Practica 1 - Ejercicio 2

Apartado 1

Hemos seguido las instrucciones dadas al pie de la letra y hemos analizado superficialmente el tráfico capturado por wireshark al ejecutar `sudo hping3 -S -p 80 www.uam.es`, lo hemos guardado en un archivo (tras deshabilitar el formato pcap-ng en las opciones de wireshark), y lo hemos vuelto a abrir para ver que se conservaba la integridad de los datos.

Hemos añadido también las columnas PO y PD desde **Edit>Preferences>Columns**, para comprobar que hay un único paquete con campo PO=53.

Apartado 2

2.1

Para filtrar los paquetes de tipo ip, con tamaño de paquete mayor que 1000 Bytes, usamos el filtro:

```
ip and ip.len>1000
```

2.2

Para exportar los paquetes mostrados tras aplicar el filtro, dentro de wireshark **File>Export Specified packets** y elegimos **Displayed** en el menú que aparece.

2.3

Comparando el tamaño de los cinco primeros paquetes IP junto con sus cabeceras, podemos ver que la diferencia de tamaño entre el protocolo ip y el tamaño del paquete IP es de solo unos pocos bytes (14 en nuestro caso) que se deben a la cabecera extra del paquete que no corresponde al protocolo IP.

Apartado 3

Para añadir la columna pedida, una vez abierto Wireshark, **Edit>Preferences>Columns** y añadimos la columna **Delta Time** con el nombre interarrival, seleccionamos **Display**.

Apartado 4

Para cambiar la visualización de la fecha, **View>Time display format** y seleccionamos **Time of day** para el primer apartado, con la visualización para humanos, o **Seconds since Epoch (1970-01-01)** para la visualización en segundos desde el 1 de enero de 1970.

Apartado 5

Abrimos wireshark, pulsamos el botón configuracion, y en el menu abierto, pulsamos el boton **Capture filter** y seleccionamos **UDP Only**. Aceptamos y comenzamos la captura. Una vez ejecutado el comando `sudo hping3 -S -p 80 www.uam.es.` esperamos unos segundos, paramos la captura, y comprobamos que, efectivamente, todo el trafico capturado es UDP.