Ejercicios de captura de tráfico

Ejercicio 1:

Hemos abierto dos consolas, una para ejecutar Wireshark con permisos de superusuario y la segunda para realizar el ping más adelante.

Ejecutamos Wireshark con el comando:

$ sudo wireshark-gtk

Se inicia Wireshark y realizando click derecho en la sección de las columnas elegimos la opción “Column Preferences…”

Se nos despliega un menú en el que añadimos una nueva columna con nombre PO de tipo Src port (unresolved) y PD de tipo Dest port (unresolved).

Empezamos a capturar el tráfico desde Wireshark y realizamos el ping en la segunda consola con el comando:

$ sudo hping3 -S -p 80 www.uam.es

Detenemos la captura de tráfico y empezamos a analizarlo.

Guardamos la captura en formato “pcap”.

Cerramos Wireshark y volvemos a lanzarlo desde su correspondiente consola.

Abrimos la captura anteriormente guardada y comprobamos que efectivamente se guardó correctamente.

Ordenamos los paquetes según el campo PO anteriormente establecido y observamos que hay un único paquete con valor 53 en el campo PO.

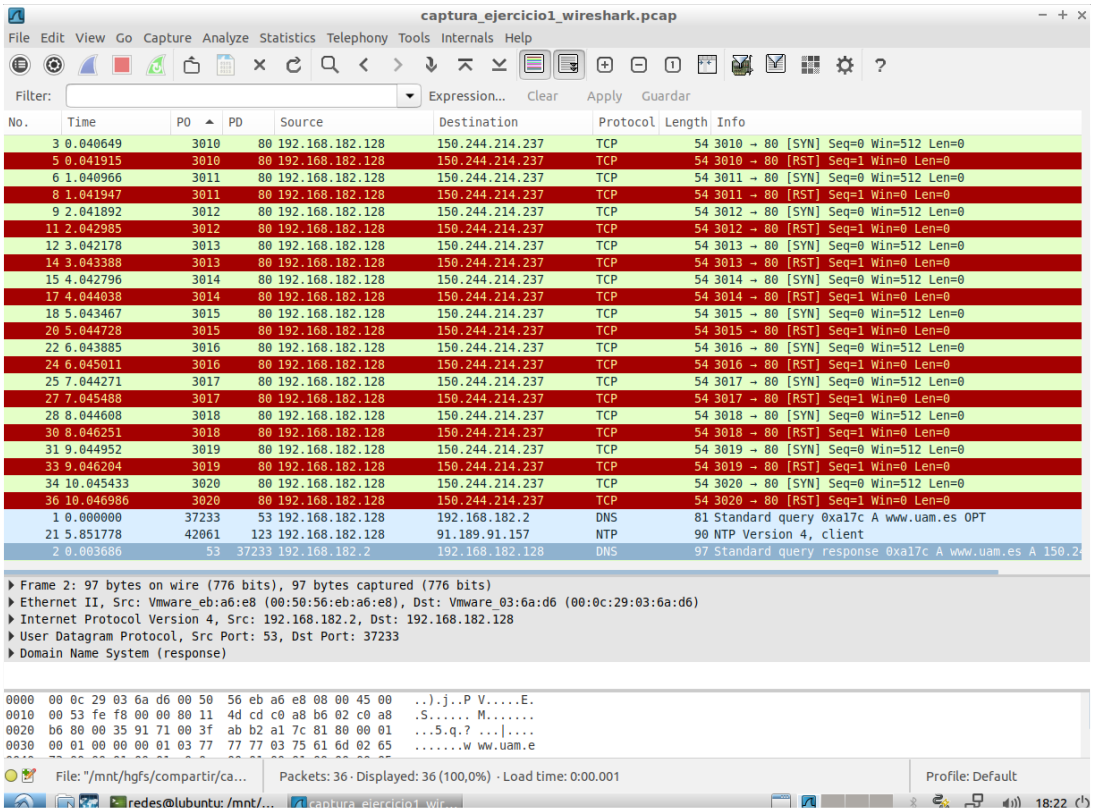

Ilustración 1: Captura de Paquetes en función del campo PO

Ejercicio 2:

Empezamos la captura con Wireshark y abrimos un navegador web para generar tráfico de paquetes.

Detenemos la captura y añadimos un filtro escribiendo la condición en la ventana “Filter”:

ip && frame.len > 1000

Este filtro solo capturará paquetes que son de tipo IP y que tengan un tamaño de paquete mayor a 1000 Bytes.

Para guardar únicamente la captura de los paquetes filtrados seleccionamos la opción

File > Export Specified Packets…

Y guardamos seleccionando la opción “Displayed”

Al comparar el tamaño de los primeros paquetes IP con el campo ‘length’ del protocolo IP podemos observar que todos ellos, algunos con distintos tamaños, difieren de 14 Bytes entre el tamaño IP y el campo ‘lenght’ del protocolo IP:

3432 - 3446, 3793 - 3807, 3541 -3555, 9777 - 9791, 9777 – 9791.

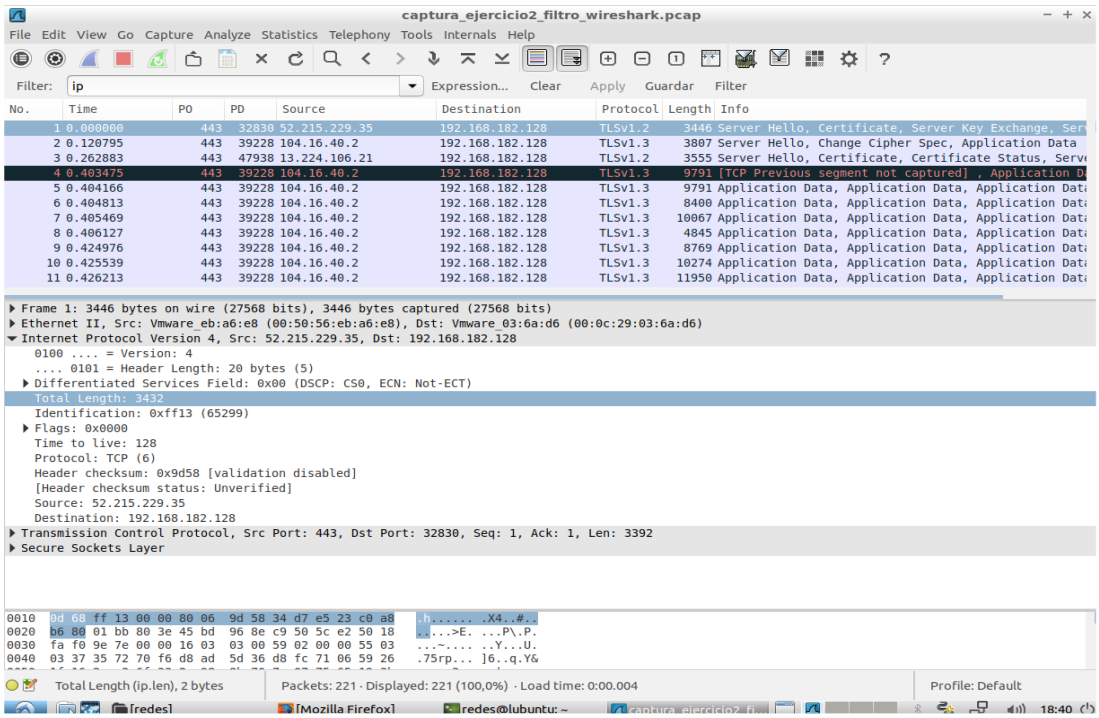

Ilustración 2: Primeros paquetes tipo IP

Creemos que esta diferencia de tamaño se debe a la encapsulación de los paquetes en función a las capas. 14 Bytes estarían reservados a la capa de Enlace, y por lo tanto no se mostrarían en el tamaño del paquete IP (capa de Red).

Ejercicio 3:

Hemos añadido una columna “interarrival” seleccionando el tipo “Delta time”. Para ello hemos hecho click derecho en las columnas y hemos seleccionado la opción “Column Preferences…”, donde se nos despliega el menú para poder añadir nuevas columnas.

Ejercicio 4:

Editamos la columna “Time” realizando click derecho en las columnas y seleccionando la opción “Column Preferences...”. Se nos despliega el menú de columnas y cambiamos el tipo de “Time” de “Time (format as specified)” a “Absolute time , as YYYY-MM-DD, and time”. Esta opción nos mostrará la fecha y la hora con minutos y segundos de la captura, y también nos mostrará un número que corresponde al tiempo Unix con resolución en segundos. Lo hemos cotejado con el tiempo Unix de nuestra práctica1.py y coinciden los valores.

Ejercicio 5:

Antes de iniciar la captura seleccionamos en las opciones de captura, en la ventana “Capture Filter” introducimos el siguiente comando: “udp”

Iniciamos la captura en Wireshark, y ésta solo captura paquetes de tipo UDP.

Empezamos a generar tráfico a través de un navegador web.

Desde una consola nueva, ejecutamos el siguiente comando:

$ sudo hping3 -S -p 80 www.uam.es

Volvemos a comprobar los paquetes y observamos que seguimos capturando solo paquetes de tipo UDP (entre ellos el paquete producido por el comando anterior).

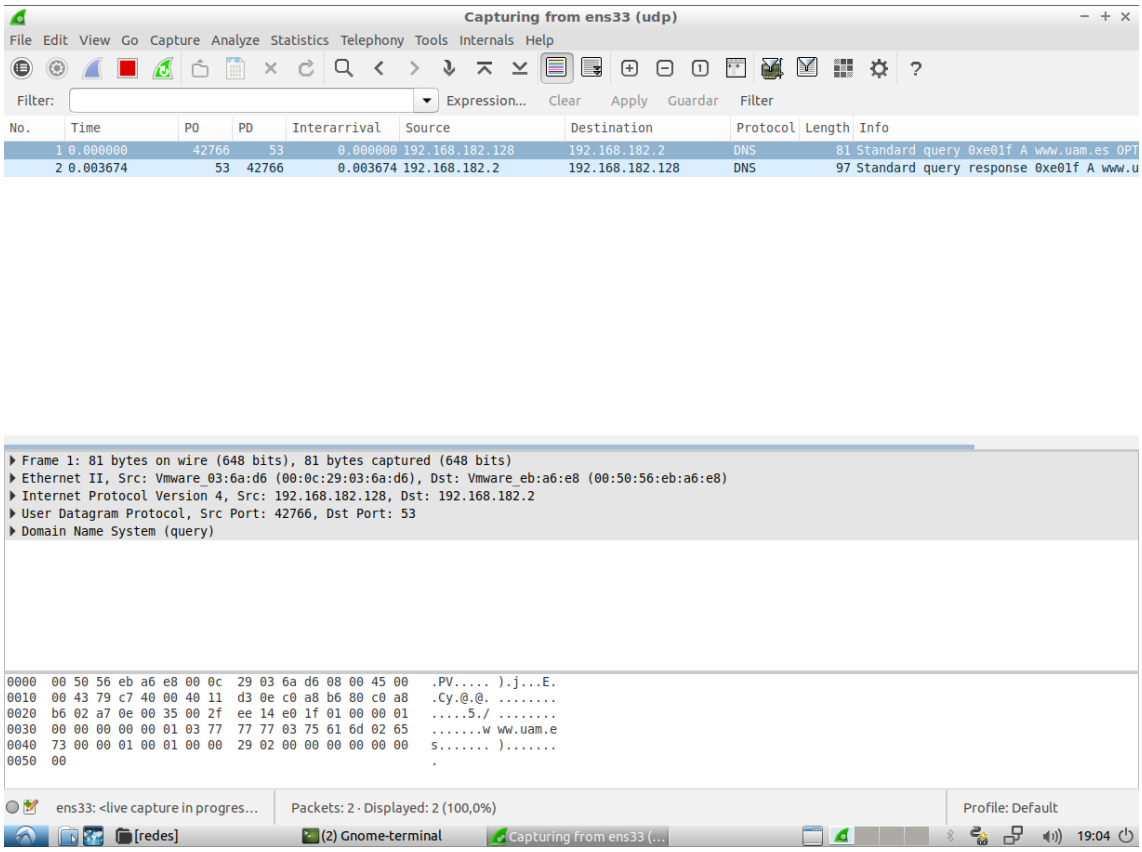

Ilustración 3: Captura de paquetes UDP