Challenge new hiring - Mercado Libre

Desarrollar una aplicación para análisis de tráfico con la responsabilidad de capturar paquetes desde
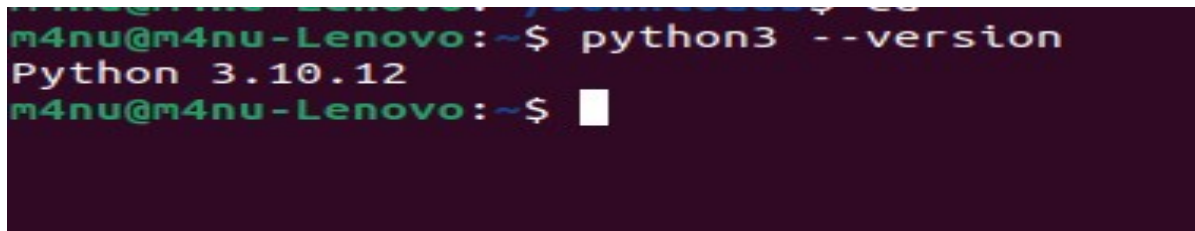una interfaz de red y mostrar estadísticas básicas sobre el mismo.

para realizar dicho trabajo tenemos varios procesos como instalaciones de aplicativos, ejecuciones y pantallazos del mismo; a continuación envió el paso a paso de cómo se realizó este aplicativo de análisis de tráfico.

1- Sistema Operativo es linux (distribución Ubuntu 22.04.4 LTS) y debemos instalar 2 aplicativos para su gestión.
- python 3.10.12
- Scapy 2.4.4

para instalar la versión de python 3.10.12 se realiza los siguientes pasos:
1. abrimos terminal y escribimos los siguientes comandos
2. sudo apt update
3. sudo apt install python3.10.12
4. python3 --version
5. wget https://www.python.org/ftp/python/3.11/Python-3.11.0.tar.gz
6. tar -xf Python-3.11.0.tar.gz
7. cd Python-3.11.0
8. ./configure --prefix=/usr/local
9. make install
10. python3 --version
11. sudo apt install python3-pip
12. python3 --version

para instalar la versión de scapy 2.4.4 se realiza los siguientes pasos:
1. abrimos terminal y escribimos los siguientes comandos
2. sudo apt install python3-pip
3. pip3 install scapy
4. sudo apt install git
5. git clone https://github.com/secdev/scapy.git
6. cd scapy
7. sudo python3 setup.py install
8. sudo scapy

```
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:671: ImportWarning: _SixMetaPathImporter.exec_module() not found; falling back to load_m
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod
<frozen importlib._bootstrap>:914: ImportWarning: _SixMetaPathImporter.find_spec() not found; falling back to find_mod


                      aSPY//YASa
                  apyyyyCY//////////YCa
                sY//////YSpcs  scpCY//Pp        |
      ayp ayyyyyyySCP//Pp         syY//C         | Welcome to Scapy
      AYAsAYYYYYYYY///Ps          cY//S          | Version 2.4.4
             pCCCCY//p         cSSps y//Y        |
              SPPPP///a        pP///AC//Y        | https://github.com/secdev/scapy
                 A//A          cyP////C          |
                 p///Ac          sC///a          | Have fun!
                P////YCpc         A//A           |
             scccccp///pSP///p     p//Y          | Craft packets before they craft
             sY/////////y  caa     S//P          | you.
             cayCyayP//Ya         pY/Ya          |              -- Socrate
              sY/PsY////YCc       aC//Yp         |
               sc  sccaCY//PCypaapyCP//YSs
                    spCPY//////YPSps
                      ccaacs
                                        using IPython 7.31.1
>>> from scapy.all import *
>>> ▯
```

2- Ya instalado los dos aplicativos, vamos a generar el script en Python3 con el siguiente
código
(adjuntamos script para su ejecución)

#Librerías importadas para utilizar en el código
import argparse
from datetime import datetime
from scapy.all import sniff, IP, TCP, UDP

#Iniciación de variables
tcp_count = 0
udp_count = 0
source_count = {} #Diccionario key:value
destination_count = {}

#Función de análisis de paquetes
def packet_handler(packet, output_file):
    global tcp_count, udp_count

    #Se extrae día, mes, hora y minuto actual para el nombre del archivo
    timestamp = datetime.now().strftime("%d_%m_%H_%M")

    #Loop para revisar todo el tráfico y llenar el archivo base de datos

```python
    with open(output_file, "a") as file:
        if IP in packet:
            src_ip = packet[IP].src
            dest_ip = packet[IP].dst
            file.write(f"{timestamp} - Source IP: {src_ip}, Destination IP: {dest_ip}\n")

            #Comparamos las IP de origen y destino para contar cada que se repitan (top 5)
            source_count[src_ip] = source_count.get(src_ip, 0) + 1
            destination_count[dest_ip] = destination_count.get(dest_ip, 0) + 1

            #Contamos los paquetes TCP y UDP
            if TCP in packet:
                tcp_count += 1
            elif UDP in packet:
                udp_count += 1


    protocol = "Unknown Protocol"

    #Tamaño del paquete
    packet_size = len(packet)

    if IP in packet:
        src_ip = packet[IP].src
        dst_ip = packet[IP].dst

        if TCP in packet:
            protocol = "TCP"
        elif UDP in packet:
            protocol = "UDP"

        #Impresión de pantalla del tráfico capturado
        print(f"Source IP: {src_ip}, Destination IP: {dst_ip}, Protocol: {protocol}, Packet Size: {packet_size}")

#Función para imprimir el top 5 de IP origen y destino con mayor tráfico
def print_top_5(count_dict, title):

    # tomando los 5 valores mayores
    sorted_dict = dict(sorted(count_dict.items(), key=lambda x: x[1], reverse=True)[:5])
    print(f"\nTop 5 {title} IP addresses:")
    for ip, count in sorted_dict.items():
        print(f"{ip}: {count} packets")

#Función para capturar el tráfico
def capture_packets(interface, timeout):
    filename = f"traffic_capture_{datetime.now().strftime('%d_%m_%H_%M')}.txt"
    sniff(iface=interface, prn=lambda pkt: packet_handler(pkt, filename), timeout=timeout)
```

```python
if __name__ == "__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument("-time", type=int, help="Total time value in seconds for packet capture")
    parser.add_argument("-interface", help="Network interface to capture packets from")
    args = parser.parse_args()


    if args.time and args.interface:
        capture_packets(args.interface, args.time)
        print(f"Total TCP packets captured: {tcp_count}")
        print(f"Total UDP packets captured: {udp_count}")
        print(f"Total packets captured: {tcp_count + udp_count}")
        print_top_5(source_count, "Source")
        print_top_5(destination_count, "Destination")

                    # imprime los datos que están en la aplicación en Scapy
    else:
        print("Please specify both arguments -time and -interface values.")
```

Lista de palabras claves.

Argparse — Analizador sintáctico (Parser) para las opciones, argumentos y sub-comandos de la línea de comandos

Sniffer - También denominado rastreador de red, es un software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que pasan por una red.

TCP - El Protocolo de Control de Transmisión (Transmission Control Protocol en inglés o TCP) es el método de comunicación de datos por defecto entre distintos dispositivos, a través de una red
(subida - descarga)

UDP - es un protocolo ligero de transporte de datos que funciona sobre protocolo de internet (IP). Dicho de otra manera, permite el envío rápido de datagramas en redes IP, sin necesidad de establecer una conexión previa. (streaming)

Packet_handler - función que se ejecuta en el servidor web cuando se hace una petición a cierta url (endpoint) de dicho servidor web.

Lambda - forma corta de declarar funciones pequeñas y anónimas (no es necesario proporcionar un nombre para las funciones lambda)

Parser - proporciona una interfaz para el analizador sintáctico interno de Python y para el compilador de código de bytes

3- Se realizan las capturas desde python local con su código


```
traficored.py
~/Downloads

#Librerías importadas para utilizar en el código
import argparse
from datetime import datetime
from scapy.all import sniff, IP, TCP, UDP

#Iniciación de variables
tcp_count = 0
udp_count = 0
source_count = {} #Diccionario key:value
destination_count = {}

#Función de análisis de paquetes
def packet_handler(packet, output_file):
    global tcp_count, udp_count

    #Se extrae día, mes, hora y minuto actual para el nombre del archivo
    timestamp = datetime.now().strftime("%d_%m_%H_%M")

    #Loop para revisar todo el tráfico y llenar el archivo base de datos
    with open(output_file, "a") as file:
        if IP in packet:
            src_ip = packet[IP].src
            dest_ip = packet[IP].dst
            file.write(f"{timestamp} - Source IP: {src_ip}, Destination IP: {dest_ip}\

            #Comparamos las IP de origen y destino para contar cada que se repitan (te
            source_count[src_ip] = source_count.get(src_ip, 0) + 1
            destination_count[dest_ip] = destination_count.get(dest_ip, 0) + 1

            #Contamos los paquetes TCP y UDP
            if TCP in packet:
                tcp_count += 1
            elif UDP in packet:
                udp_count += 1

    protocol = "Unknown Protocol"
```

4- para ejecutar el script en terminal con Scapy, verificamos la interfaz de red con la que deseamos mirar las salidas y entradas del direccionamiento, para ello revisamos desde terminal con el comando ifconfig en ubuntu. El cual implementamos la interfaz "wlp2s0"

```
m4nu@m4nu-Lenovo:~$ ifconfig
enp1s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 98:29:a6:57:4d:6f  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enx00e04c3610d8: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:e0:4c:36:10:d8  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 22285  bytes 2384132 (2.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22285  bytes 2384132 (2.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:c6:e3:d0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.45  netmask 255.255.255.0  broadcast 192.168.20.255
        inet6 fe80::927:6c4d:5b70:a397  prefixlen 64  scopeid 0x20<link>
        ether 94:b8:6d:8a:39:5a  txqueuelen 1000  (Ethernet)
        RX packets 2372922  bytes 3062485316 (3.0 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

si desean ejecutar el script con interfaz desde otro sistema operativo :

macOS de MacBook es con el comando ifconfig
Windows de Microsoft es con el comando ipconfig

5- para ejecutar el script y se visualice el análisis y proceso de tráfico hacemos lo siguiente.

- guardamos el script en una ruta local, puede ser en *descargas*
- vamos a la terminal y dentro de python3 ejecutamos la siguiente linea
  sudo python3 traficored.py -time 4 -interface wlp2s0 dentro del código sería así
  print("Please specify both arguments -time and -interface values.")}
- luego nos muestra todo el tráfico Origen y Destino con IPs y los protocolos TCP y UDP
- tambíen nos visualiza total de paquetes capturados con los dos protocolos TCP y UDP

- al finalizar el monitoreo nos enseña las 5 IPs de origen y las 5 IPs de destino

adjunto pantallazos del proceso

Nombre

📁 Python-3.12.4
📄 challenge mercado libre.odt
🗜 Python-3.12.4.tar.xz
🗜 Sentinel-Release-24-1-1-7353_macos_v24_1_1_7353.pkg
📄 traffic_capture_10_06_22_47.txt
📄 traffic_capture_10_06_22_48.txt
📄 traffic_capture_10_06_22_49.txt
🐍 traficored.py

```
m4nu@m4nu-Lenovo:~$ ls
Descargas    Downloads    Imágenes    Plantillas    scapy    Vídeos
Documentos   Escritorio   Música      Público       snap
m4nu@m4nu-Lenovo:~/Downloads$ sudo python3 traficored.py -time 4 -interface wlp2s0
[sudo] contraseña para m4nu:
Source IP: 192.168.20.45, Destination IP: 35.201.89.89, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.218.131, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 3.163.60.125, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 162.247.243.39, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 172.217.28.101, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 104.18.3.92, Protocol: TCP, Packet Size: 66
Source IP: 35.201.89.89, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 142.250.218.131, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 162.247.243.39, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 3.163.60.125, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 172.217.28.101, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 162.247.243.29, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 162.247.243.29, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 162.247.243.29, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 162.247.243.29, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 162.247.243.29, Protocol: TCP, Packet Size: 66
Source IP: 104.18.3.92, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 162.247.243.29, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 162.247.243.29, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 162.247.243.29, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 162.247.243.29, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 162.247.243.29, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 18.231.65.122, Protocol: TCP, Packet Size: 120
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 113
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 109
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 104.18.42.150, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 141
Source IP: 192.168.20.45, Destination IP: 104.18.42.150, Protocol: TCP, Packet Size: 66
Source IP: 18.231.65.122, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 122
Source IP: 192.168.20.45, Destination IP: 18.231.65.122, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1020
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 150
Source IP: 192.168.2.1, Destination IP: 192.168.2.255, Protocol: UDP, Packet Size: 76
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 75
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 1287
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 437
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 239
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 81
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 239.255.255.250, Protocol: UDP, Packet Size: 215
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 68
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.45, Destination IP: 142.251.132.138, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 18.155.252.113, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 181.54.162.226, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.218.131, Protocol: TCP, Packet Size: 66
```

```
Source IP: 192.168.20.45, Destination IP: 181.54.162.226, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.218.131, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.218.131, Protocol: TCP, Packet Size: 66
Source IP: 142.251.132.138, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 181.54.162.226, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.218.131, Protocol: TCP, Packet Size: 66
Source IP: 18.155.252.113, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 142.250.218.131, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 142.250.218.131, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 142.250.218.131, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 239.255.255.250, Protocol: UDP, Packet Size: 215
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 113
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 109
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1018
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 3.33.235.18, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 104
Source IP: 192.168.20.45, Destination IP: 3.33.235.18, Protocol: TCP, Packet Size: 66
Source IP: 3.33.235.18, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 3.33.235.18, Protocol: TCP, Packet Size: 66
Source IP: 104.18.42.150, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 144
Source IP: 192.168.20.45, Destination IP: 104.18.42.150, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 239.255.255.250, Protocol: UDP, Packet Size: 215
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Source IP: 192.168.20.28, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 388
Total TCP packets captured: 57
Total UDP packets captured: 33
Total packets captured: 90

Top 5 Source IP addresses:
192.168.20.45: 36 packets
192.168.20.28: 20 packets
34.128.165.207: 6 packets
162.247.243.29: 5 packets
142.250.78.100: 5 packets

Top 5 Destination IP addresses:
192.168.20.45: 53 packets
34.128.165.207: 6 packets
162.247.243.29: 5 packets
142.250.218.131: 4 packets
142.250.78.100: 4 packets
m4pu@m4pu-Lenovo:~/Downloads$ sudo python3 traficored.py -time 4 -interface wlp2s0
```

```
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 109
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 172.217.30.206, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 172.217.30.206, Protocol: UDP, Packet Size: 784
Source IP: 172.217.30.206, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 172.217.30.206, Protocol: UDP, Packet Size: 75
Source IP: 172.217.30.206, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 1027
Source IP: 172.217.30.206, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 102
Source IP: 192.168.20.45, Destination IP: 172.217.30.206, Protocol: UDP, Packet Size: 81
Source IP: 192.168.20.45, Destination IP: 172.217.30.206, Protocol: UDP, Packet Size: 75
Source IP: 172.217.30.206, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 68
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 152
Source IP: 142.250.218.106, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 201
Source IP: 104.18.42.150, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 90
Source IP: 192.168.20.45, Destination IP: 104.18.42.150, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 104.18.42.150, Protocol: TCP, Packet Size: 94
Source IP: 192.168.20.45, Destination IP: 142.250.218.106, Protocol: UDP, Packet Size: 75
Source IP: 142.250.218.106, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 201
Source IP: 192.168.20.45, Destination IP: 142.250.218.106, Protocol: UDP, Packet Size: 76
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 75
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 1287
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 438
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 273
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 81
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 75
Source IP: 104.18.42.150, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 68
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1018
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 104.18.42.150, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 144
Source IP: 192.168.20.45, Destination IP: 104.18.42.150, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 113
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 109
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 142.250.218.106, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 121
Source IP: 192.168.20.45, Destination IP: 142.250.218.106, Protocol: UDP, Packet Size: 76
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1018
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Total TCP packets captured: 22
Total UDP packets captured: 27
Total packets captured: 49

Top 5 Source IP addresses:
192.168.20.45: 23 packets
34.128.165.207: 7 packets
172.217.30.206: 6 packets
142.250.78.100: 5 packets
104.18.42.150: 4 packets

Top 5 Destination IP addresses:
192.168.20.45: 25 packets
34.128.165.207: 7 packets
172.217.30.206: 5 packets
104.18.42.150: 4 packets
142.250.78.100: 4 packets
m4pu@m4pu-Lenovo:~/Downloads$ sudo python3 traficored.py -time 4 -interface wlp2s0
```

```
Source IP: 192.168.20.45, Destination IP: 142.250.218.106, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 142.251.132.142, Protocol: UDP, Packet Size: 414
Source IP: 142.250.218.106, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 136
Source IP: 192.168.20.45, Destination IP: 142.250.218.106, Protocol: UDP, Packet Size: 79
Source IP: 142.251.132.142, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 142.251.132.142, Protocol: UDP, Packet Size: 75
Source IP: 142.250.218.106, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 67
Source IP: 142.251.132.142, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 152
Source IP: 142.251.132.142, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 78
Source IP: 192.168.20.45, Destination IP: 142.251.132.142, Protocol: UDP, Packet Size: 81
Source IP: 192.168.20.45, Destination IP: 142.251.132.142, Protocol: UDP, Packet Size: 75
Source IP: 142.251.132.142, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 68
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 112
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 108
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1020
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1020
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 104.18.42.150, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 144
Source IP: 192.168.20.45, Destination IP: 104.18.42.150, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 199.232.49.91, Protocol: TCP, Packet Size: 66
Source IP: 199.232.49.91, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 153
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 75
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 75
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 1287
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 437
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 120
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 81
Source IP: 192.168.20.45, Destination IP: 142.250.78.100, Protocol: UDP, Packet Size: 75
Source IP: 192.168.2.1, Destination IP: 192.168.2.255, Protocol: UDP, Packet Size: 76
Source IP: 142.250.78.100, Destination IP: 192.168.20.45, Protocol: UDP, Packet Size: 68
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 1020
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 112
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 66
Source IP: 34.128.165.207, Destination IP: 192.168.20.45, Protocol: TCP, Packet Size: 108
Source IP: 192.168.20.45, Destination IP: 34.128.165.207, Protocol: TCP, Packet Size: 66
Total TCP packets captured: 30
Total UDP packets captured: 45
Total packets captured: 75

Top 5 Source IP addresses:
192.168.20.45: 36 packets
142.250.78.100: 10 packets
34.128.165.207: 9 packets
142.250.218.106: 5 packets
104.18.42.150: 4 packets

Top 5 Destination IP addresses:
192.168.20.45: 38 packets
34.128.165.207: 9 packets
142.250.78.100: 8 packets
142.250.218.106: 5 packets
104.18.42.150: 4 packets
```

6- Número de paquetes por protocolo (por ejemplo, TCP, UDP).

Las 5 principales direcciones IP de origen con mayor tráfico.
Las 5 principales direcciones IP de destino con mayor tráfico.

nos enseña que la IP 192.168.20.45 es de mi red local

```
Total TCP packets captured: 57
Total UDP packets captured: 33
Total packets captured: 90

Top 5 Source IP addresses:
192.168.20.45: 36 packets
192.168.20.28: 20 packets
34.128.165.207: 6 packets
162.247.243.29: 5 packets
142.250.78.100: 5 packets

Top 5 Destination IP addresses:
192.168.20.45: 53 packets
34.128.165.207: 6 packets
162.247.243.29: 5 packets
142.250.218.131: 4 packets
142.250.78.100: 4 packets
```

```
Source IP: 192.168.20.45, Destinatio
Total TCP packets captured: 22
Total UDP packets captured: 27
Total packets captured: 49

Top 5 Source IP addresses:
192.168.20.45: 23 packets
34.128.165.207: 7 packets
172.217.30.206: 6 packets
142.250.78.100: 5 packets
104.18.42.150: 4 packets

Top 5 Destination IP addresses:
192.168.20.45: 25 packets
34.128.165.207: 7 packets
172.217.30.206: 5 packets
104.18.42.150: 4 packets
142.250.78.100: 4 packets
```

```
Source IP: 192.168.20.45, Destinatic
Total TCP packets captured: 30
Total UDP packets captured: 45
Total packets captured: 75

Top 5 Source IP addresses:
192.168.20.45: 36 packets
142.250.78.100: 10 packets
34.128.165.207: 9 packets
142.250.218.106: 5 packets
104.18.42.150: 4 packets

Top 5 Destination IP addresses:
192.168.20.45: 38 packets
34.128.165.207: 9 packets
142.250.78.100: 8 packets
142.250.218.106: 5 packets
104.18.42.150: 4 packets
```

7- Se crean 3 archivos en formato txt con una base de datos que muestra los paquetes de origen y destino. (se adjunta archivos en el repositorio)