**EJERCICIOS DE CAPTURA DE TRÁFICO**

**EJERCICIO 1.**

**-Paso 1.** Abrimos Wireshark con el comando “sudo wireshark-gtk”. De esta forma obtendremos los permisos necesarios.

Texto

Descripción generada automáticamente

**-Paso 2:**

**-2.1** Ejecutamos Wireshark.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-2.2** Configuramos la interfaz a capturar (ens33).

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-Paso 3.** Utilizamos el botón “Start” para iniciar la captura.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**-Paso 4.** En una nueva terminal, ahora escribimos el comando “sudo hping3 -S -p 80 [www.uam.es](http://www.uam.es)”

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-Paso 5.** Utilizamos el botón “Stop” para detener la captura de tráfico.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-Paso 6.** Analizamos el tráfico capturado:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

En la anterior captura podemos apreciar en la parte superior todos los paquetes capturados, por ejemplo, el primero … Después de seleccionar dicho paquete, podemos observar en la parte media, la decodificación del paquete seleccionado, viendo así datos relevantes como:

Imagen que contiene Aplicación

Descripción generada automáticamente

Por último, también podríamos comentar el volcado hexadecimal del paquete analizado previamente, con tan solo dar click en algún campo como por ejemplo … podemos ver que … bytes le configuran. Estos bytes se encuentran alineados en grupos de 16.

**-Paso 7.** Guardamos la traza en un fichero con formato pcap.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-Paso 8.** Cerramos Wireshark y después volvemos a abrirlo. Solo tendríamos que repetir el paso 1 con su respectiva captura.

**-Paso 9.** Abrimos el fichero que habíamos previamente guardado para comprobar que se almacenó correctamente.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-Paso 10:**

Los puntos 10.1 y 10.2 se realizan al principio de manera igual, por tanto, para los puntos comunes pondremos solo una captura de pantalla.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Abrimos el menú de columns, añadimos el tipo de campo que queremos para la nueva columna y pulsamos añadir.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**-10.1** Añadimos columna ‘PO’.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Para cambiar el nombre, simplemente pinchamos en el nombre actual y escribimos PO

**-10.2** Añadimos columna ‘PD’.

Procedemos de la misma forma que en 10.1 seleccionando esta vez el campo Dst port (unresolved) y cambiamos su nombre por PD.

Resultado final al añadir las dos columnas:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-10.3** Ordenamos en sentido descendente respecto al campo “PO”.

Para ordenar en orden descendente los paquetes según el valor de “PO”, tenemos dos opciones. O bien dar clic sobre el nombre de la columna (“PO”) hasta que veamos una flecha hacia abajo, o bien dar click derecho y seleccionar la opción de descendente.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**-10.4** Contabilizamos el número de paquetes en el que el campo “PO” tiene valor 53.

Utilizamos un filtro de visualización (udp.port==53) que nos muestre los puertos de origen y destino con valor 53 y observamos que solo existe un paquete en el que el campo “PO” tiene valor 53.

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Algunos problemas que encontramos durante la realización de este ejercicio fueron:

* La interfaz para capturar no fue eth0 como el enunciado indica sino ens33.
* Wireshark daba algunos problemas como “gtk\_box\_gadget\_distribute assertion 'size = 0' failed in gtkscrollbar”, el cual se arregló reajustando la ventana.
* Además, al ordenar los paquetes en orden descendente según el campo PO, nos costó un poco darnos cuenta de que no se ordenan absolutamente todos, sino que se van ordenando agrupados por tipo.

**EJERCICIO 2.**

**2.1 Filtro realizado:**

ip && frame.len > 1000

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Hasta este momento no teníamos paquetes tan grandes, asi que hemos reruneado la captura y abierto un navegador para tenerlos.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**2.2 Almacenar la captura de los paquetes mostrados:**

Exportamos y guardamos el fichero con formato pcap.

Desplegamos file🡪Export Specified Packets y nos lleva a esta ventana:

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

**2.3 Después de comparar el tamaño del primer paquete IP, y el campo “length” del protocolo IP del mismo, y repetir este proceso para los primeros 5 paquetes, observamos:**

Que el valor del campo “length” es de 1514 bytes, el cual coincide con el valor de la parte de decodificación.

Además, se observa que entre el ‘frame.len’ e ‘ip.len’ hay 14 unidades de diferencia, valor que coincide con el tamaño del header.

**EJERCICIO 3.**

**3.1** Desplegamos la opción de “Edit” y seleccionamos “Preferences”.

**3.2** Seleccionamos “Columns”.

**3.3** En el menú de la derecha, añadimos una nueva columna con el nombre de “interarrival” y del tipo “Delta time displayed”.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**EJERCICIO 4.**

Realizamos los pasos del ejercicio 3 hasta llegar al menú de las columnas. Una vez ahí, seleccionamos el “field type” correspondiente a ‘UTC Date’.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**EJERCICIO 5.**

**5.1** Utilizamos el filtro “udp”.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**5.2** Generamos tráfico.

**5.3** Ejecutamos en la terminal el comando “sudo hping3 -S -p 80 [www.uam.es](http://www.uam.es)”.

**5.4** Comprobamos que solo se capturan paquetes UDP.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente