Ethereal – Analysis on a Budget

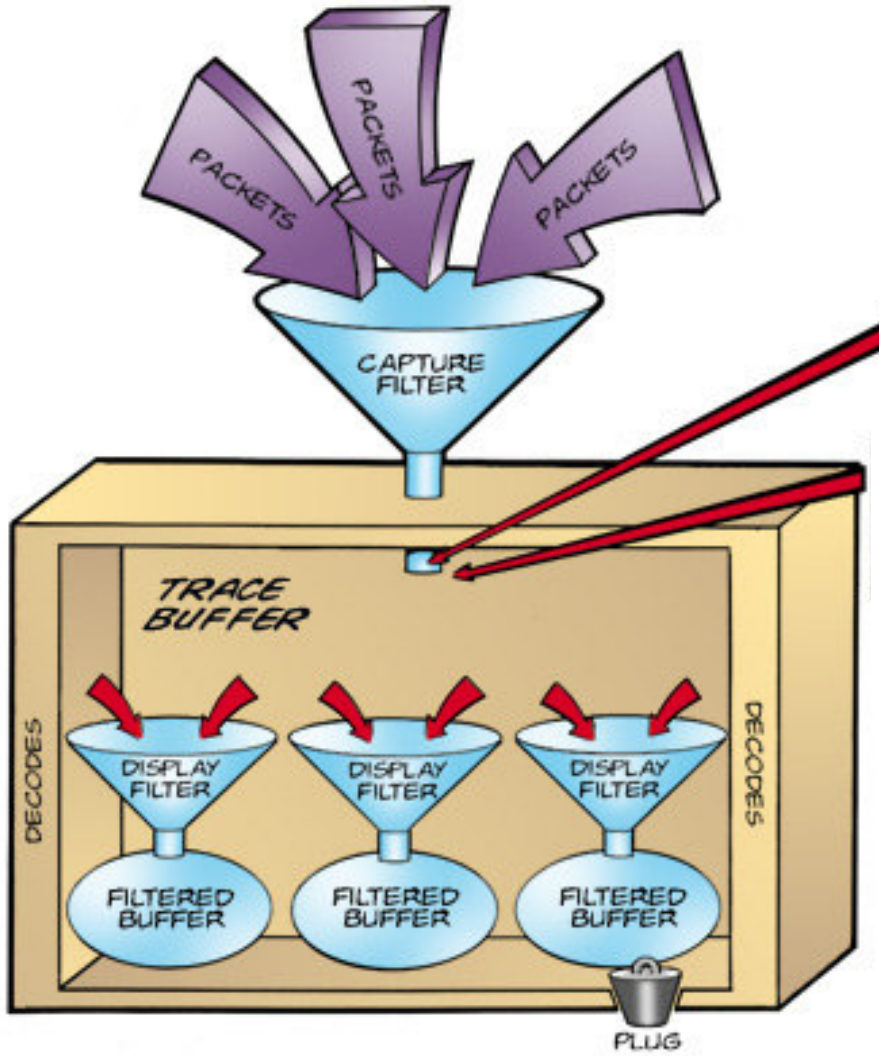
Laura Chappell
Protocol Analysis Institute, Inc.
lchappell@packet-level.com
www.packet-level.com
www.podbooks.com

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



TCP Stream Analysis

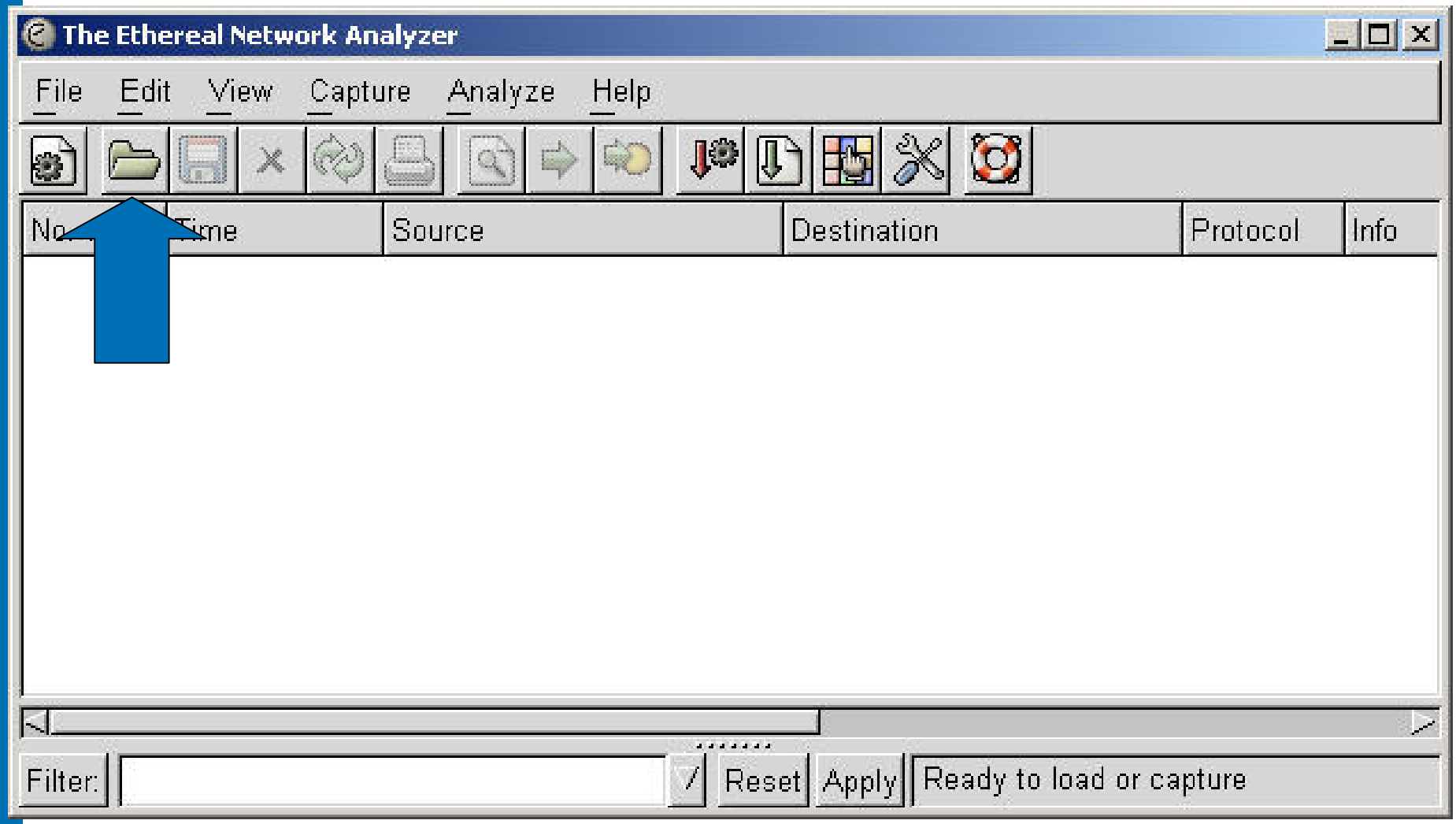
User-Specified Decodes

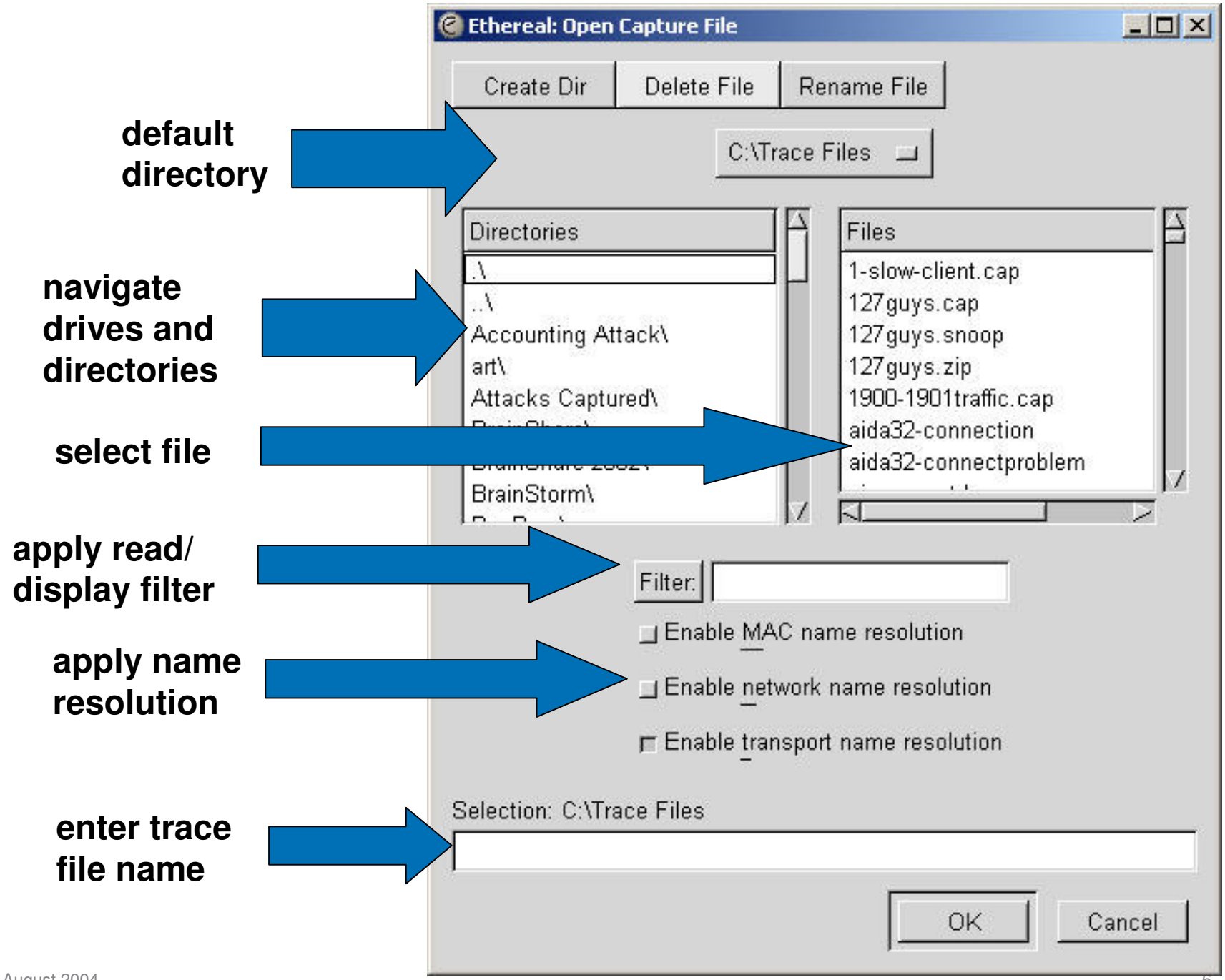
Loading Ethereal

- Binary distributions and ready-to-compile source code available online at www.ethereal.com.

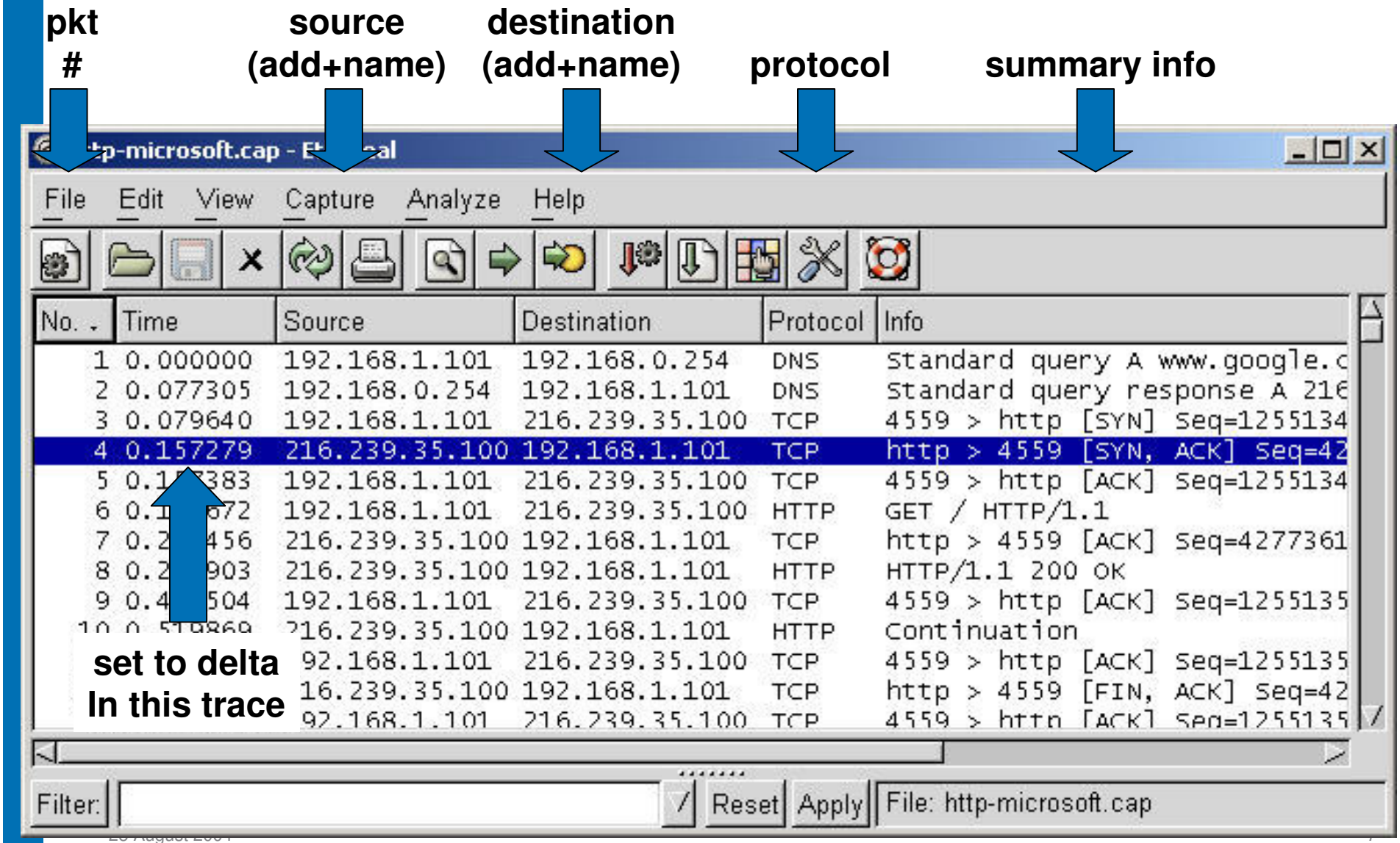
- For Windows, two components are needed:
  - Windows Packet Capture driver (*WinPcap*)
  - Ethereal binary

Opening Trace Files



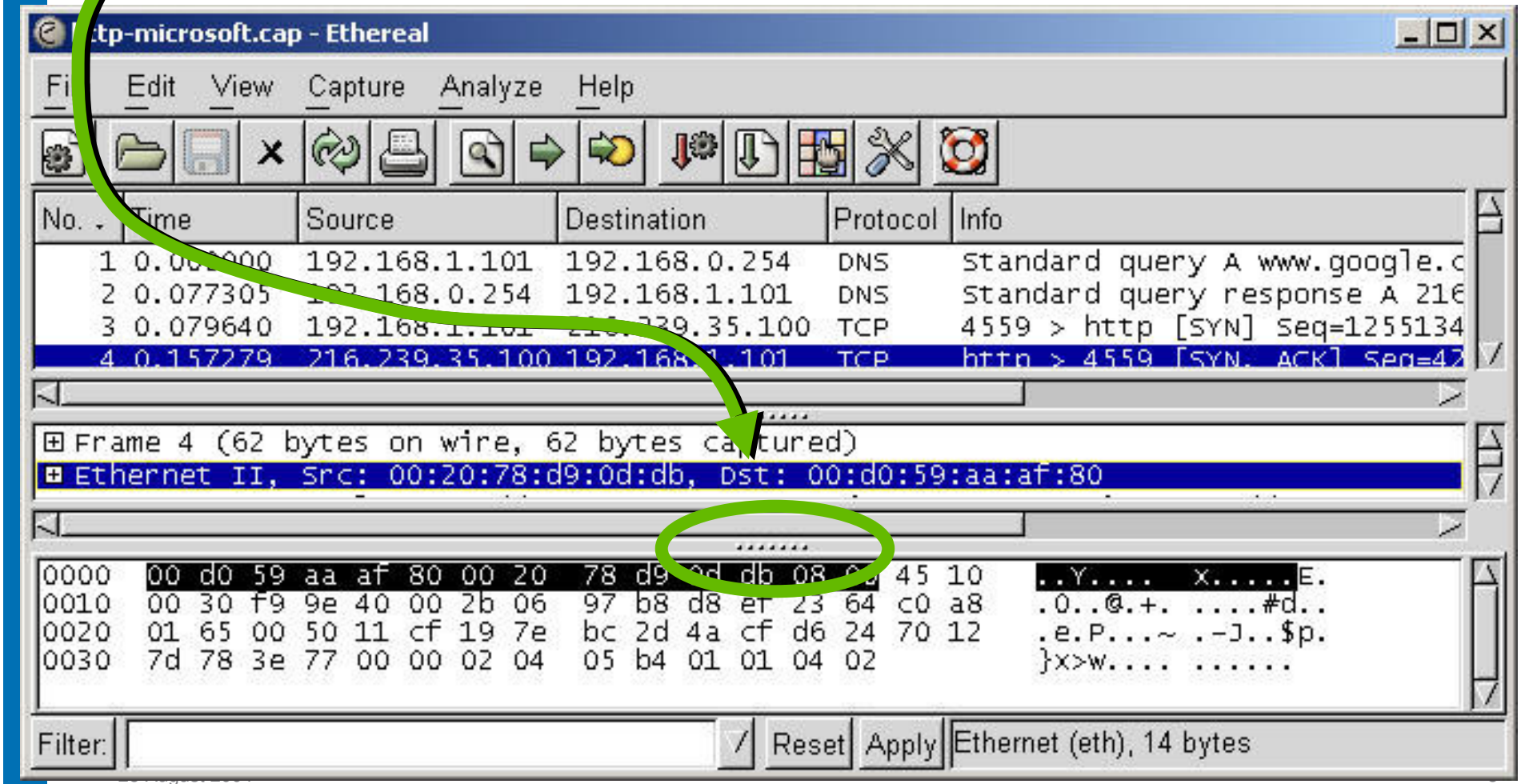

default directory
navigate drives and directories
select file
apply read/ display filter
apply name resolution
enter trace file name
Ethereal: Open Capture File
Create Dir
Delete File
Rename File
C:\Trace Files
Directories
.\
..\
Accounting Attack\
art\
Attacks Captured\
BrainStorm\
Files
1-slow-client.cap
127guys.cap
127guys.snoop
127guys.zip
1900-1901traffic.cap
aida32-connection
aida32-connectproblem
Filter:
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Selection: C:\Trace Files
OK
Cancel

Opening Trace Files (w/o filter)



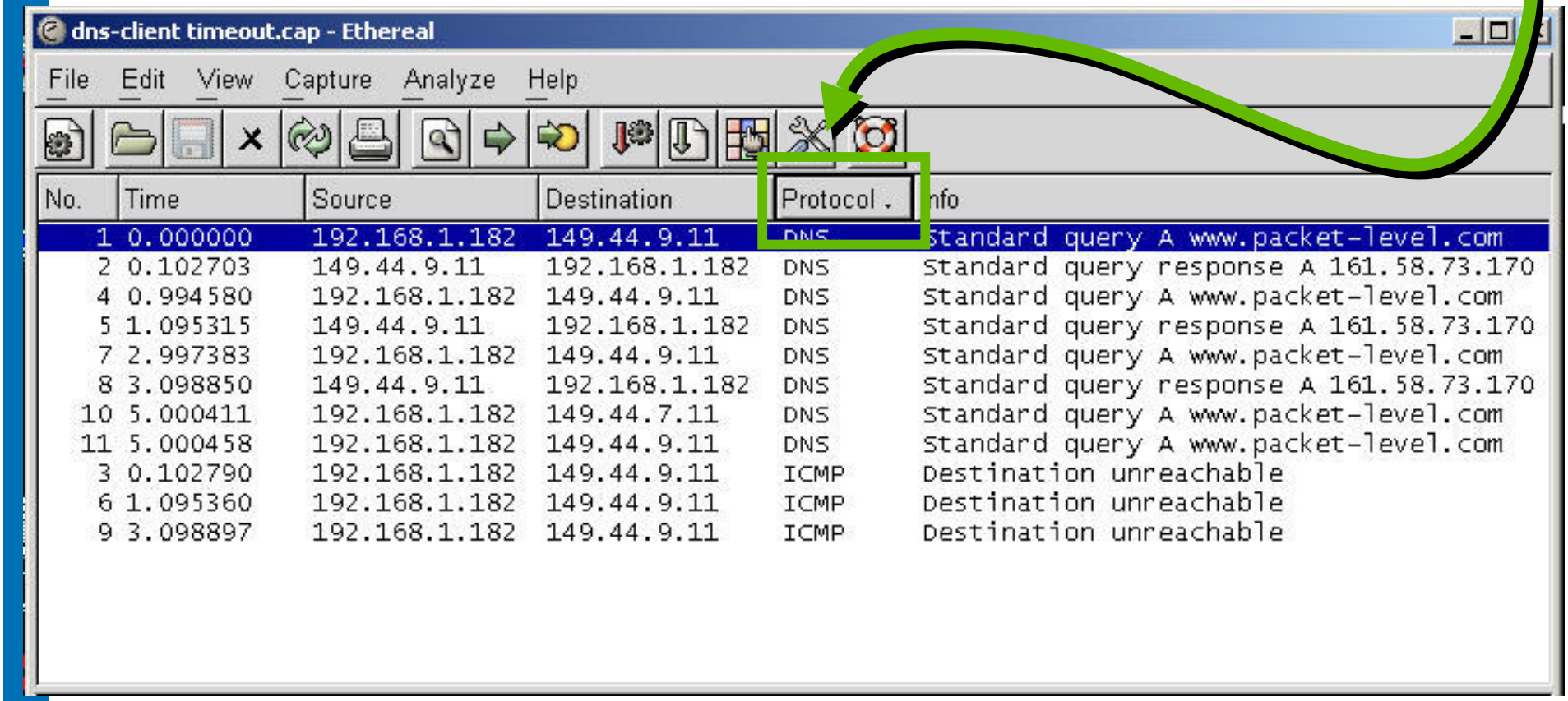
Opening Other Windows

Click and drag to open decode and hex windows

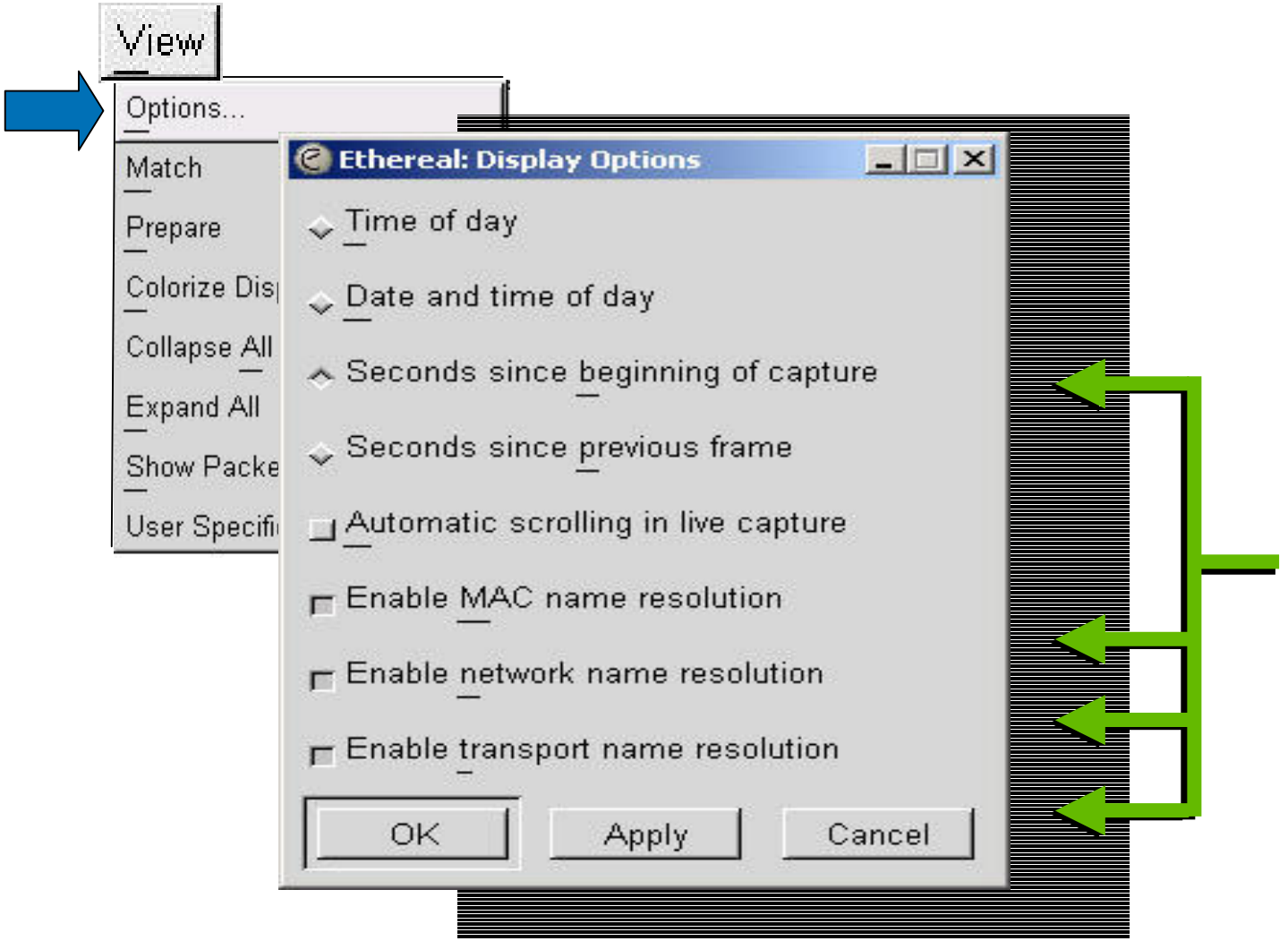


Sorting Trace Columns

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

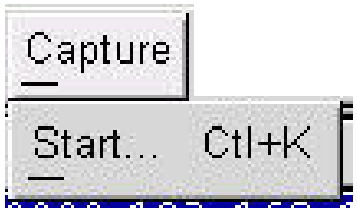


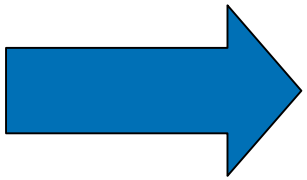
Changing the Display

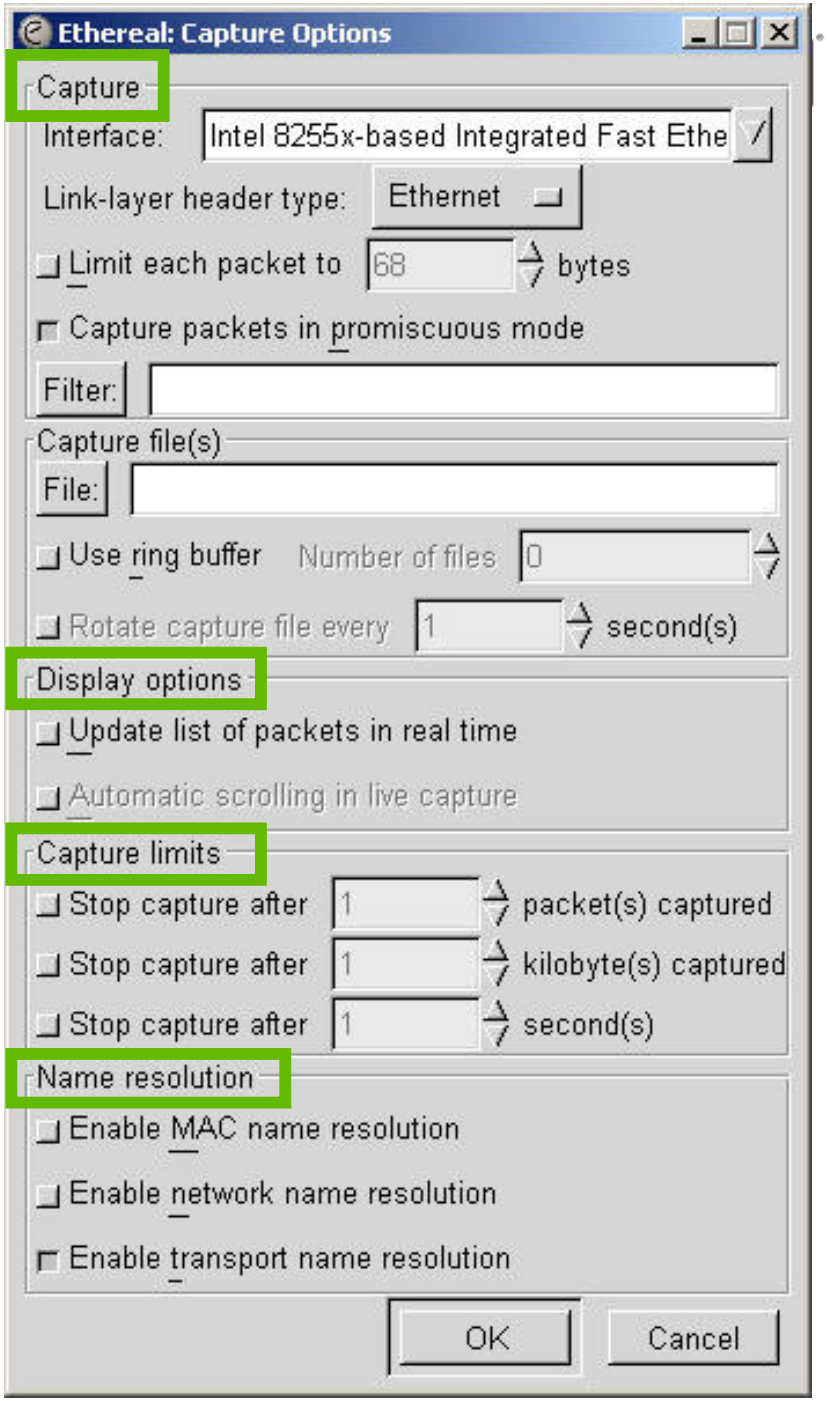


Default Settings

Capturing Packets

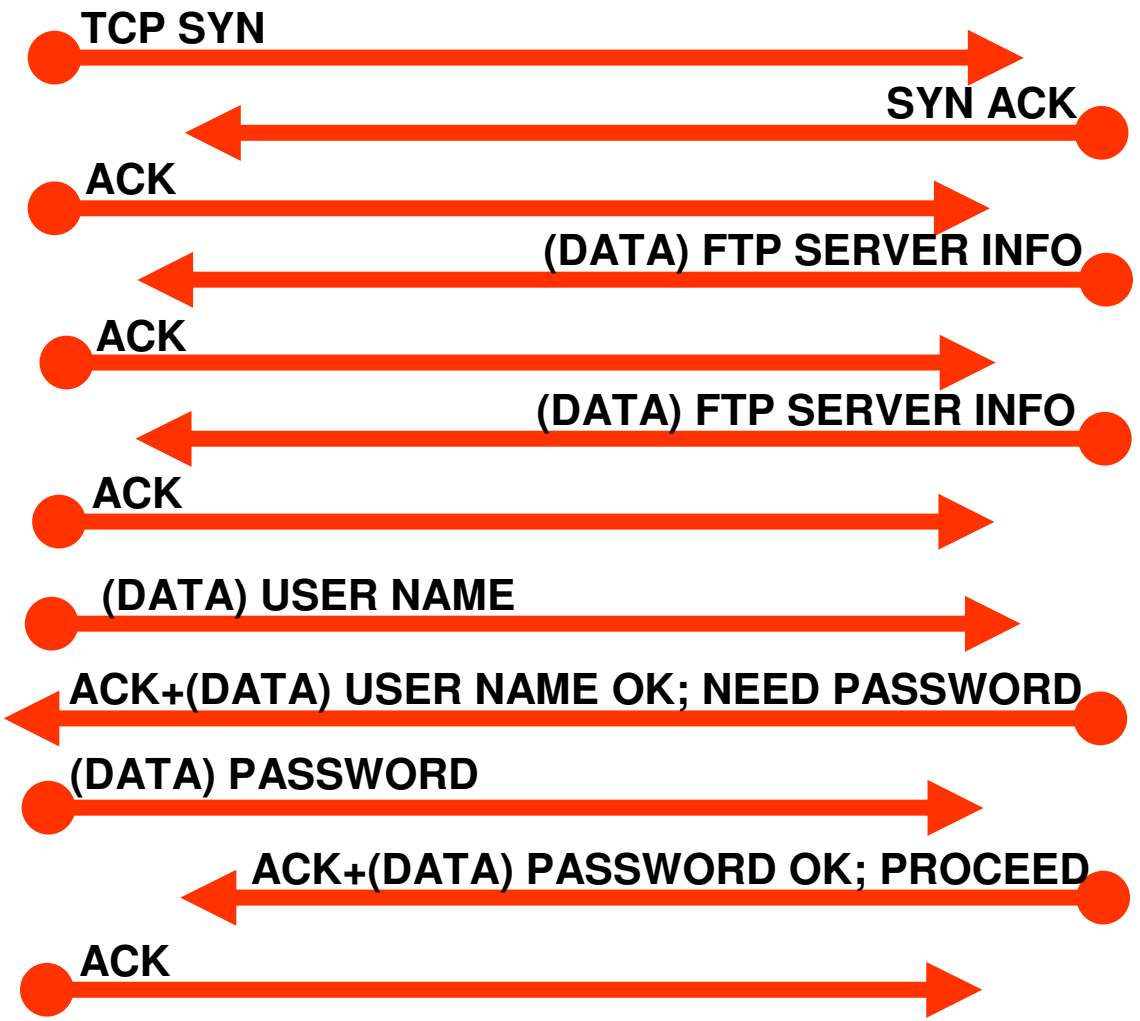






Following TCP Streams

Client



Server

Following TCP Streams

Client

Server

TCP SYN

SYN ACK

ACK

(DATA) FTP SERVER INFO

ACK

(DATA) FTP SERVER INFO

ACK

(DATA) USER NAME

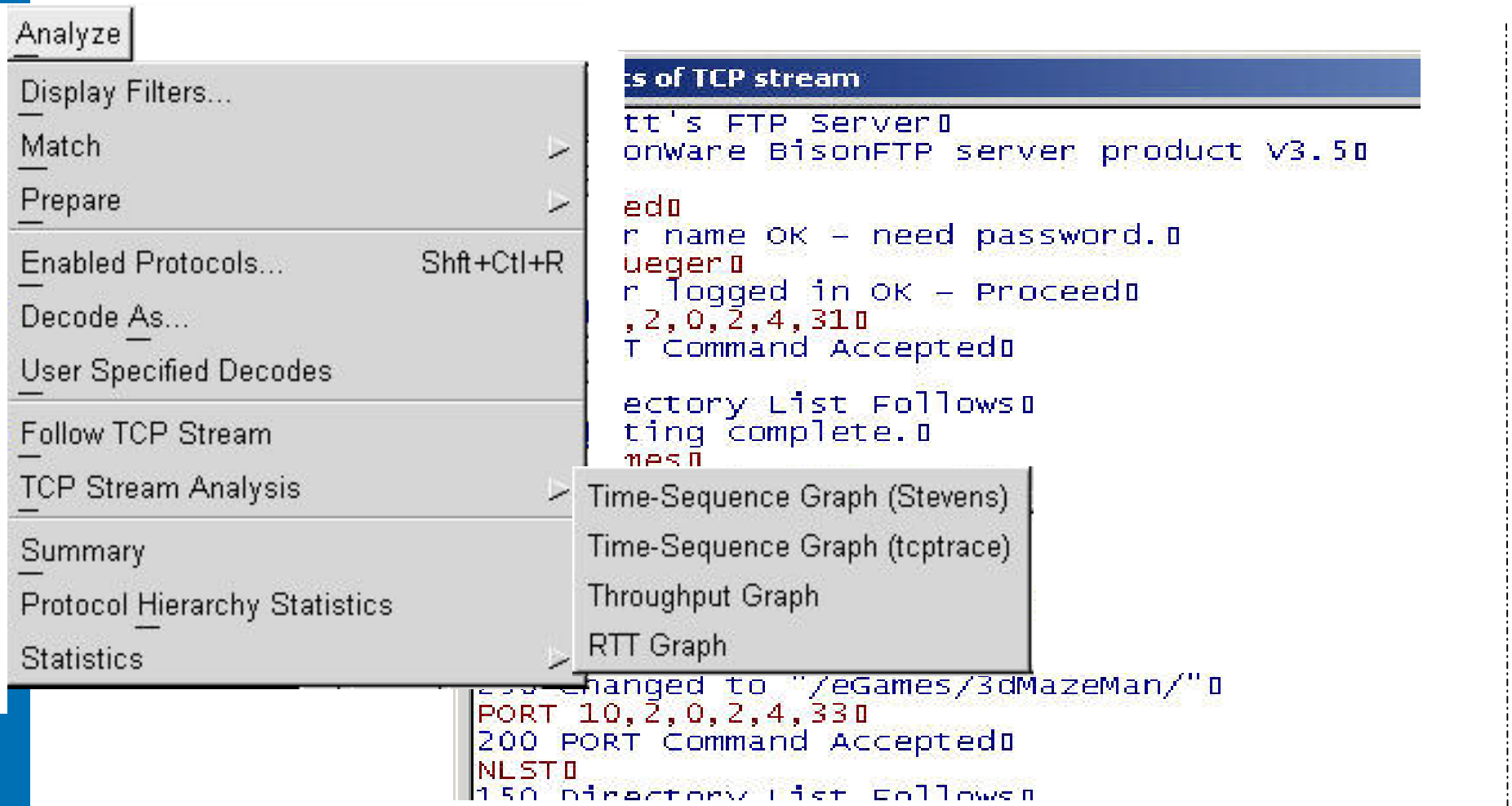
ACK+(DATA) USER NAME OK; NEED PASSWORD

(DATA) PASSWORD

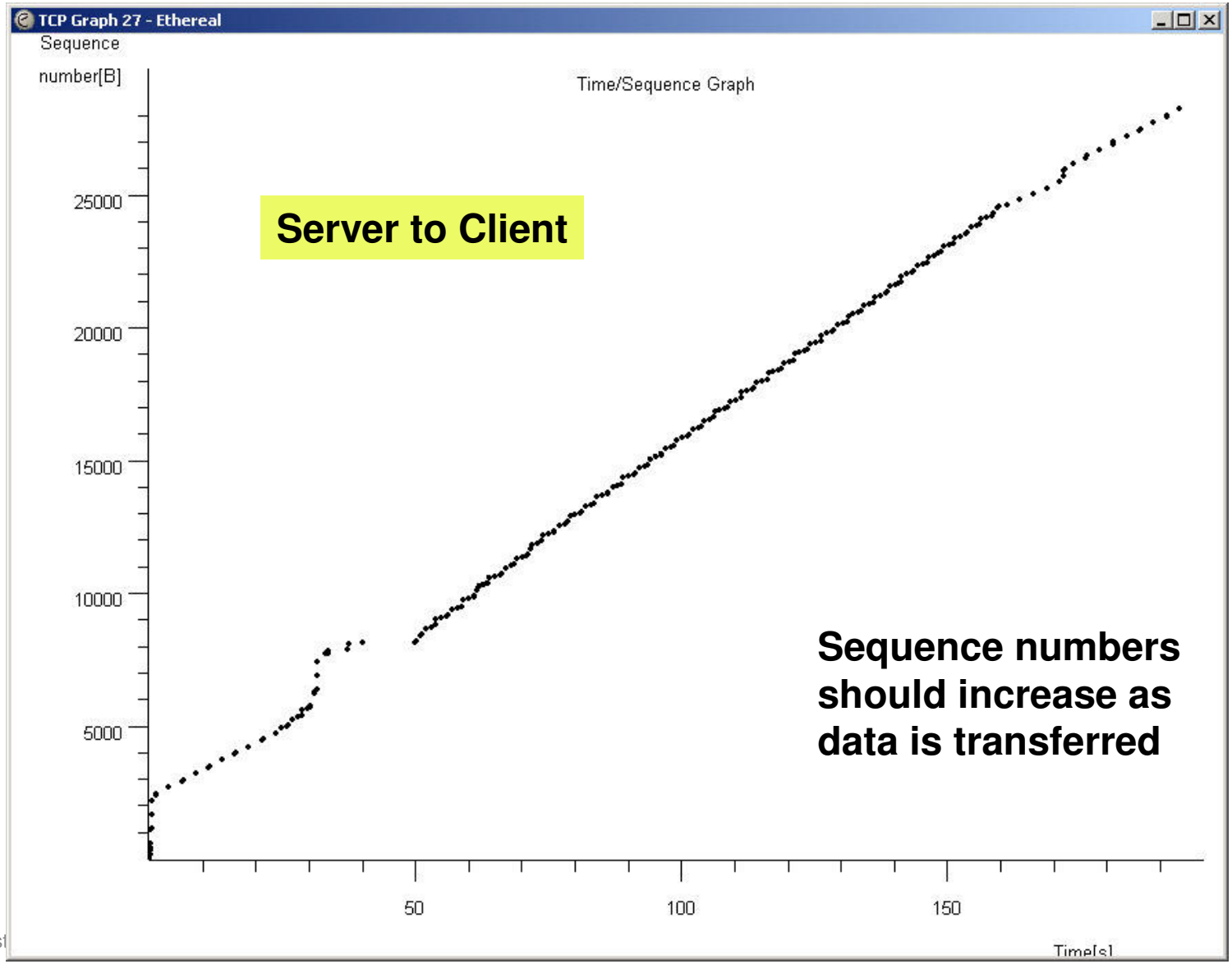
ACK+(DATA) PASSWORD OK; PROCEED

ACK

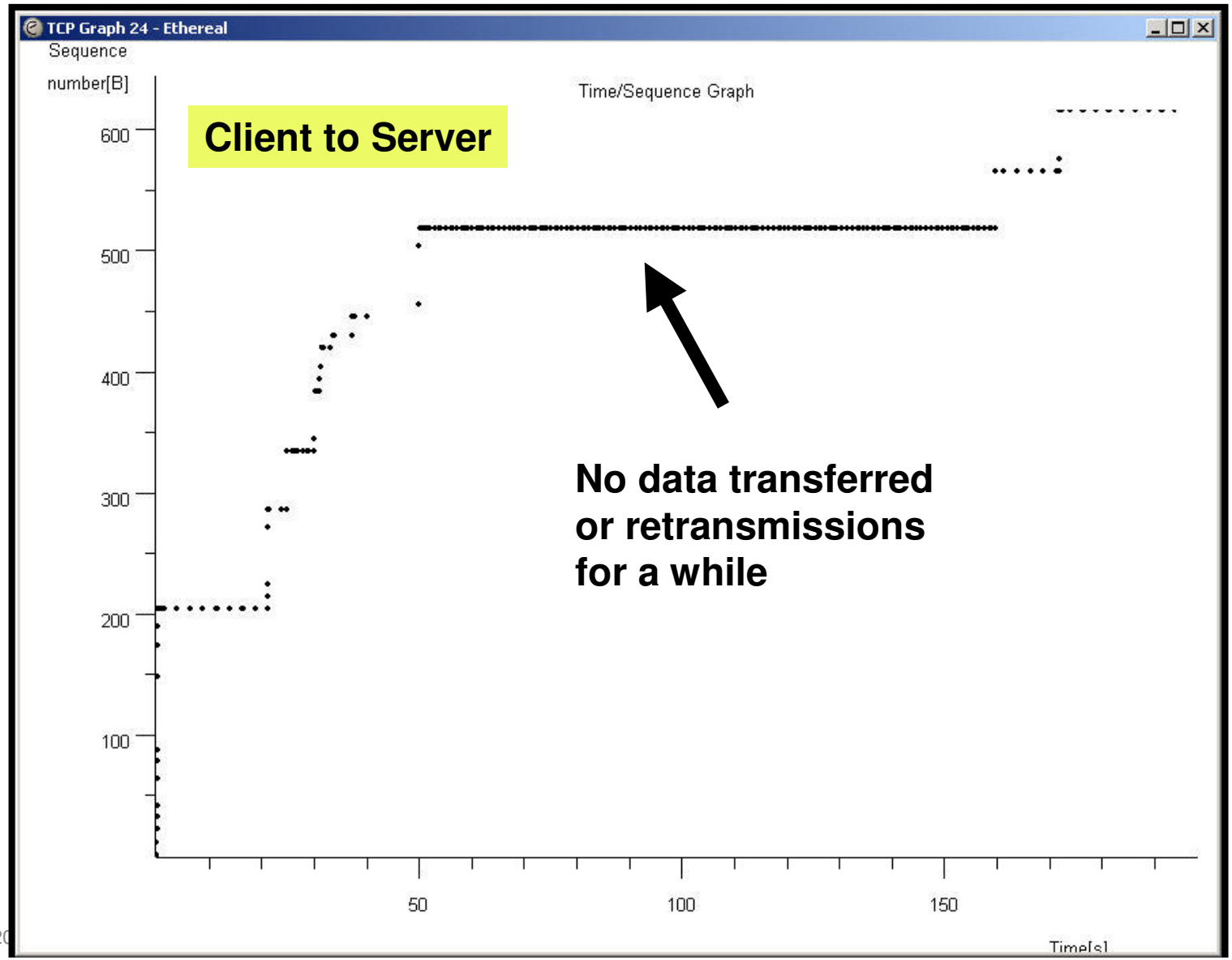
Following TCP Streams



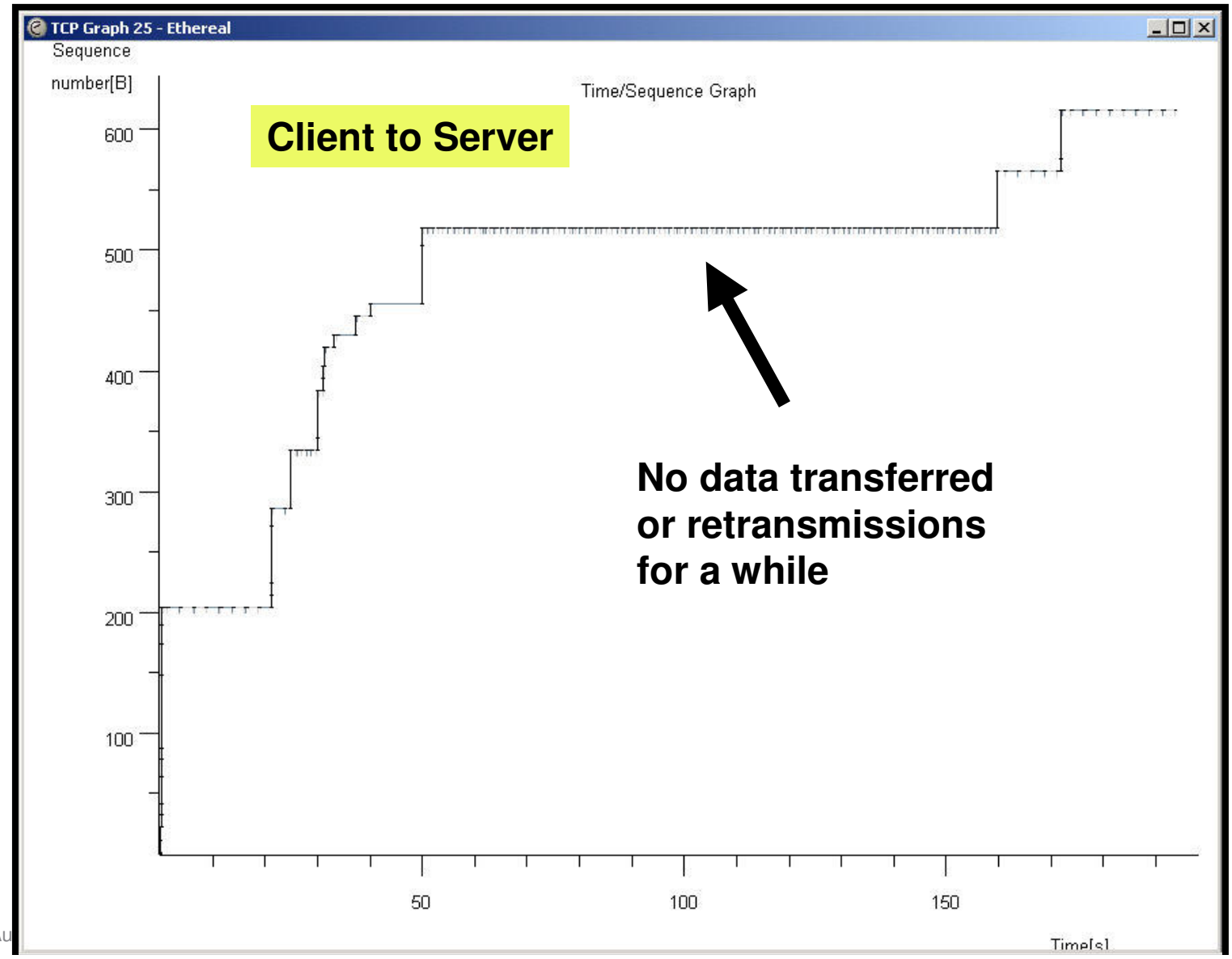
TCP Time-Sequence Graph (Stevens)



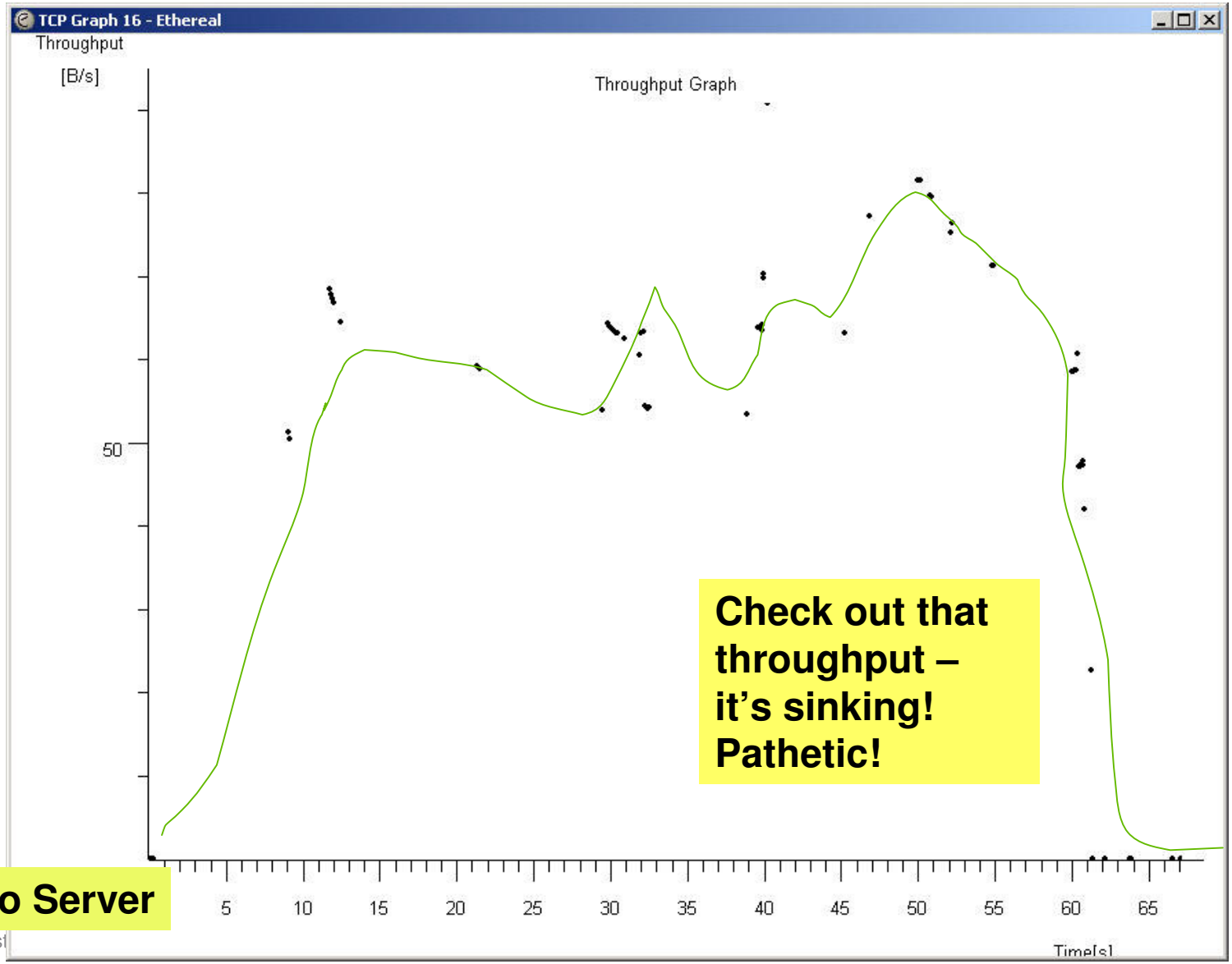
TCP Time-Sequence Graph (Stevens)



TCP Time-Sequence Graph (tcptrace)

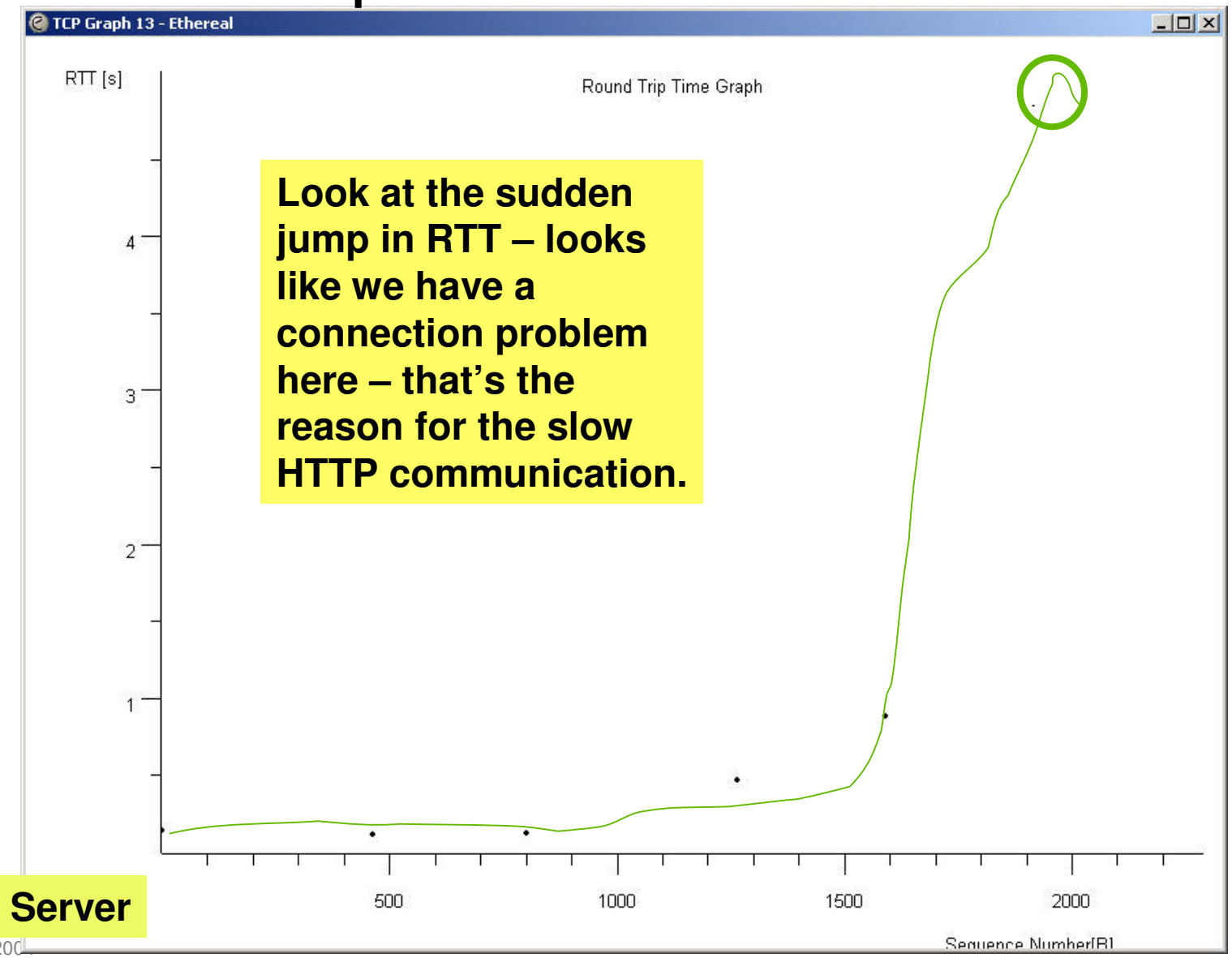


TCP Throughput Graph



Client to Server

TCP RTT Graph

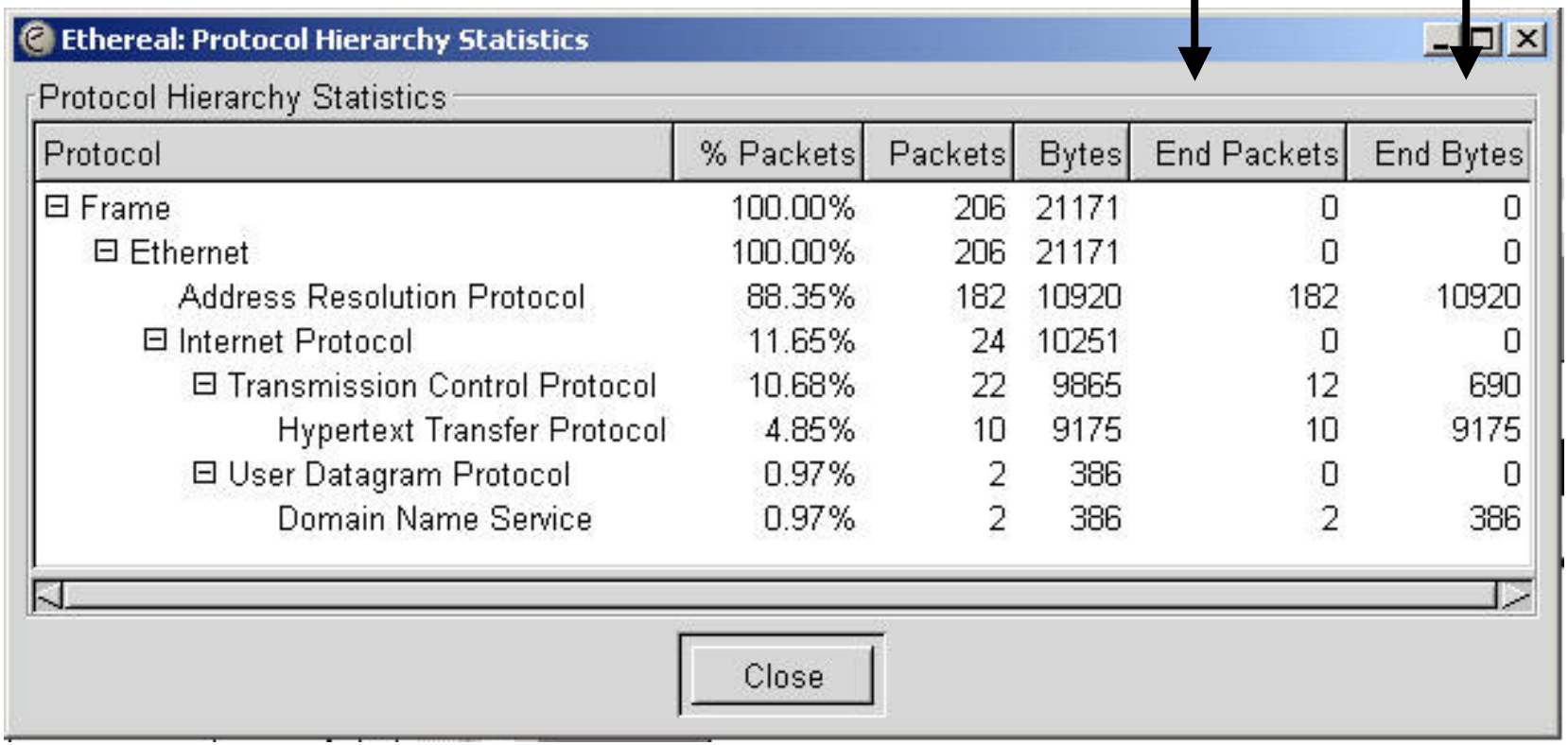


Look at the sudden jump in RTT – looks like we have a connection problem here – that's the reason for the slow HTTP communication.

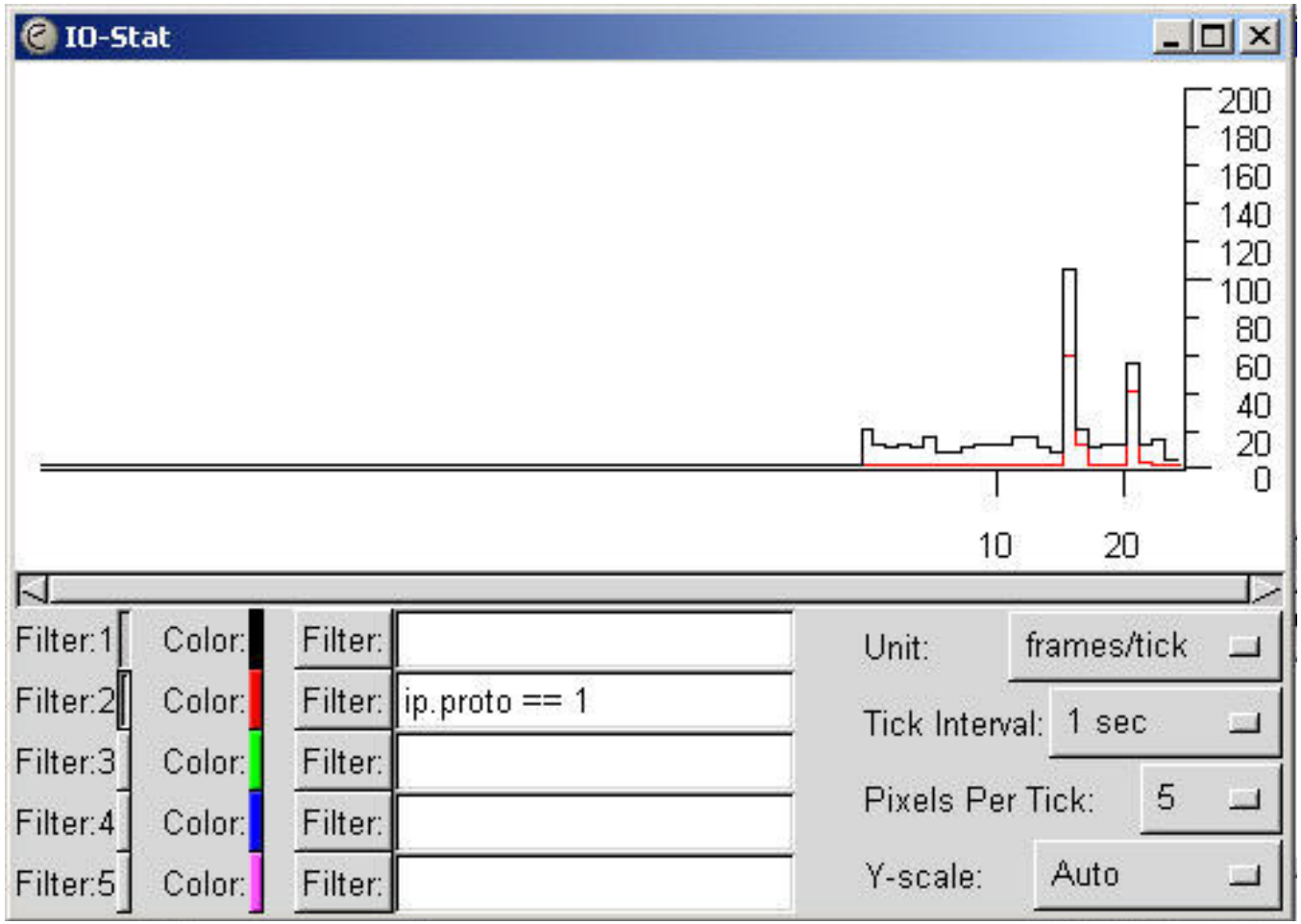
Client to Server

Protocol Statistics

Totals per Protocol

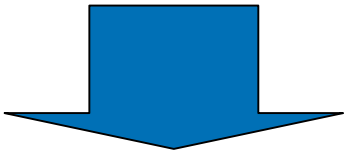


Looking at IO Stats

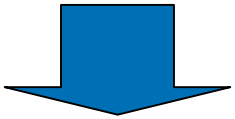


Building and Applying Filters

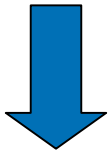
Stored Filters



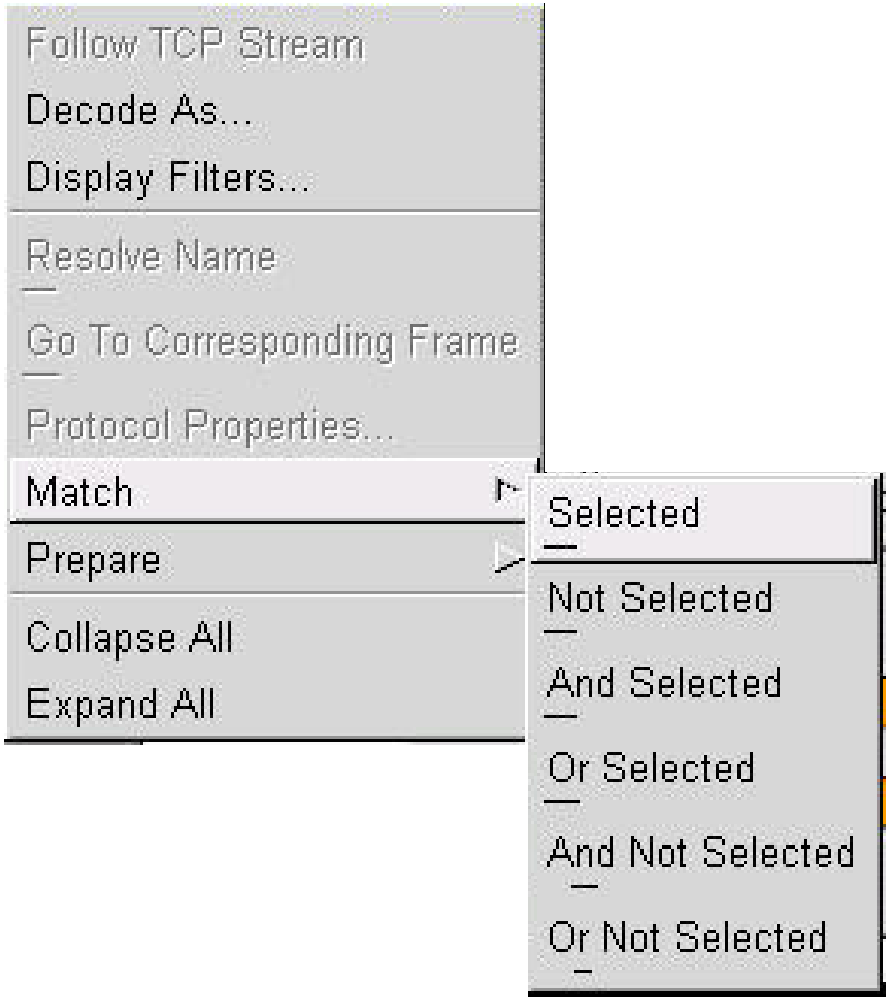
Capture Filters



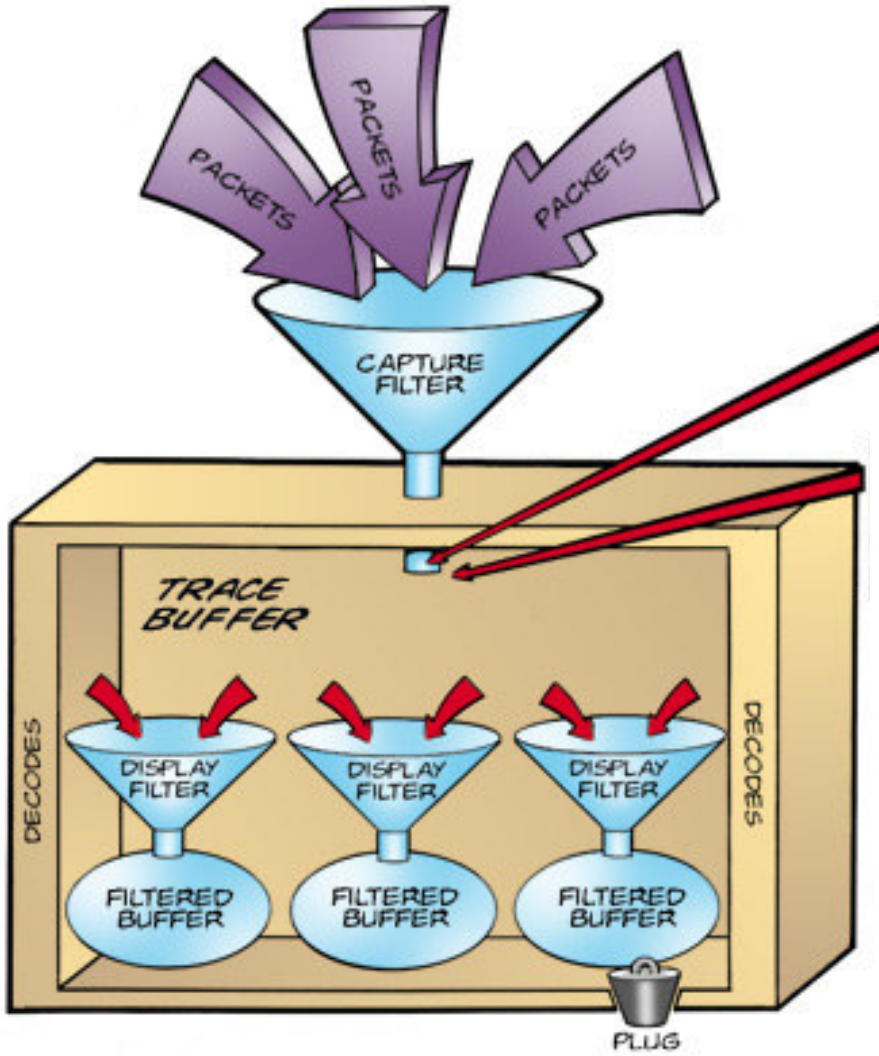
Display Filters



Temporary Filters



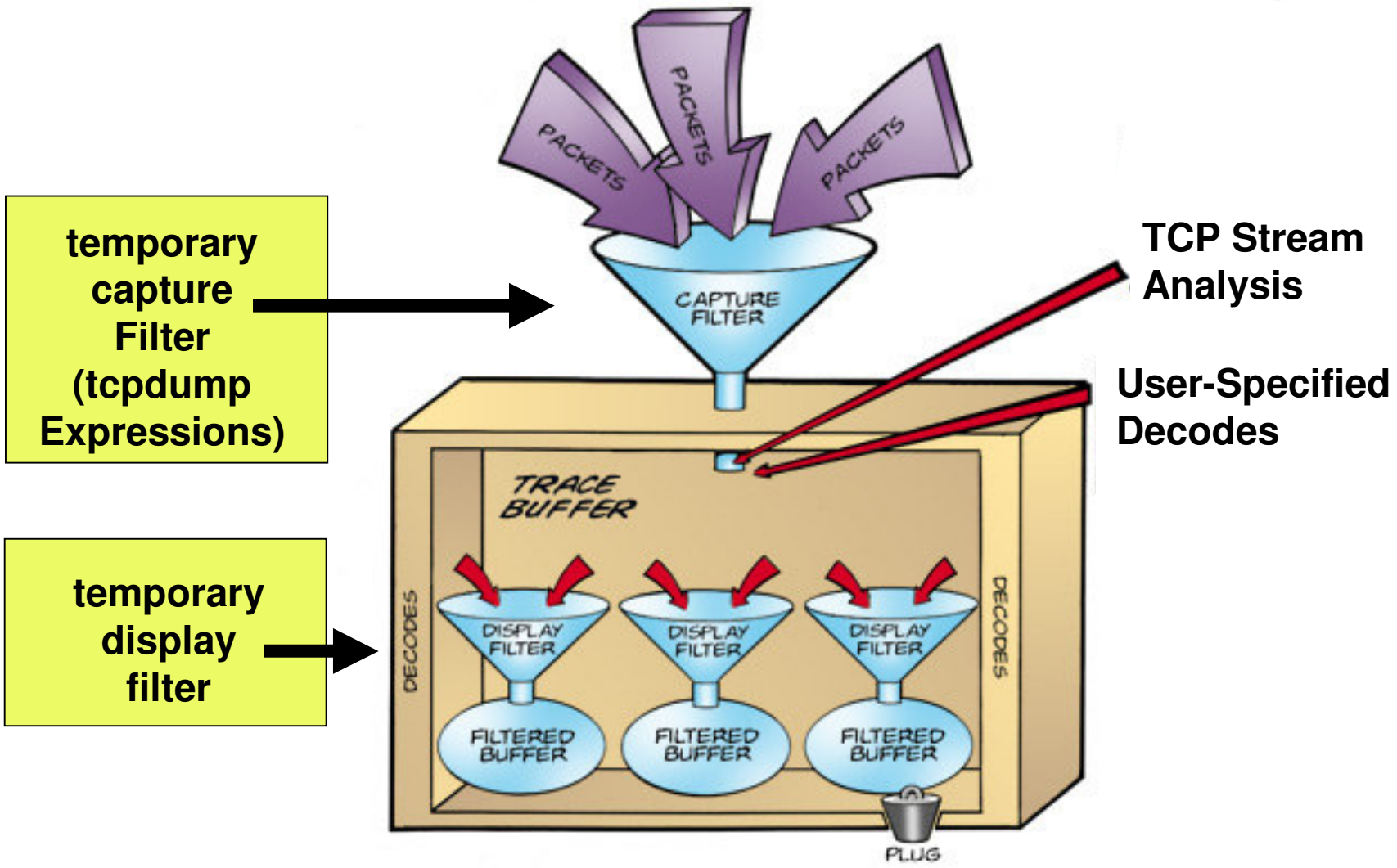
Where Filters are Applied



TCP Stream Analysis

User-Specified Decodes

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.