

Monitorización

Introducción:

1. Porcentajes de paquetes (puede incluir una captura de pantalla):

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**).

2. Top 5 de direcciones IP activas (en bytes y paquetes) y top 5 de puertos (en bytes y paquetes) (una captura de pantalla puede ser suficiente).

```
Se procesaron 58305 paquetes.

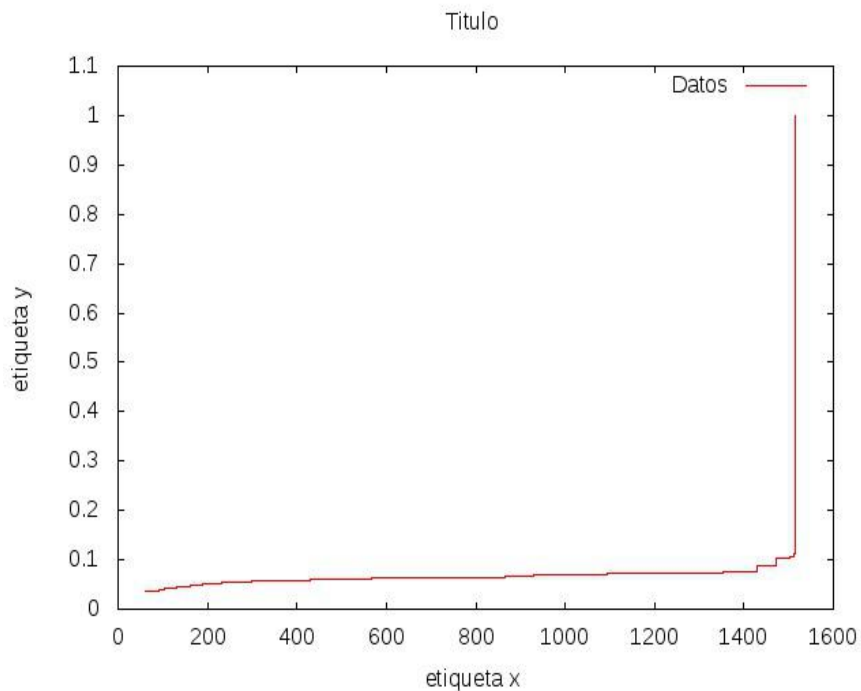
Hay 553 paquetes NO IP
Hay 57752 paquetes IP
Hay 768 paquetes IP que no son ni TCP ni UDP
Hay 49378 paquetes IP/TCP
Hay 7606 paquetes IP/UDP
Hay un porcentaje de un 99.051539 % de paquetes IP con respecto al total.
    Dentro de este porcentaje:
        -Hay un porcentaje de un 85.500069 % de paquetes TCP con respecto al total de ip.
        -Hay un porcentaje de un 13.170107 % de paquetes UDP con respecto al total de ip.
        -Hay un porcentaje de un 1.329824 % de paquetes de otro tipo con respecto al total de ip.
Hay un porcentaje de un 0.948461 % de paquetes NO IP con respecto al total.
Por ultimo, el numero de TAGs VLAN encontrados ha sido: 6423

TopFivePack:
1.80 con 48982
2.55934 con 6909
3.24704 con 6423
4.8024 con 6423
5.55860 con 5411

TopFiveSize:
1.8024 con 53931024
2.34053 con 8324572
3.46857 con 6505558
4.64131 con 4849192
5.64324 con 3281612
```

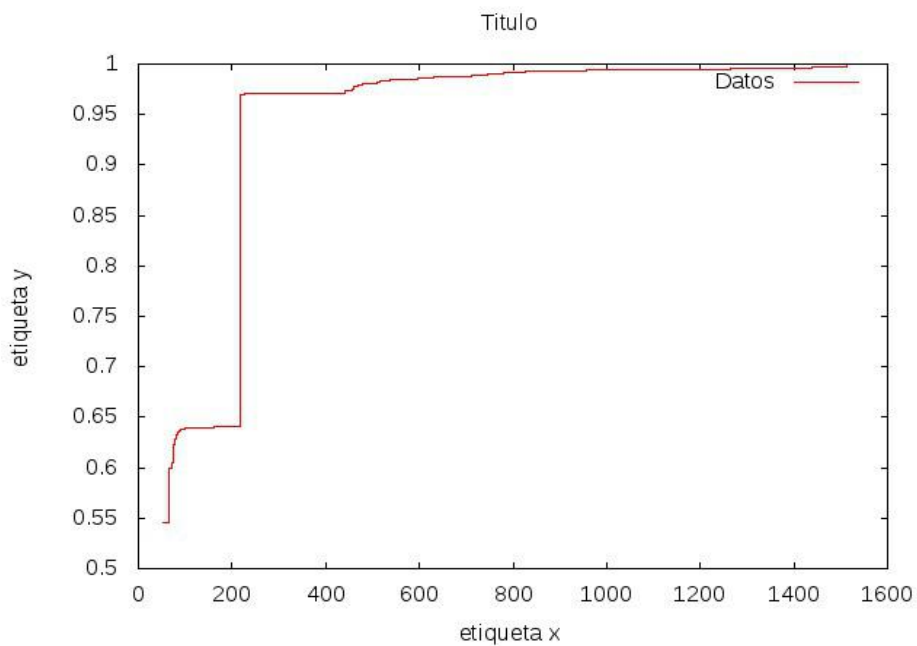
3. ECDF de los tamaños a nivel 2 de los paquetes de la traza (una por sentido, utilice la dirección MAC proporcionada por el generador).

MAC origen 00:11:88:CC:33:9B



La gráfica indica que el terminal con la MAC requerida ha enviado una gran cantidad de paquetes muy grandes, de tamaño máximo 1514 bytes, muy utilizada junto a protocolos TCP, ya que a la hora de transmitir un usuario normal solo precisa de compartir una información de forma fiable, asegurando que llegue a su destino.

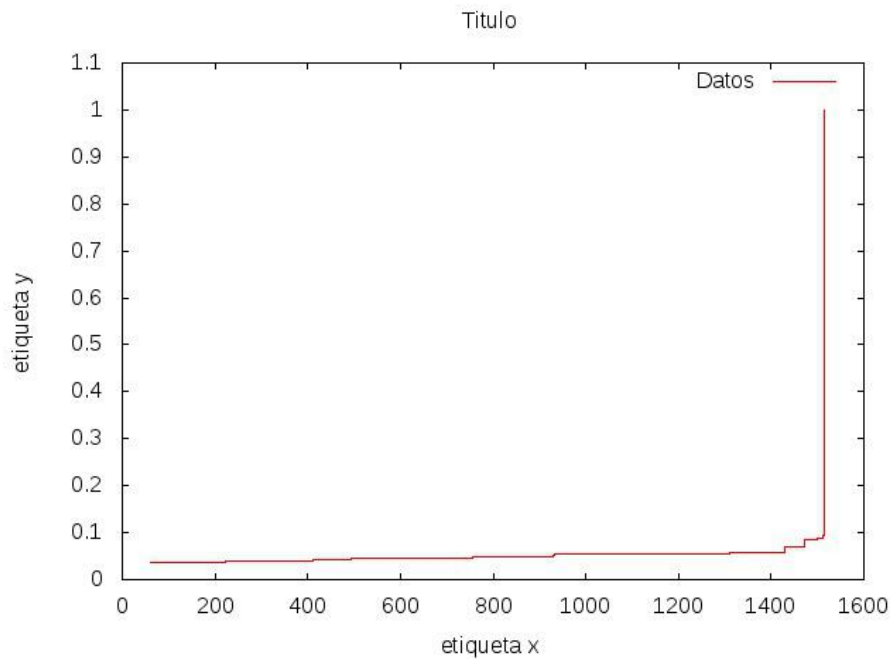
MAC destino 00:11:88:CC:33:9B



Sin embargo el mismo terminal ha recibido paquetes mas variopintos en cuanto al tamaño, debido al la diferencia de contenido recibida.

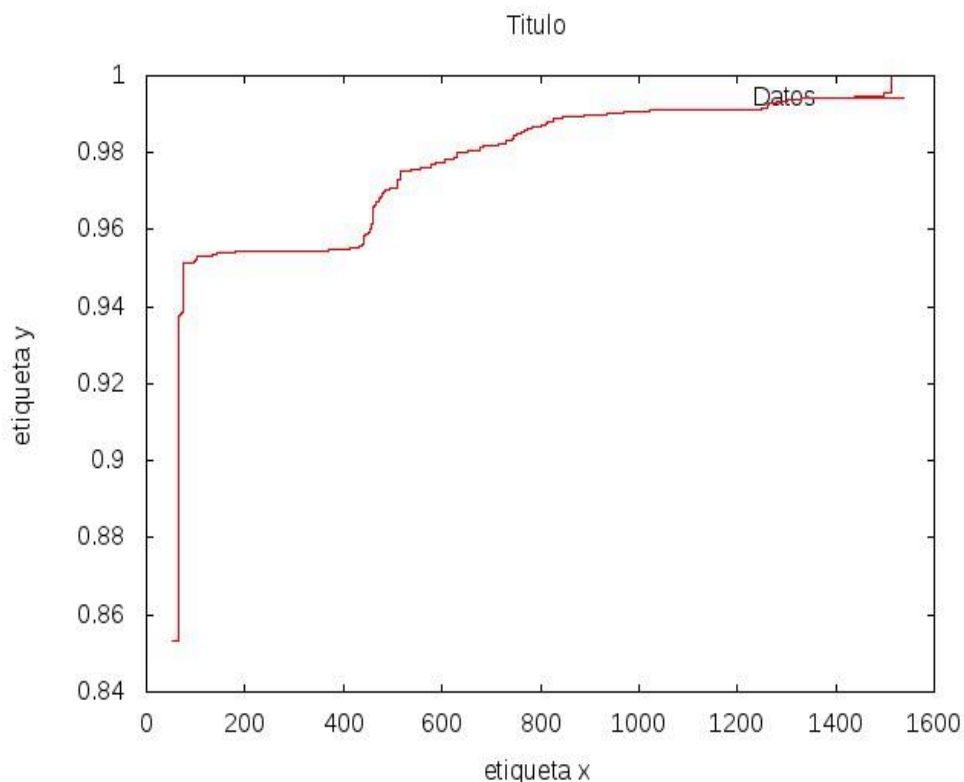
4. ECDF de los tamaños a nivel 2 de los paquetes HTTP de la traza (una por sentido a nivel 4). Entenderemos como HTTP todos aquellos paquetes que usen el puerto 80.

Puerto origen 80



Se presenta una cantidad de paquetes enviados de tipo HTTP, donde predominan los de gran tamaño. Paquetes propios de información relativa a paginas de internet, peticiones a los servidores en su mayoría, que coincide con los tamaños de paquetes enviados por el terminal local.

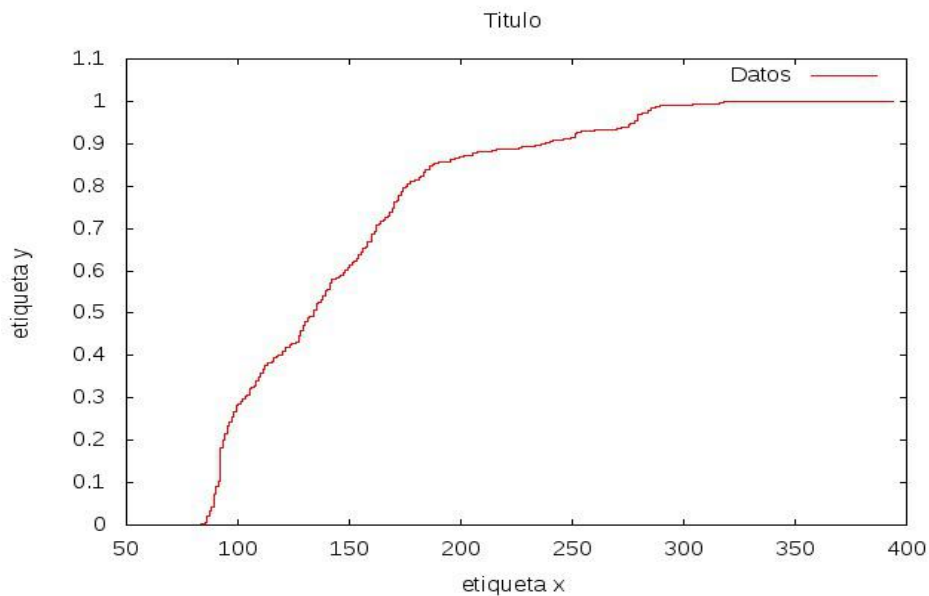
Puerto
destino
80



Que lleguen de tipo HTTP son mas variados como pasaba anteriormente, podría decirse por los diferentes contenidos relacionados con las paginas web que visita el terminal.

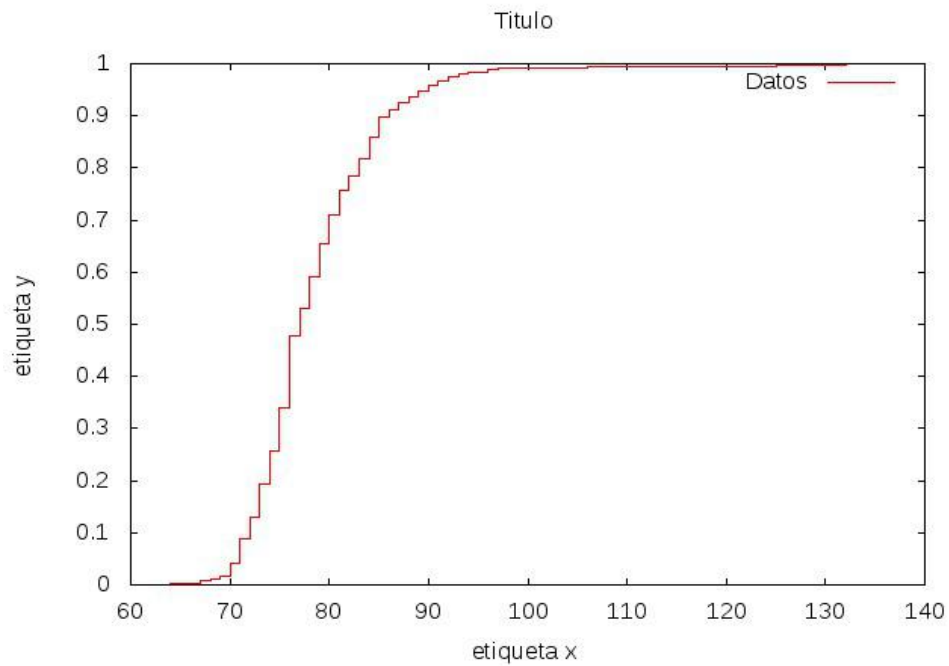
5. ECDF de los tamaños a nivel 2 de los paquetes DNS de la traza (una por sentido a nivel 4). Entenderemos como DNS todos aquellos paquetes que usen el puerto 53.

Puerto origen 53



Los paquetes DNS enviados, no son tan grandes como los anteriores se mueven en torno a tamaños medios, ya que se encargan de la resolución de direcciones ip mediante dominios, por lo que no se necesita tanta cantidad de información.

Puerto destino 53



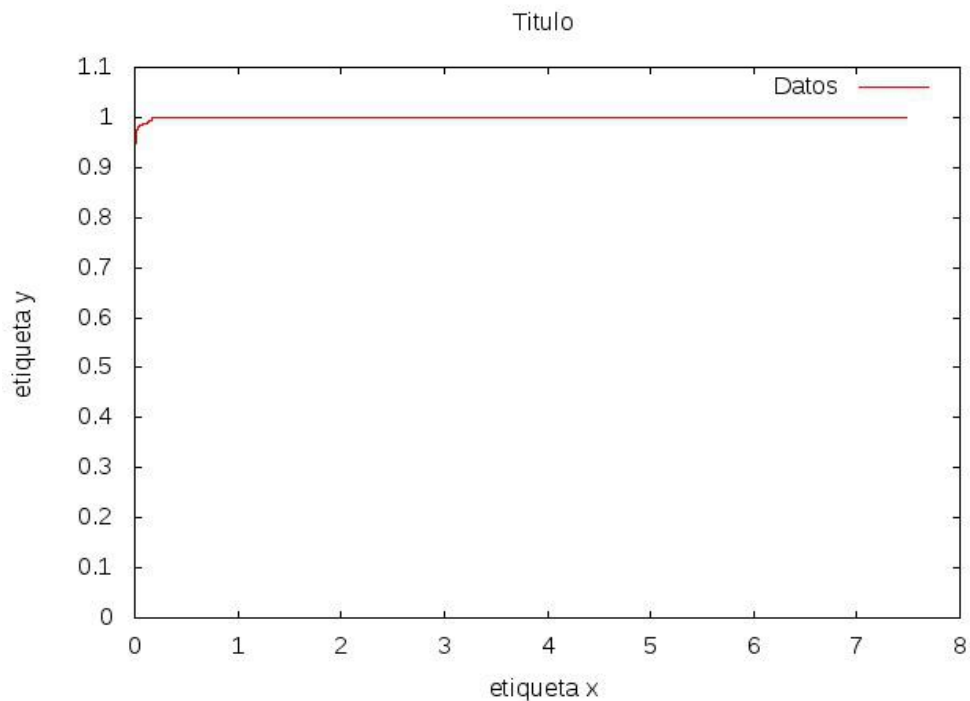
De igual manera los paquetes DNS recibidos son incluso mas pequeños, ya que solo resuelven IPs relativas a dominios.

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

IP TCP

82.200.86.

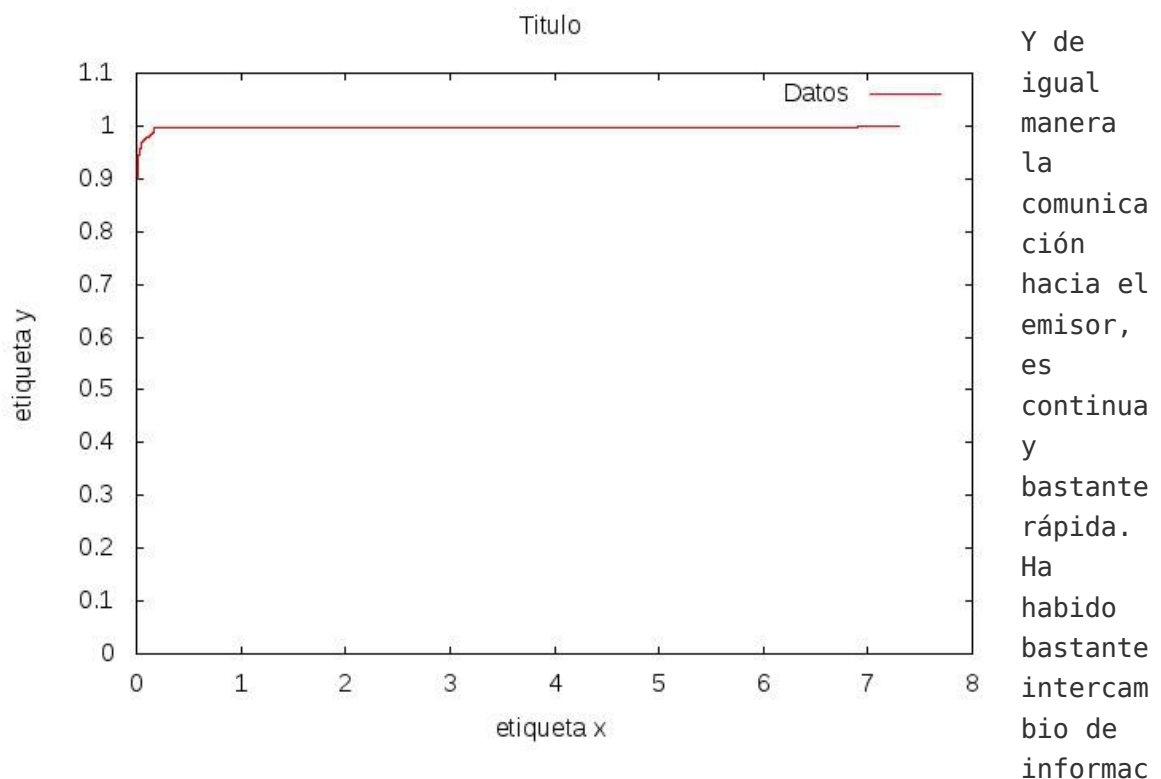
41 Origen



El flujo de TCP de la traza indicado por el generador de trazas, deja ver que no suelen tardar mas de 0,2 segundos en enviar un nuevo paquete, por lo que se

entiende que se realizaba cierta comunicación continua hacia los receptores, con algunas excepciones de distensión en el espacio entre envío de información.

IP TCP 82.200.86.41 Destino



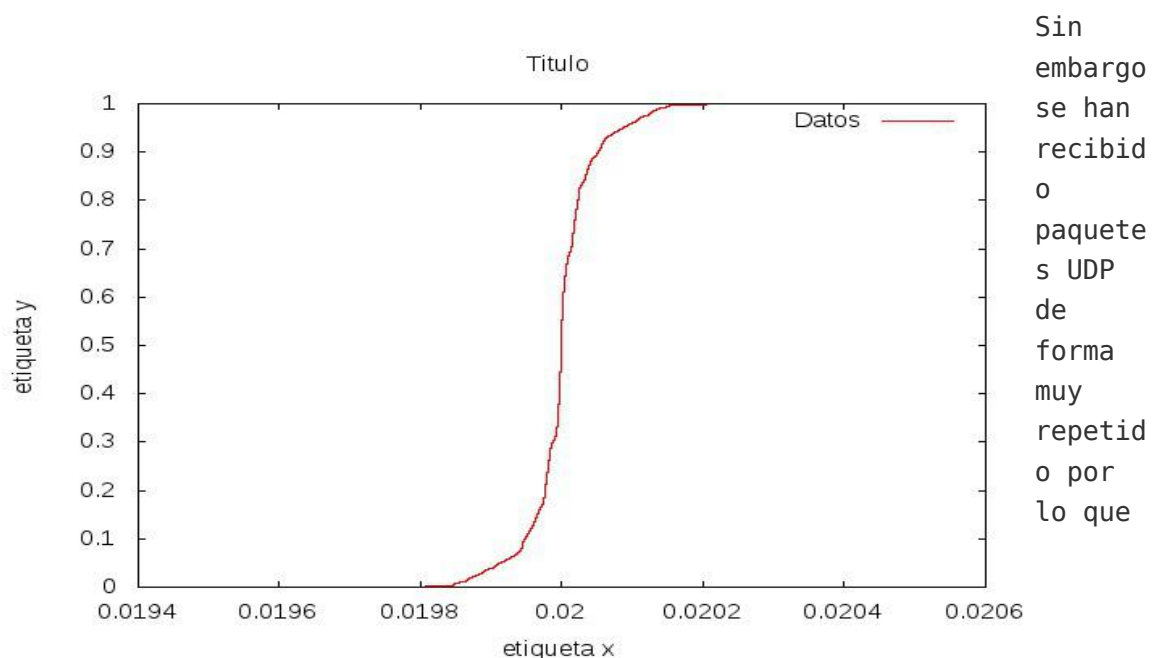
ión.

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

Puerto UDP origen 8024

No había ningún paquete coincidente. Son paquetes que se suelen utilizar en el envío de algún tipo de vídeo como Youtube, Skype, y que el emisor no ha empleado, por lo que no ha enviado ningún vídeo a tiempo real o en diferido.

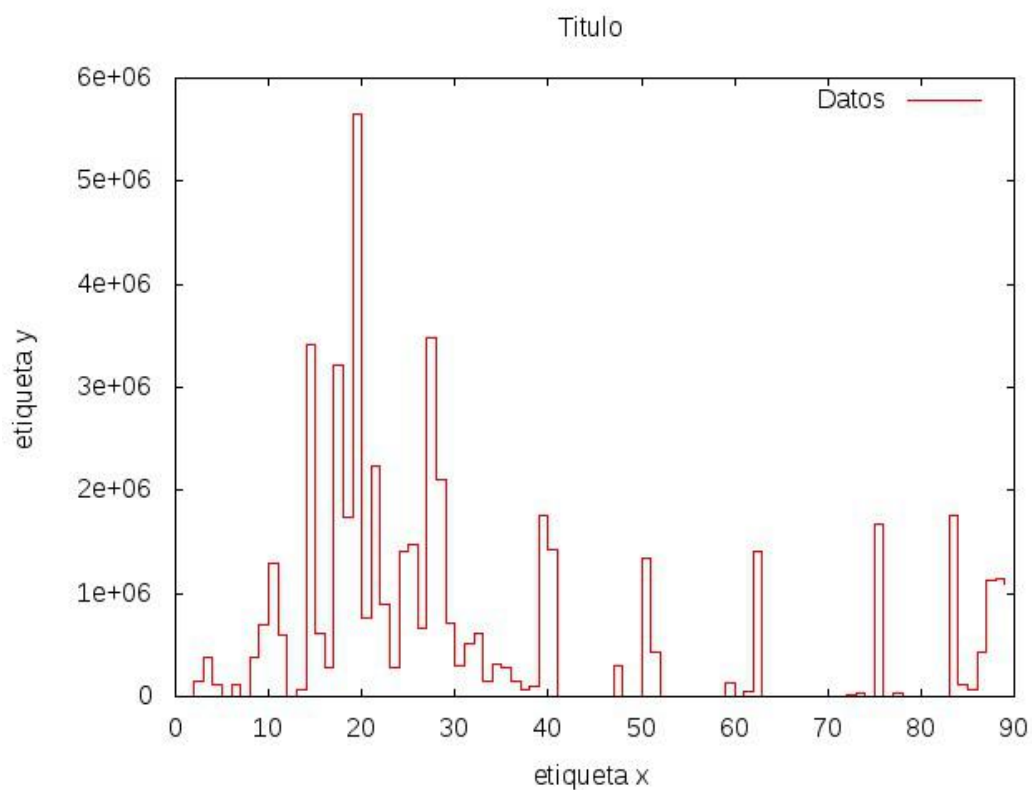
Puerto UDP destino 8024



se podría suponer que el receptor estaría viendo algún vídeo, ya sea en el ordenador o la television.

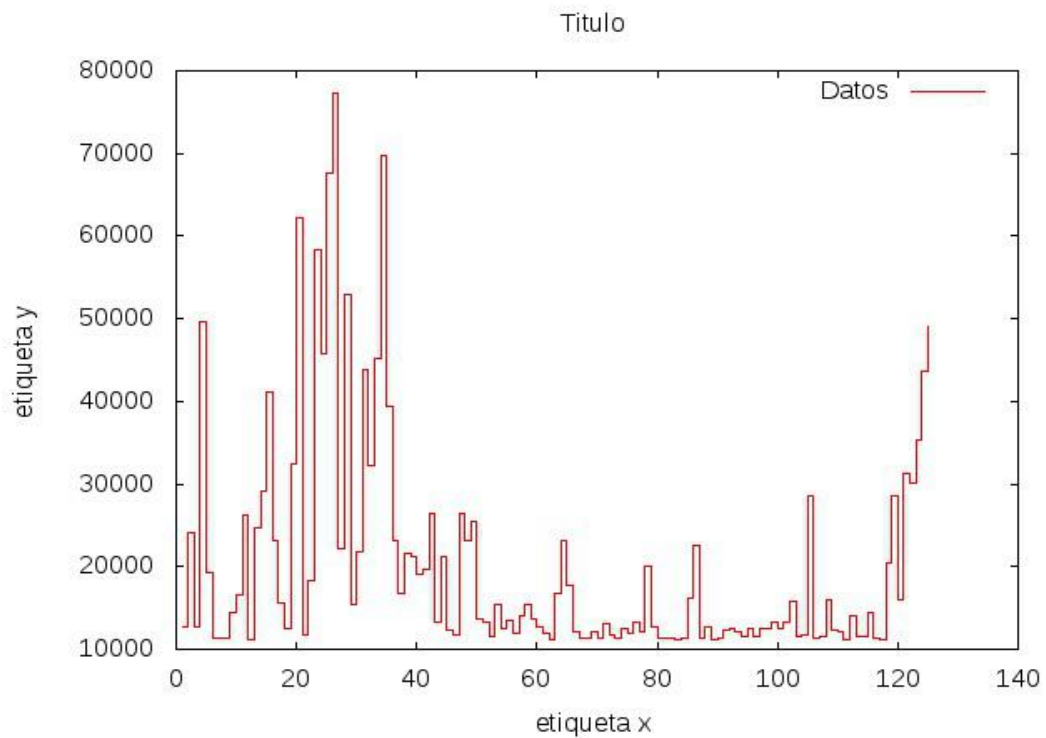
8.Figura (o figuras) que muestre(n) el caudal/*throughput*/tasa/ancho de banda a **nivel 2 en bits por segundo (b/s)** y por sentido (asuma que la dirección Ethernet origen o destino es la indicada por el generador de trazas).

MAC origen 00:11:88:CC:33:9B



como vídeos o algún archivo de gran tamaño, que se des-fragmenta. Una vez terminada la transmisión, el flujo de información es mas normal, parecido a la navegación por la web.

MAC destino 00:11:88:CC:33:9B



El nivel de actividad recibiendo información es muy similar al nivel de actividad enviando, exceptuando

el ultimo tramo de tiempo en el que recibe cierta información adicional como puede ser un vídeo streaming.

Conclusiones:

La red se comporta de forma normal cuando se ve algun video en la television o en el ordenador el uso de la red aumenta como es normal, ya que se envian paquetes de forma mas constante y con un tamaño de informacion mayor. Ya que se trata de la recepcion de video streaming y no de emision, solo existe trafico UDP en recepcion, y no en transmision. Ademas del envio continuo de informacion, al tratarse de un streaming se reciben datos continuamente exceptuando los momentos en los que se deja de consumir contenido, que el trafico disminuye.