Análisis del tráfico de red del servicio DHCP

Wireshark

Juan Carlos Navidad García

Servicios en Red

Índice

¿Qué es Wireshark?:

Wireshark, antes conocido como **Ethereal**, es un analizador de protocolos utilizado para **realizar análisis y solucionar problemas en redes de comunicaciones**, **para desarrollo de software y protocolos, y como una herramienta didáctica**. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

Wireshark es una de las mejores herramientas para analizar el **tráfico en redes** informáticas para lo que incluye algunas de las mejores herramientas de código abierto disponible para plataformas **Windows** y **Unix**.

¿Cómo instalar Wireshark en Linux?:

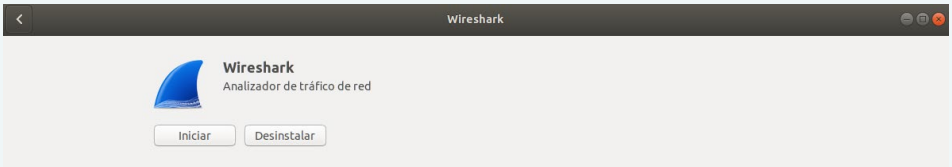
Como tenemos instalados todos los servidores en Ubuntu, para analizar el tráfico de a red, vamos a tener que instalar Wireshark en Ubuntu.

Instalar **Wireshark** en **Linux** es muy simple:

1. Debemos actualizar los repositorios de **Ubuntu** con **sudo apt-get update**
2. Una vez actualizados los repositorios, instalaremos Wireshark con sudo **apt-get install wireshark**

```
jnav@jnav2:~$ sudo apt-get install wireshark
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
```

3. En el caso de que no queramos hacerlo mediante comandos, **podemos instalarlo desde la tienda de aplicaciones de Ubuntu**



¿Qué es lo que vamos a comprobar con Wireshark?:

La función principal de **Wireshark** es **capturar el tráfico de la red**. Por eso, vamos a utilizar **Wireshark** para comprobar la **comunicación entre el cliente y el servidor DHCP**, obteniendo el conjunto completo de mensajes entre ellos para la configuración **DHCP del cliente**.

Debemos de Filtrar el tráfico obtenido para el protocolo **DHCP (BOOTP) y analizarlo**.

En la comunicación entre el **cliente** y el **servidor DHCP**, se intercambian los siguientes mensajes:

- **DHCP DISCOVER:** lo envía el cliente, es una trama de difusión, para detectar los servidores DHCP disponibles en la intranet.

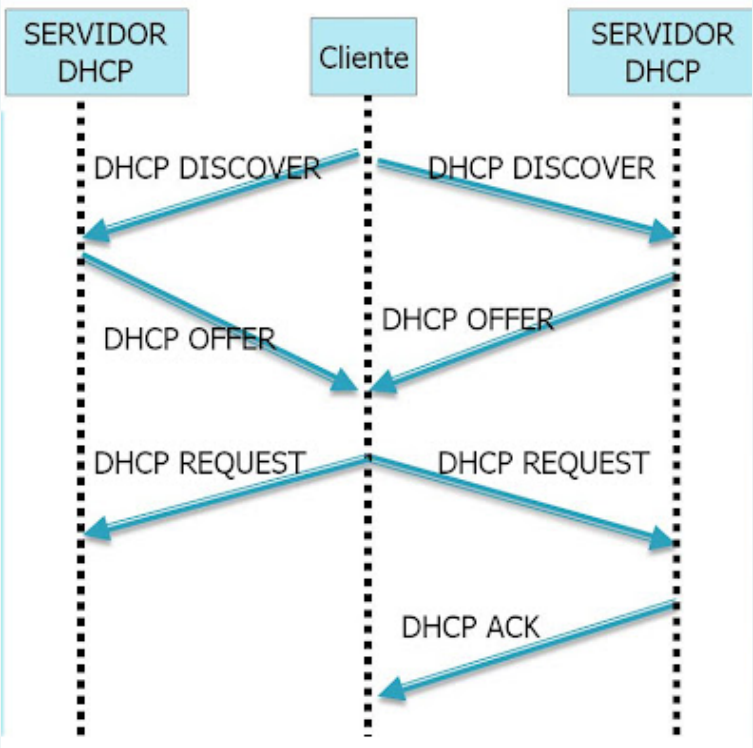
- **DHCP OFFER:** lo envía el servidor en respuesta al DHCP DISCOVER con la oferta de los parámetros de configuración.

- **DHCP REQUEST:** tipo de mensaje encapsulado en una trama de difusión, de un cliente a un servidor para:

    - Aceptar la oferta de un servidor determinado y, por tanto, rechazar el resto de ofertas recibidas.
    - Confirmar la exactitud de la información asignada antes del reinicio de la tarjeta de red configurada.
    - Extender el contrato de una dirección IP determinada.

- **DHCP ACK:** lo envía el servidor al cliente con los parámetros de configuración, incluida la dirección de red comprometida.

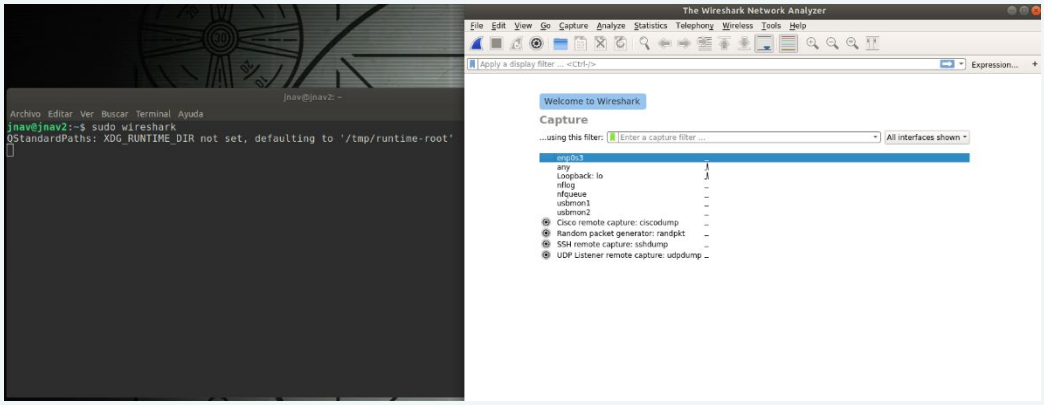
Siguen el siguiente orden:



¿Cómo iniciar y analizar el tráfico en Wireshark?:

Necesitamos iniciar **Wireshark** como **administrador** para poder **analizar el tráfico** de la red sin tener ningún problema de **permisos**.

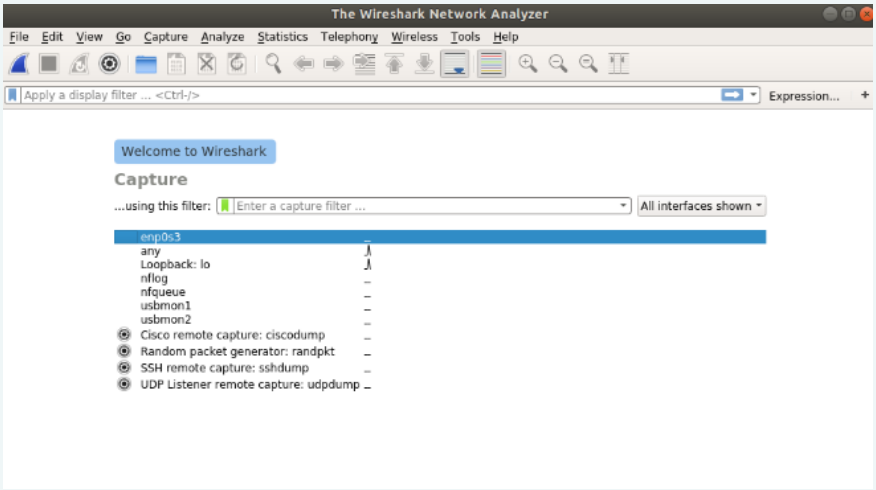
Para iniciar Wireshark como administrador, abriremos una terminal y pondremos **"sudo wireshark".**



Podemos iniciarlo también desde la **interfaz gráfica**, pero se nos iniciará como usuario normal y no como **root**. Por lo tanto, no tendrá los permisos necesarios para poder capturar la red.

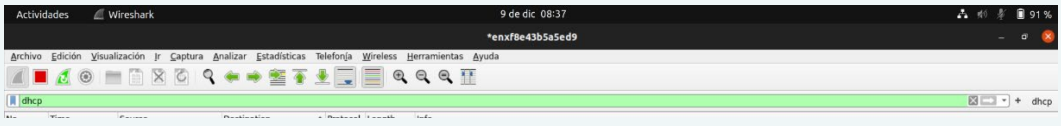
Ahora veremos como comprobar los **paquetes DHCP** desde **Wireshark**:

Una vez iniciado **Wireshark** como **administrador**, nos saldrá la siguiente pantalla de **selección de tarjeta de red**:

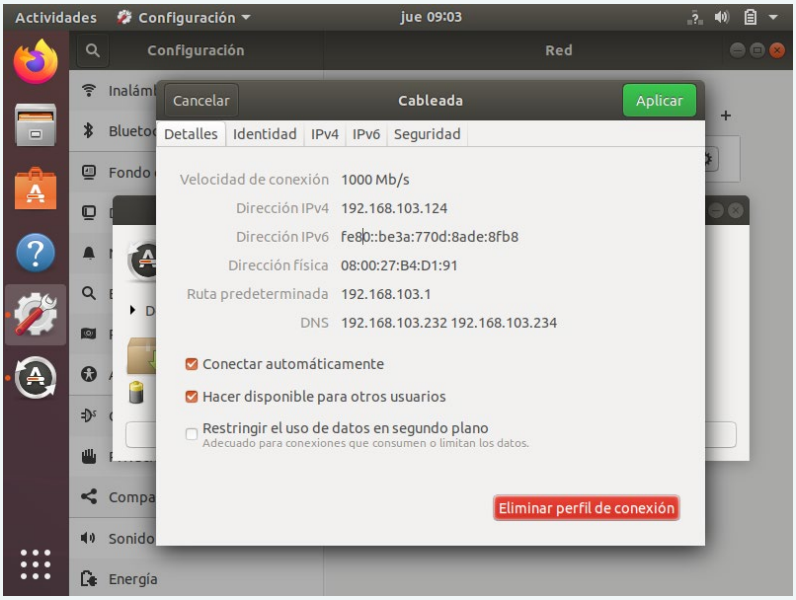


En mi caso, la interfaz de red configurada para el **servidor DHCP**, es la **enp0s3**, haremos doble clic en la tarjeta de red.

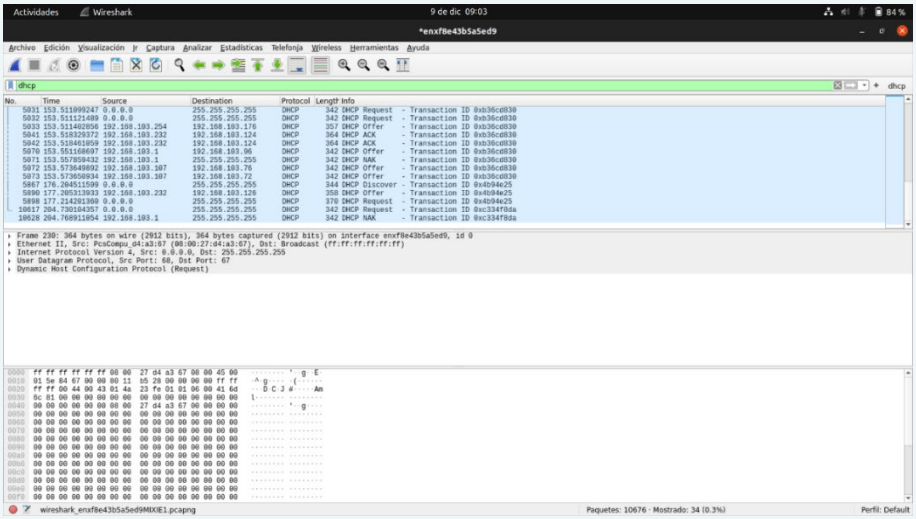
Una vez sobre la **tarjeta de red**, empezará a capturar todo el tráfico, pero nosotros solo queremos los **paquetes DHCP**. Por lo tanto, le aplicaremos el **filtro de búsqueda** "**dhcp**" en la barra superior de búsqueda:



Antes de nada, he conectado un cliente al servidor DHCP con la IP **192.168.103.124**:

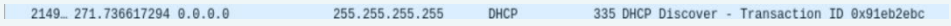


A partir de ahí, nos aparecerán todos los **paquetes DHCP** que están trabajando con nuestra **tarjeta de red**, tendremos que fijarnos en tener el **servidor DHCP** en funcionamiento junto a algunos **clientes** conectados. Si todo funciona bien nos tendrían que salir un conjunto de paquetes:

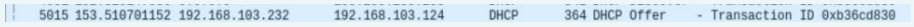


Como los **paquetes** no están en orden por el filtro de búsqueda, el orden de comunicación sería el siguiente:

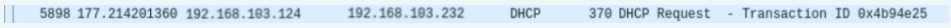
- Primero el cliente debe de hacer un **DHCP Discover** para identificar los servidores DHCP que hay en la red:



- Después de que el cliente haga un **Discover**, el servidor DHCP le contesta con un **DHCP Offer**, ofreciéndole algunos parámetros de configuración de la red junto a la dirección IP asignada:



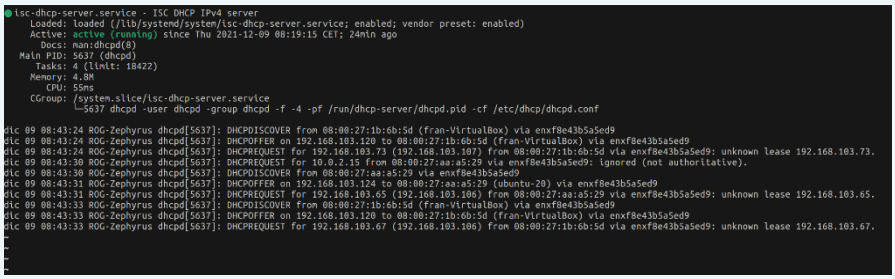
- Para saber si el cliente ha recibido el **Offer**, tendremos que analizar el tráfico con Wireshark desde el cliente y observar si ha enviado algún **DHCP Request**:



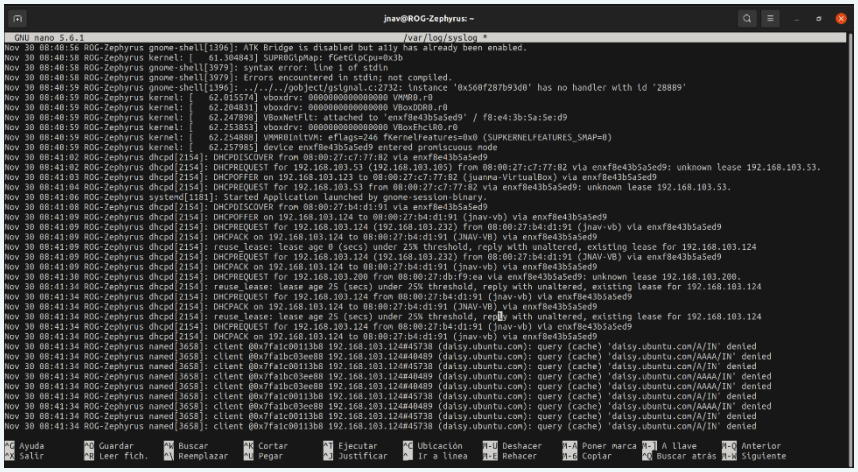
- Una vez que el cliente haya enviado un **Request** solicitando los parámetros de configuración de la red, el servidor le debe contestar con un **ACK** de confirmación:

Para confirmar todo lo que nos ha devuelto Wireshark, podemos hacer un "**sudo service isc-dhcp-server status**" o mirar el **log** del sistema */var/log/syslog*.

- Con **sudo service isc-dhcp-server status**:



- Revisando el **log del sistema**:
  Al abrir el archivo **syslog con nano**, tendremos muchisimos logs, por lo tanto, tendremos que buscar paquete por paquete púlsando **ctrl+w**:



Buscaremos **DHCPDISCOVER, DHCPOFFER, DHCPREQUEST** y **DHCPACK**:

DHCP Discover:

```
ROG-Zephyrus dhcpd[2154]: DHCPDISCOVER from 08:00:27:d7:96:bd via enxf8e43b5a5ed9
```

DHCP Offer:

```
ROG-Zephyrus dhcpd[25609]: DHCPOFFER on 192.168.103.124 to 24:be:05:21:1b:30 (JNAV-VB) via enxf8e43b5a5ed9
```

DHCP Request:

```
ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.124 (192.168.103.232) from 08:00:27:b4:d1:91 (JNAV-VB) via enxf8e43b5a5ed9
```

DHCP Ack:

```
ROG-Zephyrus dhcpd[2154]: DHCPACK on 192.168.103.124 to 08:00:27:b4:d1:91 (JNAV-VB) via enxf8e43b5a5ed9
```