

# Práctica 6

## Ejercicio 1 (1 punto)

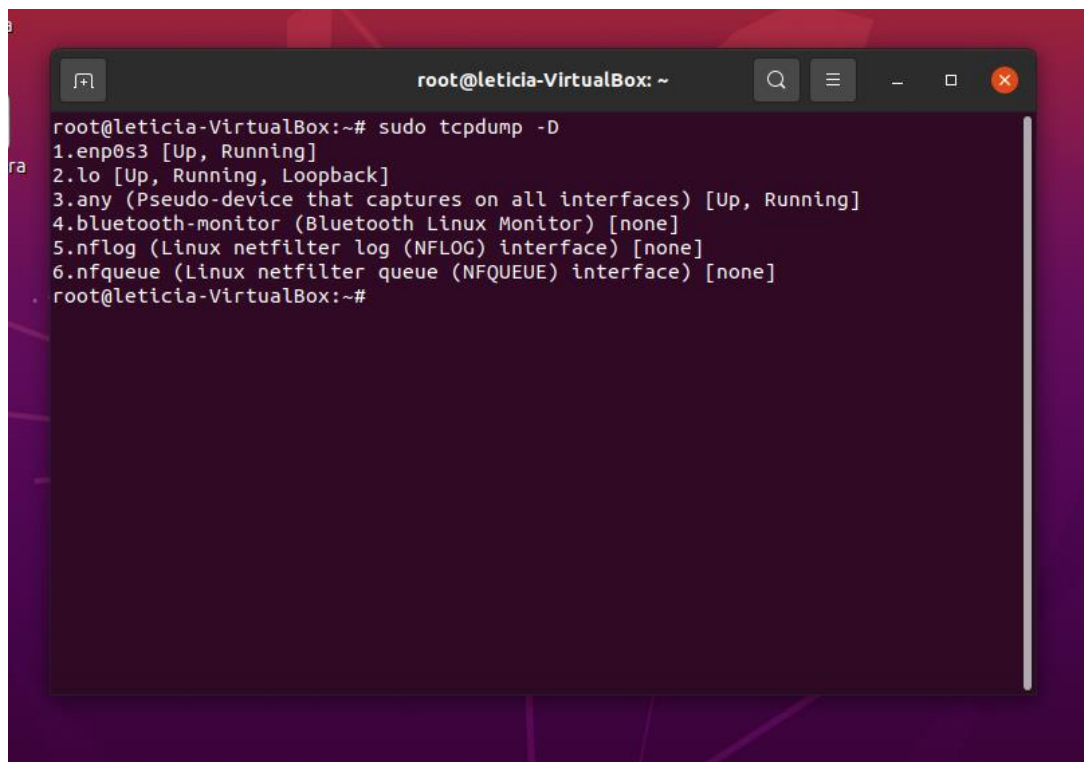
Instala tcpdump en una máquina virtual con Ubuntu. Indica los pasos que has realizado para llevarlo a cabo

```
root@leticia-VirtualBox:~# sudo apt install tcpdump
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.
  libfprint-2-tod1 libllvm10
Utilice «sudo apt autoremove» para eliminarlos.
Se actualizarán los siguientes paquetes:
  tcpdump
1 actualizados, 0 nuevos se instalarán, 0 para eliminar y 443 no actualizados.
Se necesita descargar 369 kB de archivos.
Se utilizarán 0 B de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 tcpdump amd64
4.9.3-4ubuntu0.1 [369 kB]
Descargados 369 kB en 4s (101 kB/s)
(Leyendo la base de datos ... 192799 ficheros o directorios instalados actualmen
te.)
Preparando para desempaquetar .../tcpdump_4.9.3-4ubuntu0.1_amd64.deb ...
```

## Ejercicio 2 (9 puntos)

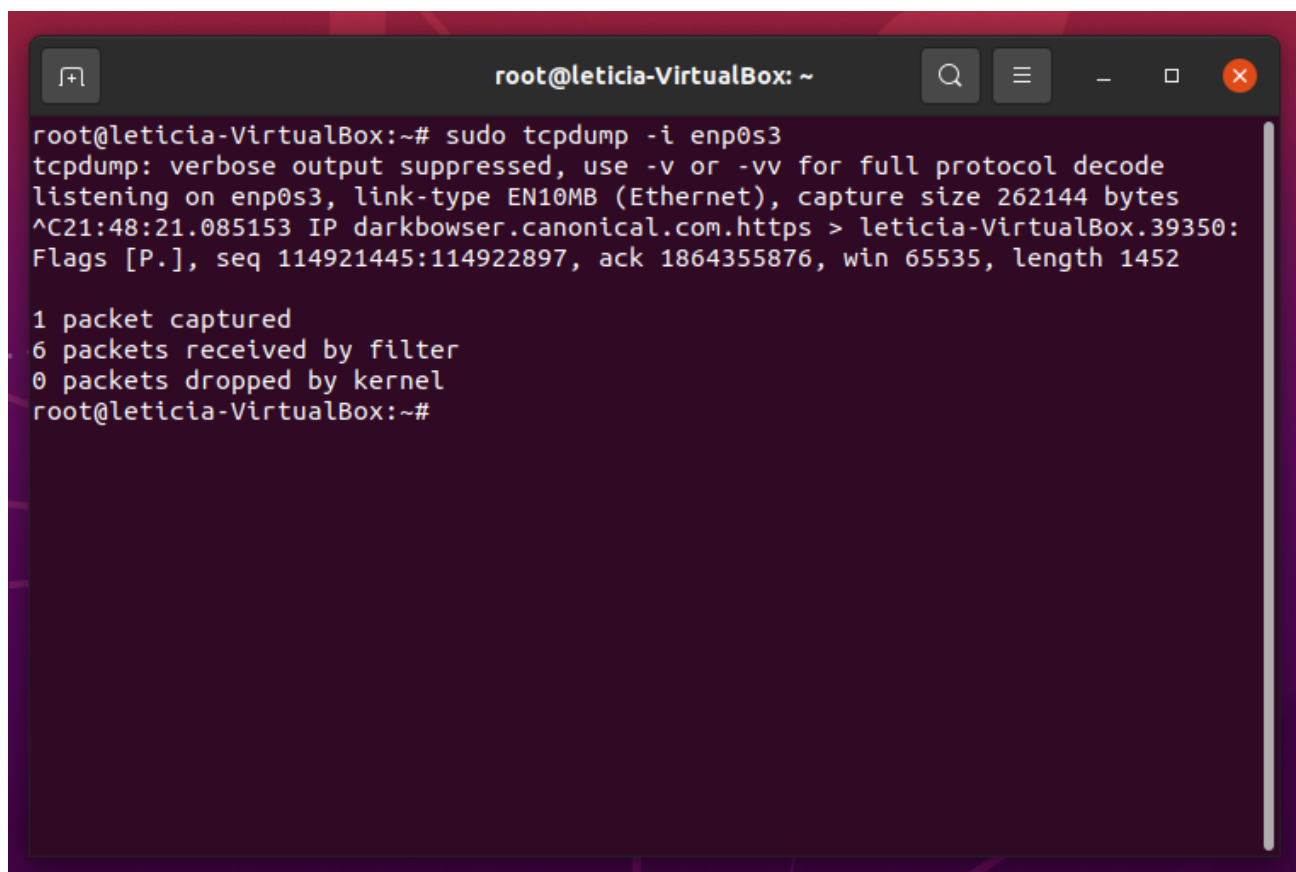
Instala tcpdump en una máquina virtual con Ubuntu y a continuación realiza lo siguiente. Tienes que indicar el comando y el resultado obtenido

- Listado de las interfaces disponibles para capturar tráfico con tcpdump



```
root@leticia-VirtualBox: ~  
root@leticia-VirtualBox:~# sudo tcpdump -D  
1.enp0s3 [Up, Running]  
2.lo [Up, Running, Loopback]  
3.any (Pseudo-device that captures on all interfaces) [Up, Running]  
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]  
5.nflog (Linux netfilter log (NFLOG) interface) [none]  
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]  
root@leticia-VirtualBox:~#
```

b) Capturar todo el tráfico de entrada y salida de una interfaz de red concreta



```
root@leticia-VirtualBox: ~  
root@leticia-VirtualBox:~# sudo tcpdump -i enp0s3  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes  
^C21:48:21.085153 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350:  
Flags [P.], seq 114921445:114922897, ack 1864355876, win 65535, length 1452  
  
1 packet captured  
6 packets received by filter  
0 packets dropped by kernel  
root@leticia-VirtualBox:~#
```

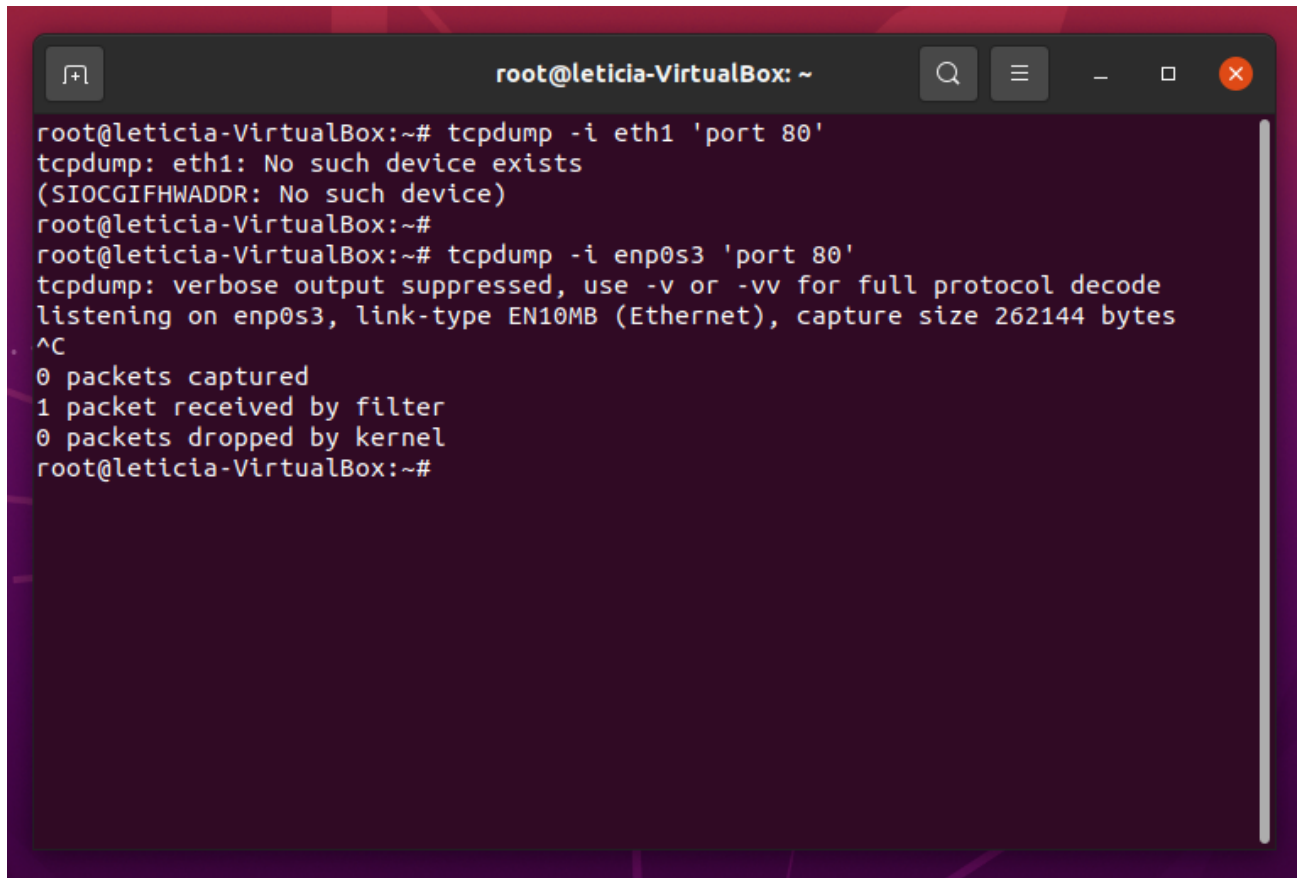
- c) Redirigir la salida estándar de tcpdump a un fichero llamado trafico.log

```
root@leticia-VirtualBox: ~  
root@leticia-VirtualBox:~# sudo tcpdump -i enp0s3 > trafico.log  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes  
^C2460 packets captured  
2567 packets received by filter  
0 packets dropped by kernel  
root@leticia-VirtualBox:~# ls  
trafico.log  
root@leticia-VirtualBox:~# cat trafico.log  
21:49:13.940350 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Fl  
ags [P.], seq 124458181:124459633, ack 1864355876, win 65535, length 1452  
21:49:13.940382 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Fl  
ags [.], ack 1452, win 65535, length 0  
21:49:13.945043 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Fl  
ags [P.], seq 1452:2904, ack 1, win 65535, length 1452  
21:49:13.949747 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Fl  
ags [P.], seq 2904:4356, ack 1, win 65535, length 1452  
21:49:13.949761 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Fl  
ags [.], ack 4356, win 65535, length 0  
21:49:13.954083 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Fl  
ags [P.], seq 4356:5808, ack 1, win 65535, length 1452  
21:49:13.958620 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Fl  
ags [P.], seq 5808:7260, ack 1, win 65535, length 1452  
21:49:13.958632 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Fl
```

- d) Además de especificar la interfaz de red por la que queremos capturar tráfico, especificar que el tráfico a capturar sea ICMP

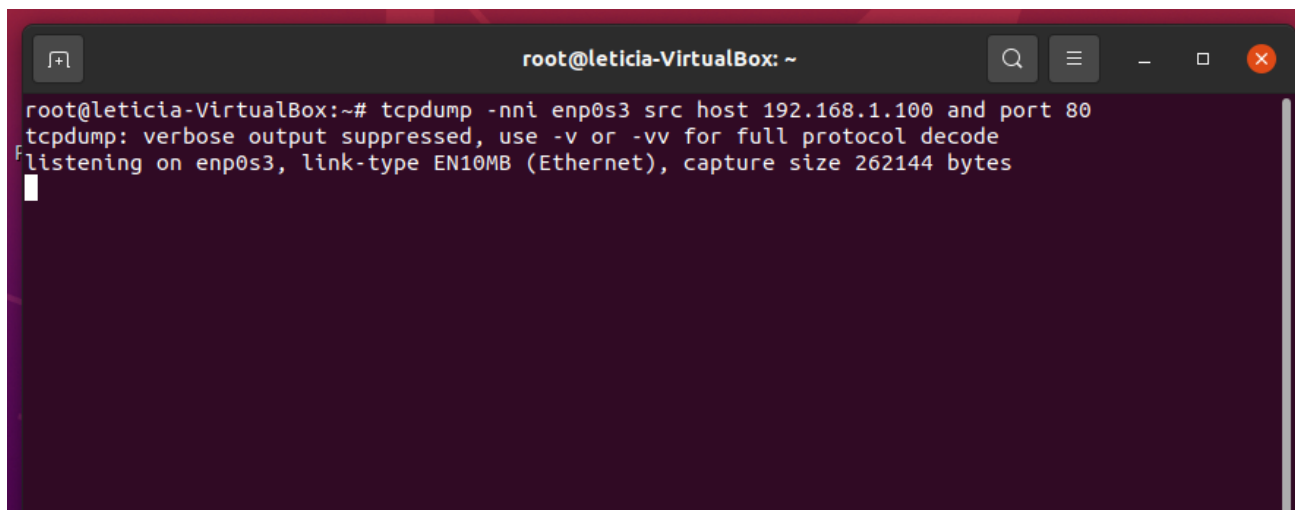
```
root@leticia-VirtualBox:~# sudo tcpdump -i enp0s3 icmp  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes  
^C  
0 packets captured  
1 packet received by filter  
0 packets dropped by kernel  
root@leticia-VirtualBox:~#
```

- e) Además del protocolo especificamos el puerto sobre el cual queremos capturar el tráfico, por ejemplo el puerto TCP 80 para capturar tráfico HTTP

A terminal window titled 'root@leticia-VirtualBox: ~' with standard window controls. The terminal shows the execution of two tcpdump commands. The first command, 'tcpdump -i eth1 'port 80'', results in an error: 'tcpdump: eth1: No such device exists (SIOCGIFHWADDR: No such device)'. The second command, 'tcpdump -i enp0s3 'port 80'', successfully starts listening on the interface enp0s3. It shows that 0 packets were captured, 1 packet was received by the filter, and 0 packets were dropped by the kernel. The terminal text is as follows:

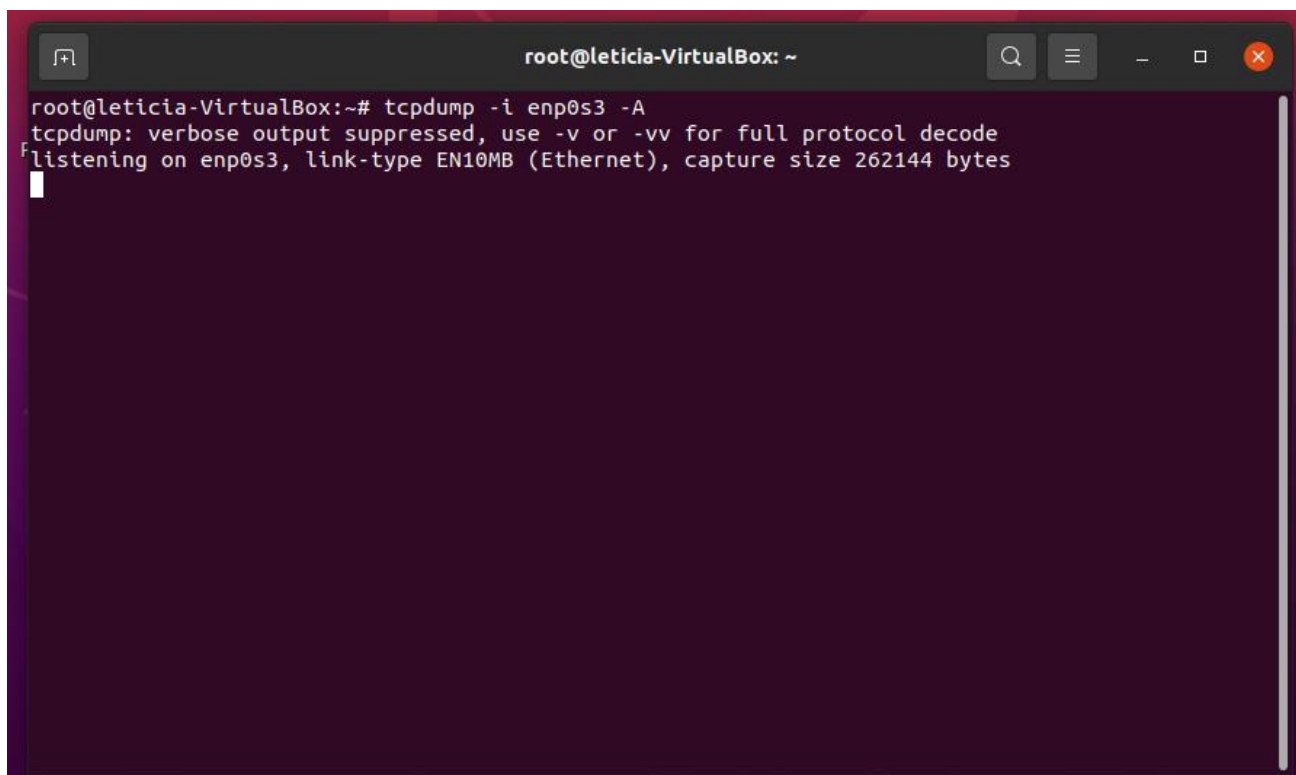
```
root@leticia-VirtualBox:~# tcpdump -i eth1 'port 80'
tcpdump: eth1: No such device exists
(SIOCGIFHWADDR: No such device)
root@leticia-VirtualBox:~#
root@leticia-VirtualBox:~# tcpdump -i enp0s3 'port 80'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
1 packet received by filter
0 packets dropped by kernel
root@leticia-VirtualBox:~#
```

- f) Capturar el tráfico TCP por el puerto 80, pero sólo visualizamos el tráfico originado desde la IP 192.168.1.100

A terminal window titled 'root@leticia-VirtualBox: ~' with standard window controls. The terminal shows the execution of a tcpdump command with a source IP filter: 'tcpdump -nni enp0s3 src host 192.168.1.100 and port 80'. The output shows it is listening on enp0s3. The terminal text is as follows:

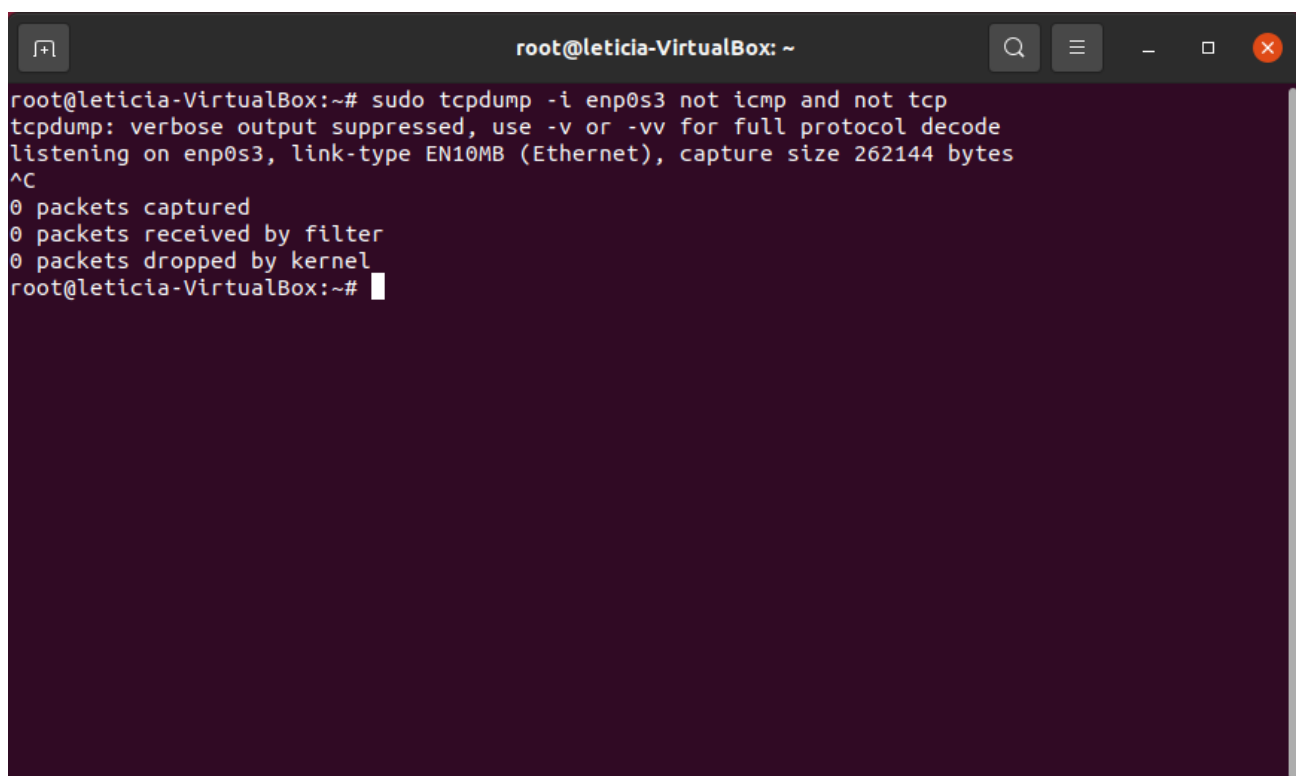
```
root@leticia-VirtualBox:~# tcpdump -nni enp0s3 src host 192.168.1.100 and port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

- g) Mostrar el contenido de los paquetes en formato ASCII

A terminal window titled 'root@leticia-VirtualBox: ~' with search, menu, and window control icons. The terminal shows the command 'tcpdump -i enp0s3 -A' being executed. The output indicates that verbose output is suppressed and that the program is listening on the enp0s3 interface with a capture size of 262144 bytes. The cursor is on the line following the output.

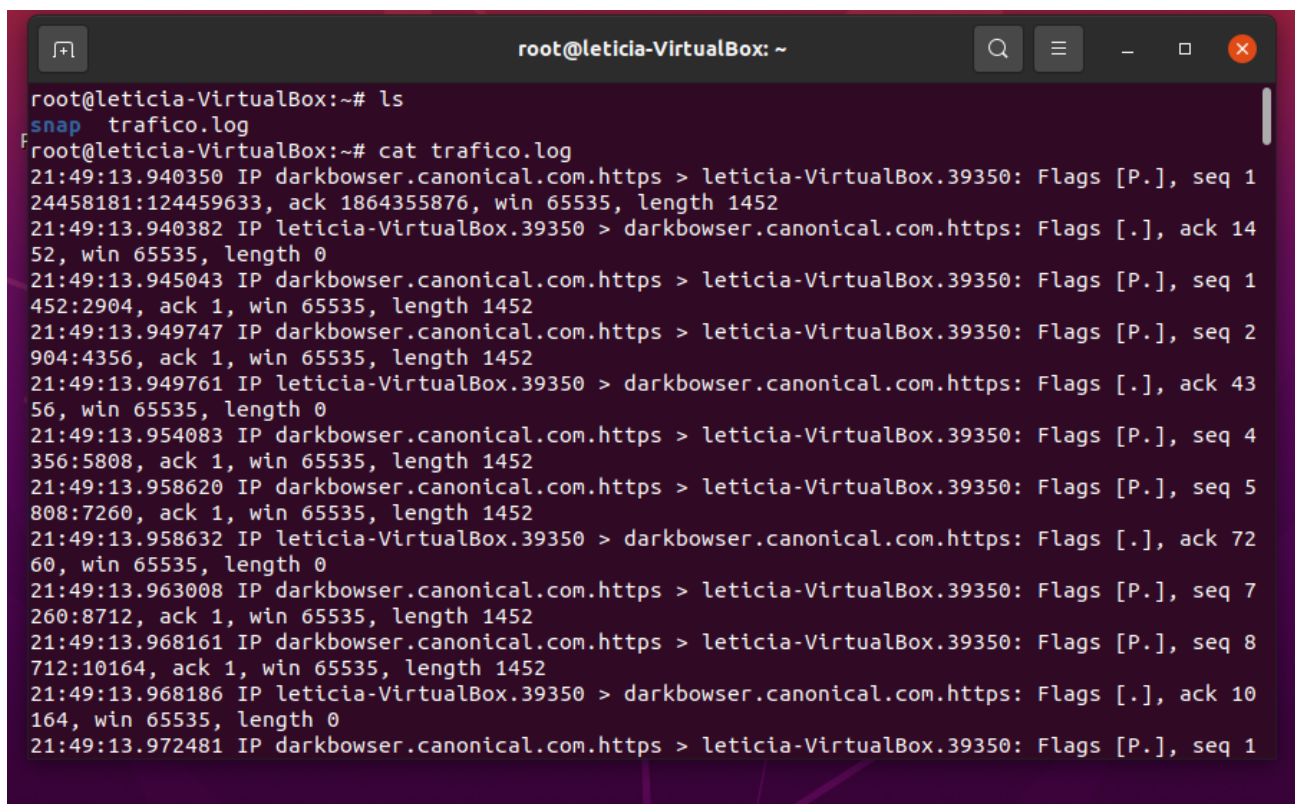
```
root@leticia-VirtualBox:~# tcpdump -i enp0s3 -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

- h) Capturar todo el tráfico a excepción del ICMP y el TCP

A terminal window titled 'root@leticia-VirtualBox: ~' with search, menu, and window control icons. The terminal shows the command 'sudo tcpdump -i enp0s3 not icmp and not tcp' being executed. The output shows that no packets were captured, received by the filter, or dropped by the kernel. The cursor is on the line following the output.

```
root@leticia-VirtualBox:~# sudo tcpdump -i enp0s3 not icmp and not tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@leticia-VirtualBox:~#
```

- i) Leer captura de tráfico almacenada en el archivo trafico.log

A screenshot of a terminal window titled 'root@leticia-VirtualBox: ~'. The terminal shows the command 'ls' followed by 'snap trafico.log', and then 'cat trafico.log'. The output of 'cat' displays a series of network traffic logs in a structured format, including timestamps, IP addresses, and sequence numbers. The logs show a sequence of packets between 'darkbrowser.canonical.com.https' and 'leticia-VirtualBox.39350'.

```
root@leticia-VirtualBox:~# ls
snap trafico.log
root@leticia-VirtualBox:~# cat trafico.log
21:49:13.940350 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 1
24458181:124459633, ack 1864355876, win 65535, length 1452
21:49:13.940382 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Flags [.], ack 14
52, win 65535, length 0
21:49:13.945043 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 1
452:2904, ack 1, win 65535, length 1452
21:49:13.949747 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 2
904:4356, ack 1, win 65535, length 1452
21:49:13.949761 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Flags [.], ack 43
56, win 65535, length 0
21:49:13.954083 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 4
356:5808, ack 1, win 65535, length 1452
21:49:13.958620 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 5
808:7260, ack 1, win 65535, length 1452
21:49:13.958632 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Flags [.], ack 72
60, win 65535, length 0
21:49:13.963008 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 7
260:8712, ack 1, win 65535, length 1452
21:49:13.968161 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 8
712:10164, ack 1, win 65535, length 1452
21:49:13.968186 IP leticia-VirtualBox.39350 > darkbrowser.canonical.com.https: Flags [.], ack 10
164, win 65535, length 0
21:49:13.972481 IP darkbrowser.canonical.com.https > leticia-VirtualBox.39350: Flags [P.], seq 1
```