Redes 1 - Práctica 1

WIRESHARK

Alfonso Camblor - Ingeniería Informática - UAM

Contenido

Ejercicio 1

Abierta la consola o Shell, ejecuto el comando

“sudo wireshark-gtk”

Para abrir el programa Wireshark con funciones de captura de paquetes habilitadas.

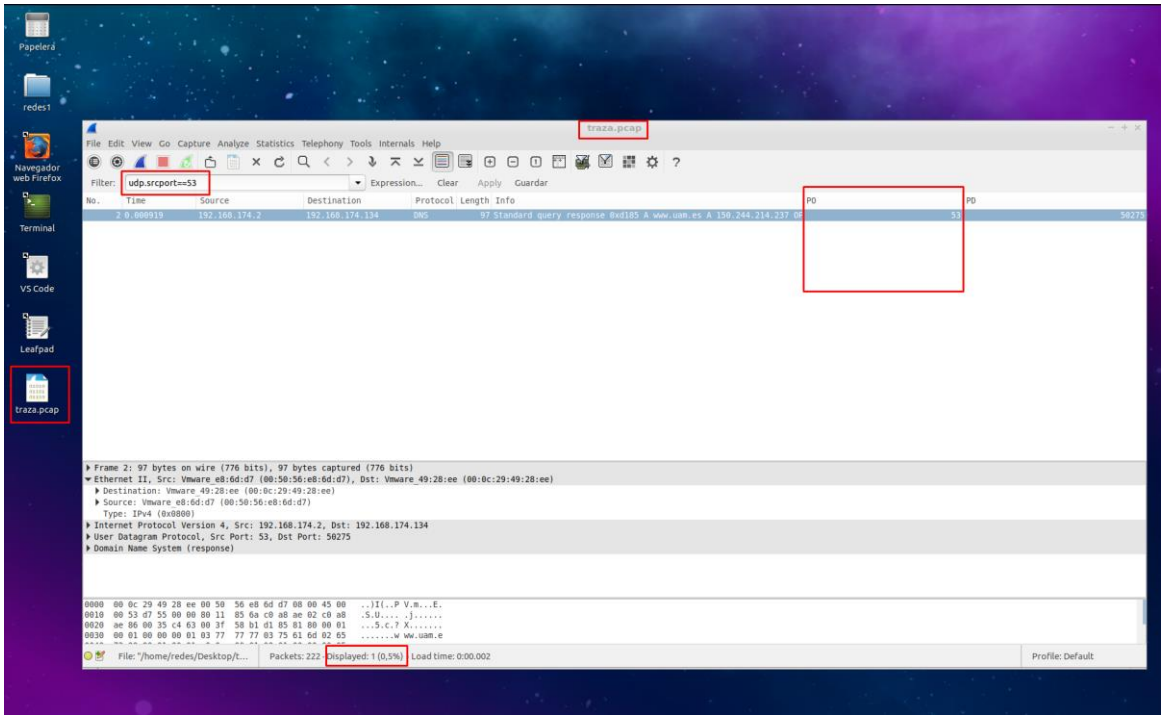
Hecho esto, comienzo la captura de la interfaz “ens33” y simultáneamente en otra terminal introduzco el comando

“sudo hping3 -S -p 80 www.uam.es”

El resultado de estas acciones es la captura de gran cantidad de paquetes por parte de Wireshark. El ejercicio nos pide guardar la traza en un formato que no sea “pcap-ng”, por lo que fue usado el formato “pcap”. Reiniciamos Wireshark y abrimos el fichero guardado.

Anteriormente habíamos creado las columnas PO y PD, asignándolas al valor de puerto de origen y el del puerto destino correspondientemente.

Una vez ordenamos en función de PO de forma descendente, encontramos:



Contabilizamos 1 paquete, pues es indicado en la parte inferior del programa (Displayed).

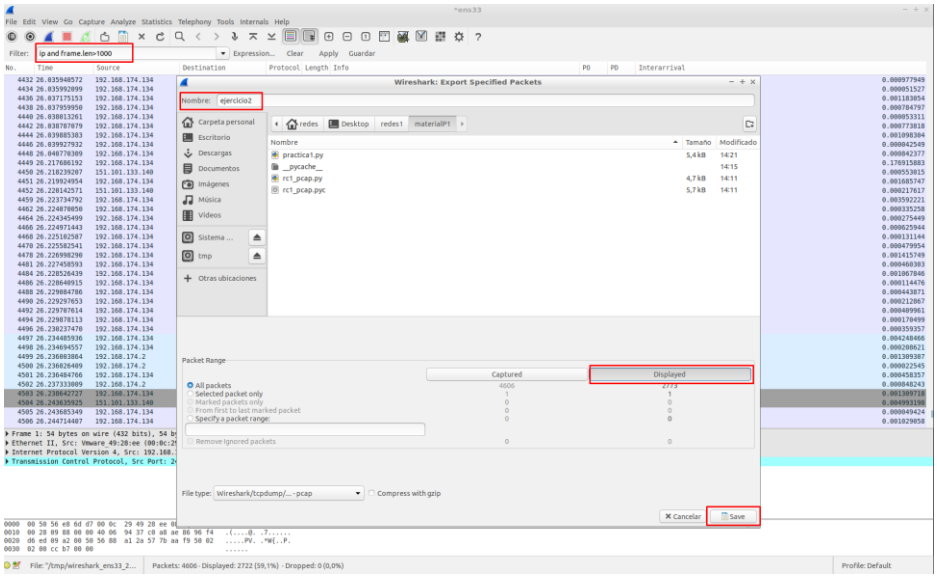
Ejercicio 2

Empezamos activando la captura de tráfico y abriendo “www.reddit.com” en el navegador.

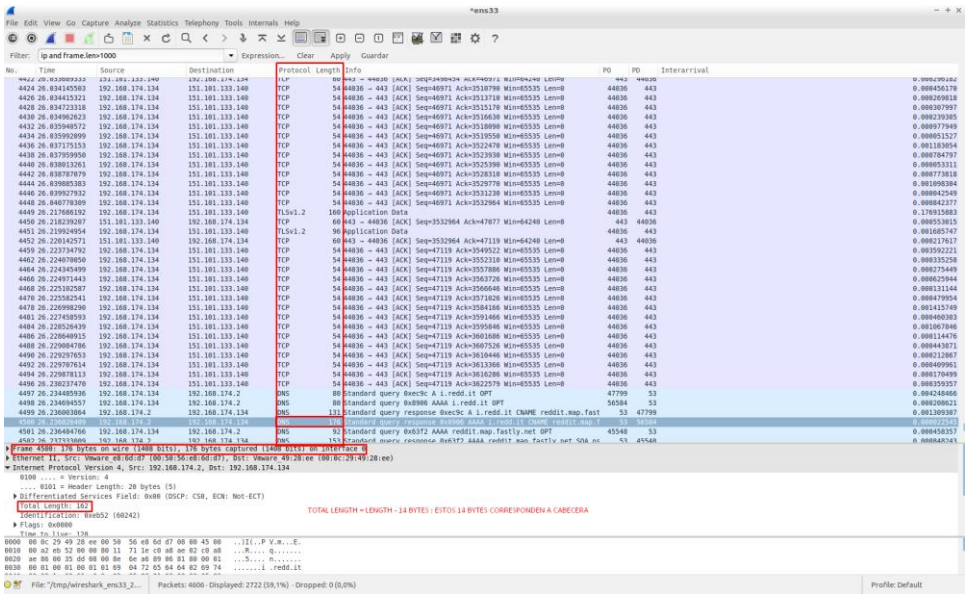
Capturamos paquetes durante unos 20 segundos.

Introducimos el filtro “ip and frame.len > 1000” para asegurarnos de filtrar los paquetes de tipo IP y cuyo tamaño sea MAYOR a 1000bytes.

Guardamos una traza con los paquetes filtrados:



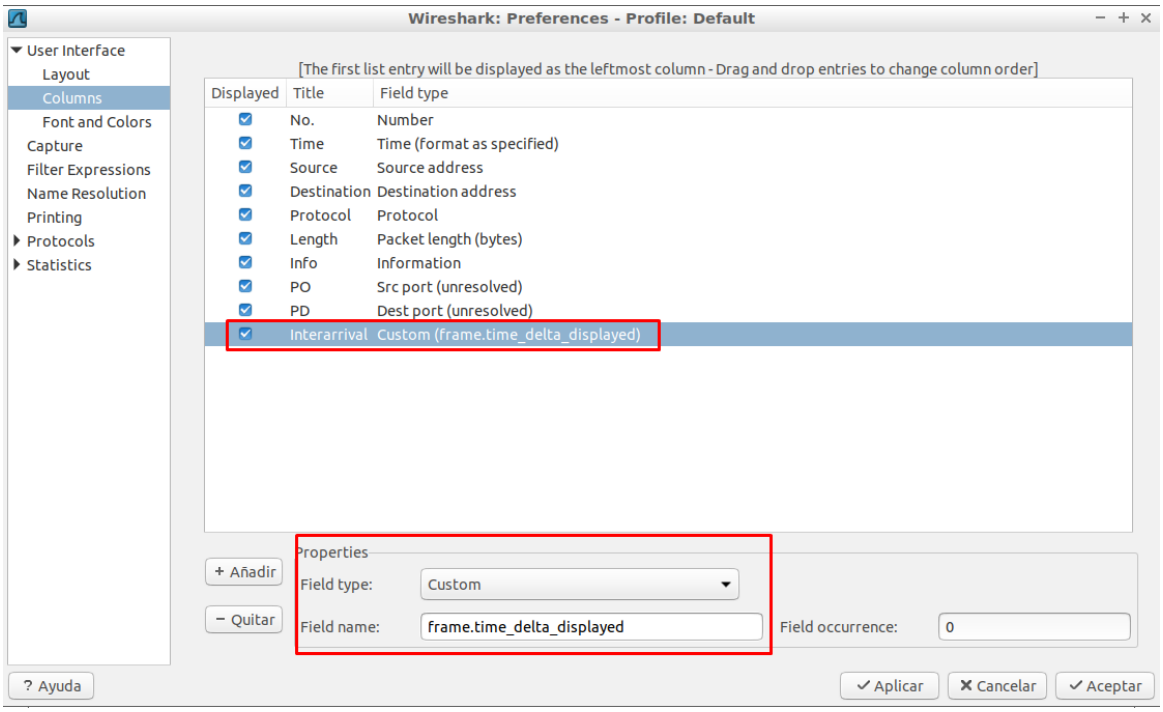
Determinamos que los 14 primeros bytes de cada paquete corresponden a la cabecera del paquete:



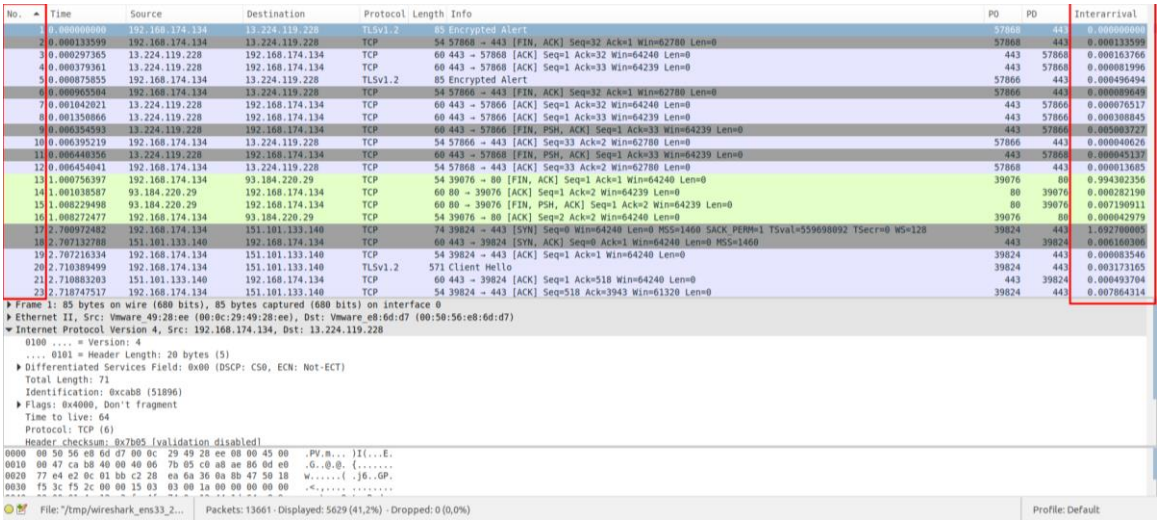
Ejercicio 3

Para añadir la columna, empezamos creando una nueva y declarándola de tipo custom, con el comando:

“frame.time_delta_displayed” en Field name.

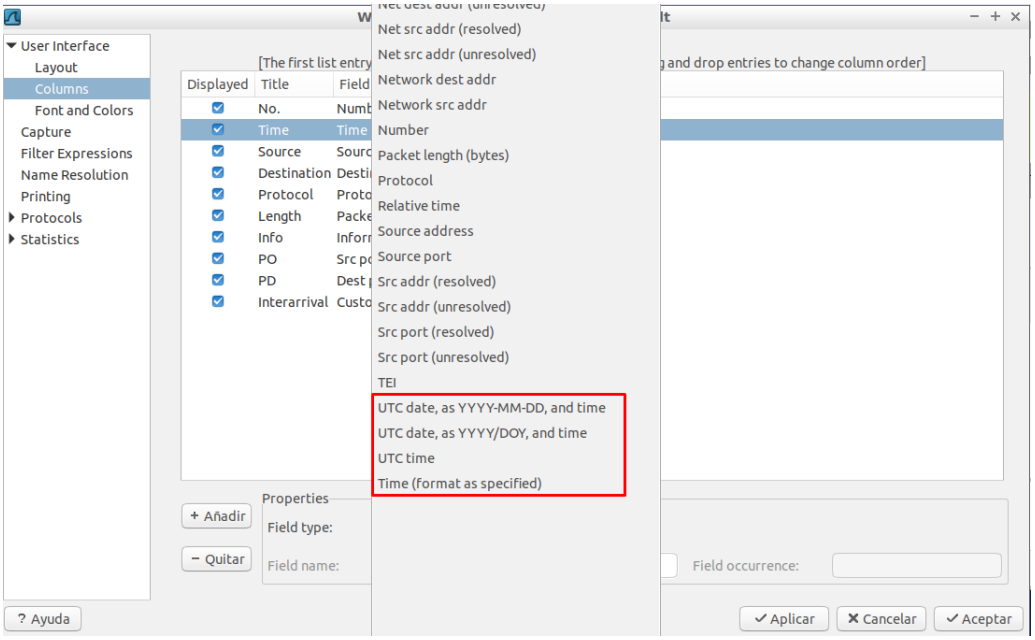


Apreciamos la nueva columna (Primer paquete tiene delta_time=0 dado que anteriormente no se captura ninguno):

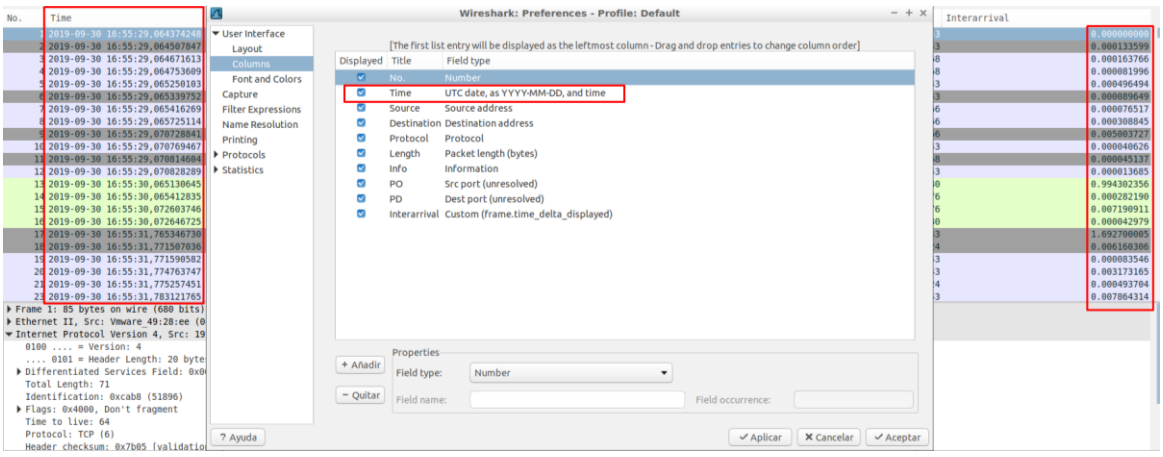


Ejercicio 4

Entramos en las opciones de columna y modificamos la columna Time. Tendremos las siguientes opciones:



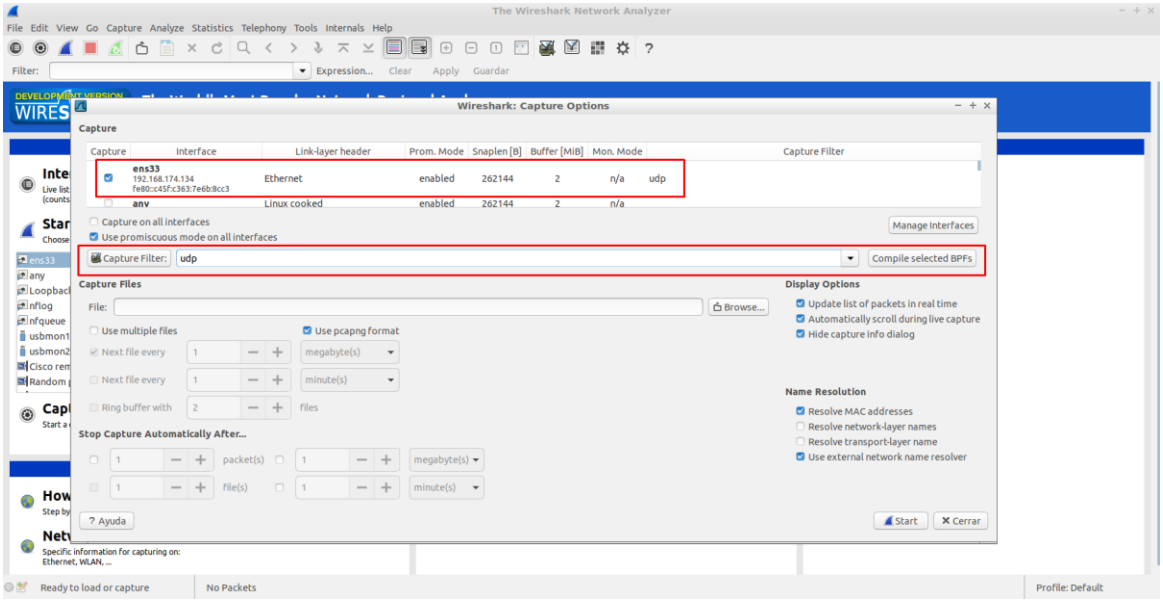
De estas, seleccionamos la mostrada (Se puede apreciar la corrección al corresponder el tiempo entre paquetes a la columna Interarrival que introdujimos en el ejercicio 3):



Ejercicio 5

Para realizar este ejercicio, comenzamos preparando Wireshark para capturar paquetes en la interfaz “ens33”, una terminal para ejecutar “sudo hping3 -S -p 80 www.uam.es”, y el navegador de internet listo para abrir “www.reddit.com”.

En Wireshark configuramos la captura de paquetes para que únicamente sean los paquetes UDP:



Procedemos entonces a iniciar el ping, abrir Reddit y capturar el tráfico generado por estas acciones, comprobando que una vez acaba la captura, al introducir un filtro que muestre únicamente paquetes UDP, se muestran todos los paquetes capturados sin excepción: