

UNIVERSIDAD AUTÓNOMA



REDES DE COMUNICACIONES I

PRÁCTICA 3

---

# Memoria

---

*Autores:*

Adrián FERNÁNDEZ

Santiago GONZÁLEZ-CARVAJAL

12 de noviembre de 2017

# Índice

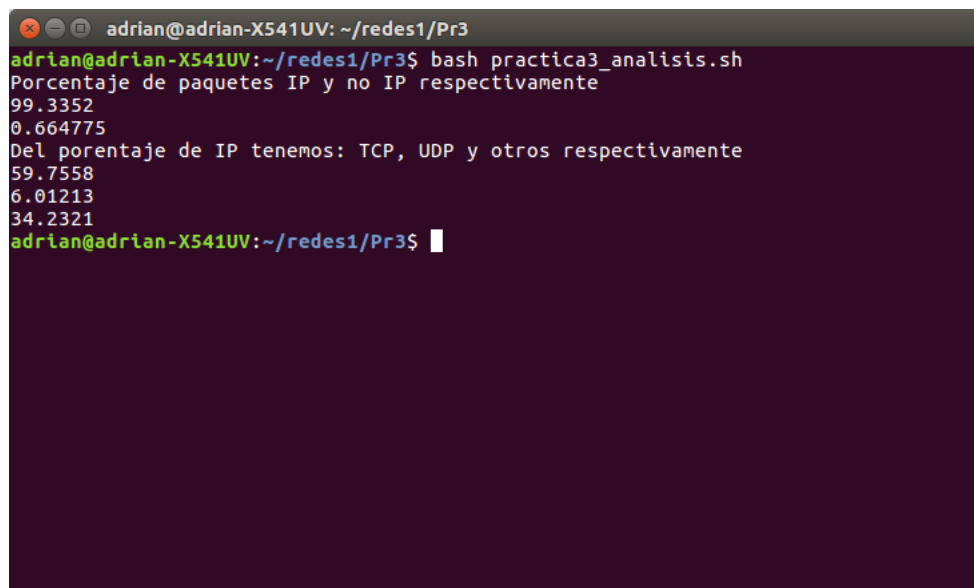
1. Introducción	2
2. Apartado 1	2
3. Apartado 2	3
4. Apartado 3	7
5. Apartado 4	8
6. Apartado 5	12
7. Apartado 6	15
8. Apartado 7	17
9. Conclusión	18

## 1. Introducción

Con motivo de la practica 3 de Redes de Comunicaciones I, debemos utilizar scripts para analizar una traza que simula el trafico real de una red. En concreto, debemos distinguir los paquetes IP y los no IP y analizar varios parámetros de los paquetes IP, como las direcciones IP destino y origen o, en el caso en el que se trate de TCP o UDP, los puertos destino y origen. Una vez recopilados estos datos, debemos representarlos en ECDF's mediante scripts y explicar los resultados obtenidos.

## 2. Apartado 1

*Captura de la ejecución:*

A screenshot of a terminal window with a dark background. The window title is 'adrian@adrian-X541UV: ~/redes1/Pr3'. The prompt is 'adrian@adrian-X541UV:~/redes1/Pr3\$'. The user has entered 'bash practica3\_analisis.sh'. The script outputs the following text: 'Porcentaje de paquetes IP y no IP respectivamente', '99.3352', '0.664775', 'Del porcentaje de IP tenemos: TCP, UDP y otros respectivamente', '59.7558', '6.01213', '34.2321', and then returns to the prompt 'adrian@adrian-X541UV:~/redes1/Pr3\$' with a cursor.

```
adrian@adrian-X541UV: ~/redes1/Pr3
adrian@adrian-X541UV:~/redes1/Pr3$ bash practica3_analisis.sh
Porcentaje de paquetes IP y no IP respectivamente
99.3352
0.664775
Del porcentaje de IP tenemos: TCP, UDP y otros respectivamente
59.7558
6.01213
34.2321
adrian@adrian-X541UV:~/redes1/Pr3$
```

Porcentajes:

IP: 99.3352 % - Filtro: (eth.type eq 0x0800 || vlan.etype eq 0x0800)

No IP: 0.664775 % - Filtro: ((eth.type ne 0x0800&&eth.type ne 0x8100)||((eth.type eq 0x8100&&vlan.etype ne 0x0800))

Dentro de los IP(contados con awk):

TCP: 59.7558 % - Filtro: (ip.proto == 6)

UDP: 6.01213 % - Filtro: (ip.proto == 17)

Otros: 34.2321 % - Filtro: paquetes restantes

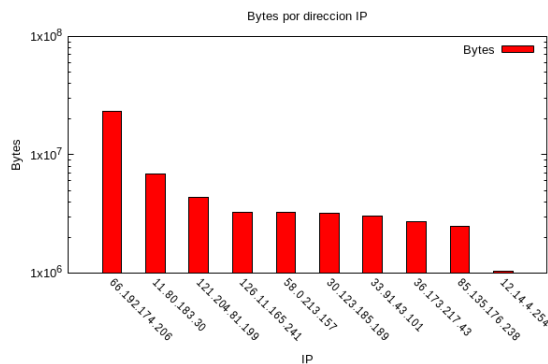
Como podemos ver, casi el total de los paquetes es de tipo IP, y dentro del tipo IP, el tipo principal es el TCP.

### 3. Apartado 2

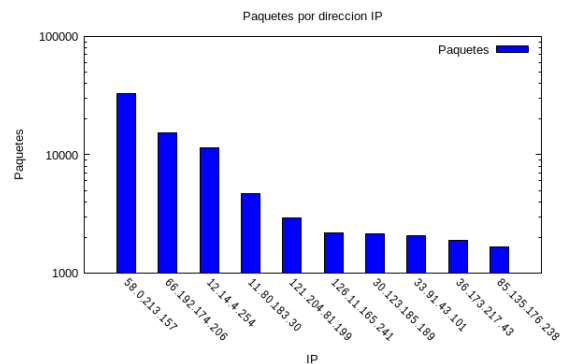
Nótese que el eje vertical está en escala logarítmica para que se puedan apreciar las direcciones IP o puertos que tienen menos tráfico. Las barras sin altura implican que esa dirección o puerto solo ha estado implicado en la transmisión de un paquete.

Direcciones IP origen:

Por bytes:



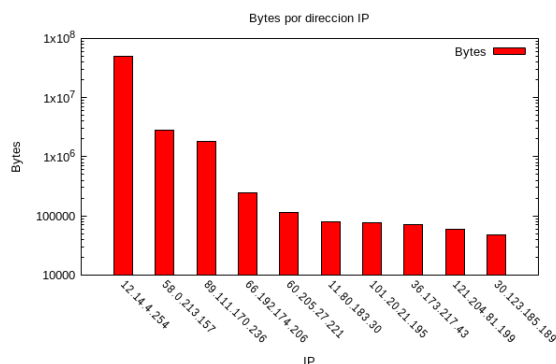
Por paquetes:



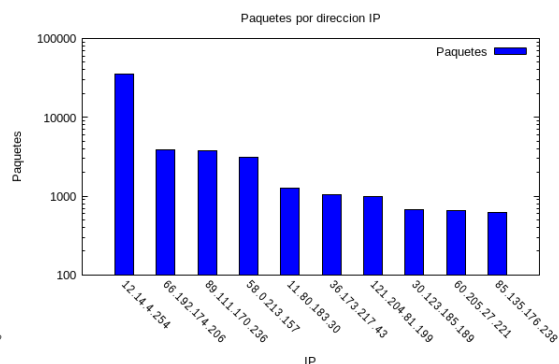
Como podemos apreciar, estas gráficas representan un elevado número de Bytes y de paquetes debidos al gran número de paquetes IP que tiene la traza generada.

Direcciones IP destino:

Por bytes:



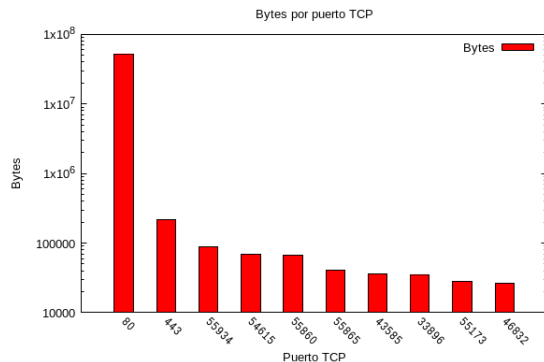
Por paquetes:



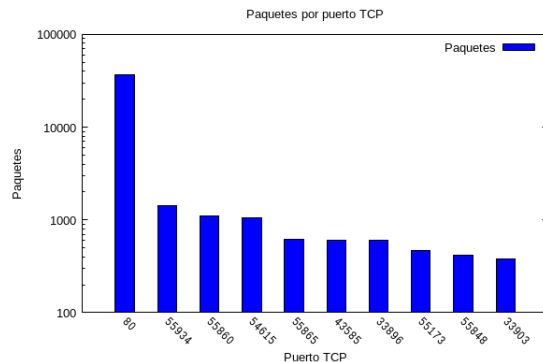
Como podemos apreciar, estas gráficas representan un elevado número de Bytes y de paquetes debidos al gran número de paquetes IP que tiene la traza generada.

Puertos TCP origen:

Por bytes:



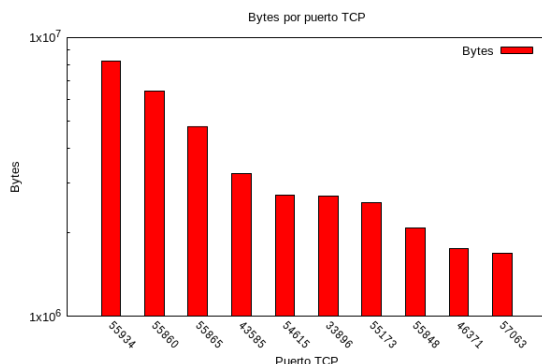
Por paquetes:



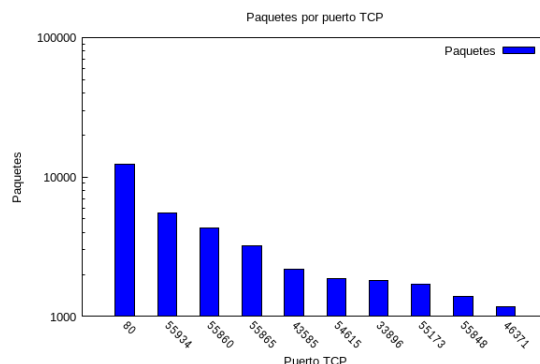
Como podemos observar, estos valores son menores que los obtenidos en las gráficas para paquetes IP. Esto es debido al menor número de paquetes.

Puertos TCP destino:

Por bytes:



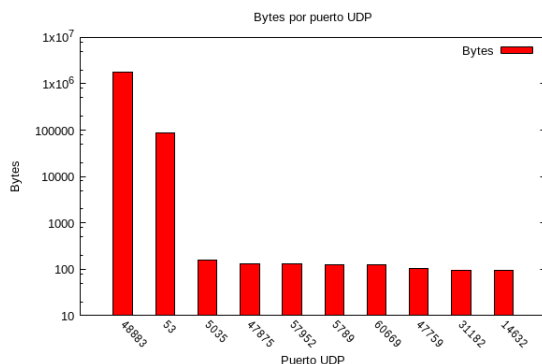
Por paquetes:



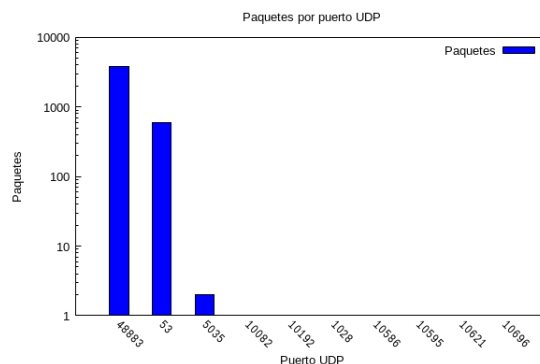
Como podemos observar, estos valores son menores que los obtenidos en las gráficas para paquetes IP. Esto es debido al menor número de paquetes.

Puertos UDP origen:

Por bytes:



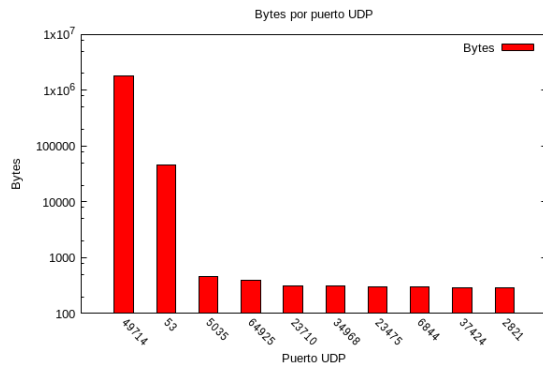
Por paquetes:



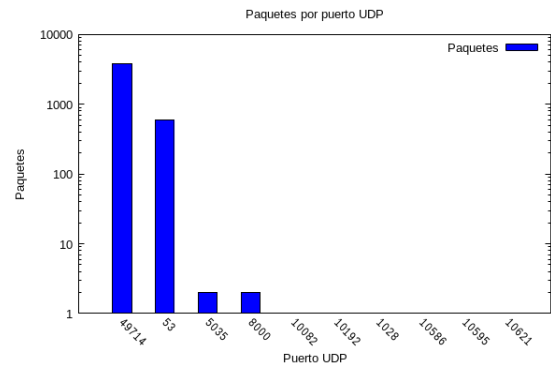
En estas gráficas podemos observar los bajos valores debidos al limitado número de paquetes UDP.

Puertos UDP destino:

Por bytes:



Por paquetes:

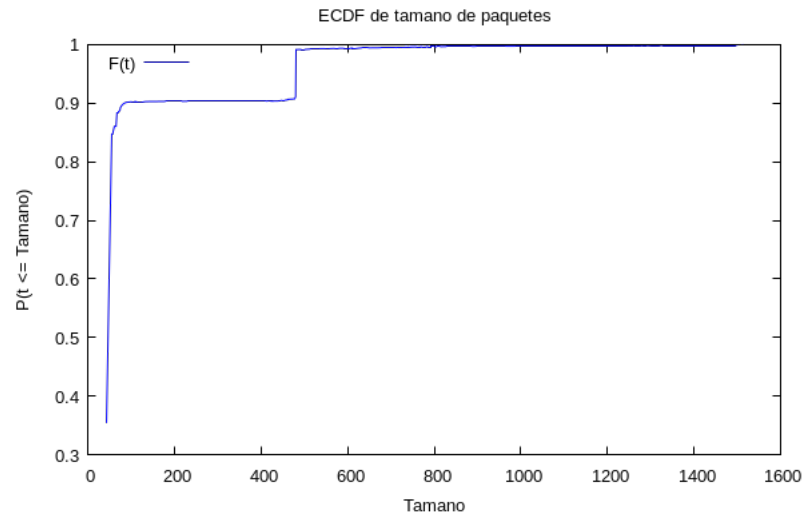


En estas gráficas podemos observar los bajos valores debidos al limitado número de paquetes UDP.

Comentar que, aunque obviamente el top 10 por Bytes y por paquetes no es igual (lo cual se debe a que todos los paquetes no son del mismo tamaño), podríamos decir que existe una relación débil entre ambos "tops". Ya que cuantos más paquetes se envían, más Bytes se están enviando. Esto se aplica a todas las gráficas de este apartado.

## 4. Apartado 3

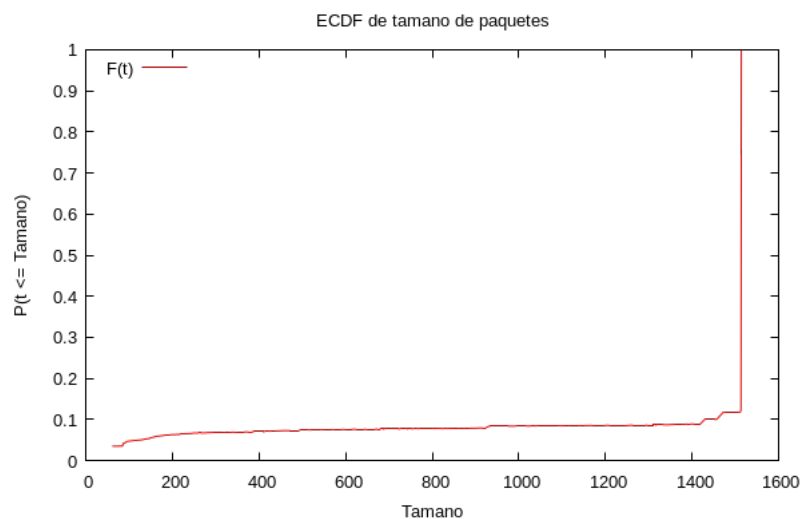
*ECDF de tamaños a nivel 2 de paquetes (origen):*



Esta ECDF nos dice que la mayoría de los paquetes enviados desde la dirección MAC indicada en el generador de trazas tienen en general un tamaño de cerca de o bien unos 100 Bytes (con una probabilidad muy elevada), o bien unos 450 Bytes (con una probabilidad un poco menor que la anterior), y que rara vez se dan casos de paquetes con tamaño distinto.



*ECDF de tamaños a nivel 2 de paquetes (destino):*

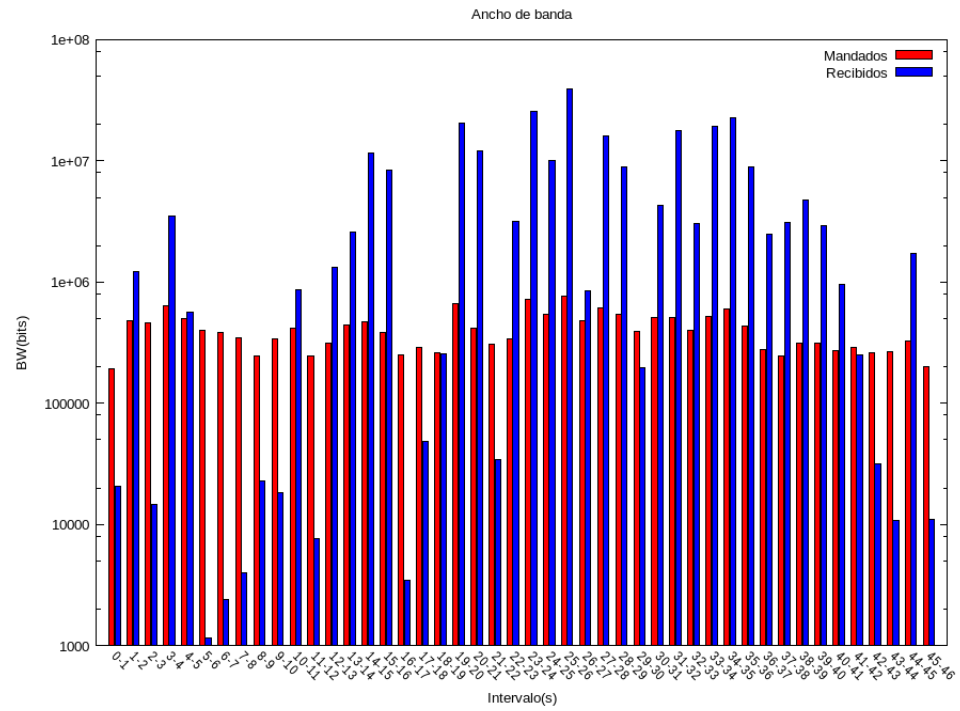


En cambio, los recibidos tienen en general un tamaño de entre 1400 Bytes y 1550 Bytes (aunque obviamente algunos paquetes tienen tamaños menores, pero la probabilidad de obtenerlos es remota).

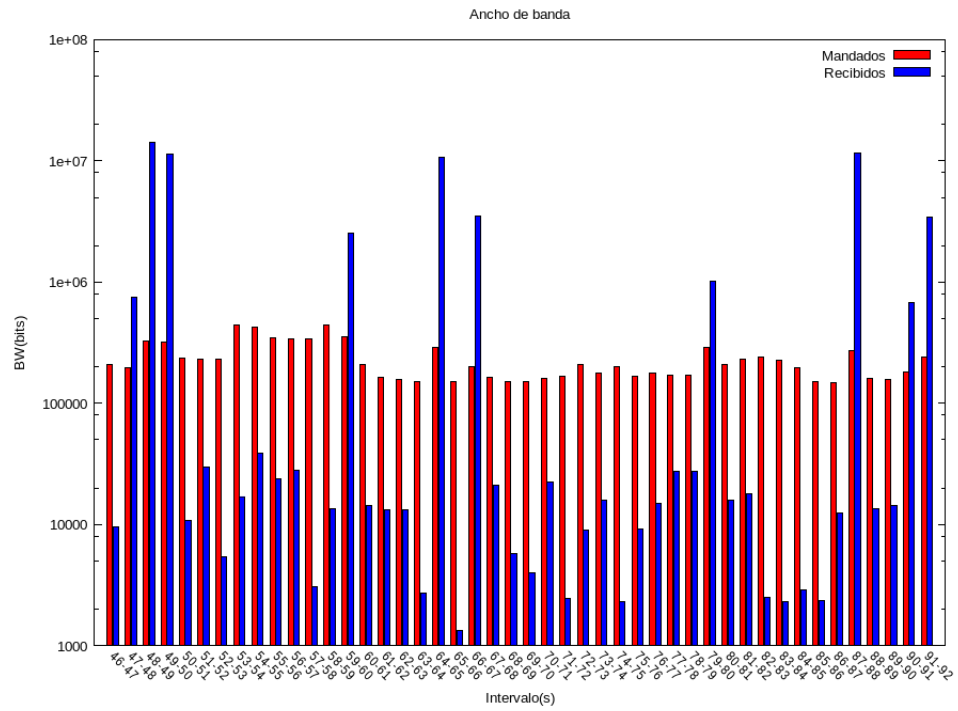
## 5. Apartado 4

Nótese que el eje vertical está en escala logarítmica para que se pueda apreciar el ancho de banda de los bits mandados.

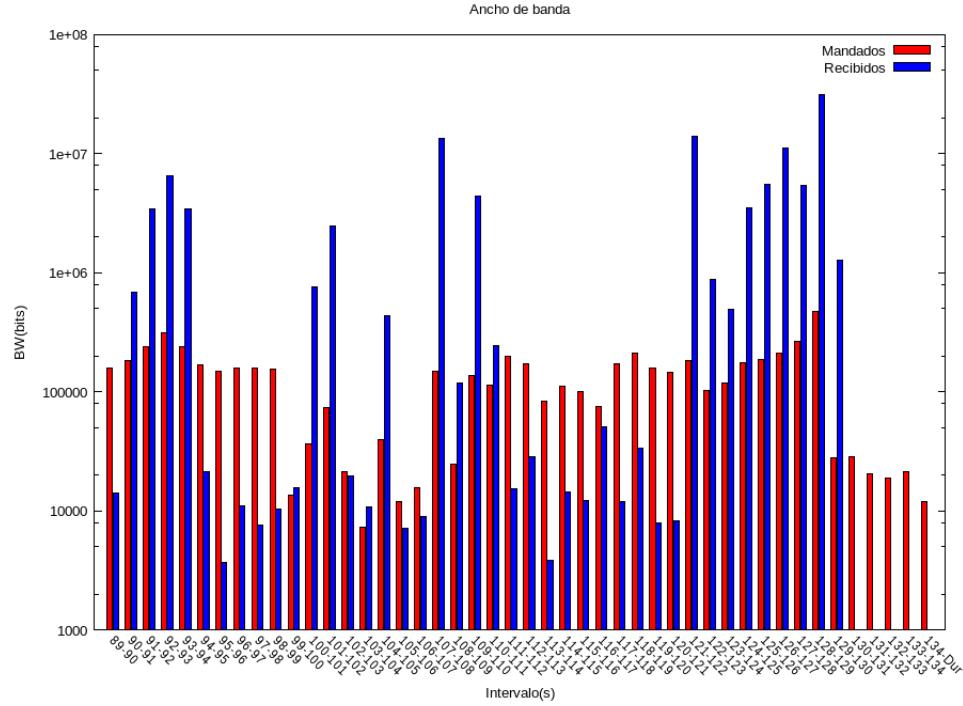
*BW en los primeros 46 segundos:*



*BW en los segundos 46 - 92:*



*BW en los últimos segundos:*



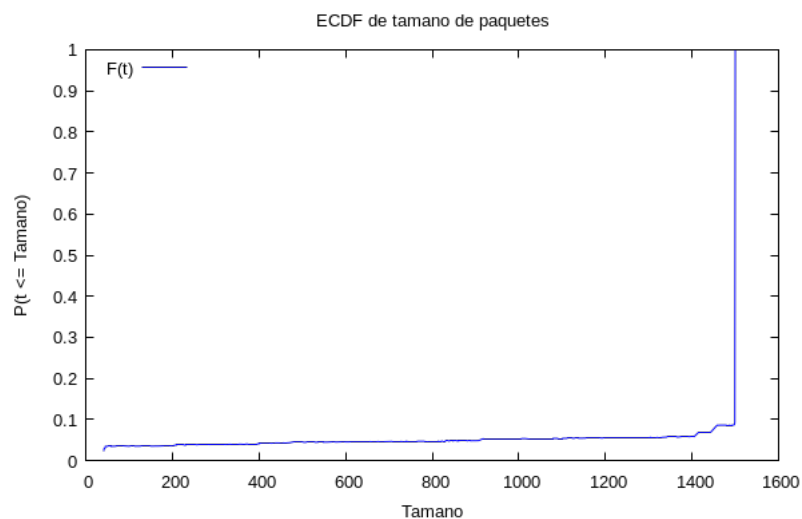
En estas gráficas podemos apreciar el ancho de banda con granularidad de 1 segundo. Podemos observar que el ancho de banda de los paquetes enviados desde la dirección MAC proporcionada se mantiene a grandes rasgos, (esto es, oscila, pero en general los valores no cambian más de 40K b/s) salvo en los últimos segundos donde hay una bajada considerable.

En cambio, los valores de los recibidos no se mantienen para nada. Podemos observar que en los primeros segundos (hasta el segundo 20 aproximadamente) los valores son muy bajos, luego los valores se disparan (hasta el segundo 42), y a partir de ese momento los valores son bajos en general con algunas subidas puntuales (que no se mantienen) hasta el segundo 92. De ahí en adelante los valores oscilan en gran medida hasta los últimos 5 segundos, donde no existe tráfico en este sentido.

## 6. Apartado 5

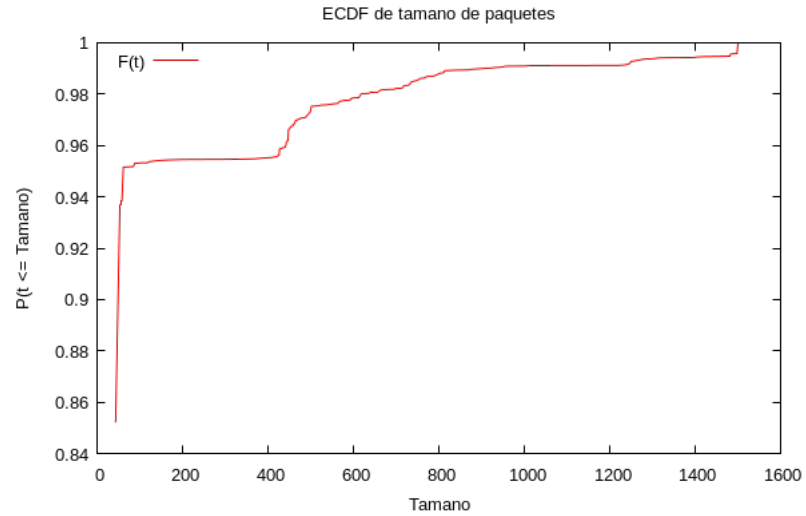
*ECDF de los tamaños a nivel 3 de los paquetes DNS de la traza (una por sentido a nivel 4). Entenderemos como DNS todos aquellos paquetes que usen el puerto 53 de UDP en origen o destino.*

*ECDF de tamaños a nivel 3 (http origen):*



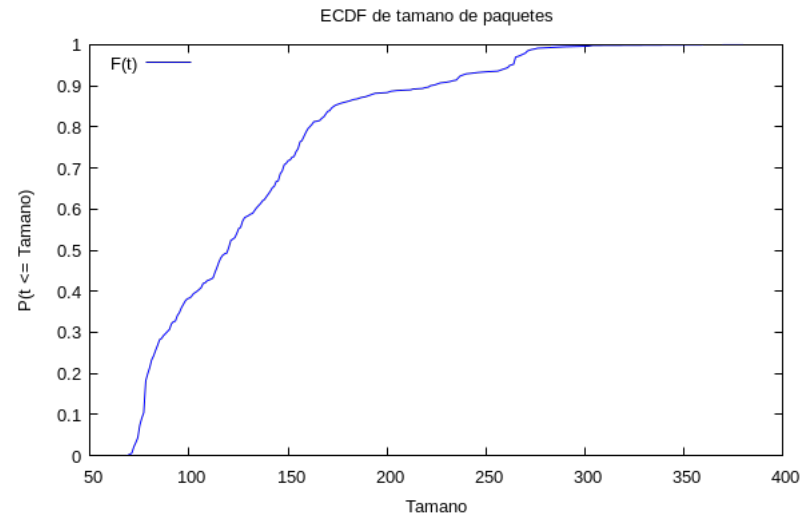
Aquí podemos observar que en general todos los paquetes HTTP de origen tienen un tamaño de unos 1500 Bytes.

*ECDF de tamaños a nivel 3 (http destino):*



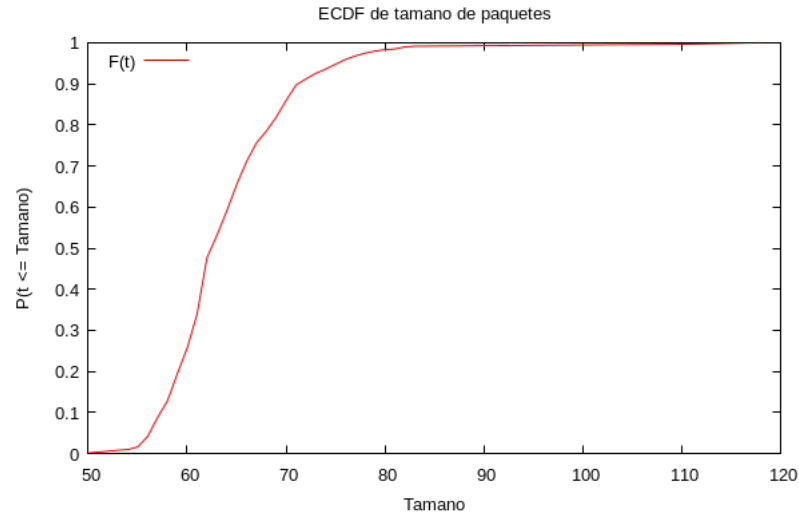
En cambio, en esta gráfica podemos observar que el tamaño de los paquetes HTTP destino cambia, y los valores predominantes son unos 50 Bytes, y entre 400 y 1500 Bytes (aunque estos últimos con menor probabilidad).

*ECDF de tamaños a nivel 3 (dns origen):*



Podemos apreciar que el tamaño de este tipo de paquetes oscila entre 75 y 275 Bytes, tomando valores más bajos (dentro de este intervalo) con más probabilidad que valores altos.

*ECDF de tamaños a nivel 3 (dns destino):*



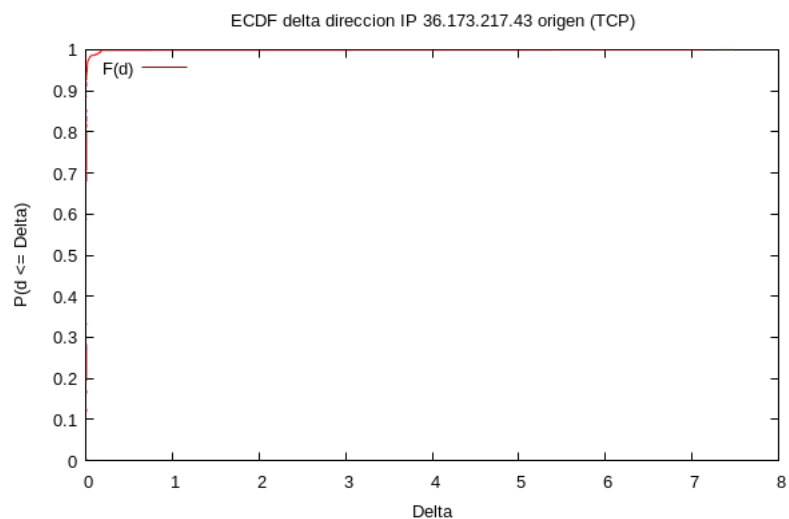
Podemos observar que los valores del tamaño de este tipo de paquetes oscila entre 55 y 80 Bytes tomando valores más pequeños (en este intervalo) con mayor probabilidad que valores mayores.

## 7. Apartado 6

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

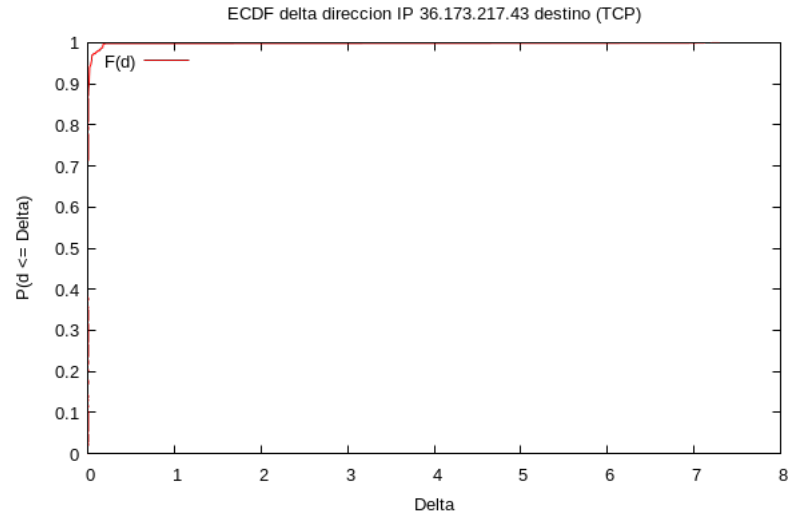


*ECDF de los tiempos entre llegadas de paquetes del flujo tcp (origen):*



Podemos observar que los tiempos entre llegada de paquetes de este flujo son muy cercanos a 0, es decir, estos paquetes están llegando a un ritmo constante muy rápido en general. Aunque existen excepciones que provocan este resultado, estas se tratan de paquetes que llegan unos 7 segundos después.

*ECDF de los tiempos entre llegadas de paquetes del flujo tcp (destino):*



Podemos observar que los tiempos entre llegada de paquetes de este flujo son muy cercanos a 0, es decir, estos paquetes están llegando a un ritmo constante muy rápido en general. Aunque existen excepciones que provocan este resultado, estas se tratan de paquetes que llegan unos 7 segundos después.

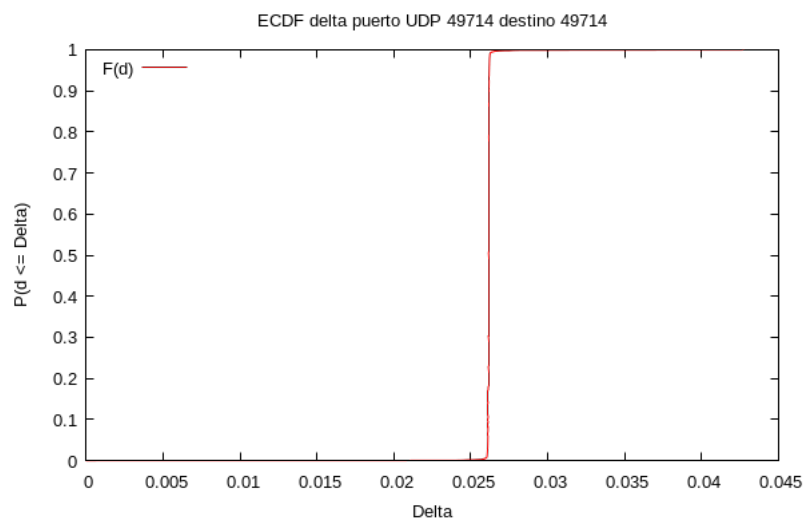
Apréciase el parecido entre ambas gráficas.

## 8. Apartado 7

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

Nótese que solo hay gráfica para el flujo udp pedido con el puerto dado como destino, ya que no hay ningún paquete con dicho puerto como origen y por lo tanto no hay datos a partir de los cuales generar la gráfica.

*ECDF de los tiempos entre llegadas de paquetes del flujo udp (destino):*



Podemos observar que los tiempos entre llegada de paquetes de este flujo son muy cercanos a 0 en general, y no existen excepciones. Es decir, el tiempo máximo no llega en ningún caso ni a 0.5 segundos siquiera.

## 9. Conclusión

Hemos aprendido a obtener las características básicas de una red mediante el análisis combinado de la herramienta tshark y los scripts. En particular, el shell scripting y el manejo de la potente herramienta awk.