



---

# Ethereal

Roberto Gómez Cárdenas

rogomez@itesm.mx

<http://webdia.cem.itesm.mx/ac/rogomez>



- Ethereal es un analizador de tráfico de red, o "sniffer", para sistemas operativos Unix y sistemas basados en Unix, así como sistemas Windows
- Utiliza:
  - GTK+, una librería que provee una interface de usuario grafica,
  - libpcap, una librería para filtrar y capturar paquetes,
- Posee la posibilidad de ver la reconstrucción del fluido de una sesión TCP.
- Autor: Gerald Combs (julio 1998 - version 0.2.0. )



- AIX
- Tru64 Unix (formalmente Digital Unix)
- Debian GNU/Linux
- Red Hat Linux
- FreeBSD
- NetBSD
- OpenBSD
- HP/UX
- Sparc / Solaris 8
- Windows 2000, Windows NT y Windows Me/98/95



- Posible obtenerlo de
  - <http://www.ethereal.com>
- Versión actual: 0.9.6 (septiembre 2002)
- Requisitos
  - GTK+, el GIMP Tool Kit y Glin
  - libpcap ([www.tcpdump.org](http://www.tcpdump.org))
- Unix
  - rpm, paquetes debian. .tar.gz
- Windows
  - winpcap



- Datos pueden ser capturados del cable de una conexión viva, o leídos de un archivo capturado.
- Puede leer archivos de datos de diferentes paquetes de captura de datos
  - tcpdump (libpcap), NAI's Sniffer&trade; (compressed and uncompressed), Sniffer&trade; Pro, NetXray&trade;, Sun snoop and atmsnoop, Shomiti/Finisar Surveyor, AIX's iptrace, Microsoft's Network Monitor, Novell's LANalyzer, RADCOM's WAN/LAN Analyzer, etc

## Más características



- Datos pueden ser capturados de Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM, e interfaces tipo loopback
  - no todos los tipos son soportados en todas las plataformas
- Datos pueden verse a través de un GUI o de una terminal en texto plano.
- La salida puede ser guardada o impresa como texto plano o Postscript
- Toda, o parte, de la captura puede ser almacenada en disco.
- Se cuenta con una guía del usuario en html

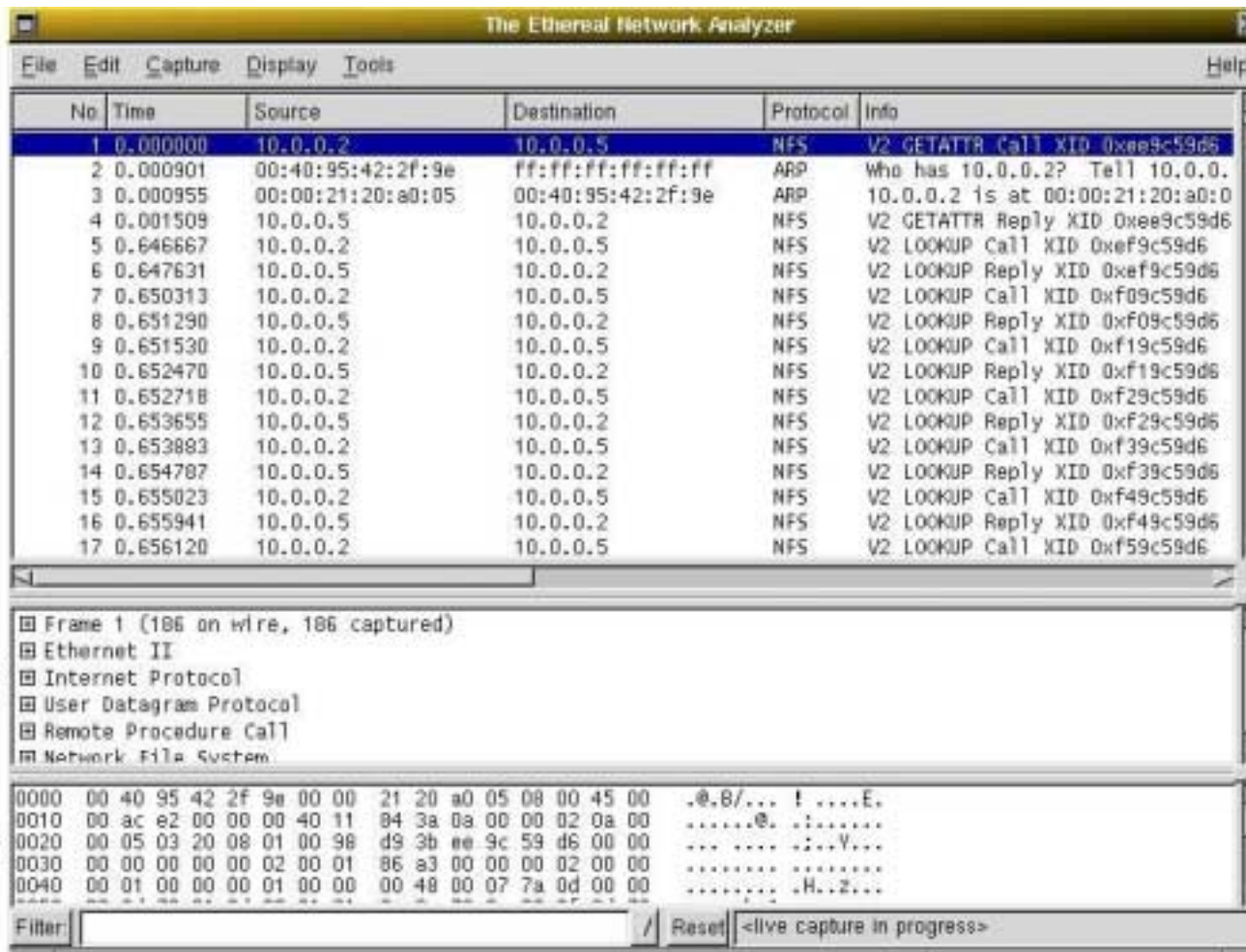


- Panel alto (list pane)
  - “summary” de cada paquete capturado
  - eligiendo en esta ventana se despliega las otras dos
- Panel de en medio (tree view)
  - despliega paquete seleccionado en el panel superior pero en más detalle
- Panel bajo (data view)
  - despliega datos del paquete seleccionado en el panel alto, y “highlights” el campo seleccionado en el panel de enmedio

# Usando ethereal



packet list pane



The screenshot shows the 'The Ethereal Network Analyzer' window. It has a menu bar (File, Edit, Capture, Display, Tools, Help) and a toolbar. The main area is divided into three panes:

- Packet List Pane (1):** A table showing captured packets. The first packet is selected.
- Tree View Pane (2):** A hierarchical view of the selected packet's structure, showing Ethernet II, Internet Protocol, User Datagram Protocol, Remote Procedure Call, and Network File System.
- Data View Pane (3):** A hex dump of the selected packet's data, showing hexadecimal values and their ASCII representation.

At the bottom, there is a 'Filter:' field, a 'Reset' button, and a status bar indicating '<live capture in progress>'.

tree view pane

data view pane

A Filter: B C D displays informational messages

enter or edit filter strings Reset



# Menu principal y captura de paquetes



**bootparams.cap – Ethereal**

File Edit Capture Display Tools Help

No.	Time	Start... Ctl+K	Destination	Protocol	Info
1	0.00000	Stop Ctl+E	131.151.32.129	Portmap	V2 GETPORT Call XID 0x392f03fd
2	0.00129		131.151.32.21	Portmap	V2 GETPORT Reply XID 0x392f03fd
3	0.001452		131.151.32.129	BOOTPARAMS	V1 GETFILE Call XID 0x392f03c8
4	0.024121		131.151.32.21	BOOTPARAMS	V1 GETFILE Reply XID 0x392f03c8
5	2.300095		131.151.32.129	Portmap	V2 GETPORT Call XID 0x39239720
6	2.301287		131.151.32.21	Portmap	V2 GETPORT Reply XID 0x39239720
7	2.301588		131.151.32.129	BOOTPARAMS	V1 GETFILE Call XID 0x39239714
8	2.324385		131.151.32.21	BOOTPARAMS	V1 GETFILE Reply XID 0x39239714
9	7.432976		131.151.32.129	Portmap	V2 GETPORT Call XID 0x39206e36
10	7.434178		131.151.32.21	Portmap	V2 GETPORT Reply XID 0x39206e36
11	7.434450		131.151.32.129	BOOTPARAMS	V1 WHOAMI Call XID 0x39206e5b
12	7.460175		131.151.32.21	BOOTPARAMS	V1 WHOAMI Reply XID 0x39206e5b

Frame 1 (98 on wire, 98 captured)

- Ethernet II
- Internet Protocol, Src Addr: 131.151.32.21 (131.151.32.21), Dst Addr: 131.151.32.129 (131.151.32.129)
- User Datagram Protocol, Src Port: 760 (760), Dst Port: sunrpc (111)
- Remote Procedure Call

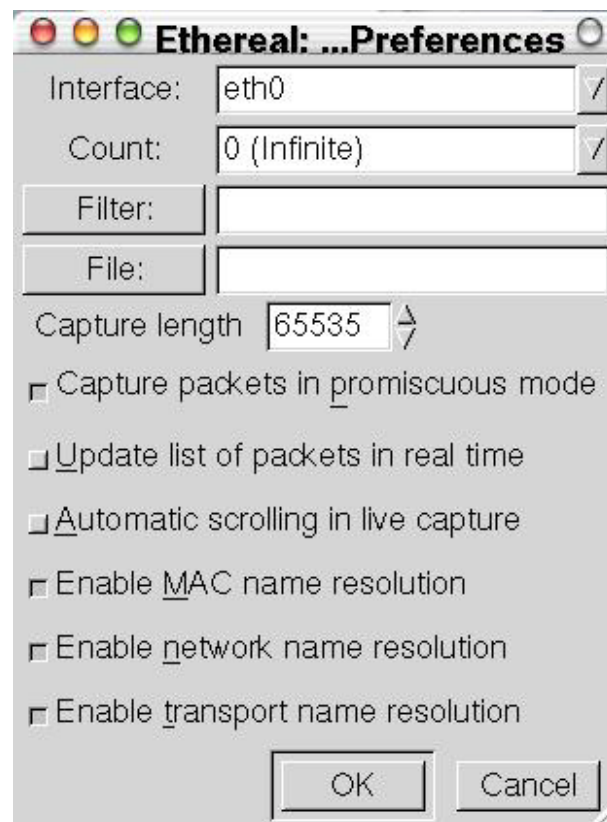
```

0000  00 40 05 40 ef 24 00 60 08 9f b1 f3 08 00 45 00  .@.@.$.' .....E.
0010  00 54 bd fc 00 00 40 11 74 d8 83 97 20 15 83 97  .T....@. t... ..
0020  20 81 02 f8 00 ff 00 40 69 a0 39 2f 03 fd 00 00  ....n.@ i.9/....
  
```

Filter: [ ] [v] Reset File: bootparams.cap



## The Capture Preferences dialog box



<capture> - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.5	10.0.0.2	TCP	23 > 1037 [RST, ACK] Seq=0 Ack=3444297104
2	0.859769	10.0.0.5	10.0.0.2	TCP	23 > 1038 [RST, ACK] Seq=0 Ack=344613046
3	1.884001	10.0.0.5	10.0.0.2	TCP	23 > 1039 [RST, ACK] Seq=0 Ack=343559969

Frame 1 (60 on wire, 60 captured)

Ethernet II

Internet Protocol

Transmission Control Protocol, Src Port: 23 (23), Dst Port: 1037 (1037), Seq: 0, Ack: 3444297104

Source port: 23 (23)

Destination port: 1037 (1037)

Sequence number: 0

Acknowledgement number: 3444297104

Header length: 20 bytes

Flags: 0x0014 (RST, ACK)

Window size: 0

Checksum: 0xfcc9

0000	00 00 21 20 a0 05 00 40	95 42 2f 9e 08 00 45 10	..! ...@ .B/...E.
0010	00 28 4a 6a 00 00 ff 06	5d 4f 0a 00 00 05 0a 00	.(Tj.... ]0.....
0020	00 02 00 17 04 0d 00 00	00 00 cd 4b cd 90 50 14	..... ..K..P.
0030	00 00 fc c9 00 00 20 46	44 45 42 45	..... F DEBE

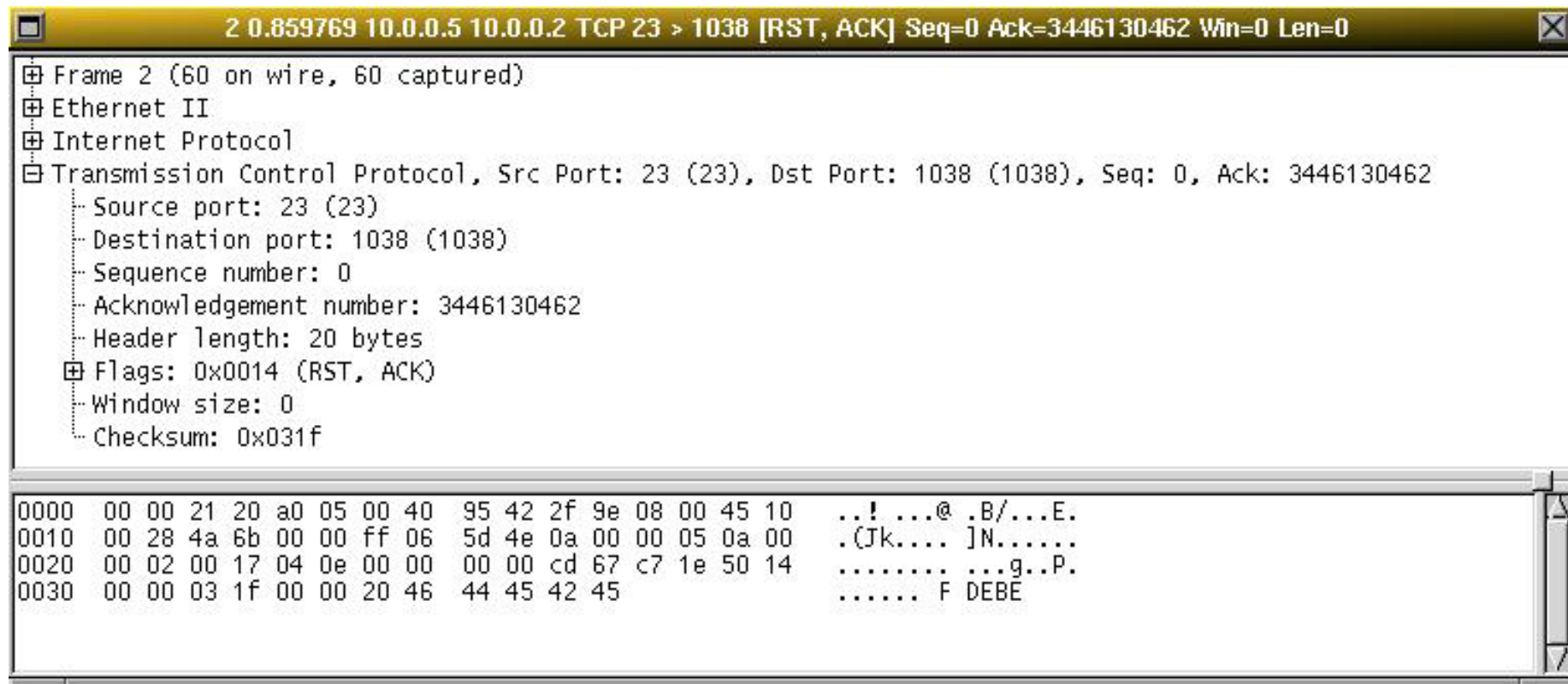
Filter:

/

Reset

File: <capture> Drops: 0

# Viendo paquete en ventana separada





-B <byte view height> | -T <height> | -P <height>

- asigna el valor inicial del ancho de la ventana del panel de datos ( B panel bajo/bottom), del panel de arbol ( T ) y del panel de paquetes ( P )

-c <count>

- especifica número paquetes a capturar cuando se capturan datos en vivo

-f <capture filter>

- asigna la expresión inicial a usar por el filtro

-h

- opción de ayuda, despliega las opciones

-v

despliega versión de ethereal

-i <interface>

- especifica la interfaz de captura (p.e. ethereal -i eth0 )

# Los menús de ethereal



- File
  - abrir, guardar archivos de captura, imprimir archivos captura, etc.
- Edit
  - encontrar un frame, ir a un frame, marcar uno o más frames, asignar preferencias, crear filtro y activar/desactivar disección protocolos
- Capture
  - empezar/terminar captura de paquetes
- Display
  - desplegar plugins. seguir un stream TCP, obtener un resumen de los paqueres capturados, desplegar estadísticas de protocolos, colorear frames
- Help
  - ayuda básica de ethereal



# El menú de archivos



- **Open** abrir archivo captura
- **Close** cerrar archivo captura
- **Save** guardar archivo captura
- **Save As...** guardar archivo captura
- **Reload** recargar archivo actual captura
- **Print...** imprimir todos paquetes de archivo de captura
- **Print Packet** imprimir el paquete actual
- **Quit** salir de ethereal

<u>O</u> pen...	Ctrl+O
<u>C</u> lose	Ctrl+W
<u>S</u> ave	Ctrl+S
Sa <u>v</u> e As...	
<u>R</u> eload	Ctrl+R
<u>P</u> rint...	
Print <u>P</u> acket	Ctrl+P
<u>Q</u> uit	Ctrl+Q

# Menú de edición



- **Find Frame** buscar frame a través de un filtro.
- **Go to Frame** permite ir a un frame a través de un número
- **Mark Frame** marca el frame seleccionado
- **Mark all frames** marca todos los frames
- **Unmark all frames** desmarca todos los frames
- **Preferences** asignar preferencias para diferentes parámetros que controla ethereal
- **Capture files** crear y editar filtros
- **Protocols** activar/desactivar disección de protocolos

Find Frame...	Ctrl+F
Find Next	Ctrl+N
Find Previous	Ctrl+B
Go To Frame...	Ctrl+G
Mark Frame	Ctrl+M
Mark All Frames	
Unmark All Frames	
Preferences...	
Capture Filters...	
Display Filters...	
Protocols...	



# Menú de captura



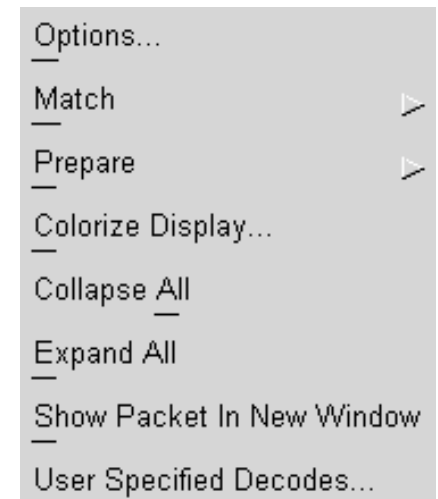
Start... Ctl+K  
—

- **Start** despliega las opciones de captura
- **Stop** detiene la captura de paquetes

# Menú de despliegue



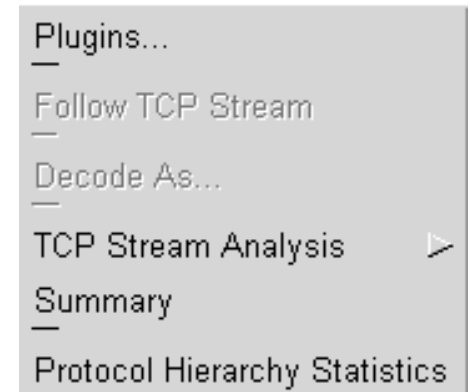
- **Options** controla forma desplegar información acerca de paquetes
- **Match Selected** seleccionar paquetes que tienen un campo seleccionado en panel árbol
- **Colorize Display** colorear paquetes
- **Collapse All** retrae los subárboles menú árbol
- **Expand All** expande los subárboles menú árbol
- **Show packet...** despliega paquetes seleccionados en una ventana aparte
- **User Specified ...** decodificar algunos paquetes como un protocolo en particular



# Menú de herramientas



- **Plugins** permite manejar plugins de ethereal
- **Follow ...** desplegar todos los segmentos capturados que se pertenezcan a la misma conexión TCP del campo seleccionado
- **Decode** forzar a decodificar ciertos paquetes como un protocolo en particular
- **Summary** ventana información estadística acerca de los paquetes capturados
- **Protocol** despliega árbol jerárquico de estadísticas de paquetes

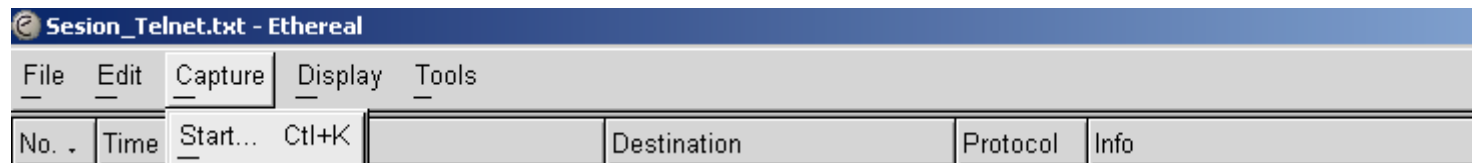




- Dos métodos para capturar paquetes con ethereal
  - En la línea de comandos teclear

`ethereal -i eth0 -k`

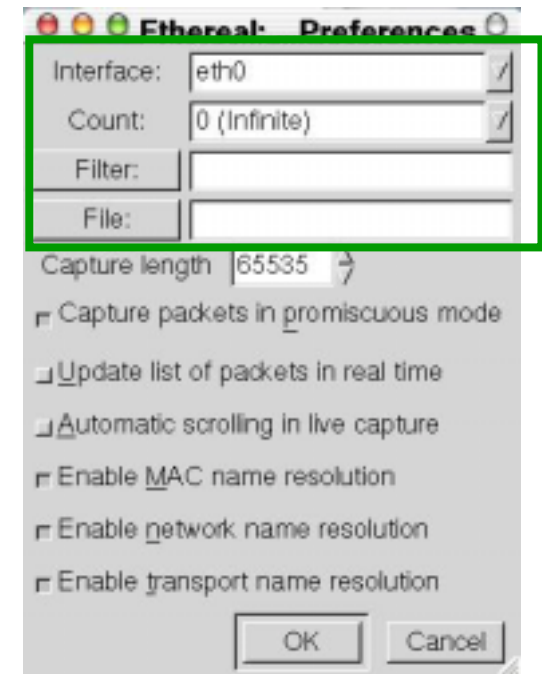
- Arrancar ethereal y seleccionar Start... del menú de captura
  - se despliega menú de preferencias de captura



# El cuadro de dialogo de captura (1/4)



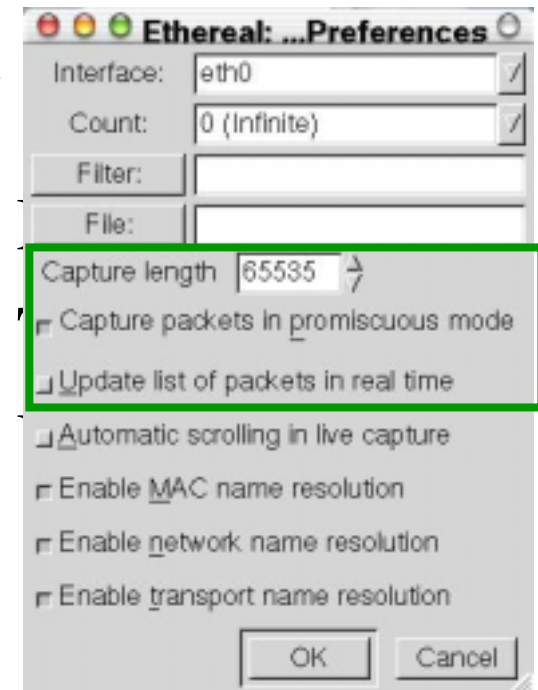
- **Interface** especifica la interfaz de captura
  - solo se puede capturar en una interfaz
  - en algunas sistemas no es posible usar interfaces tipo loopback
  - misma función que la opción `-i <interface>`
- **Count** número de paquetes a capturar
  - numero por default: 0, que significa que no pare de capturar
- **Filter** especificar un filtro de captura
- **File** nombre archivo donde se va a almacenar los paquetes capturados



# El cuadro de dialogo de captura (2/4)



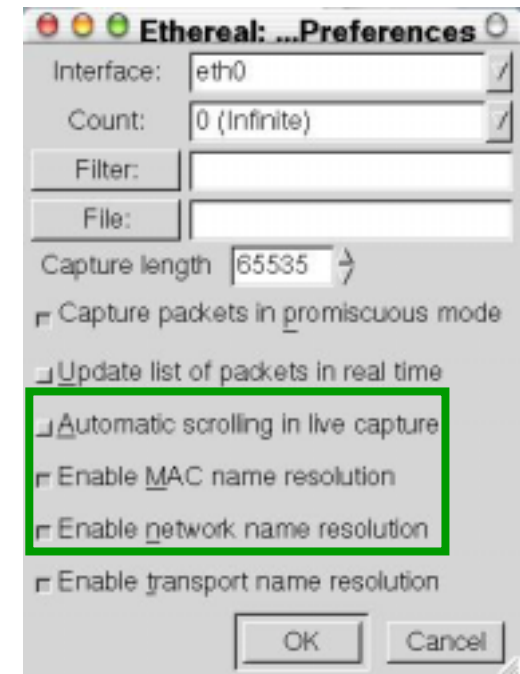
- **Capture length** máxima cantidad de datos a capturar en cada paquete (snaplen)
  - default: 65535
  - al menos la MTU de la interfaz usada
- **promiscuous** interfaz en modo promiscuo
  - si no es especificada solo se capturan paquetes que salen o llegan a ala computadora (no todos los paquetes que pasen por ahí)
- **update** actualizar el panel de paquetes en tiempo real
  - en caso contrario no se despliega ningún paquete hasta que se detenga la captura



# El cuadro de dialogo de captura (3/4)



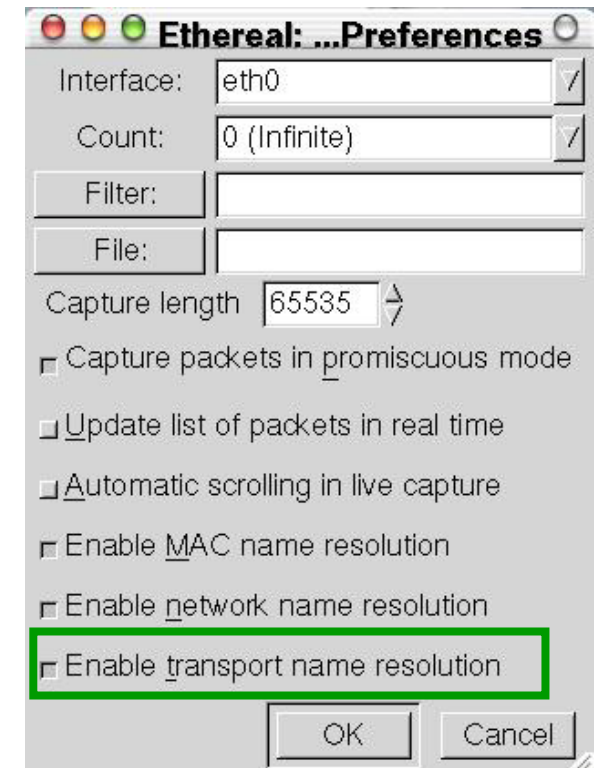
- **automatic ...** ethereal scroll el panel de paquetes conforme llegan nuevos
  - siempre se ve el último paquete
  - en caso contrario se añaden paquetes nuevos al final de la lista pero no se lleva a cabo ningún scroll
- **enable MAC** traducción de los primeros tres bytes de la dirección MAC en nombre del fabricante (IETF)
- **enable Network** traducción direcciones IP en nombre dominio DNS



# El cuadro de dialogo de captura (4/4)



- **enable transport** traducción de número de puertos en protocolos





# Filtrando paquetes



- Ethernet utiliza lenguaje libpcap para definir sus filtros.
  - mayor información man page de tcpdump
- Filtro se define en el campo filter de las preferencias del cuadro diálogo captura
- Un filtro esta formado por una serie de expresiones primitivas conectadas por conjunciones:

[not] primitiva [and | or [not] primitiva ... ]

- Ejemplos

tcp port 23 and host 10.0.0.5

tcp port 23 and not host 10.0.0.5

# Lista de primitivas (1/3)



- [src| dst ] host <host>
  - filtra un host, por IP o por nombre
  - opciones src, dst especifica tráfico entrada o salida
- ether [src | dst] host <ehost>
  - filtro de direcciones ethernet
- gateway host <host>
  - filtrar paquetes que usan host como gateway
  - dirección ethernet fuente o destino es host pero no la dirección fuente ni la destino es host
- less | greater <length>
  - filtra paquetes de longitud menor o igual a un determinado valor
  - paquetes que son mayores o iguales a un determinado valor

# Lista de primitivas (2/3)



- [src | dst ] net <net> [{ mak <mask> } | { len<len> } ]
  - filtrar en número de red
  - opciones src, dst especifica tráfico entrada o salida
  - posible especificar netmask de la red
- [tcp | udp ] [src | dst ] port <port>
  - filtrar en números de puerto TCP y UDP
  - opciones src, dst especifica tráfico entrada o salida
  - opciones tcp, udp especifica paquetes TCP o UDP
  - tcp, udp debe aparecer antes que src, dst
- ip | ether proto <protocol>
  - filtrar a nivel IP o ethernet

# Lista de primitivas (3/3)

---



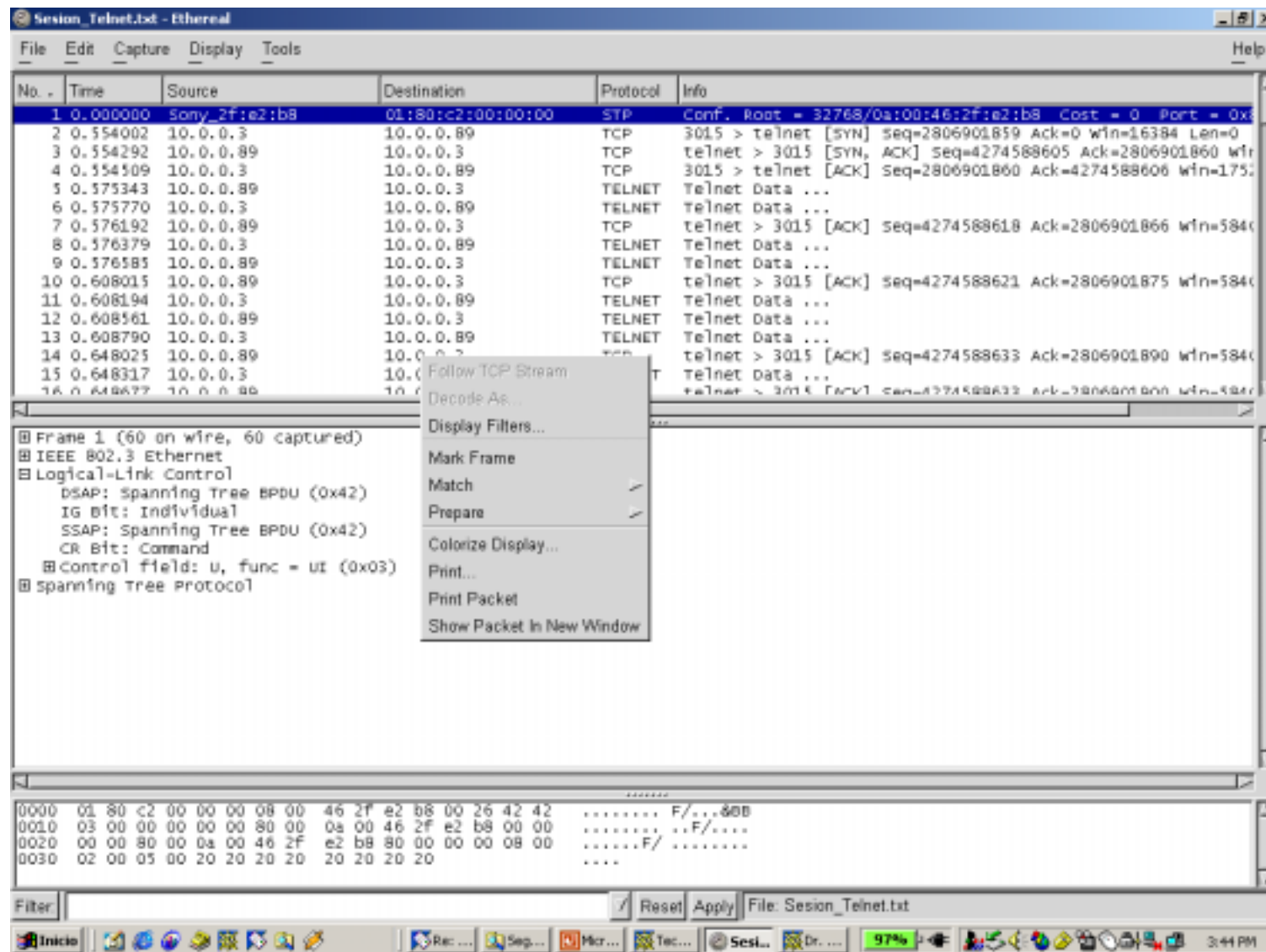
- ether | ip broadcast | multicast
  - filtrar broadcast o multicast tipo Ethernet o IP
- <expr> relop <expr>
  - creación de expresiones complejas de filtros que seleccionen bytes o rangos de bytes en paquetes
  - mayor información: man tcpdump

# Viendo paquetes capturando



- Posible ver los paquetes capturados.
- Paquetes capturados en tiempo real
- Ver paquetes en ventanas separadas
- Existe un menú que puede activarse cuando se selecciona un paquete

# Menú de paquetes

**Sesion\_Telnet.txt - Ethereal**

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x...
2	0.554002	10.0.0.3	10.0.0.89	TCP	3015 > telnet [SYN] seq=2806901859 Ack=0 win=16384 Len=0
3	0.554292	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [SYN, ACK] seq=4274588605 Ack=2806901860 win=...
4	0.554509	10.0.0.3	10.0.0.89	TCP	3015 > telnet [ACK] seq=2806901860 Ack=4274588606 win=175...
5	0.575343	10.0.0.89	10.0.0.3	TELNET	Telnet Data ...
6	0.575770	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
7	0.576192	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588618 Ack=2806901866 win=584...
8	0.576379	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
9	0.576585	10.0.0.89	10.0.0.3	TELNET	Telnet Data ...
10	0.608015	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588621 Ack=2806901875 win=584...
11	0.608194	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
12	0.608561	10.0.0.89	10.0.0.3	TELNET	Telnet Data ...
13	0.608790	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
14	0.648025	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588633 Ack=2806901890 win=584...
15	0.648317	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
16	0.648677	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588633 Ack=2806901890 win=584...

**Frame 1 (60 on wire, 60 captured)**

- IEEE 802.3 Ethernet
- Logical-Link Control
  - DSAP: Spanning Tree BPDU (0x42)
  - IG Bit: Individual
  - SSAP: Spanning Tree BPDU (0x42)
  - CR Bit: Command
- Control field: U, func = UT (0x03)
- Spanning tree Protocol

**Packet Bytes:**

```

0000  01 80 c2 00 00 00 08 00 46 2f e2 b8 00 26 42 42  ....F/...800
0010  03 00 00 00 00 00 80 00 0a 00 46 2f e2 b8 00 00  ...F/....
0020  00 00 80 00 0a 00 46 2f e2 b8 80 00 00 00 08 00  ....F/.....
0030  02 00 05 00 20 20 20 20 20 20 20 20  ....
  
```

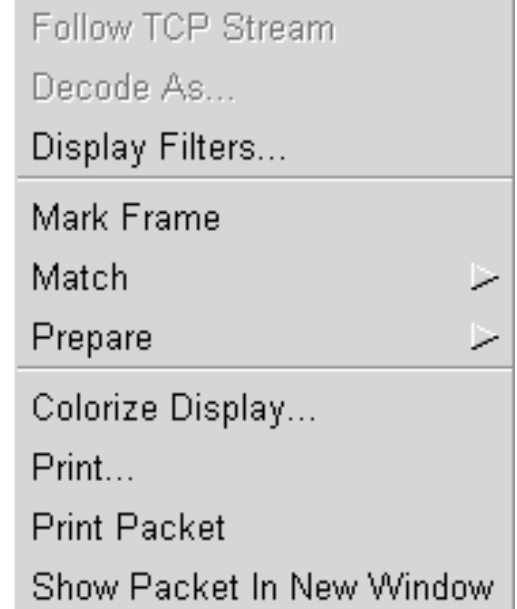
Filter: [ ] Reset Apply File: Sesión\_Telnet.txt

97% 3:41 PM

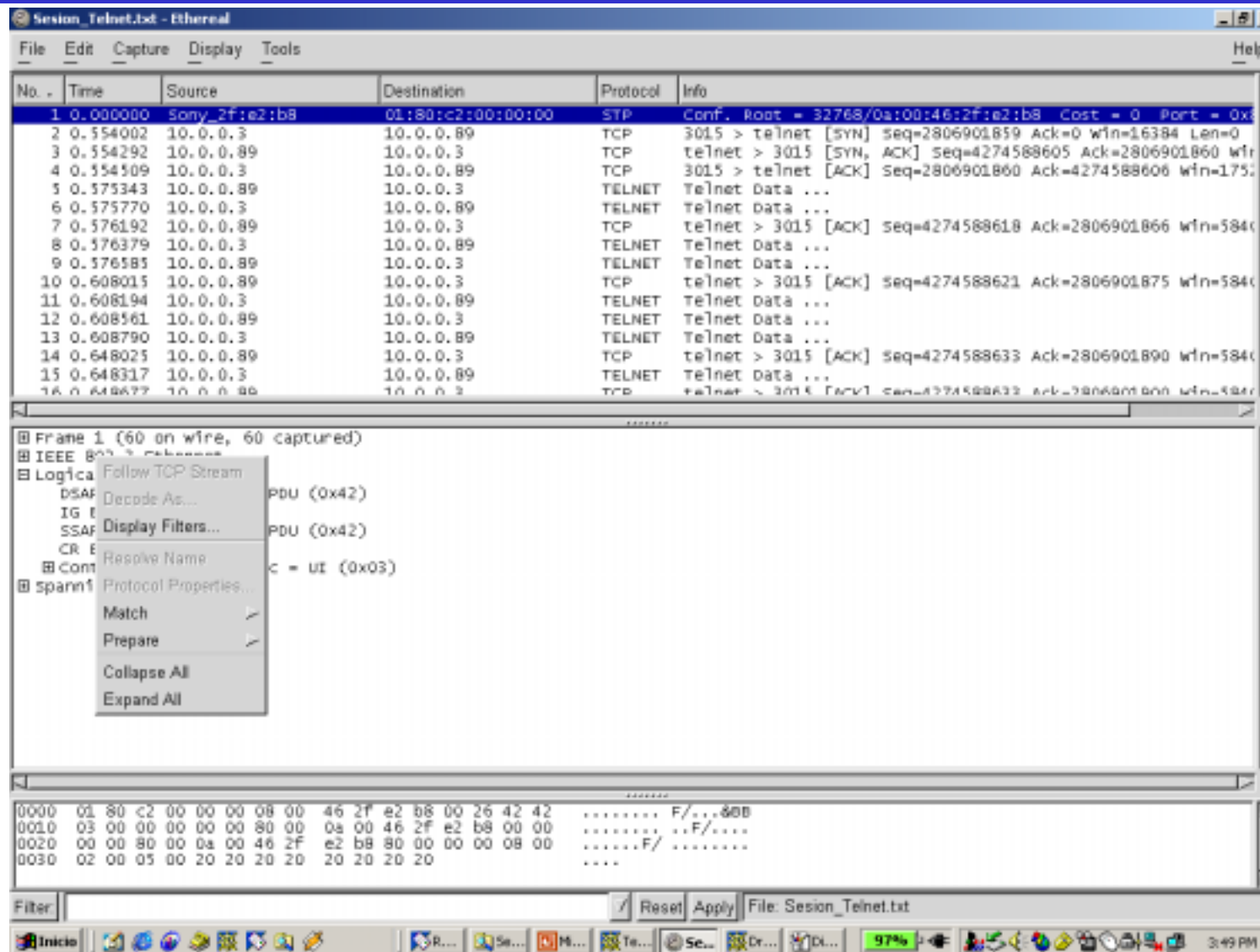
# Opciones menú Packet Pane pop-up



- **Follow** ver todos los datos de un stream TCP entre un par de nodos
- **Decode** mismo que el de menú de Display
- **Display** especificar y manipular filtros
- **Colorize** colorear paquetes
- **Print** imprimir paquetes
- **Print** imprimir paquete seleccionado
- **Show** desplegar el paquete seleccionado en otra ventana



# Menú del árbol de tres vistas

Sesion\_Telnet.txt - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x...
2	0.554002	10.0.0.3	10.0.0.89	TCP	3015 > telnet [SYN] seq=2806901859 Ack=0 win=16384 Len=0
3	0.554292	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [SYN, ACK] seq=4274588605 Ack=2806901860 win=...
4	0.554509	10.0.0.3	10.0.0.89	TCP	3015 > telnet [ACK] seq=2806901860 Ack=4274588606 win=175...
5	0.575343	10.0.0.89	10.0.0.3	TELNET	Telnet Data ...
6	0.575770	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
7	0.576192	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588618 Ack=2806901866 win=584...
8	0.576379	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
9	0.576585	10.0.0.89	10.0.0.3	TELNET	Telnet Data ...
10	0.608015	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588621 Ack=2806901875 win=584...
11	0.608194	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
12	0.608561	10.0.0.89	10.0.0.3	TELNET	Telnet Data ...
13	0.608790	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
14	0.648025	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588633 Ack=2806901890 win=584...
15	0.648317	10.0.0.3	10.0.0.89	TELNET	Telnet Data ...
16	0.648677	10.0.0.89	10.0.0.3	TCP	telnet > 3015 [ACK] seq=4274588633 Ack=2806901890 win=584...

Frame 1 (60 on wire, 60 captured)

- IEEE 802.3 Ethernet II
- Logical: Follow TCP Stream
  - DSAP: PDU (0x42)
  - IGMP: Decode As...
  - SSAP: PDU (0x42)
  - CR: Resolve Name
  - Com: c = ut (0x03)
  - spann: Protocol Properties...
- Match ☒
- Prepare ☒
- Collapse All
- Expand All

0000 01 80 c2 00 00 00 08 00 46 2f e2 b8 00 26 42 42 ..... F/...80B

0010 03 00 00 00 00 00 80 00 0a 00 46 2f e2 b8 00 00 .....F/....

0020 00 00 80 00 0a 00 46 2f e2 b8 80 00 00 08 00 .....F/.....

0030 02 00 05 00 20 20 20 20 20 20 20 20 ..... ....

Filter: / Reset Apply File: Sesion\_Telnet.txt

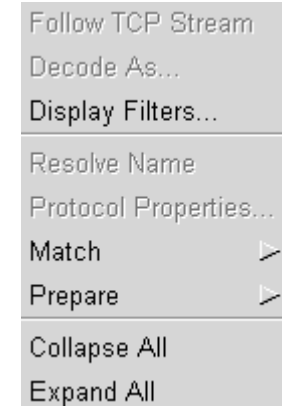
Inicio R... Se... M... Te... Se... Dr... 97% 3:49 PM



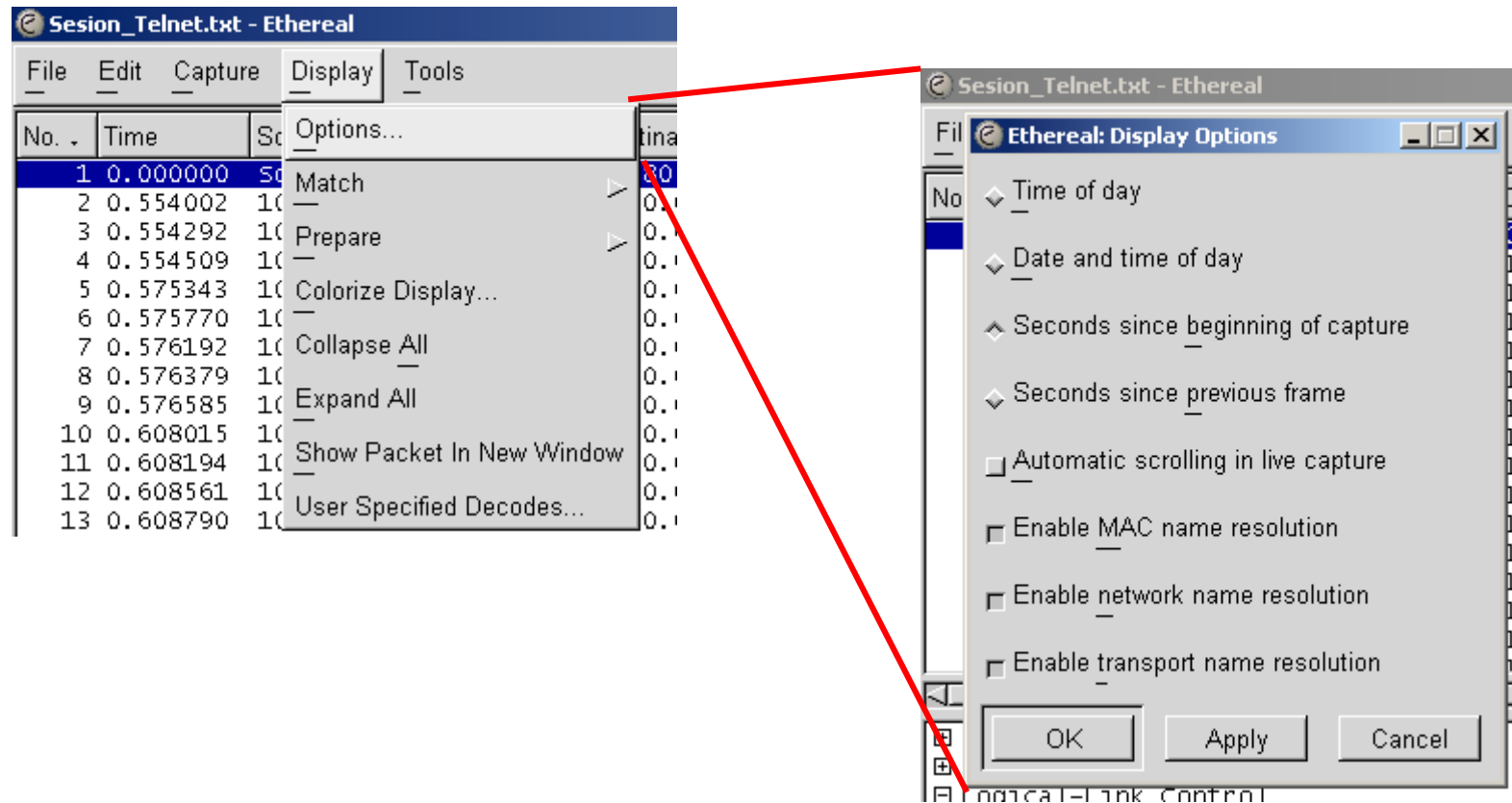
# Opciones menú



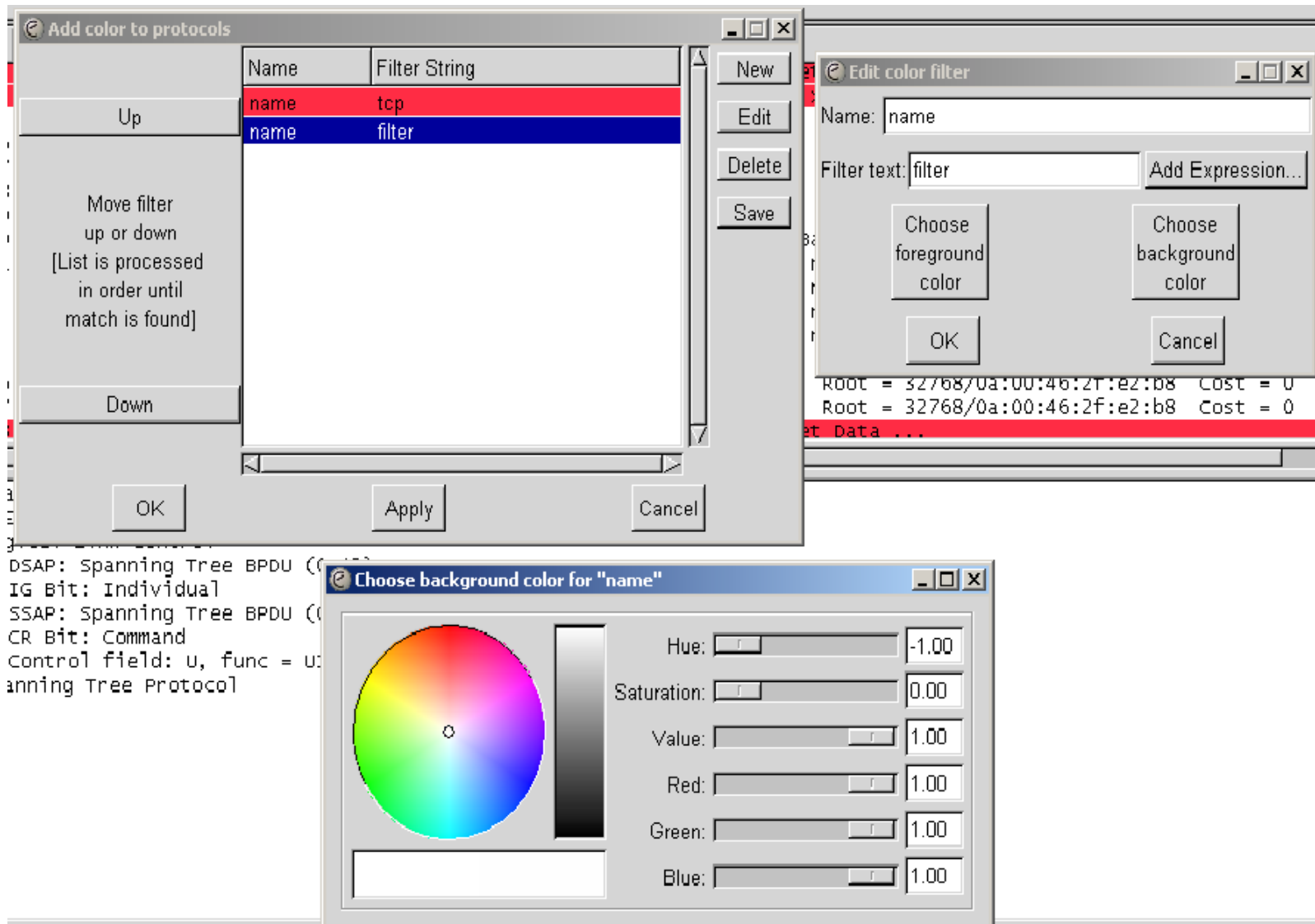
- Follow
- Decode
- Display
- Resolve Name
- Protocol Properties
- Match Selected
- Collapse All
- Expand All



# Opciones despliegue



# Coloreando paquetes

The image displays three overlapping windows from a network analysis tool:

- Add color to protocols:** A window with a table listing filters. The 'name' filter is highlighted in red.
 

	Name	Filter String
Up	name	tcp
	name	filter

 Controls include 'Up', 'Down', 'Move filter up or down [List is processed in order until match is found]', 'OK', 'Apply', and 'Cancel'.
- Edit color filter:** A window for editing the 'name' filter. It shows 'Filter text: filter' and buttons for 'Choose foreground color' and 'Choose background color'. 'OK' and 'Cancel' buttons are at the bottom.
- Choose background color for "name":** A color selection dialog featuring a color wheel, a vertical grayscale bar, and sliders for Hue, Saturation, Value, Red, Green, and Blue. The Value slider is set to 1.00.

Background text from the packet list is visible:

```

DSAP: Spanning Tree BPDU (0x00000000)
IG Bit: Individual
SSAP: Spanning Tree BPDU (0x00000000)
CR Bit: Command
Control field: u, func = 0x00000000
Spanning Tree Protocol
  
```

# Ejemplo: tcp colo rojo



Sesion\_Telnet.txt - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
43	5.588436	10.0.0.89	10.0.0.3	TELNET	Telnet data ...
44	5.788458	10.0.0.3	10.0.0.89	TCP	3015 > telnet [ACK] seq=2806901923 Ack=4274588738 win=173
45	6.008742	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
46	8.011655	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
47	10.014570	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
48	12.017486	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
49	14.020395	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
50	15.354595	10.0.0.3	10.255.255.255	BROWSER	GET Backup List Request
51	15.382422	0.0a00462fe2b8	0.ffffffffffffff	NBIPX	Find name MSHOME <ld>
52	15.382648	0.0800462fe2b8	0.ffffffffffffff	NBIPX	Find name MSHOME <ld>
53	15.442307	0.0a00462fe2b8	0.ffffffffffffff	NBIPX	Find name ZERO_CEM <00>
54	15.442729	0.0800462fe2b8	0.ffffffffffffff	NBIPX	Find name ZERO_CEM <00>
55	16.023314	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
56	18.026228	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
57	20.029141	Sony_2f:e2:b8	01:80:c2:00:00:00	STP	Conf. Root = 32768/0a:00:46:2f:e2:b8 Cost = 0 Port = 0x1
58	21.515786	10.0.0.3	10.0.0.89	TELNET	Telnet data ...

Frame 1 (60 on wire, 60 captured)

- IEEE 802.3 Ethernet
- Logical-Link Control
  - DSAP: spanning tree BPDU (0x42)
  - IG Bit: Individual
  - SSAP: Spanning Tree BPDU (0x42)
  - CR Bit: Command
  - Control field: U, func = UI (0x03)
- Spanning Tree Protocol

```

0000 01 80 c2 00 00 00 08 00 46 2f e2 b8 00 26 42 42 ..... F/...&B
0010 03 00 00 00 00 00 80 00 0a 00 46 2f e2 b8 00 00 ..... F/...
0020 00 00 80 00 0a 00 46 2f e2 b8 80 00 00 00 08 00 ..... F/ .....
0030 02 00 05 00 20 20 20 20 20 20 20 20 .....
  
```

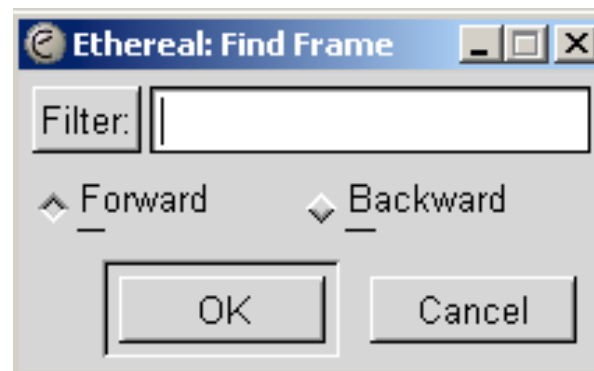
Filter: / Reset Apply File: Sesion\_Telnet.txt

97% 3:55 PM

# Busqueda de frames



- Seleccionar Find Frame del menú Edit





- Seleccionar el stream en el panel de tres vistas de árbol
- Tres formatos
  - ASCII
    - datos de cada lado en ASCII, pero alternados
    - caracteres no imprimibles no se despliegan
  - EBCDIC
    - for the big-iron freaks out there
  - HEX Dump
    - ver todos los datos, pero no se ve en ASCII