Ejercicios Wiresark

Ejercicio 1. Abrimos wireshark con el comando sudo wireshark-gtk para que nos de los permisos correspondientes. Capturamos la interfaz ens33. Al usar el comando dado en el apartado 4, empezamos a observar en el programa tráfico de paquetes. Guardamos la traza en un fichero llamado practica1.pcap.

Hemos abierto el fichero y visto que se almacenaba correctamente. Lo ordenamos respecto al campo ‘PO’ y vimos que había un paquete con el valor 53 en ese campo.

Ejercicio 2. El filtro realizado ha sido ip && len > 1000. Almacenamos la captura guardándola como un archivo .pcap

Si seleccionamos el primer paquete, podemos ver que su length es 1514 bytes y en la parte de decodificación también es de 1524 bytes

Ejercicio 3. Clickamos en edit, preferences, columns, añadimos una nueva columna nombrada interarrival, del tipo delta time displayed.

Ejercicio 4. Clikcamos en edit column details, y en el field type seleccionamos UTC date

Ejercicio 5. Usamos el filtro indicado, udp, empezamos la captura, escribimos el comando indicado y realizamos una búsqueda de páginas webs, comprobando que los resultados solo son del tipo User Datagram Protocol