Práctica 3: Análisis de tráfico

Número de pareja y DNI (para ejecutar el programa): 11 y 02746297

1. Abre, lee, cierra un fichero de captura

- ¿Cuántos paquetes tiene el fichero? **1340**
- ¿Cuál es el tamaño medio del paquete? **327**
- ¿Cuál es la tasa media en bps (bits por segundo) del enlace que monitoriza la traza? ¿Y en pps (paquetes por segundo)? **89938 bps y 34 pps**

2. Abre, recorre, cierra un fichero de captura

- ¿Cuál es la tasa (en Mb/s) del tráfico con MAC destino 90:fb:a6:86:32:93? **61926 bps**
- ¿Y con MAC origen: 90:fb:a6:86:32:93? **11277 bps**
- ¿Cuántos paquetes hay que no tengan esta MAC en origen ni en destino? **501**

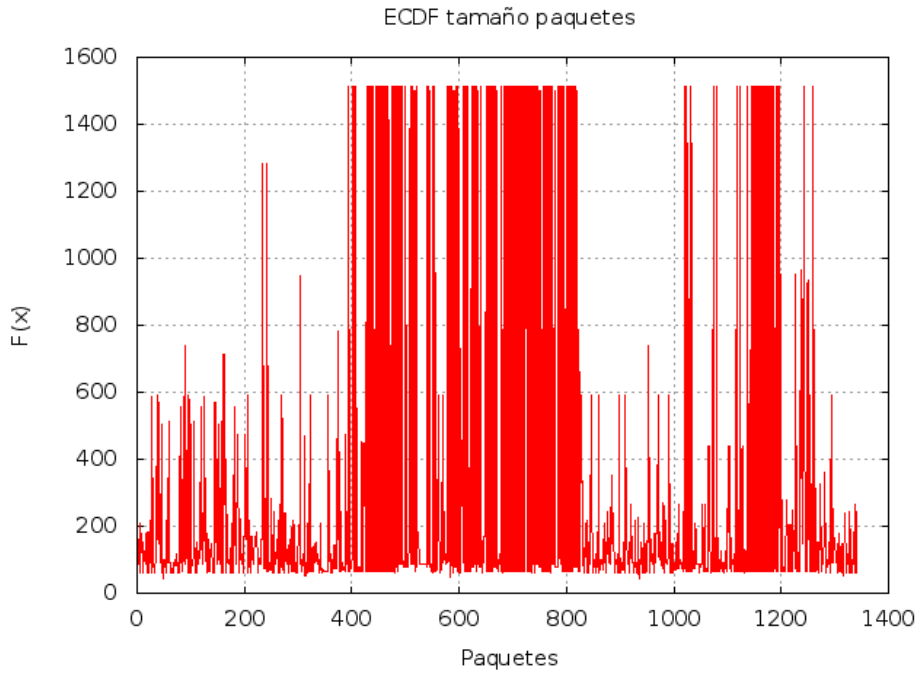
3. Análisis de protocolos a nivel de paquetes

- ¿Cuántos paquetes de la traza son IP? **1102** ¿y ARP? **108** ¿y hay otro tipo de paquetes? En caso afirmativo ¿sabrías decir que paquetes son? **Sí, hay 130 paquetes IPv6**

- De los paquetes IP, ¿cuántos paquetes TCP hay en la traza? **641** ¿y UDP? **374** ¿e ICMP? **80** ¿Hay paquetes de otros protocolos? En caso afirmativo ¿sabrías decir que paquetes son? **Si hay 1102 paquetes IP y 641 son TCP, 374 son UDP y 80 ICMP (1095 en total), tenemos 7 paquetes no conocidos que serán, viendo la traza en Wireshark, IGMPv2, IGMPv3 y PIMv2.**

- Abrir la traza con Wireshark y anotar la dirección IP origen y destino así como el puerto origen y destino del tercer paquete. Usar dicha información en el programa en C para obtener el número de paquetes y la tasa media (bps) del flujo UDP definido por la información extraída. **Tasa flujo: 66 bps y paquetes flujo: 2**

- Pintar la ECDF para el tamaño de los paquetes. ¿Se observa alguna moda? ¿Qué porcentaje paquetes son mayores de 400 bytes? **Se observa una moda en 1500 bytes (que deben ser http) y la gran mayoría de paquetes son mayores de 400 bytes (aprox. Un 80%).**



• ¿Cuáles son los 5 puertos (destino y origen) más populares tanto en número de paquetes como en número de bytes? ¿A qué se debe la diferencia de popularidad en paquetes y en bytes?

La diferencia se debe a que puede ser que un puerto reciba menos paquetes pero de un tamaño mayor y por ello esté en el top 5 en bytes pero no en paquetes o al revés. Por ejemplo, un puerto que reciba pocos paquetes pero todos de HTTP no estará en el top 5 de paquetes pero si de bytes.

Puertos más populares	Origen	Destino
Paquetes	Puerto 64: 229 paquetes Puerto 41316: 130 paquetes Puerto 68: 92 paquetes Puerto 1: 68 paquetes Puerto 37: 60 paquetes	Puerto 64: 247 paquetes Puerto 41316: 130 paquetes Puerto 289: 84 paquetes Puerto 68: 75 paquetes Puerto 1: 70 paquetes
Bytes	Puerto 64: 239910 bytes Puerto 287: 49845 bytes Puerto 68: 23858 bytes Puerto 41316: 11804 bytes Puerto 43296: 7908 bytes	Puerto 41316: 177114 bytes Puerto 43296: 41050 bytes Puerto 41317: 35527 bytes Puerto 64: 29242 bytes Puerto 289: 14021 bytes