Practica 1. Redes 1

VM y Wireshark (wireshark_captura.pcap se corresponde con practipa1.pcap)

Ejercicio 1:

El proceso que hemos seguido es el siguiente:

1) Hemos ejecutado Wireshark y lo hemos configurado para se capture el tráfico de "eth0".

2) Iniciamos la captura de tráfico mientras que comenzamos a navegar para que pueda captar los paquetes que se intercambian y podamos analizar los resultados obtenidos.

3) En este caso introducimos por consola el comando "sudo hping3 -S -p 80 www.uam.es" por el cual accedemos a la página de la uam.

4) Paramos el tráfico y lo guardamos en un archivo .pcap.

5) Al volver a abrir la captura almacenada lo que observamos son los paquetes que hemos obtenido de la captura realizada; más concretamente nos vamos a fijar en las dos columnas que previamente hemos añadido:

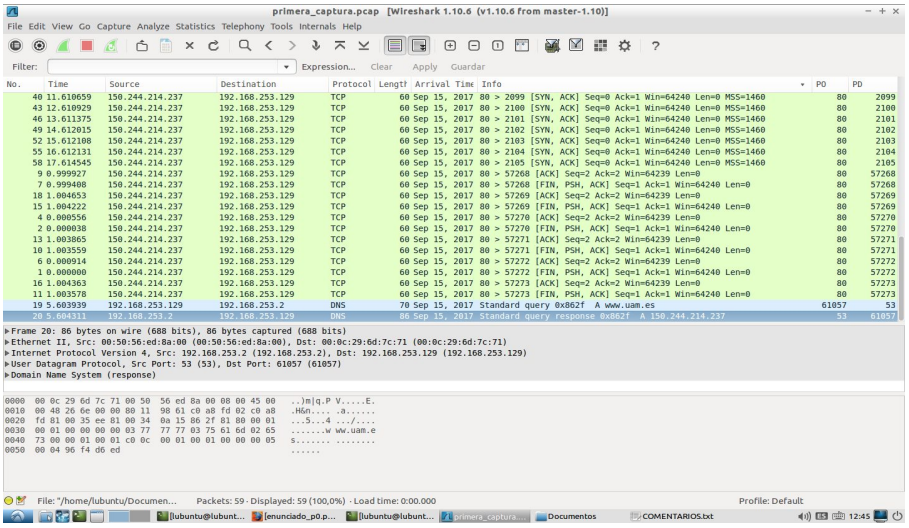
-PO: puerto de origen.

-PD: puerto de destino.

En estas columnas observamos que el puerto número 53 aparece una única vez en cada columna (PD y PO). Este puerto se corresponde con la página que hemos buscado por terminal. Esto quiere decir que lo que estamos preguntando por debajo al ordenador es la dirección IP de 150.244.214.237; es más, si buscamos en la columna de puerto de destino el número 53 vemos que se corresponde con la dirección de www.uam.es.

Los problemas que nos hemos encontrado a lo largo de la realización del ejercicio no han sido muchos ni importantes.

Simplemente lo que nos costó al principio fue familiarizarnos con el programa y posteriormente entender lo que
significaban cada uno de los datos que nos proporcionaba Wireshark.



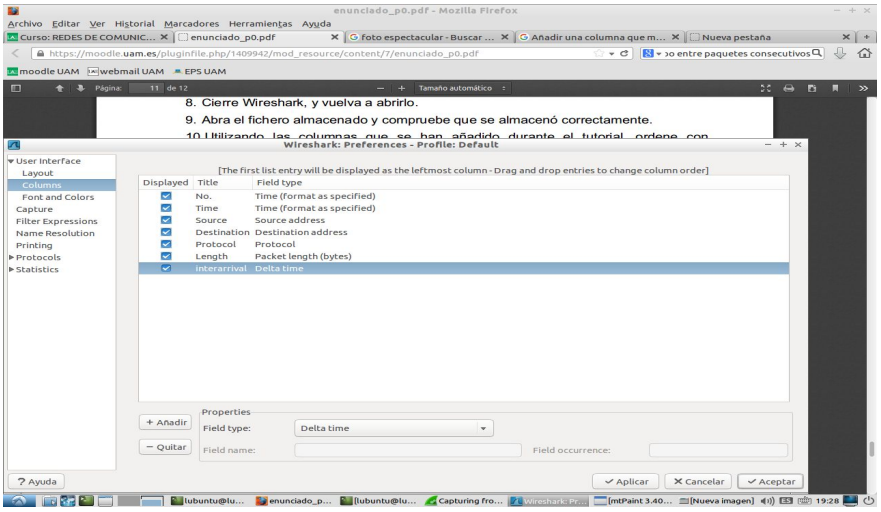
Ejercicio 2:

En este ejercicio lo primero que hicimos fue generar una captura de tráfico mediante la visualización de páginas web. Posteriormente cuando nos pidieron que aplicásemos ciertos filtros a la captura realizada vimos que teníamos dos opciones. La primera de ellas la encontrábamos a la hora previa de hacer la captura (más concretamente en su configuración), donde se nos daba la oportunidad de aplicar directamente un filtro(por ejemplo ip), para que todo el tráfico capturada tuviera que cumplir la condición de ser una dirección IP y ya después una vez finalizada la captura escribir en el apartado de “Filter” lo siguiente: “frame.cap_len>1000” de tal forma que sólo nos aprezcan los paquetes IP mayores de 1000 bytes(dato que apreciamos en la columan de “Length”). La segunda opción que vimos, y por la cual nos decantamos, es la de aplicar los dos filtros a la vez, escribiendo en el apartado de “Filter” lo siguiente: “ip && frame.cap_len>1000”. A la hora de almacenar la captura con los filtros que nos pedían no hayamos la solución para que aparecieran los dos a la vez. Por lo que la solución que vimos era hacer una captura de tráfico normal y una vez hecha, al abrirla introducir los dos filtros. El tamaño de los paquetes IP en comparación con el tamaño del protocolo IP es una diferencia de 14 bytes en cada uno de los casos (eso sí sólo entre los que son direcciones IP). Esta diferencia se debe a que la cabecera de una dirección IP es siempre de 14 bytes independientemente del paquete.

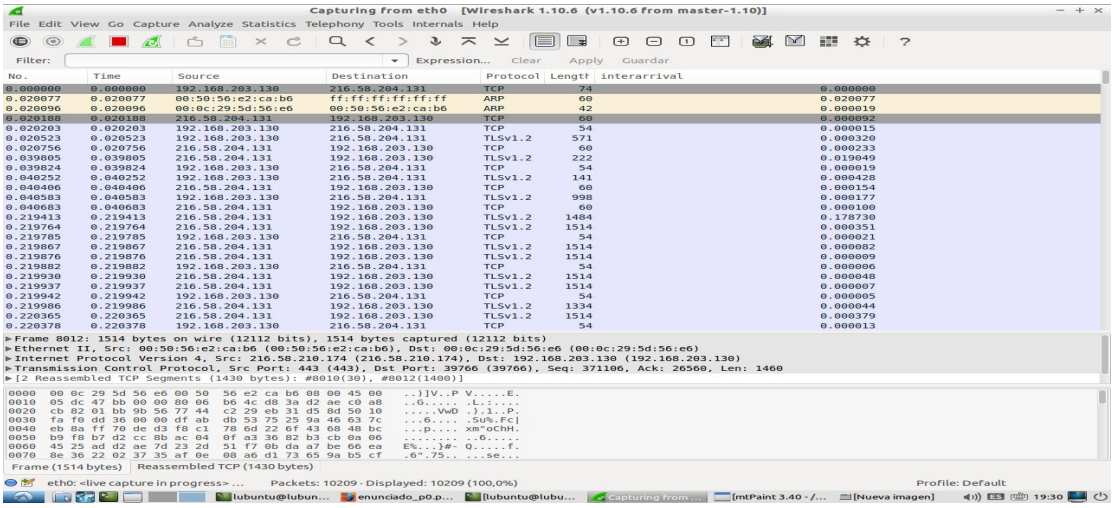
Ejercicio 3:

Para añadir una columna en la que se especifique el tiempo entre paquetes consecutivos cliqueamos al menú 'Edit'->'Preferences'. Aparecerá la ventana de edición de preferencias, en la que podremos configurar distintos aspectos de Wireshark. Entramos en el apartado 'User Interface'→'Columns' nos aparecerá la opción de añadir unas columnas a las ya existentes. Elegimos esta opción y designamos a esta columna con el nombre de “interarrival” . A continuación, elegimos en “Field Time” la opción de “Delta Time” que es la que nos ofrece el valor requerido.

En esta imagen se ve cómo añadimos la columna de “interarrival”:



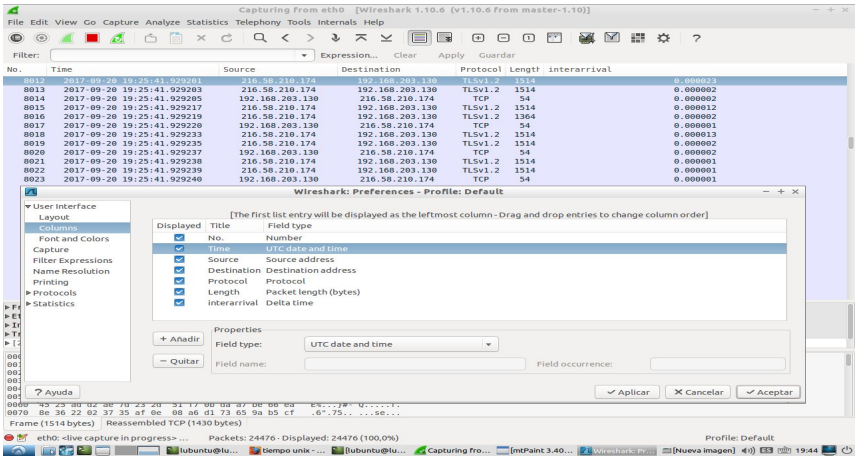
En esta imagen vemos cómo se ven los valores del interarrival:



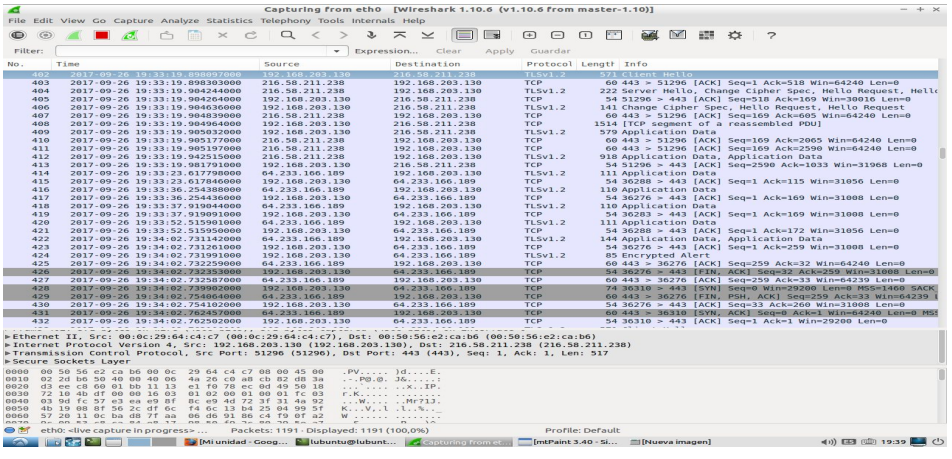
Ejercicio 4

Modificamos la columna del tiempo para que este se muestre en formato humano y formato UNIX. Para el formato humano establecemos el tiempo como UTC date and time, mostrándose así la fecha y hora actual. Para establecer el tiempo UNIX, segundos transcurridos desde el 1 de Enero de 1970, cambiamos la configuración de medida del tiempo. Para ello, vamos a View → Time Display Format → Seconds since 1970-01-01

En esta imagen vemos cómo añadimos el tiempo UTC:



En esta imagen vemos el tiempo unix de cada paquete en la columna:



Ejercicio 5

En este ejercicio lo que hicimos fue en la configuración previa a la captura de paquetes establecer como filtro que sólo fueran paquetes UDP los paquetes capturados. De esta forma al ejecutar el comando “sudo hping3 -S -p 80 www.uam.es.” en la terminal, todos los paquetes capturados por el programa Wireshark se ven que son UDP. Esto lo podemos ver en la ventana del medio, clickeando sobre “Internal Protocol” vemos que todos son del tipo especificado.

Vemos que todos los paquetes son DNS, cuyo protocolo interno es UDP.