



Ethereal – Analysis on a Budget

Laura Chappell
Protocol Analysis Institute, Inc.
lchappell@packet-level.com
www.packet-level.com
www.podbooks.com

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



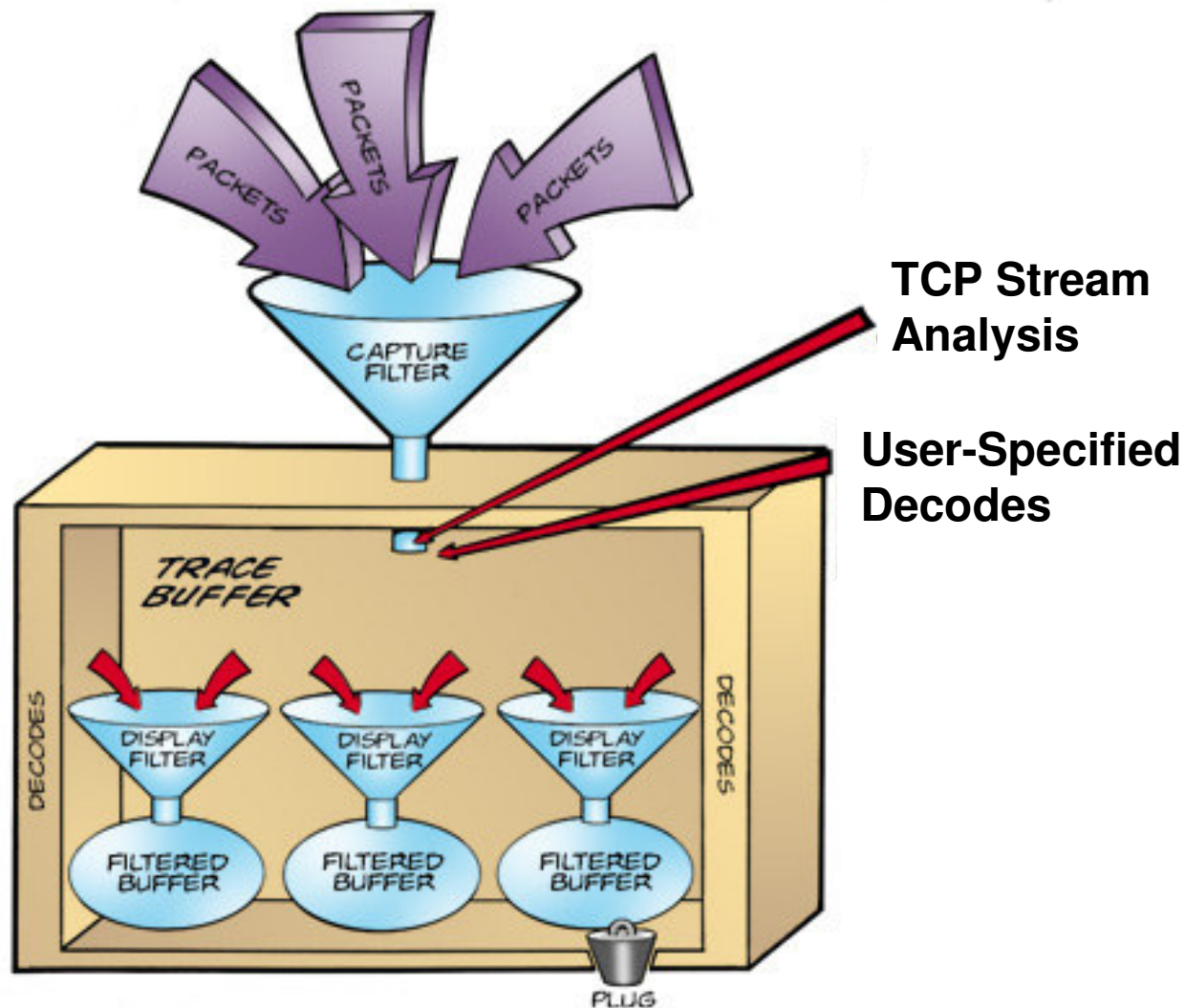
Course Contents



*“Sniffing the
glue that holds
the Internet
together”*

- What is Ethereal?
- Placing Ethereal on the Network
- Loading Ethereal
- Working with Trace Files
- Capturing Packets
- Following TCP Streams
- Protocol Statistics
- Building and Applying Filters
- Changing Display Options
- Changing Preferences

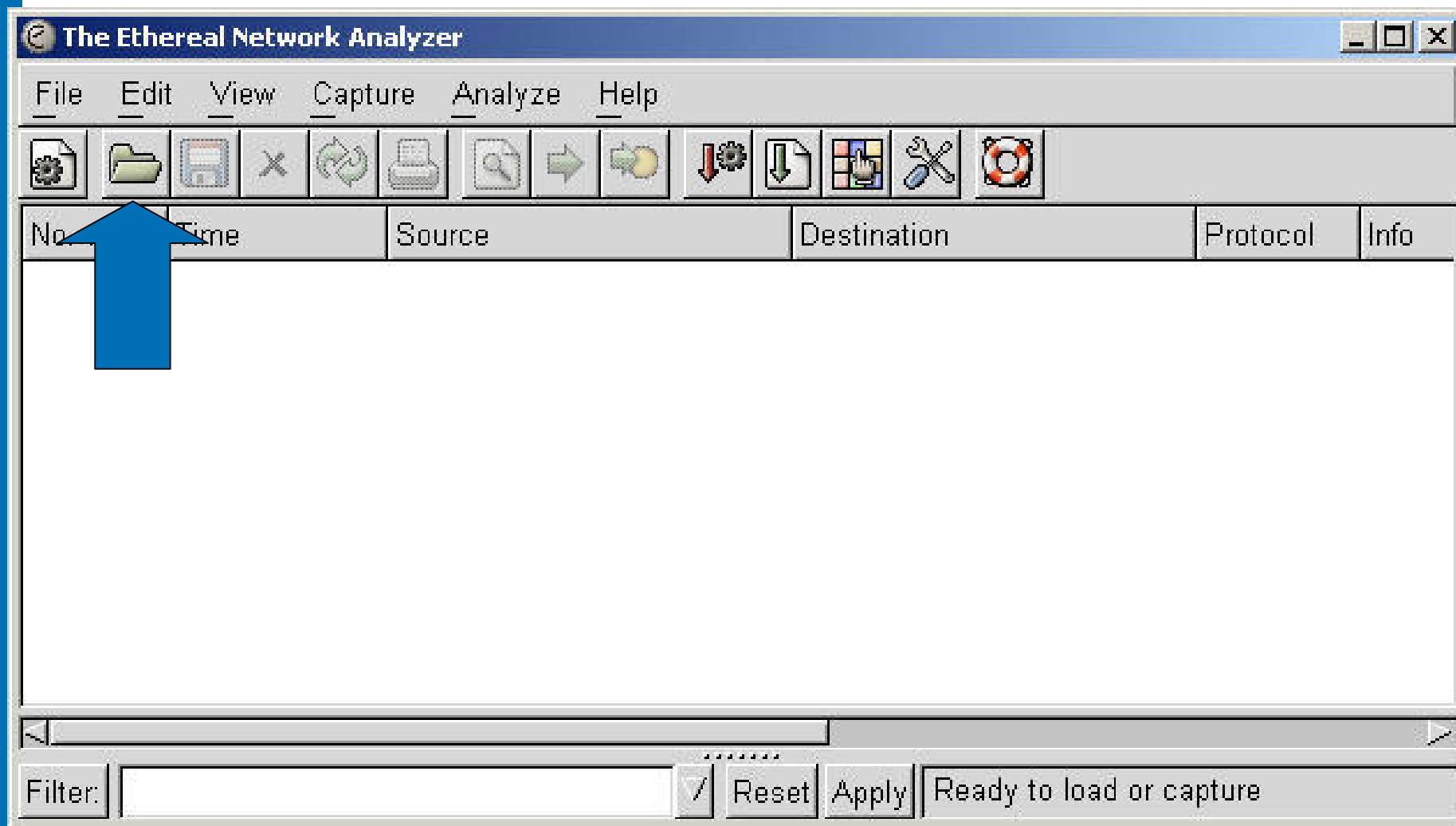
Ethereal Analyzer Elements

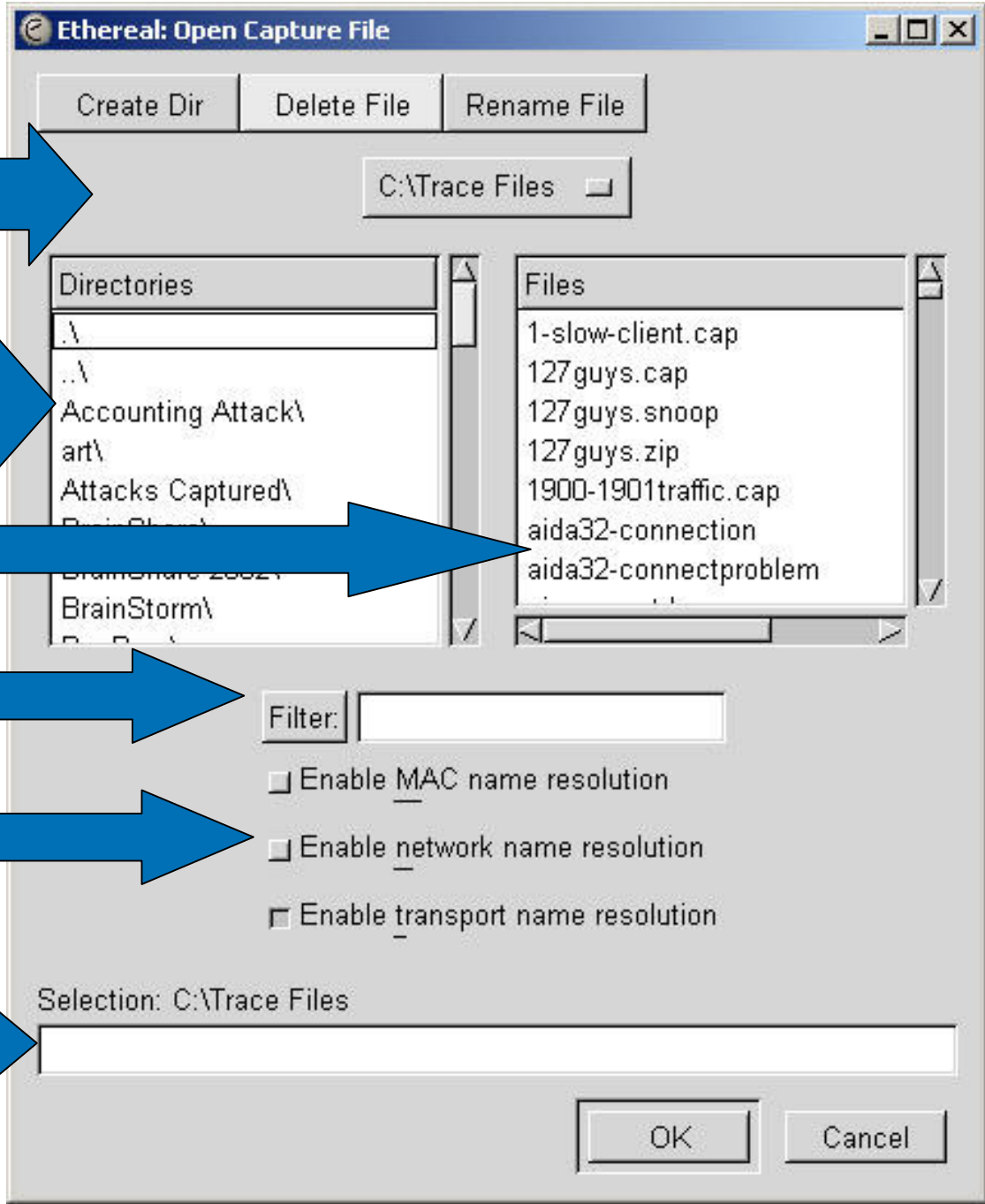


Loading Ethereal

- Binary distributions and ready-to-compile source code available online at www.ethereal.com.
- For Windows, two components are needed:
 - Windows Packet Capture driver (*WinPcap*)
 - Ethereal binary

Opening Trace Files





default directory

navigate drives and directories

select file

apply read/display filter

apply name resolution

enter trace file name

Opening Trace Files (w/o filter)

pkt # source (add+name) destination (add+name) protocol summary info

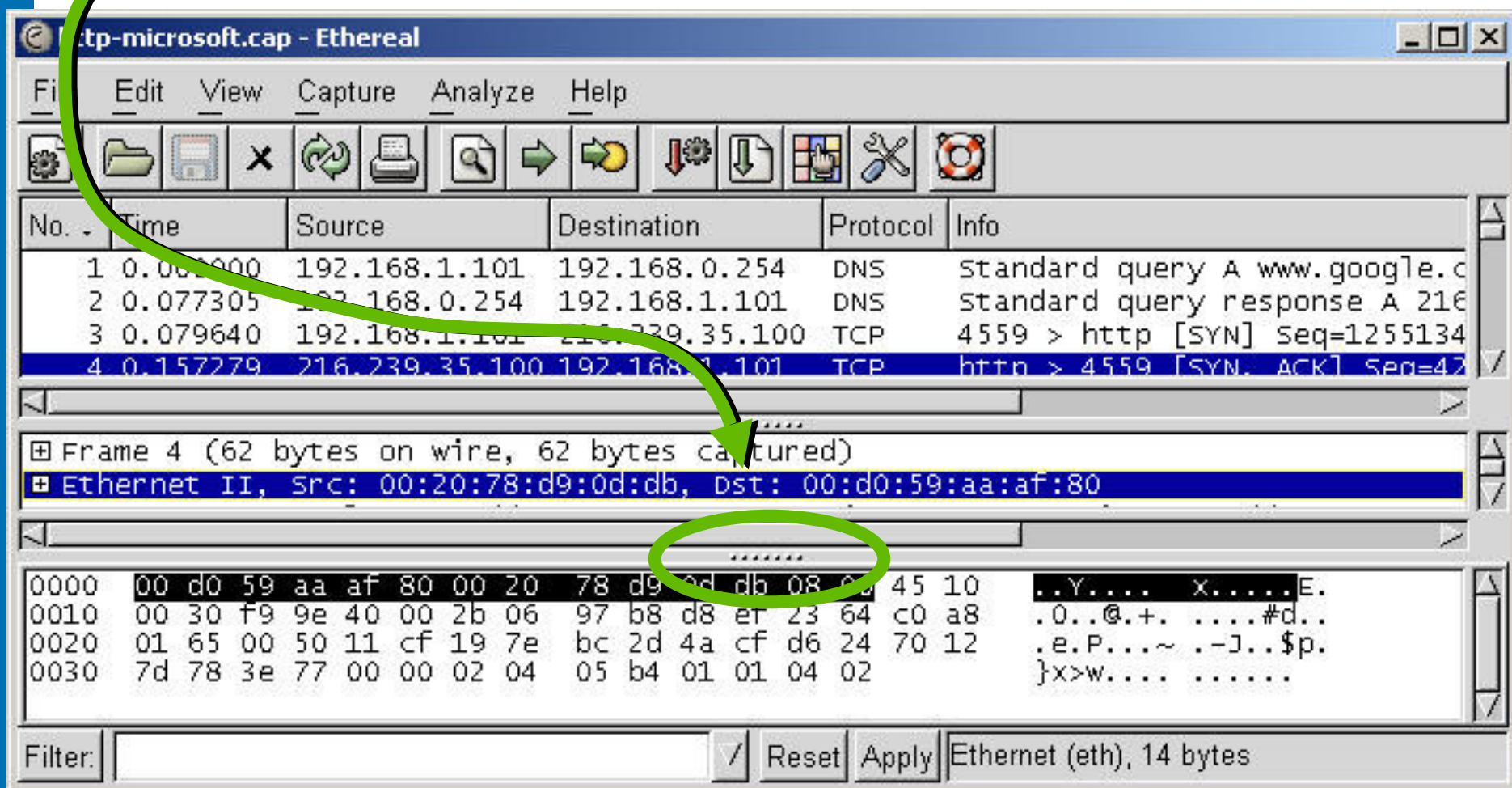
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.101	192.168.0.254	DNS	standard query A www.google.c
2	0.077305	192.168.0.254	192.168.1.101	DNS	standard query response A 216
3	0.079640	192.168.1.101	216.239.35.100	TCP	4559 > http [SYN] Seq=1255134
4	0.157279	216.239.35.100	192.168.1.101	TCP	http > 4559 [SYN, ACK] Seq=42
5	0.157383	192.168.1.101	216.239.35.100	TCP	4559 > http [ACK] Seq=1255134
6	0.157672	192.168.1.101	216.239.35.100	HTTP	GET / HTTP/1.1
7	0.214456	216.239.35.100	192.168.1.101	TCP	http > 4559 [ACK] Seq=4277361
8	0.214903	216.239.35.100	192.168.1.101	HTTP	HTTP/1.1 200 OK
9	0.414504	192.168.1.101	216.239.35.100	TCP	4559 > http [ACK] Seq=1255135
10	0.510260	216.239.35.100	192.168.1.101	HTTP	Continuation
		192.168.1.101	216.239.35.100	TCP	4559 > http [ACK] Seq=1255135
		16.239.35.100	192.168.1.101	TCP	http > 4559 [FIN, ACK] Seq=42
		192.168.1.101	216.239.35.100	TCP	4559 > http [ACK] Seq=1255135

**set to delta
In this trace**

Filter: / Reset Apply File: http-microsoft.cap

Opening Other Windows

Click and drag to open decode and hex windows



The screenshot shows the Wireshark interface with a packet capture of an HTTP SYN-ACK. The packet list shows four packets, with packet 4 selected. The packet details pane shows the Ethernet II protocol selected, with the source and destination MAC addresses highlighted. The hex dump pane shows the raw bytes of the packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.101	192.168.0.254	DNS	standard query A www.google.c
2	0.077305	192.168.0.254	192.168.1.101	DNS	standard query response A 216
3	0.079640	192.168.1.101	216.239.35.100	TCP	4559 > http [SYN] Seq=1255134
4	0.157279	216.239.35.100	192.168.1.101	TCP	http > 4559 [SYN, ACK] Seq=42

Frame 4 (62 bytes on wire, 62 bytes captured)

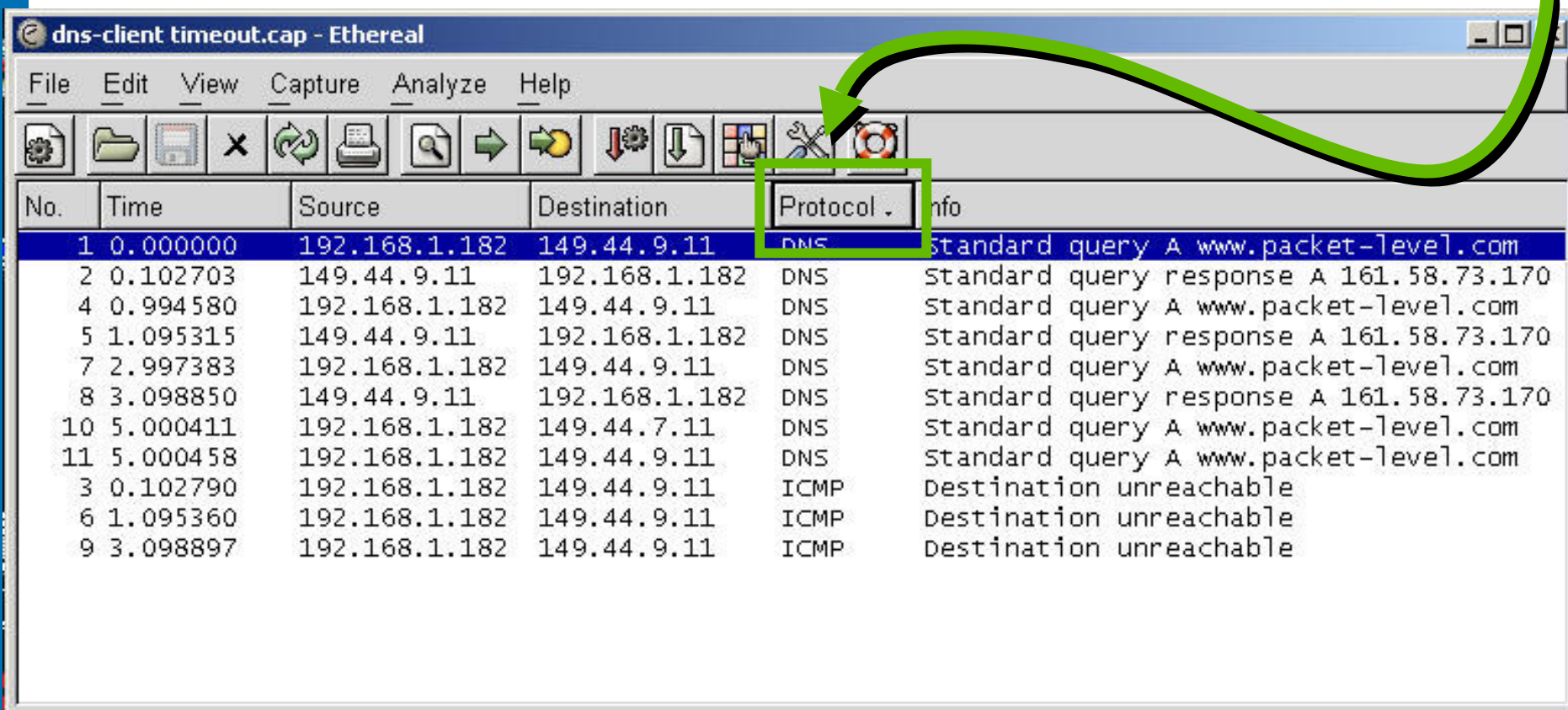
Ethernet II, Src: 00:20:78:d9:0d:db, Dst: 00:d0:59:aa:af:80

```
0000  00 d0 59 aa af 80 00 20 78 d9 0d db 08 00 45 10  ..Y.... x....E.
0010  00 30 f9 9e 40 00 2b 06 97 b8 d8 e1 23 64 c0 a8  .0..@.+ . . . .#d..
0020  01 65 00 50 11 cf 19 7e bc 2d 4a cf d6 24 70 12  .e.P...~ .-J..$p.
0030  7d 78 3e 77 00 00 02 04 05 b4 01 01 04 02     }x>w.... .....
```

Filter: / Reset Apply Ethernet (eth), 14 bytes

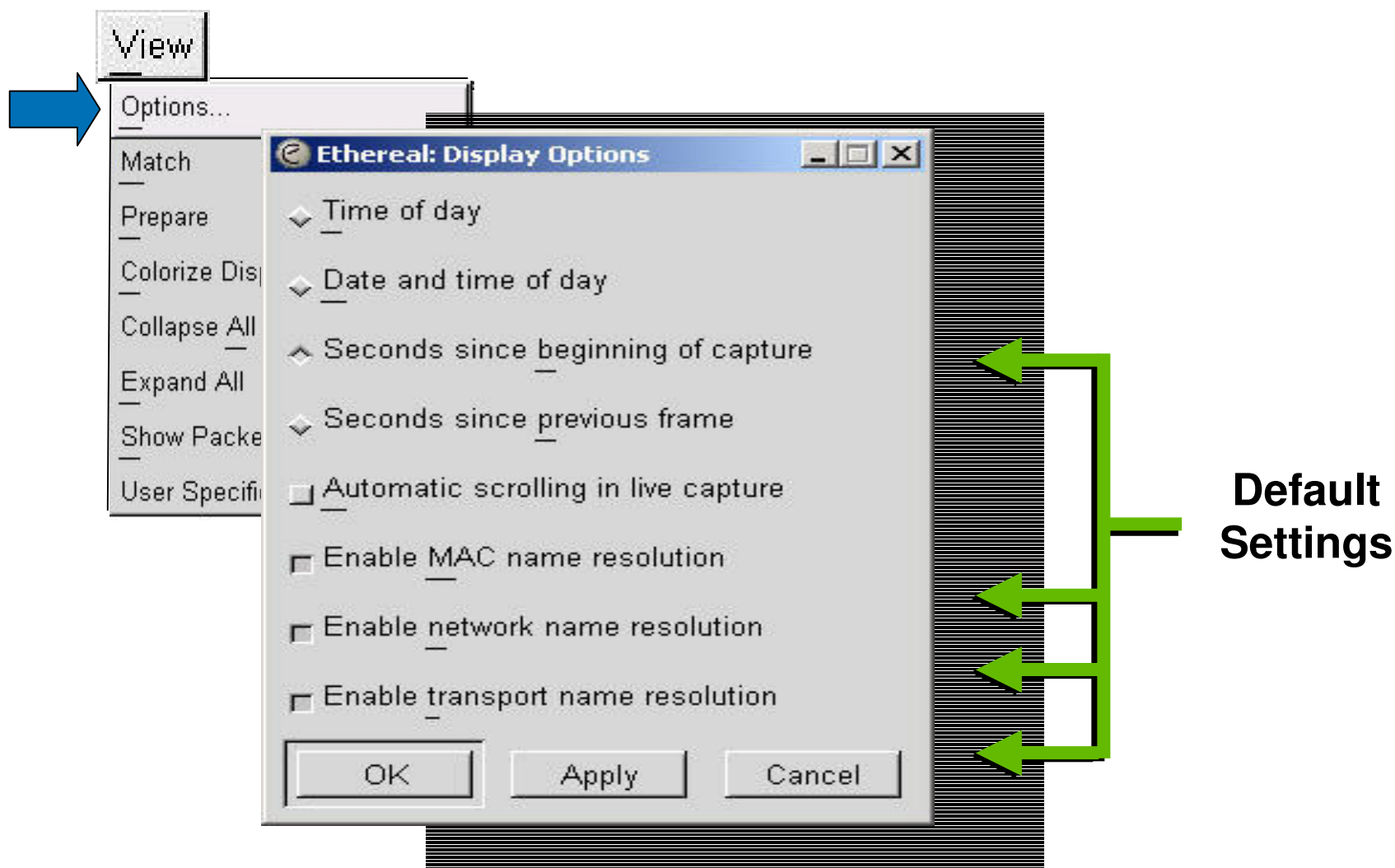
Sorting Trace Columns

Click on any column heading to sort (“No.”=default sort)

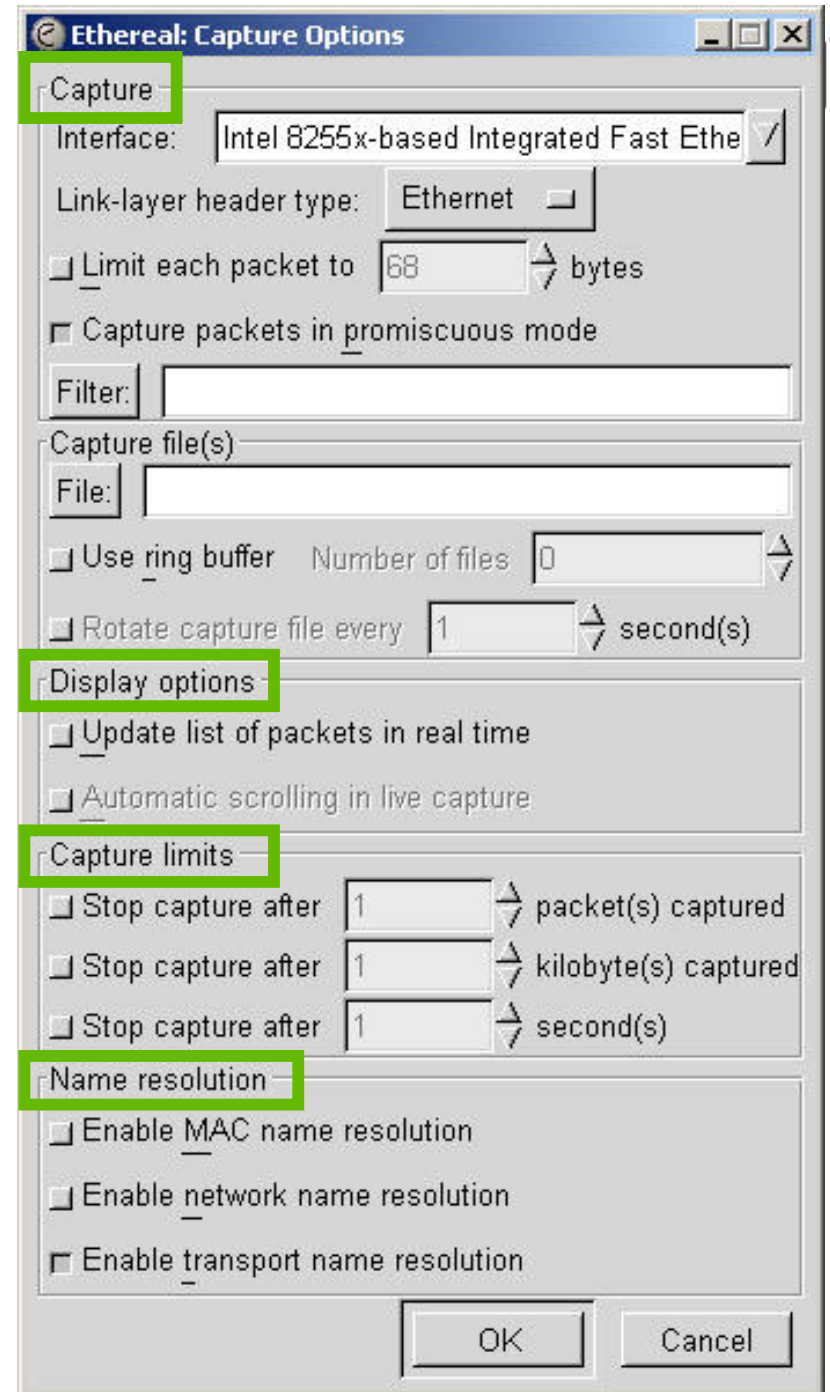
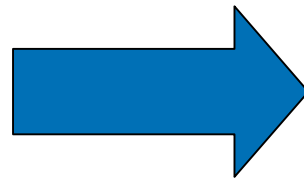


No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.182	149.44.9.11	DNS	Standard query A www.packet-level.com
2	0.102703	149.44.9.11	192.168.1.182	DNS	Standard query response A 161.58.73.170
4	0.994580	192.168.1.182	149.44.9.11	DNS	Standard query A www.packet-level.com
5	1.095315	149.44.9.11	192.168.1.182	DNS	Standard query response A 161.58.73.170
7	2.997383	192.168.1.182	149.44.9.11	DNS	Standard query A www.packet-level.com
8	3.098850	149.44.9.11	192.168.1.182	DNS	Standard query response A 161.58.73.170
10	5.000411	192.168.1.182	149.44.7.11	DNS	Standard query A www.packet-level.com
11	5.000458	192.168.1.182	149.44.9.11	DNS	Standard query A www.packet-level.com
3	0.102790	192.168.1.182	149.44.9.11	ICMP	Destination unreachable
6	1.095360	192.168.1.182	149.44.9.11	ICMP	Destination unreachable
9	3.098897	192.168.1.182	149.44.9.11	ICMP	Destination unreachable

Changing the Display



Capturing Packets



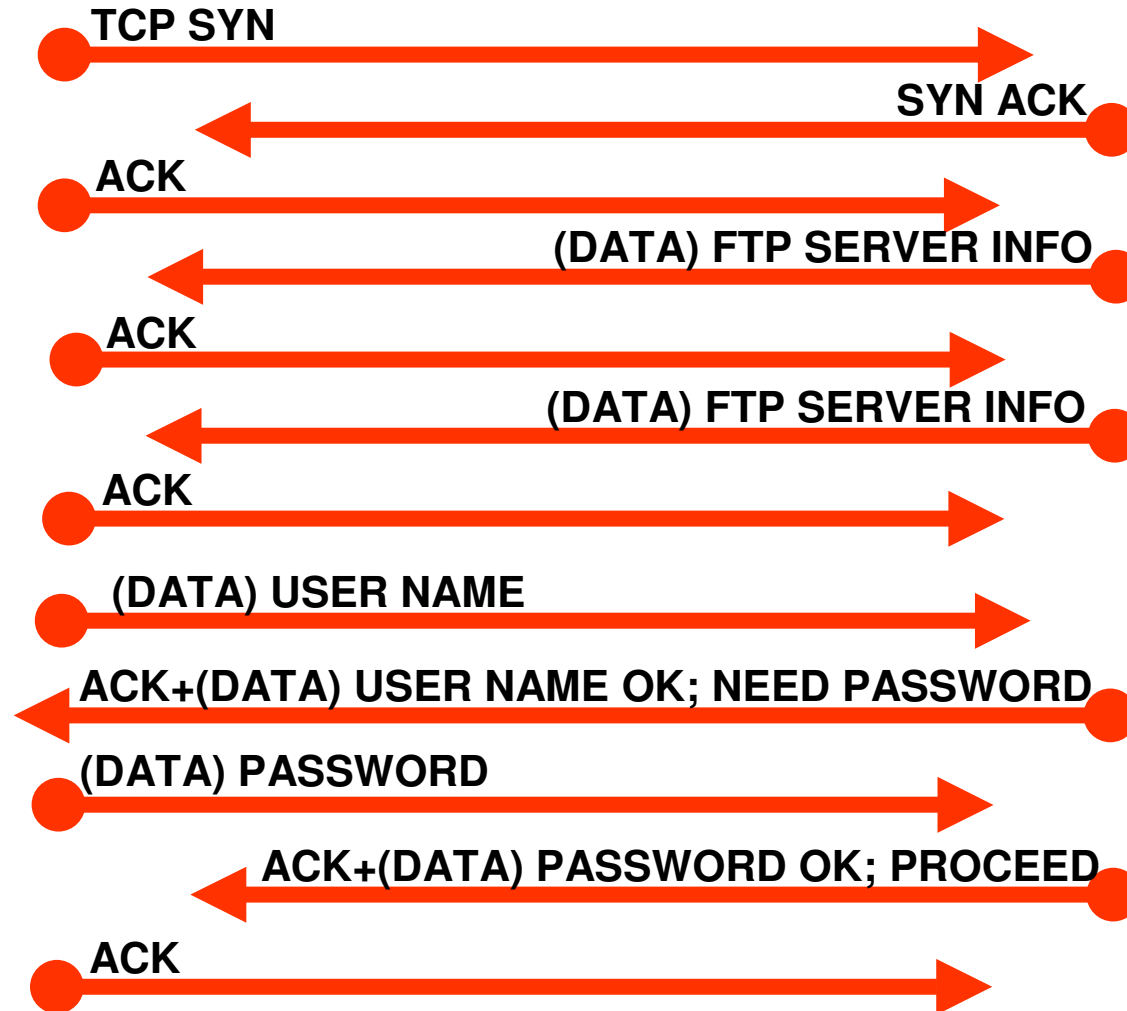
Following TCP Streams



Client



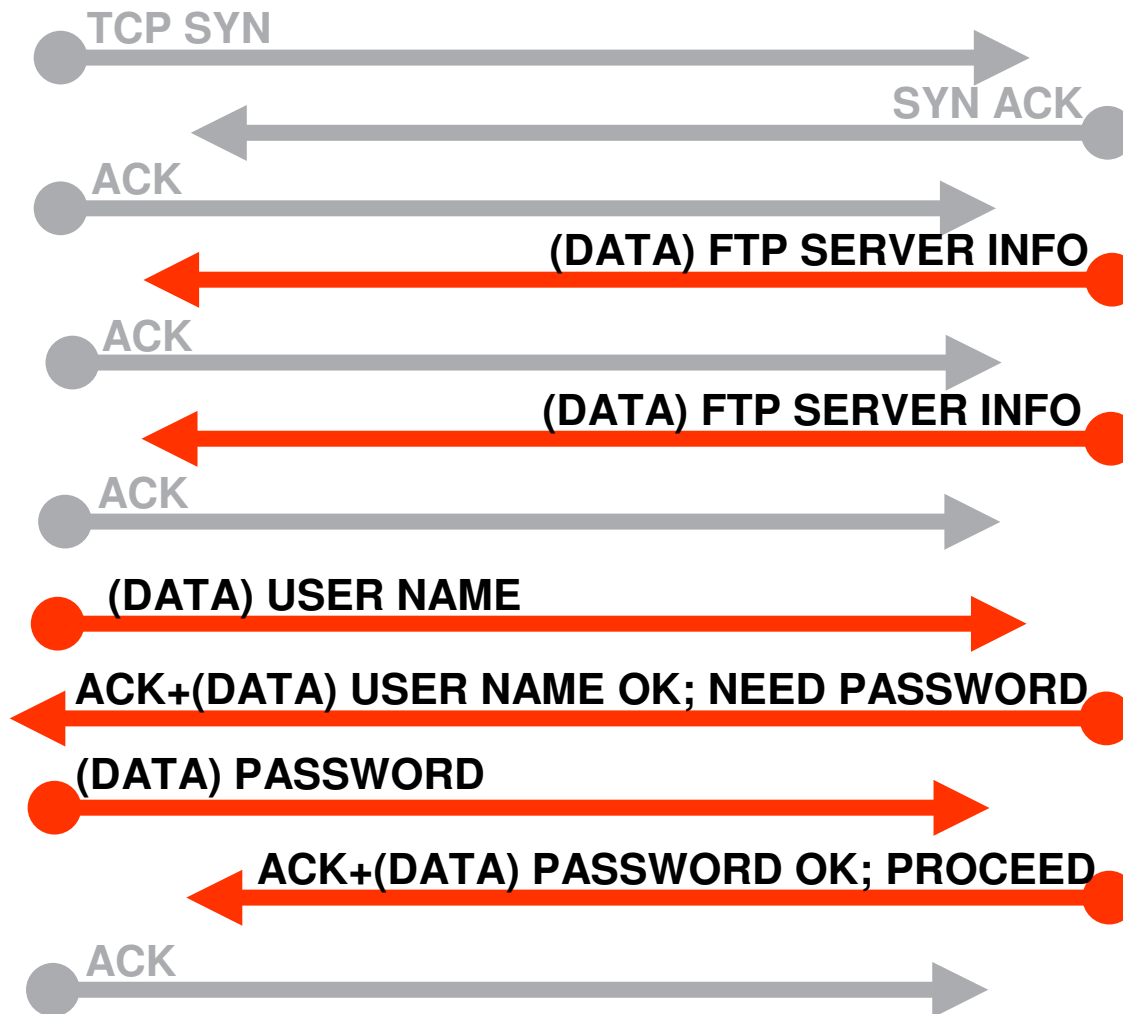
Server



Following TCP Streams



Client



Server

Following TCP Streams

Analyze

Display Filters...

Match

Prepare

Enabled Protocols...

Shift+Ctrl+R

Decode As...

User Specified Decodes

Follow TCP Stream

TCP Stream Analysis

Summary

Protocol Hierarchy Statistics

Statistics

Contents of TCP stream

```
tt's FTP Server []  
onware BisonFTP server product V3.5 []
```

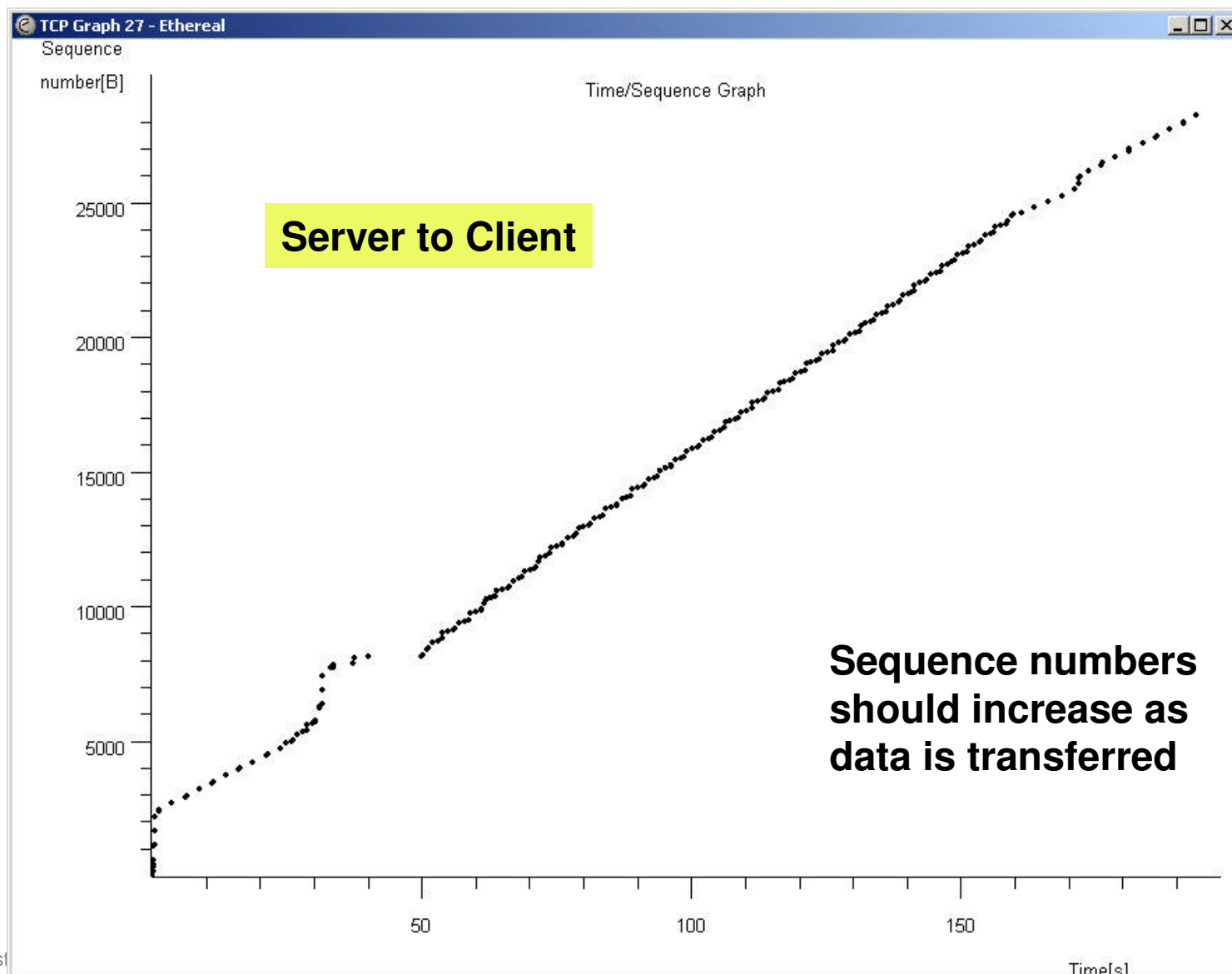
```
ed []  
r name OK - need password. []  
ueger []  
r logged in OK - Proceed []  
, 2, 0, 2, 4, 31 []  
T Command Accepted []
```

```
ectory List Follows []  
ting complete. []  
mes []
```

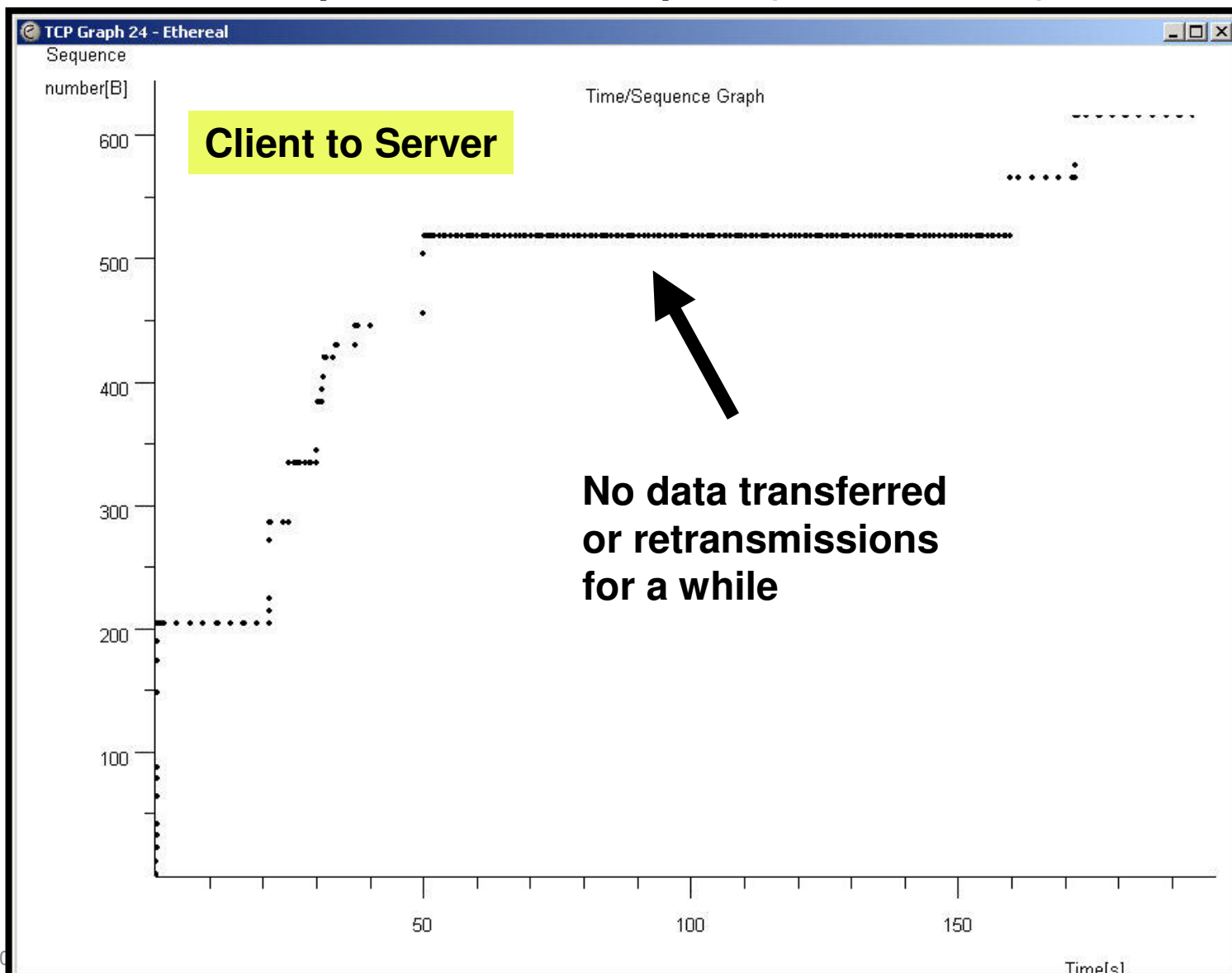
Time-Sequence Graph (Stevens)
Time-Sequence Graph (tcptrace)
Throughput Graph
RTT Graph

```
... changed to "/eGames/3dMazeman/" []  
PORT 10, 2, 0, 2, 4, 33 []  
200 PORT Command Accepted []  
NLST []  
150 directory list follows []
```

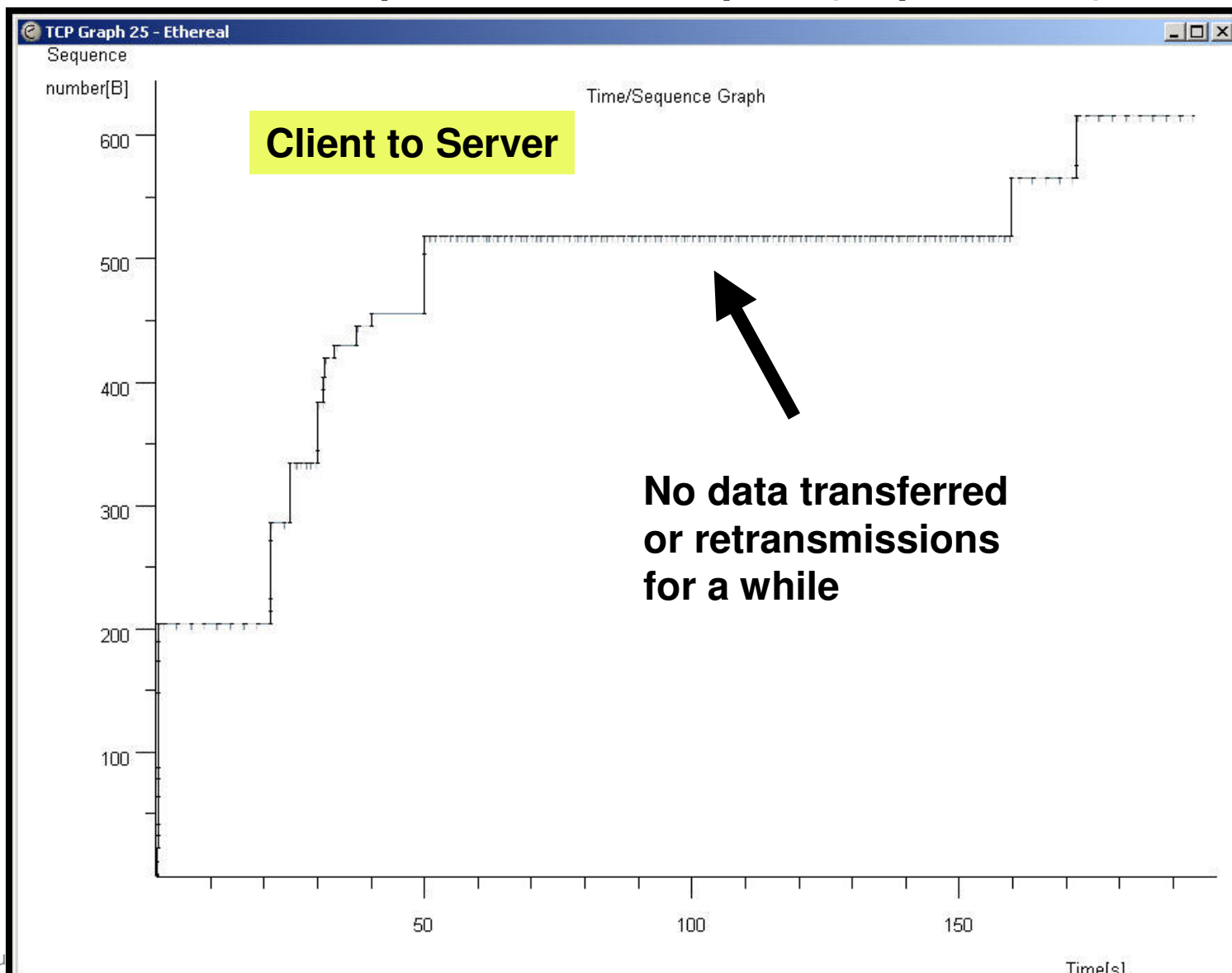
TCP Time-Sequence Graph (Stevens)



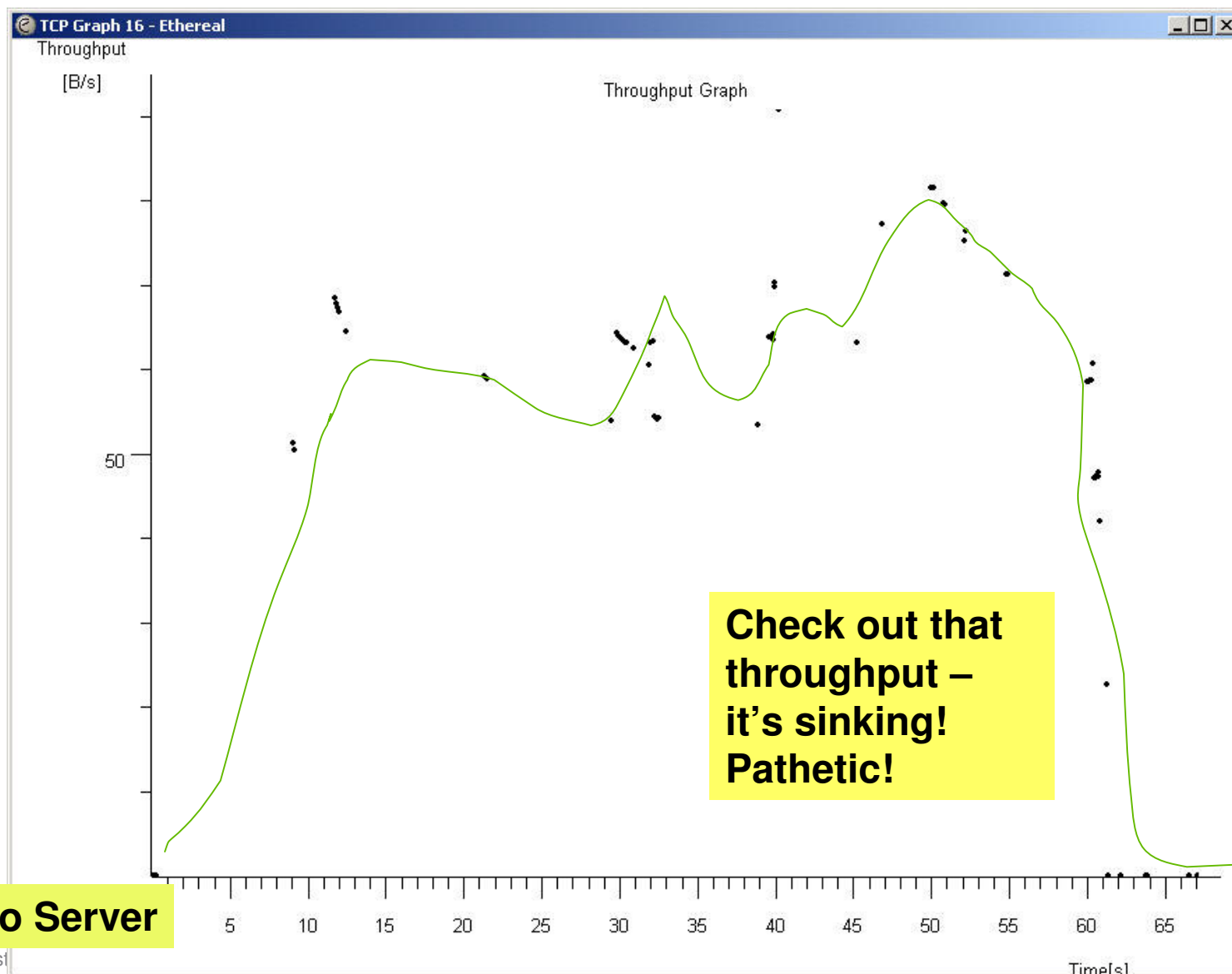
TCP Time-Sequence Graph (Stevens)



TCP Time-Sequence Graph (tcptrace)



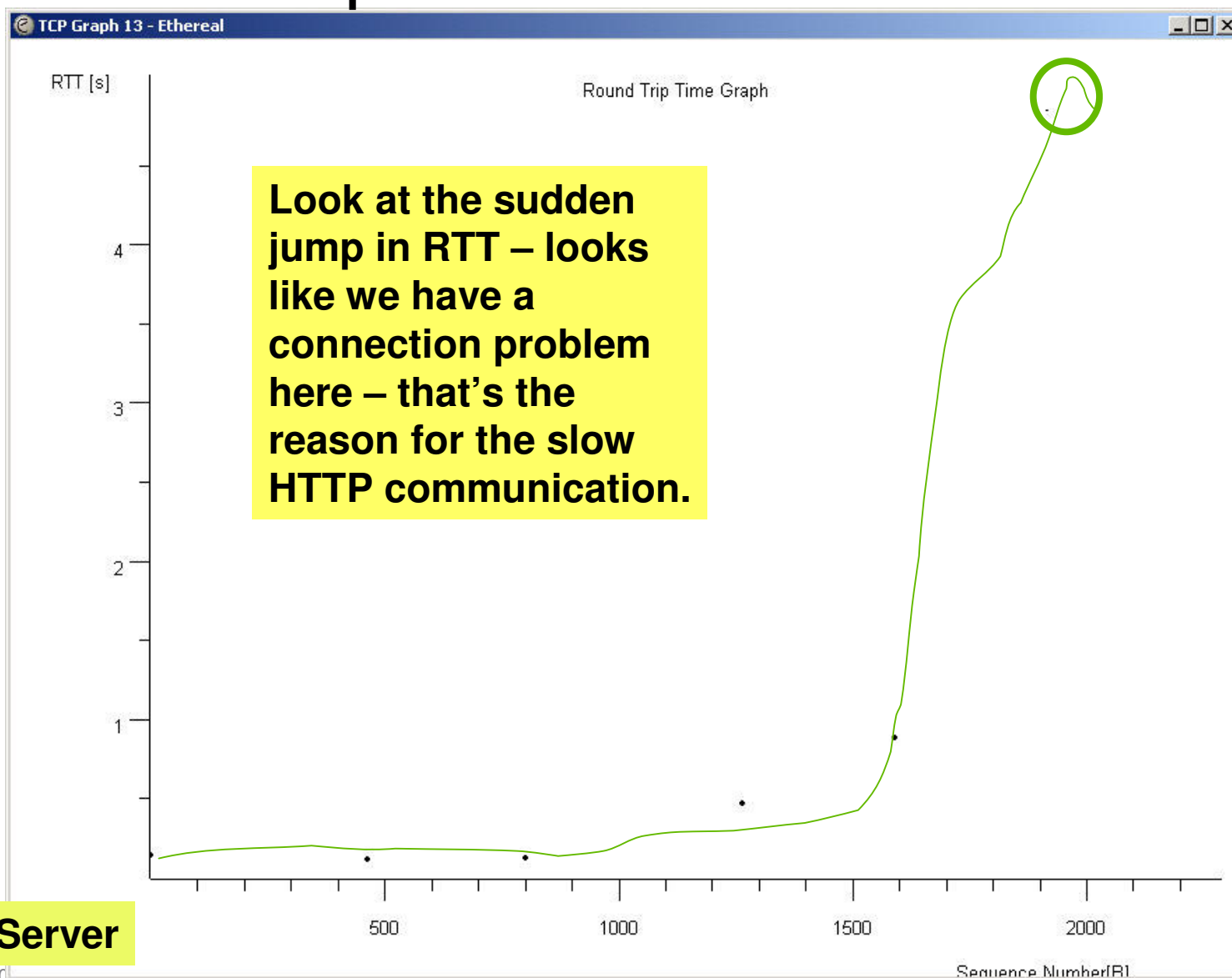
TCP Throughput Graph



Client to Server

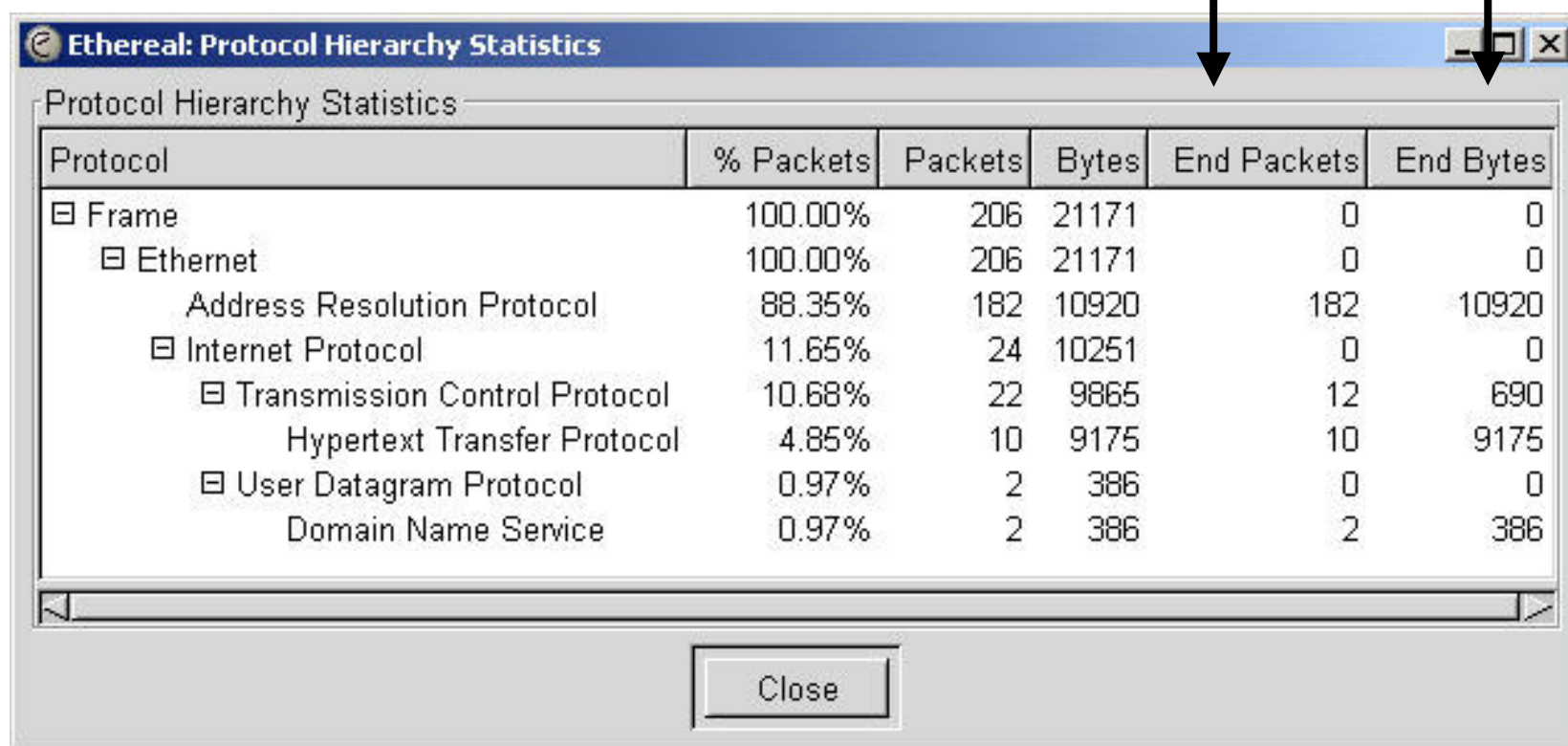
25 August

TCP RTT Graph



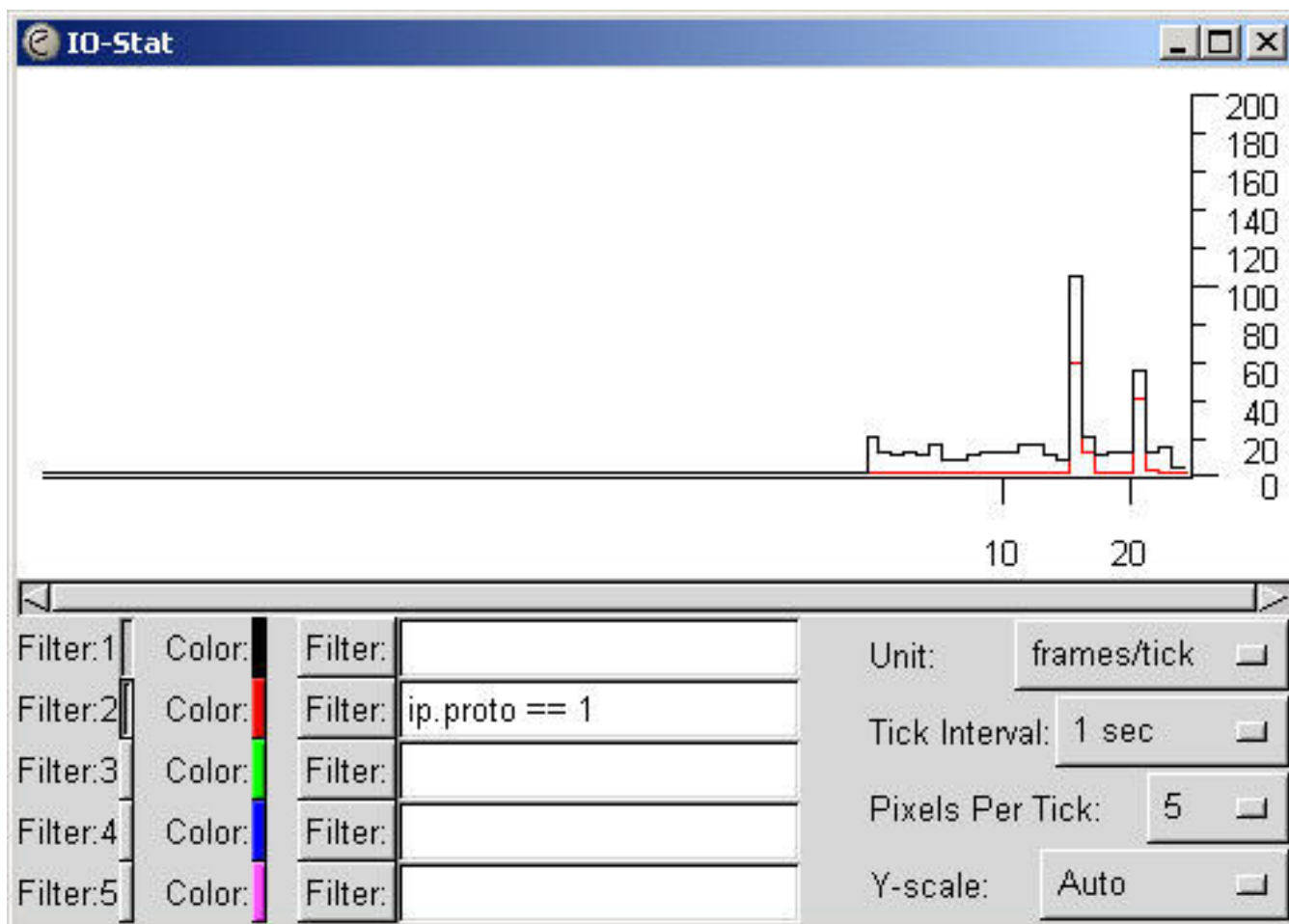
Protocol Statistics

Totals per Protocol



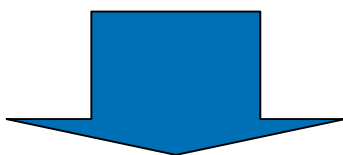
Protocol	% Packets	Packets	Bytes	End Packets	End Bytes
[-] Frame	100.00%	206	21171	0	0
[-] Ethernet	100.00%	206	21171	0	0
Address Resolution Protocol	88.35%	182	10920	182	10920
[-] Internet Protocol	11.65%	24	10251	0	0
[-] Transmission Control Protocol	10.68%	22	9865	12	690
Hypertext Transfer Protocol	4.85%	10	9175	10	9175
[-] User Datagram Protocol	0.97%	2	386	0	0
Domain Name Service	0.97%	2	386	2	386

Looking at IO Stats



Building and Applying Filters

Stored Filters



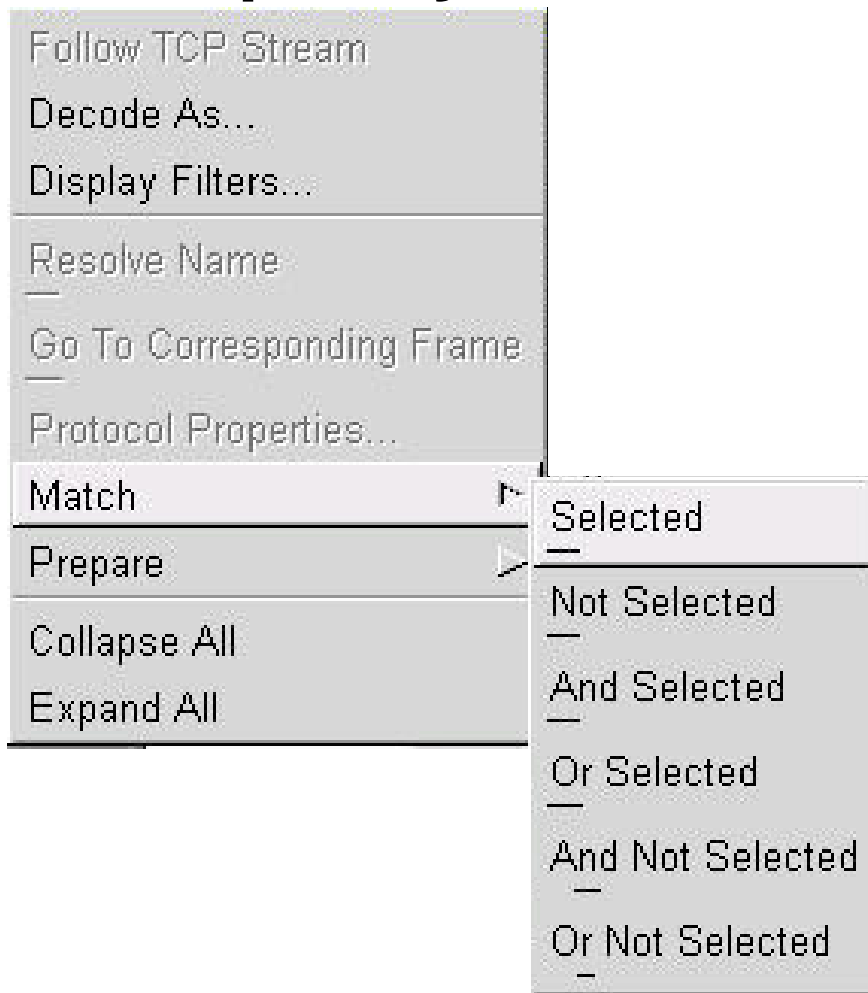
Capture Filters



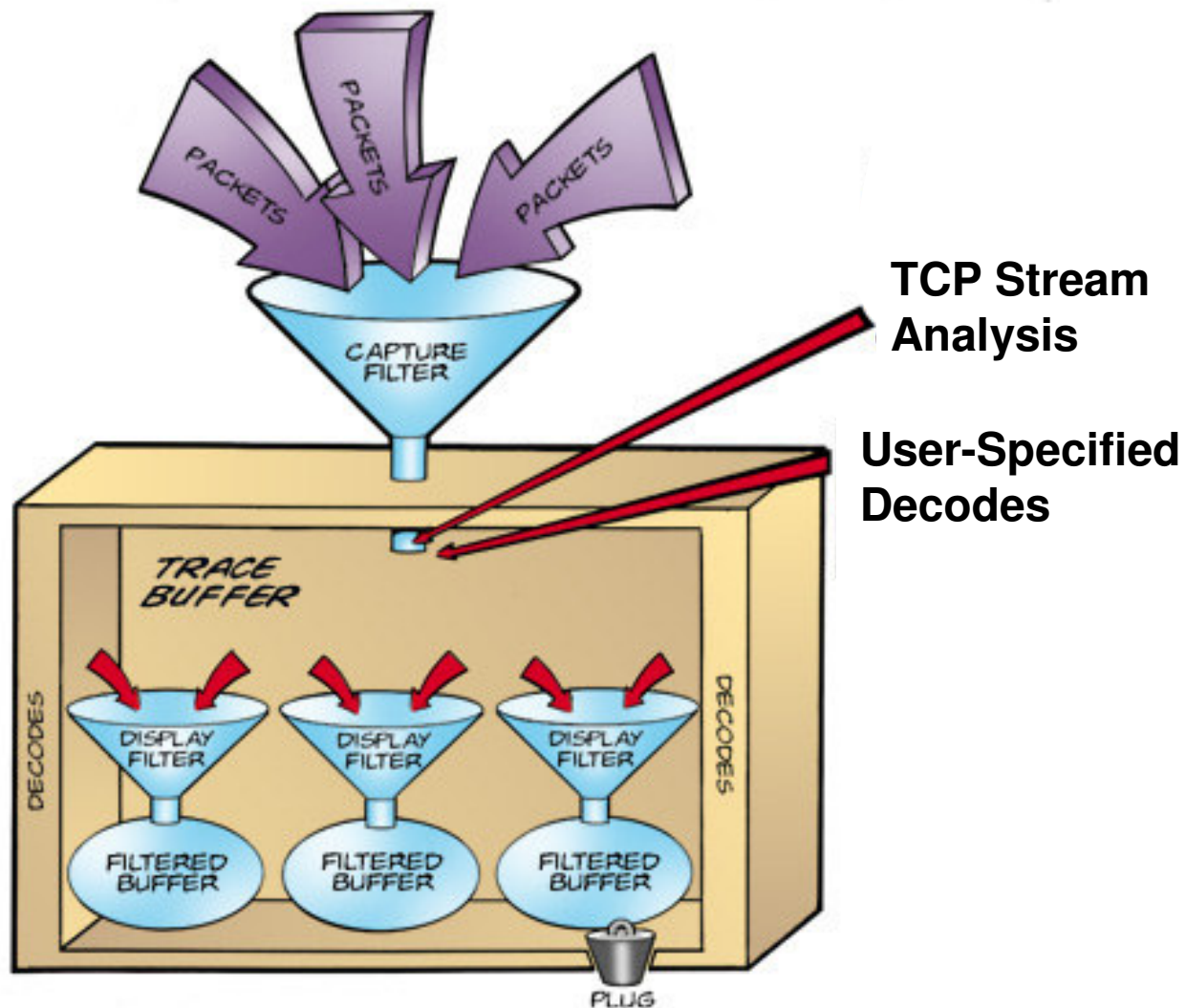
Display Filters



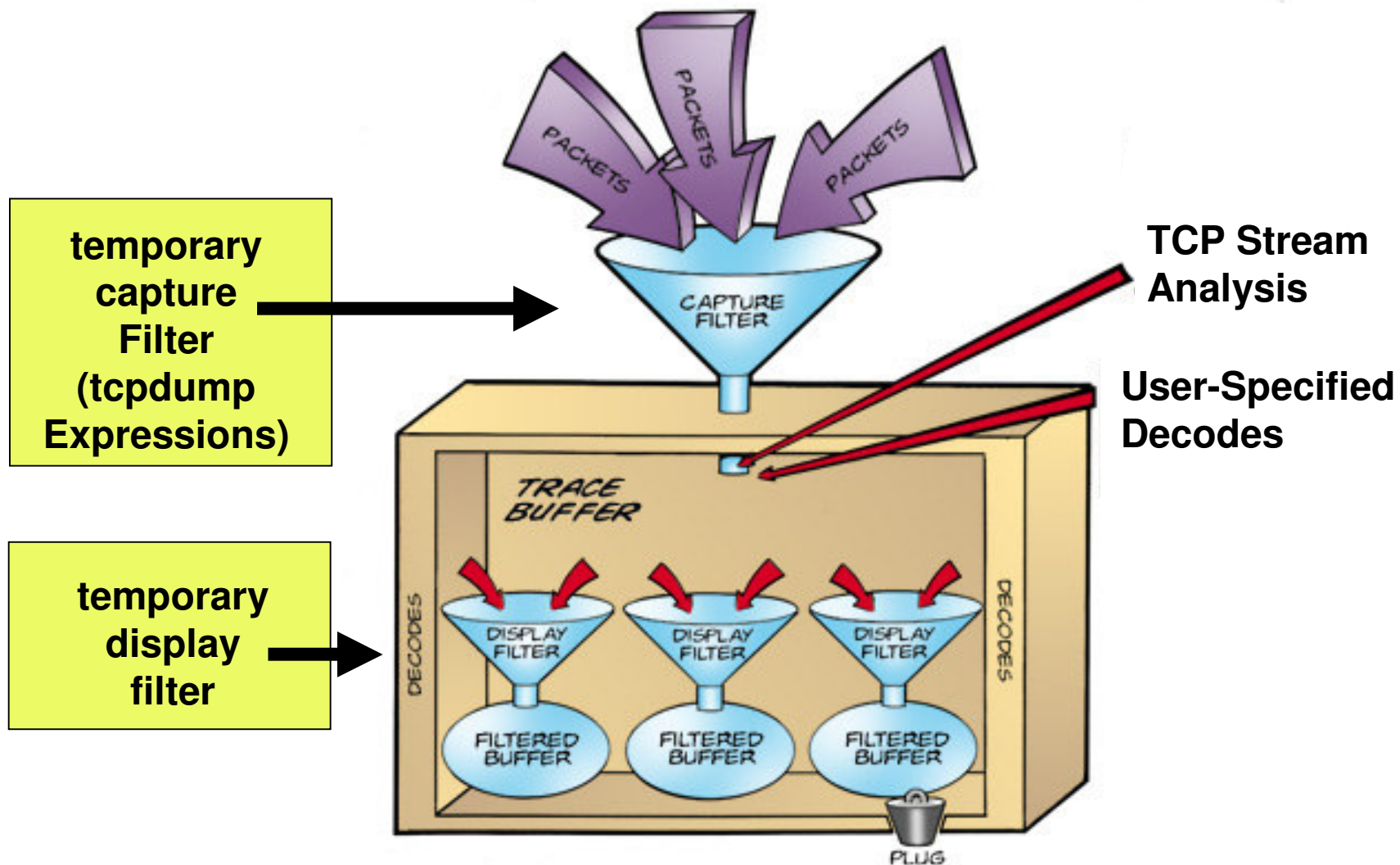
Temporary Filters



Where Filters are Applied



Where Filters are Applied



Capture Filter Expression Format

- Tcpdump expressions
 - host 10.2.2.3
 - dst host 10.5.5.5
 - ether host 00:D0:59:AA:AF:80
 - not ether src 00:D0:59:AA:AF:80
 - gateway host 10.1.1.1
 - net 12.234.0.0/16
 - tcp port 4444
 - udp port 53
 - ip proto 1
 - ip broadcast
 - ether multicast

Display Filter Expression Format

ID, operand, qualifier

1. eth.dst== ff:ff:ff:ff:ff:ff
2. eth.src== 00:d0:59:34:33:34
3. eth.type==0x0800
4. frame[0:14]== ff:ff:ff:ff:ff:ff:00:d0:59:34:33:34:08:00
5. arp.src.hw_mac==00:40:3a:30:02:22
6. ip.proto==0x01 (or 01, 1 works also)
7. udp.dstport==53
8. ip.src==10.4.3.2
9. ip.dst==255.255.255.255

Display Filter Expression Format

- NOT operand (!)
 - `!(eth.type==0x0800)` – not IP
 - `!(ip.proto==0x01)` - not ICMP
- AND operand (&&)
 - `(eth.type==0x0800) && (eth.src== 00:d0:59:34:33:34)`
 - `(ip.src==10.4.3.2) && (udp.dstport==53)`
- OR operand (||)
 - `(eth.type==0x0800) || (eth.type==0x0806)`
 - `(tcp.dstport==53) || (udp.dstport==53)`

Display Filter Expression Format

- AND NOT operand
 - `!(eth.type==0x0800) && !(udp.dstport==53)`
 - `!(ip.proto==0x01) && !(ip.src==10.4.3.2)`
- OR NOT operand
 - `(eth.type==0x0800) || !(eth.type==0x0806)`
 - `(tcp.dstport==53) || !(ip.src==10.4.3.2)`
- Other
 - `ip.addr == 10.1.2.0/24` (CIDR format!)

Resources, References and Reading

- Ethereal Site
 - www.ethereal.com
 - <http://winpcap.polito.it/>
- RFCs
 - www.ietf.org
- Registered Numbers
 - www.iana.org
- TCP Expressions
 - Search for “*tcpdump man*”
- Gerald Coombs/Richard Sharpe Book from O'Reilly

Conclusion

- Ethereal is a free analyzer distributed under the GNU license
- It is worth your time to learn how Ethereal works
- Ethereal offers real-time packet display, sortable trace columns, strong decodes and TCP stream analysis.