

UNIVERSIDAD AUTÓNOMA DE MADRID



Redes I
(2019-2020)

PRÁCTICA 1

Alba Ramos Pedroviejo
Javier Lozano Almeda

Grupo 1361

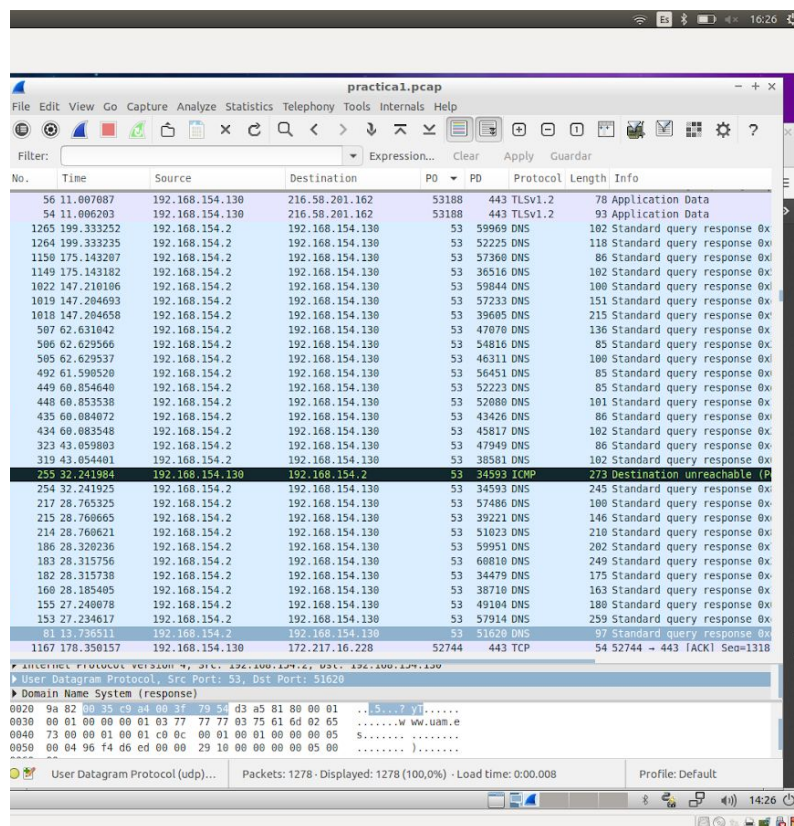
Madrid, 3 de octubre de 2019

Ejercicios de captura de tráfico

Ejercicio 1:

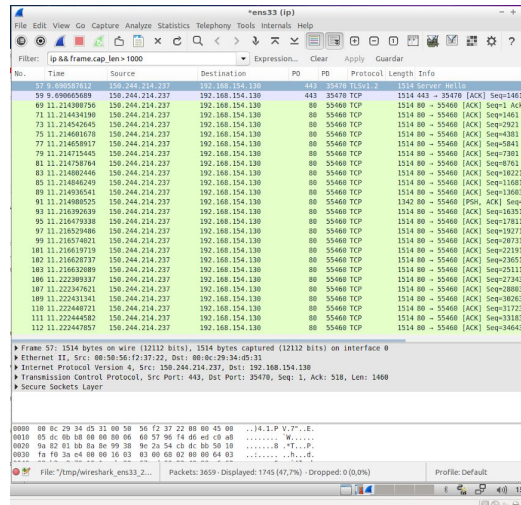
Para este ejercicio, hemos lanzado wireshark desde la terminal de ubuntu usando el comando sudo para que tenga derechos de administrador. Antes de iniciar la captura sobre la interfaz esn33, que es la correspondiente al ethernet en nuestra máquina virtual, hemos procedido a configurarla desactivando todas la opciones de "Name Resolution". A continuación hemos abierto una ventana del terminal y ejecutado el comando "sudo hping3 -S -p 80 www.uam.es", casi al instante hemos podido ver en wireshark que se empezaban a leer un montón de paquetes.

Una vez que se ha considerado que se habían leído suficientes paquetes, se ha procedido a detener la captura y guardar la traza en un archivo ".pcap". Para comprobar que la traza se había guardado correctamente, hemos abierto el archivo guardado y hemos comprobado que contenía lo mismos que teníamos en la captura en vivo. Para terminar con este ejercicio, hemos añadido a la visualización las columnas PO ('Src port (unresolved)') y PD ('Dst port (unresolved)'), este último no nos aparecía y se le ha asignado el tipo 'Dest port (unresolved)', y hemos ordenado las trazas por orden ascendente. Como se puede ver en la siguiente imagen, nos aparecen 29 paquetes en los que su PO es 53.

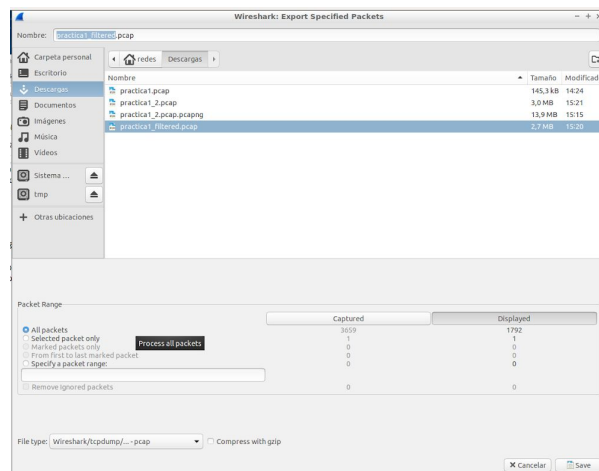


Ejercicio 2:

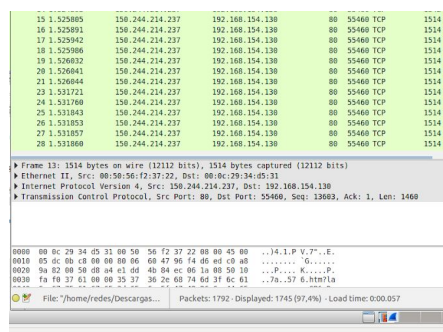
1. Se a usado el filtro “ip && frame.cap_len > 1000”.



2. Para guardar solo los paquetes que se visualizan tras aplicar el filtro, debemos:
 1. Ir a “file”.
 2. seleccionar “Export Specified Packets”.
 3. En la nueva ventana que nos aparecerá habrá que seleccionar la opción “Displayed”, indicar el tipo de fichero como “.pcap” y hacer click en “save”.

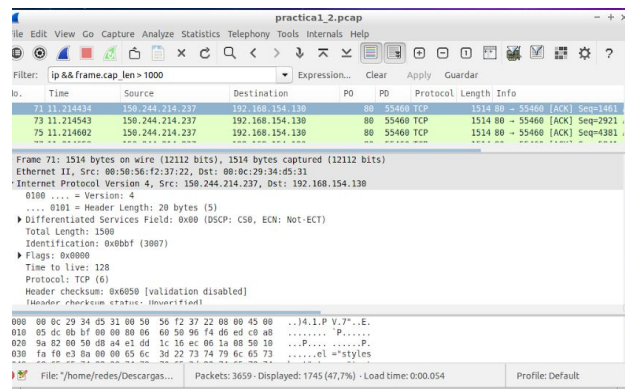


Una vez guardado el fichero, lo hemos abierto nuevamente. Tras ello hemos podido observar que el número de paquetes totales coincide con el número de paquetes visualizados en la traza filtrada.



Por alguna razón, que hemos sido incapaces de solucionar, cuando se guarda la traza con los paquetes visualizados esta te dice que se van a guardar 1792, cuando en la visualización se mostraban 1745.

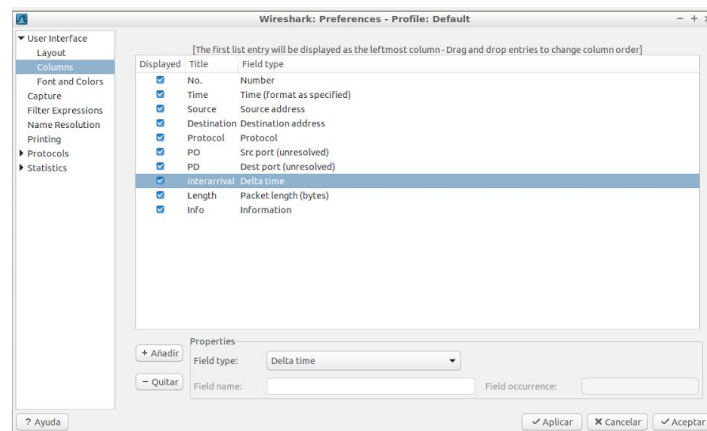
- Tras comparar el tamaño de los 5 primeros paquetes con el tamaño del campo 'length' del protocolo ip, hemos podido comprobar que todos ellos tenían un tamaño de paquete que era 14 Bytes mayor que el tamaño del protocolo IP.



Ejercicio 3:

En este ejercicio se nos pedía añadir una columna que mostrase el tiempo entre paquetes consecutivos, para ello hemos realizado los siguientes pasos:

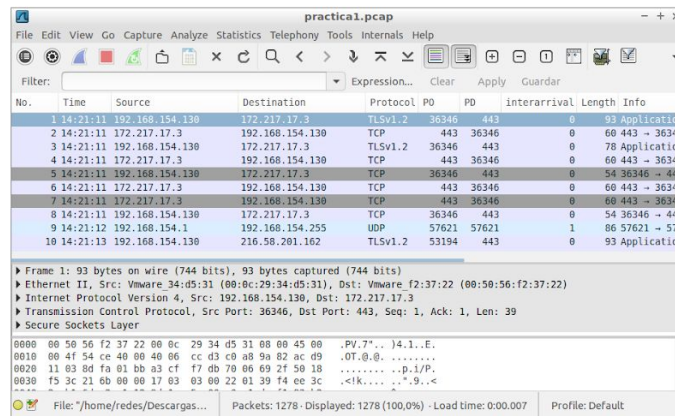
- Ir a "edit".
- Seleccionar "Preferences".
- En la nueva ventana que nos aparecerá habrá que seleccionar "columns" en el menú situado a la izquierda.
- Hacer click en añadir y cambiar el nombre por *interarrival*.
- Seleccionar la nueva columna creada y en "Field Type" seleccionar "Delta Time".
- Hacer click en aplicar y después en aceptar. Algunas veces no se muestra la columna cread, por lo que habrá que volver a realizar los pasos del 1 al 5 para volver a la ventana correspondiente y marcar la columna *interarrival* como visible.



Ejercicio 4:

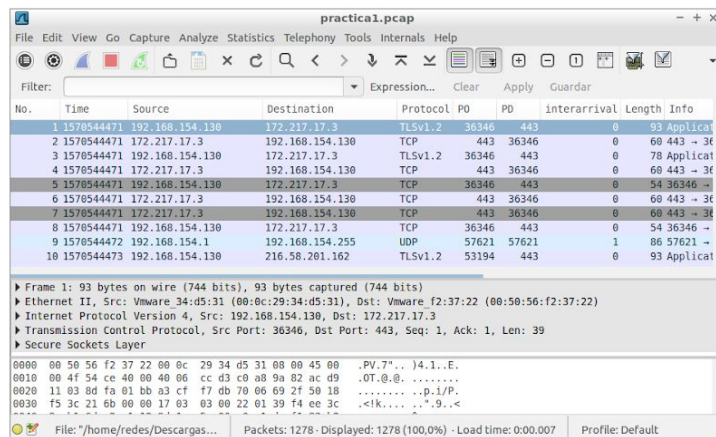
Para cambiar el formato en el que se visualiza la columna time a un formato para humanos, hemos realizado los siguientes pasos:

1. Ir a “View”.
2. Posicionar el ratón sobre “Time Display Format”.
3. En el desplegable que aparece seleccionar “Time of Day”.



Para cambiar el formato en el que se visualiza la columna time a un formato para humanos, hemos realizado los siguientes pasos:

1. Ir a “View”.
2. Posicionar el ratón sobre “Time Display Format”.
3. En el desplegable que aparece seleccionar “Seconds Since Epoch”.



Ejercicio 5:

Para cambiar el formato en el que se visualiza la columna time a un formato para humanos, hemos realizado los siguientes pasos:

1. Hacer click en el botón de ajustes de captura.
2. Hacer click en el botón “capture filter”.
3. En la nueva ventana, seleccionar “UDP Only” y hacer click en aceptar.
4. Hacer click en el botón “Start”.

The image displays three screenshots illustrating the steps to configure Wireshark for capturing UDP traffic in a human-readable time format.

Top Left: Wireshark: Capture Filter - Profile: Default
This window shows the 'Capture Filter' configuration. The 'Filter name' is 'UDP only' and the 'Filter string' is 'udp'. The 'Properties' section shows 'Filter name: UDP only' and 'Filter string: udp'. The 'Aceptar' (Accept) button is highlighted.

Top Right: Wireshark: Capture Options
This window shows the 'Capture Options' configuration. The 'Capture' section shows 'Interface: ens33' and 'Link-layer header: Ethernet'. The 'Capture Files' section shows 'Use pcapng format' and 'Next file every: 1 megabyte(s)'. The 'Display Options' section shows 'Update list of packets in real time' and 'Hide capture info dialog'. The 'Start' button is highlighted.

Bottom: Wireshark Main Window
This window shows the main Wireshark interface. The 'Filter' bar is empty. The 'Packets' list shows a table of captured packets. The 'Packet Details' pane shows the details of the selected packet (Frame 20: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0). The 'Packet Bytes' pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	P.O.	P.D.	Interarrival	Length	Info
14	20:33:40	192.168.154.2	192.168.154.130	DNS	53	41943	0	130	Standard c
15	20:33:43	192.168.154.130	192.168.154.2	DNS	49658	53	3	87	Standard c
16	20:33:43	192.168.154.130	192.168.154.2	DNS	50881	53	0	87	Standard c
17	20:33:43	192.168.154.2	192.168.154.130	DNS	53	49658	0	103	Standard c
18	20:33:43	192.168.154.2	192.168.154.130	DNS	53	50881	0	115	Standard c
19	20:33:55	192.168.154.130	192.168.154.2	DNS	55744	53	12	86	Standard c
20	20:33:55	192.168.154.2	192.168.154.130	DNS	53	55744	0	182	Standard c
21	20:33:55	192.168.154.2	192.168.154.130	DNS	53	51796	0	114	Standard c
22	20:33:55	192.168.154.2	192.168.154.130	DNS	53	51796	0	114	Standard c
23	20:33:57	192.168.154.1	192.168.154.255	UDP	57621	57621	1	86	57621 - 57