



PRÁCTICA 1

Analizador de protocolo LLC



Redes de Computadoras • Escuela Superior de Cómputo • Instituto Politécnico Nacional

- En esta práctica se realizará una función que analice tramas del protocolo LLC y se alimentara con las tramas capturadas por un programa que emplea la librería winpcap.

Introducción

El protocolo LLC (control lógico de enlace) es un protocolo de capa de enlace de datos derivado de HDLC, del cual hereda su campo de control, y fue estandarizado por la IEEE bajo la denominación 802.2. Igual que en HDLC se tienen tramas de información, supervisión y no numeradas distinguiéndose entre ellas por los bits menos significativos de su campo de control.

Investigue el formato de las tramas LLC (802.2) encapsuladas dentro del protocolo 802.3 y analice las siguientes tramas llenando la tabla que se encuentra al final de las mismas. En la tabla se incluye el análisis de la primera trama para servir de ejemplo.

```
1
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 03 f0 f0
7f 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 43 05 90 6d
2
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 03 f0 f1
73 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 54 90 6d
3
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 04 f0 f0
01 01 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 41 a3 90 6d
4
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 01 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 f2 90 6d
5
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 12 f0 f0
00 01 0e 00 ff ef 19 8f bc 05 7f 00 23 00 7f 23
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 41 91 6d
6
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 12 f0 f0
00 03 0e 00 ff ef 17 81 bc 05 23 00 7f 00 23 7f
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 90 91 6d
7
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 03 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 df 91 6d
8
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 04 f0 f1
01 03 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
00 00 00 00 00 00 00 00 00 00 00 00 18 ac 92 6d
9
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 ac f0 f0
02 02 0e 00 ff ef 16 04 00 00 00 00 28 00 7f 23
ff 53 4d 42 72 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 77 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4d 49 43 52
4f 53 4f 46 54 20 4e 45 54 57 4f 52 4b 53 20 33
2e 30 00 02 44 4f 53 20 4c 4d 31 2e 32 58 30 30
32 00 02 44 4f 53 20 4c 41 4e 4d 41 4e 32 2e 31
00 02 57 69 6e 64 6f 77 73 20 66 6f 72 20 57 6f
72 6b 67 72 6f 75 70 73 20 33 2e 31 61 00 02 4e
54 20 4c 4d 20 30 2e 31 32 00 00 fb 92 6d 86 df
10
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 04 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 7b 93 6d
11
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 5f f0 f0
02 04 0e 00 ff ef 16 0c 00 00 28 00 28 00 23 7f
ff 53 4d 42 72 00 00 00 00 80 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
11 05 00 02 02 00 01 00 68 0b 00 00 00 00 01 00
7f 07 00 80 03 02 00 00 e5 fe 29 25 7c c2 01
2c 01 08 08 00 7f 07 00 80 32 3e b9 3d 00 ca 93
12
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 04 f0 f1
01 04 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 7c 94 6d
13
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 91 f0 f0
04 04 0e 00 ff ef 16 0c 00 00 28 00 28 00 7f 23
ff 53 4d 42 73 00 00 00 00 10 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
0d 75 00 5d 00 68 0b 02 00 00 00 7f 07 00 80 00
00 00 00 00 00 00 01 00 00 00 20 00 00 00 45
53 43 4f 4d 00 57 69 6e 64 6f 77 73 20 34 2e 30
00 57 69 6e 64 6f 77 73 20 34 2e 30 00 04 ff 00
00 00 02 00 02 00 17 00 20 00 5c 5c 50 52 4f 47
59 44 45 53 41 5c 49 50 43 24 00 49 50 43 00 00
14
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 06 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 32 95 6d
15
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 46 f0 f0
04 06 0e 00 ff ef 16 0c 00 00 28 00 28 00 23 7f
ff 53 4d 42 73 00 00 00 00 90 00 00 00 00 00
00 00 00 00 00 00 00 00 00 03 c0 00 00 00 82 09
03 75 00 29 00 00 00 00 00 02 ff 00 00 00 04 00
49 50 43 00 00 81 95 6d 86 cb 94 6d 86 0d 09 0e
```

```

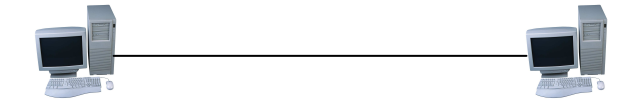
16
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 04 f0 f1
01 06 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 20 96 6d
17
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 7e f0 f0
06 06 0e 00 ff ef 16 0c 00 00 28 00 28 00 7f 23
ff 53 4d 42 25 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 03 c0 00 00 00 00 82 0a
0e 20 00 00 00 08 00 00 10 00 00 00 00 88 13 00
00 00 00 20 00 4c 00 00 00 00 00 00 00 2d 00 5c
50 49 50 45 5c 4c 41 4e 4d 41 4e 00 68 00 57 72
4c 65 68 44 7a 00 42 31 36 42 42 44 7a 00 01 00
00 10 ff ff ff ff 45 53 43 4f 4d 00 00 6f 96 6d
18
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 08 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 be 96 6d
19
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 04 f0 f1
01 08 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 5d 97 6d
20
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 7e f0 f0
08 08 0e 00 ff ef 16 0c 00 00 28 00 28 00 7f 23
ff 53 4d 42 25 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 03 c0 00 00 00 00 02 0b
0e 20 00 00 00 08 00 00 10 00 00 00 00 88 13 00
00 00 00 20 00 4c 00 00 00 00 00 00 00 2d 00 5c
50 49 50 45 5c 4c 41 4e 4d 41 4e 00 68 00 57 72
4c 65 68 44 7a 00 42 31 36 42 42 44 7a 00 01 00
00 10 00 00 00 80 45 53 43 4f 4d 00 00 ac 97 6d
21
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 0a 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 fb 97 6d
22
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 04 f0 f1
01 0a 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 4a 98 6d
23
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 12 f0 f0
0a 0b 0e 00 ff ef 14 00 00 00 28 00 00 00 7f 23
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 01 99 98 6d
24
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 0d 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 45 99 6d
25
03 00 00 00 00 01 00 04 ac 44 4d 02 00 8b f0 f0
03 2c 00 ff ef 08 00 00 00 00 00 00 00 42 34 20
20 20 20 20 20 20 20 20 20 20 20 20 1b 49 42 4d
53 45 52 56 45 52 20 20 20 20 20 20 00 ff 53 4d
42 25 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 11 00 00
06 00 00 00 00 00 00 00 00 00 e8 03 00 00 00 00
00 00 00 00 06 00 56 00 03 00 01 00 01 00 02 00
17 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57
53 45 00 09 04 33 17 00 00 00 9b 99 6d 86 99 98
26
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 35 f0 f0
0c 0a 0e 00 ff ef 16 04 00 00 00 00 28 00 7f 23
ff 53 4d 42 71 00 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 00 00 00 03 c0 00 00 00 00 01 50
00 00 00 45 f1 99 6d 86 45 99 6d 86 1f 09 52 5b
27
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 35 f0 f0
0a 0e 0e 00 ff ef 16 0c 00 00 28 00 28 00 23 7f
ff 53 4d 42 71 00 00 00 00 80 01 00 00 00 00 00
00 00 00 00 00 00 00 00 03 c0 00 00 00 00 01 50
00 00 00 00 40 9a 6d 86 9b 99 6d 86 20 09 75 5b
28
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 12 f0 f0
0e 0d 0e 00 ff ef 14 00 00 00 28 00 00 00 7f 23
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 8f 9a 6d
29
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 11 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 de 9a 6d

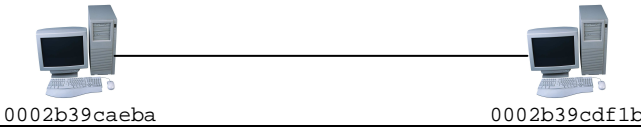
```

```

30
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 12 f0 f0
10 0d 0e 00 ff ef 18 00 00 00 00 00 00 00 7f 23
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 2d 9b 6d
31
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 04 f0 f1
01 13 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 7c 9b 6d
32
00 02 b3 9c ae ba 00 02 b3 9c df 1b 00 03 f0 f0
53 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 cb 9b 6d
33
00 02 b3 9c df 1b 00 02 b3 9c ae ba 00 03 f0 f1
73 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 77 9c 6d

```

No. Trama	Tamaño (bytes)	Campo de Control (en binario)	Tipo de Trama	N(s)	N(r)	P/F	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							

No. Trama	Tamaño (bytes)	Campo de Control (en binario)	Tipo de Trama	N(s)	N(r)	P/F		
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								

6 bytes	6 bytes	2 bytes	1 byte	1 byte	1 ó 2 bytes	variable	variable
Dir. Destino	Dir . Origen	Tamaño	SAP Destino	SAP Origen	Control	Información	Relleno

Una vez realizado el análisis, programar una función en lenguaje C que analice tramas LLC bajo la especificación siguiente:

```
int llc(char trama[], int longitud, char resultado[],
int longresultado)
```

La función recibe cuatro parámetros:

trama: un arreglo de caracteres que contiene los bytes de la trama

longitud: contiene el numero de bytes de la trama

resultado: un arreglo de caracteres que servirá de búfer para regresar el análisis de la trama

longresultado: el tamaño de resultado en bytes.

La función debe verificar que la trama contenga el protocolo LLC y en su caso analizarla, guardando el resultado del análisis en el búfer resultado, cuidando de no sobrepasar la longitud del mismo; en caso de que la trama contenga el protocolo LLC la función devolverá 1, en caso contrario devolverá 0.

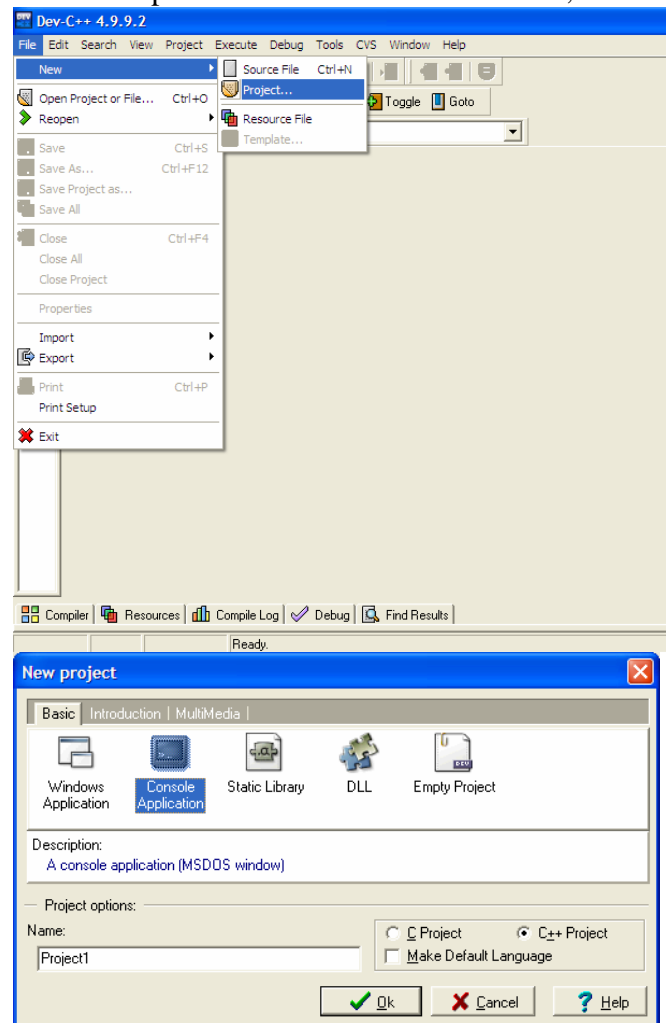
El formato de la salida del analisis debe ser similar a los ejemplos mostrados a continuación:

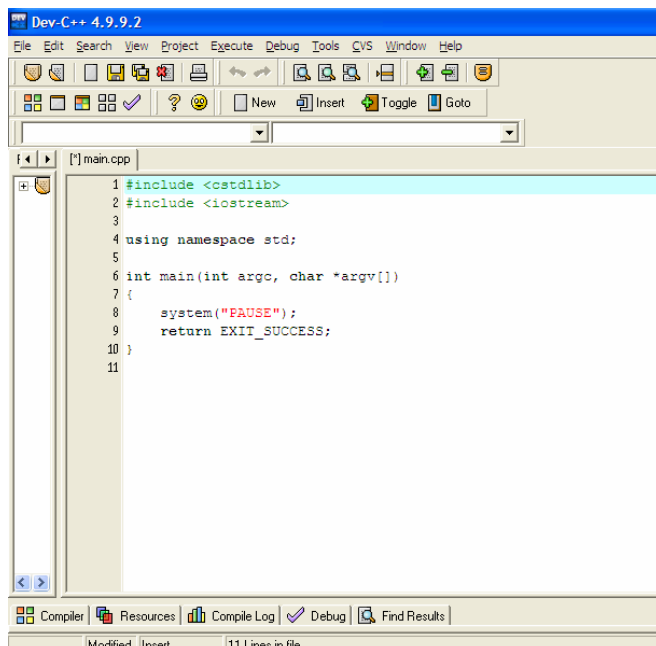
```
0002b39caeba 0002b39cdf1b LLC C S=f0
D=f0 SABME-p
0002b39cdf1b 0002b39caeba LLC R S=f0
D=f0 UA-f
0002b39caeba 0002b39cdf1b LLC C S=f0
D=f0 RR-p NR=0
0002b39cdf1b 0002b39caeba LLC R S=f0
D=f0 RR NR=4
0002b39cdf1b 0002b39caeba LLC C S=f0
D=f0 I NR=2 NS=1
0002b39caeba 0002b39cdf1b LLC C S=f0
D=f0 I-p NR=5 NS=5
0002b39cdf1b 0002b39caeba LLC R S=f0
D=f0 RR-f NR=12
030000000001 0004ac444d02 LLC C S=f0
D=f0 UI
0002b39caeba 0002b39cdf1b LLC C S=f0
D=f0 DISC-p
```

Conteniendo la dirección MAC de destino, la dirección origen, una etiqueta indicando si la trama es LLC, C o R si se trata de un Comando o una Respuesta, el SAP origen, el SAP destino y un resumen del tipo de trama que se trate, (el bit p/f se indica solamente si esta encendido y se indica como p cuando la trama es un comando y como f cuando se trata de una respuesta).

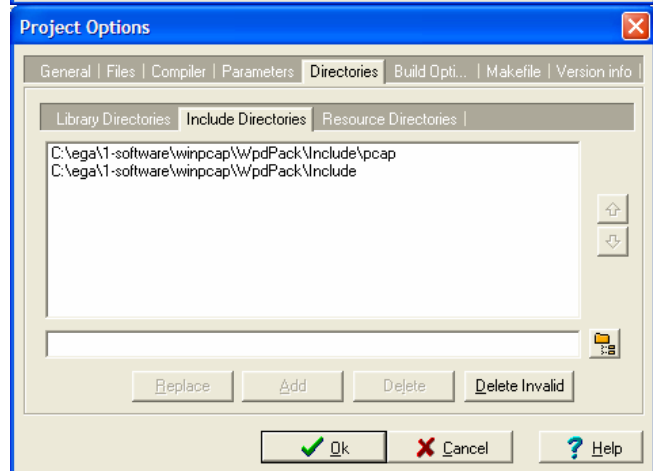
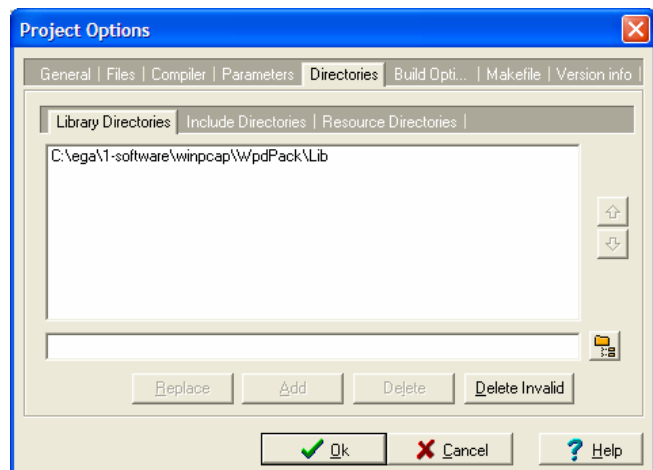
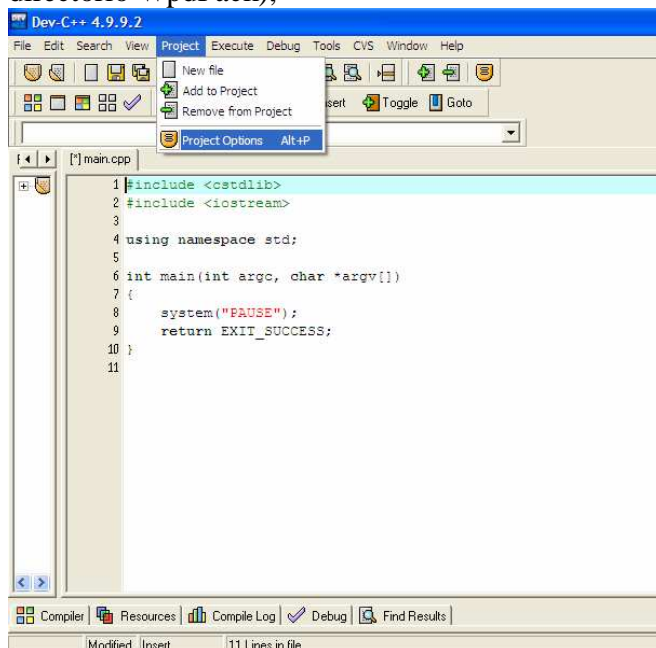
Para probar esta función se compilará un ejemplo de la librería winpcap que permite capturar tramas de la tarjeta de red y trabajar con ella; por lo que hay que asegurarse de que la librería se encuentra instalada en el equipo (si se tiene instalado el analizador de protocolos wireshark es altamente probable que la librería también se encuentre instalada), y de que se cuenta con el paquete de desarrollo de la librería (wpcap).

Para compilar el ejemplo se crea un proyecto nuevo de tipo consola en el IDE de DevC++,

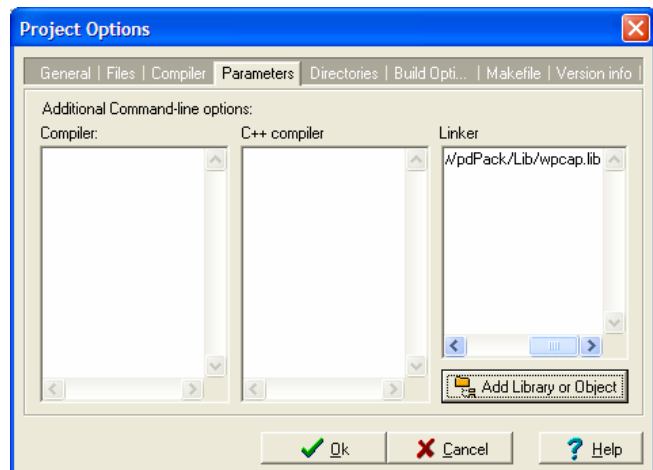




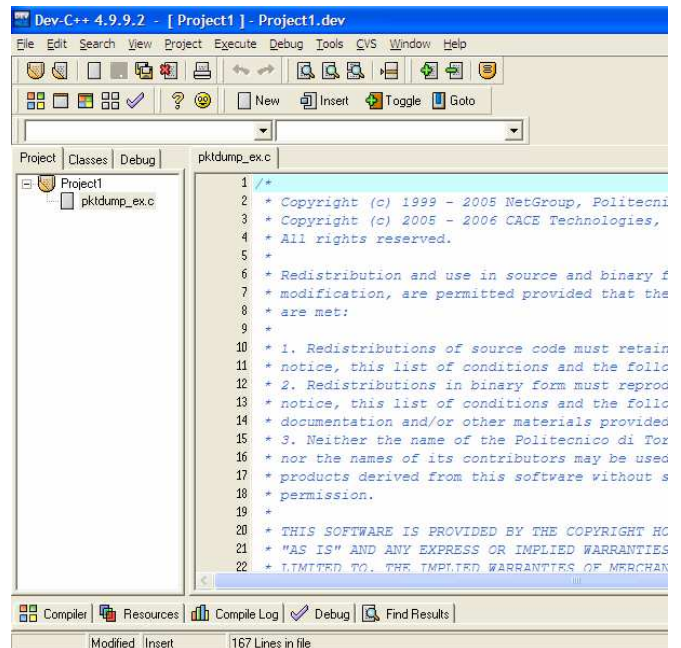
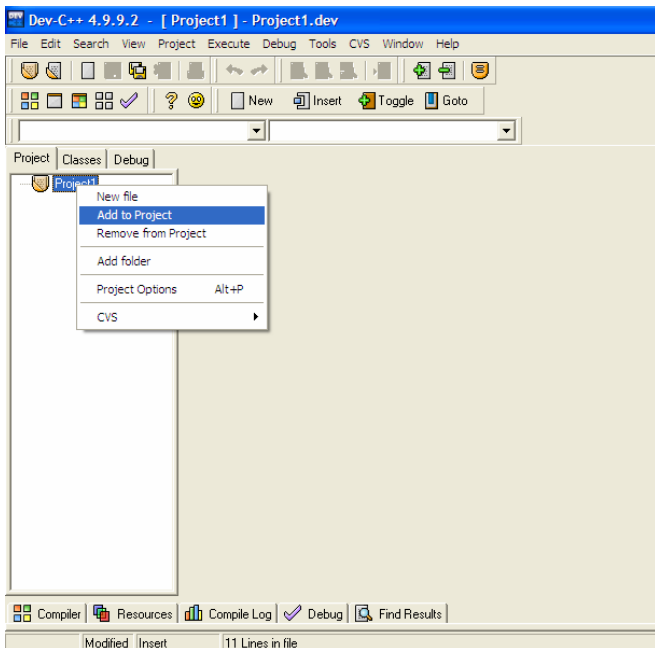
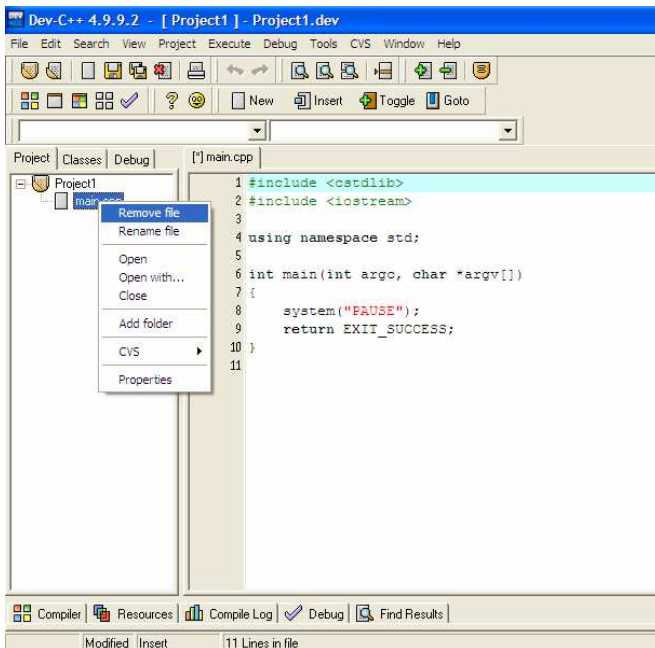
En las opciones del proyecto se deben adicionar los directorios de las librerías correspondientes a winpcap (directorios lib, include\pcap e include del directorio WpdPack);



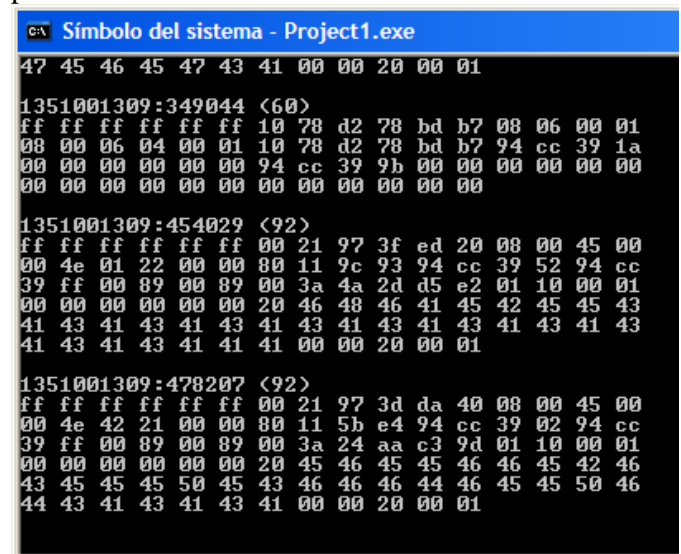
se debe añadir la librería wpcap.lib en la parte de Project Options -> Parameters -> Linker.



Sustituya el archivo main.cpp generado automáticamente por el archivo pktdump_ex.c



Compiele el programa y ejecútelo; el programa empezará a recibir tramas por la tarjeta de red que se seleccione y mostrará los bytes de las mismas en pantalla.



Analice el código del ejemplo compilado para buscar la variable donde se encuentra almacenada la trama y la longitud de la misma, añada además un arreglo de caracteres donde almacenar el resultado del análisis y sustituya la porción de código que despliega las tramas por un conjunto de sentencias que manden llamar a su función y en su caso desplieguen el resultado del análisis:

```
if(llc(trama, longitud,resultado,sizeof(resultado)))
{
    printf("%s",resultado);
}
```

Una vez que se encuentre funcionando correctamente su analizador de tramas LLC avise a su profesor para que le sean transmitidas las tramas que se emplearán para verificar el funcionamiento de su programa, mientras que ejecuta su programa redireccionando la salida a un archivo de texto que será entregado a su profesor por el medio que el le indique.