Ejercicios de captura de tráfico

1. Durante la realización de las prácticas, será muy común disponer de una consola donde ejecutaremos comandos que mandan y reciben tramas por un interfaz de red. En paralelo tendremos en ejecución a Wireshark, que estará capturando el tráfico que nos interese. Este ejercicio muestra un ejemplo típico a realizar en prácticas posteriores:

1. Abra una consola o *shell*, y déjela abierta en espera de ejecutar algún comando.
2. Ejecute Wireshark y seleccione y configure el interfaz por el que se capturará el tráfico (habitualmente será **eth0**) Acuérdese de seleccionar las opciones de visualización que más le convenga.
3. Inicie la captura de tráfico pulsando en el botón 'Start'.
4. Vuelva a la consola y ejecute el siguiente comando (tecléelo y pulse <enter>):

   ```
   $ sudo hping3 -S -p 80 www.uam.es
   ```

5. Detenga la captura de tráfico mediante el botón 'Stop'.
6. Analice el tráfico capturado (aunque no lo entienda en detalle)
7. Guarde la traza en un fichero **(Importante: no utilizar el formato pcap-ng)**.
8. Cierre Wireshark, y vuelva a abrirlo.
9. Abra el fichero almacenado y compruebe que se almacenó correctamente.
10. Utilizando las columnas que se han añadido durante el tutorial, ordene con respecto al campo 'PO' en sentido descendente y contabilice el número de paquetes en el que este campo tiene valor 53.

Describa el proceso realizado y discuta los problemas que haya encontrado durante la realización del ejercicio.

2. Tras haber leído las documentación online facilitada, empiece a capturar tráfico. Abra un navegador y genere tráfico a partir de la visualización de páginas web. Pare la captura, y añada un filtro en el interfaz de modo que solo se visualicen paquetes que sean de tipo IP y que tengan un tamaño de paquete mayor a 1000 Bytes.

1. Copie el filtro realizado.
2. ¿Cómo almacenaría en una captura solo los paquetes mostrados?
3. Compare el tamaño del primer paquete IP, y el campo 'length' del protolo IP del mismo. Repita para los primeros 5 paquetes, ¿qué relación encuentra?

3. Añada una columna llamada *interarrival* que muestre el tiempo entre paquetes consecutivos. Explique brevemente qué menús y opciones ha seleccionado.

4. Modifique la forma en que Wireshark muestra la información en la columna 'Time' de cada paquete. En concreto muestre los tiempos en formato para humanos, y en tiempo Unix con resolución en segundos. Explique brevemente los pasos realizados.

5. Inicie una captura en Wireshark pero aplicando **filtros de captura**, en concreto solo queremos capturar tráfico UDP. Mientras captura tráfico, genere durante algunos instantes

tráfico a partir de la visualización de páginas web, y ejecute al mismo tiempo en una consola el comando

```
$ sudo hping3 -S -p 80 www.uam.es.
```

Compruebe que solo se capturan paquetes UDP, y describa brevemente los pasos realizados.