**El concepto básico de sockets a bajo nivel es enviar un solo paquete por vez con todos los encabezados de los protocolos completados dentro del programa en lugar de usar el kernel.**

**Unix provee dos tipo de sockets para el acceso directo a la red:**

**SOCK_PACKET, recibe y envía datos al dispositivo ubicado en la capa de enlace. Esto significa que el "header" de la placa de red incluido en los datos puede ser escrito o leído. En general es el header de Ethernet. Todos los encabezados de los protocolos subsecuentes también deben ser incluidos en los datos.**

**SOCK_RAW, es el que usaremos por ahora, que incluye los encabezados IP, protocolos y datos subsecuentes.**

**Desde el momento que lo creamos se puede enviar cualquier tipo de paquetes IP por este socket. También se pueden recibir cualquier tipo de paquetes que lleguen al host, después que el socket fue creado, si se hace un "read()" desde él. Se puede observar que aunque el socket es una interfaz al header IP, es tambiés específico para una capa de transporte. Esto significa que para escuchar tráfico TCP, UDP, ICMP hay que crear 3 raw sockets por separado, usando IPPROTO_TCP, IPPROTO_UDP y IPPROTO_ICMP (números de protocolo son 0 ó 6 para tcp, 17 para udp y 1 para icmp).**

**Con esta información es posible crear un simple "sniffer", que muestre todo el contenido de los paquetes TCP que se reciban. ( En este ejemplo se evitan los headers IP y TCP, y se imprime solamente el "payload" con encabezados IP y TCP contenidos en el paquete ).**

**Utilizando el código raw.c como base escribir un "sniffer" que es un programa que muestra el contenido del tráfico que llega.**
**Enviar tráfico al "sniffer" desde el cliente escrito en la parte A del TP1**
**Enviar tráfico ICMP al "sniffer" y mostrar los resultados del LOG con comentarios.**
**Mostrar resultados.**

En el siguiente código obtenido de haber corrido el código raw.c para analizar los paquetes que se envían entre C/S, podemos ver el intercambio de paquetes realizados en el puerto 8080

**********TCP Packet**********

IP encabezado
  |-IP Version        : 4
  |-IP longitud encabezado : 5 DWORDS or 20 Bytes
  |-Type Of Service   : 0
  |-IP longitud total   : 132  Bytes(Tam. paquete)
  |-Id  : 33994
  |-TTL      : 64
  |-Protocolo : 6
  |-Checksum : 47015

```
   |-Origen IP        : 127.0.0.1
   |-Destino IP   : 127.0.0.1

TCP encabezado
   |-Origen Puerto     : 53932
   |-Destino Puerto: 8080
   |-Numero Secuencia   : 2786119005
   |-Numero Ack: 1842515853
   |-Encabezado Longitud      : 8 DWORDS or 32 BYTES
   |-Urgent Flag          : 0
   |-AckFlag : 1
   |-Push Flag            : 1
   |-Reset Flag           : 0
   |-Synchronise Flag     : 0
   |-Finish Flag          : 0
   |-Window         : 512
   |-Checksum       : 65144
   |-Puntero Urgente: 0

                        DATA Dump
IP encabezado
    45 00 00 84 84 CA 40 00 40 06 B7 A7 7F 00 00 01         E.....@.@......
    7F 00 00 01                                             ...
TCP encabezado
    D2 AC 1F 90 A6 10 CD 5D 6D D2 8F 8D 80 18 02 00         .......]m...?...
    FE 78 00 00 01 01 08 0A 12 6E 5E 18 12 6E 1B 9A         .x.......n^..n..
Contenido de Datos en el Paquete
    68 6F 6C 61 0A 00 00 00 00 00 00 00 00 00 00 00         hola............
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................

#################################################################

**********TCP Packet**********

IP encabezado
   |-IP Version        : 4
   |-IP longitud encabezado : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP longitud total   : 52  Bytes(Tam. paquete)
   |-Id  : 33995
   |-TTL      : 64
   |-Protocolo : 6
   |-Checksum : 47094
   |-Origen IP        : 127.0.0.1
   |-Destino IP   : 127.0.0.1
```

TCP encabezado
  |-Origen Puerto     : 53932
  |-Destino Puerto: 8080
  |-Numero Secuencia   : 2786119085
  |-Numero Ack: 1842515933
  |-Encabezado Longitud      : 8 DWORDS or 32 BYTES
  |-Urgent Flag          : 0
  |-AckFlag : 1
  |-Push Flag            : 0
  |-Reset Flag           : 0
  |-Synchronise Flag     : 0
  |-Finish Flag          : 0
  |-Window         : 512
  |-Checksum       : 65064
  |-Puntero Urgente: 0

                    DATA Dump
IP encabezado
   45 00 00 34 84 CB 40 00 40 06 B7 F6 7F 00 00 01         E..4..@.@.....
   7F 00 00 01                                             ...
TCP encabezado
   D2 AC 1F 90 A6 10 CD AD 6D D2 8F DD 80 10 02 00         ........m...�...
   FE 28 00 00 01 01 08 0A 12 6E 6A 8F 12 6E 6A 8F         .(.......nj..nj.
Contenido de Datos en el Paquete

#####################################################################

**********TCP Packet**********

IP encabezado
  |-IP Version        : 4
  |-IP longitud encabezado : 5 DWORDS or 20 Bytes
  |-Type Of Service   : 0
  |-IP longitud total   : 132  Bytes(Tam. paquete)
  |-Id  : 33996
  |-TTL      : 64
  |-Protocolo : 6
  |-Checksum : 47013
  |-Origen IP        : 127.0.0.1
  |-Destino IP   : 127.0.0.1

TCP encabezado
  |-Origen Puerto     : 53932
  |-Destino Puerto: 8080
  |-Numero Secuencia   : 2786119085
  |-Numero Ack: 1842515933
  |-Encabezado Longitud      : 8 DWORDS or 32 BYTES

```
   |-Urgent Flag          : 0
   |-AckFlag : 1
   |-Push Flag            : 1
   |-Reset Flag           : 0
   |-Synchronise Flag     : 0
   |-Finish Flag          : 0
   |-Window         : 512
   |-Checksum       : 65144
   |-Puntero Urgente: 0

                        DATA Dump
IP encabezado
   45 00 00 84 84 CC 40 00 40 06 B7 A5 7F 00 00 01         E.....@.@......
   7F 00 00 01                                             ...
TCP encabezado
   D2 AC 1F 90 A6 10 CD AD 6D D2 8F DD 80 18 02 00         ........m...?...
   FE 78 00 00 01 01 08 0A 12 6E 97 B6 12 6E 6A 8F         .x.......n...nj.
Contenido de Datos en el Paquete
   64 61 73 0A 00 00 00 00 00 00 00 00 00 00 00 00         das.............
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................

#################################################################
```

1) Aqui se muestra el tráfico ICMP que se manda al sniffer, el cual se realiza mediante la funciond de **ping <dns o  ip adress>** en la terminal

```
**********************ICMP Packet*************************

IP encabezado
   |-IP Version        : 4
   |-IP longitud encabezado : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP longitud total   : 84  Bytes(Tam. paquete)
   |-Id  : 0
   |-TTL      : 118
   |-Protocolo : 1
   |-Checksum : 18777
   |-Origen IP        : 142.251.133.14
   |-Destino IP   : 172.26.59.44
```

ICMP encabezado
  |-Tipo : 0  (ICMP Echo Reply)
  |-Code : 0
  |-Checksum : 46418

IP encabezado
   45 00 00 54 00 00 00 00 76 01 49 59 8E FB 85 0E        E..T....v.IY....
   AC 1A 3B 2C                                            ..;,
UDP encabezado
   00 00 B5 52 A4 2A 00 05                                ...R.*..
Contenido de Datos en el Paquete
   72 88 49 64 00 00 00 00 28 BE 03 00 00 00 00 00        r.Id....(.......
   10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F        ................
   20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F        !"#$%&'()*+,-./
   30 31 32 33 34 35 36 37                                01234567

#################################################################

**********ICMP Packet**********

IP encabezado
  |-IP Version        : 4
  |-IP longitud encabezado : 5 DWORDS or 20 Bytes
  |-Type Of Service   : 0
  |-IP longitud total   : 84  Bytes(Tam. paquete)
  |-Id  : 0
  |-TTL      : 118
  |-Protocolo : 1
  |-Checksum : 18777
  |-Origen IP        : 142.251.133.14
  |-Destino IP   : 172.26.59.44

ICMP encabezado
  |-Tipo : 0  (ICMP Echo Reply)
  |-Code : 0
  |-Checksum : 16461

IP encabezado
   45 00 00 54 00 00 00 00 76 01 49 59 8E FB 85 0E        E..T....v.IY....
   AC 1A 3B 2C                                            ..;,
UDP encabezado
   00 00 40 4D A4 2A 00 06                                ..@M.*..
Contenido de Datos en el Paquete
   73 88 49 64 00 00 00 00 9C C2 03 00 00 00 00 00        s.Id............
   10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F        ................
   20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F        !"#$%&'()*+,-./
   30 31 32 33 34 35 36 37                                01234567

```
#################################################################

**********************ICMP Packet*************************

IP encabezado
   |-IP Version        : 4
   |-IP longitud encabezado : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP longitud total   : 84  Bytes(Tam. paquete)
   |-Id  : 0
   |-TTL      : 118
   |-Protocolo : 1
   |-Checksum : 18777
   |-Origen IP        : 142.251.133.14
   |-Destino IP   : 172.26.59.44

ICMP encabezado
   |-Tipo : 0  (ICMP Echo Reply)
   |-Code : 0
   |-Checksum : 56648

IP encabezado
    45 00 00 54 00 00 00 00 76 01 49 59 8E FB 85 0E         E..T....v.IY....
    AC 1A 3B 2C                                             ..;,
UDP encabezado
    00 00 DD 48 A4 2A 00 07                                 ...H.*..
Contenido de Datos en el Paquete
    74 88 49 64 00 00 00 00 FE C5 03 00 00 00 00 00         t.Id............
    10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F          ................
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F          !"#$%&'()*+,-./
    30 31 32 33 34 35 36 37                                 01234567

#################################################################
```