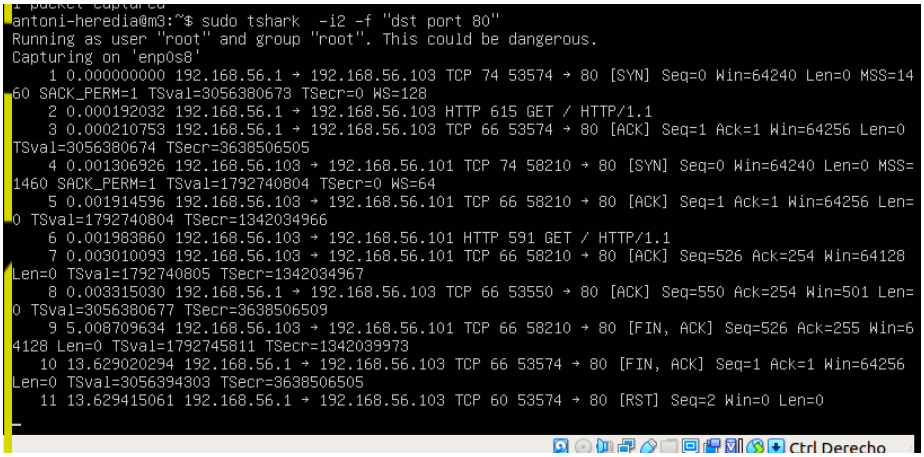
Ejercicio T5.1: Wireshark

Instalar Wireshark y observar cómo fluye el tráfico de red en el balanceador de la máquina M3 mientras se le hacen peticiones HTTP y HTTPS. Ejecuta al menos 3 peticiones al balanceador. Realiza un análisis de una sesión TCP (establecer conexión y cierre) de peticiones HTTP y HTTPS y escribe tus propias conclusiones. Puedes ilustrarlo con capturas de pantalla

Como **M3** tiene un sistema operativo de server, no tiene modo grafico. Por lo tanto no he podido instalar **Wireshark** y por lo tanto he tenido que instalar y usar **tshark**. Adjunto las capturas de tres conexiónes que he realizado. Dos de http y una de https. Captura 1, puerto 80.



Lo primero que el cliente quiere establecer la conexión con **syn**. Como solo hemos capturado los paquetes del puerto 80, no podemos ver la confirmación que envía el servidor con el paquete **syn-ack**. Pero si vemos la contestación que realiza el cliente con el paquete **ack**. Se cuelan unos pocos paquetes mas y podemos ver el paquete **fin** que indica el final de la conexión

Captura 2, puerto 443.

```
antoni-heredia@m3:~$ sudo tshark  -i2 -f "dst port 443"
Running as user "root" and group "root". This could be dangerous.
Capturing on 'enp0s8'
    1 0.000000000 192.168.56.1 → 192.168.56.103 TCP 74 56474 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
460 SACK_PERM=1 TSval=3057349406 TSecr=0 WS=128
    2 0.000229330 192.168.56.1 → 192.168.56.103 TCP 66 56474 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=
 TSval=3057349406 TSecr=3639475250
    3 0.000538423 192.168.56.1 → 192.168.56.103 TLSv1 583 Client Hello
    4 0.029191873 192.168.56.1 → 192.168.56.103 TCP 66 56474 → 443 [ACK] Seq=518 Ack=157 Win=64128 
en=0 TSval=3057349435 TSecr=3639475279
    5 0.029437727 192.168.56.1 → 192.168.56.103 TLSv1.2 73 Alert (Level: Fatal, Description: Certif
cate Unknown)
    6 0.029811702 192.168.56.1 → 192.168.56.103 TCP 66 56474 → 443 [FIN, ACK] Seq=525 Ack=157 Win=6
128 Len=0 TSval=3057349436 TSecr=3639475279
    7 0.029856626 192.168.56.1 → 192.168.56.103 TCP 66 56474 → 443 [ACK] Seq=526 Ack=158 Win=64128 
en=0 TSval=3057349436 TSecr=3639475279
    8 0.030208296 192.168.56.1 → 192.168.56.103 TCP 74 56476 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
460 SACK_PERM=1 TSval=3057349436 TSecr=0 WS=128
    9 0.030352271 192.168.56.1 → 192.168.56.103 TCP 66 56476 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=
 TSval=3057349437 TSecr=3639475280
   10 0.030609807 192.168.56.1 → 192.168.56.103 TLSv1 583 Client Hello
   11 0.031150741 192.168.56.1 → 192.168.56.103 TCP 66 56476 → 443 [ACK] Seq=518 Ack=157 Win=64128 
en=0 TSval=3057349437 TSecr=3639475281
   12 0.031429429 192.168.56.1 → 192.168.56.103 TLSv1.2 117 Change Cipher Spec, Encrypted Handshake
Message
   13 0.031638031 192.168.56.1 → 192.168.56.103 TLSv1.2 657 Application Data
   14 0.056549041 192.168.56.1 → 192.168.56.103 TCP 66 56476 → 443 [ACK] Seq=1160 Ack=503 Win=64128
Len=0 TSval=3057349463 TSecr=3639475306
   15 0.064393069 192.168.56.1 → 192.168.56.103 TCP 66 56472 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 L
n=0 TSval=3057349471 TSecr=3639460823
   16 0.064865620 192.168.56.1 → 192.168.56.103 TCP 60 56472 → 443 [RST] Seq=2 Win=0 Len=0
   17 0.064880787 192.168.56.1 → 192.168.56.103 TCP 60 56472 → 443 [RST] Seq=2 Win=0 Len=0
   18 0.156214976 192.168.56.1 → 192.168.56.103 TLSv1.2 587 Application Data
```

Captura 3, puerto 80.

```
antoni-heredia@m3:~$ sudo tshark  -i2 -f "dst port 80"
Running as user "root" and group "root". This could be dangerous.
Capturing on 'enp0s8'
    1 0.000000000 192.168.56.103 → 192.168.56.101 TCP 74 60510 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
1460 SACK_PERM=1 TSval=1794002023 TSecr=0 WS=64
    2 0.033483818 192.168.56.1 → 192.168.56.103 TCP 66 56226 → 80 [FIN, ACK] Seq=1 Ack=1 Win=501 Len
=0 TSval=3057641913 TSecr=3639752313
    3 0.033908289 192.168.56.1 → 192.168.56.103 TCP 66 56226 → 80 [ACK] Seq=2 Ack=2 Win=501 Len=0 TS
val=3057641914 TSecr=3639767760
    4 2.834563159 192.168.56.1 → 192.168.56.103 TCP 66 56228 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len
=0 TSval=3057644714 TSecr=3639747905
    5 2.834605628 192.168.56.1 → 192.168.56.103 TCP 74 56232 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
60 SACK_PERM=1 TSval=3057644714 TSecr=0 WS=128
    6 2.834685928 192.168.56.1 → 192.168.56.103 TCP 74 56234 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
60 SACK_PERM=1 TSval=3057644714 TSecr=0 WS=128
    7 2.834870758 192.168.56.1 → 192.168.56.103 TCP 66 56232 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
TSval=3057644715 TSecr=3639770561
    8 2.834891053 192.168.56.1 → 192.168.56.103 TCP 66 56234 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
TSval=3057644715 TSecr=3639770561
    9 2.835112981 192.168.56.1 → 192.168.56.103 TCP 66 56228 → 80 [ACK] Seq=2 Ack=2 Win=502 Len=0 TS
val=3057644715 TSecr=3639770561
   10 2.835575239 192.168.56.1 → 192.168.56.103 HTTP 530 GET / HTTP/1.1
   11 2.835816224 192.168.56.103 → 192.168.56.102 TCP 74 33818 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
1460 SACK_PERM=1 TSval=1395372395 TSecr=0 WS=64
   12 2.836333810 192.168.56.103 → 192.168.56.102 TCP 66 33818 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=
0 TSval=1395372396 TSecr=1521662632
   13 2.836544671 192.168.56.103 → 192.168.56.102 HTTP 562 GET / HTTP/1.1
   14 2.837468107 192.168.56.103 → 192.168.56.102 TCP 66 33818 → 80 [ACK] Seq=497 Ack=254 Win=64128
Len=0 TSval=1395372397 TSecr=1521662633
   15 2.837739158 192.168.56.103 → 192.168.56.102 TCP 66 33818 → 80 [FIN, ACK] Seq=497 Ack=254 Win=6
4128 Len=0 TSval=1395372397 TSecr=1521662633
   16 2.838150266 192.168.56.103 → 192.168.56.102 TCP 66 33818 → 80 [ACK] Seq=498 Ack=255 Win=64128
Len=0 TSval=1395372398 TSecr=1521662633
   17 2.838187415 192.168.56.1 → 192.168.56.103 TCP 66 56232 → 80 [ACK] Seq=465 Ack=318 Win=64128 Le
n=0 TSval=3057644718 TSecr=3639770564
```