

Ejercicios de captura de tráfico

Ejercicio1

Lo primero que se nos pide en el ejercicio es abrir una shell, la cual dejaremos abierta a espera de ejecutar algún comando, a continuación configuramos la interfaz para linux ens33 (para MacOSX en0).

Iniciamos la captura de tráfico con Wireshark y ejecutamos el comando `sudo hping3 -S -p 80 www.uam.es`. Tras unos segundos dejamos de capturar paquetes de red. El siguiente paso es analizar la traza que se ha generado (Imagen1), como podemos observar

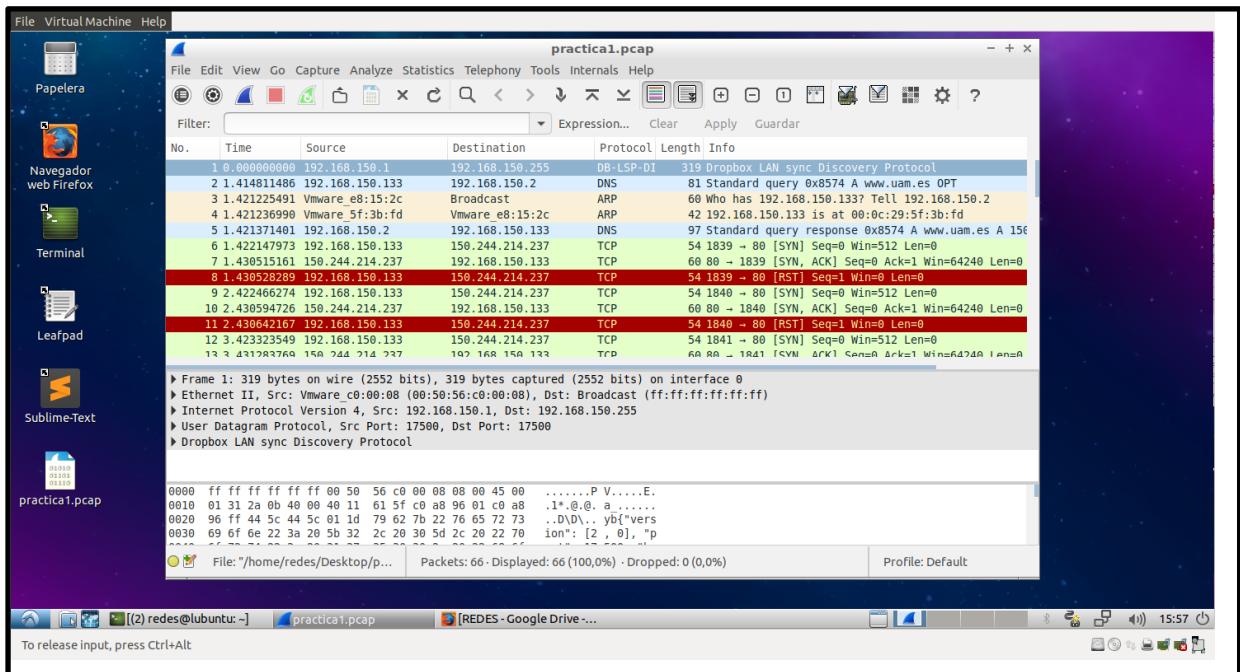


Imagen 1

que la interfaz de Wireshark está dividida en 3, en el primer segmento se encuentra un tabla donde se van situando los paquetes capturados y en la fila de cada paquete para cada columna se muestra cierta información del propio paquete. En el segundo segmento se muestra la información de cada uno de los niveles del paquete seleccionado por el usuario y finalmente en el tercer segmento se muestra la misma información que en el segundo solo que en bytes. A continuación, cerramos Wireshark y abrimos el fichero .pcap de la captura que hemos realizado hace unos instantes. En este punto añadimos una columna de nombre 'PO' en sentido descendente y contamos el número de paquetes que tienen como valor un 53 en este campo, en nuestro caso sólo hemos capturado un paquete que cumple dicha condición.

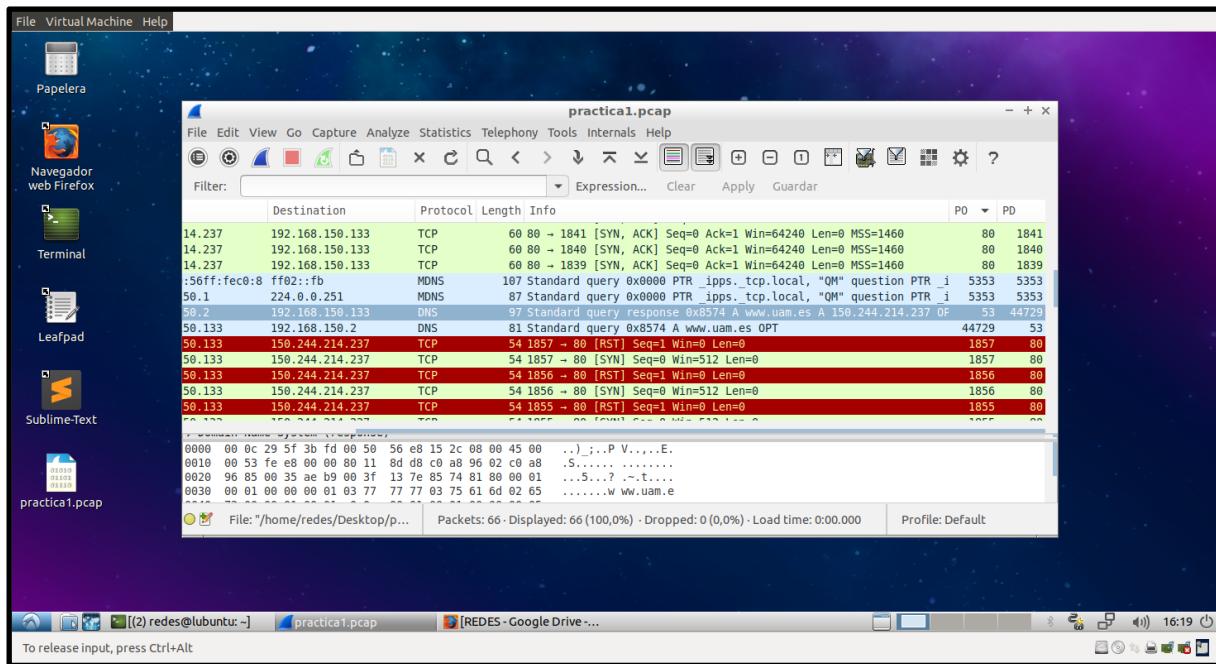


Imagen 2

Ejercicio2

Para mostrar únicamente los paquetes de más de 1000 Bytes, utilizamos el filtro “frame.len > 1000 and ip” (Imagen3)

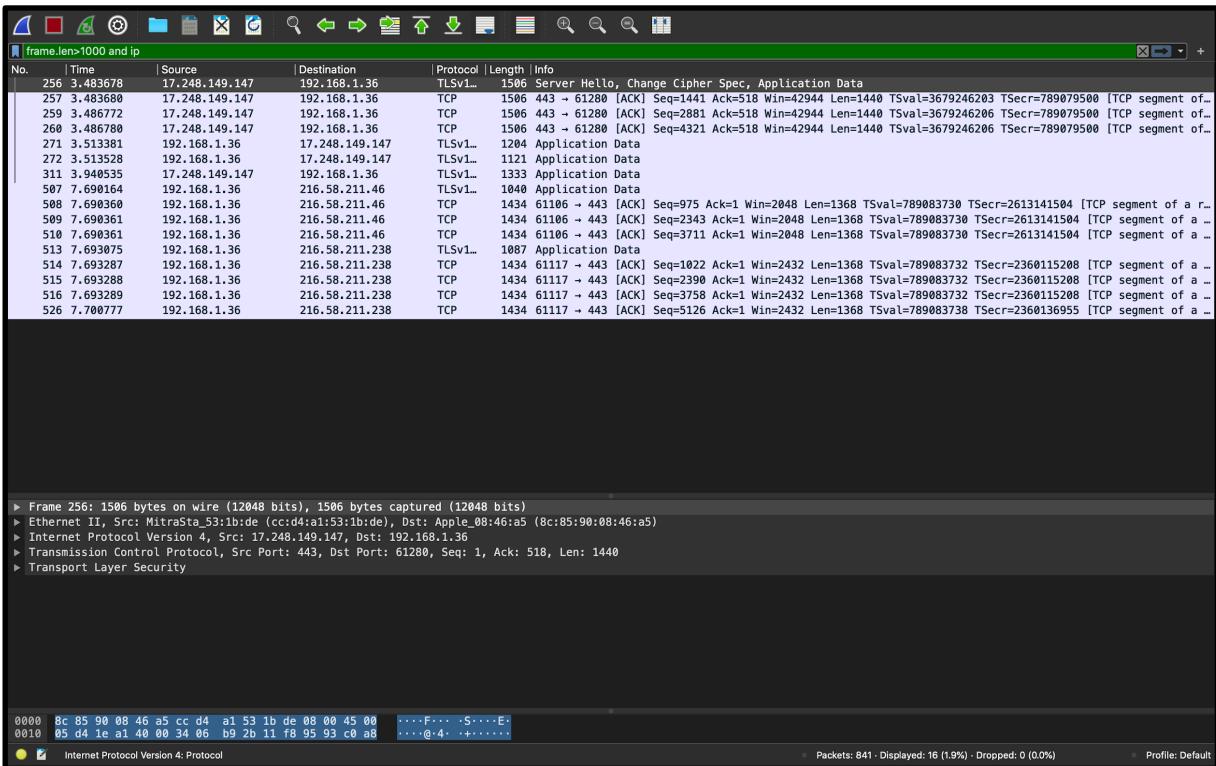


Imagen3

Para guardar esta captura con el filtro aplicado bastaría con aplicar el filtro, exportar el archivo desde Wireshark mediante la opción “Export Specified Packets...” y seleccionar “Displayed” (Imagen4)

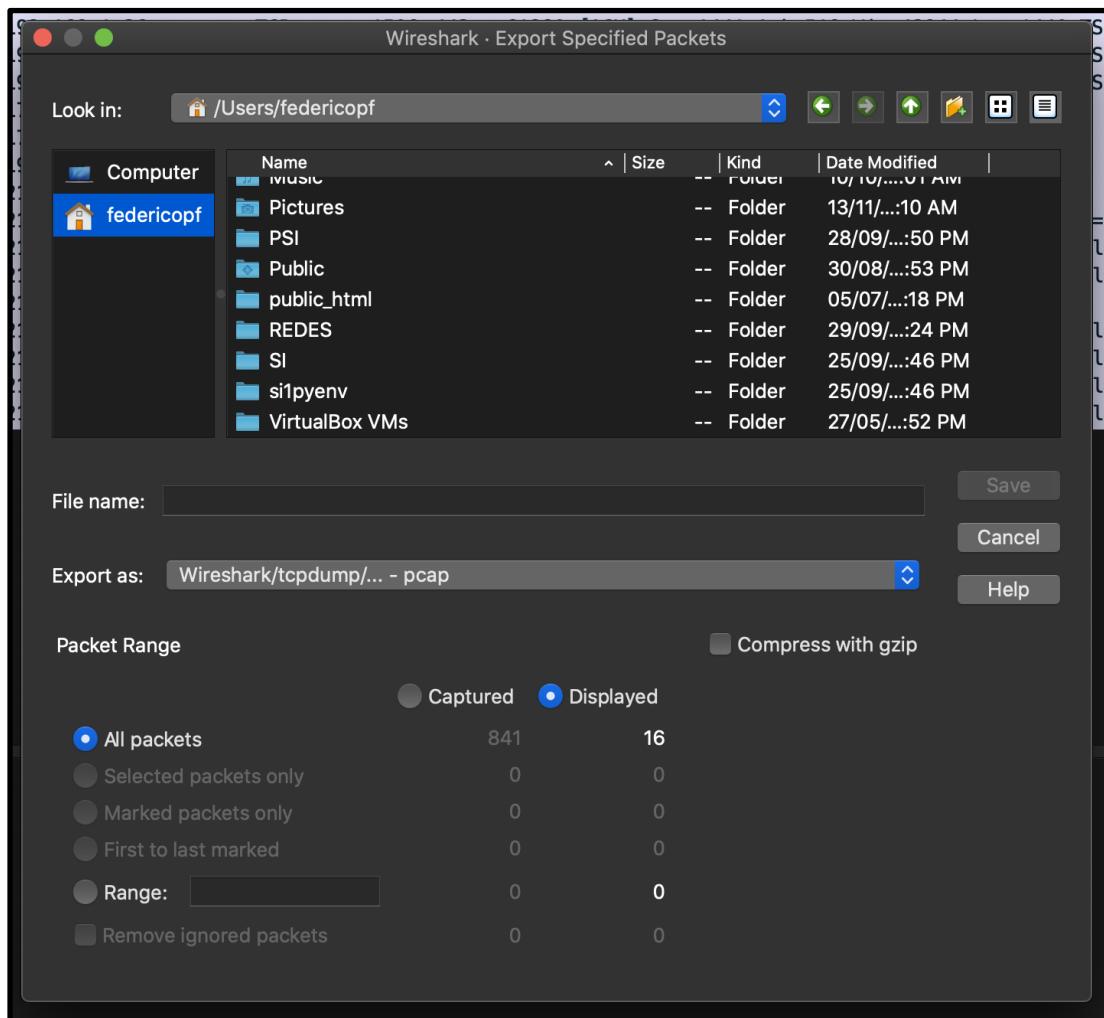


Imagen4

Debido a la estructura en capas de los distintos protocolos de la red (pila de protocolos), podemos observar como el tamaño varía según el protocolo que se observe del paquete. En el caso de IP, el tamaño marcado por el campo “length” es menor al que se muestra en el mismo campo del protocolo TCP ya que este último añade su cabecera y aumenta el tamaño del paquete.

Ejercicio3

Para añadir la columna “interarrival” que muestra el tiempo entre paquetes consecutivos, hemos hecho click sobre cualquier paquete de la traza y hemos desplegado la información correspondiente al frame que se encuentra en segundo segmento, donde buscamos el campo en el que se nos muestra el tiempo delta de la captura del paquete previo, hacemos click derecho sobre dicha información donde se nos desplegará un menú y en él seleccionaremos la opción de aplicar como columna y ya tendremos la columna “interarrival” añadida (Imagen5).

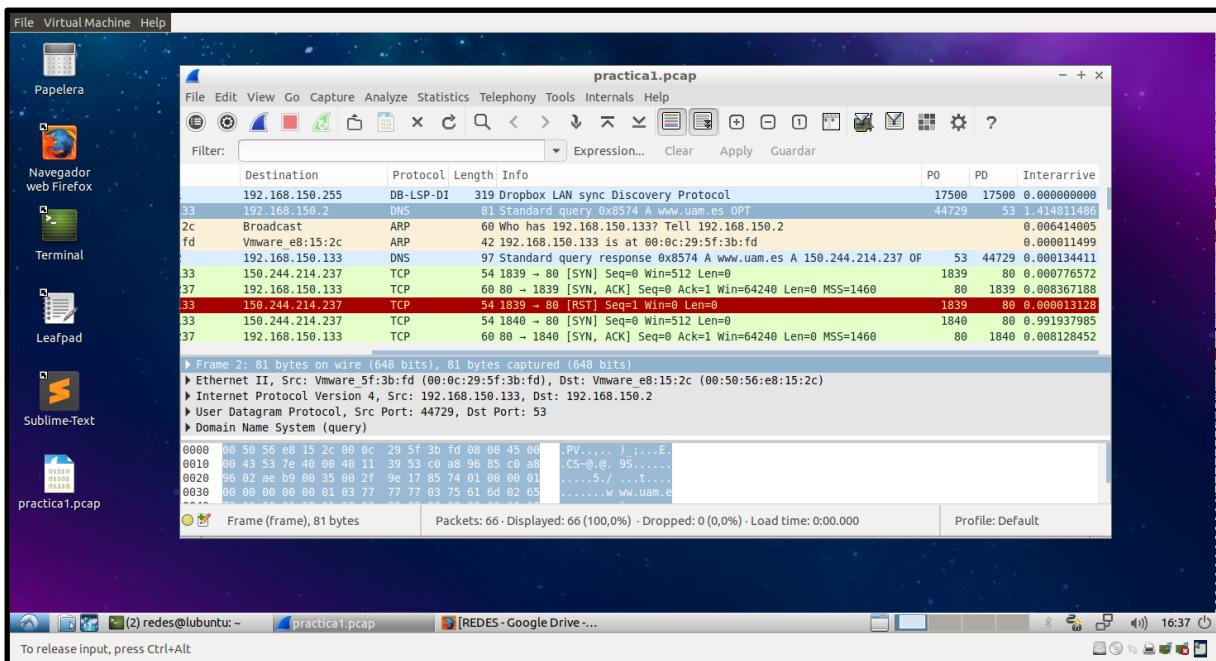


Imagen5

Ejercicio4

Para modificar la columna “Time” y ver el tiempo en formato humano en Wireshark basta con hacer click-derecho sobre la propia columna, seleccionar “Edit Column” y escoger la opción deseada, en este caso “UTC as YYYY-MM-DD” (Imagen6).

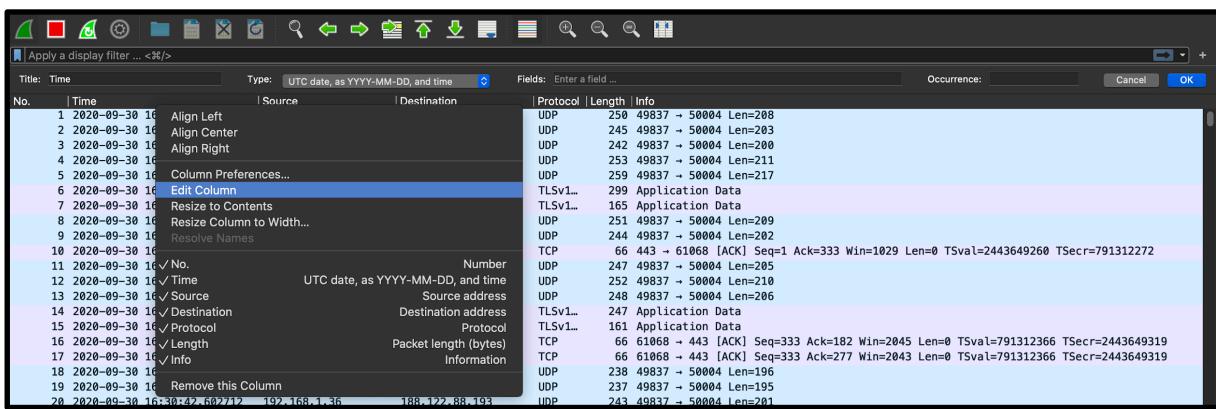


Imagen6

Por otro lado, para mostrar el tiempo Epoch, seleccionamos el apartado “Frame” en el recuadro del medio de Wireshark y hacemos click-derecho sobre el campo “Epoch time” y seguidamente en la opción “Apply as column” para agregar el campo como columna a nuestro recuadro superior (Imagen7).

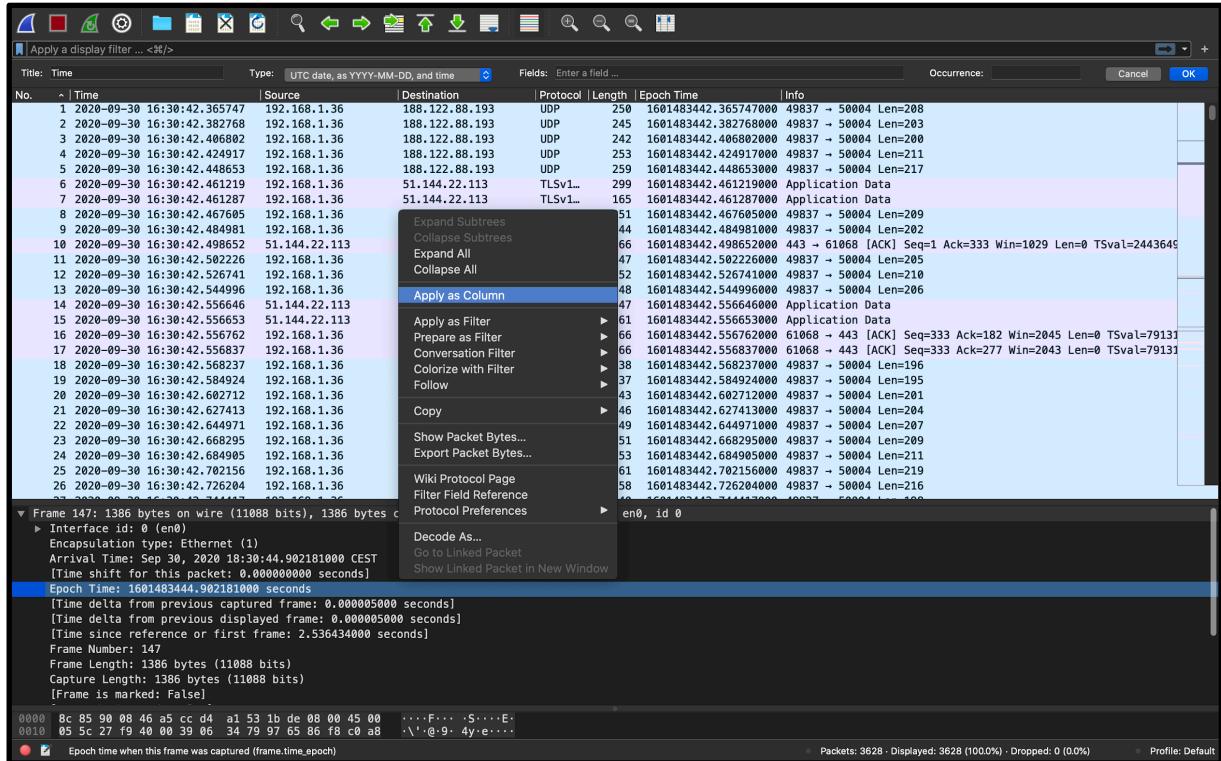


Imagen7

Ejercicio5

Para realizar un captura de una traza con filtros, tenemos que hacer click sobre el icono que tiene como imagen una rueda de engranaje, donde se nos desplegará una ventana donde podremos elegir los filtros que queremos añadir, elegimos como interfaz en nuestro caso o bien ens33 para ubuntu o bien en0 para MacOSX, añadimos el filtro solo para que se capture tráfico UDP y procedemos a iniciar la captura (Image8), al mismo tiempo ejecutamos en una consola shell el comando `sudo hping3 -S -p 80 www.uam.es`. dejamos capturando por unos segundos y lo detenemos (Imagen9).

Para comprobar que solo se ha capturado tráfico UDP, en la ventana donde se muestran todos los paquetes que se han capturado filtramos en búsqueda de paquetes UDP y el número de paquetes encontrados tiene que ser igual al número de paquetes que teníamos al principio, sin el filtro (Imagen10). En nuestro caso en principio tenemos capturados 15 paquetes y después de la búsqueda también tenemos los mismo 15 paquetes.

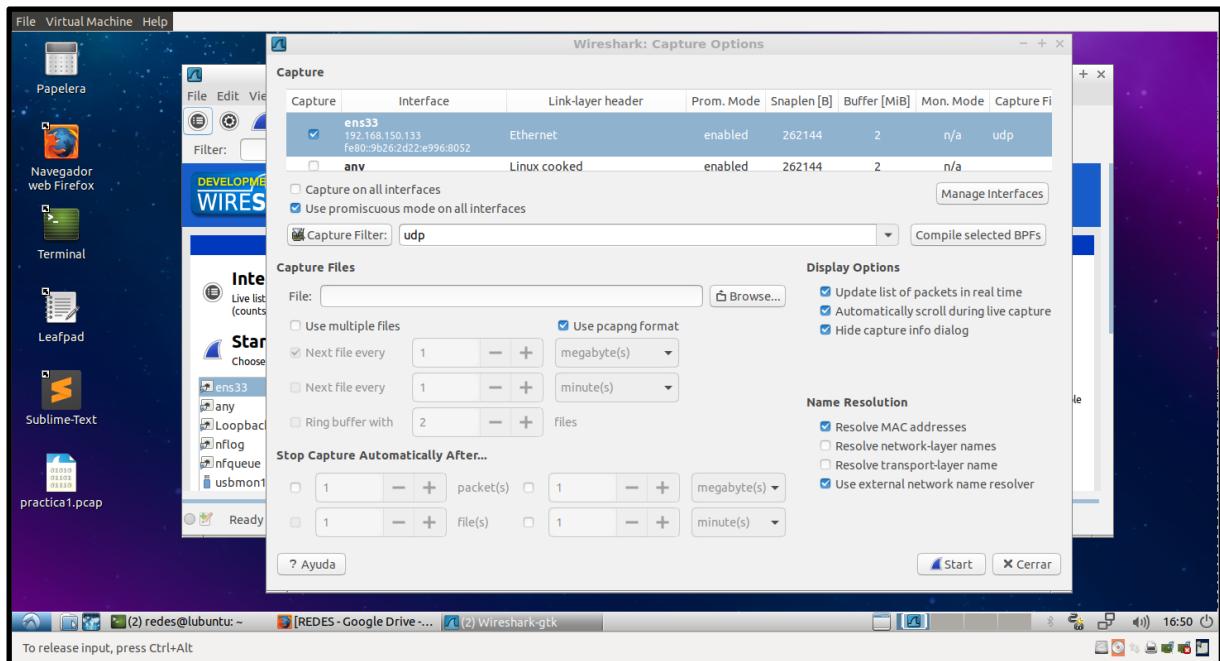


Imagen8

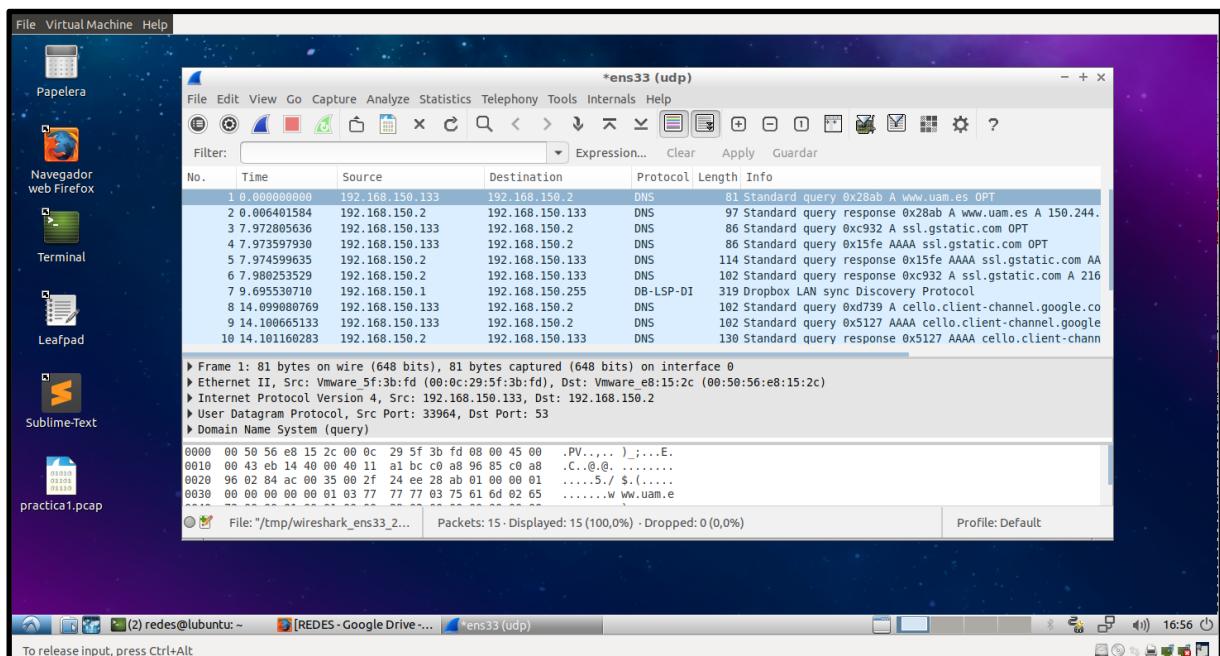


Imagen9

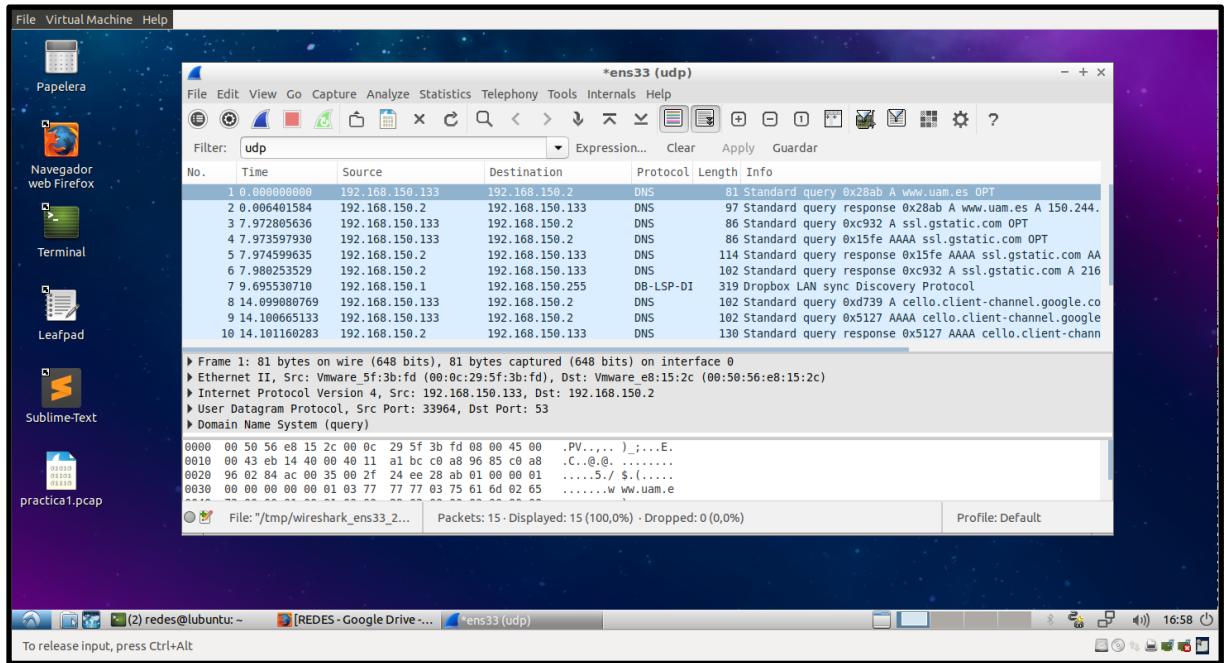


Imagen10