Using the Ethereal and tcpdump Protocol Analyzers

Doug Toppin
Nov 2003

toppin.com

What is Ethereal?

“ Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.”

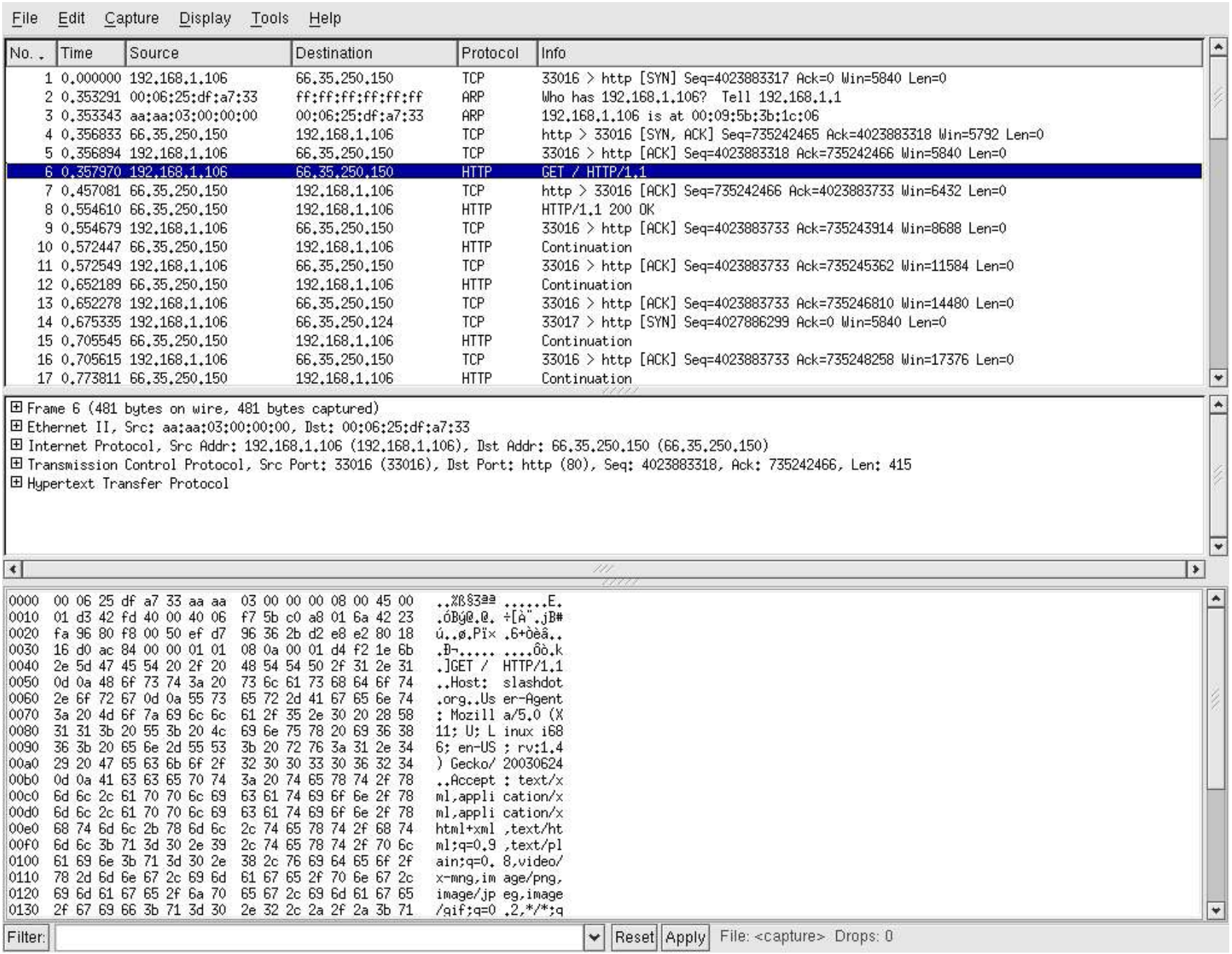
Similar Tools

- tethereal - textual version of ethereal
- tcpdump - textual protocol analyzer

These tools use the pcap (libpcap) packet capture library (which can be used to generate custom capture apps)

What does ethereal look like?

- gui composed of 4-fields:
  - Menu bar
  - List of captured packets
  - Top-level info on selected packet
  - Detail of selected packet
  - See following slide for example

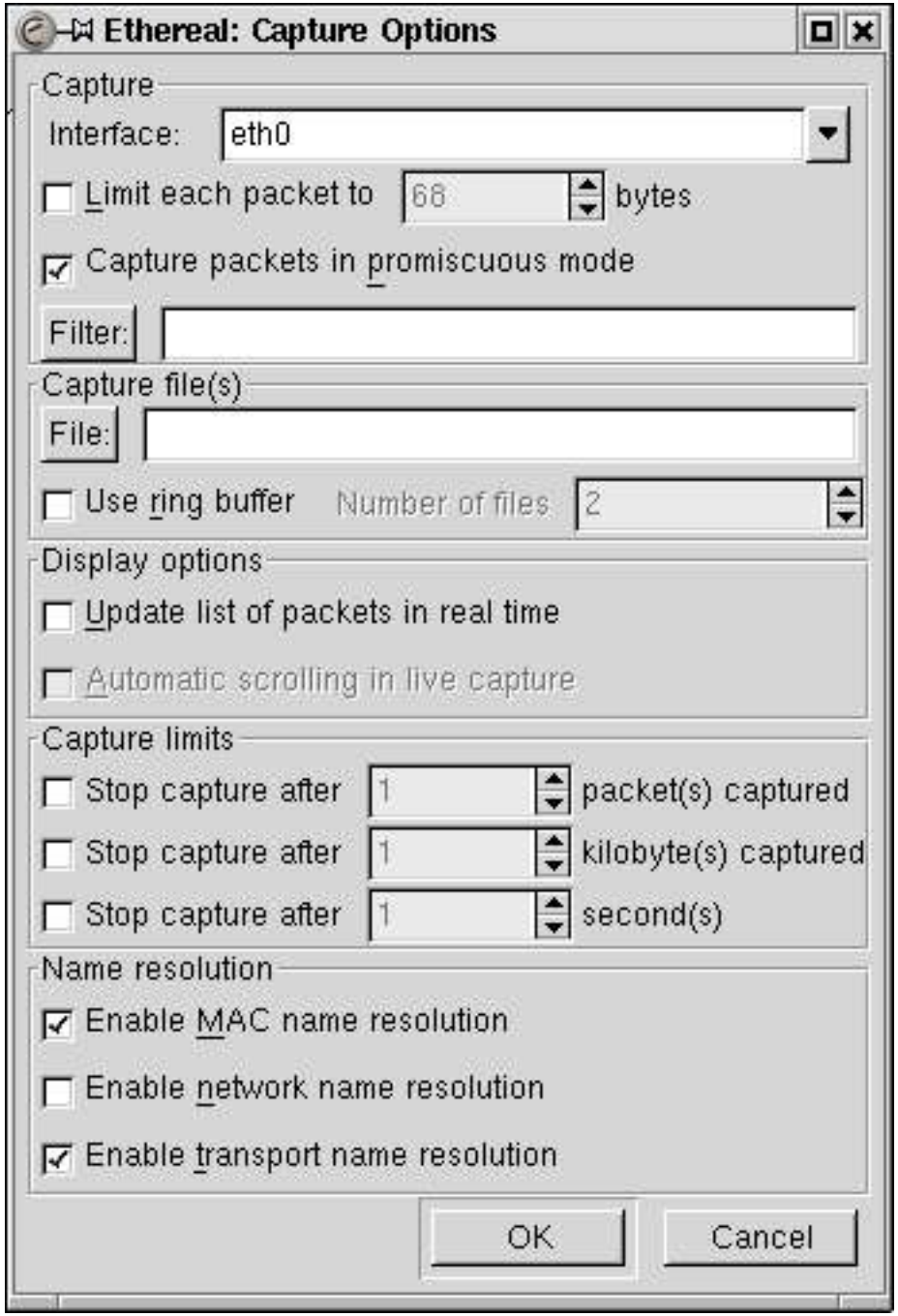


captured packet list

overhead of selected packet

detail of selected packet

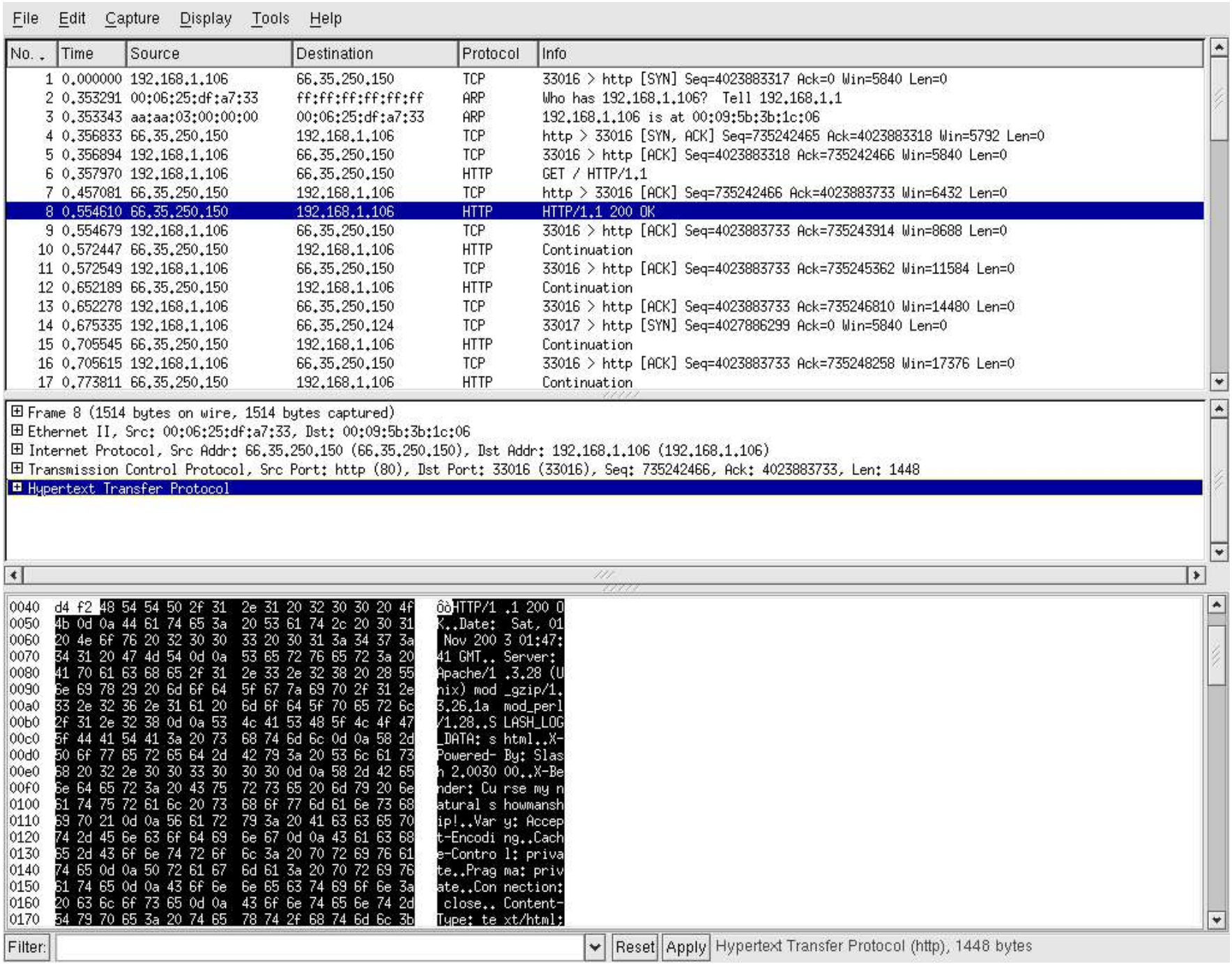
Illus-1 gui



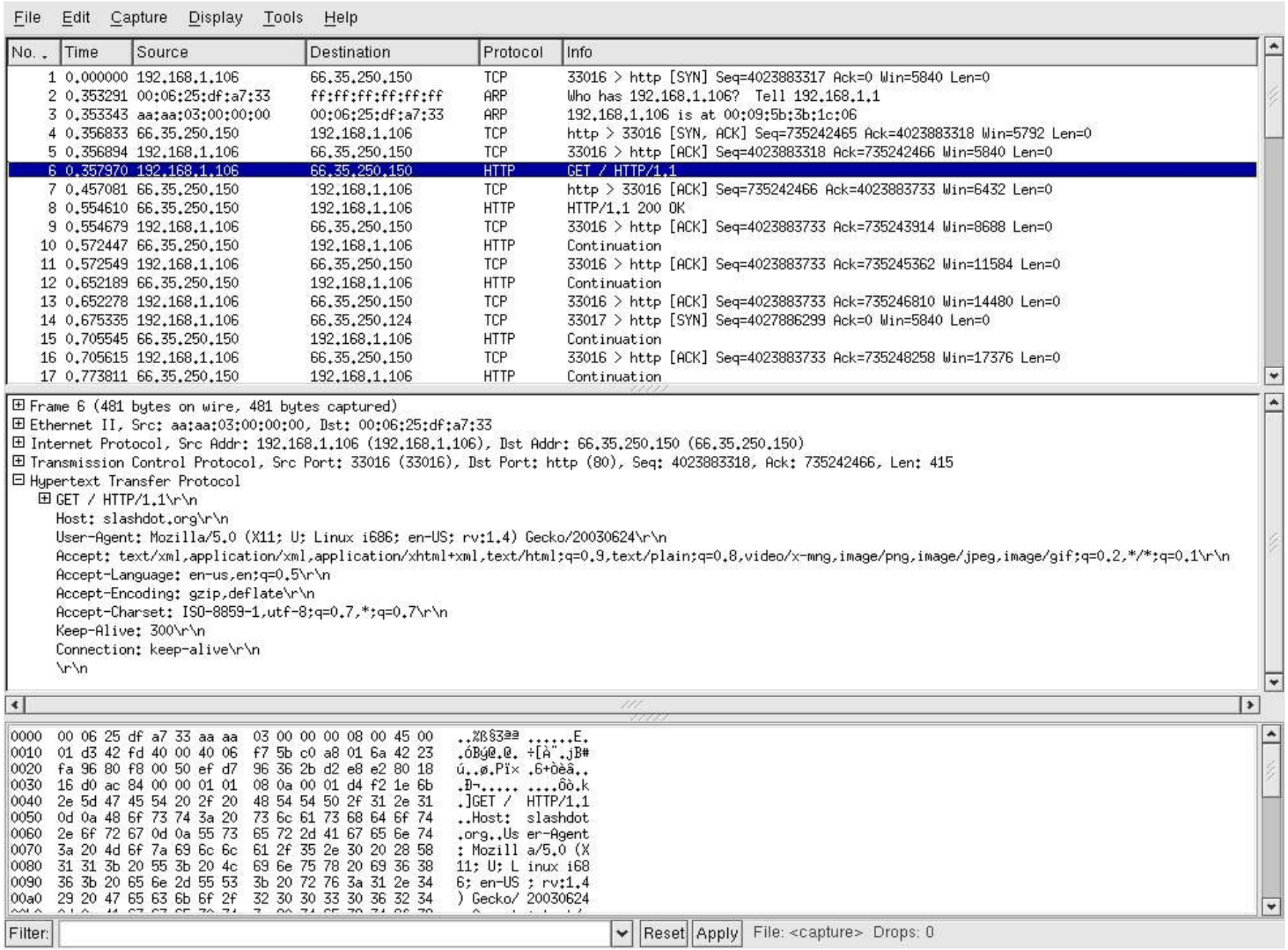
Illus-2 Capture initiator

uses for these tools

- find messages that have errors in them without modifying code (adding debug prints)
- monitor/analyze lan traffic for activity/load/latency measurement
- save captured packets for later analysis (“ evidence” attached to an bug report)
- frequently used for passive intrusion detection and monitoring
- just to see what your network is up to

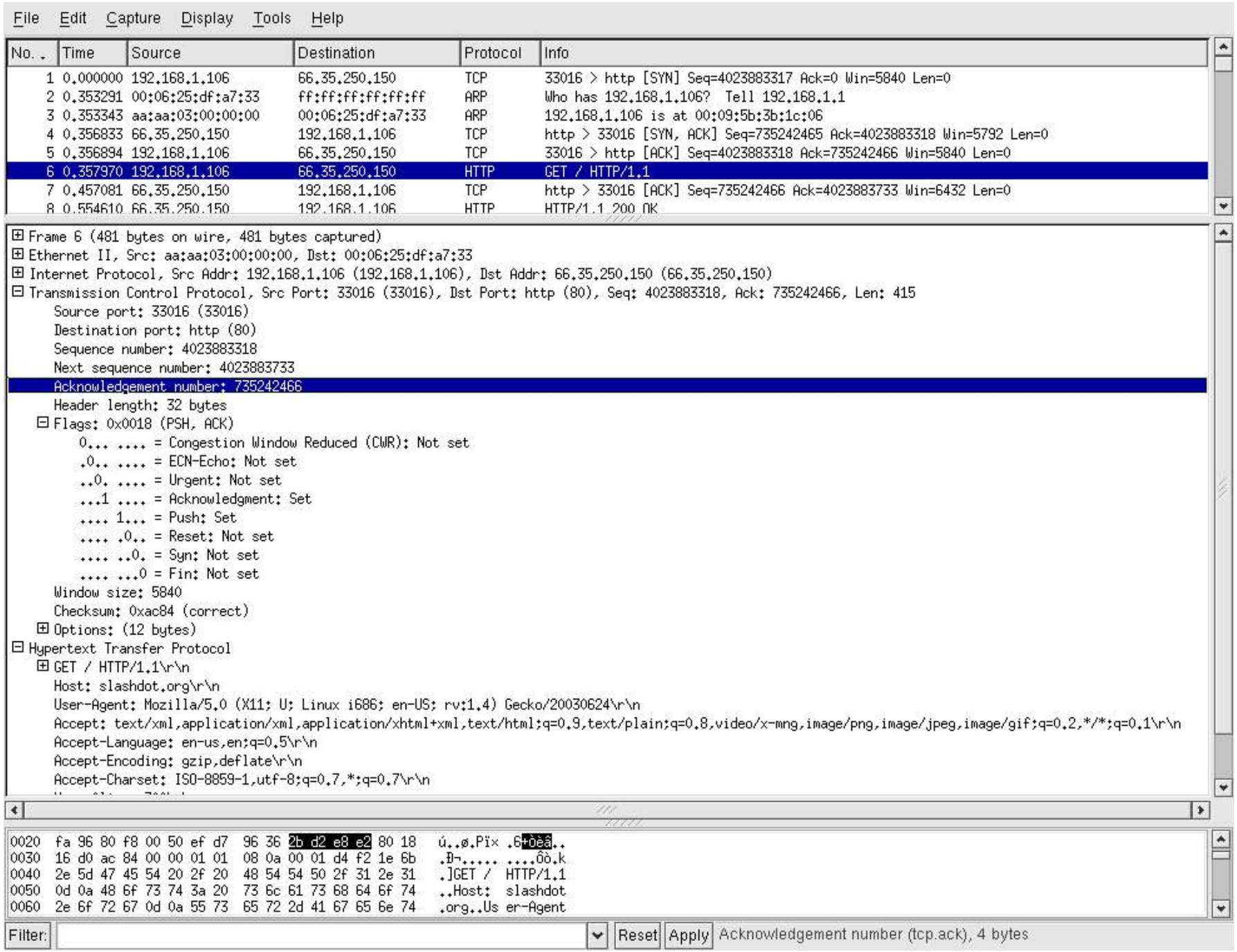


Illus-3 capture with payload selected (http)



Illus-4

note http text



Illus-5
note header
field decode
and selection

notes on use

- after capture/load:
  - can search for packets of interest
  - colorize particular packets
  - mark and save particular packets
  - graph I/O stats, round-trip time, throughput
  - can select packets from graphs to move to in gui

notes on use

- network interface is put into "promiscuous" mode meaning that it will pass all packets up to the os for processing rather than just those addressed to this machine
- use a simple hub to to get access to the LAN from a monitor machine (do not use a switch unless you can configure it to act as a hub)

more detailed uses

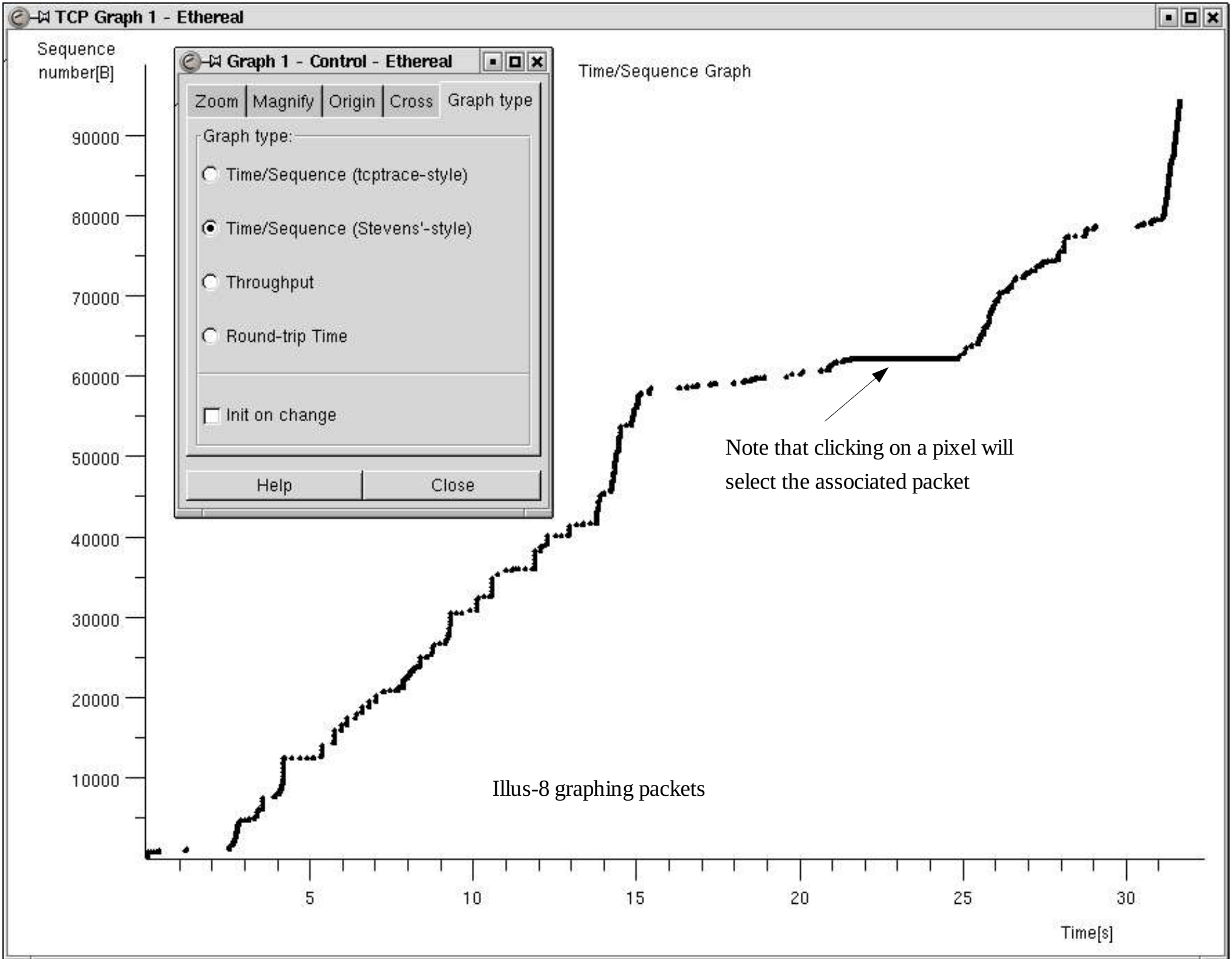
- custom protocol decoders can be written and added (for corba: www.linuxjournal.com/article.php?sid=5453)
- monitor results/effects of changes such as changing window/timing/buffer settings (fewer but larger packets)
- monitor nfs
- monitor/measure audio latency

example of ethereal filters

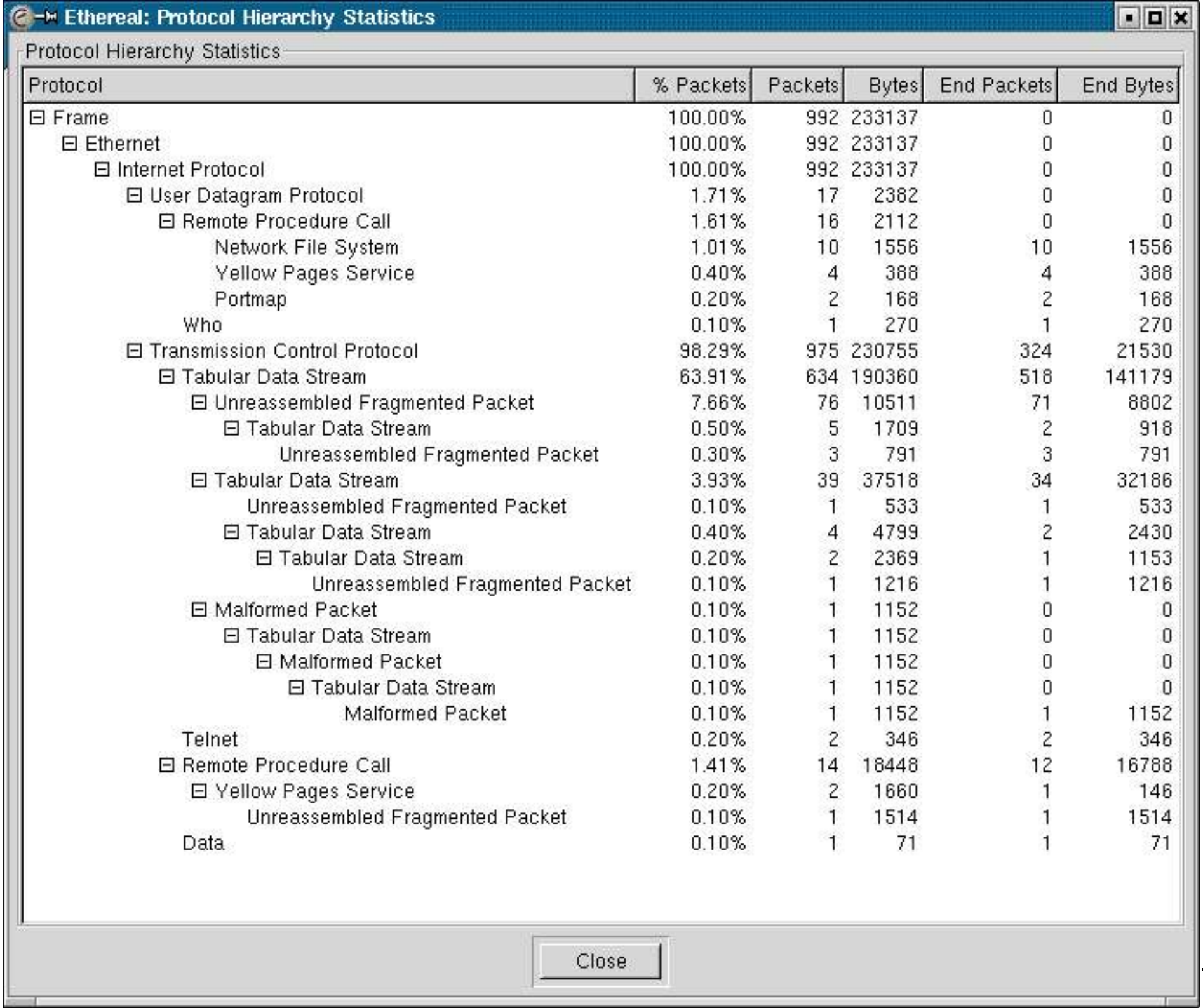
- all packets to/from a host:
  - host 192.168.1.5
- non-nfs traffic to/from a specific host:
  - host 192.168.1.5 and not port nfs
- DB traffic to/from a specific host:
  - host 192.168.1.5 and port (4501 or 4509)

example of tcpdump filters

- filter and output summary of an existing capture file:
  - tcpdump -r test01.eth host hostname.com and port 4501
- filter and output detail of an existing capture file:
  - tcpdump -xX -r test01.eth dst hostname.com and port 4501
- output all tcp connections (syn/ack set):
  - tcpdump -r temp01.eth tcp[13]==18
- count nfs traffic:
  - tcpdump -r test08.eth 'port nfs' | wc



Illus-8 graphing packets



Protocol	% Packets	Packets	Bytes	End Packets	End Bytes
⊟ Frame	100.00%	992	233137	0	0
⊟ Ethernet	100.00%	992	233137	0	0
⊟ Internet Protocol	100.00%	992	233137	0	0
⊟ User Datagram Protocol	1.71%	17	2382	0	0
⊟ Remote Procedure Call	1.61%	16	2112	0	0
Network File System	1.01%	10	1556	10	1556
Yellow Pages Service	0.40%	4	388	4	388
Portmap	0.20%	2	168	2	168
Who	0.10%	1	270	1	270
⊟ Transmission Control Protocol	98.29%	975	230755	324	21530
⊟ Tabular Data Stream	63.91%	634	190360	518	141179
⊟ Unreassembled Fragmented Packet	7.66%	76	10511	71	8802
⊟ Tabular Data Stream	0.50%	5	1709	2	918
Unreassembled Fragmented Packet	0.30%	3	791	3	791
⊟ Tabular Data Stream	3.93%	39	37518	34	32186
Unreassembled Fragmented Packet	0.10%	1	533	1	533
⊟ Tabular Data Stream	0.40%	4	4799	2	2430
⊟ Tabular Data Stream	0.20%	2	2369	1	1153
Unreassembled Fragmented Packet	0.10%	1	1216	1	1216
⊟ Malformed Packet	0.10%	1	1152	0	0
⊟ Tabular Data Stream	0.10%	1	1152	0	0
⊟ Malformed Packet	0.10%	1	1152	0	0
⊟ Tabular Data Stream	0.10%	1	1152	0	0
Malformed Packet	0.10%	1	1152	1	1152
Telnet	0.20%	2	346	2	346
⊟ Remote Procedure Call	1.41%	14	18448	12	16788
⊟ Yellow Pages Service	0.20%	2	1660	1	146
Unreassembled Fragmented Packet	0.10%	1	1514	1	1514
Data	0.10%	1	71	1	71

Illus-9 capture statistics

security concerns

- must be used responsibly (it is just like listening in on the phone)
- can capture private information
- you will get into trouble if you exercise poor judgement when using this tool

ways that prot analyzers can help you

- what is happening on the network?
- what is a host in particular up to?
- network app is hung, what is it doing? (capture all traffic to/from host and see)
- what is going on during when my app starts up and talks to the database?
- exactly what query is the db getting?

protocol dissectors

- a protocol dissector is custom code that can decode and output fields from custom packets
- protocol dissectors can be written and added to ethereal, ethereal will call the decode function(s) when packets of the target type are encountered
- get ethereal source and take a look at ethereal/plugins/ for how they are done

generating idl plug-ins

- You need:
  - ethereal source (contains plugin source and idl2eth)
  - omniorb.sourceforge.net (some/all?)
- export PYTHONPATH=/usr/lib/python1.5/
- concatentate idl files into a single file
- cat /tmp/custom1.idl /tmp/custom2.idl > /tmp/custom.idl
- idl2eth /tmp/custom.idl > /tmp/custom.c
- cp /tmp/custom.c cvs-ethereal/ethereal/plugins/custom/packet-custom.c
- cd cvs-ethereal/ethereal
- make
- cd cvs-ethereal/ethereal/plugins/custom/
- make install
- (plug-ins get put into /usr/lib/ethereal/plugins/VERSION)

related stuff

- libpcap - lib for writing your own packet capture apps
- editcap - edit and/or translate the format of capture files (extract packets of interest)
- mergecap – combine multiple capture files into a single file
- text2pcap – create capture file from plain (hex) text
- idl2eth - CORBA IDL to Ethereal Plugin Generator

links

- www.ethereal.com
- etherape.sourceforge.net
- www.tcpdump.org
- Corba protocol decode: www.linuxjournal.com/article.php?sid=5453
- www.richardsharpe.com
- http://staff.washington.edu/dittrich/talks/core02/tools/tcpdump-filters.txt