

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	2
2	Estructura del programa	2
3	Muestras de salidas	3
4	Leeme.txt	4
5	Conclusión	5

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 continuación se muestran unas salidas del programa de ejemplo.

-Ejecución del programa con un argumento de entrada y examinado por Valgrind:

```
root@lubuntu: ~/Desktop/P1
Archivo Edición Pestañas Ayuda

(65) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(65) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
00 50 56 fe 12 a6 00 0c 29 ba

(66) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(66) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
00 0c 29 ba 2f 19 00 50 56 fe

(67) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(67) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
ff ff ff ff ff ff 00 50 56 c0

(68) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(68) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
00 50 56 fe 12 a6 00 0c 29 ba

(69) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(69) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
00 0c 29 ba 2f 19 00 50 56 fe

(70) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(70) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
00 0c 29 ba 2f 19 00 50 56 fe

(71) - Nuevo paquete capturado a las Wed Oct 17 01:31:55 2018
(71) - Paquete guardado como capturado a las Wed Oct 17 02:01:55 2018
00 50 56 fe 12 a6 00 0c 29 ba
^CControl C pulsado
NUMERO DE PAQUETES CAPTURADOS/ANALIZADOS = 71
==4390==
==4390== HEAP SUMMARY:
==4390==      in use at exit: 0 bytes in 0 blocks
==4390==    total heap usage: 156 allocs, 156 frees, 5,551 bytes allocated
==4390==
==4390== All heap blocks were freed -- no leaks are possible
==4390==
==4390== For counts of detected and suppressed errors, rerun with: -v
==4390== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

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

```
root@lubuntu: ~/Desktop/P1
Archivo Edición Pestañas Ayuda

(65) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(65) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
00 50 56 fe 12 a6 00 0c 29 ba

(66) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(66) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
00 0c 29 ba 2f 19 00 50 56 fe

(67) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(67) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
ff ff ff ff ff ff 00 50 56 c0

(68) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(68) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
00 50 56 fe 12 a6 00 0c 29 ba

(69) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(69) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
00 0c 29 ba 2f 19 00 50 56 fe

(70) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(70) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
00 0c 29 ba 2f 19 00 50 56 fe

(71) - Nuevo paquete capturado a las Wed Oct 17 02:01:55 2018
(71) - Paquete guardado como capturado a las Wed Oct 17 02:31:55 2018
00 50 56 fe 12 a6 00 0c 29 ba
No mas paquetes o limite superado practica1.c 139.
NUMERO DE PAQUETES CAPTURADOS/ANALIZADOS = 71
==4403==
==4403== HEAP SUMMARY:
==4403==      in use at exit: 0 bytes in 0 blocks
==4403==    total heap usage: 150 allocs, 150 frees, 4,892 bytes allocated
==4403==
==4403== All heap blocks were freed -- no leaks are possible
==4403==
==4403== For counts of detected and suppressed errors, rerun with: -v
==4403== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

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

```
root@lubuntu: ~/Desktop/P1
Archivo Edición Pestañas Ayuda
d 68 82 cb cc 29 99 1f 1f 36 2b 60 58 9e 73 9a f7 34 29 d7 67 c8 f3 4c 45 f0 56 98 42 4c 66 ba 45 a0 27 d4 c9 de f6 76 0a e1 c0 f5 b3 eb ba 8b 4d
9a 1e f3 65 8c 75 94 f6 d7 62 d7 19 72 f1 13 3a c5 78 3d f5 93 ec 39 24 bc b0 1e 66 23 cc 4a d4 4d 81 80 a7 a8 a6 41 89 97 ce 56 e5 43 c8 4f 28 74
0b 88 8e f8 75

(408) - Nuevo paquete capturado a las Wed Oct 17 01:29:05 2018
(408) - Paquete guardado como capturado a las Wed Oct 17 01:59:05 2018
00 0c 29 ba 2f 19 00 50 56 fe 12 a6 00 00 45 00 01 f4 23 02 00 00 00 06 5c 1b ac d9 10 e4 c0 a8 3b 81 01 bb ba 1c 5e d9 22 c8 34 8b 9f 7a 50 18 fa
f0 d7 52 00 00 23 b6 25 58 d7 72 b0 8a 0f 54 57 c9 ff c0 2e 58 6f 00 72 cf db cc 6a 1a 74 e2 7a c1 0e f9 ec 3c f6 98 89 11 42 7a 48 f7 27 1c c3 a
e 6d 61 d6 08 b4 04 6e b2 6e f9 95 0d 00 3a 7e 19 be e3 98 8c 3e ad f8 74 d8 1c 64 3a 06 cd bf 6f 41 0e 79 18 e8 41 9e 69 4d 11 60 24 09 23 0e 86
07 24 c8 d6 a7 92 23 1a 1a d6 f4 2e db 13 59 70 74 23 d3 5c 3b 5b 50 36 f4 62 30 9b 4a fd 36 0c 01 7a d1 a4 84 d8 51 f8 ae 9b 9b 73 40 68 c8 0b 26
a1 7f 07 52 e4 31 0d 21 db 56 3c d8 9e 1a 65 f6 78 ab 73 da cc 8e 2b b0 38 7a 40 62 97 87 e8 67 a5 c9 28 ec b5 be 64 6b d1 aa 68 39 c4 78 90 e2 0
7 5d 96 1c 25 f9 4e 32 2d 88 6d d8 0a da c3 96 d7 46 be 6c fc b2 38 0b 5f 05 98 f4 33 aa 1b e2 ad 30 19 cf d7 05 14 28 88 83 c9 40 91 bb 15 ad 7c
24 fe e1 08 2a bb 08 02 62 ae 21 32 e8 ee 91 c5 5d fb 54 f1 3c b9 3e ce 86 b5 6a 0d 2e 1b 87 19 c2 c6 ee f5 9d 54 7b b9 d5 1d fe d9 c8 e8 c4 83 97
4c 9e 5b fd 5b 55 15 b4 37 fa f3 6d dd bd 28 b7 10 44 67 67 69 09 f4 84 b4 5f d5 67 3a 82 09 da cd 21 8f 2a bd e0 00 01 7d 03 3e b5 5b d0 da 68 c
7 e3 7f 8c 6e d0 f9 e5 80 cc 33 a3 d8 63 63 ee d2 6f 1e e8 ce e9 ed d6 21 14 5c da 29 d5 76 dc 6c 0b 4f e1 08 92 c7 1f e5 23 a2 fc fb bc a8 0e da
1c 36 b4 be 4e df 77 33 9d b6 ec 91 79 8e f4 c5 3d c1 21 0e 19 59 7b b7 ae 7a 8e 20 65 e1 51 e3 78 8b 4a d7 42 64 28 f4 c7 3d 7f 2e 12 ae 28 28 25
da 8f 51 29 b3 cb 9e 81 7b 1e 27 e3 93 d5 98 89 07 56 e0 8a 86 26 8f c7 da e9 d3

(409) - Nuevo paquete capturado a las Wed Oct 17 01:29:05 2018
(409) - Paquete guardado como capturado a las Wed Oct 17 01:59:05 2018
00 50 56 fe 12 a6 00 0c 29 ba 2f 19 08 00 45 00 00 28 ea 52 40 00 00 06 96 96 c0 a8 3b 81 ac d9 10 e4 ba 1c 01 bb 34 8b 9f 7a 5e d9 00 90 50 10 fa
f0 0b b6 00 00

(410) - Nuevo paquete capturado a las Wed Oct 17 01:29:05 2018
(410) - Paquete guardado como capturado a las Wed Oct 17 01:59:05 2018
00 50 56 fe 12 a6 00 0c 29 ba 2f 19 08 00 45 00 00 28 ea 53 40 00 00 06 96 95 c0 a8 3b 81 ac d9 10 e4 ba 1c 01 bb 34 8b 9f 7a 5e d9 0b f8 50 10 fa
f0 00 4e 00 00

(411) - Nuevo paquete capturado a las Wed Oct 17 01:29:05 2018
(411) - Paquete guardado como capturado a las Wed Oct 17 01:59:05 2018
00 50 56 fe 12 a6 00 0c 29 ba 2f 19 08 00 45 00 00 28 ea 54 40 00 00 06 96 94 c0 a8 3b 81 ac d9 10 e4 ba 1c 01 bb 34 8b 9f 7a 5e d9 17 60 50 10 fa
f0 f4 e5 00 00

(412) - Nuevo paquete capturado a las Wed Oct 17 01:29:05 2018
(412) - Paquete guardado como capturado a las Wed Oct 17 01:59:05 2018
00 50 56 fe 12 a6 00 0c 29 ba 2f 19 08 00 45 00 00 28 ea 55 40 00 00 06 96 93 c0 a8 3b 81 ac d9 10 e4 ba 1c 01 bb 34 8b 9f 7a 5e d9 22 c8 50 10 fa
f0 e9 7d 00 00
NUMERO DE PAQUETES CAPTURADOS/ANALIZADOS = 412
CUIDADO: El numero de bytes que se quieren mostrar es mayor que el numero maximo de bytes que se guardan
```

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 "practical.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.