INFORME PRÁCTICA 1

Alejandro Santorum Varela - alejandro.santorum@estudiante.uam.es
David Cabornero Pascual - david.cabornero@estudiante.uam.es
Redes de Comunicaciones I - Práctica 1 - Pareja 4
Universidad Autónoma de Madrid

17-10-2018

Contents

1 Introducción

Este documento consiste en el informe de la práctica 1 de Redes de Comunicaciones I. Se recoge el diseño, estructura y salidas del código pedido para esta práctica, que consiste en introducirnos en el uso de la librería *Libpcap*.

2 Estructura del programa

El programa se puede ejecutar con uno o dos argumentos de entrada, el primero es siempre el número de bytes de cada paquete que se quieren mostrar por pantalla; el segundo es opcional, y sería en el caso que se quisiese analizar una traza de tráfico ya captura con anterioridad, por lo que sería el nombre del archivo .pcap ya guardado.

Lo primero que hace nuestro código es **comprobar que el primer parámetro de entrada es verdaderamente un entero**, pues si no lo fuese (por cualquier fallo del usuario) el programa fallaría.

A continuación, si solo se ha introducido un parámetro, el programa considera que se quiere capturar tráfico en vivo en el momento de ejecución. Primero se **comprueba que el número de bytes que se quieren mostrar es menor que el tamaño máximo del paquete** (en esta práctica este máximo es de 1514). En caso de que fuese mayor, sería **limitado al tamaño máximo de paquete** (1514) y se mostraría un **mensaje de advertencia** al final de la ejecución del programa. Después se abre la interfaz de captura con *pcap_open_live(...)* y se abre el dumper donde se guardará la traza con *pcap_open_dead(...)* y *pcap_dump_open(...)*. Por el contrario, si se hubiesen introducido dos parámetros de entrada, se consideraría que se quiere analizar una traza ya guardada. Simplemente se utilizaría la función *pcap_open_offline(...)* para abrir el archivo .pcap ya guardado.

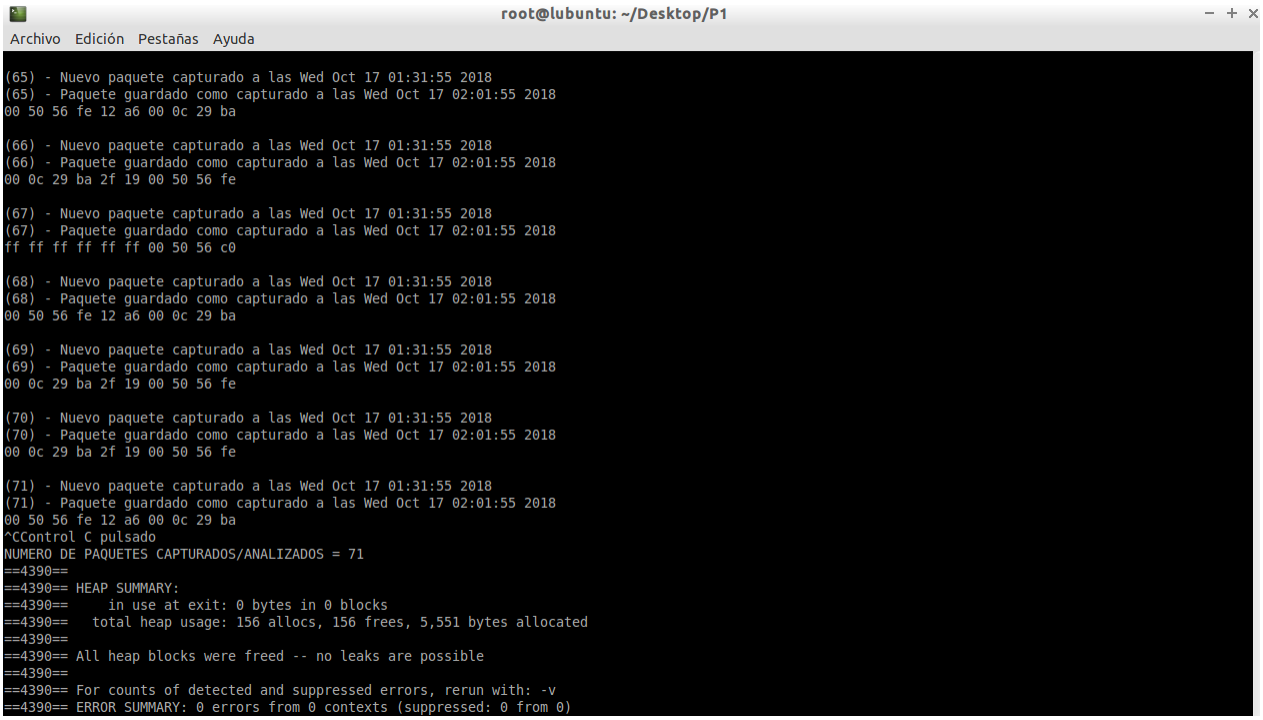
A partir de aquí el programa funciona independientemente del número de parámetros de entrada, usando la función *pcap_loop(...)* y la función de atención al paquete para analizar cada paquete.

Comentar que si el número de bytes del paquete es menor que el número de bytes que se quieren mostrar, el **número de bytes mostrados es limitado**, como cabía esperar, **al número de bytes del paquete**.

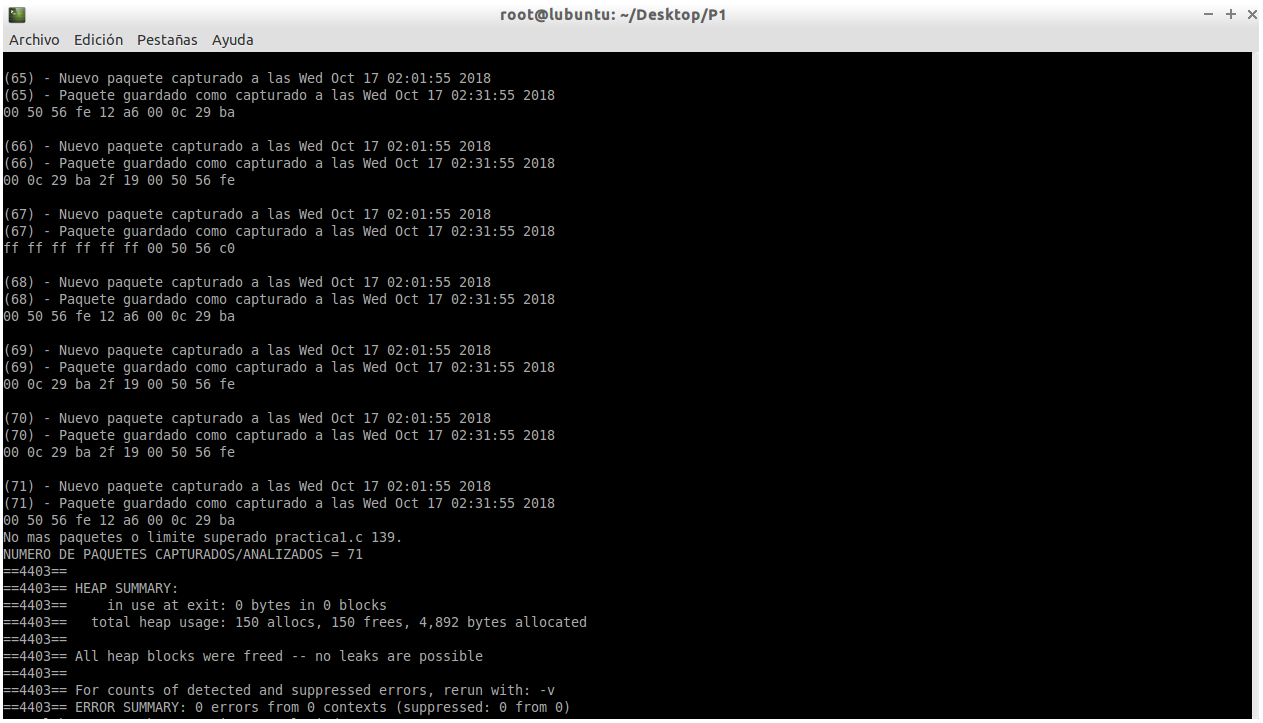
El programa termina con ctrl+c (mediante *pcap_breakloop(...)*), cuando se han analizado todos los paquetes o cuando se ha superado el límite de paquetes analizables. Se elimina toda la memoria reservada y se cierran los descriptores y dumpers para la correcta finalización del programa.

3 Muestras de salidas

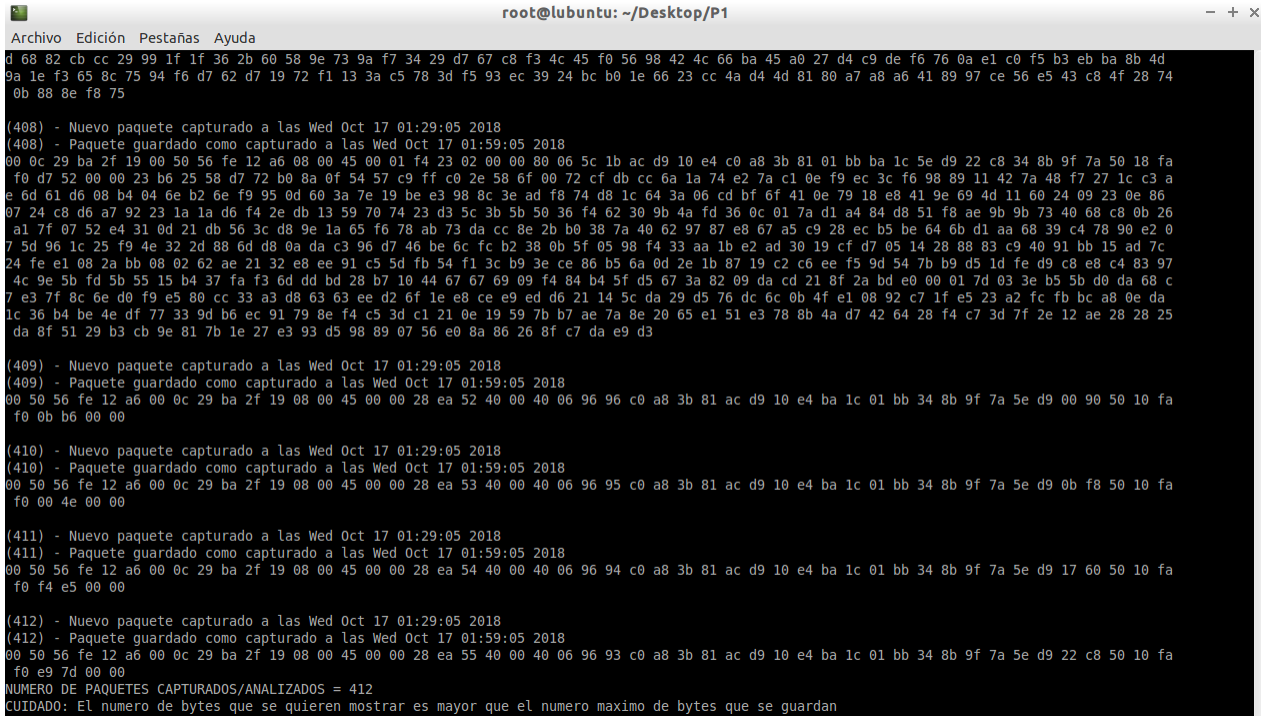
A continaución se muestran unas salidas del programa de ejemplo.
-Ejecución del programa con un argumento de entrada y examinado por Valgrind:



-Ejecución del programa con dos argumentos de entrada y examinado por Valgrind:



-Ejecución del programa con un argumento de entrada superior al tamaño máximo de paquete:



4 Leeme.txt

Esta sección va también incluida en el fichero *leeme.txt* pero se reincluye aquí para mayor claridad:

· **Normativa de entrega cumplida en su totalidad** Realizado: el enunciado ha sido leído varias veces.
· **Contar paquetes de una traza** Realizado: Se ha comprobado su correctitud con Wireshark.
· **Contar paquetes de la interfaz de red** Realizado: Coinciden con el ID auxiliar que le hemos añadido con el último paquete analizado.
· **Almacenar en una traza el tráfico capturado en vivo** Realizado: Se ha comprobado su correctitud con la ayuda de Wireshark, repitiendo el proceso con varios paquetes.
· **Modificar fecha correctamente** Realizado: Comprobado viendo la ejecución del propio programa.
· **Imprimir los N primeros bytes** Realizado: Además se comprueba el tamaño de N con snaplen y con el tamaño real del paquete.
· **Ejercicios de captura de tráfico** Realizado: comprobar documento "practica1.pdf".

5 Conclusión

En esta práctica se nos ha introducido al uso y manejo de Wireshark y de la librería Libpcap. Esperamos haber hecho un buen trabajo, ya que las próximas prácticas dependen de esta, que cimienta las bases de las prácticas de la asignatura.