Redes de Comunicaciones I

Práctica 3

UAM 2017-2018

Óscar Gómez Borzdynski
José Ignacio Gómez García
14-Noviembre-2017

1. Introducción

En esta práctica hemos realizado una monitorización de red. Para ello se nos ha proporcionado un archivo *.pcap* que hemos tenido que analizar utilizando la herramienta *tshark*. Para simplificar la ejecución de la práctica, hemos ido introduciendo todos los comandos en una serie de ejecutables *.sh* que recogen todos los requisitos del enunciado.

El programa generador de trazas nos ha otorgado los siguientes valores:

- IP: 119.25.90.131
- MAC: 00:11:88:CC:33:E5
- Puerto UDP: 27884

2. Requisitos

A continuación, vamos a analizar los puntos requeridos en el enunciado:

2.1 Porcentajes

Para estudiar los porcentajes de paquetes IP hemos utilizado los siguientes filtros de tshark:

tshark -r traza.pcap -T fields -e frame.len (así obtenemos todos los paquetes y los podemos contar con un *wc* para poder obtener los porcentajes)

tshark -r traza.pcap -T fields -e ip.dst -e ip.src -e udp.dstport -e udp.srcport -e tcp.dstport -e tcp.srcport -e frame.len -Y 'eth.type eq 0x00000800 or vlan.etype eq 0x00000800' (así obtenemos TODOS los paquetes IP, TCP y UDP y luego analizamos el resultado obtenido mediante *awk*, obteniendo los datos necesarios)

El resultado obtenido es el siguiente:

```
Porcentajes de paquetes IP y no IP
IP: 99.01%
NO IP: 0.99%


Porcentajes de paquetes UDP, TCP y OTROS respecto al total de paquetes IP
IP-TCP: 89.59%
IP-UDP: 9.73%
IP-OTROS: 0.67%
```

Como se puede apreciar en la imagen, el 99.01% de los paquetes son IP, lo que indica que la inmensa mayoría del tráfico de red capturado utiliza dicho protocolo en sus comunicaciones.

Por otro lado, el 89.59% del tráfico IP capturado emplea el protocolo de transporte IP-TCP, que garantiza la entrega sin errores de los datos, en el mismo orden que se transmitieron. Claramente, es el protocolo de transporte IP más utilizado (posiblemente gracias a las características descritas), frente al 9.73% del UDP y el 0.67% de otros protocolos.

Podemos sacar ciertas conclusiones acerca de este último punto, como descartar la posibilidad de estar realizando o recibiendo un *streaming,* debido al escaso tráfico UDP. El protocolo TCP

estándar se emplea, por ejemplo, en páginas web comunes (es decir, protocolo HTTP), por lo que podemos suponer que los usuarios de la red se dedican a este tipo de navegación.

2.2 TOPS 10 POR PAQUETES

Para obtener los tops 10 que nos solicitan, hemos utilizado el resultado obtenido de la consulta *tshark* anterior y, empleando las herramientas *awk* (para quedarnos con las columnas que nos interesan y darles formato)*, sort* (para ordenar los resultados)*, sed* (para borrar líneas vacías)*, uniq* (para agrupar los datos iguales y contabilizar su cantidad) *y head* (para imprimir los 10 primeros).

El resultado obtenido es el siguiente:

Top 10 IPs destino

pos	paquetes	ip destino
1	34986	29.181.234.168
2	3881	84.98.180.17
3	3785	43.173.78.150
4	2857	12.184.227.62
5	1273	30.123.185.189
6	1046	119.25.90.131
7	983	12.120.218.2
8	666	48.110.121.14
9	664	14.115.82.222
10	619	40.168.48.112

Podemos ver que la mayoría de los paquetes se dirigen a la IP 29.181.234.168. Nuestra IP (119.25.90.131) se encuentra en la sexta posición

Top 10 IPs origen

pos	paquetes	ip origen
1	15454	84.98.180.17
2	11463	29.181.234.168
3	5805	12.184.227.62
4	4657	30.123.185.189
5	2906	12.120.218.2
6	2188	80.42.58.249
7	2161	48.110.121.14
8	2048	51.144.208.175
9	1883	119.25.90.131
10	1652	40.168.48.112

En este caso, la IP que genera el mayor número de paquetes es la 84.98.180.17. Nuestra IP se encuentra en la novena posición.

Top 10 Puertos TCP destino

pos	paquetes	puerto tcp destino
1	12342	80
2	5486	55934
3	4313	55860
4	3204	55865
5	2188	43585
6	1883	54615
7	1813	33896
8	1717	55173
9	1396	55848
10	1174	46371

Se puede apreciar que el puerto que recibe el mayor tráfico es el puerto 80, asociado al protocolo HTTP. Esto nos confirma la observación de que los usuarios se dedican a la navegación en páginas web con este protocolo.

Top 10 Puertos TCP origen

pos	paquetes	puerto tcp origen
1	36640	80
2	1423	55934
3	1096	55860
4	1046	54615
5	617	55865
6	607	43585
7	603	33896
8	471	55173
9	418	55848
10	380	33903

En el caso de los puertos de origen, de nuevo destaca ampliamente el puerto 80, reforzando aún más nuestra hipótesis.

Top 10 Puertos UDP destino

pos	paquetes	puerto udp destino
1	3785	27884
2	591	53
3	134	5355
4	124	547
5	95	5353
6	42	1900
7	2	5035
8	2	12013
9	1	9920
10	1	9800

La mayoría de paquetes UDP se dirigen al puerto 27884, el cual no hemos podido relacionar con ningún servicio conocido. Sin embargo, en segunda posición se encuentra el puerto 53, asociado al Sistema de Nombres de Dominio (DNS), encargado (entre otras cosas) de “traducir” las URL’s

de las páginas web a IP's con las que poder establecer conexión. De nuevo, estamos reforzando la hipótesis de una navegación estándar en la web.

Top 10 Puertos UDP origen

pos	paquetes	puerto udp origen
1	3785	48883
2	592	53
3	124	546
4	95	5353
5	12	1900
6	6	63423
7	6	58532
8	6	55421
9	6	49169
10	3	61153

En el caso de los puertos de origen, podemos ver que el más recurrido es el 48883, mientras que nuestro puerto referencia (27884) no aparece en la lista. Más adelante veremos que no se generan paquetes con origen en este puerto.

2.3 TOPS 10 POR BYTES

Top 10 IPs destino

pos	tamaño	ip destino
1	50345203	29.181.234.168
2	2853122	12.184.227.62
3	1816645	43.173.78.150
4	249160	84.98.180.17
5	115206	14.115.82.222
6	79229	30.123.185.189
7	76301	119.51.200.125
8	70017	119.25.90.131
9	59576	12.120.218.2
10	47886	48.110.121.14

Pese a que la primera posición se mantiene, nuestra dirección IP se ve relegada a la octava posición. Esto nos hace pensar que los paquetes que llegan a nuestra IP son de pequeño tamaño. El tamaño total de los paquetes enviados a la IP que encabeza la lista es casi 20 veces mayor que el segundo. Esta relación aumenta frente al número de paquetes, que equivale a casi 10 veces el de la segunda posición. Por ello es fácil concluir que los paquetes enviados a la IP 29.181.234.168 son de gran tamaño en general.

Top 10 IPs origen

pos	tamaño	ip origen
1	23098523	84.98.180.17
2	6918040	30.123.185.189
3	4344112	12.120.218.2
4	3245100	80.42.58.249
5	3193577	48.110.121.14
6	3009353	51.144.208.175
7	2730262	119.25.90.131
8	2473818	40.168.48.112
9	1970587	12.184.227.62
10	1025537	29.181.234.168

En este caso, la primera posición se mantiene invariante mientras que nuestra IP ha avanzado dos posiciones. Podemos concluir que los paquetes enviados desde nuestra IP son, relativamente, de mayor tamaño que los enviados desde otras direcciones.

Top 10 Puertos TCP destino

pos	tamaño	puerto tcp destino
1	8236507	55934
2	6437994	55860
3	4808618	55865
4	3245100	43585
5	2730262	54615
6	2707440	33896
7	2566453	55173
8	2072650	55848
9	1756652	46371
10	1690967	57063

Se puede apreciar que el puerto 80 no está en el top 10 por número de bytes. Esto parece indicar que los paquetes destinados a este puerto, pese a ser muchos, son de escaso tamaño. Posiblemente se trate de peticiones a páginas web.

Top 10 Puertos TCP origen

pos	tamaño	puerto tcp origen
1	52857665	80
2	217800	443
3	88065	55934
4	70017	54615
5	67367	55860
6	40574	55865
7	36512	43585
8	35533	33896
9	28338	55173
10	26382	46832

En esta imagen volvemos a tener de nuevo al puerto 80 como el más recurrente. El hecho de que los paquetes originados en este puerto sean también los que acumulen el mayor número

de bytes puede hacernos pensar que haya algún servidor transmitiendo contenido web HTTP (por ejemplo, algún servicio Apache).

Top 10 Puertos UDP destino

pos	tamaño	puerto udp destino
1	1816645	27884
2	46391	53
3	23317	5353
4	18337	547
5	12015	1900
6	11460	5355
7	533	12013
8	461	5035
9	394	64925
10	318	23710

Al igual que en la ordenación por paquetes, la primera posición la ocupa nuestro puerto: el 27884. De nuevo, el puerto 53, asociado al DNS, se encuentra en la segunda posición.

Top 10 Puertos UDP origen

pos	tamaño	puerto udp origen
1	1816645	48883
2	85720	53
3	23317	5353
4	18337	546
5	6447	1900
6	1080	63423
7	1080	58532
8	1080	55421
9	1080	49169
10	624	61153

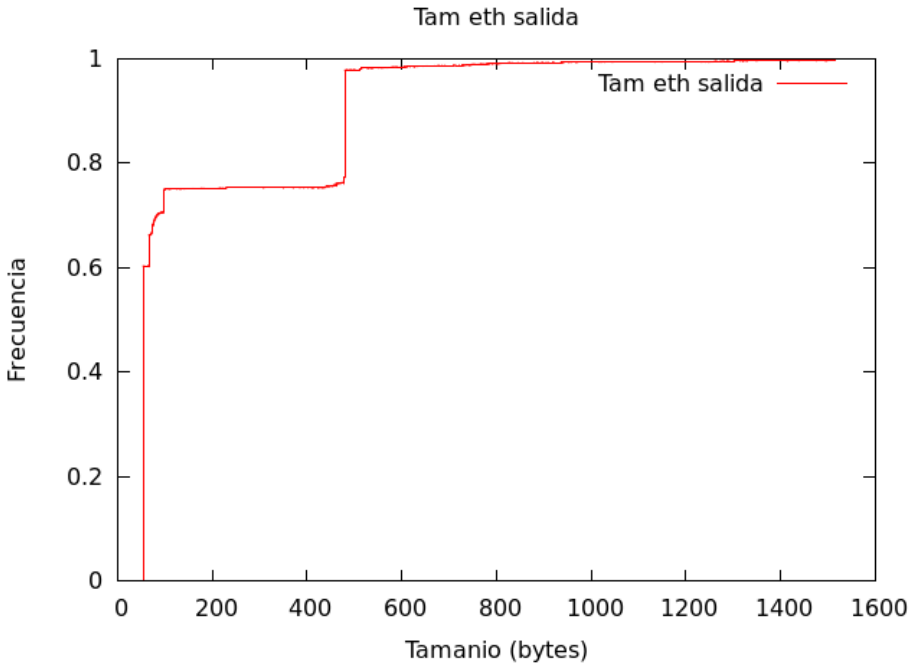
En el caso de los puertos de origen, podemos ver que el más recurrido es el 48883, mientras que nuestro puerto referencia (27884) no aparece en la lista. Más adelante veremos que no se generan paquetes con origen en este puerto.

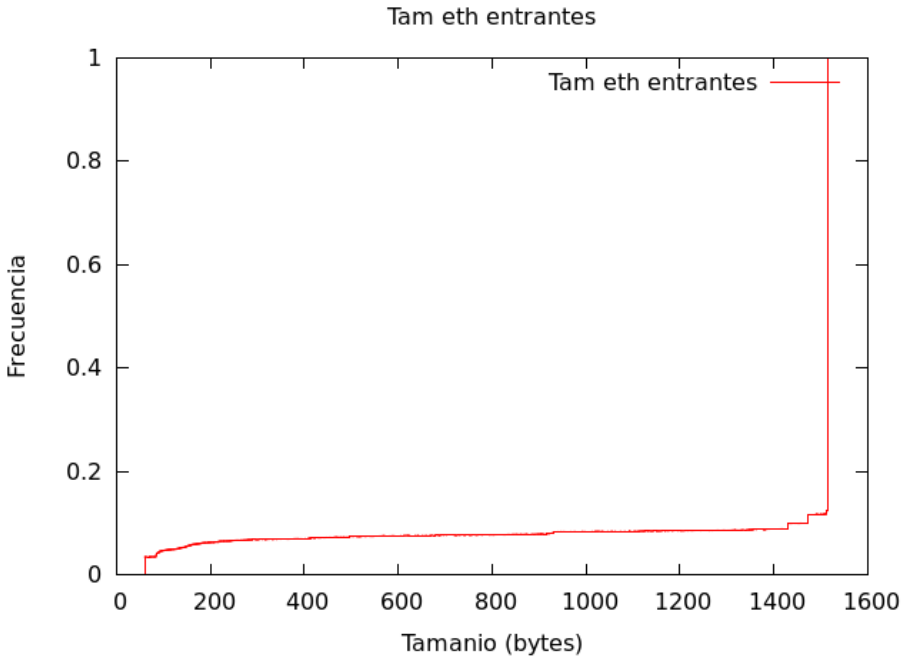
2.4 ECDF'S

En este apartado analizamos las diferentes gráficas ECDF que se nos solicitaba. Para ello hemos realizado diversas consultas *tshark*, para posteriormente analizarlas mediante *awk* y obtener las frecuencias acumuladas para las ECDF en los script *hacer_ECDF_...sh*

tshark -r traza.pcap -T fields -e frame.len -e eth.src -e eth.dst -Y "eth.addr=00:11:88:CC:33:E5"

Con esta consulta obtenemos el tamaño de los paquetes que utilizan nuestra dirección MAC como origen o destino, y separamos ambos casos usando *awk*. El resultado es el siguiente:





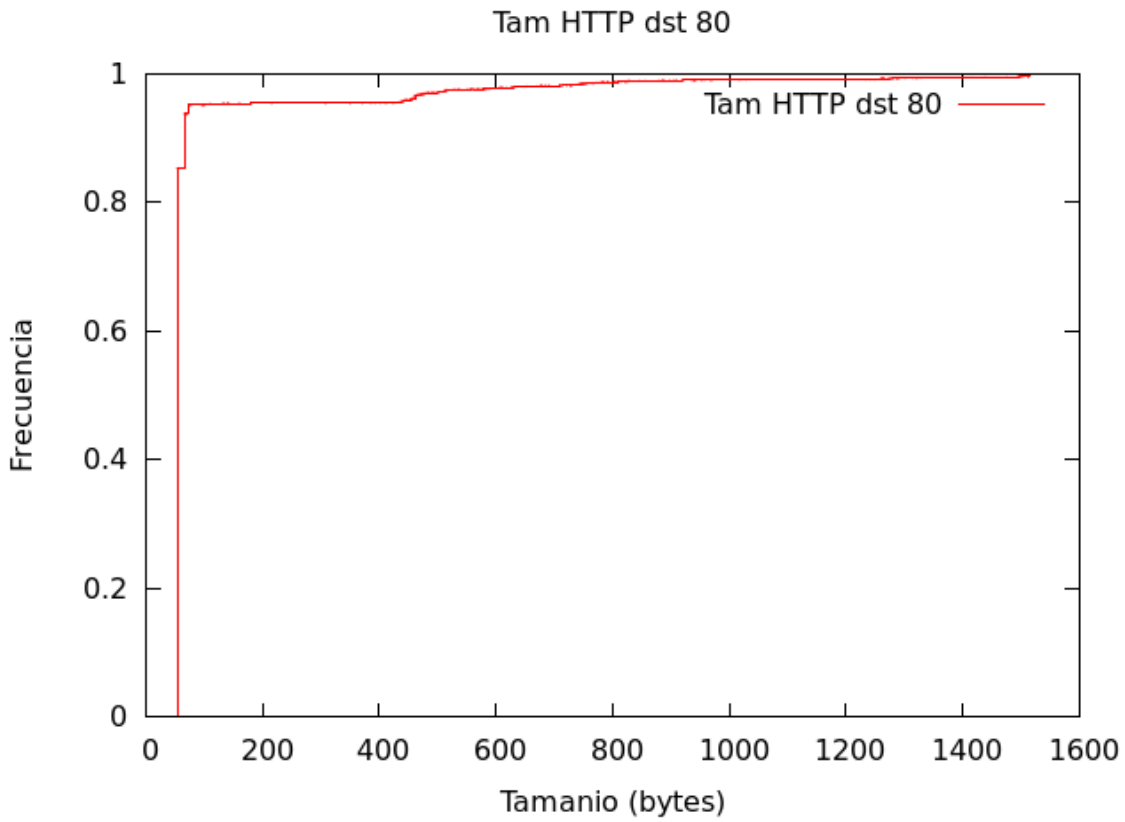
En el caso de los paquetes entrantes (dirigidos a nuestra MAC), podemos ver que la inmensa mayoría tiene un tamaño alrededor de los 1500 Bytes. Hay menos de un 10% con un tamaño inferior. Sin embargo, viendo la gráfica de los paquetes originados en nuestra dirección, vemos que cerca del 80% tienen un tamaño inferior a 200 Bytes y que, además, hay un considerable número de paquetes de tamaño cercano a los 500 Bytes.

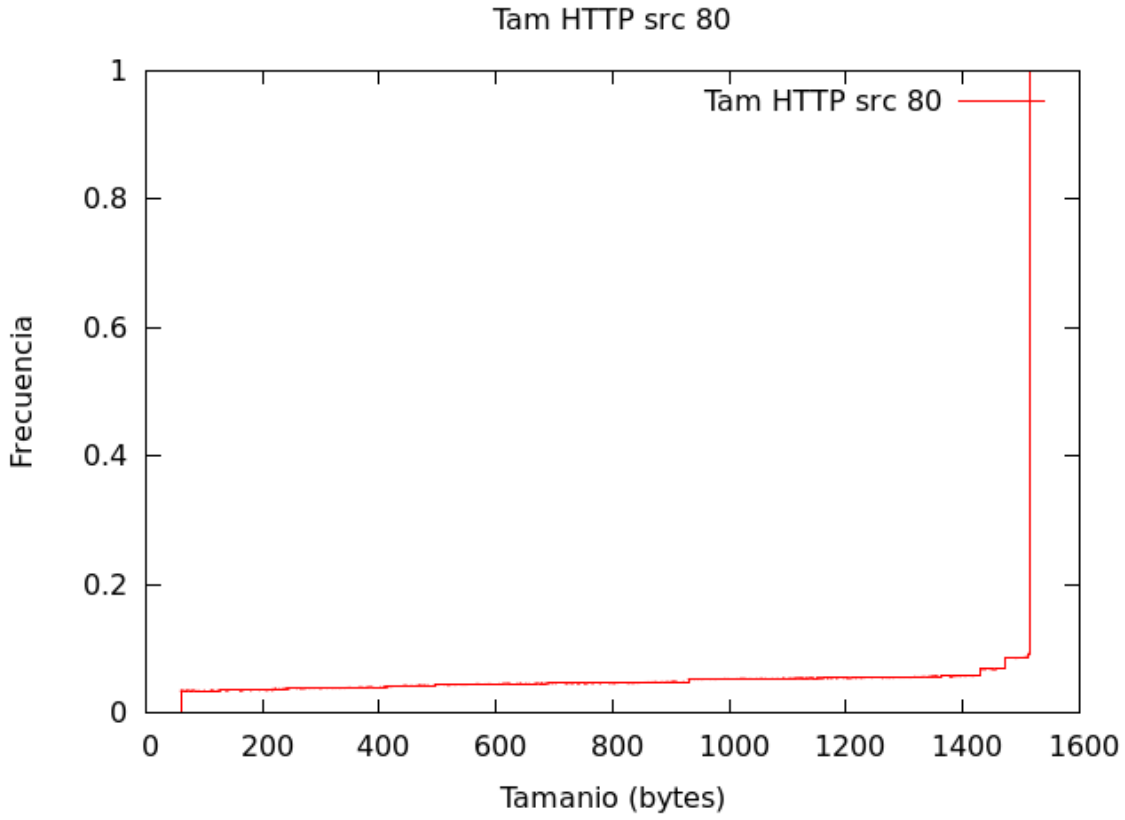
tshark -r traza.pcap -T fields -e frame.len -e tcp.srcport -e tcp.dstport

Con esta consulta obtenemos el tamaño de los paquetes TCP y vamos a quedarnos sólo con los HTTP (aquellos que empleen el puerto 80) mediante comandos *awk*.

awk -v port=80 '$2 == port {print $1}' (con origen en el puerto 80)

awk -v port=80 '$3 == port {print $1}' (con destino el puerto 80)





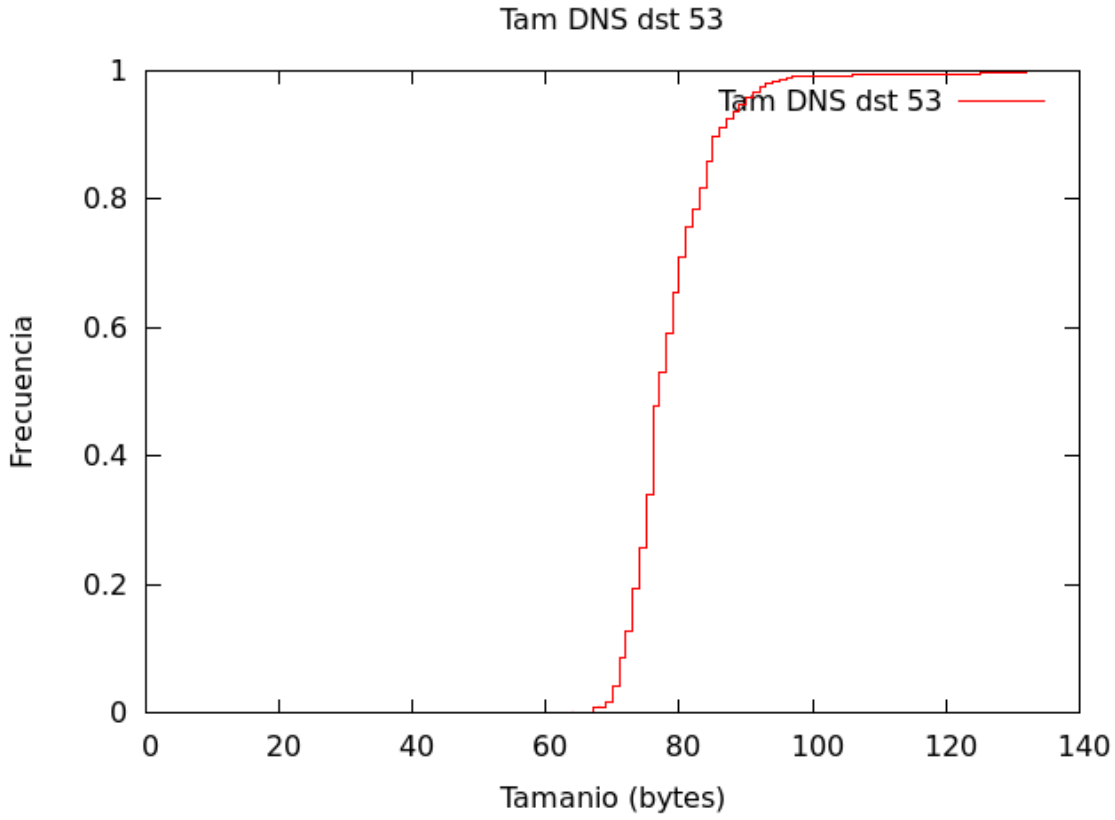
Podemos ver que más del 90% de los paquetes HTTP dirigidos a nuestra dirección tienen un tamaño inferior a 200 Bytes, mientras que los originados en dicha dirección son, en su mayoría, de un tamaño cercano a los 1500 Bytes. De nuevo, esto nos hace pensar que tratamos con paquetes originados en algún tipo de servidor que recibe muchos paquetes de pequeño tamaño (peticiones) y sirve paquetes de gran tamaño, que serán el contenido del web.

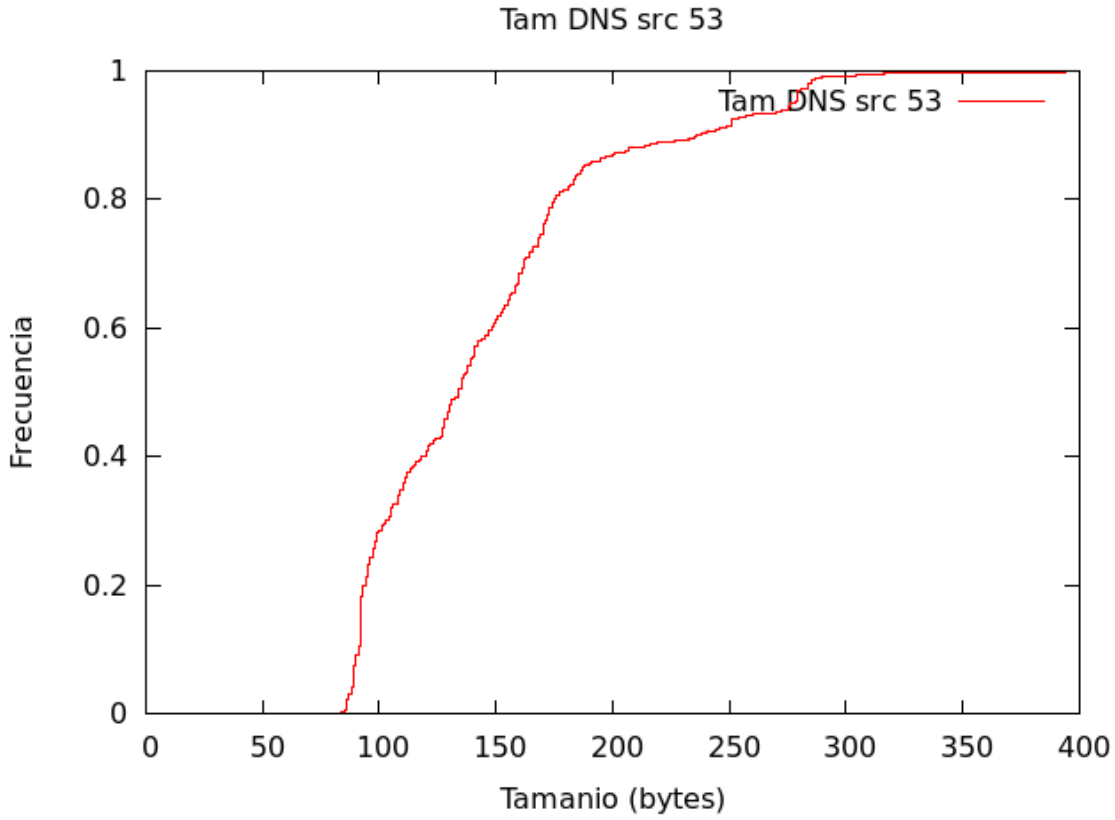
tshark -r traza.pcap-T fields -e frame.len -e udp.srcport -e udp.dstport

Con esta consulta obtenemos el tamaño de los paquetes UDP y vamos a quedarnos sólo con los DNS (aquellos que empleen el puerto 53) filtrando mediante *awk.*

awk -v port=53 '$2 == port {print $1}' (con origen en el puerto 53)

awk -v port=53 '$3 == port {print $1}' (con destino el puerto 53)





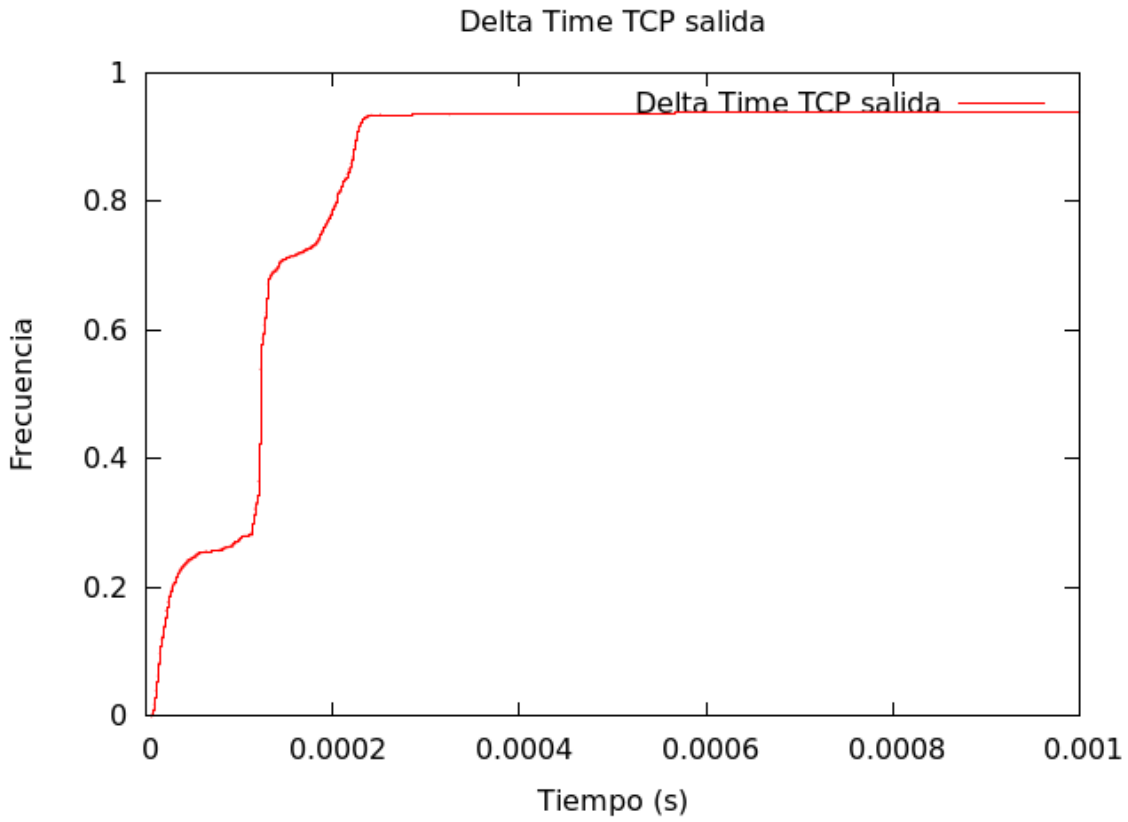
En el caso de los paquetes DNS entrantes, observamos una distribución logarítmica de los datos, de forma que la mayoría de paquetes tienen un tamaño de entre 70 y 100 Bytes. Si nos fijamos en los paquetes salientes, la distribución es ligeramente similar, aunque menos estable, y en

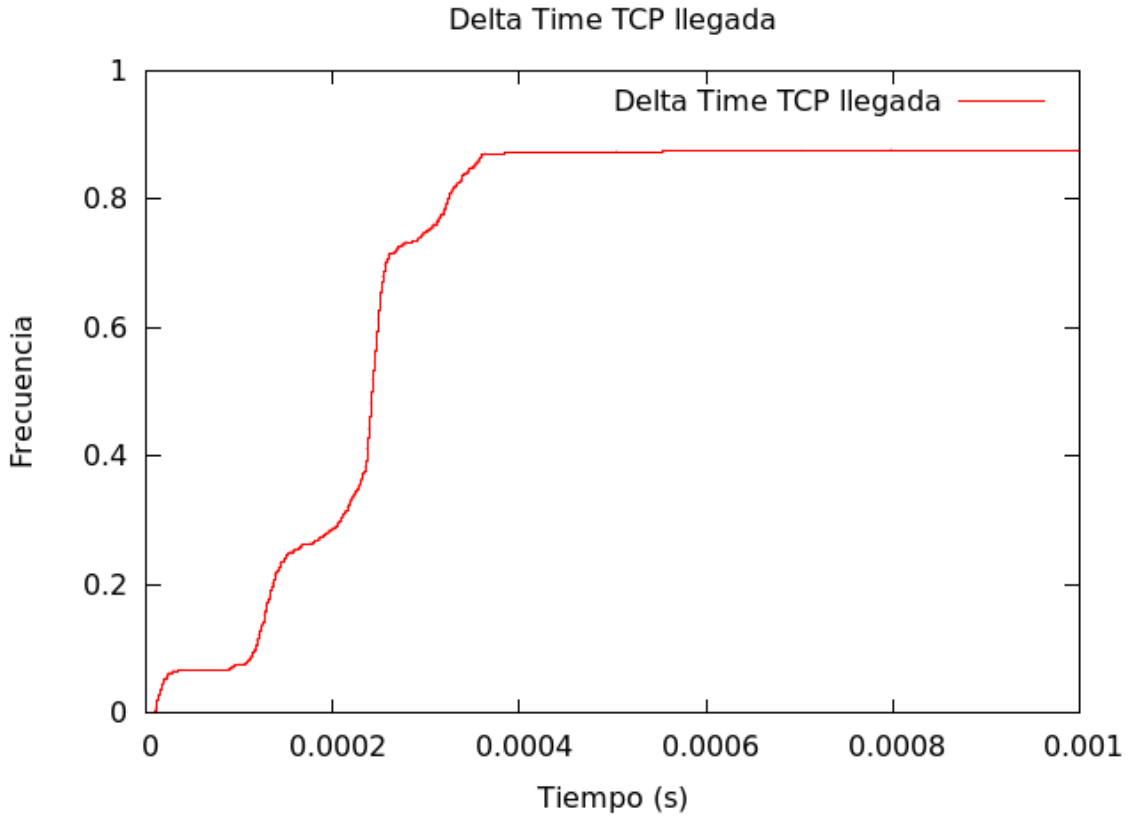
este caso los tamaños se reparten entre los 70 Bytes y los 300 Bytes. Viendo que los paquetes que salen son de mayor tamaño que los de entran, se puede suponer que se están realizando *querys* y *responses* DNS, ya que los paquetes de pequeño tamaño se pueden asociar a peticiones DNS, mientras que los de mayor tamaño pueden asociarse a respuestas que incluyan la dirección asociada al nombre solicitad0.

tshark -r traza.pcap-T fields -e frame.time_relative -e ip.src -e ip.dst -Y 'tcp'

Con esta consulta obtenemos los tiempos absolutos de todos los paquetes TCP. Mediante comandos *awk* vamos a filtrar aquellos que tienen nuestra IP como origen/destino y luego vamos a calcular el tiempo entre paquetes.

awk 'BEGIN{antigua = $1} {delta = $1-antigua; printf("%.7f\n", delta); antigua = $1 }' (ejemplo de comando *awk* para calcular el tiempo relativo entre paquetes)



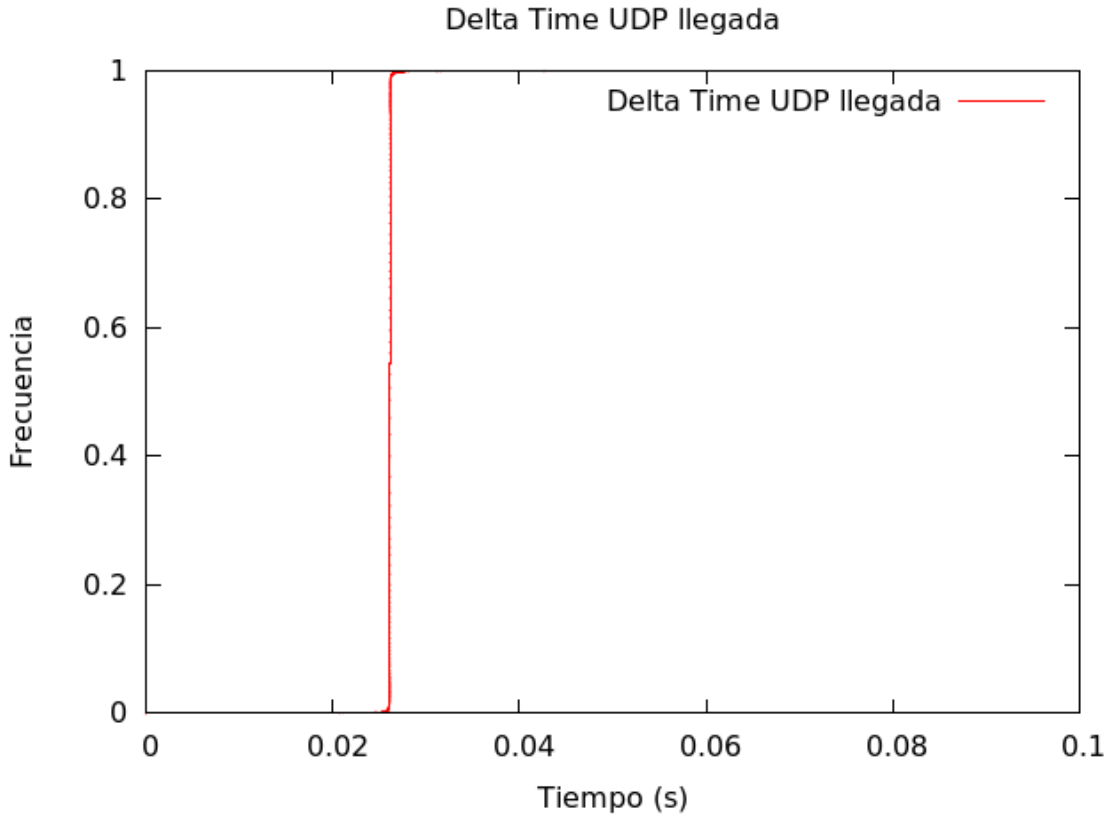


Se puede ver que, en el caso de los paquetes entrantes, hay ciertas oscilaciones hasta los 0.0004 nanosegundos donde ya se estabiliza, lo que quiere decir que más del 80% de los paquetes tienen una diferencia de tiempo menor a 0.0004. Por motivos visuales, nuestra gráfica no alcanza la frecuencia total, sino que se queda en 0.9. Esto se debe a que, si aumentamos el rango de tiempos, no podemos apreciar correctamente las oscilaciones que tienen lugar antes de los 0.004 nanosegundos.

En el caso de los paquetes salientes, tenemos unas oscilaciones muy similares, que llegan hasta poco más de los 0.0002 nanosegundos. En este caso, algo más del 90% de los paquetes tienen una diferencia de tiempo menor que 0.0003 nanosegundos.

tshark -r traza.pcap-T fields -e frame.time_relative -e udp.srcport -e udp.dstport -Y 'udp.port == 27884'

Con esta consulta obtenemos los tiempos absolutos de los paquetes UDP que utilizan el nuestro puerto. De la misma forma que en el caso anterior, usaremos *awk* para separar entre tráfico entrante y saliente y calcular el tiempo relativo entre paquetes, obteniendo los siguientes resultados:



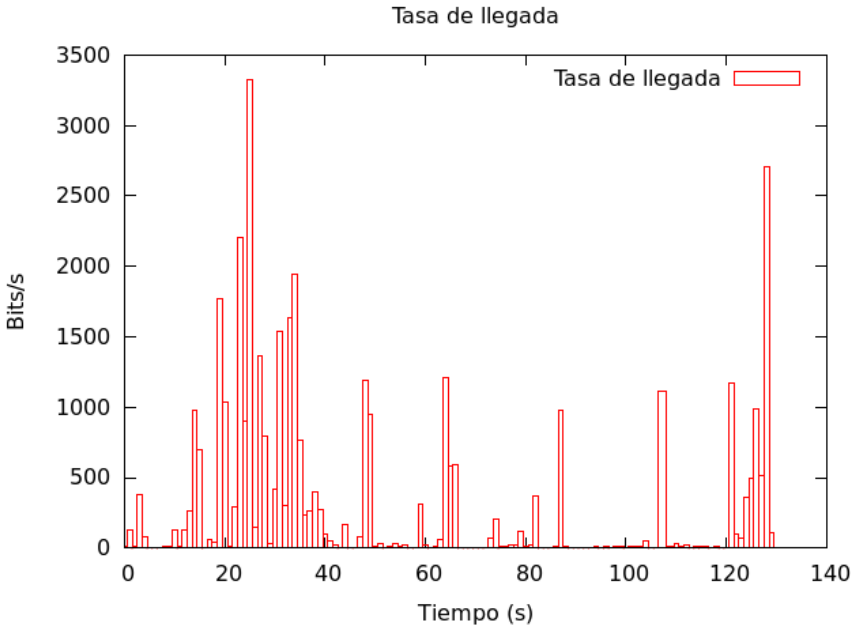
Se puede ver que el tiempo entre los paquetes entrantes es muy similar, del orden de 0.02 nanosegundos, en todos los casos. Sin embargo, no hay paquetes UDP cuyo origen sea nuestro puerto.

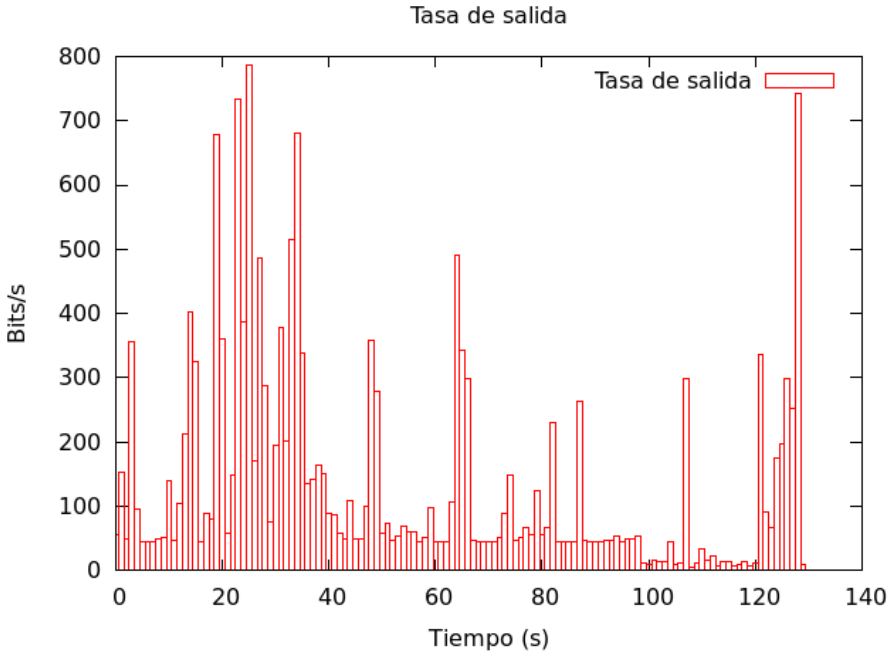
2.3 Tasa de transferencia

Para hallar la tasa de transferencia cada segundo, utilizamos:

tshark -r traza.pcap -T fields -e frame.len -e frame.time_relative -e eth.src -e eth.dst -Y "eth.addr==00:11:88:cc:33:e5"

Luego utilizaremos awk para truncar el tiempo, quedándonos sólo con la parte entera y se lo pasaremos a hacer-grafica_tasa.sh con los parámetros adecuados.





Podemos apreciar que la tasa de llegada de nuestra MAC es significativamente más alta que la tasa de salida. Esto puede indicar que dicho dispositivo ha sido utilizado para navegar por la web, de manera que los paquetes salientes son peticiones a páginas web y los paquetes recibidos son la respuesta por el servidor que nos envía el contenido de la página.

3. Conclusiones

Tras el análisis completo de la traza proporcionada, podemos realizar una serie de suposiciones acerca del tráfico presentado.

1) No hay indicios de la realización o recepción de alguna clase de streaming debido al escaso tráfico UDP.
2) La mayoría del tráfico es mediante el protocolo IP-TCP-HTTP, por lo que podemos suponer que el usuario ha utilizado su navegador para acceder a páginas web.
3) La MAC proporcionada tiene más tasa de llegada que de salida, por lo que es un terminal de usuario, no un servidor.