Mateo Andres Rodriguez Pereira
Sebastian Campiño Figueroa
Juan Sebastian León Sánchez

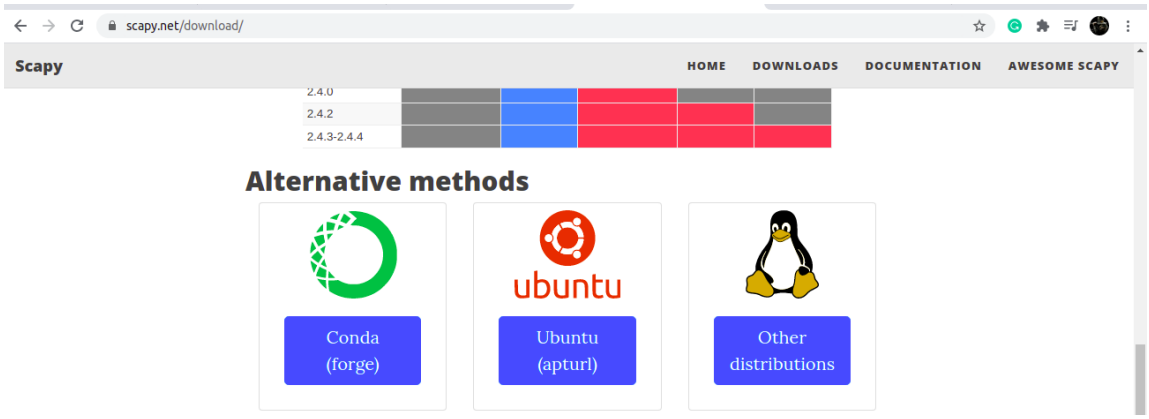
Manual de usuario
Punto 5. Captura de tramas

1. Requerimientos del programa:

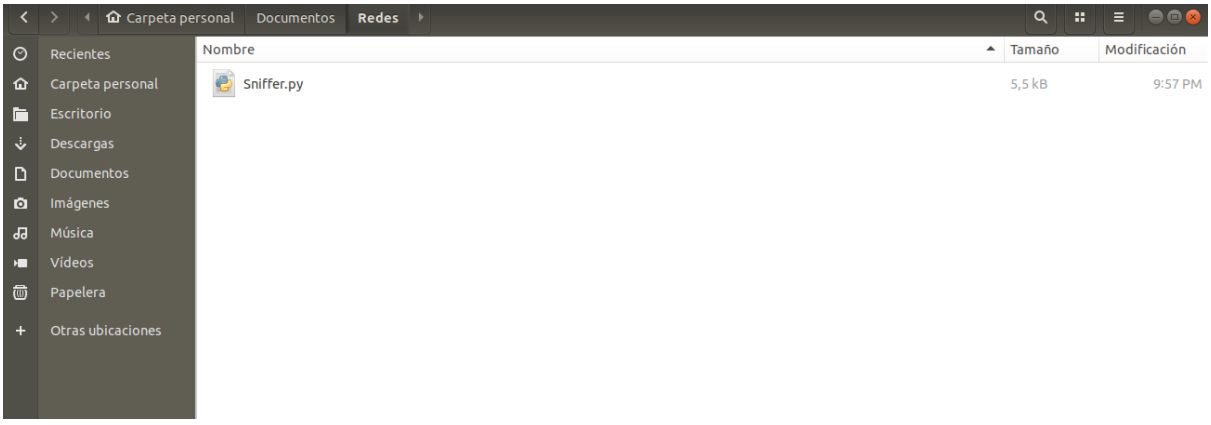
- Sistema operativo basado en Linux
- Scapy (herramienta de manipulación de paquetes para redes de computadoras)

2. Ejecución del programa:

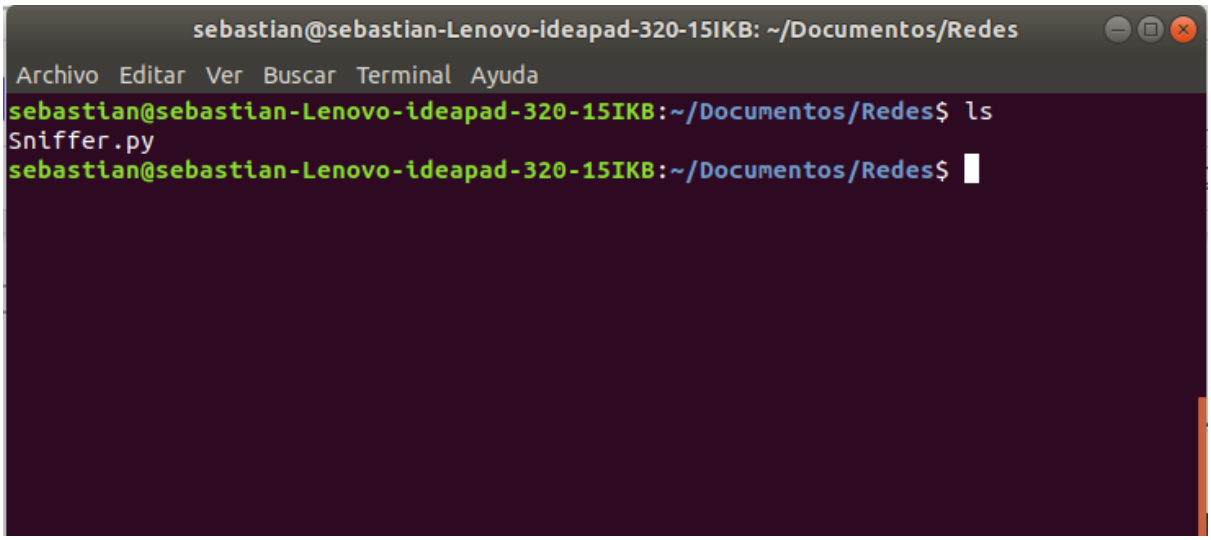
- Para ejecutar el programa es importante tener instalado el programa de manipulación de paquetes "Scapy"
  Instalaremos la versión que se acomode a nuestro sistema operativo basado en Linux



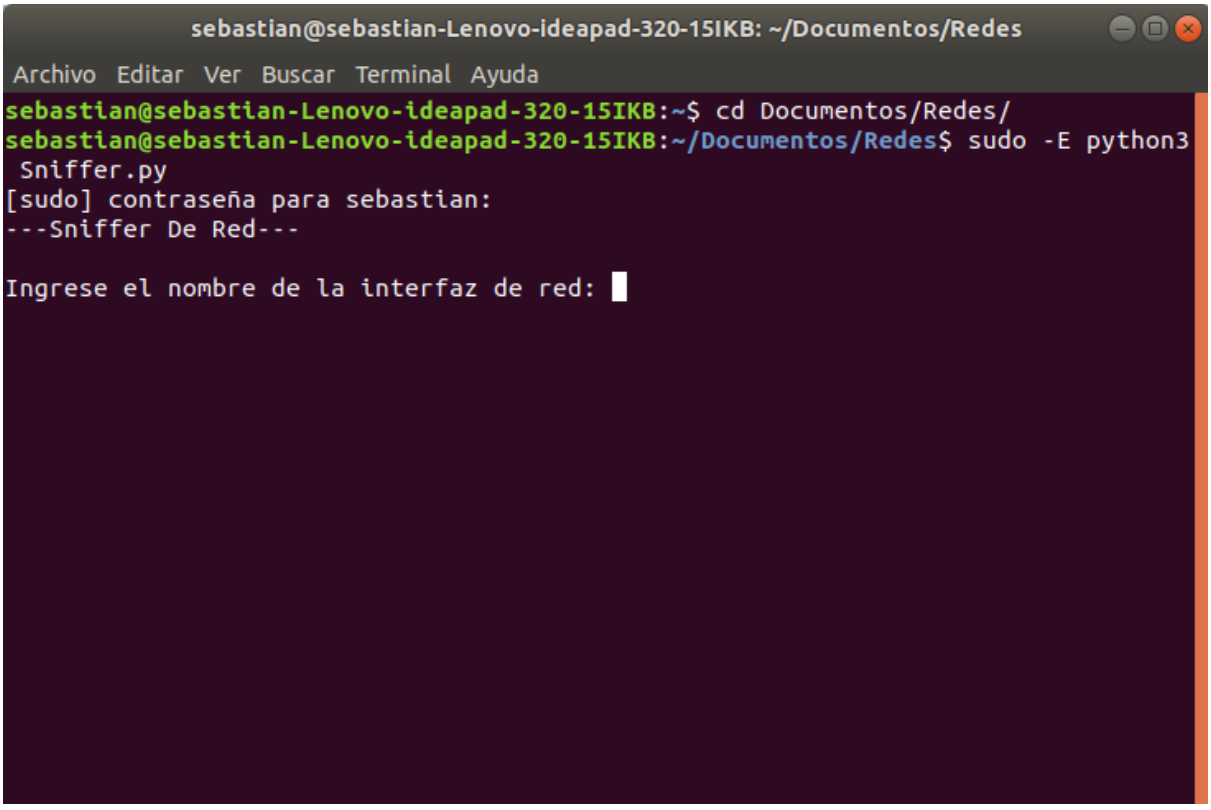
- A continuación descargamos el archivo "Sniffer.py" el cuál está anexo a este manual o directo desde el link de github



- Esta es una aplicación diseñada para la consola, entonces procedemos a entrar a la ubicación del archivo "Sniffer.py"



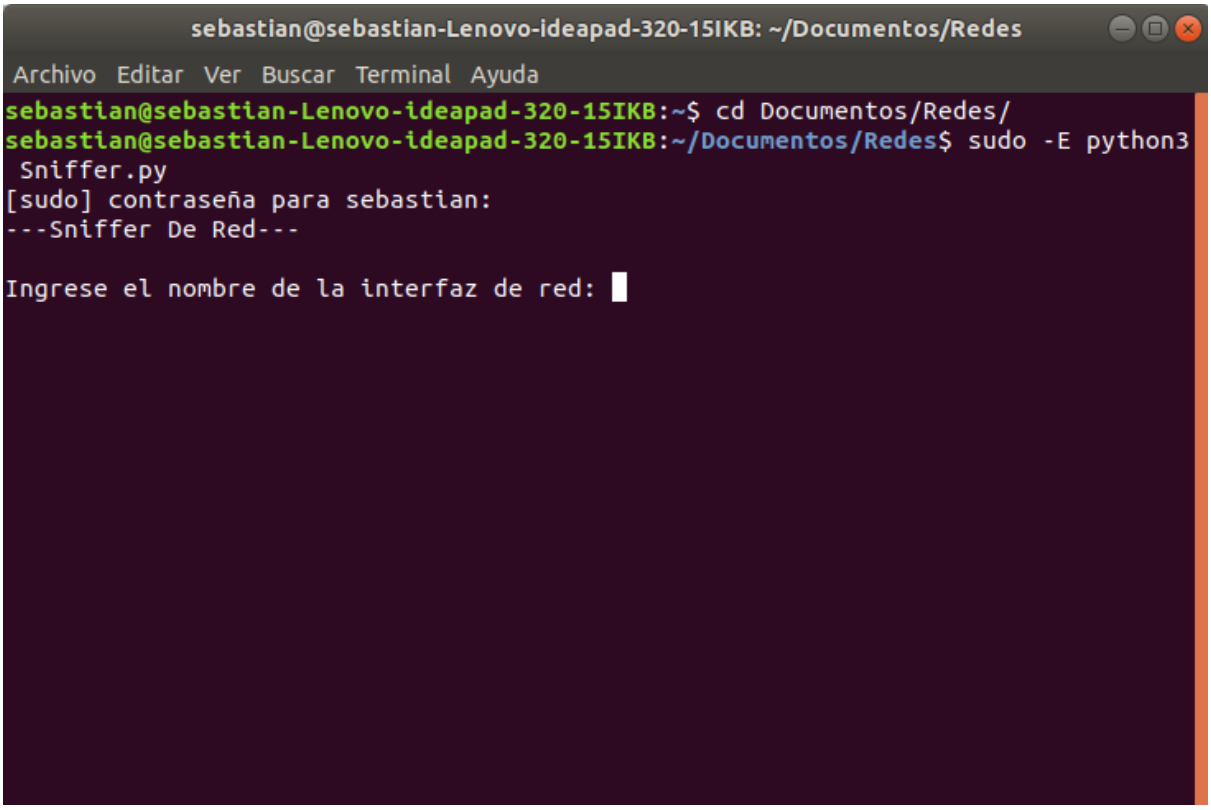
- A continuación usando el comando << sudo - E python3 Sniffer.py >> ejecutaremos el archivo



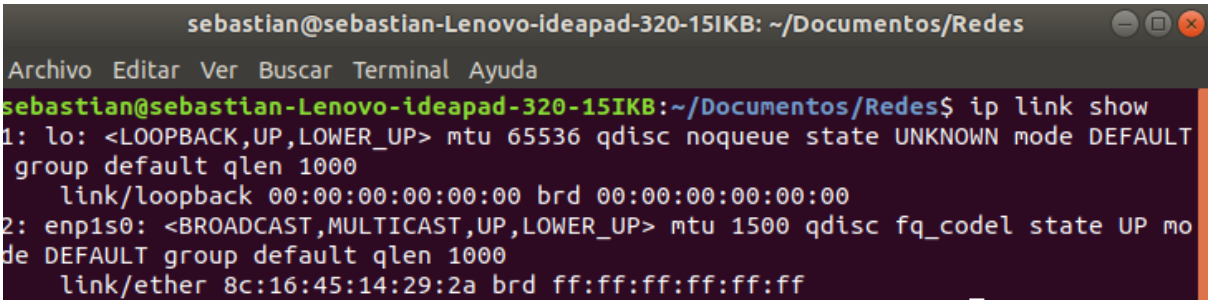
- Para este punto, el programa ya estará corriendo y listo para ser utilizado

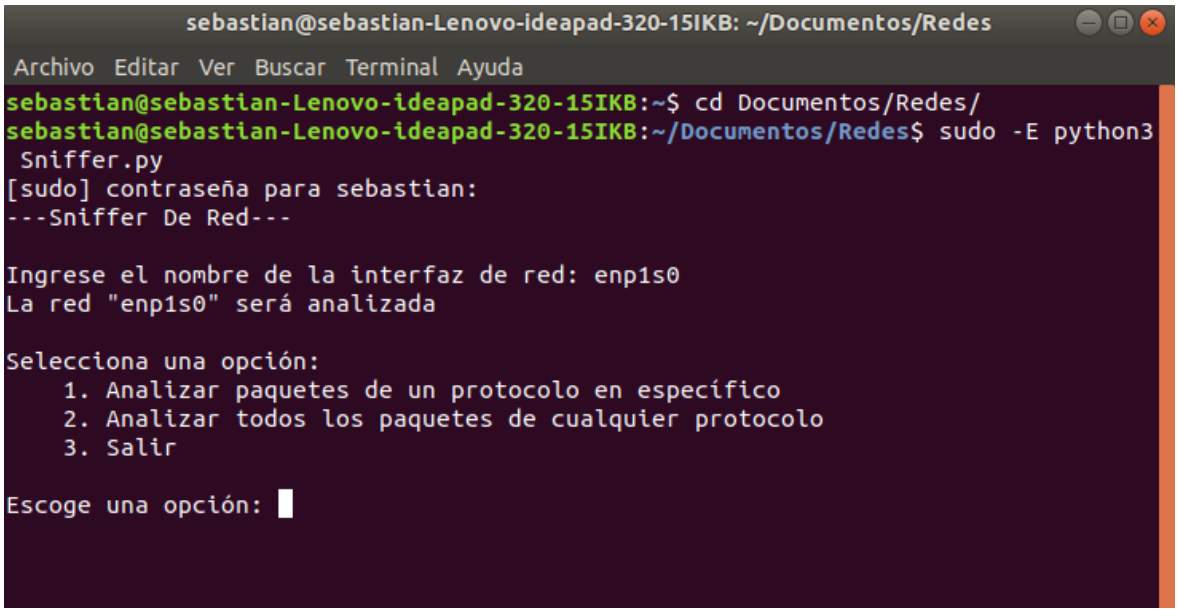
3. Funcionamiento:

- El programa mostrará instrucciones paso a paso para el correcto funcionamiento del programa



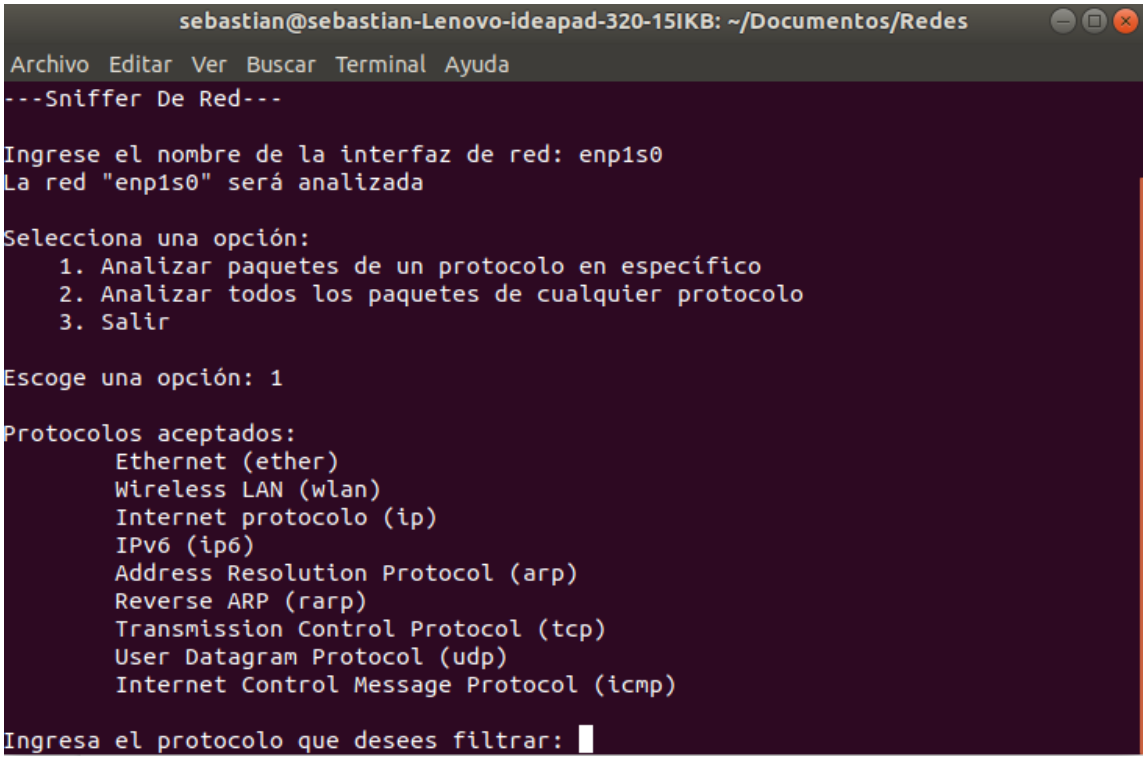
- Aquí tendremos que ingresar el nombre de la interfaz de red a analizar, para obtener el nombre se recomienda usar el comando
<< ip link show >>



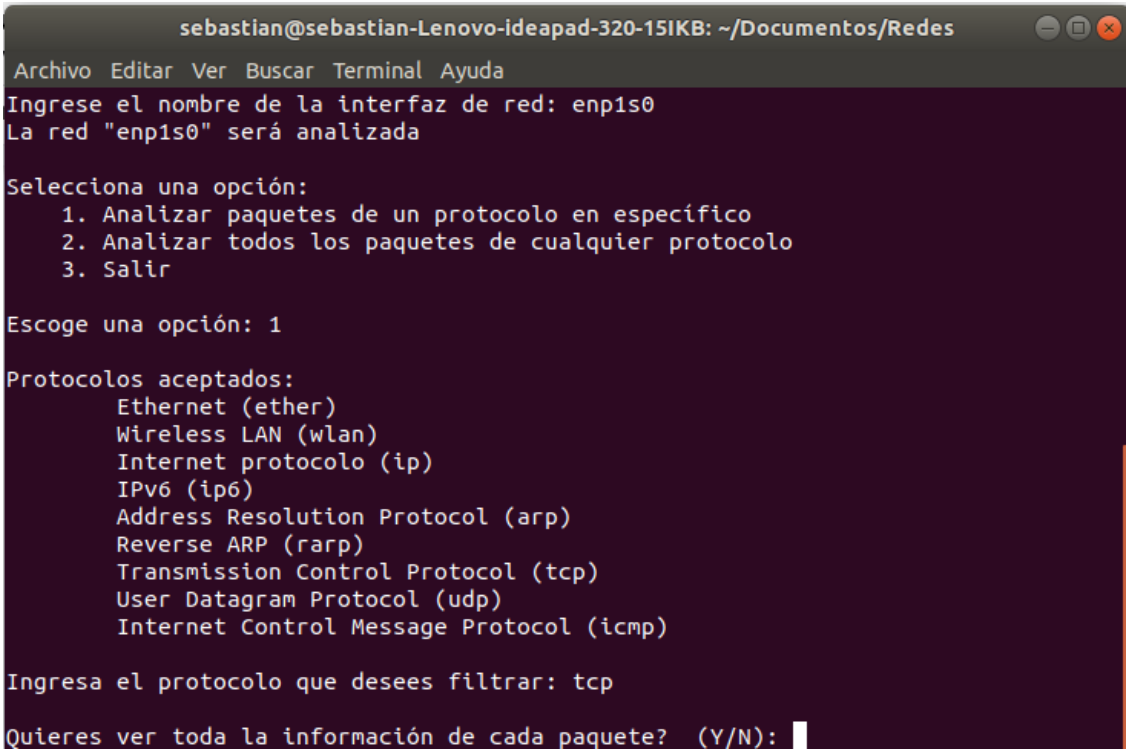


- En este punto podremos ver el menú principal donde podremos escoger si queremos salir de la aplicación o acceder a alguna de las funciones que tiene el programa

3.1 Opción 1 - Sniffing de paquetes por protocolo



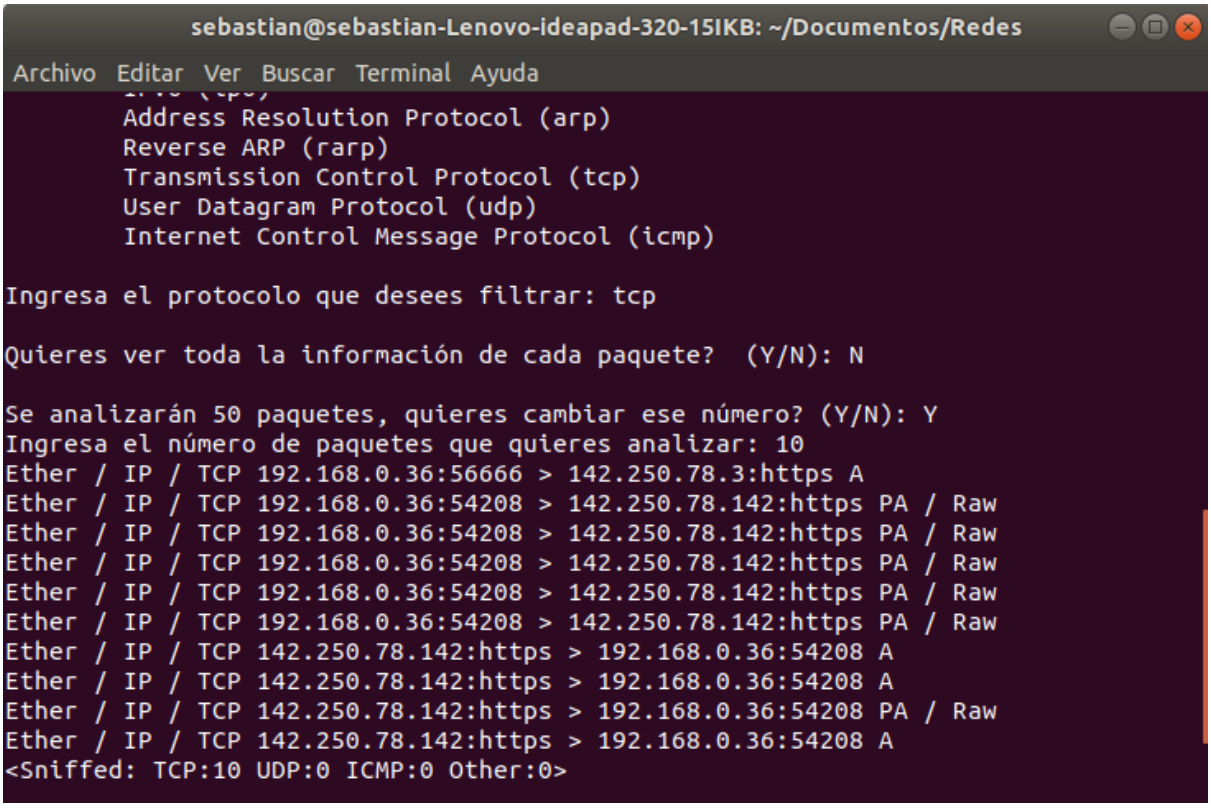
- Esta función nos permitirá filtrar los paquetes de un protocolo específico de nuestra elección. Lo primero que se verá al seleccionar esta opción es una lista de los protocolos disponibles para analizar; aquí tendremos que escribir el acrónimo del protocolo que queramos observar



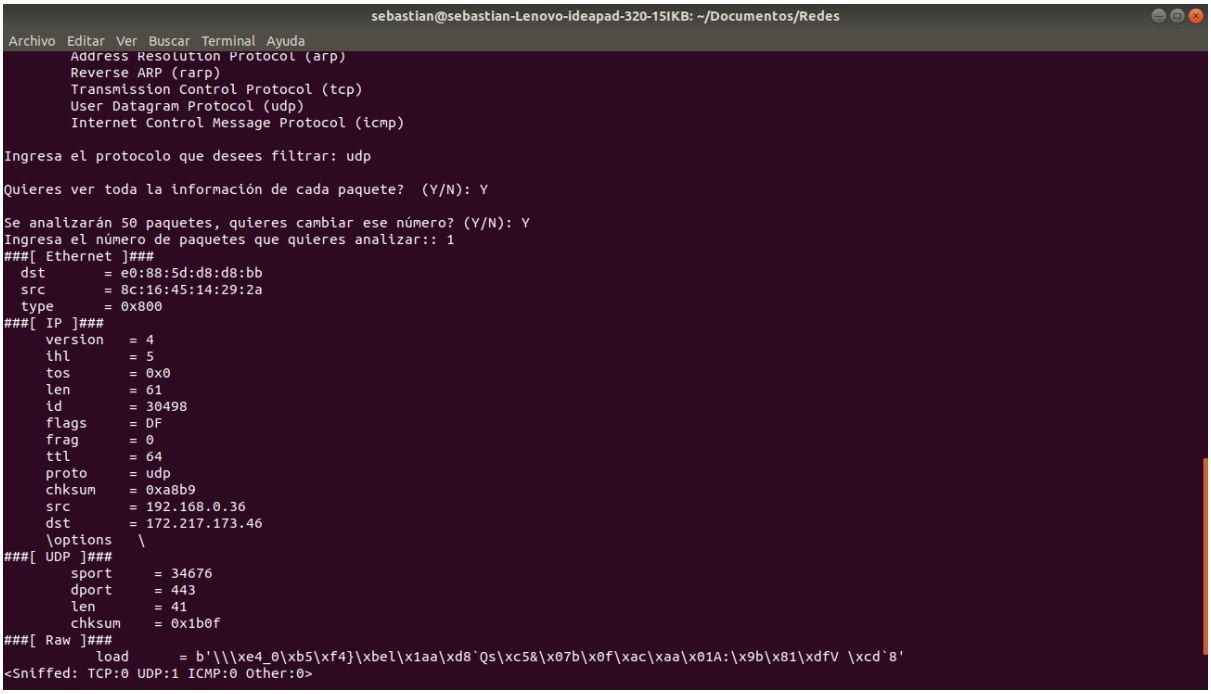
- En este punto nos dará a escoger si queremos una versión resumida o una versión completa de los detalles del paquete. A manera de ejemplo veremos primero la versión resumida de paquetes del protocolo **tcp**.

- Después (sin importar la opción que escojamos) se nos preguntará cuántos paquetes se quieren analizar. De manera predeterminada, se analizarán 50 paquetes pero se puede escoger una cantidad personalizada.

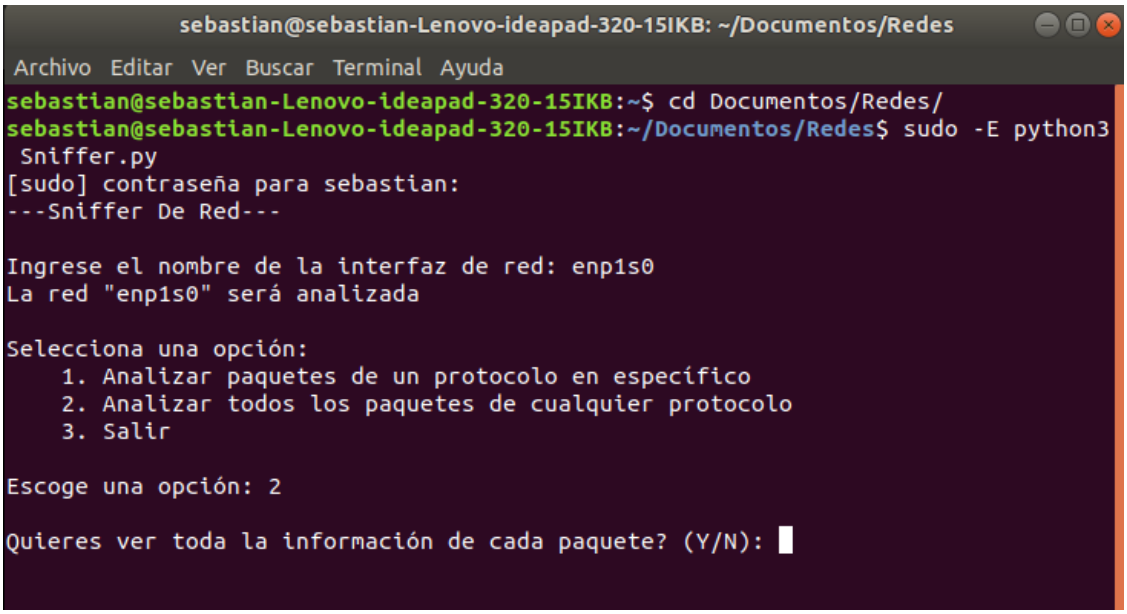
Luego se mostrará los resultados del análisis de paquetes:



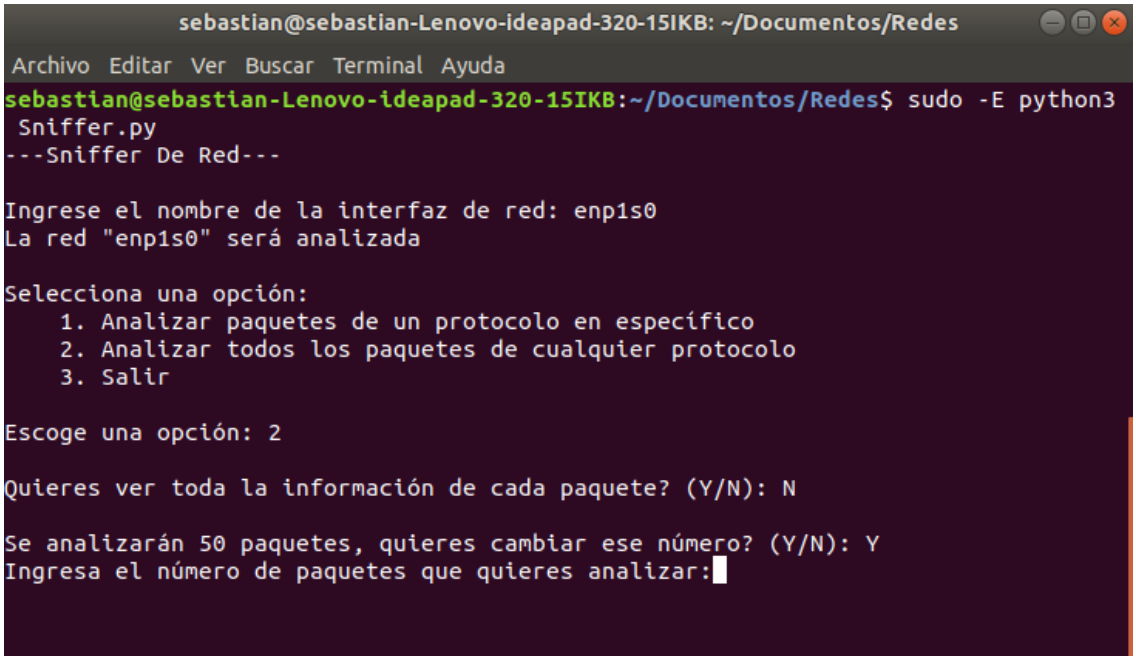
- Funciona de manera similar si queremos ver la versión completa de los detalles de los paquetes. Simplemente tendremos que escoger “Y” cuando nos pregunten si queremos ver la información completa de cada paquete.



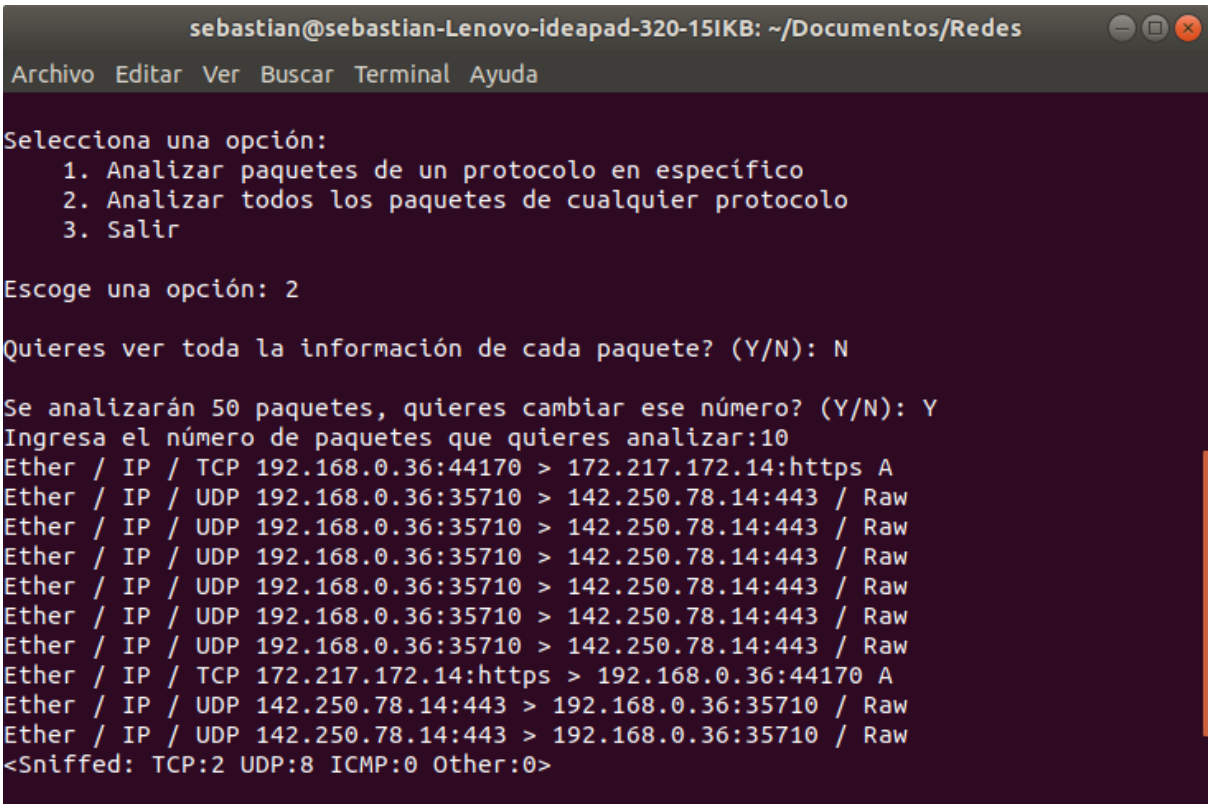
3.2 Opción 2 - Sniffing de todos los paquetes



- Esta función muestra todos los paquetes sin importar el protocolo.
  De manera similar a la función vista anteriormente, en este punto se nos dará a escoger si queremos una versión resumida o una versión completa de los detalles de los paquetes.



- Después (sin importar la opción que escojamos) se nos preguntará cuántos paquetes se quieren analizar. De manera predeterminada, se analizarán 50 paquetes pero se puede escoger una cantidad personalizada.
  Luego se mostrará los resultados del análisis de paquetes:



- Al igual que en la función anterior, si queremos ver la versión completa de los detalles de los paquetes. Simplemente tendremos que escoger “Y” cuando nos pregunten si queremos ver la información completa de cada paquete.