José Ignacio Gómez García y Óscar Gómez Borzdynski

Ejercicios de captura de tráfico:

1)

Tras abrir Wireshark y seguir el tutorial para añadir las columnas y elegir las opciones de visualización que nos interesan, comenzamos a capturar el tráfico de nuestra interfaz de red (eth0).

Realizamos el hping3 al puerto 80 de la página de la UAM, obteniendo así tráfico en nuestra interfaz, comprobamos que Wireshark está recopilando esa información y mostrándonosla por pantalla.

Analizamos el tráfico capturado, vemos algunos protocolos NTP y DNS, luego la mayoría pasan a ser TCP con dirección a 150.244.214.237.

Guardamos el fichero mediante el botón de “guardar como” en formato .pcap, reiniciamos el programa y abrimos el fichero, vemos que todo se ha guardado correctamente.

Ordenando los paquetes por el puerto de origen, encontramos que solo 1 paquete proviene del puerto 53.

2)

El filtro utilizado ha sido: ip and ip.len > 1000

Para guardar la captura podemos utilizar la función “Export Specified Packets” en la pestaña “File”, seleccionamos “Displayed” y elegimos el formato pcap.

En nuestro caso los primeros 5 paquetes IP tienen una longitud de 1492 bytes, aunque no sabemos si es alguna coincidencia.

3)

Para crear la columna interarrival, hemos entrado a las preferencias de Wireshark, en el apartado columnas y hemos añadido una nueva con el nombre adecuado. En el tipo de campo hemos utilizado “Delta time”

4)

Para realizar este ejercicio, añadimos otra columna que llamaremos time. Para mostrar el tiempo en formato para humanos seleccionaremos el tipo “Absolute date and time”. En la pestaña “View” encontramos la opción “time Display Format”, donde escogeremos la precisión en segundos.Para la fecha UNIX, seleccionaremos “UTC date and time” en la columna y en el apartado “Time Display Format” elegiremos “Seconds Since Epoch (1970-01-01)”

5)

Antes de comenzar la captura le damos al botón de opciones de captura, en los filtros añadiremos “udp” y comenzaremos a capturar. Podemos comprobar que todos los paquetes recibidos son UDP.