

Análisis del tráfico de red del servicio DHCP



Wireshark

Juan Carlos Navidad García
Servicios en Red

Índice

¿Qué es Wireshark?:	3
¿Cómo instalar Wireshark en Linux?:	3
¿Qué es lo que vamos a comprobar con Wireshark?:.....	4
¿Cómo iniciar y analizar el tráfico en Wireshark?:.....	6



¿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?:

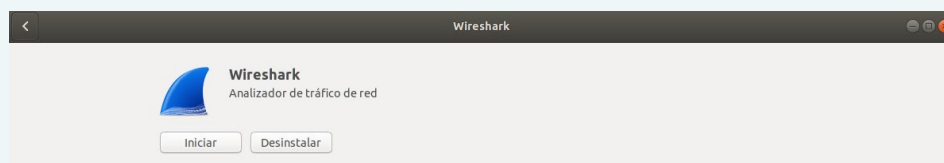
Como tenemos instalados todos los servidores en Ubuntu, para analizar el tráfico de a red, vamos a tener que instalar Wireshark en Ubuntu.

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?:

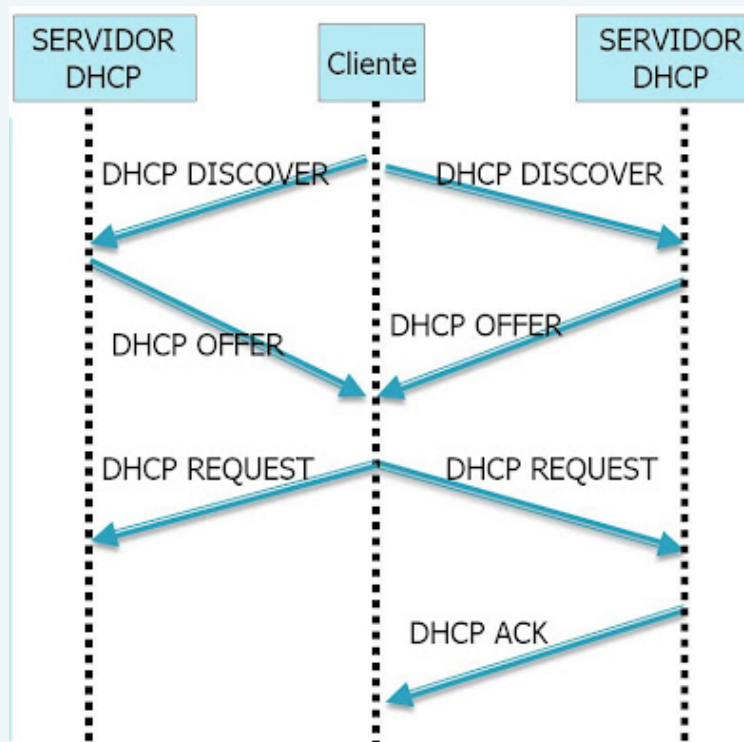
La función principal de **Wireshark** es **capturar el tráfico de la red**. Por eso, vamos a utilizar **Wireshark** para comprobar la **comunicación entre el cliente y el servidor DHCP**, obteniendo el conjunto completo de mensajes entre ellos para la configuración **DHCP del cliente**.

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.

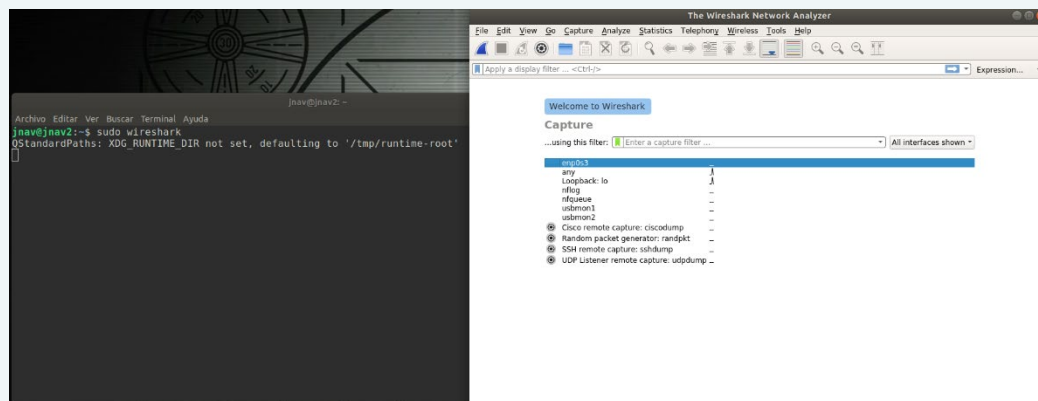
Siguen el siguiente orden:



¿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**.

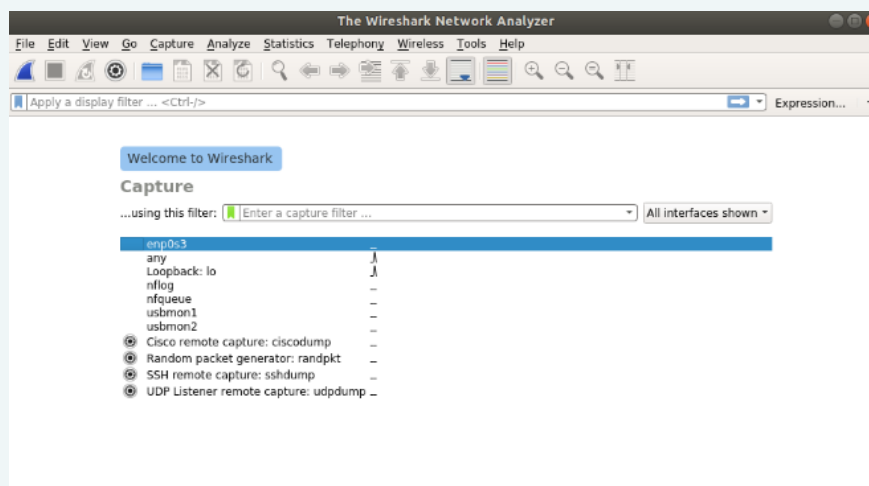
Para iniciar Wireshark como administrador, abriremos una terminal y pondremos **“sudo wireshark”**.



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.

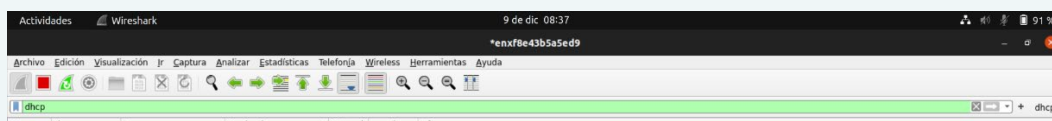
Ahora veremos como comprobar los **paquetes DHCP** desde **Wireshark**:

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

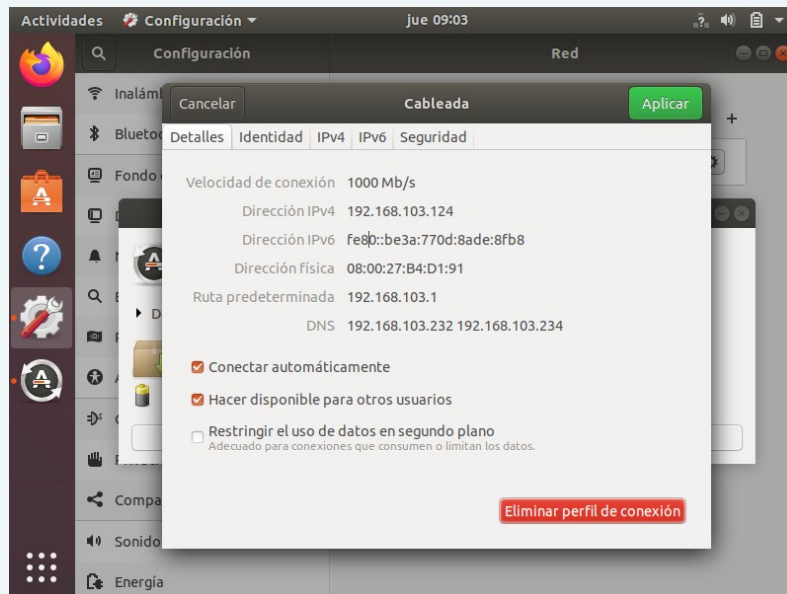


En mi caso, la interfaz de red configurada para el **servidor DHCP**, es la **enp0s3**, haremos doble clic en la tarjeta de red.

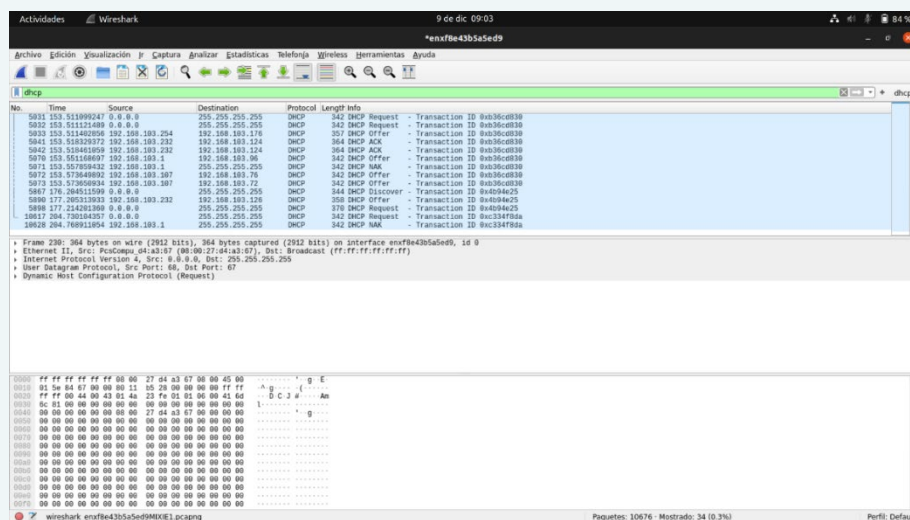
Una vez sobre la **tarjeta de red**, empezará a capturar todo el tráfico, pero nosotros solo queremos los **paquetes DHCP**. Por lo tanto, le aplicaremos el **filtro de búsqueda "dhcp"** en la barra superior de búsqueda:



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 tendrán 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:

```
2149 271.736617294 0.0.0.0 255.255.255.255 DHCP 335 DHCP Discover - Transaction ID 0x91eb2ebc
```

- 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:

```
5015 153.510701152 192.168.103.232 192.168.103.124 DHCP 364 DHCP Offer - Transaction ID 0xb36cd830
```

- 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**:

```
5898 177.214201360 192.168.103.124 192.168.103.232 DHCP 370 DHCP Request - Transaction ID 0x4b94e25
```

- 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:

```
5041 153.518329372 192.168.103.232 192.168.103.124 DHCP 364 DHCP ACK - Transaction ID 0xb36cd830
```

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**:

```
isc-dhcp-server.service - ISC DHCP IPv4 server
Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2021-12-09 08:19:15 CET; 24mn ago
Docs: man:dhcpd(8)
Main PID: 5637 (dhcpd)
Tasks: 4 (limit: 18422)
Memory: 4.8M
CPU: 55ms
CGroup: /system.slice/isc-dhcp-server.service
└─5637 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

dic 09 08:43:24 ROG-Zephyrus dhcpd[5637]: DHCPDISCOVER from 08:00:27:1b:6b:5d (fran-VirtualBox) via enx8e43b5a5ed9
dic 09 08:43:24 ROG-Zephyrus dhcpd[5637]: DHCPOFFER on 192.168.103.120 to 08:00:27:1b:6b:5d (fran-VirtualBox) via enx8e43b5a5ed9
dic 09 08:43:24 ROG-Zephyrus dhcpd[5637]: DHCPREQUEST for 192.168.103.73 (192.168.103.107) from 08:00:27:1b:6b:5d via enx8e43b5a5ed9: unknown lease 192.168.103.73.
dic 09 08:43:30 ROG-Zephyrus dhcpd[5637]: DHCPREQUEST for 10.0.2.15 from 08:00:27:aa:a5:29 via enx8e43b5a5ed9: ignored (not authoritative).
dic 09 08:43:30 ROG-Zephyrus dhcpd[5637]: DHCPDISCOVER from 08:00:27:aa:a5:29 via enx8e43b5a5ed9
dic 09 08:43:31 ROG-Zephyrus dhcpd[5637]: DHCPOFFER on 192.168.103.124 to 08:00:27:aa:a5:29 (ubuntu-20) via enx8e43b5a5ed9
dic 09 08:43:31 ROG-Zephyrus dhcpd[5637]: DHCPREQUEST for 192.168.103.65 (192.168.103.106) from 08:00:27:aa:a5:29 via enx8e43b5a5ed9: unknown lease 192.168.103.65.
dic 09 08:43:33 ROG-Zephyrus dhcpd[5637]: DHCPDISCOVER from 08:00:27:1b:6b:5d (fran-VirtualBox) via enx8e43b5a5ed9
dic 09 08:43:33 ROG-Zephyrus dhcpd[5637]: DHCPOFFER on 192.168.103.120 to 08:00:27:1b:6b:5d (fran-VirtualBox) via enx8e43b5a5ed9
dic 09 08:43:33 ROG-Zephyrus dhcpd[5637]: DHCPREQUEST for 192.168.103.67 (192.168.103.106) from 08:00:27:1b:6b:5d via enx8e43b5a5ed9: unknown lease 192.168.103.67.
```

- Revisando el **log del sistema**:

Al abrir el archivo **syslog con nano**, tendremos muchísimos logs, por lo tanto, tendremos que buscar paquete por paquete pulsando **ctrl+w**:

```
GNU nano 5.6.1 /var/log/syslog
Nov 30 08:40:56 ROG-Zephyrus gnome-shell[1396]: ATK Bridge is disabled but a11y has already been enabled.
Nov 30 08:40:58 ROG-Zephyrus gnome-shell[1397]: syntax error: line 1 of stdin
Nov 30 08:40:58 ROG-Zephyrus gnome-shell[1397]: Errors encountered in stdin: not compiled.
Nov 30 08:40:59 ROG-Zephyrus kernel: [ 62.915574] vboxdrv: 0000000000000000 VMMR0.r0
Nov 30 08:40:59 ROG-Zephyrus kernel: [ 62.260831] vboxdrv: 0000000000000000 VBOXDR0.r0
Nov 30 08:40:59 ROG-Zephyrus kernel: [ 62.247898] VBoxNetFlt: attached to 'enx8e43b5a5ed9' / f8:e4:3b:5a:5e:d9
Nov 30 08:40:59 ROG-Zephyrus kernel: [ 62.253853] vboxdrv: 0000000000000000 VBoxEhC180.r0
Nov 30 08:40:59 ROG-Zephyrus kernel: [ 62.254880] VMXintInfo: e11aps:246 / KernelFeatures=dmf (SMPKERNFEATURES_SNAP=0)
Nov 30 08:40:59 ROG-Zephyrus kernel: [ 62.257985] device enx8e43b5a5ed9 entered promiscuous mode
Nov 30 08:41:02 ROG-Zephyrus dhcpd[2154]: DHCPDISCOVER from 08:00:27:c7:77:82 via enx8e43b5a5ed9
Nov 30 08:41:02 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.53 (192.168.103.105) from 08:00:27:c7:77:82 via enx8e43b5a5ed9: unknown lease 192.168.103.53.
Nov 30 08:41:03 ROG-Zephyrus dhcpd[2154]: DHCPOFFER on 192.168.103.123 to 08:00:27:c7:77:82 (Juanna-VirtualBox) via enx8e43b5a5ed9
Nov 30 08:41:04 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.53 from 08:00:27:c7:77:82 via enx8e43b5a5ed9: unknown lease 192.168.103.53.
Nov 30 08:41:06 ROG-Zephyrus systemd[1181]: Started Application launched by gnome-session-binary.
Nov 30 08:41:08 ROG-Zephyrus dhcpd[2154]: DHCPDISCOVER from 08:00:27:b4:d1:91 via enx8e43b5a5ed9
Nov 30 08:41:09 ROG-Zephyrus dhcpd[2154]: DHCPOFFER on 192.168.103.124 to 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:09 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.124 (192.168.103.232) from 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:09 ROG-Zephyrus dhcpd[2154]: DHCPACK on 192.168.103.124 to 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:09 ROG-Zephyrus dhcpd[2154]: reuse lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease for 192.168.103.124
Nov 30 08:41:09 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.124 (192.168.103.232) from 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:09 ROG-Zephyrus dhcpd[2154]: DHCPACK on 192.168.103.124 to 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:30 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.200 from 08:00:27:db:f9:ea via enx8e43b5a5ed9: unknown lease 192.168.103.200.
Nov 30 08:41:34 ROG-Zephyrus dhcpd[2154]: reuse lease: lease age 25 (secs) under 75% threshold, reply with unaltered, existing lease for 192.168.103.124
Nov 30 08:41:34 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.124 from 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:34 ROG-Zephyrus dhcpd[2154]: DHCPACK on 192.168.103.124 to 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:34 ROG-Zephyrus dhcpd[2154]: DHCPREQUEST for 192.168.103.124 from 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:34 ROG-Zephyrus dhcpd[2154]: DHCPACK on 192.168.103.124 to 08:00:27:b4:d1:91 (jnav-vb) via enx8e43b5a5ed9
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
Nov 30 08:41:34 ROG-Zephyrus named[3658]: client 08:7fa1bc0113b8 192.168.103.124448489 (daisy.ubuntu.com): query (cache) 'daisy.ubuntu.com/AAAA/IN' denied
```

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

DHCP Discover:

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

DHCP Offer:

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

DHCP Request:

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