

# Using the Ethereal and tcpdump Protocol Analyzers

Doug Toppin

Nov 2003

[toppin.com](http://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

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.106	66.35.250.150	TCP	33016 > http [SYN] Seq=4023883317 Ack=0 Win=5840 Len=0
2	0.353291	00:06:25:df:a7:33	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.106? Tell 192.168.1.1
3	0.353343	aa:aa:03:00:00:00	00:06:25:df:a7:33	ARP	192.168.1.106 is at 00:09:5b:3b:1c:06
4	0.356833	66.35.250.150	192.168.1.106	TCP	http > 33016 [SYN, ACK] Seq=735242465 Ack=4023883318 Win=5792 Len=0
5	0.356894	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883318 Ack=735242466 Win=5840 Len=0
6	0.357970	192.168.1.106	66.35.250.150	HTTP	GET / HTTP/1.1
7	0.457081	66.35.250.150	192.168.1.106	TCP	http > 33016 [ACK] Seq=735242466 Ack=4023883733 Win=6432 Len=0
8	0.554610	66.35.250.150	192.168.1.106	HTTP	HTTP/1.1 200 OK
9	0.554679	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735243914 Win=8688 Len=0
10	0.572447	66.35.250.150	192.168.1.106	HTTP	Continuation
11	0.572549	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735245362 Win=11584 Len=0
12	0.652189	66.35.250.150	192.168.1.106	HTTP	Continuation
13	0.652278	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735246810 Win=14480 Len=0
14	0.675335	192.168.1.106	66.35.250.124	TCP	33017 > http [SYN] Seq=4027886299 Ack=0 Win=5840 Len=0
15	0.705545	66.35.250.150	192.168.1.106	HTTP	Continuation
16	0.705615	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735248258 Win=17376 Len=0
17	0.773811	66.35.250.150	192.168.1.106	HTTP	Continuation

Frame 6 (481 bytes on wire, 481 bytes captured)

- Ethernet II, Src: aa:aa:03:00:00:00, Dst: 00:06:25:df:a7:33
- Internet Protocol, Src Addr: 192.168.1.106 (192.168.1.106), Dst Addr: 66.35.250.150 (66.35.250.150)
- Transmission Control Protocol, Src Port: 33016 (33016), Dst Port: http (80), Seq: 4023883318, Ack: 735242466, Len: 415
- Hypertext Transfer Protocol

```

0000  00 06 25 df a7 33 aa aa 03 00 00 08 00 45 00  ..%83@a .....E.
0010  01 d3 42 fd 40 00 40 06 f7 5b c0 a8 01 6a 42 23  .0By@.@. +[â".jB#
0020  fa 96 80 f8 00 50 ef d7 96 36 2b d2 e8 e2 80 18  ú..ø.Pix ,6+0èâ..
0030  16 d0 ac 84 00 00 01 01 08 0a 00 01 d4 f2 1e 6b  .B-..... ..ôð.k
0040  2e 5d 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  .]GET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 73 6c 61 73 68 64 6f 74  ..Host: slashdot
0060  2e 6f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74  .org..Us er-Agent
0070  3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58  ; Mozill a/5.0 (X
0080  31 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38  11; U; L inux i68
0090  36 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 34  6; en-US ; rv:1.4
00a0  29 20 47 65 63 6b 6f 2f 32 30 30 33 30 36 32 34  ) Gecko/ 20030624
00b0  0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78  ..Accept : text/x
00c0  6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78  ml,appli cation/x
00d0  6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78  ml,appli cation/x
00e0  68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74  html+xml ,text/ht
00f0  6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c  ml;q=0.9 ,text/pl
0100  61 69 6e 3b 71 3d 30 2e 38 2c 76 69 64 65 6f 2f  ain;q=0.8,video/
0110  78 2d 6d 6e 67 2c 69 6d 61 67 65 2f 70 6e 67 2c  x-mng,im age/png,
0120  69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67 65  image/jp eg,image
0130  2f 67 69 66 3b 71 3d 30 2e 32 2c 2a 2f 2a 3b 71  /gif;q=0.2,*/*;q

```

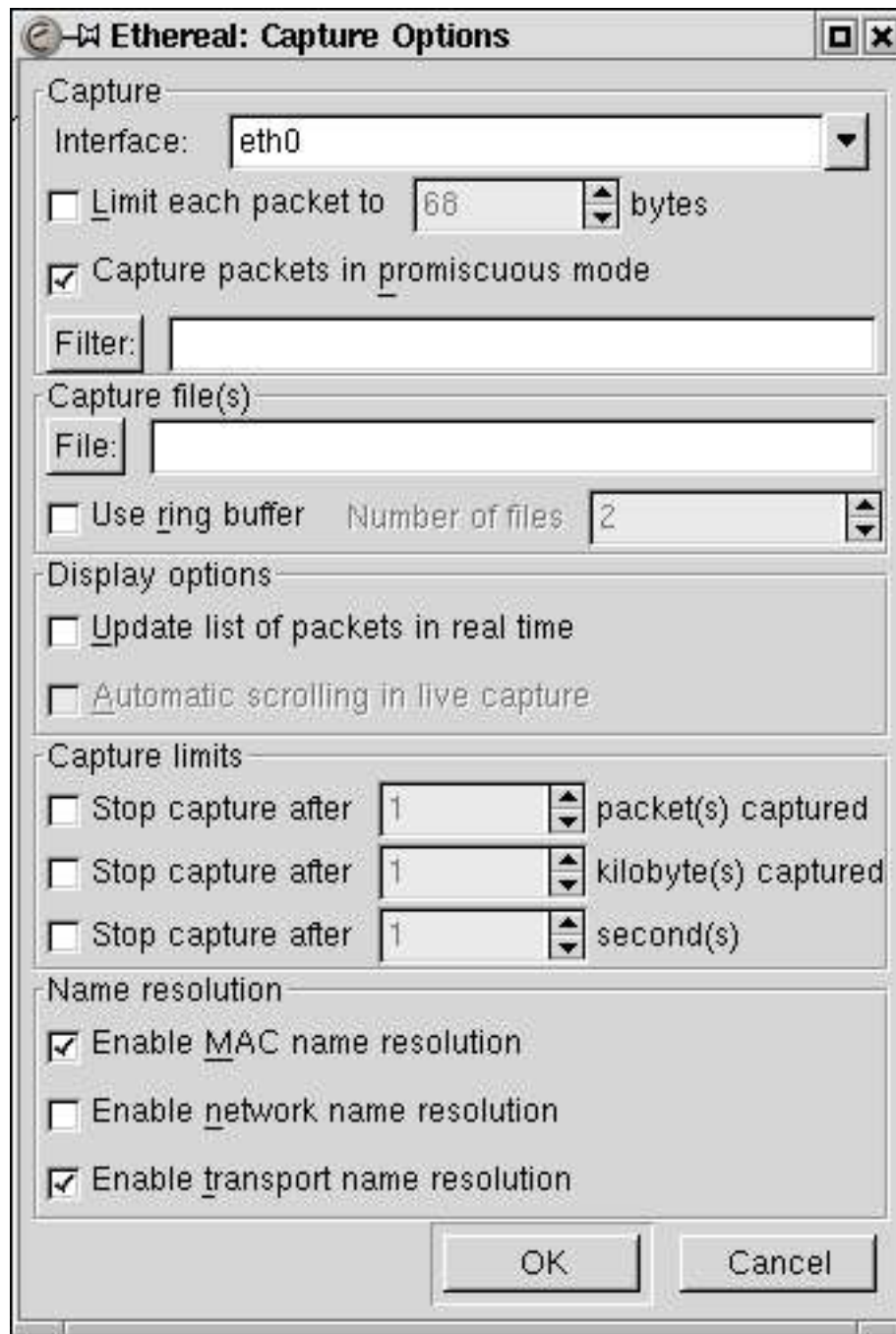
Filter: [ ] [Reset] [Apply] File: <capture> Drops: 0

→ 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

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.106	66.35.250.150	TCP	33016 > http [SYN] Seq=4023883317 Ack=0 Win=5840 Len=0
2	0.353291	00:06:25:df:a7:33	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.106? Tell 192.168.1.1
3	0.353343	aa:aa:03:00:00:00	00:06:25:df:a7:33	ARP	192.168.1.106 is at 00:09:5b:3b:1c:06
4	0.356833	66.35.250.150	192.168.1.106	TCP	http > 33016 [SYN, ACK] Seq=735242465 Ack=4023883318 Win=5792 Len=0
5	0.356894	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883318 Ack=735242466 Win=5840 Len=0
6	0.357970	192.168.1.106	66.35.250.150	HTTP	GET / HTTP/1.1
7	0.457081	66.35.250.150	192.168.1.106	TCP	http > 33016 [ACK] Seq=735242466 Ack=4023883733 Win=6432 Len=0
8	0.554610	66.35.250.150	192.168.1.106	HTTP	HTTP/1.1 200 OK
9	0.554679	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735243914 Win=8688 Len=0
10	0.572447	66.35.250.150	192.168.1.106	HTTP	Continuation
11	0.572549	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735245362 Win=11584 Len=0
12	0.652189	66.35.250.150	192.168.1.106	HTTP	Continuation
13	0.652278	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735246810 Win=14480 Len=0
14	0.675335	192.168.1.106	66.35.250.124	TCP	33017 > http [SYN] Seq=4027886299 Ack=0 Win=5840 Len=0
15	0.705545	66.35.250.150	192.168.1.106	HTTP	Continuation
16	0.705615	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735248258 Win=17376 Len=0
17	0.773811	66.35.250.150	192.168.1.106	HTTP	Continuation

Frame 8 (1514 bytes on wire, 1514 bytes captured)  
 Ethernet II, Src: 00:06:25:df:a7:33, Dst: 00:09:5b:3b:1c:06  
 Internet Protocol, Src Addr: 66.35.250.150 (66.35.250.150), Dst Addr: 192.168.1.106 (192.168.1.106)  
 Transmission Control Protocol, Src Port: http (80), Dst Port: 33016 (33016), Seq: 735242466, Ack: 4023883733, Len: 1448  
 Hypertext Transfer Protocol

```

0040 d4 f2 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 68 HTTP/1.1 200 O
0050 4b 0d 0a 44 61 74 65 3a 20 53 61 74 2c 20 30 31 K.,Date: Sat, 01
0060 20 4e 6f 76 20 32 30 30 33 20 30 31 3a 34 37 3a Nov 2003 01:47:
0070 34 31 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 GMT., Server:
0080 41 70 61 63 68 65 2f 31 2e 33 2e 32 38 20 28 55 Apache/1.3.28 (U
0090 5e 69 78 29 20 6d 6f 64 5f 67 7a 69 70 2f 31 2e nix) mod_gzip/1.
00a0 33 2e 32 36 2e 31 61 20 6d 6f 64 5f 70 65 72 6c 3.26.1a mod_perl
00b0 2f 31 2e 32 38 0d 0a 53 4c 41 53 48 5f 4c 4f 47 /1.28.,S LASH_LOG
00c0 5f 44 41 54 41 3a 20 73 68 74 6d 6c 0d 0a 58 2d _LATA: s html.,X-
00d0 50 6f 77 65 72 65 64 2d 42 79 3a 20 53 6c 61 73 Powered- By: Sias
00e0 68 20 32 2e 30 30 33 30 30 30 0d 0a 58 2d 42 65 h 2,0030 00.,X-Be
00f0 5e 64 65 72 3a 20 43 75 72 73 65 20 6d 79 20 6e nder: Cu rse my n
0100 61 74 75 72 61 6c 20 73 68 6f 77 6d 61 6e 73 68 atural s howmansh
0110 69 70 21 0d 0a 56 61 72 79 3a 20 41 63 63 65 70 ipl.,Var y: Accep
0120 74 2d 45 6e 63 6f 64 69 6e 67 0d 0a 43 61 63 68 t-Encoding.,Cach
0130 65 2d 43 6f 6e 74 72 6f 6c 3a 20 70 72 69 76 61 e-Contro l: priva
0140 74 65 0d 0a 50 72 61 67 6d 61 3a 20 70 72 69 76 te.,Prag ma: priv
0150 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a ate.,Con nection:
0160 20 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e 74 2d close., Content-
0170 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b Type: te xt/html:
  
```

Filter:  Reset Apply Hypertext Transfer Protocol (http), 1448 bytes

Illus-3  
capture with  
payload  
selected  
(http)

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.106	66.35.250.150	TCP	33016 > http [SYN] Seq=4023883317 Ack=0 Win=5840 Len=0
2	0.353291	00:06:25:df:a7:33	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.106? Tell 192.168.1.1
3	0.353343	aa:aa:03:00:00:00	00:06:25:df:a7:33	ARP	192.168.1.106 is at 00:09:5b:3b:1c:06
4	0.356833	66.35.250.150	192.168.1.106	TCP	http > 33016 [SYN, ACK] Seq=735242465 Ack=4023883318 Win=5792 Len=0
5	0.356894	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883318 Ack=735242466 Win=5840 Len=0
6	0.357970	192.168.1.106	66.35.250.150	HTTP	GET / HTTP/1.1
7	0.457081	66.35.250.150	192.168.1.106	TCP	http > 33016 [ACK] Seq=735242466 Ack=4023883733 Win=6432 Len=0
8	0.554610	66.35.250.150	192.168.1.106	HTTP	HTTP/1.1 200 OK
9	0.554679	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735243914 Win=8688 Len=0
10	0.572447	66.35.250.150	192.168.1.106	HTTP	Continuation
11	0.572549	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735245362 Win=11584 Len=0
12	0.652189	66.35.250.150	192.168.1.106	HTTP	Continuation
13	0.652278	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735246810 Win=14480 Len=0
14	0.675335	192.168.1.106	66.35.250.124	TCP	33017 > http [SYN] Seq=4027886299 Ack=0 Win=5840 Len=0
15	0.705545	66.35.250.150	192.168.1.106	HTTP	Continuation
16	0.705615	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883733 Ack=735248258 Win=17376 Len=0
17	0.773811	66.35.250.150	192.168.1.106	HTTP	Continuation

Frame 6 (481 bytes on wire, 481 bytes captured)

- Ethernet II, Src: aa:aa:03:00:00:00, Dst: 00:06:25:df:a7:33
- Internet Protocol, Src Addr: 192.168.1.106 (192.168.1.106), Dst Addr: 66.35.250.150 (66.35.250.150)
- Transmission Control Protocol, Src Port: 33016 (33016), Dst Port: http (80), Seq: 4023883318, Ack: 735242466, Len: 415
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n
  - Host: slashdot.org\r\n
  - User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4) Gecko/20030624\r\n
  - Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,\*/\*;q=0.1\r\n
  - Accept-Language: en-us,en;q=0.5\r\n
  - Accept-Encoding: gzip,deflate\r\n
  - Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n
  - Keep-Alive: 300\r\n
  - Connection: keep-alive\r\n
  - \r\n

```

0000 00 06 25 df a7 33 aa aa 03 00 00 00 08 00 45 00  ..%833@a .....E.
0010 01 d3 42 fd 40 00 40 06 f7 5b c0 a8 01 6a 42 23  .oBy@.@. +[A".jB#
0020 fa 96 80 f8 00 50 ef d7 96 36 2b d2 e8 e2 80 18  ú..ø.Pi× .6+0èä..
0030 16 d0 ac 84 00 00 01 01 08 0a 00 01 d4 f2 1e 6b  .B-..... ....ôð.k
0040 2e 5d 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  .JGET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 73 6c 61 73 68 64 6f 74  ..Host: slashdot
0060 2e 6f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74  .org..Us er-Agent
0070 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58  : Mozill a/5.0 (X
0080 31 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38  11; U; L inux i68
0090 36 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 34  6; en-US ; rv:1.4
00a0 29 20 47 65 63 6b 6f 2f 32 30 30 33 30 36 32 34  ) Gecko/ 20030624
  
```

Filter: [ ] [v] [Reset] [Apply] File: <capture> Drops: 0

Illus-4  
note http text

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.106	66.35.250.150	TCP	33016 > http [SYN] Seq=4023883317 Ack=0 Win=5840 Len=0
2	0.353291	00:06:25:df:a7:33	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.106? Tell 192.168.1.1
3	0.353343	aa:aa:03:00:00:00	00:06:25:df:a7:33	ARP	192.168.1.106 is at 00:09:5b:3b:1c:06
4	0.356833	66.35.250.150	192.168.1.106	TCP	http > 33016 [SYN, ACK] Seq=735242465 Ack=4023883318 Win=5792 Len=0
5	0.356894	192.168.1.106	66.35.250.150	TCP	33016 > http [ACK] Seq=4023883318 Ack=735242466 Win=5840 Len=0
6	0.357970	192.168.1.106	66.35.250.150	HTTP	GET / HTTP/1.1
7	0.457081	66.35.250.150	192.168.1.106	TCP	http > 33016 [ACK] Seq=735242466 Ack=4023883733 Win=6432 Len=0
8	0.554610	66.35.250.150	192.168.1.106	HTTP	HTTP/1.1 200 OK

Frame 6 (481 bytes on wire, 481 bytes captured)  
 Ethernet II, Src: aa:aa:03:00:00:00, Dst: 00:06:25:df:a7:33  
 Internet Protocol, Src Addr: 192.168.1.106 (192.168.1.106), Dst Addr: 66.35.250.150 (66.35.250.150)  
 Transmission Control Protocol, Src Port: 33016 (33016), Dst Port: http (80), Seq: 4023883318, Ack: 735242466, Len: 415  
    Source port: 33016 (33016)  
    Destination port: http (80)  
    Sequence number: 4023883318  
    Next sequence number: 4023883733  
    Acknowledgement number: 735242466  
    Header length: 32 bytes  
 Flags: 0x0018 (PSH, ACK)  
    0... .... = Congestion Window Reduced (CWR): Not set  
    .0.. .... = ECN-Echo: Not set  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 1... = Push: Set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
    Window size: 5840  
    Checksum: 0xac84 (correct)  
 Options: (12 bytes)  
 Hypertext Transfer Protocol  
 GET / HTTP/1.1\r\n  
    Host: slashdot.org\r\n  
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4) Gecko/20030624\r\n  
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,\*/\*;q=0.1\r\n  
    Accept-Language: en-us,en;q=0.5\r\n  
    Accept-Encoding: gzip,deflate\r\n  
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n

```

0020 fa 96 80 f8 00 50 ef d7 96 36 2b d2 e8 e2 80 18  ú..ø.Pi× .6+0èà..
0030 16 d0 ac 84 00 00 01 01 08 0a 00 01 d4 f2 1e 6b  .#~..... ..0ò.k
0040 2e 5d 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  .]GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 73 6c 61 73 68 64 6f 74  ..Host: slashdot
0060 2e 6f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74  .org..Us er-Agent

```

Filter:    Acknowledgement number (tcp.ack), 4 bytes

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](http://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`

Sequence number[B]

90000  
80000  
70000  
60000  
50000  
40000  
30000  
20000  
10000

Graph 1 - Control - Ethereal

Zoom Magnify Origin Cross Graph type

Graph type:

- Time/Sequence (tcptrace-style)
- Time/Sequence (Stevens'-style)
- Throughput
- Round-trip Time

Init on change

Help Close

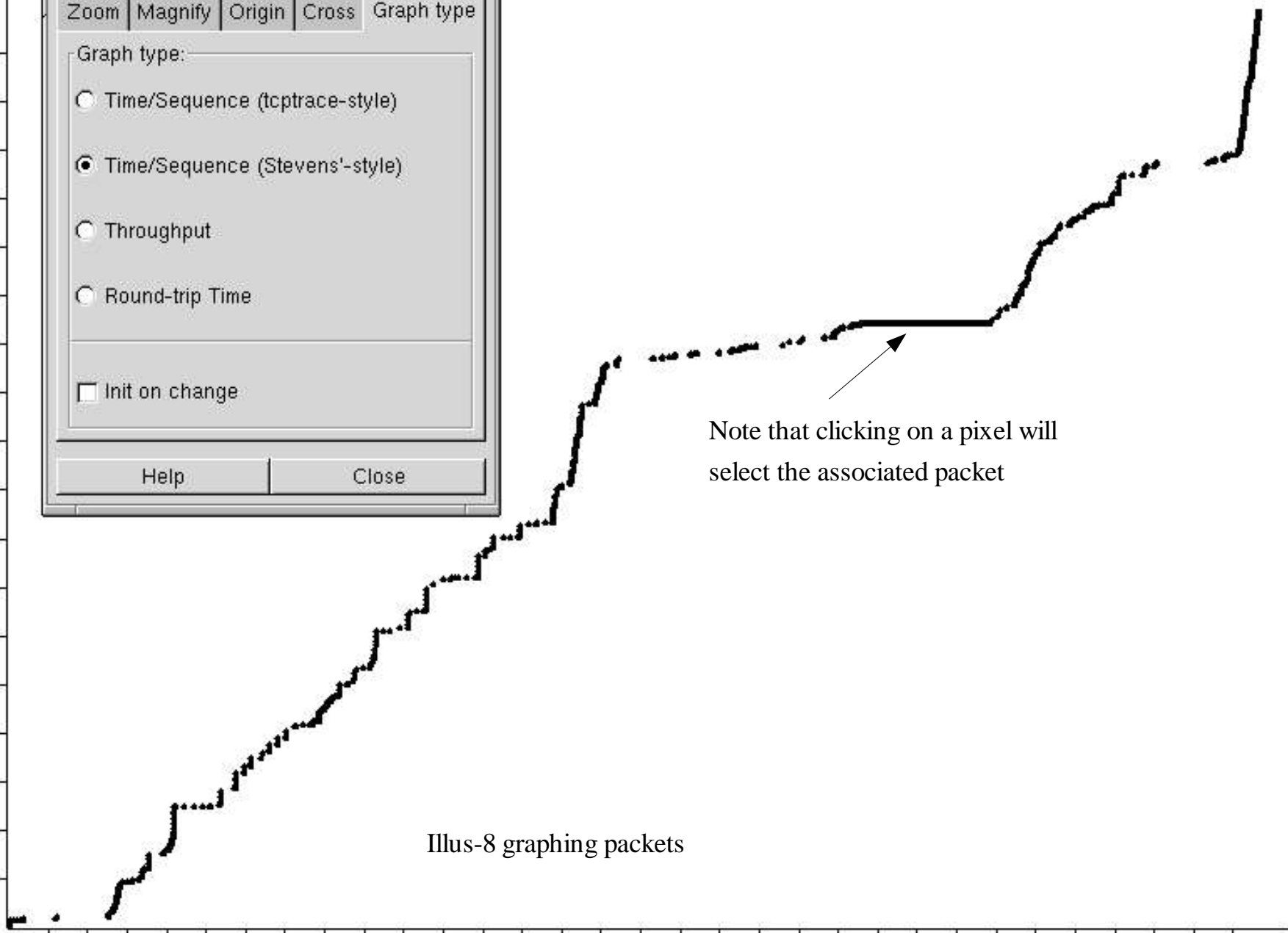
Time/Sequence Graph

5 10 15 20 25 30

Time[s]

Note that clicking on a pixel will select the associated packet

Illus-8 graphing packets



Protocol Hierarchy Statistics

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

Close

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](http://omniorb.sourceforge.net) (some/all?)
- `export PYTHONPATH=/usr/lib/python1.5/`
- concatenate 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 Ethereum Plugin Generator

# links

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