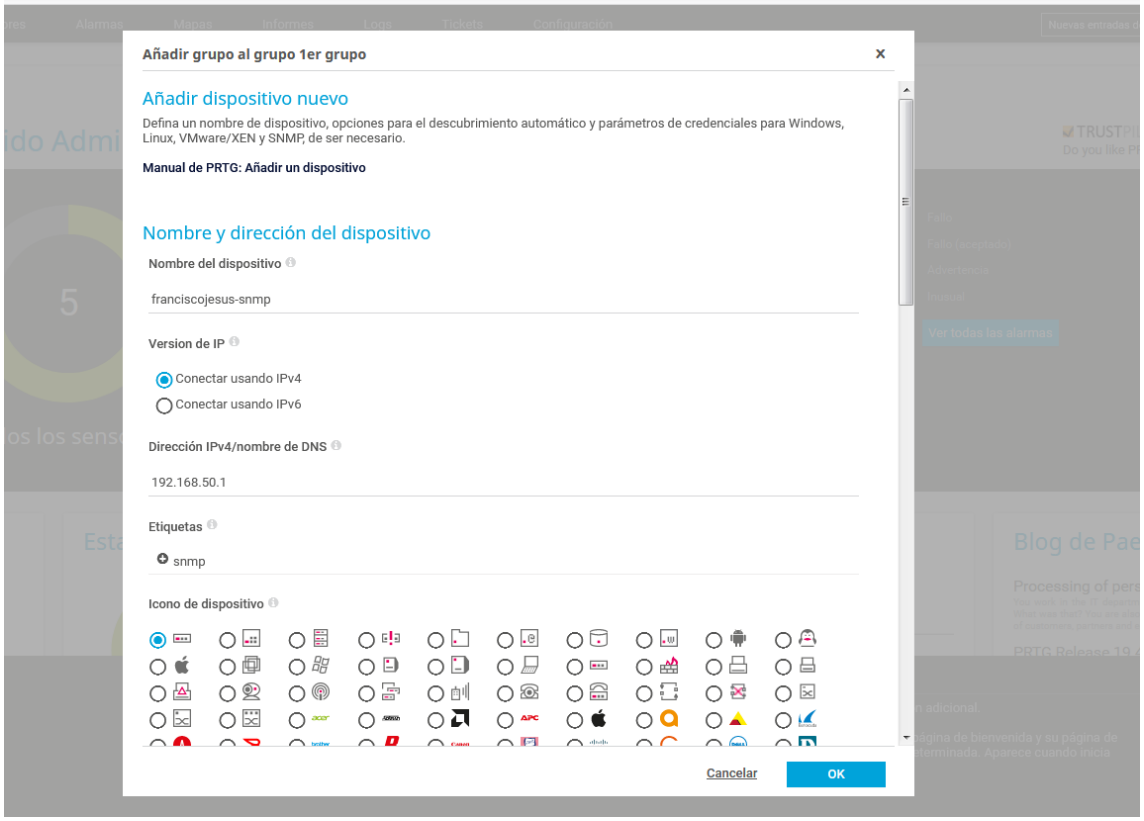
Añadiremos al router.



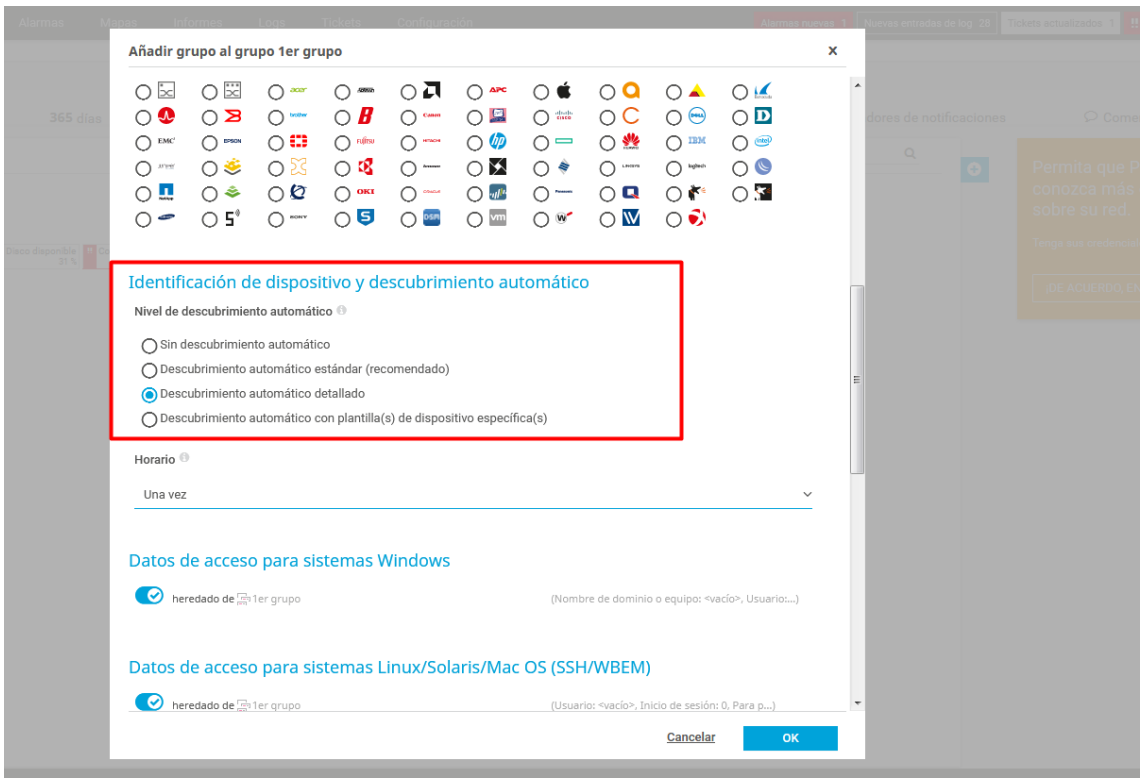
Escogemos el grupo.



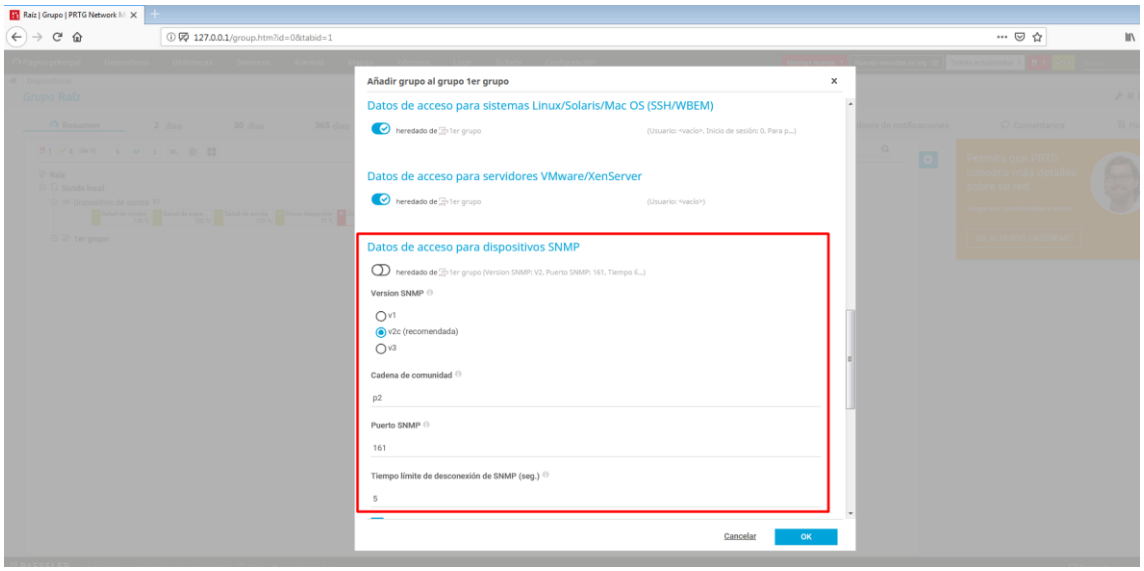
Le pondremos el nombre, la IP, etiqueta…



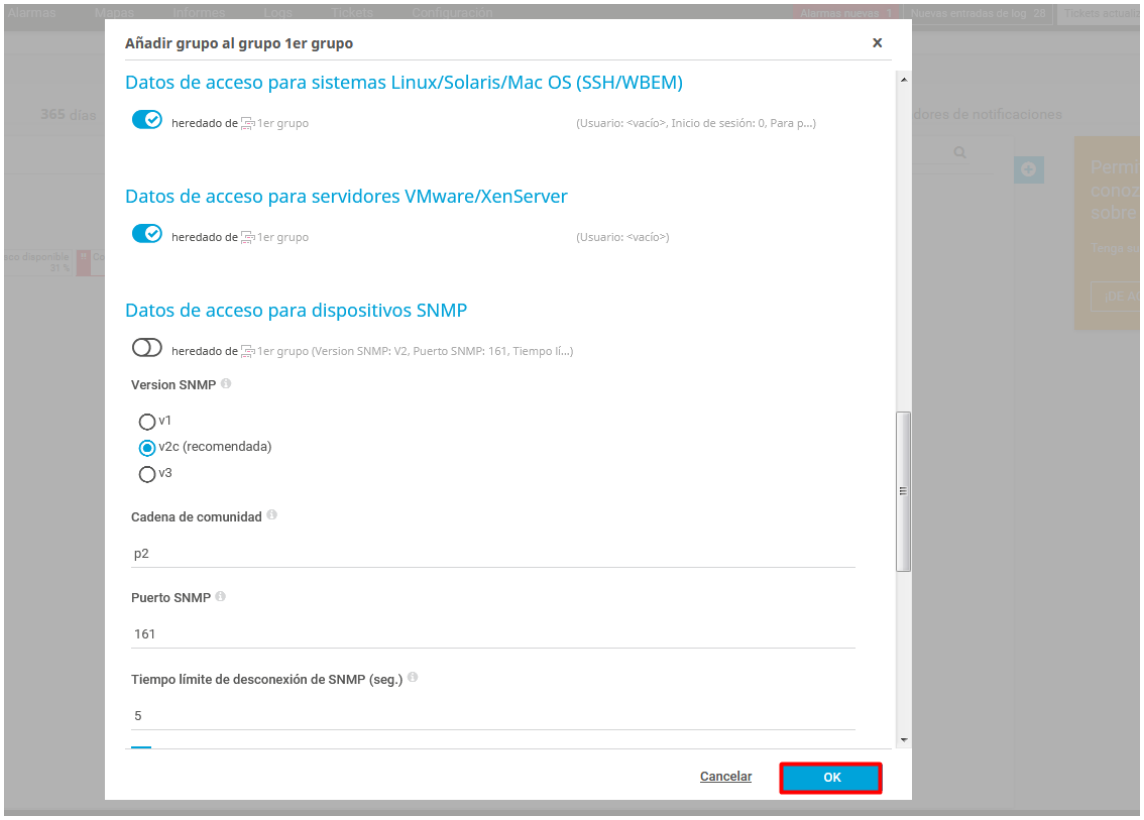
Escogemos identificar el dispositivo detalladamente una vez.



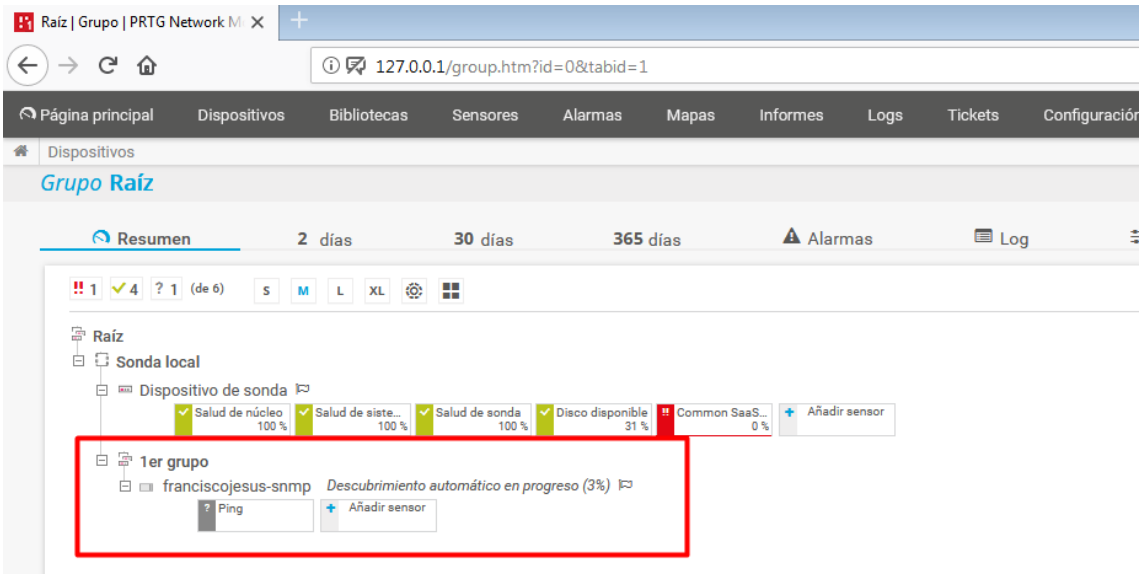
Configuramos SNMP con el usuario.



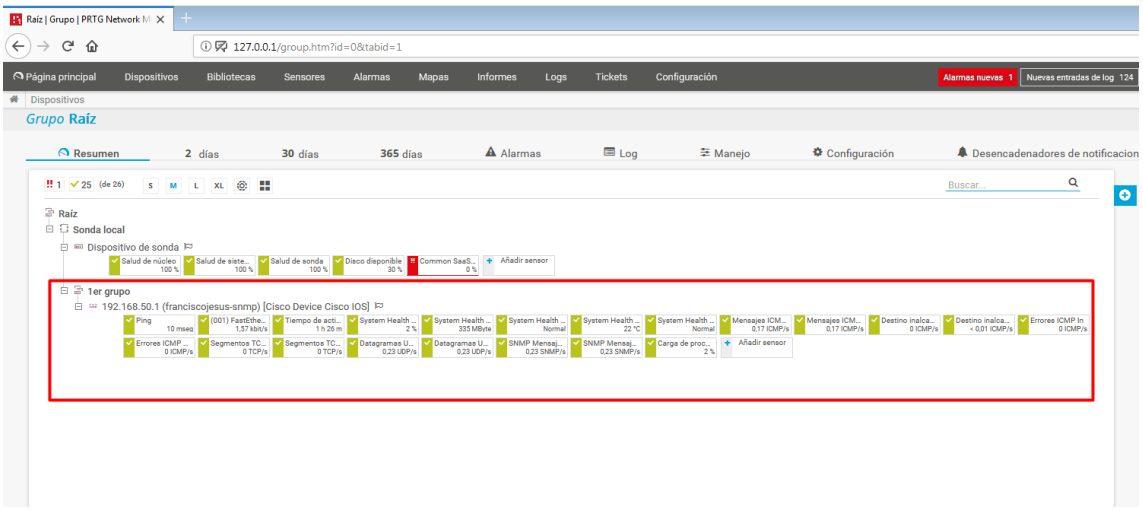
Pulsamos en *OK* para añadir el dispositivo.



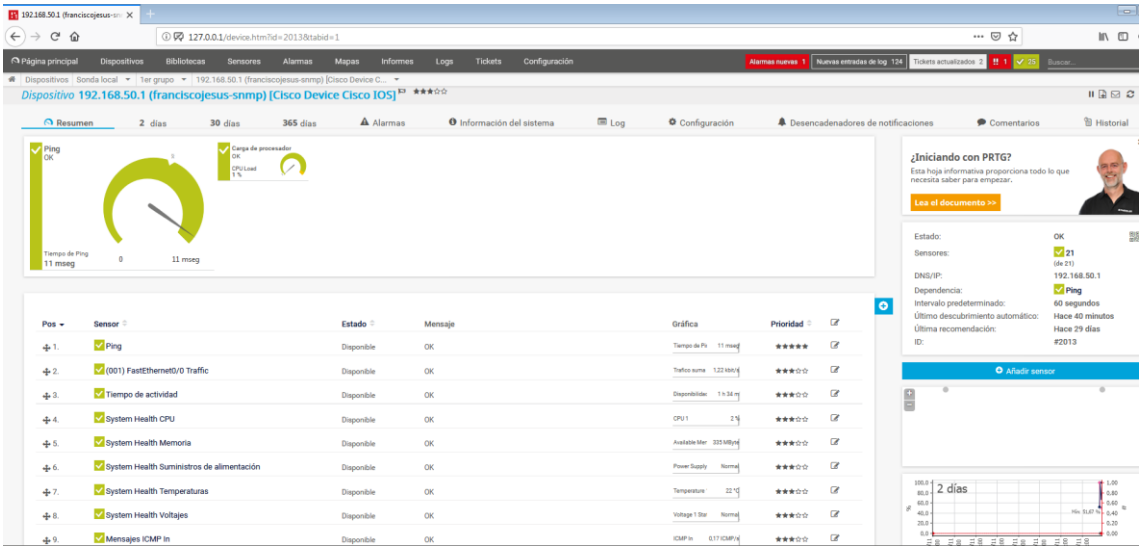
Vemos el nuevo dispositivo agregado, esperamos a que lo analice.



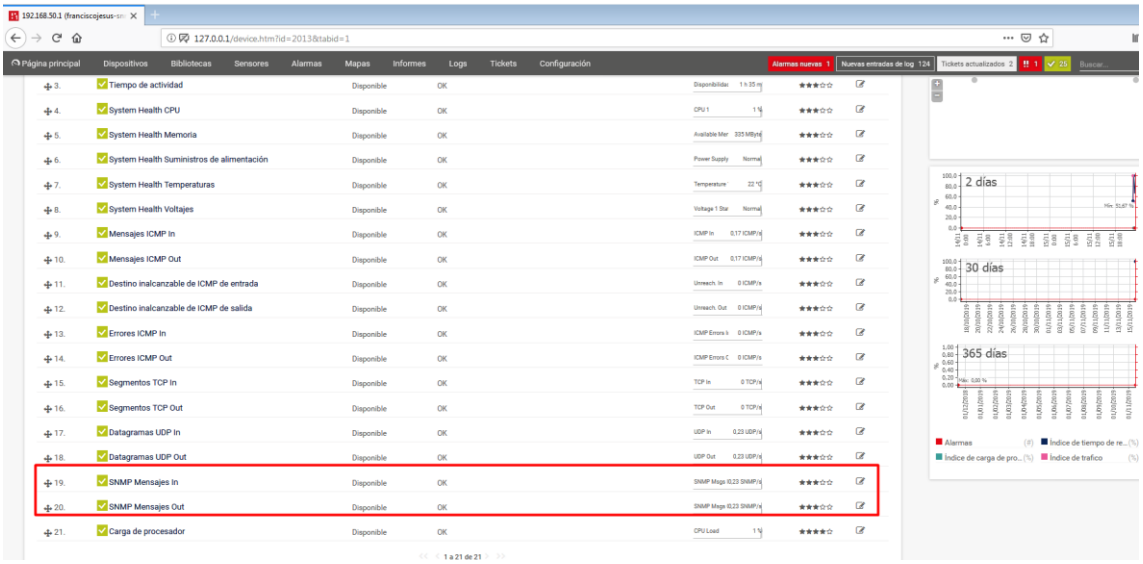
Podemos ver como lo analizo detalladamente y reconoce que es un dispositivo Cisco aparte de otros servicios.



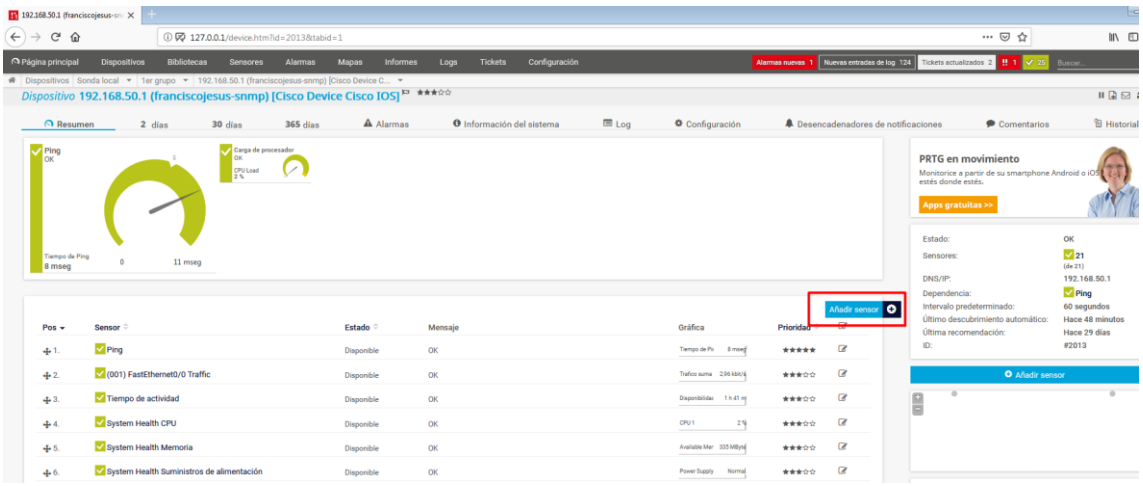
Pulsaremos en el para entrar. Podemos ver el dispositivo con los sensores activos.

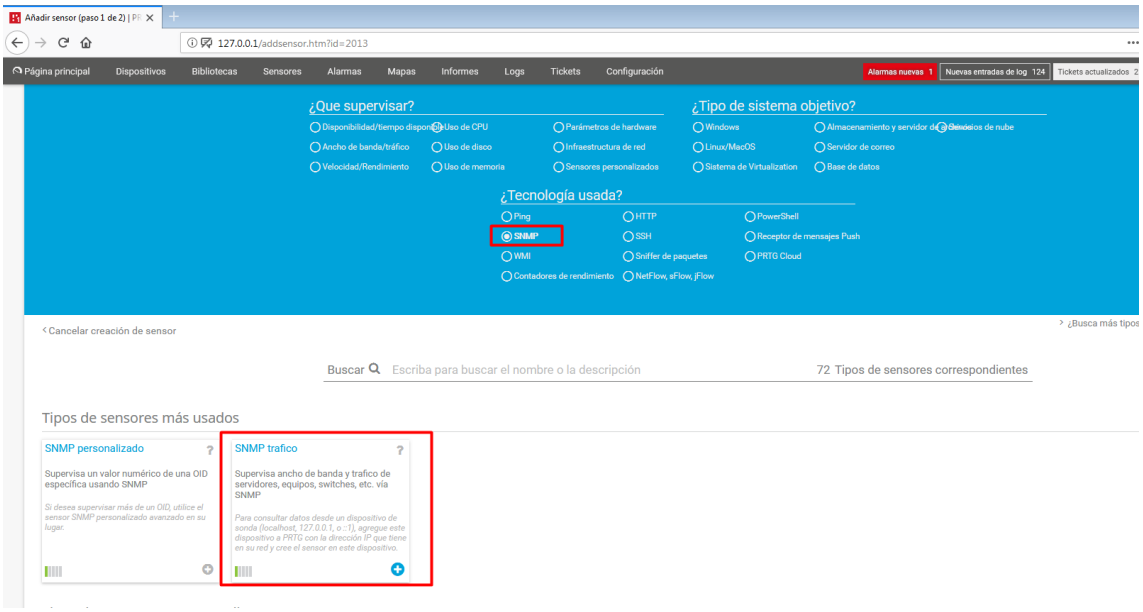


Podemos ver el SNMP debajo.

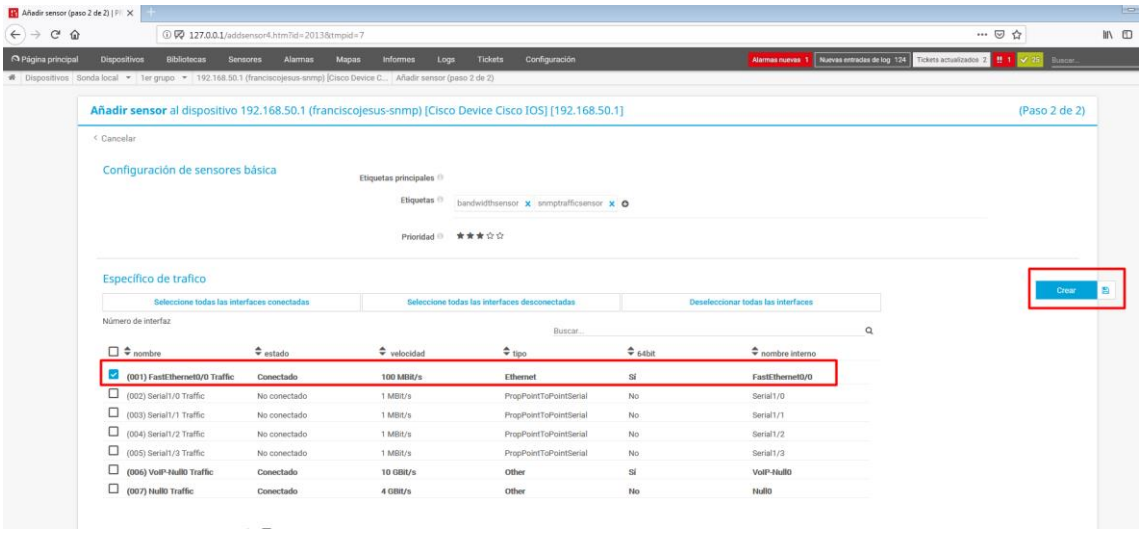


Añadiremos el sensor SNMP nuevo para poder controlarlo.

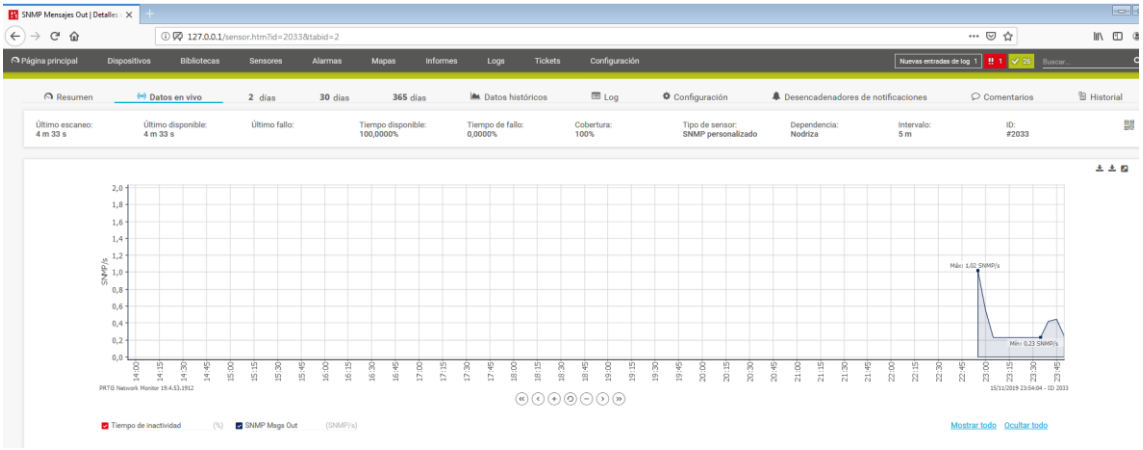


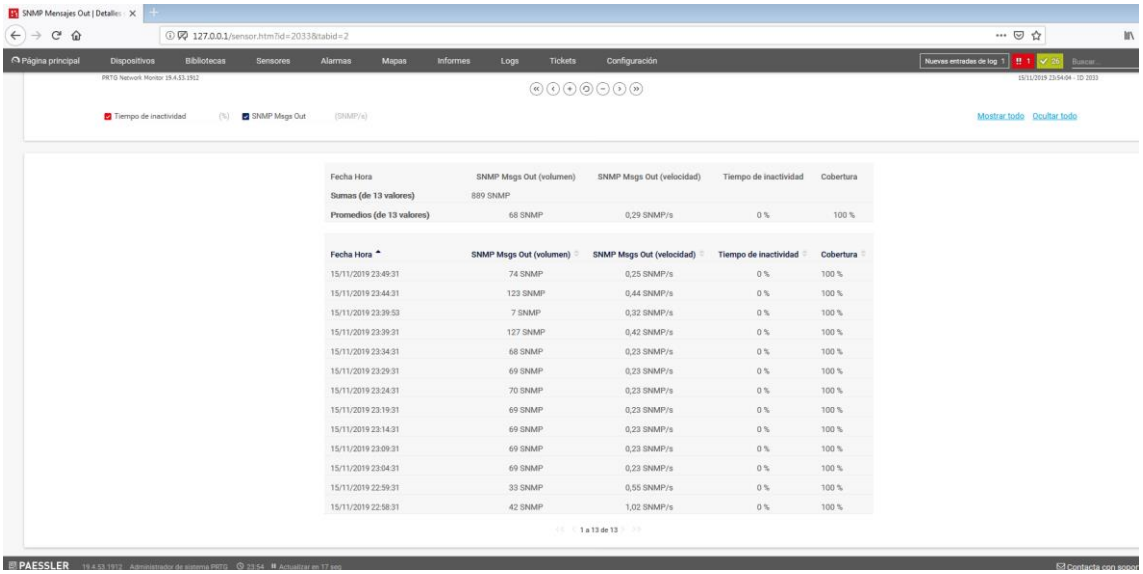


Seleccionaremos la interfaz< (la cual la detecta automáticamente por el análisis) y damos a crear.

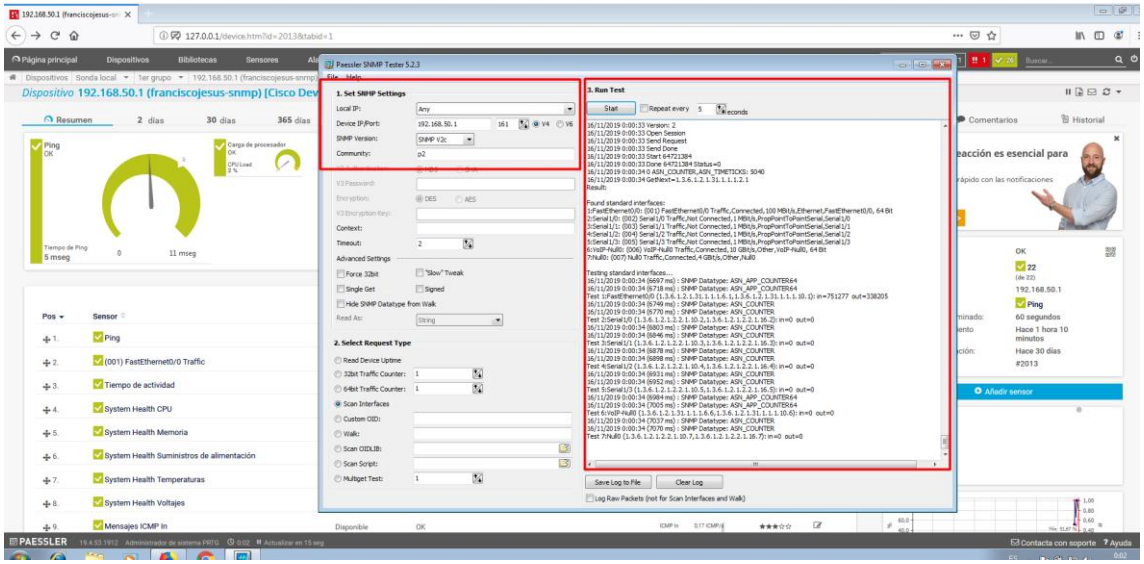


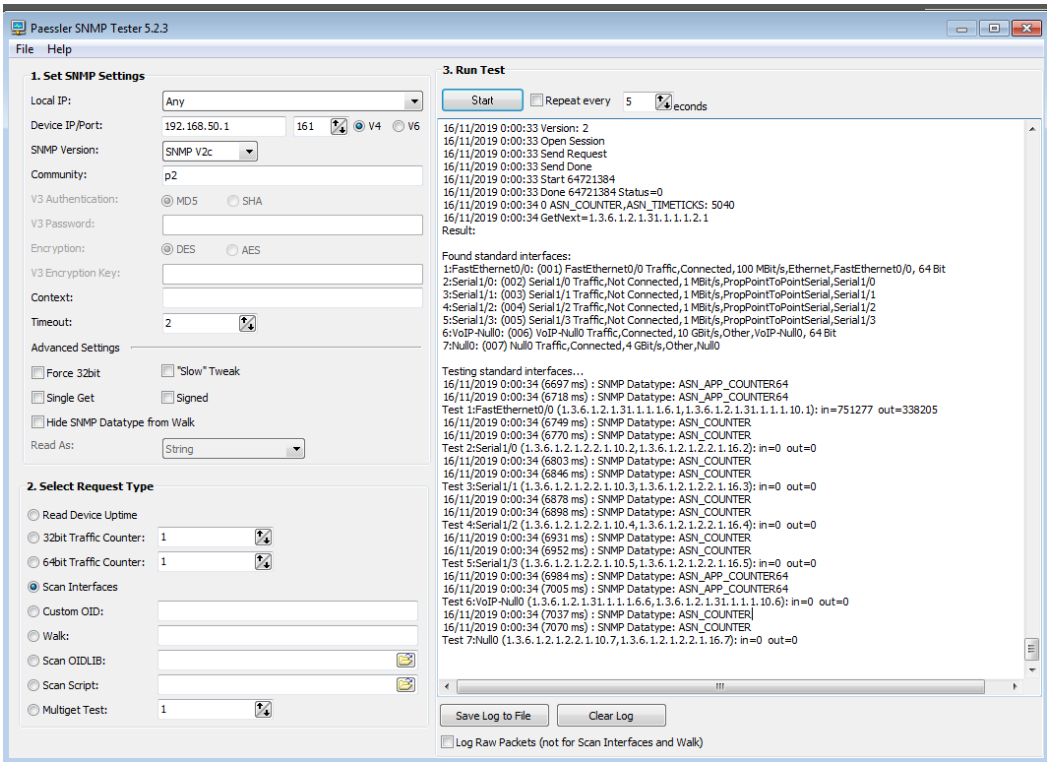
Si pulsamos en el SNMP podemos ver la información en tiempo real.



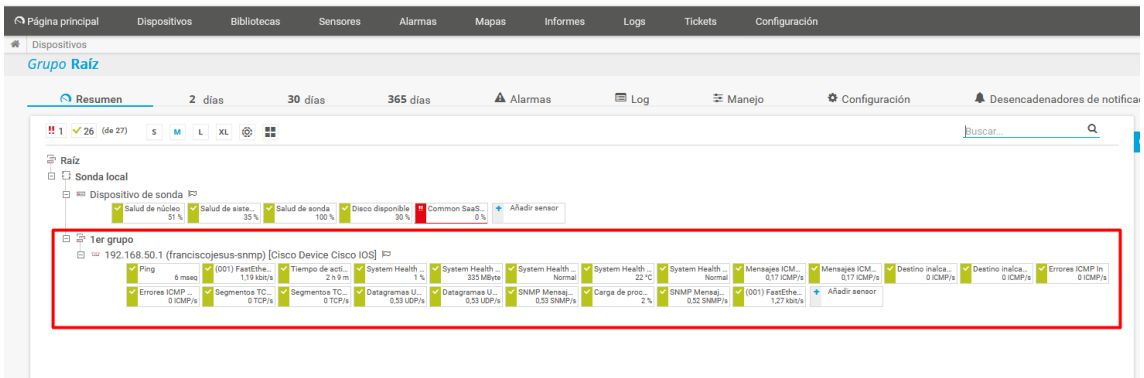


Podemos usar la aplicación de PRTG para poder entrar con SNMP.





Podemos ver como el router se encuentra totalmente operativo.

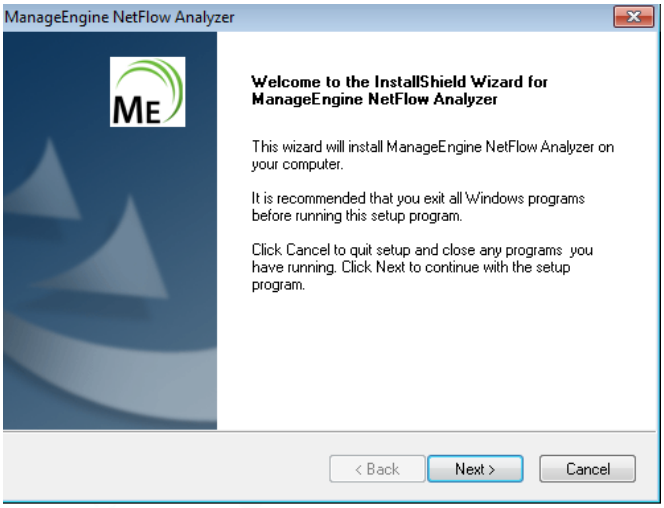


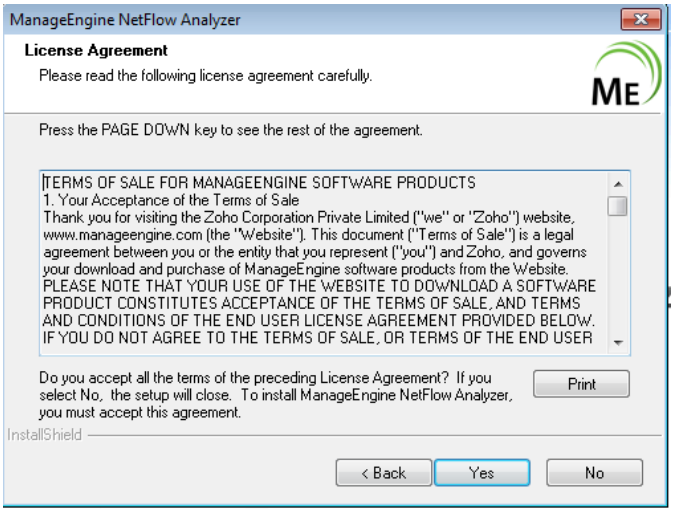
- Netflow

NetFlow es un protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP.

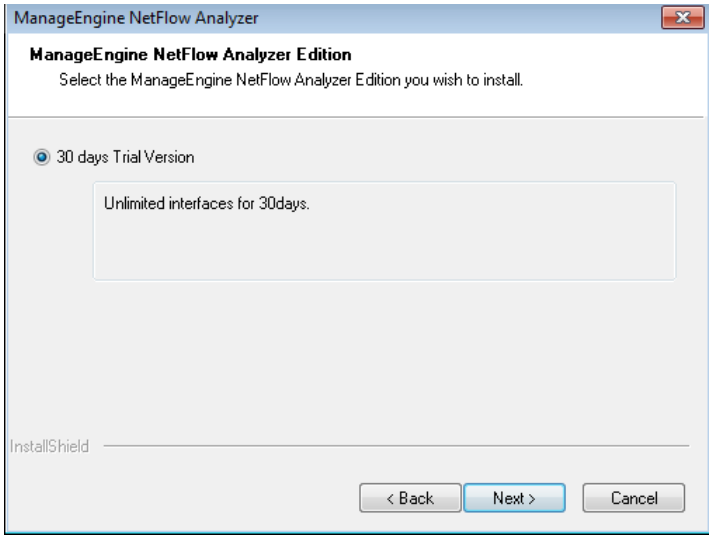
Para esta parte usare Netflow Analyzer para no repetir la misma empresa que en el apartado anterior.

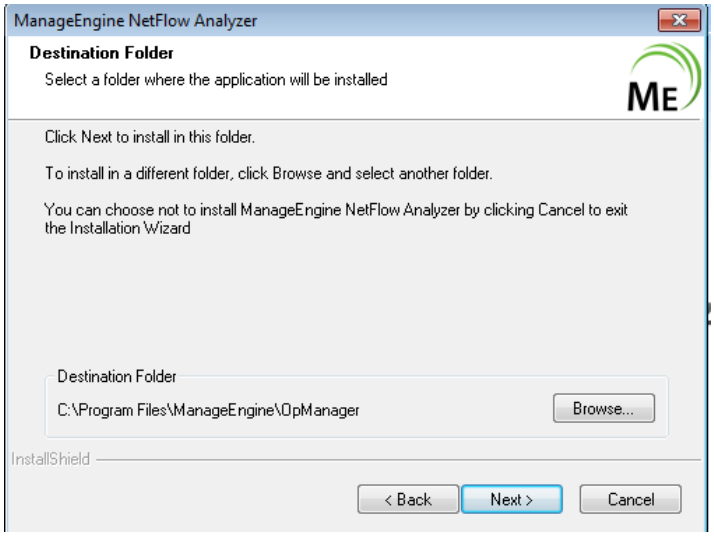
Lo descargamos y lo instalamos.



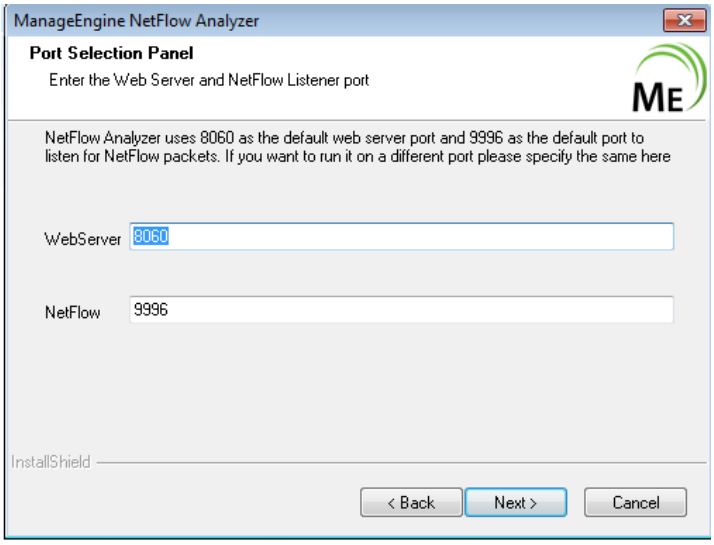


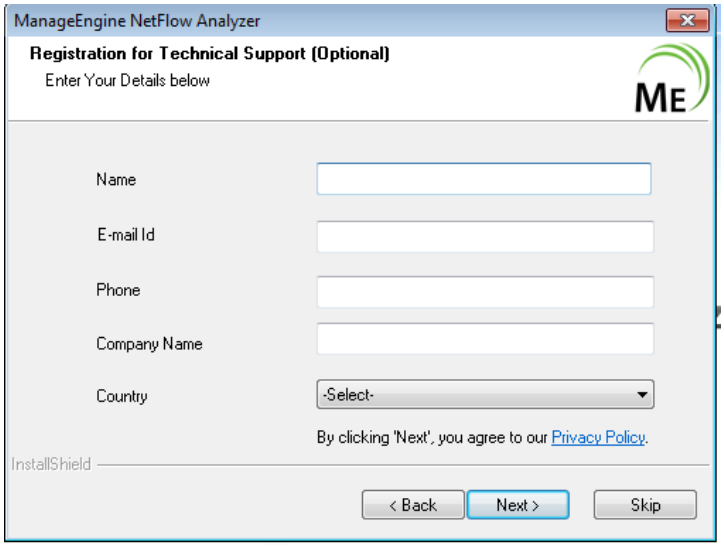
Escogemos la versión de prueba. Después escogemos la carpeta de instalación.



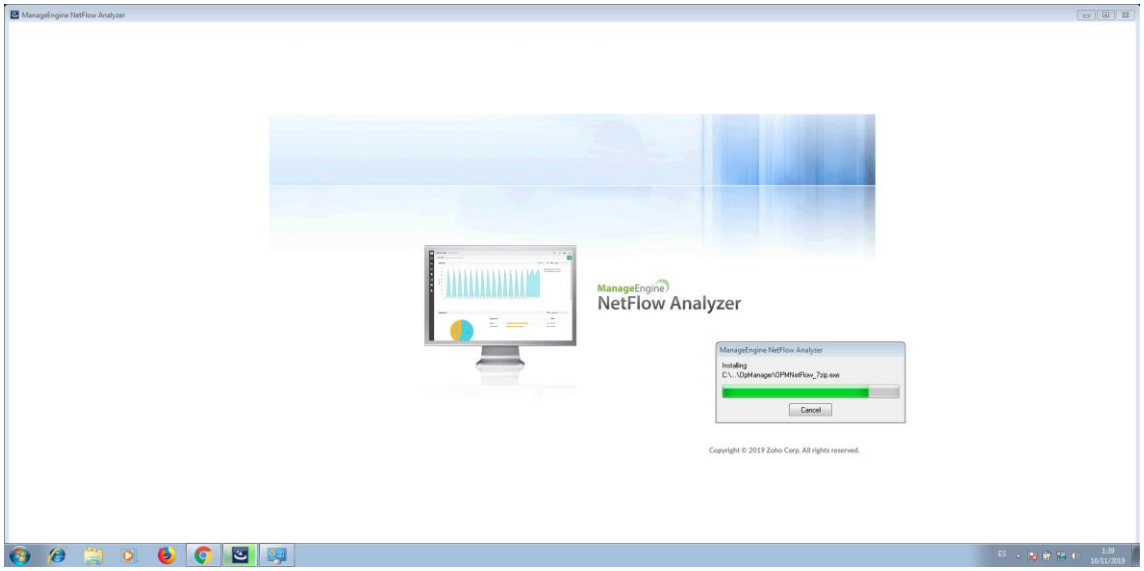


Dejamos los puertos por defecto. Rellenamos en la siguiente con nuestros datos.

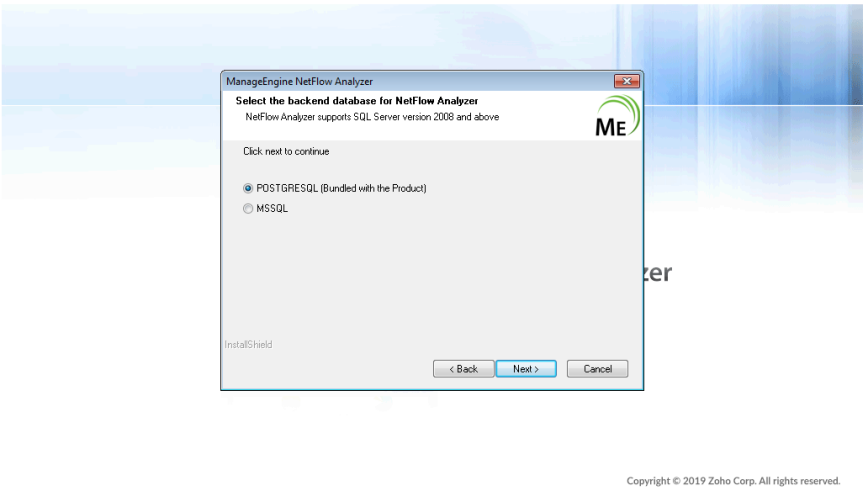




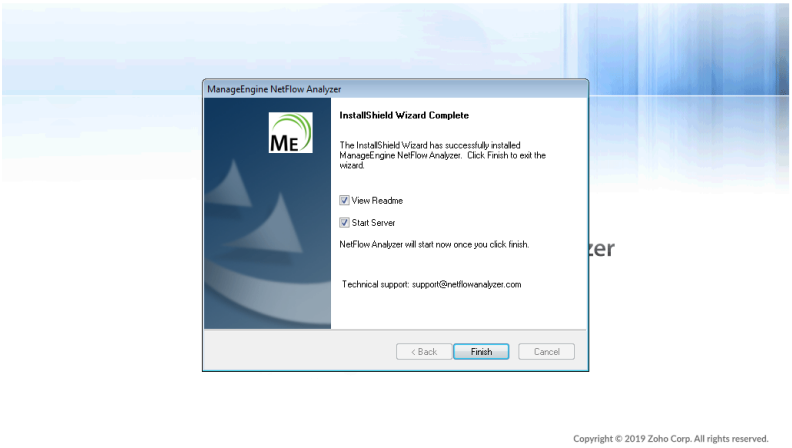
Esperamos a que se instale.



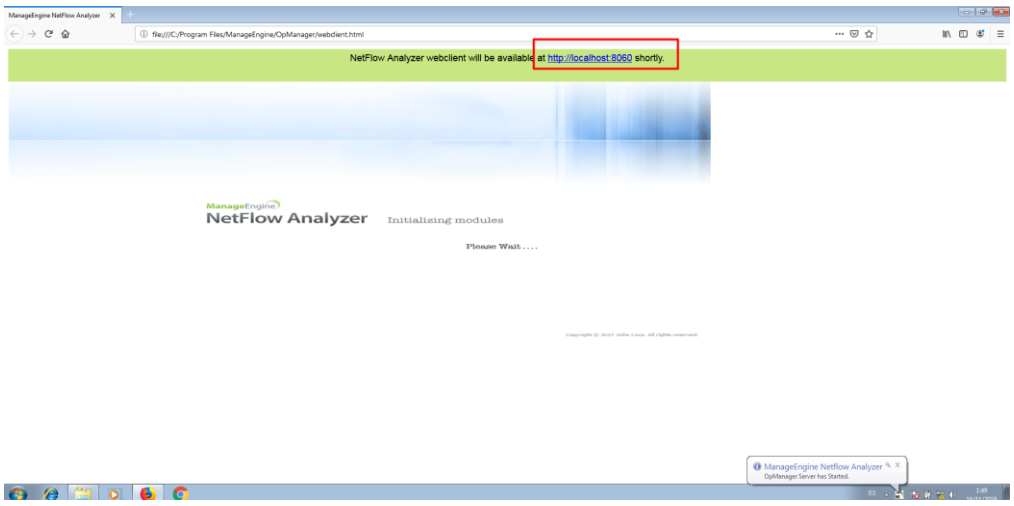
Escogemos el tipo de base de datos.



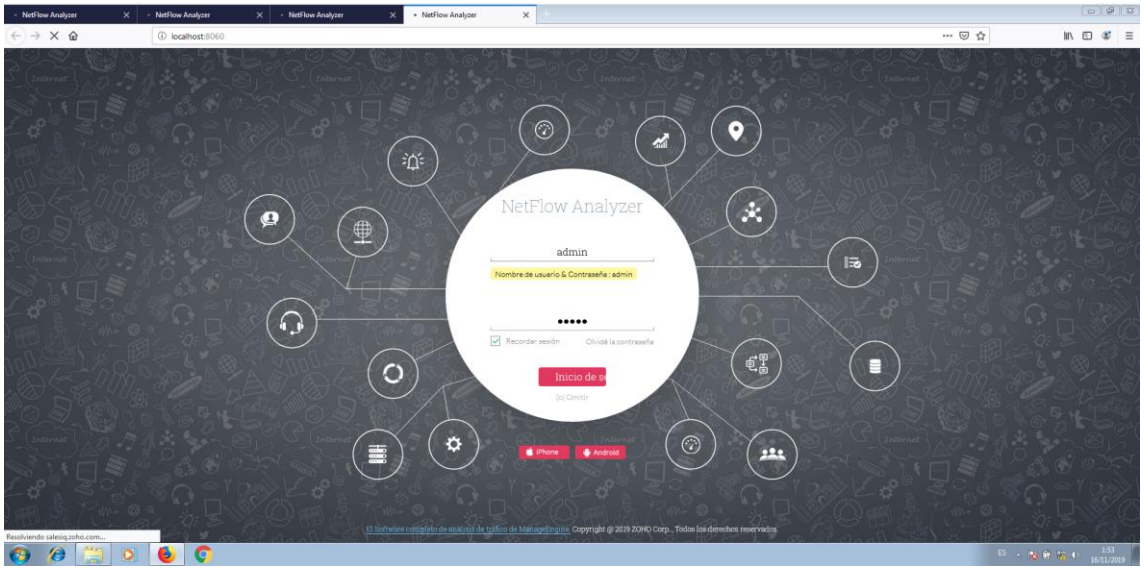
Pulsamos en *Finish* para finalizar.



Una vez finalizado solo pulsamos en el link para entrar.



Entramos con el usuario y contraseña que están por defecto.

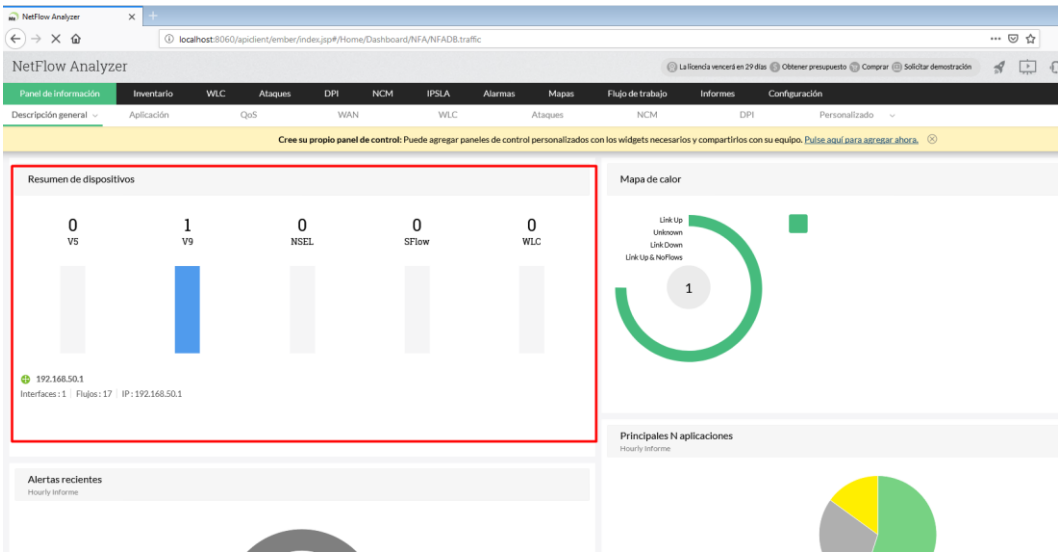


Antes de continuar configuraremos el router.

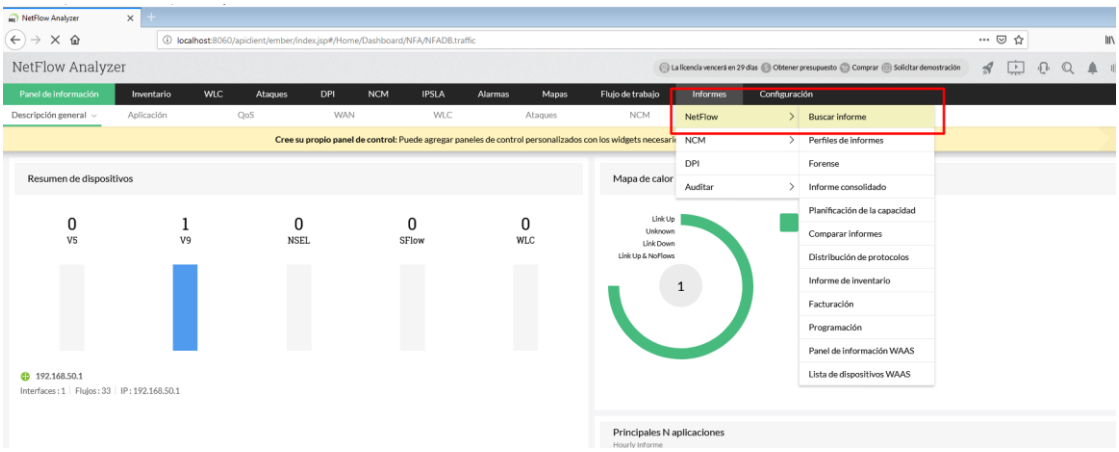
```
interface f0/0
ip flow ingress
ip flow egress
exit
ip flow-export destination 192.168.50.20 9996
ip flow-export version 9
```

```
frankynetflow(config)#int f0/0
frankynetflow(config-if)#ip flow ingress
frankynetflow(config-if)#ip flow egress
frankynetflow(config-if)#exit
frankynetflow(config)#ip flow-export destination 192.168.50.20 9966
frankynetflow(config)#ip flow-export version 9
frankynetflow(config)#end
frankynetflow#wr
Building configuration...
[OK]
```

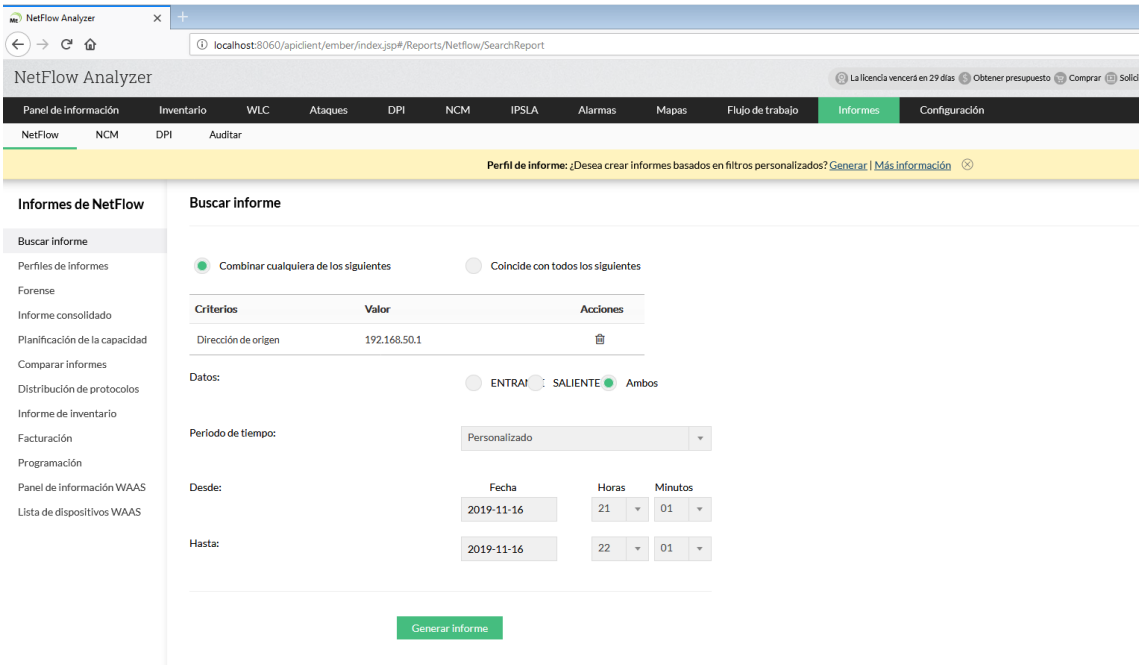
Si entramos en el panel veremos el resumen del router y podemos observar como Netflow esta configurado en su versión 9 tal cual indicamos en el router al configurarlo.



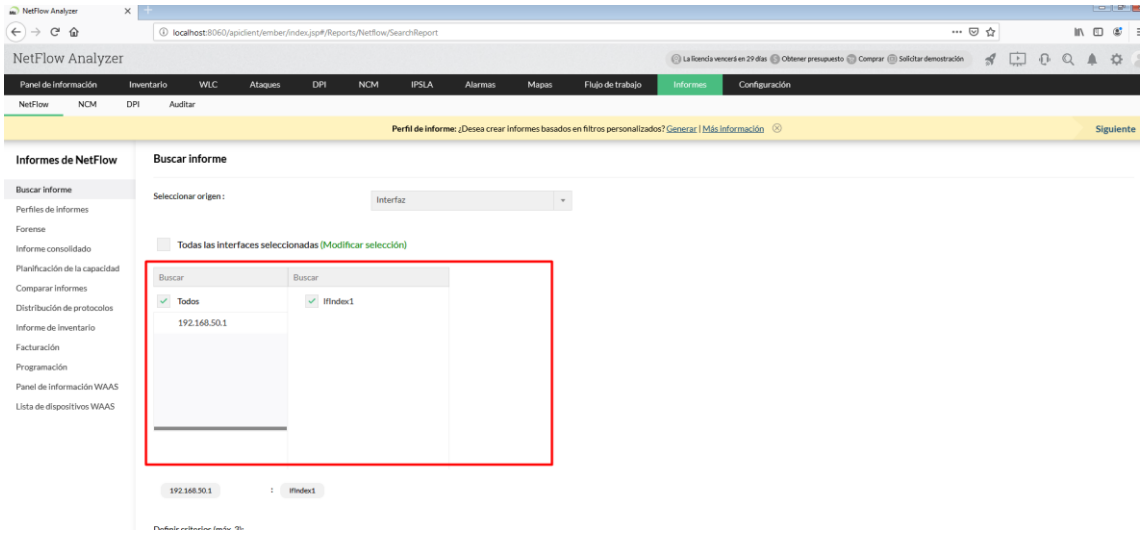
Vamos a *Informes –> Netflow* → *Buscar Informe* para generar un informe.



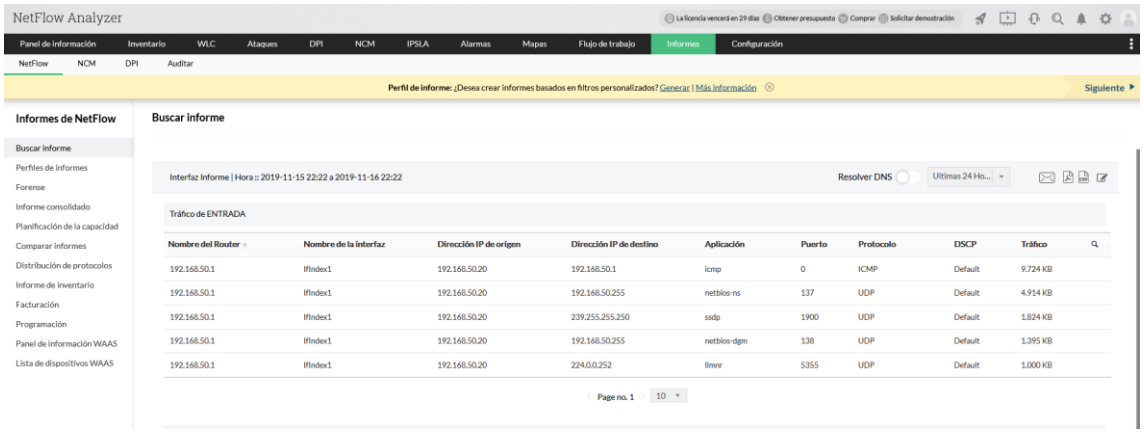
Filtraremos por la fecha que queramos.

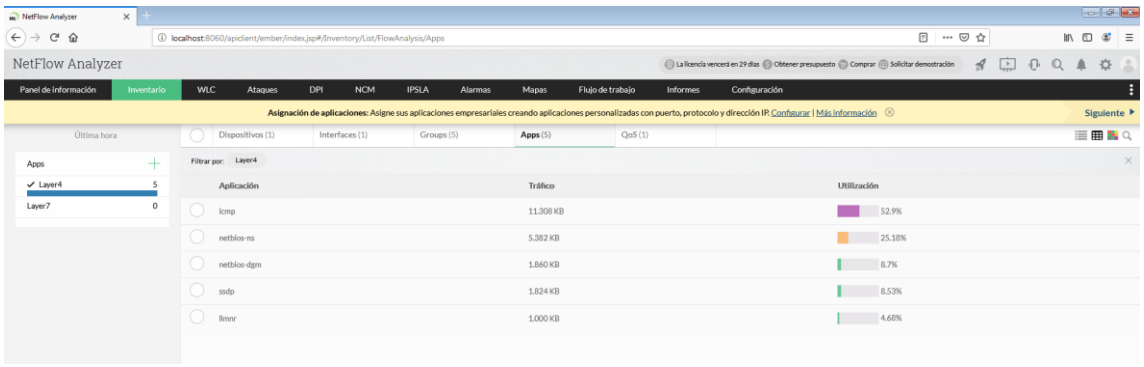


Podemos filtrar también por el dispositivo y la interfaz.



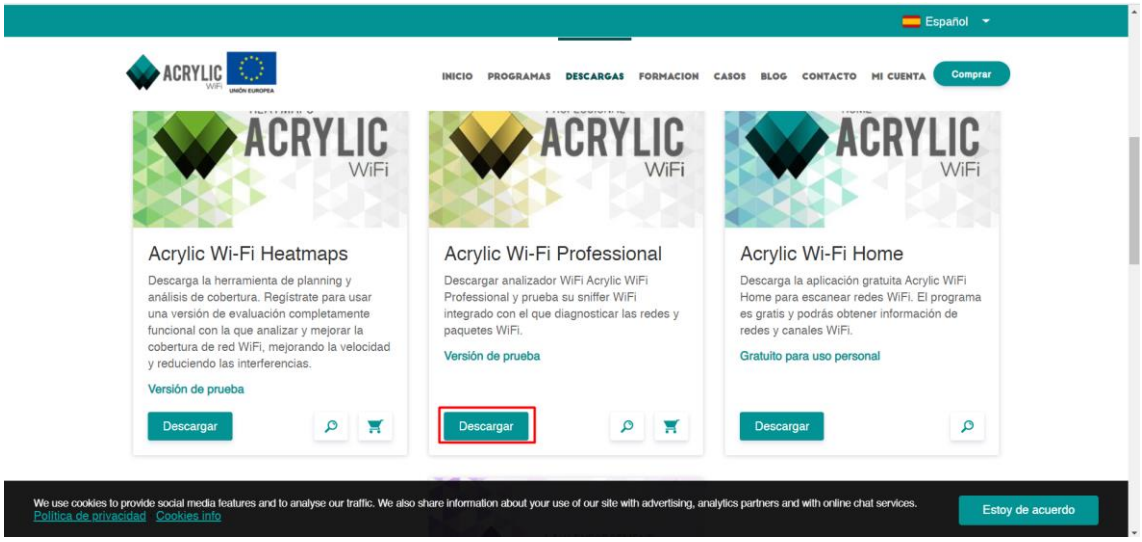
Podemos ver toda la información del dispositivo.



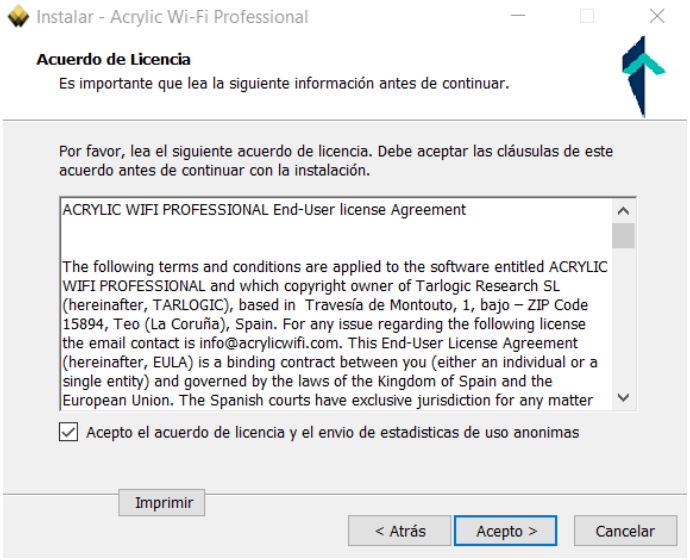


b) Descarga e instala software que monitorice redes inalámbricas y realiza filtrados de red para monitorizar sólo el tráfico deseado.

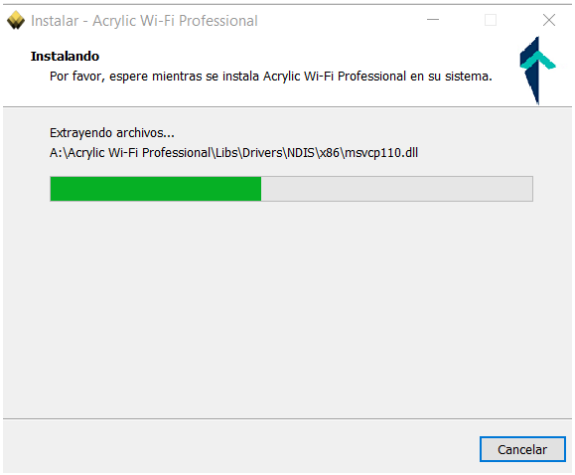
En este caso usare Acrylic WiFi. Probare su versión profesional de prueba. Lo descargaremos de su página oficial. [Link.]



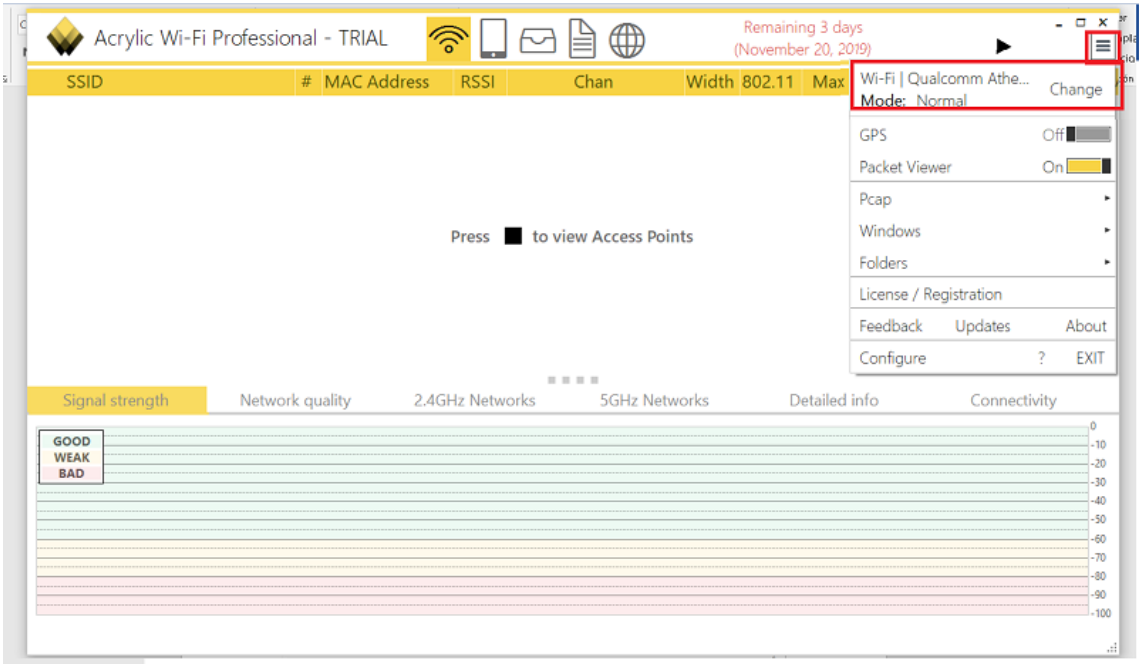
Lo descargamos e instalamos. Aceptamos términos y condiciones



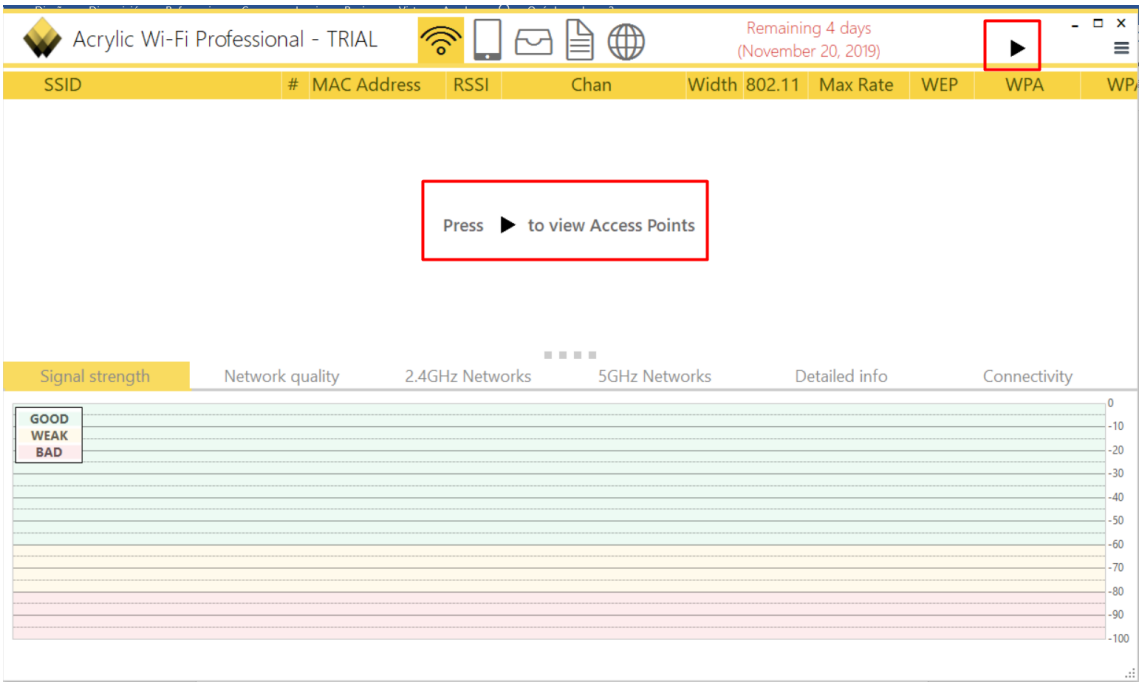
Esperamos a que se instale.



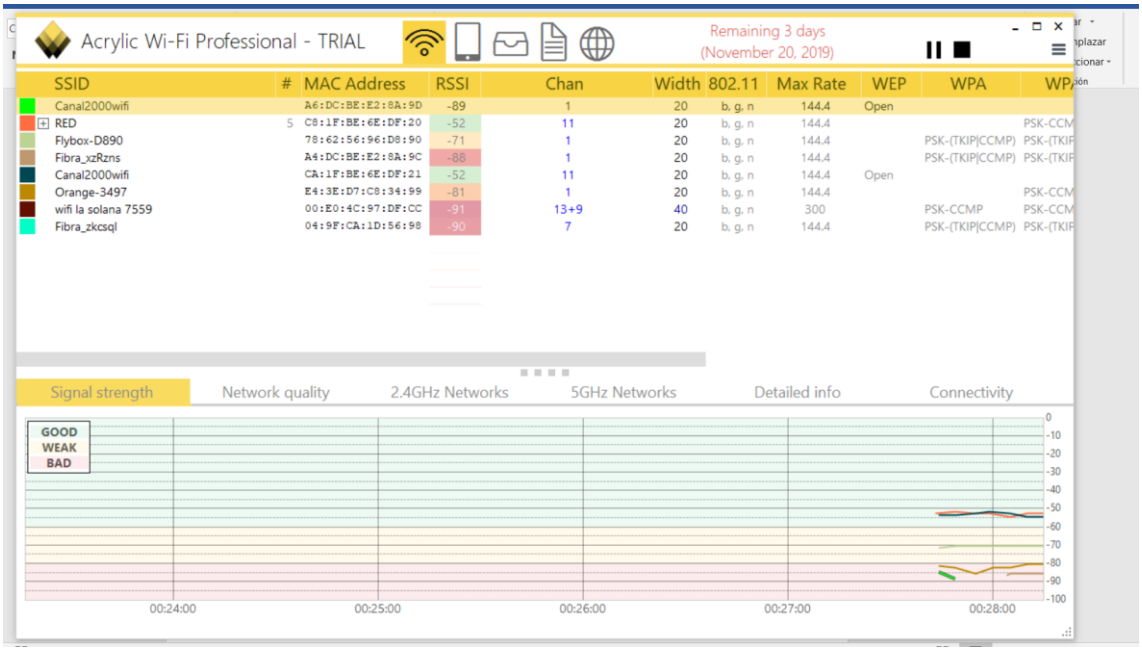
Una vez instalado lo abrimos y en el menú escogemos nuestra tarjeta de red.



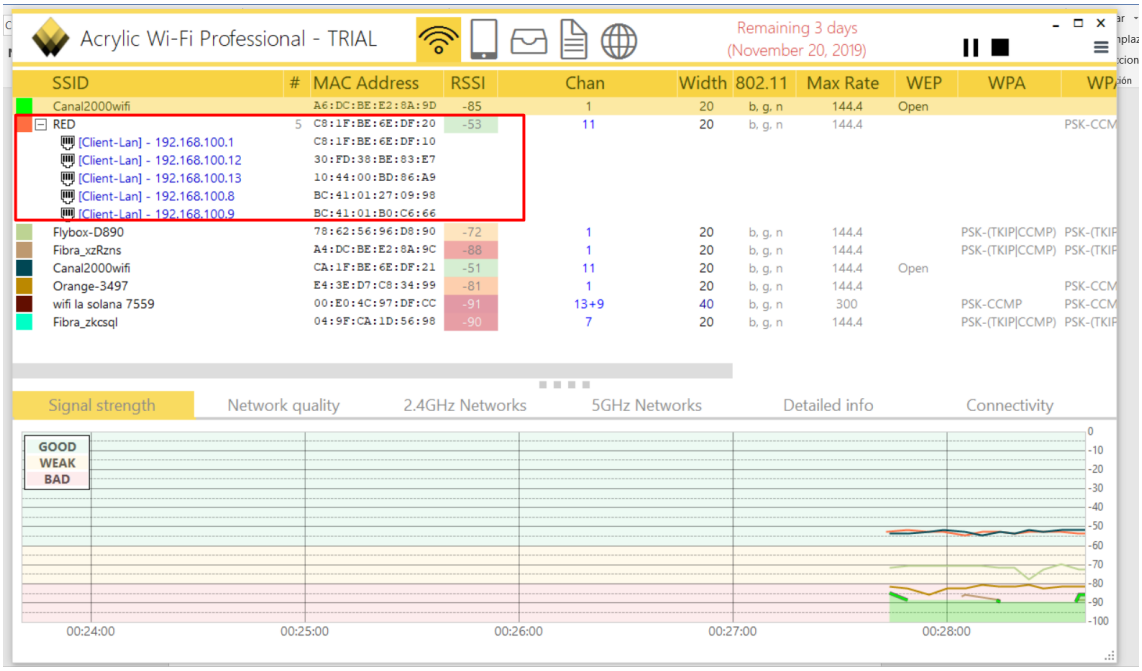
Pulsamos el menú de *Play* para analizar las redes que hay.



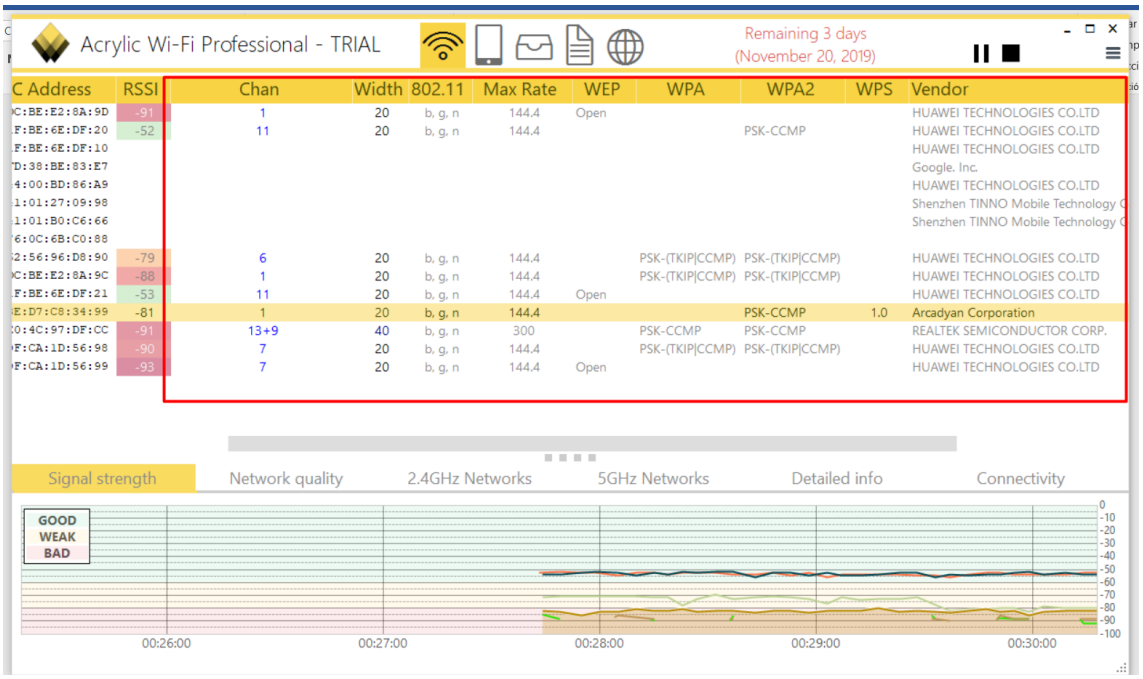
Vemos como capturo todas las redes disponibles en el alcance.



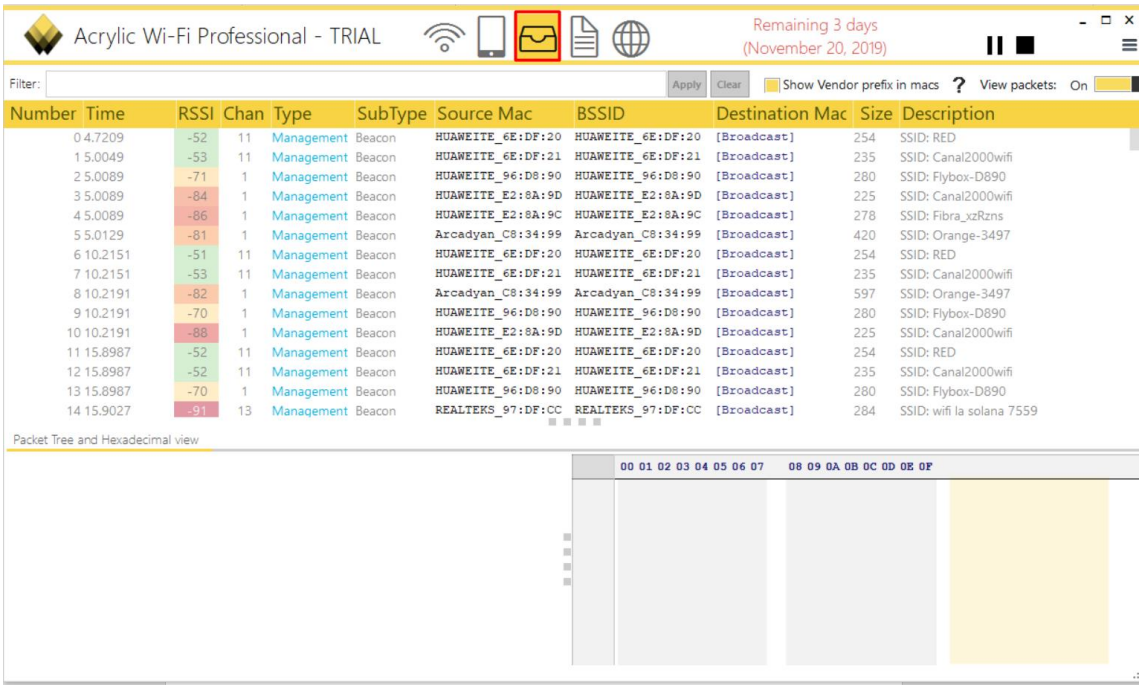
Si pulsamos en el + que esta en nuestra red veremos los dispositivos conectados.



Podemos ver toda la información sobre las redes (Vendedor, seguridad, protocolo, canal que usan…).



Podemos analizar paquetes con el programa con la propia herramienta que incorpora. También podemos filtrar estos pulsando en *Filter.*

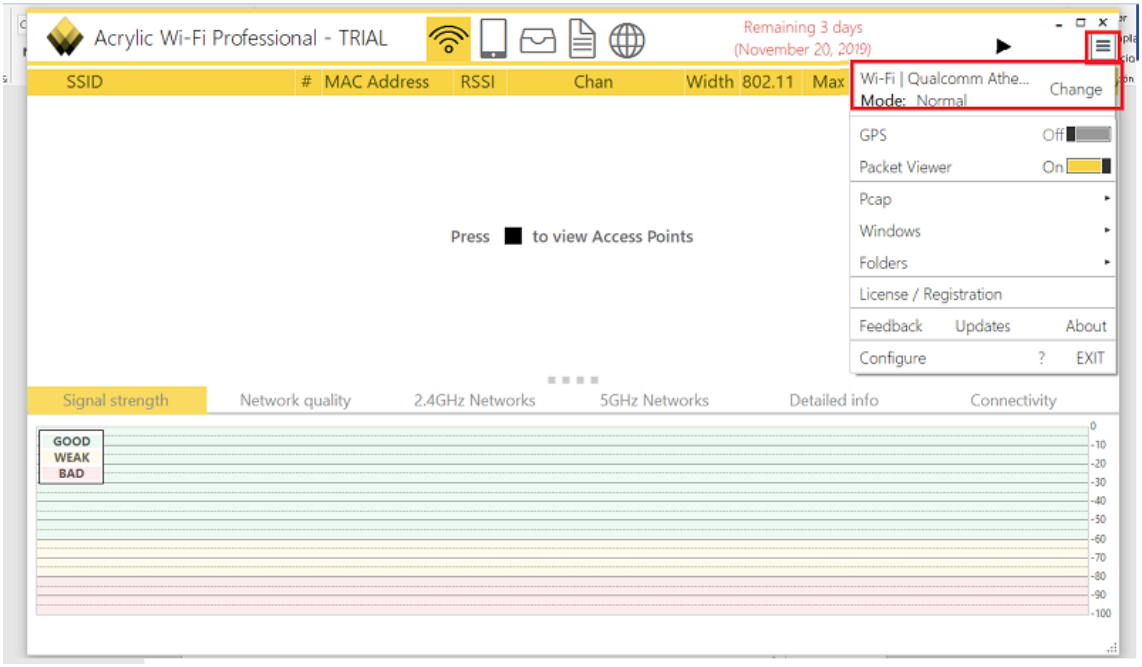


El programa permite capturar paquetes en modo monitor o promiscuo.

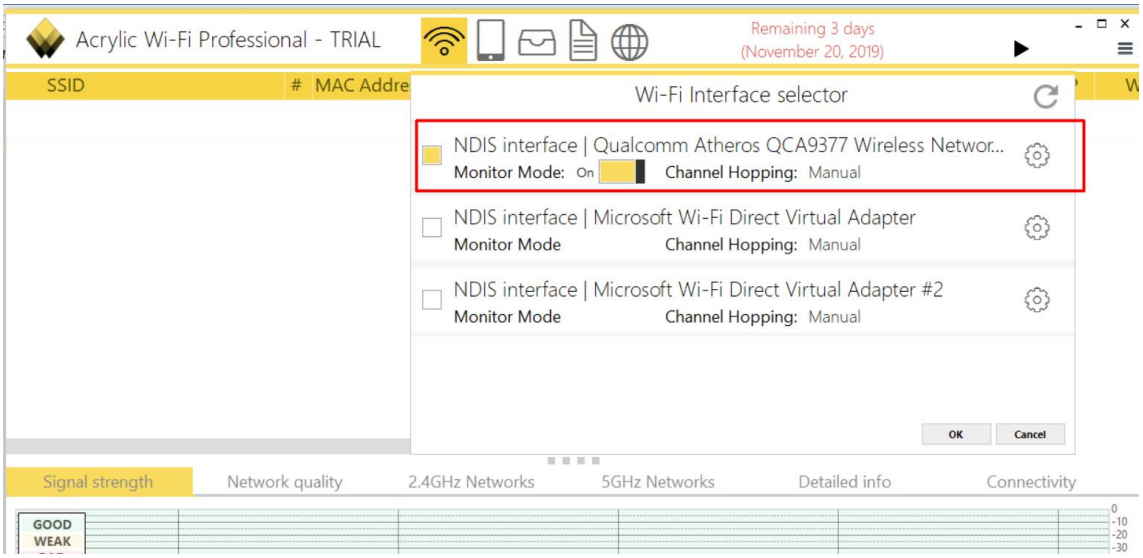
En mi caso me es imposible realizar una captura en modo monitor con el programa a mi red ya que mi tarjeta de red no soporta dicha función.

Cuando se pone la tarjeta en este modo se suelen hablar de ponerla en modo monitorización o monitor. Este modo permite la captura de los paquetes de una red Wireless (que van por el aire en ondas de radio) sin estar asociados a la red.

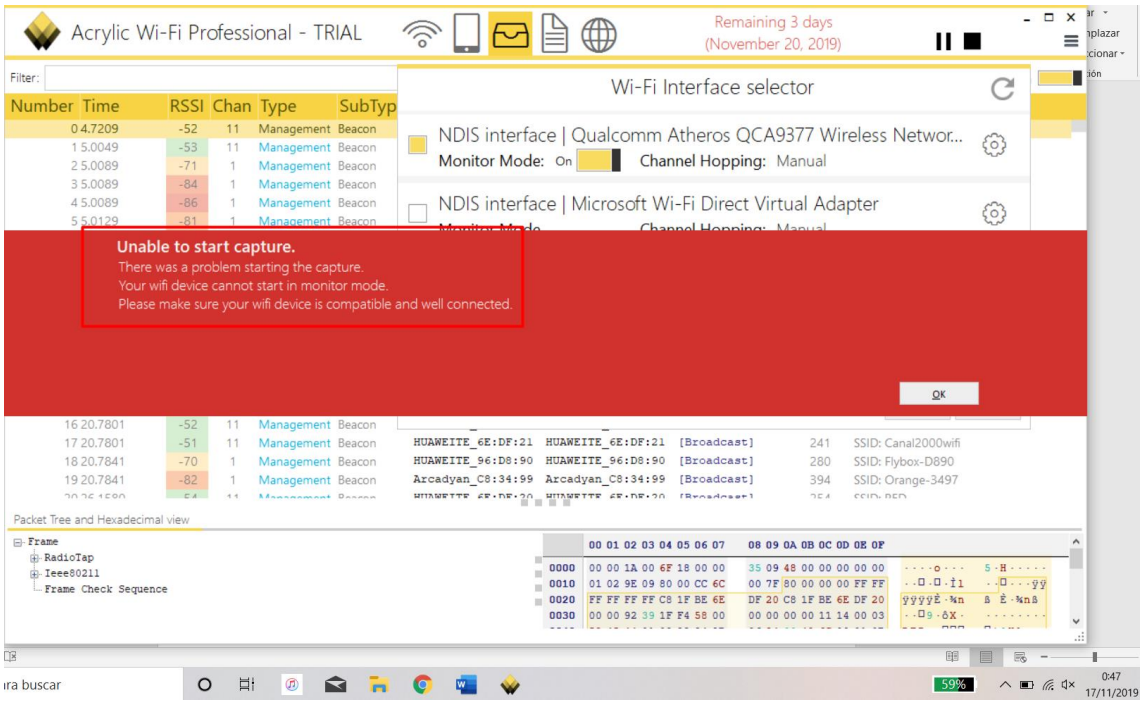
Intente instalar el driver que te ofrece el programa para estos casos, pero aun así no funcionó. Para realizar esto vamos a menú otra vez y en tarjeta de red escogemos el driver NDIS para instalar.



Activaremos la función que tiene ahora la tarjeta de red de *Monitor Mode.*



Pero cuando le damos al botón de *Play* este no iniciará ya que nuestra tarjeta de red del portátil no es compatible con el modo monitor. Nos mandará un mensaje de error.



Me quede con las ganas de realizar escuchas en modo monitor, tendré que comprarme una tarjeta de red externa que admita dicha función.