Apéndice C

Sniffer

En la figura C.1 se muestra la pestaña decodificar (*Decode Tab*) en la cual se muestran tres ventanas: la primera muestra un resumen de la captura, la segunda muestra el detalle del paquete seleccionado en la primera y en la tercera se muestra el contenido en hexadecimal del paquete.

La ventana de resumen muestra una visión general de la transacción entre dos estaciones en formato resumido. A continuación se explica el cada una de las columnas de esta ventana. (Network Associates [2002]).

- Numero de paquete (*No.*)
    - Muestra el número de paquete en el periódo de la captura.
- Estado (*Status*)
    - Muestra el estado del paquete de acuerdo a una bandera preestablecida, un ejemplo es si el paquete es un gatillo se marca como Trigger.
- Dirección fuente (*Source Address*)
    - Es la dirección de donde se origina el paquete.
- Dirección destino (*Dest Address*)
    - Es la dirección a donde se dirige el paquete.
- Resumen (*Summary*)
    - Aquí se muestra información clave del contenido del paquete.
- Longitud (*Len (Bytes)*)
    - Es la longitud del paquete.

- Tiempo Relativo (*Rel. Time*)
    - Muestra el intervalo entre el paquete elegido y el paquete marcado (hh:mm:ss:milis).

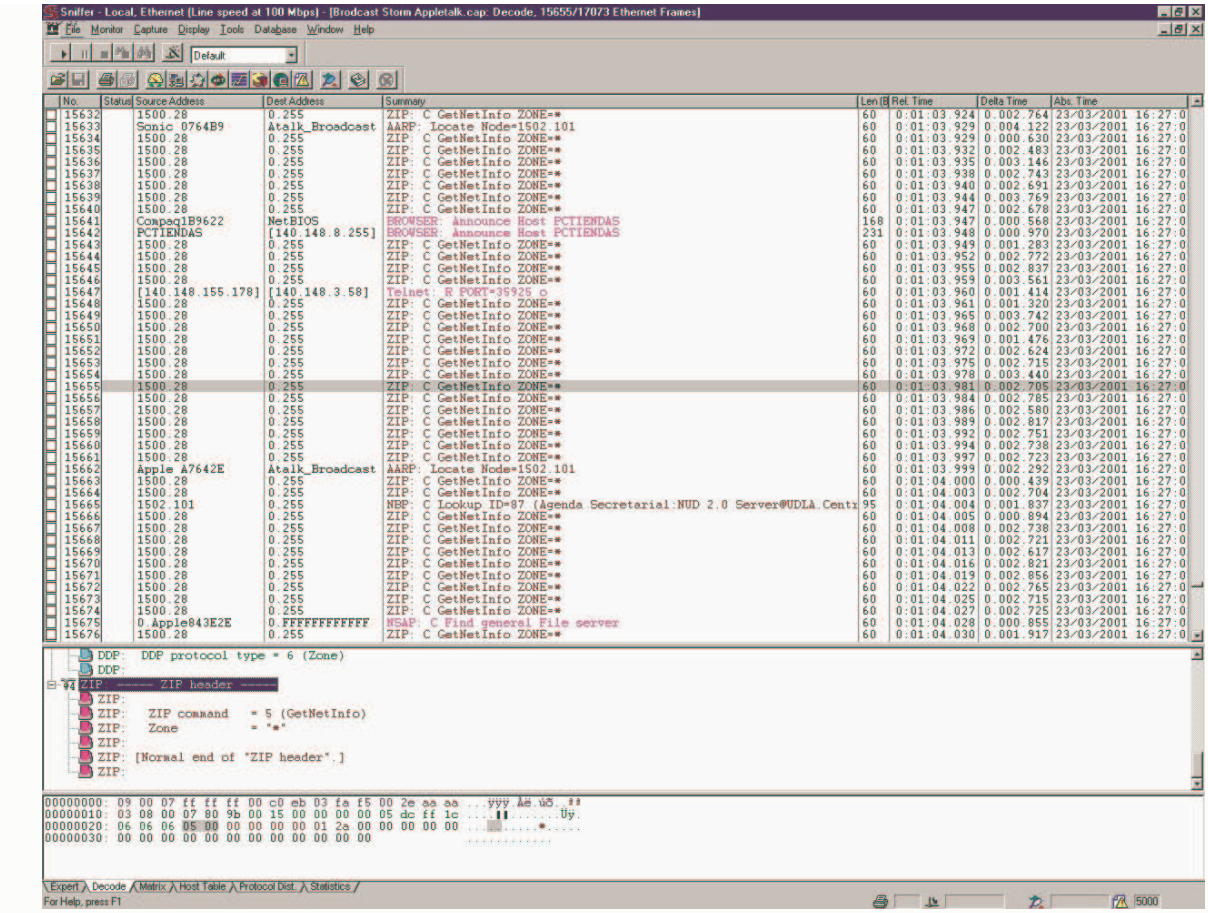

Figura C.1 *Muestra de la pestaña decode del programa sniffer*

- Tiempo Delta (*Delta Time*)
    - Muestra el intervalo entre el paquete elegido y el anterior (ss:mili-s:micro-s).
- Tiempo Absoluto (*Abs. Time*)
    - Muestra cuando el paquete fue recibido (dd/mm/aa hh:mm:ss).

La siguiente ventana es la de detalle, la cual muestra el contenido a detalle del paquete seleccionado en la ventana anterior, se muestra la interpretación de cada capa del protocolo en el paquete.

La última ventana es la de Hex, la cual muestra el paquete seleccionado en la ventana anterior, en el formato de octetos hexadecimales y en formato ASCII (o EBCDIC).

A continuación se muestra una parte de el archivo resultante de la impresion de un resumen de todos los paquetes, esta impresión se realiza con la opción *summary* seleccionada al momento de realizarse.

```
Frame Status Source               Destination          Bytes Rel Time
Delta Time   Abs time       Summary
-------------------------------------------------------------------------------
     1 M      0.Apple843E2E               0.FFFFFFFFFFFF                 60 0:00:00.000
0.000.000    23/03/2001 16:25:59 NSAP: C Find nearest File server
     2        [140.148.155.178]            [140.148.3.126]                64 0:00:00.017
0.017.663    23/03/2001 16:25:59 Telnet: R PORT=33652 No<1B>[22;27m
     3        [140.148.155.178]            [140.148.3.58]                 60 0:00:00.038
0.020.466    23/03/2001 16:25:59 Telnet: R PORT=35925 l
     4        [140.148.155.178]            [140.148.3.126]               477 0:00:00.064
0.026.352    23/03/2001 16:25:59 Telnet: R PORT=33652 <1B>[2;7m<1B>[1;72HTOP<1B>[22;27m<1...
```

después de tranferirlo a la máquina con el S.O Unix y ejecutar el siguiente comando:

grep ": " archivo entrada | awk '{print $1" "$4}' | sed "s/^0.//" > archivo salida

se obtiene el siguiente archivo del que se muestra una pequeña parte, el cual solo contiene los datos que nos interesan, en este caso el *Delta Time* y el protocolo del paquete:

```
000.000       NSAP:
017.663       Telnet:
020.466       Telnet:
026.352       Telnet:
```

Una vez teniendo este archivo, se utiliza como entrada al programa selector de datos, el cual genera las series de tiempo, de acuerdo a los parametros referidos, de este programa se obtiene el siguiente archivo del que se muestra una pequeña parte. El archivo contiene la serie de tiempo de los protocolos referenciados al ejecutar el programa.

```
 17.66 0 0 1
 38.13 0 0 1
 64.48 0 0 1
258.36 0 0 0
```

Este archivo consta de 4 columnas: la primera es el acomulativo del *Delta Time*, la segunda, tercera y cuarta corresponde al número de ocurrencias de los procolos seleccionados en el tiempo delta respectivamente. De este archivo se generan las series de tiempo respectivas.