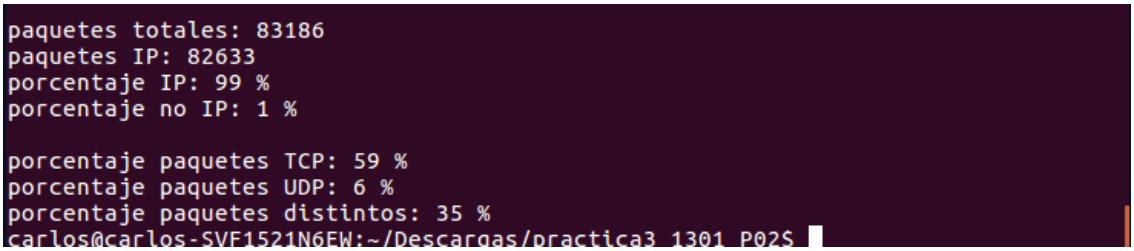
Memoria de la Práctica 3

REDES I

Javier Gómez Martínez
Carlos Li Hu

Introducción
En esta práctica nos vamos a dedicar a calcular estadísticas de una cierta traza que se genera de forma aleatoria en base a nuestro número de grupo (1301) y de pareja (2), y en base a esas estadísticas, analizaremos el tráfico que está soportando esta red.

1. **Porcentajes de paquetes (puede incluir una captura de pantalla) (punto 1 de los requisitos):**
   - **IP y NO IP (entendemos como NO-IP aquellos paquetes que no son ni ETH|IP ni ETH|VLAN|IP)**
   - **UDP, TCP, OTROS sobre los que son IP (igualmente entienda, un paquete IP como aquel que cumpla la pila ETH|IP o ETH|VLAN|IP).**



Aquí podemos observar la salida del script, donde vemos que el 99% de los paquetes son IP. Esto tiene sentido porque en general en una red de tráfico de paquetes, el protocolo IP más usado es el IP

Dentro de los paquetes IP, el 59% son TCP, el 6% UDP, y el resto de otro tipo. Podemos observar que en general hay más paquetes de TCP que de UDP ya que son paquetes que garantizan que no se pierdan los paquetes, y por tanto es más común en ámbitos como la mensajería o la carga de páginas web, mientras que UDP no garantiza que lleguen los paquetes y suele ser más comunes para contenidos multimedia.

2. **Top 10 de direcciones IP activas (en bytes y paquetes) y top 10 de puertos (en bytes y paquetes) (una captura de pantalla puede ser suficiente).**

Aquí mostramos los resultados del script para los diferentes tops 10 según el criterio que corresponda en cada apartado.

- **Top 10 direcciones IP**
  - **En paquetes**

Frecuencia absoluta	**Dirección IP**
46449	12.14.4.254
36112	58.0.213.157

19335	66.192.174.206
5930	11.80.183.30
3889	121.204.81.199
3785	89.111.170.236
2929	36.173.217.43
2827	30.123.185.189
2795	126.11.165.241
2567	33.91.43.101

- **En bytes**

Tamaño en bytes	**Dirección IP**
51370740	12.14.4.254
23347683	66.192.174.206
6997269	11.80.183.30
6083924	58.0.213.157
4403688	121.204.81.199
3281612	126.11.165.241
3241463	30.123.185.189
3041083	33.91.43.101
2800279	36.173.217.43
2510891	85.135.176.238

En estos tops 10 de IPs, podemos observar que en general, hay una gran correlación entre las IPs que más paquetes envían y reciben, y los que más bytes envían y reciben, con lo que podemos concluir, que, en esta red, en general, las IPs más activas transmiten y reciben más paquetes y bytes que el resto de IPs de la red.

- **Top 10 puertos**
  - **TCP**
    - **En paquetes**

Frecuencia absoluta	**Puerto**
48996	80
6909	55934
5409	55860
3821	55865
2929	54615
2795	43585
2416	33896
2188	55173
1814	55848
1531	46371

    - **En bytes**

Tamaño en bytes	**Puerto**

53932004	80
8324572	55934
6505361	55860
4849192	55865
3281612	43585
2800279	54615
2742973	33896
2594791	55173
2098831	55848
1778032	46371

En estos tops 10 de puertos TCP observamos un efecto similar al antes mencionado en los IPs, puesto que los puertos que envían y reciben más paquetes, suelen enviar y recibir más bytes.

- **UDP**
  - **En paquetes**

Frecuencia absoluta	**Puerto**
3785	49714
3785	48883
1183	53
4	5035
2	9920
2	9800
2	9545
2	9438
2	9434
2	9108

  - **En bytes**

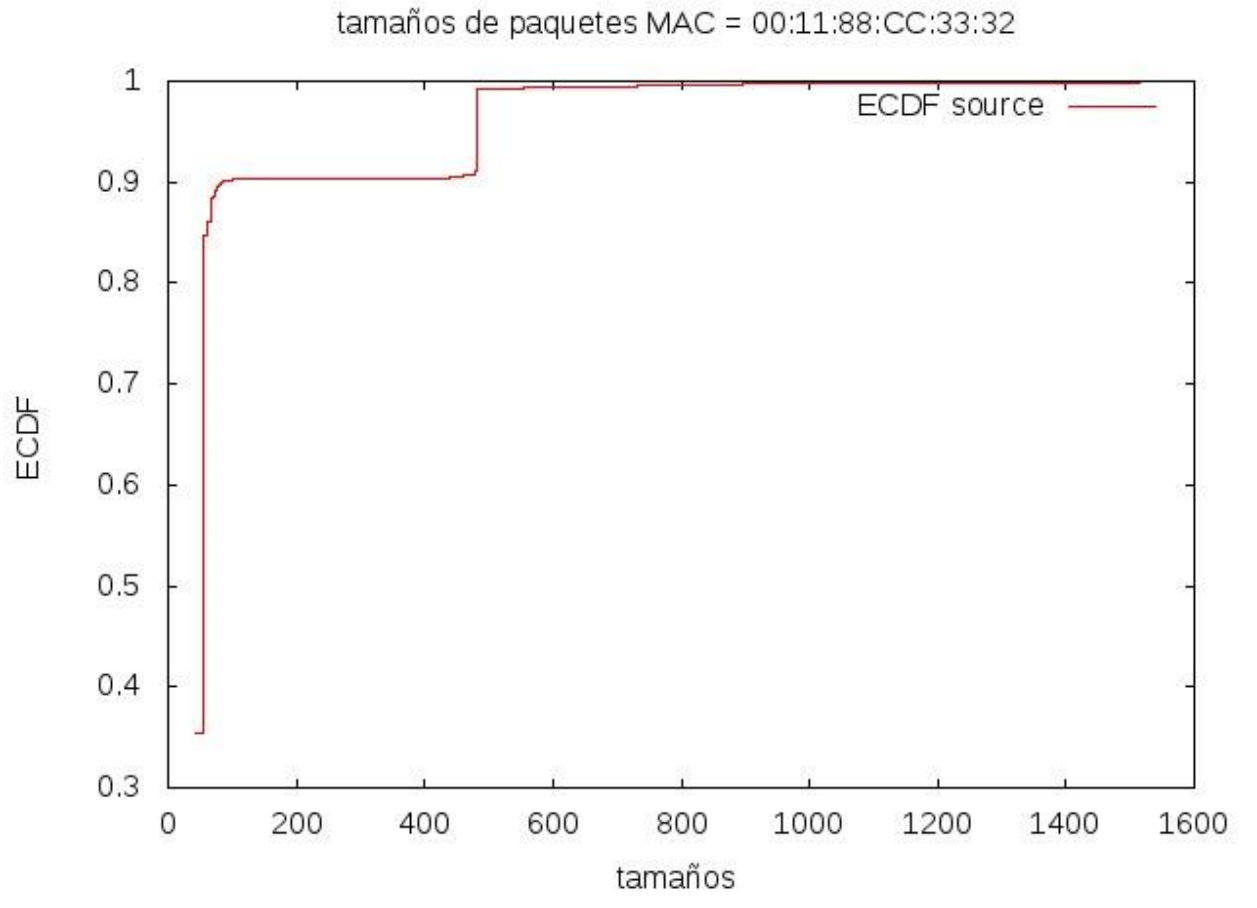
Tamaño en bytes	**Puerto**
1816645	49714
1816645	48883
132111	53
620	5035
404	34968
404	23710
394	64925
388	6844
388	23475
371	37424

En estos tops 10 por ejemplo, podemos observar el patrón que afecta a los casos anteriores, pero sólo en los 4 primeros puertos, pero en el resto, no ocurre puesto que los otros puertos UDP envían o reciben muy pocos paquetes, lo que hace que el número de bytes que envían y reciben sea tan bajo, que la correlación mencionada previamente no se mantiene.

Podemos observar que estos resultados son consistentes con los del ejercicio 1, ya que vemos que en general hay más paquetes (y bytes) de tipo TCP que de UDP, teniendo en cuenta que hay un porcentaje del 59% de paquetes TCP en la red frente al 6% de paquetes UDP.

3. **ECDF de los tamaños a nivel 2 de los paquetes de la traza (una por sentido, utilice la dirección MAC proporcionada por el generador).**

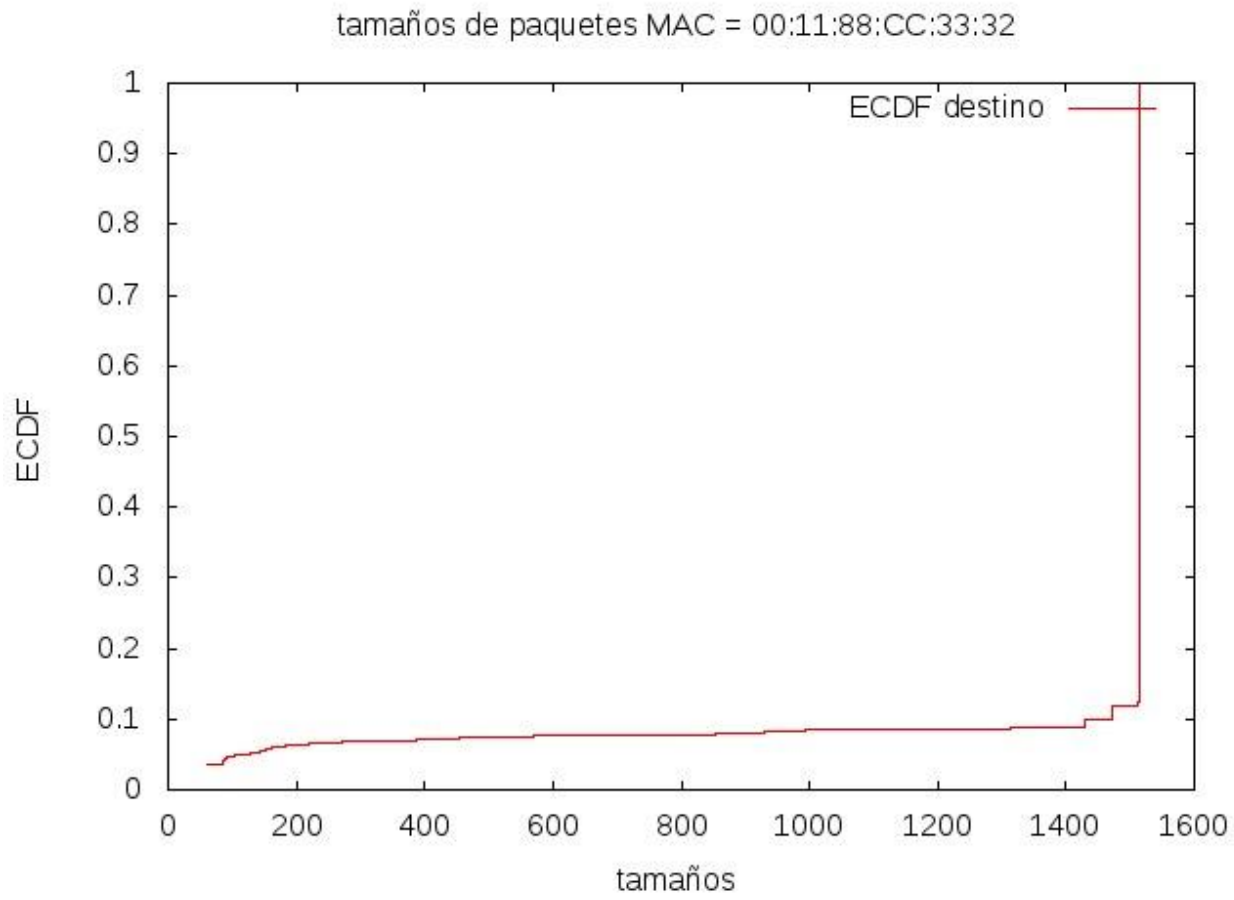
   - **Mac Source = 00:11:88:CC:32:32**



En esta gráfica vemos el ECDF de los tamaños a nivel 2 de los paquetes de la traza siendo el MAC origen el que nos proporcionan.

Podemos observar una tendencia de esta MAC a enviar paquetes en general pequeños, es decir, podemos ver, por ejemplo, cómo el 90% de los paquetes que envía son de tamaño menor a 100B y que prácticamente el 100% de los paquetes que envía son de menos de 500B

- **Mac Destino = 00:11:88:CC:32:32**



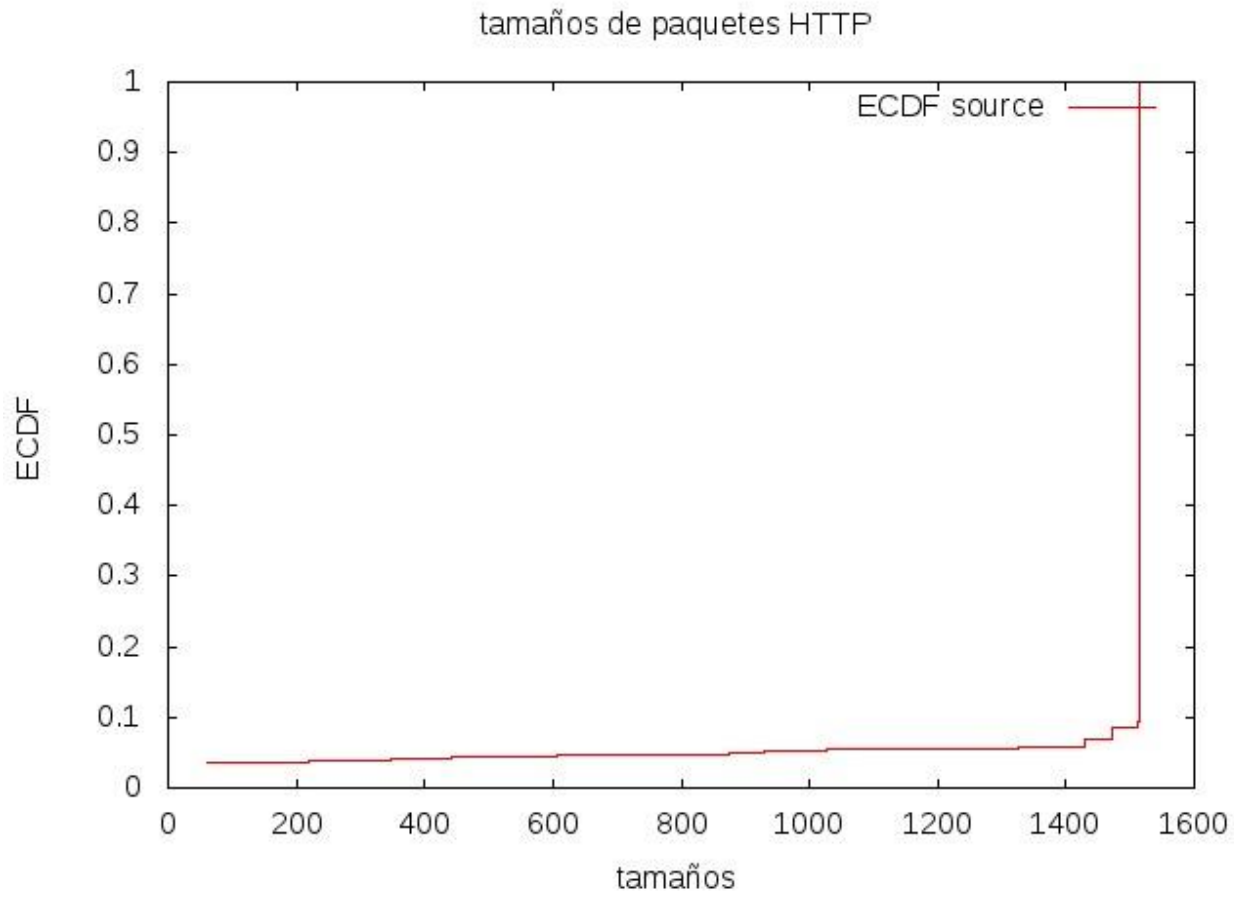
En esta gráfica vemos el ECDF de los tamaños a nivel 2 de los paquetes de la traza siendo el MAC destino el que nos proporcionan.

Podemos observar una tendencia de este MAC a recibir paquetes en generalmente grandes, puesto que sólo el 10% de los paquetes que recibe son de tamaño inferior a 1500B, pero que, a partir de ese valor, el 90% de los paquetes tienen un tamaño superior.

Estas gráficas podrían explicarse si suponemos que esta MAC corresponde a un usuario que envía peticiones a páginas web (paquetes de tamaño pequeño) y recibe las respuestas a dichas peticiones, que al ser contenidos de la página, son paquetes de mayor tamaño.

4. **ECDF de los tamaños a nivel 2 de los paquetes HTTP de la traza (una por sentido a nivel 4). Entenderemos como HTTP todos aquellos paquetes que usen el puerto 80 de TCP en origen o destino.**

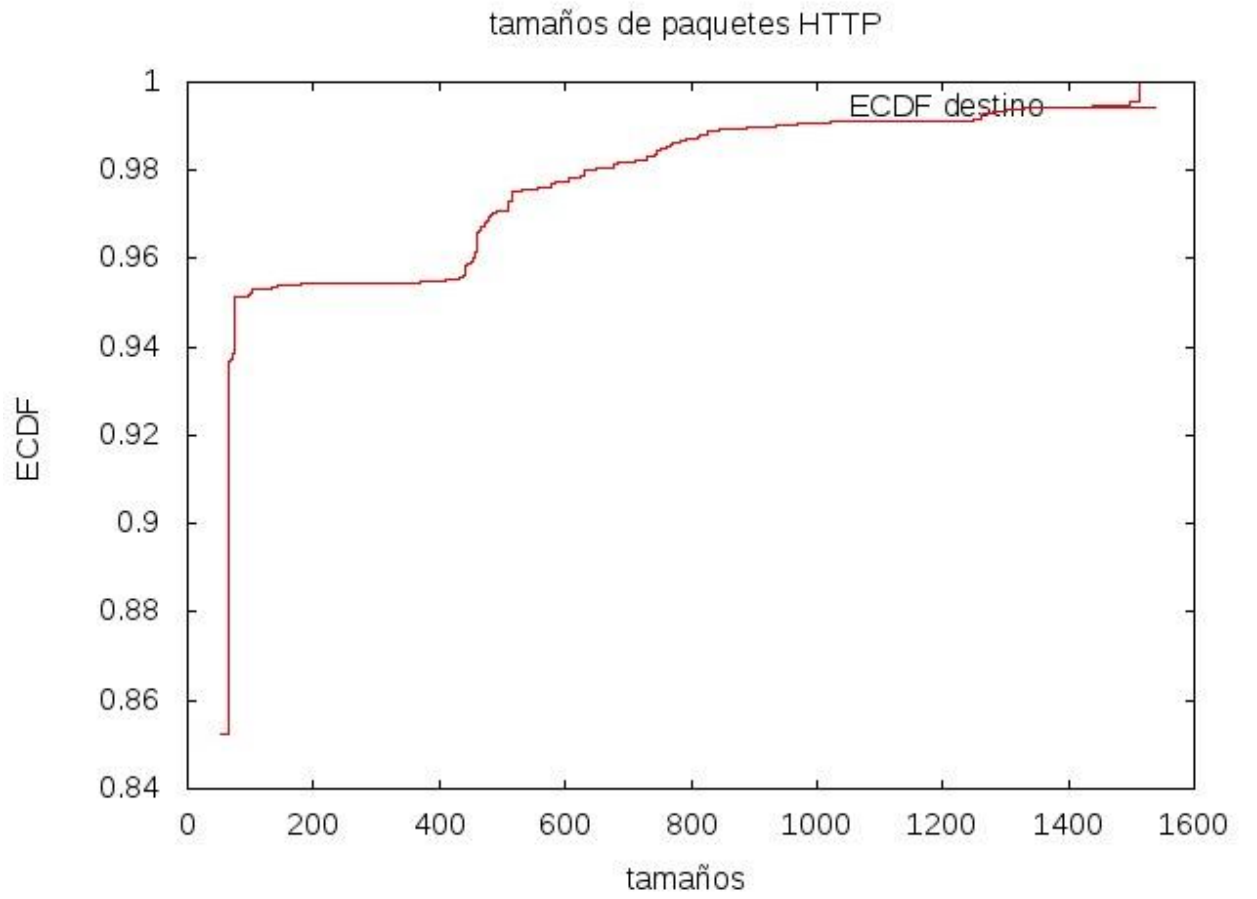
    - **HTTP origen**



En esta gráfica vemos el ECDF de los tamaños a nivel 2 de los paquetes HTTP de la traza usando como puerto origen de TCP el 80.

Podemos observar como sólo el 10% de los paquetes HTTP tienen un tamaño inferior a 1500B, mientras que el 90% restante tienen un tamaño superior a aquel, con lo que se concluye que se envían paquetes de tamaño grande generalmente.

- **HTTP Destino**

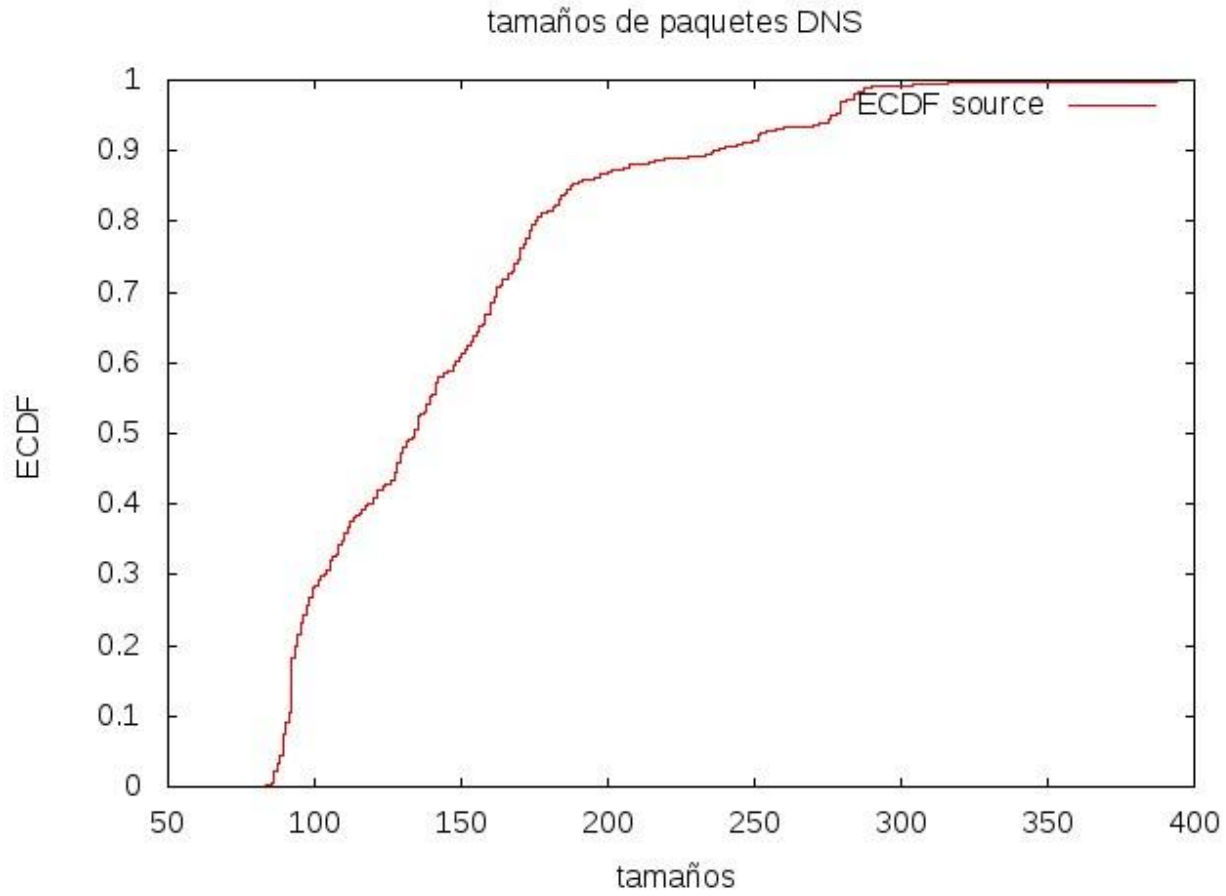


En esta gráfica vemos el ECDF de los tamaños a nivel 2 de los paquetes HTTP de la traza usando como puerto destino de TCP el 80.

En esta en cambio, vemos cómo los paquetes HTTP son generalmente pequeños, el 95% aproximadamente tienen un tamaño inferior a 100B.

5. **ECDF de los tamaños a nivel 2 de los paquetes DNS de la traza (una por sentido a nivel 4). Entenderemos como DNS todos aquellos paquetes que usen el puerto 53 de UDP en origen o destino.**

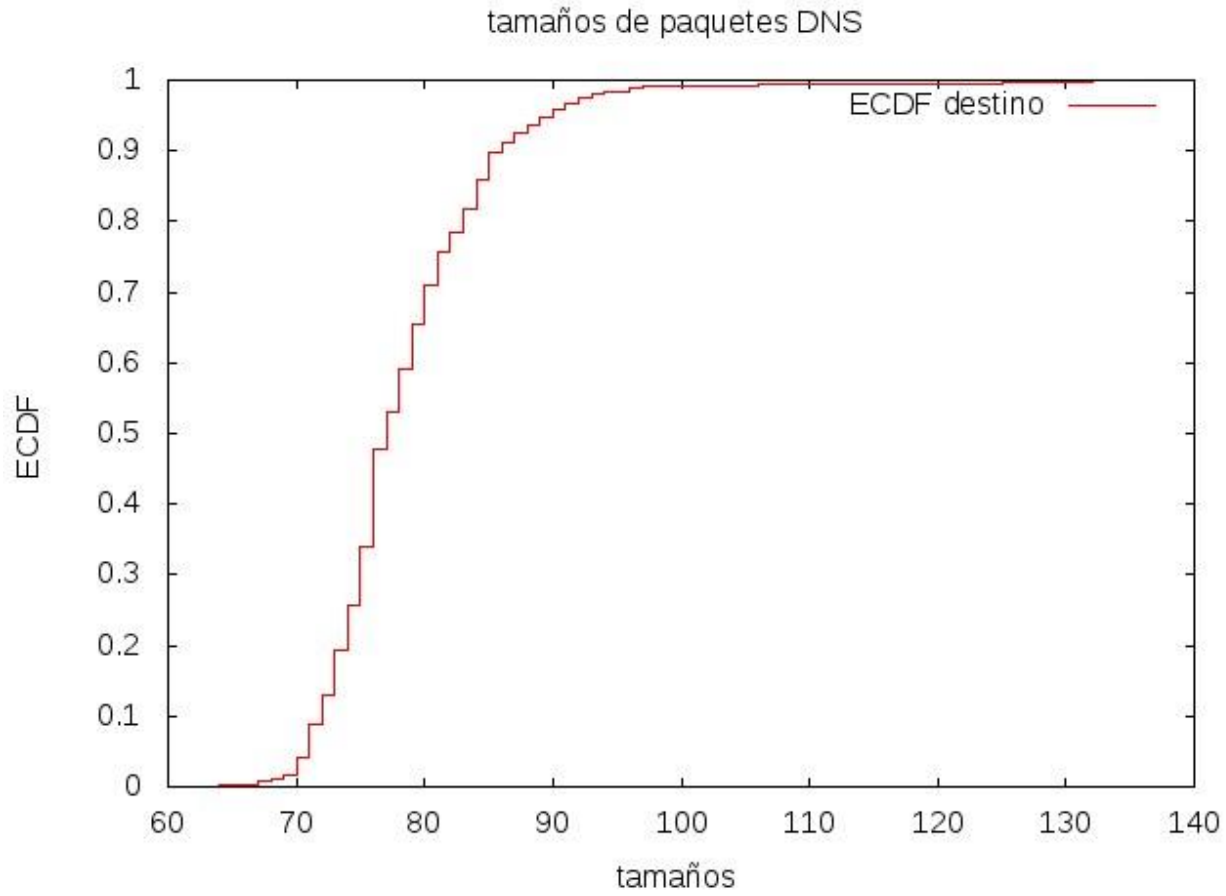
   - **DNS origen**



En esta gráfica vemos el ECDF de los tamaños a nivel 2 de los paquetes DNS de la traza usando como puerto origen de UDP el 53.

Podemos notar cómo aquí los tamaños de paquetes oscilan de forma más o menos uniforme entre 70 y 300B, dando a entender que los paquetes DNS enviados son en general pequeños.

- **DNS destino**



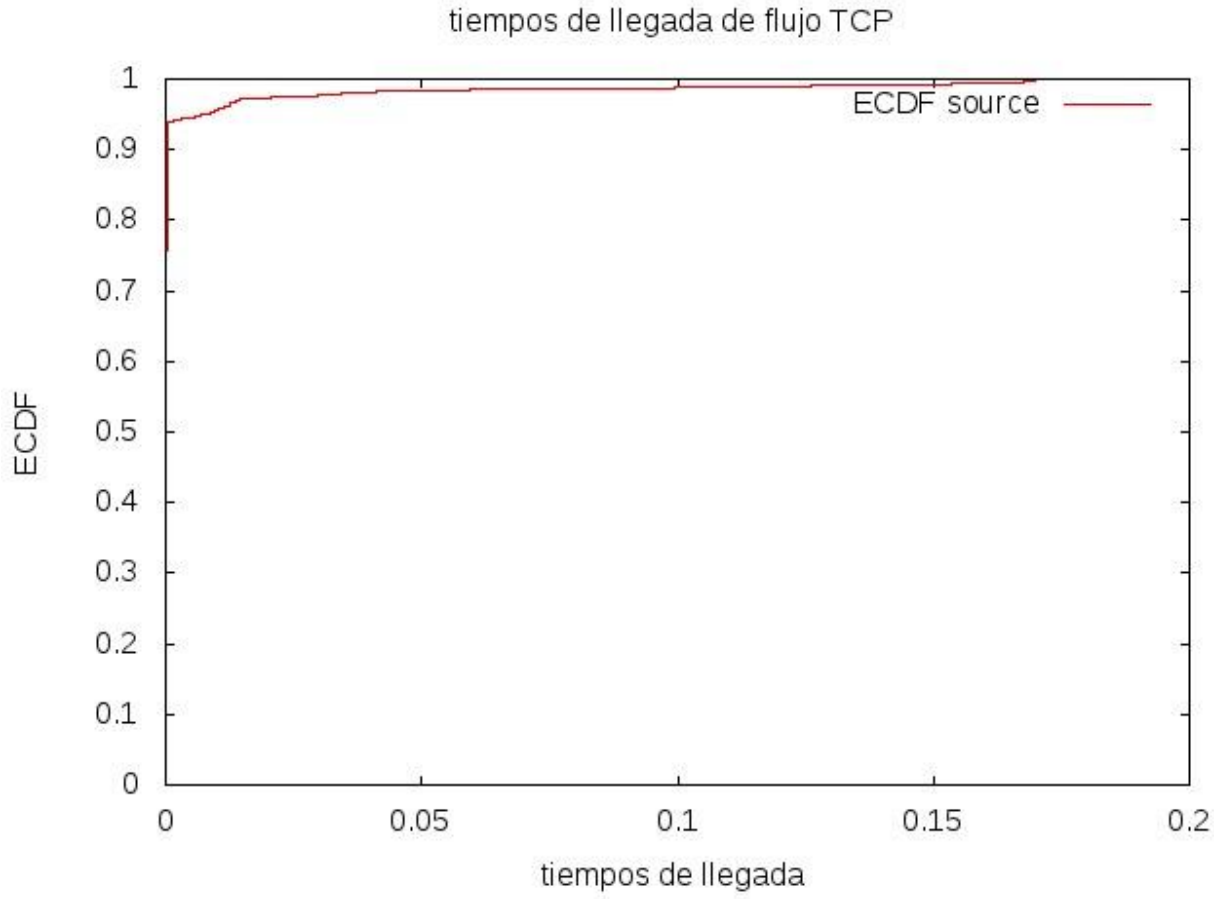
En esta gráfica vemos el ECDF de los tamaños a nivel 2 de los paquetes DNS de la traza usando como puerto destino de UDP el 53.

Aquí en cambio, vemos cómo los paquetes que se envían al puerto destino son de entre 60 y 100 B mayormente, siendo aún más pequeños que los del puerto origen.

En general los paquetes DNS son pequeños, por la naturaleza de este protocolo, ya que su propósito principal es el envío de paquetes que contienen URLs a internet y que se reciba un paquete que contenga la IP asociada a esa URL.

6. **ECDF de los tiempos entre llegadas del flujo TCP indicado por el generador de la traza (una por sentido a nivel 4).**

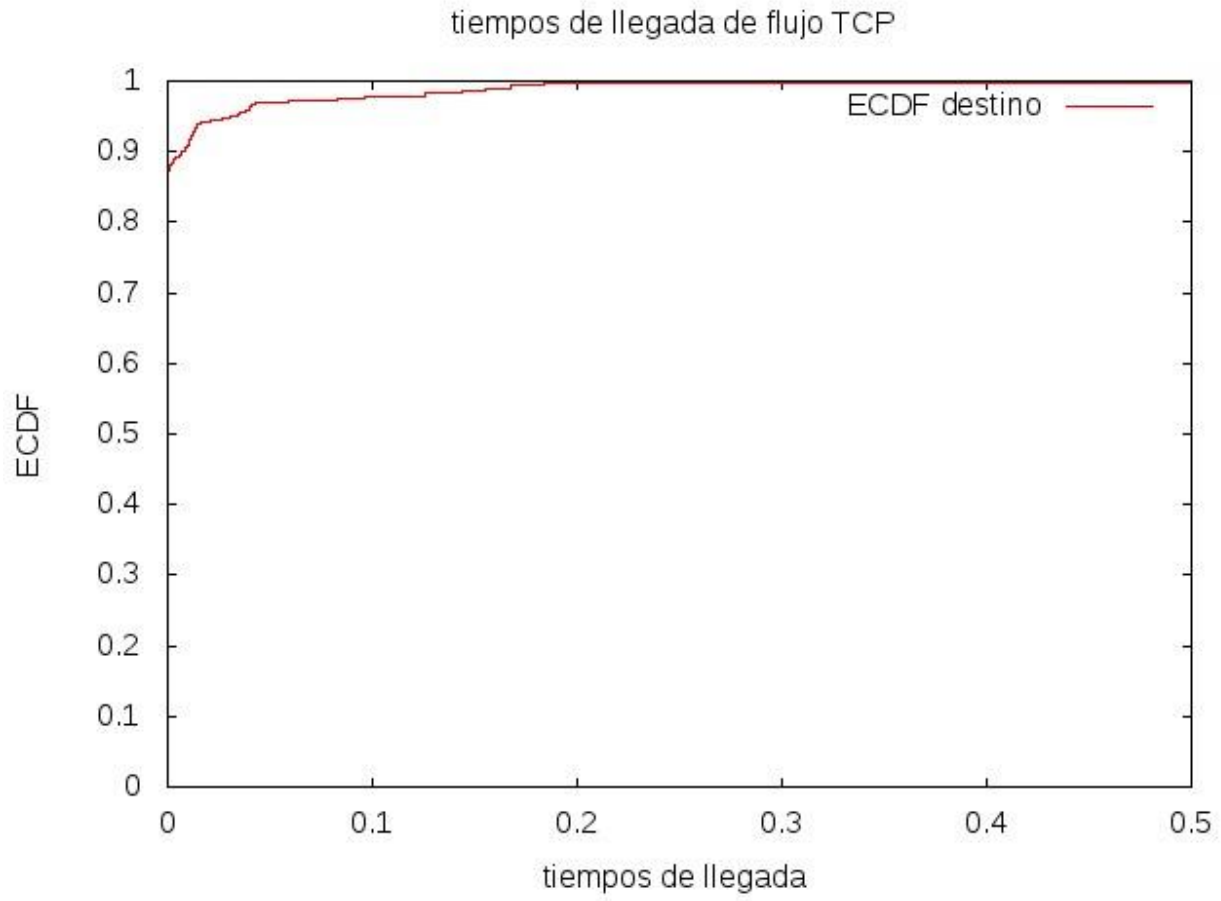
   - **Tiempos entre llegadas del flujo TCP usando como IP origen `36.173.217.43`.**



En esta gráfica vemos el ECDF de los tiempos de llegada del flujo TCP de la traza usando como IP origen `36.173.217.43`.

Hemos ampliado la gráfica para poder ver donde se da el mayor crecimiento de la ECDF, notando que los tiempos de llegada son en general muy cercanos a 0s, empezando casi en 0 el 80% de las veces, y siendo todos menores a 0.2s

- **Tiempos entre llegadas del flujo TCP usando como IP destino `36.173.217.43`.**



En esta gráfica vemos el ECDF de los tiempos de llegada del flujo TCP de la traza usando como IP destino `36.173.217.43`.

Hemos ampliado la gráfica para poder ver donde se da el mayor crecimiento de la ECDF, aquí vemos cómo casi el 90% de los paquetes llegan en casi 0s y en menos de 0.5s casi todos los paquetes

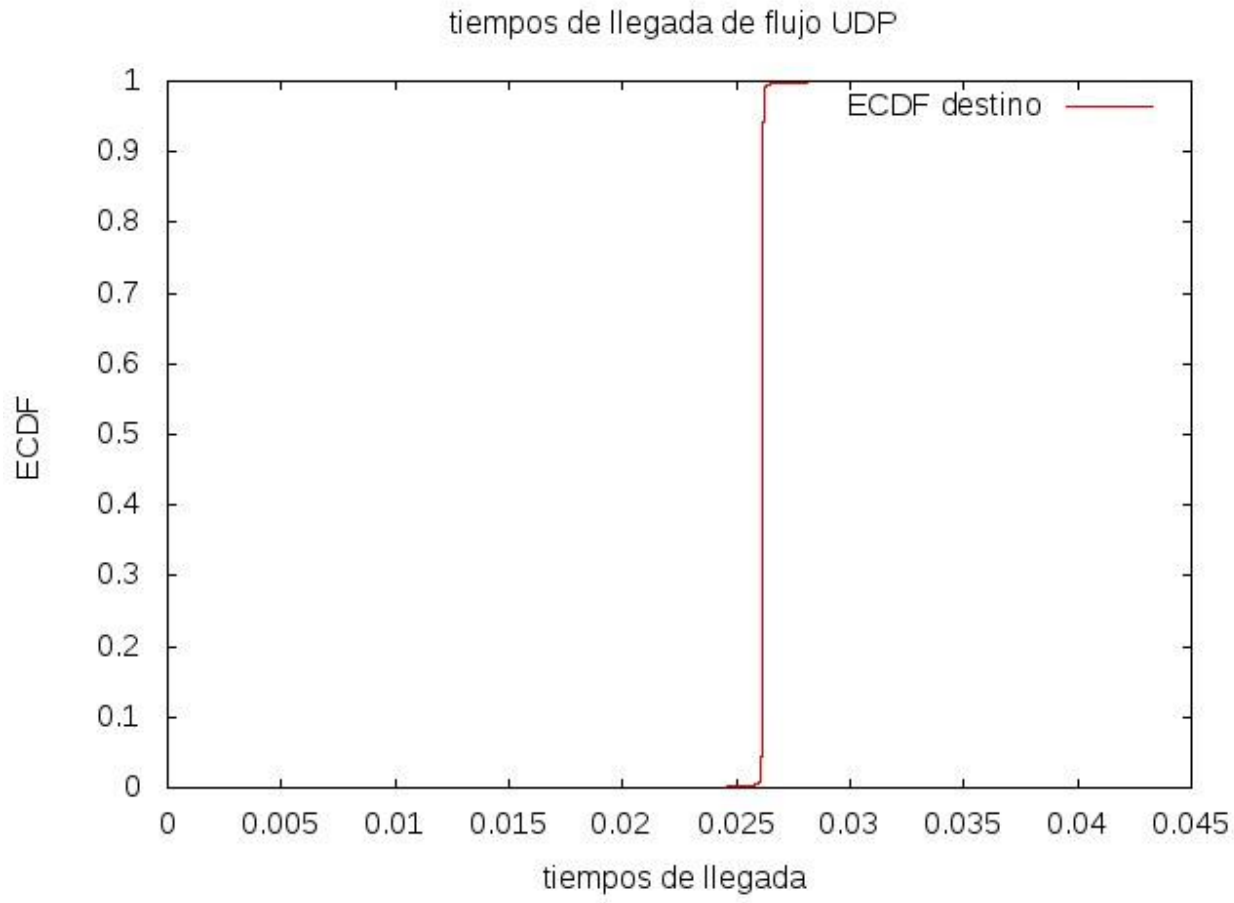
7. **ECDF de los tiempos entre llegadas del flujo UDP indicado por el generador de la traza (una por sentido a nivel 4).**

   - **Tiempos entre llegadas del flujo UDP usando como puerto origen `49714`**

En este ejercicio se nos ha dado un caso bastante interesante, y es que cogiendo los flujos UDP usando como puerto origen el 49714, no nos han salido paquetes

en el filtro, esto puede ser debido a que la comunicación que se establece no sea mediante el mismo puerto para enviar y recibir paquetes. Y por lo anterior, no existe una gráfica para este apartado.

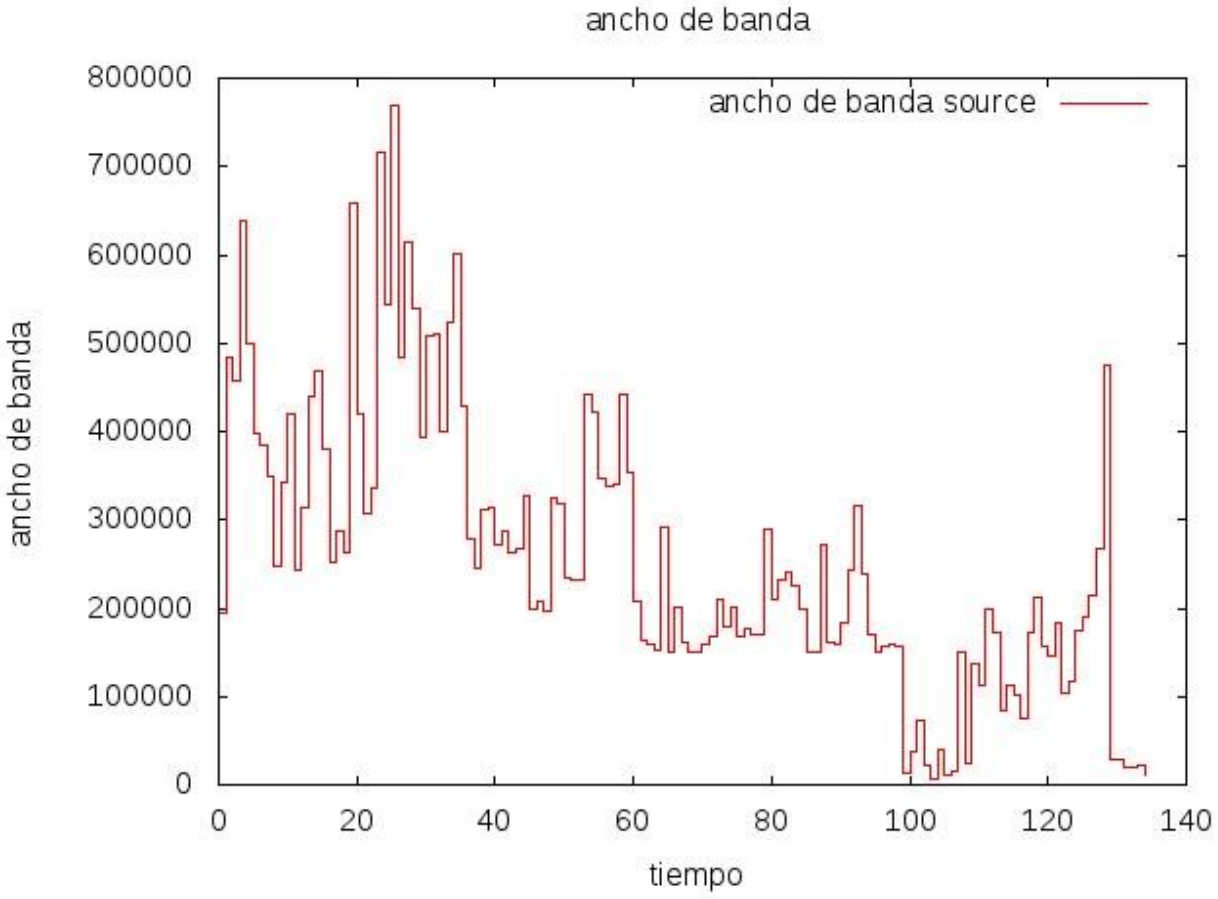
- **Tiempos entre llegadas del flujo UDP usando como puerto destino 49714**



Aquí podemos observar cómo la prácticamente los tiempos de llegada entre paquetes a ese puerto destino en el flujo UDP está entre 0.025s y 0.03s esencialmente.

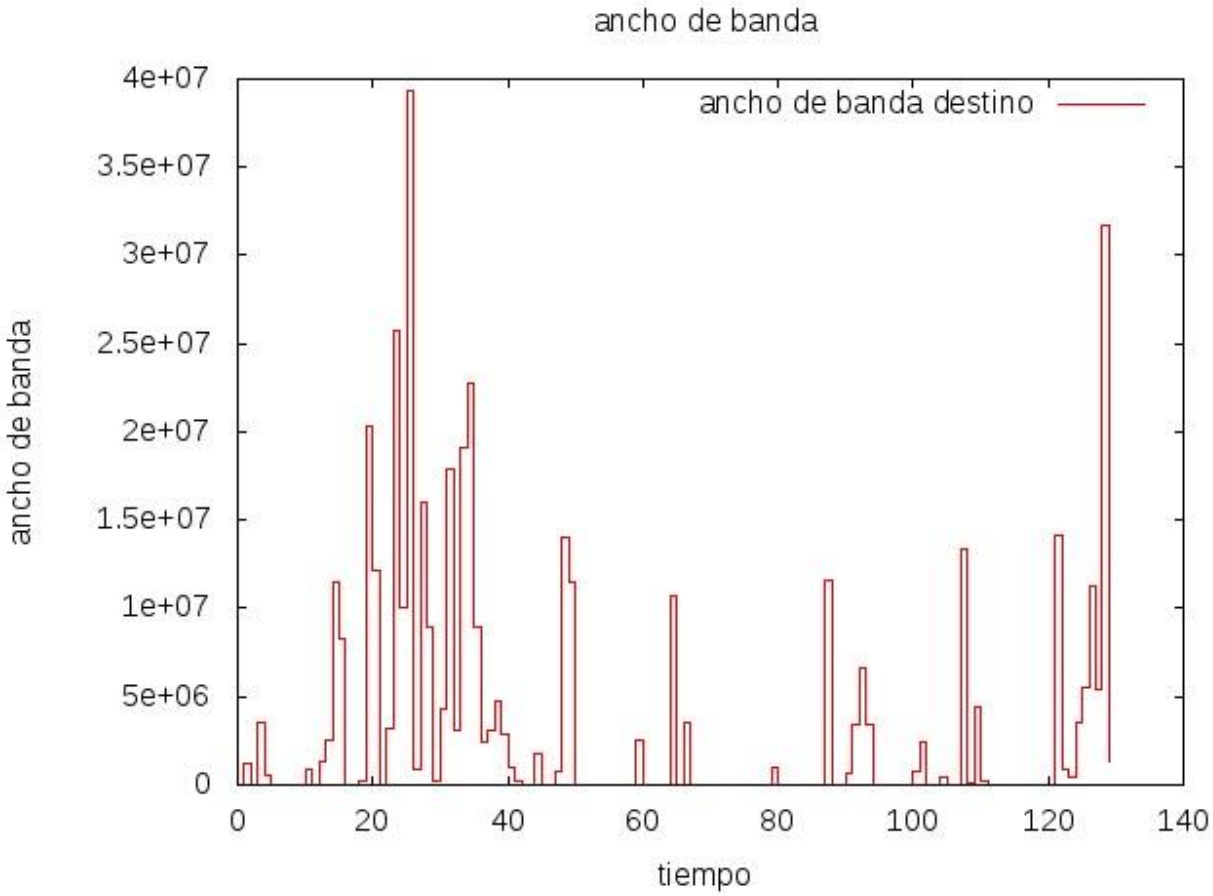
8. **Figura (o figuras) que muestre(n) el caudal/*throughput*/tasa/ancho de banda a nivel 2 en bits por segundo (b/s) y por sentido (asuma que la dirección Ethernet origen o destino es la indicada por el generador de trazas). Los segundos sin tráfico deben representarse a cero.**

- **Ancho de banda con Mac Origen = 00:11:88:CC:32:32**



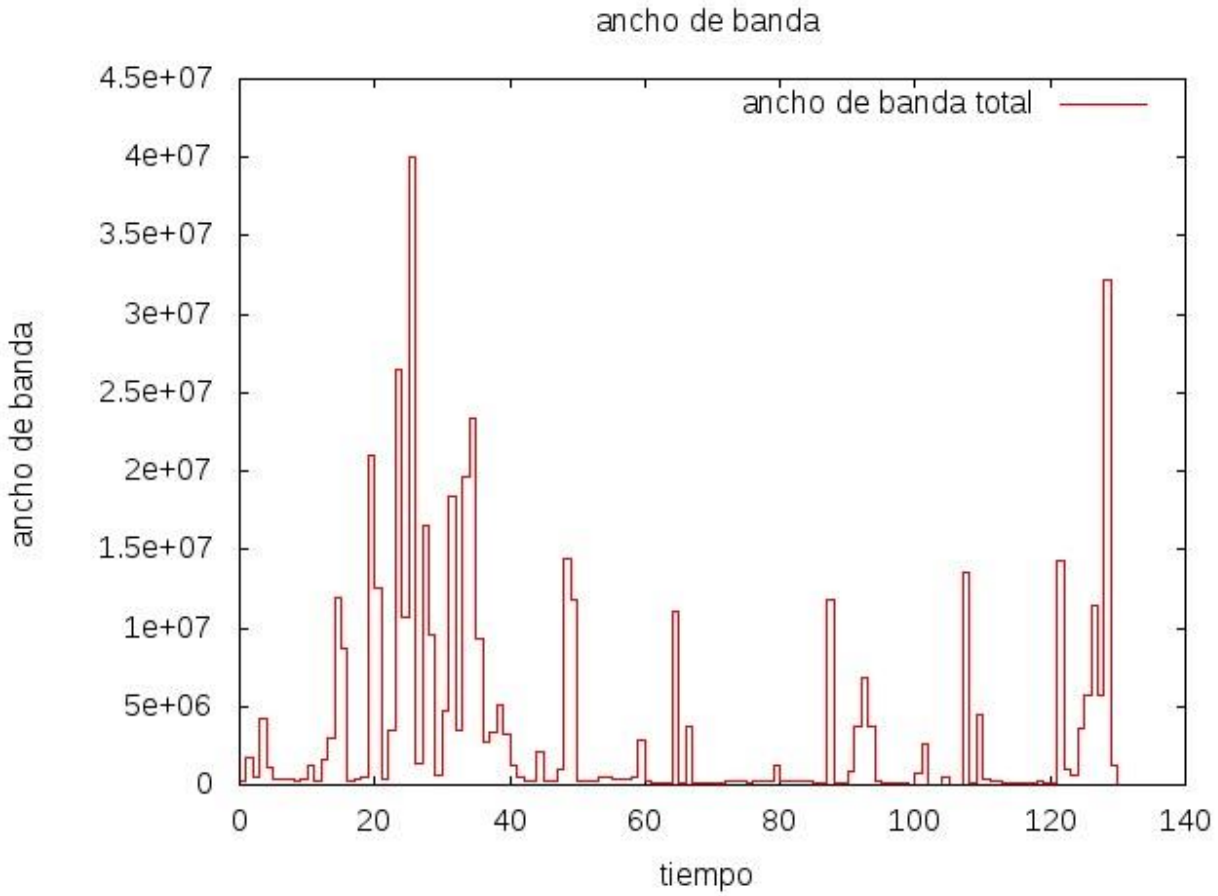
Como podemos ver en esta gráfica, el número de bits que envía el usuario de esta MAC está entre los 100000 y 800000 bits en cada instante. Aunque podemos observar que hay 2 tendencias: al principio se envían más paquetes y luego el tráfico disminuye, alcanzando un mínimo en torno a los 100s.

- **Ancho de banda con Mac Destino = 00:11:88:CC:32:32**



En cambio, en esta gráfica, el número de bits que recibe el usuario de esta MAC es notablemente mayor, ya que el máximo está en torno a los 40 millones de bits, dando a entender que el usuario recibe más bits en paquetes que los que manda, tal y como vimos en el apartado 3, donde observábamos que el tamaño de los paquetes enviados era menor que el de los recibidos.

- **Ancho de banda con Mac = 00:11:88:CC:32:32**



Aquí observamos el tráfico total en ambos sentidos que envía y recibe el usuario de esta MAC, notando cómo tiene sus picos de consumo de ancho de banda entre los 10 y 30s y a los 130s, y en contraste, en la zona entre los intervalos anteriores se hace menos uso de la red

Conclusiones

De esta práctica hemos aprendido a calcular estadísticas diferentes como la ECDF, la serie temporal o el top 10 de IPs/puertos de una red de paquetes. Y estas estadísticas las hemos aplicado sobre campos específicos de la traza, lo que nos hace reflexionar sobre el uso que tienen esas estadísticas específicas.

Para empezar, el primer ejercicio nos pedía calcular los porcentajes de paquetes de tipo IP, con lo cual hemos observado, que en general, IP es el protocolo de red más extendido y usado (como ya sabíamos). Y que, dentro de IP, los protocolos más corrientes son TCP y UDP, aunque en nuestro caso, había más paquetes de otro tipo diferente a los anteriores que de UDP.

En el segundo ejercicio hemos calculado el Top 10 de direcciones IP y el top 10 de puertos (separados en UDP y TCP), con esto, podemos deducir qué puertos son los más comunes para usar en la capa de transporte, ya que suelen ser usados siempre los mismos.

En los apartados 3-5 hemos calculado ECDFs de tamaños a nivel 2 de paquetes aplicando diferentes filtros, que son, por una MAC específica, por ser HTTP y por ser DNS.

De ello hemos podido aprender, en el caso de una MAC específica, sobre qué tamaños suelen oscilar los paquetes que envía/recibe el usuario de dicha MAC.
En el caso de los paquetes HTTP y DNS, sabiendo que estos paquetes suelen tener un uso más enfocado a ser enviados y recibidos a internet, resulta útil conocer los tamaños de estos paquetes, de cara a optimizar su envío y recibo.

En los apartados 6 y 7 hemos calculado ECDFs de tiempos de llegada de paquetes a puertos específicos de paquetes de tipo TCP o UDP, con lo que hemos observado sobre qué valores suelen oscilar los tiempos de llegada, y así saber qué paquetes tardan más en enviarse y recibirse en una red entre varios hosts.

En el apartado 8 hemos calculado el ancho de banda que ocupa un usuario con una MAC específica, con lo que hemos sido capaces de discernir si el usuario envía o recibe más paquetes y en qué intervalos de tiempo, lo que puede resultar muy útil para un administrador de red, al que le interesa conocerlo para saber optimizar la red para todos los usuarios.