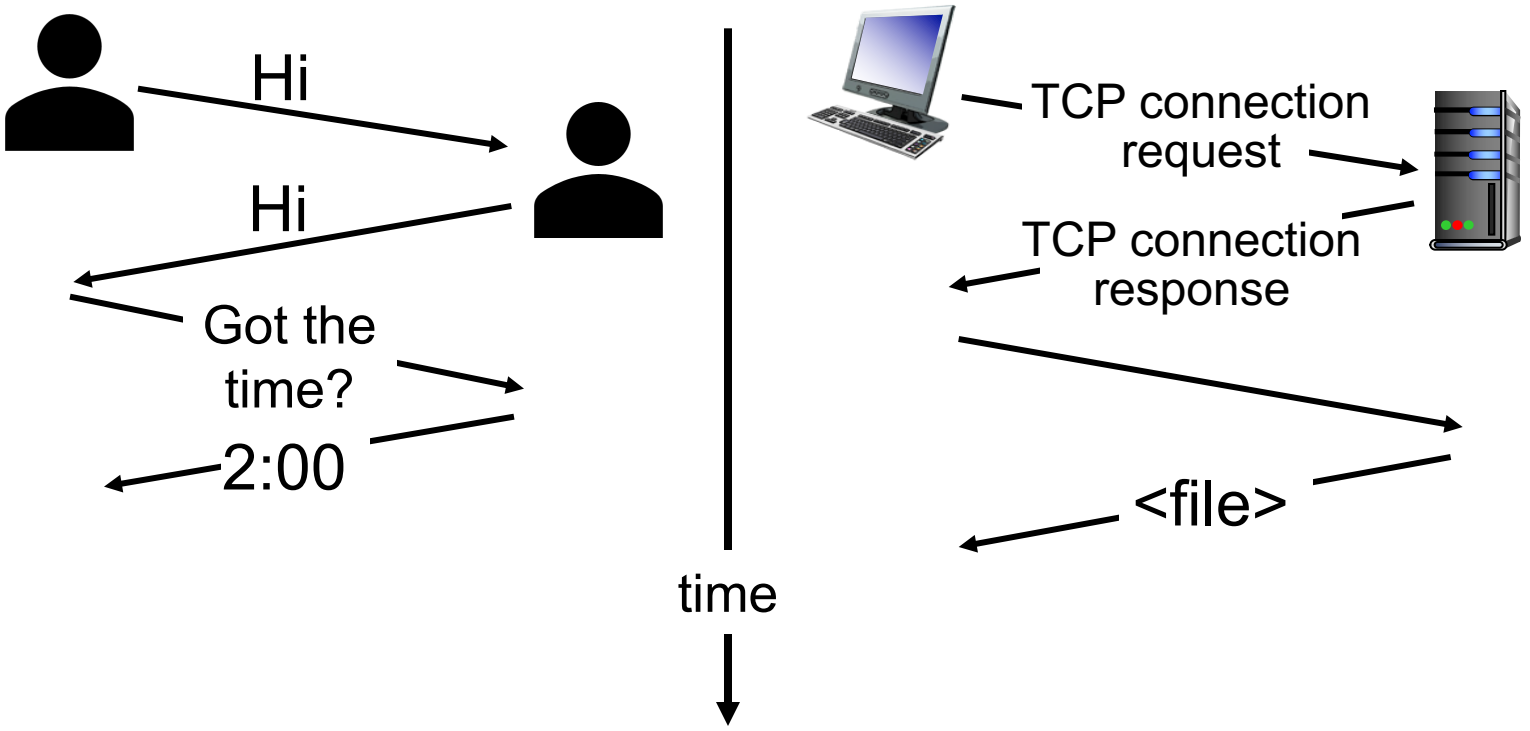
Protocol Layers & Wireshark

TDTS11:COMPUTER NETWORKS AND INTERNET PROTOCOLS

Mail

seban649@student.liu.se

Protocol


Hi
Hi
Got the time?
2:00
time
TCP connection request
TCP connection response
<file>

Whats the internet: ”nuts and bolts”

Millions of connected computing devices:

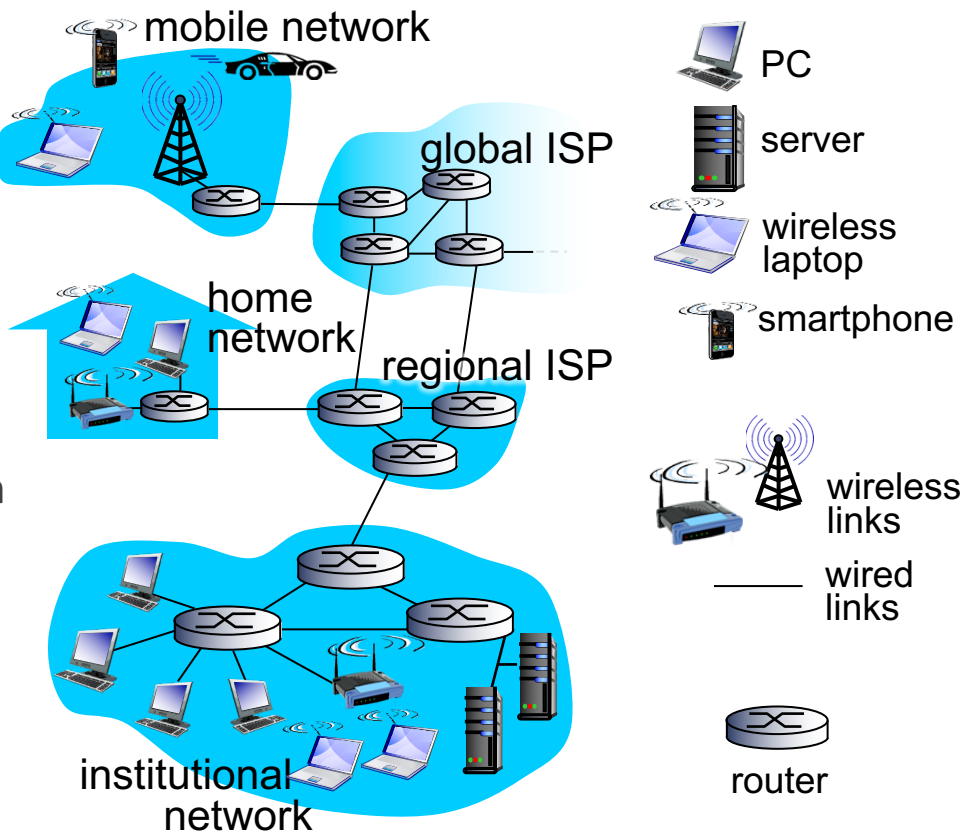
- **Hosts** = **end systems**
- Running **network apps**

Communication links

- Fiber, copper, radio, satellite
- Transmission rate: bandwidth

Packet switches: forward packets (chunks of data)

- **Routers** and **switches**



Whats the internet: ”nuts and bolts”

Millions of connected computing devices:

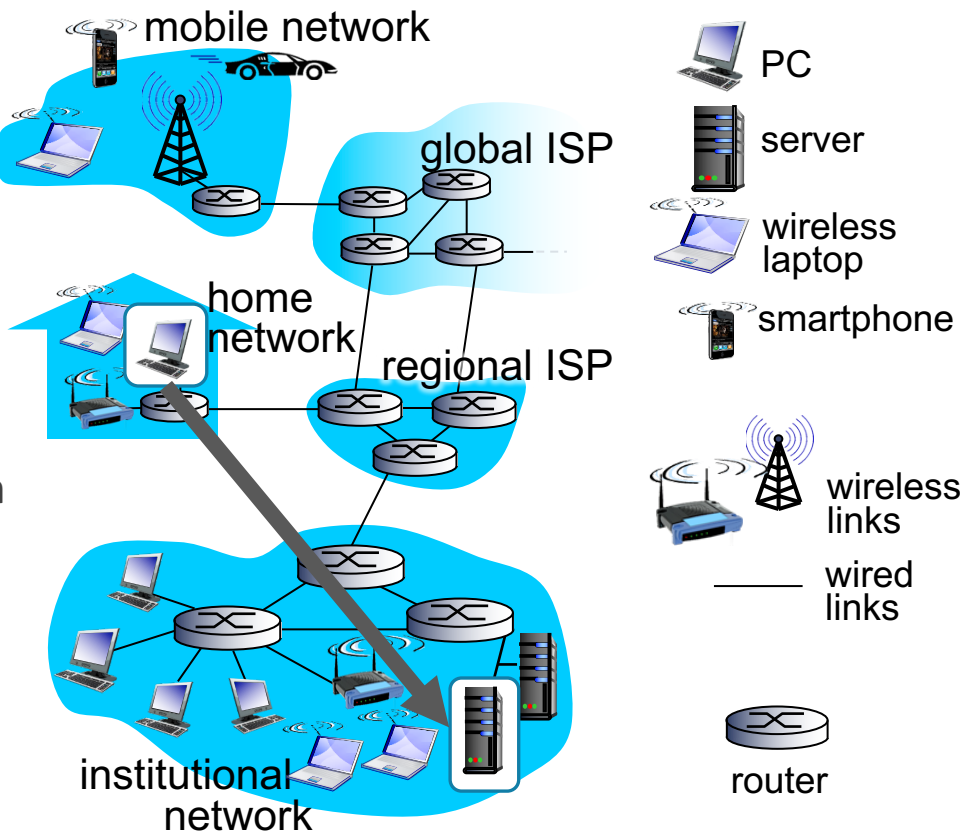
- **Hosts** = **end systems**
- Running **network apps**

Communication links

- Fiber, copper, radio, satellite
- Transmission rate: bandwidth

Packet switches: forward packets (chunks of data)

- **Routers** and **switches**



Whats the internet: ”nuts and bolts”

Millions of connected computing devices:

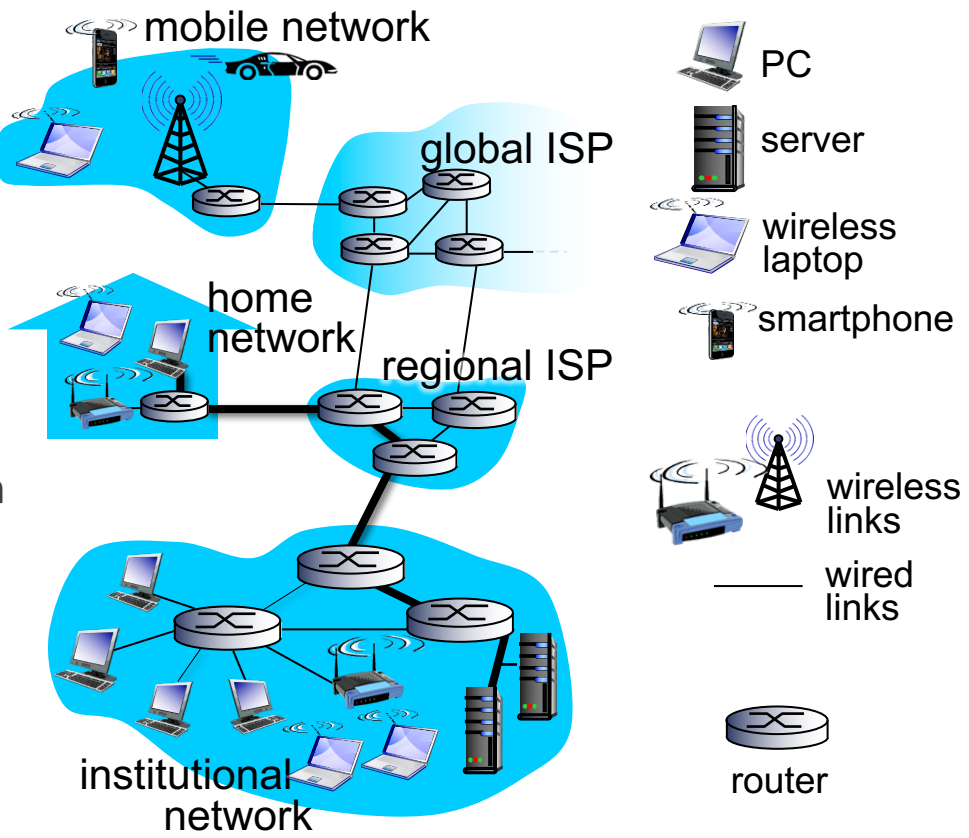
- **Hosts** = **end systems**
- Running **network apps**

Communication links

- Fiber, copper, radio, satellite
- Transmission rate: bandwidth

Packet switches: forward packets (chunks of data)

- **Routers** and **switches**



Whats the internet: ”nuts and bolts”

Millions of connected computing devices:

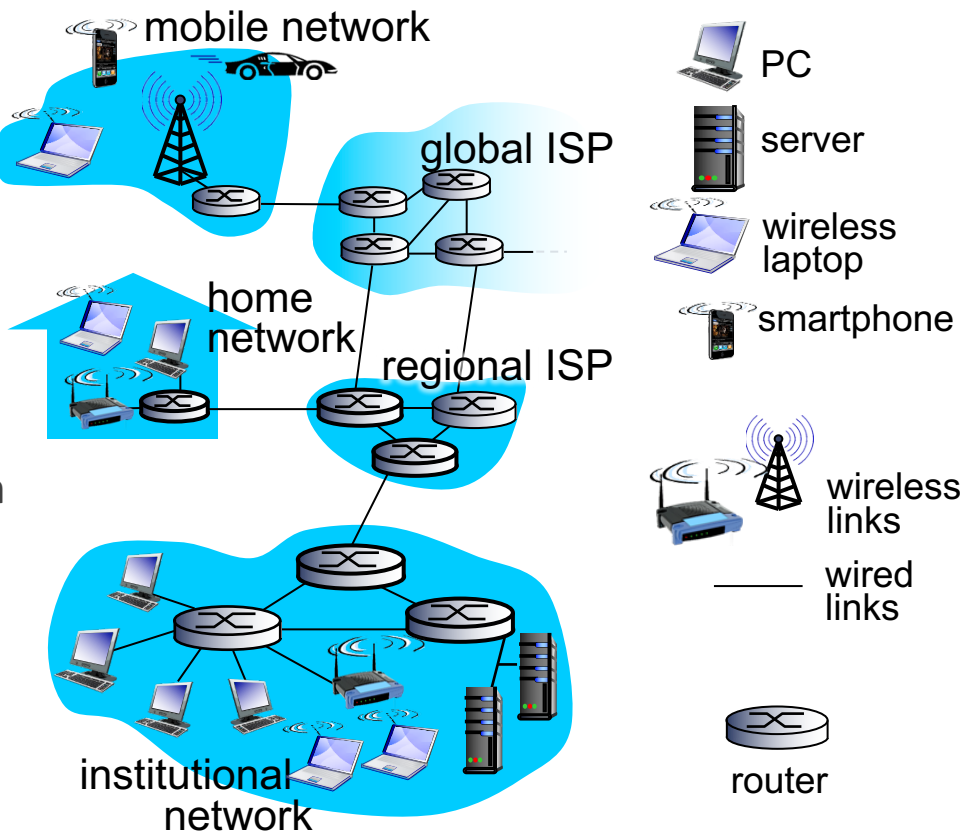
- **Hosts** = **end systems**
- Running **network apps**

Communication links

- Fiber, copper, radio, satellite
- Transmission rate: bandwidth

Packet switches: forward packets (chunks of data)

- **Routers** and **switches**



Internet protocol stack

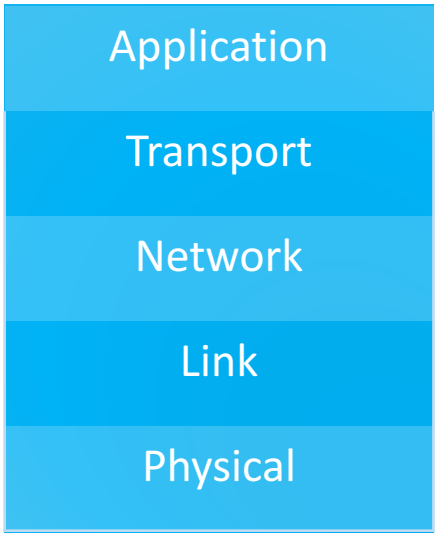
Application: supporting network applications
- FTP, SMTP, HTTP

Transport: process-process data transfer
- TCP, UDP

Network: routing of datagrams from source to destination
- IP, routing protocols

Link: data transfer between neighboring network elements
- Ethernet, 802.111 (WiFi), PPP

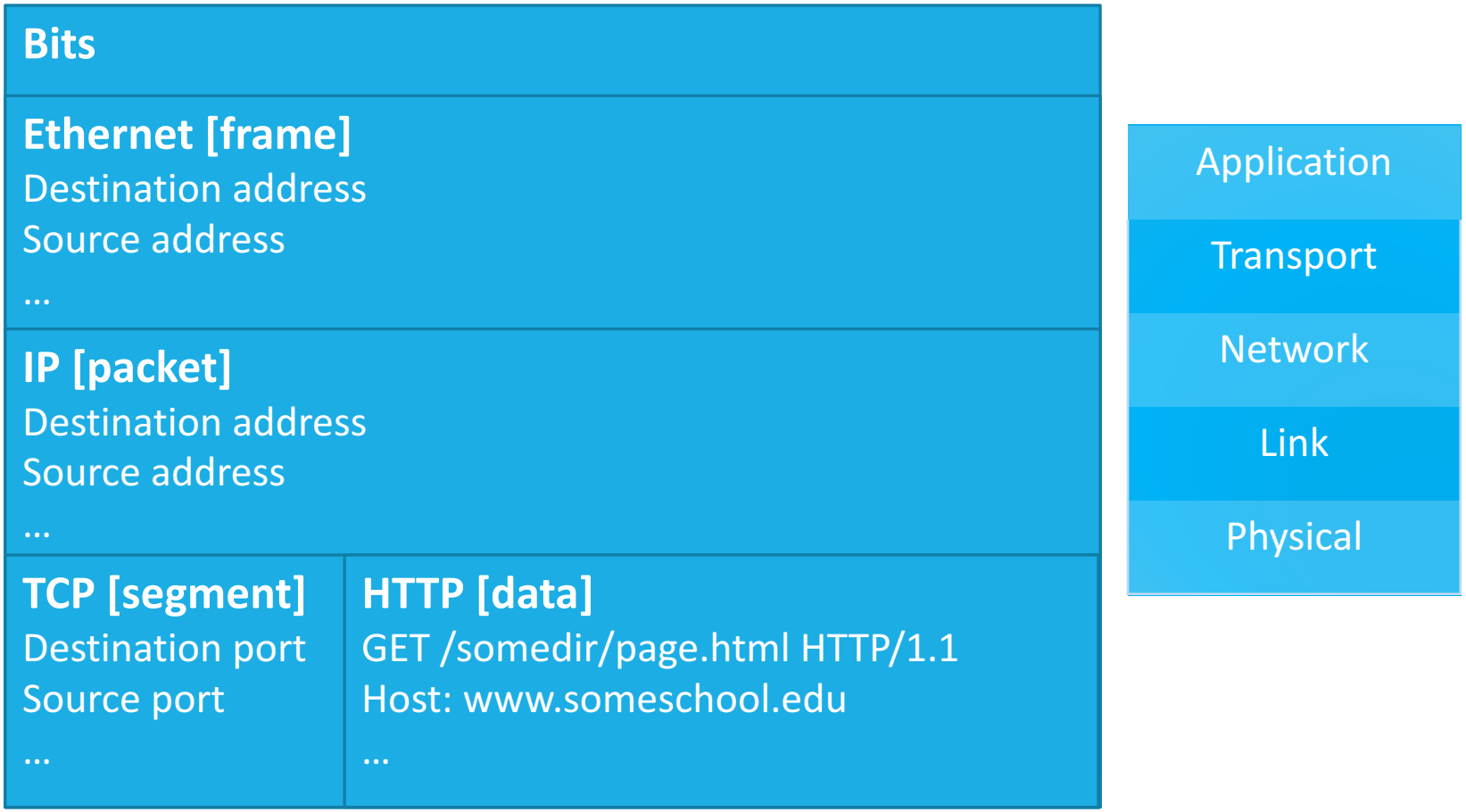
Physical: bits “on the wire”



Encapsulation

HTTP [data]
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
…

Encapsulation

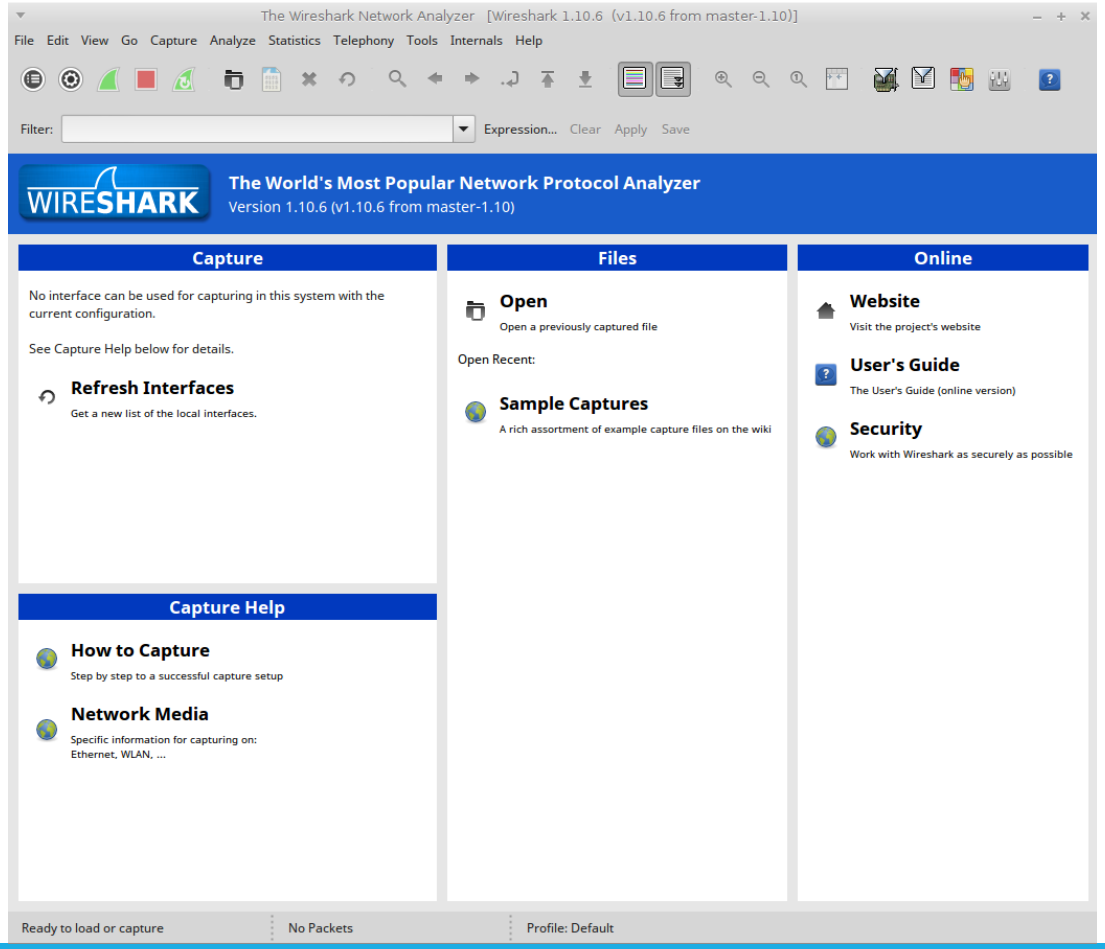


Wireshark

Packet analyzer

Capture and view network packages

Start screen of Wireshark



Wireshark's GUI

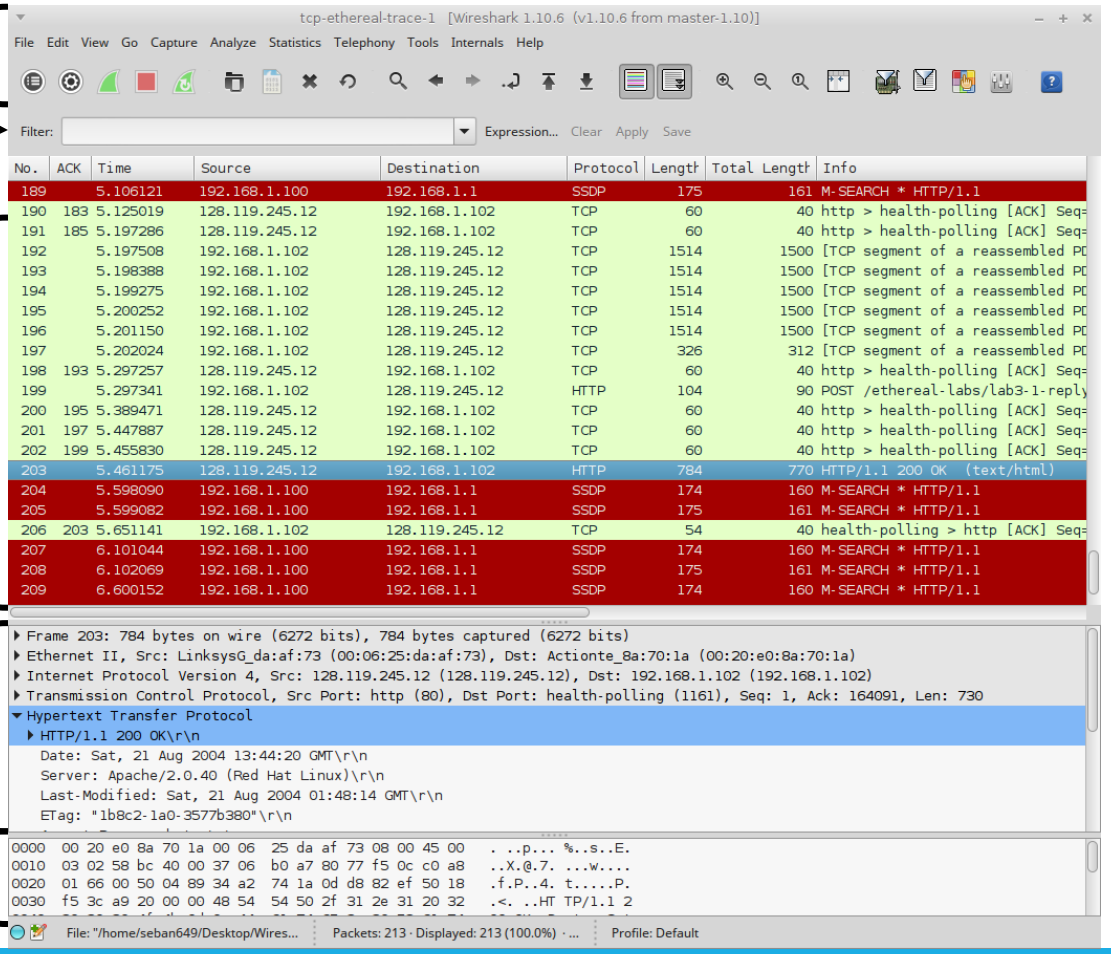
Menu

Display filter

Listing of captured packets

Details of selected packet header

Packet content in hexadecimal and ASCII



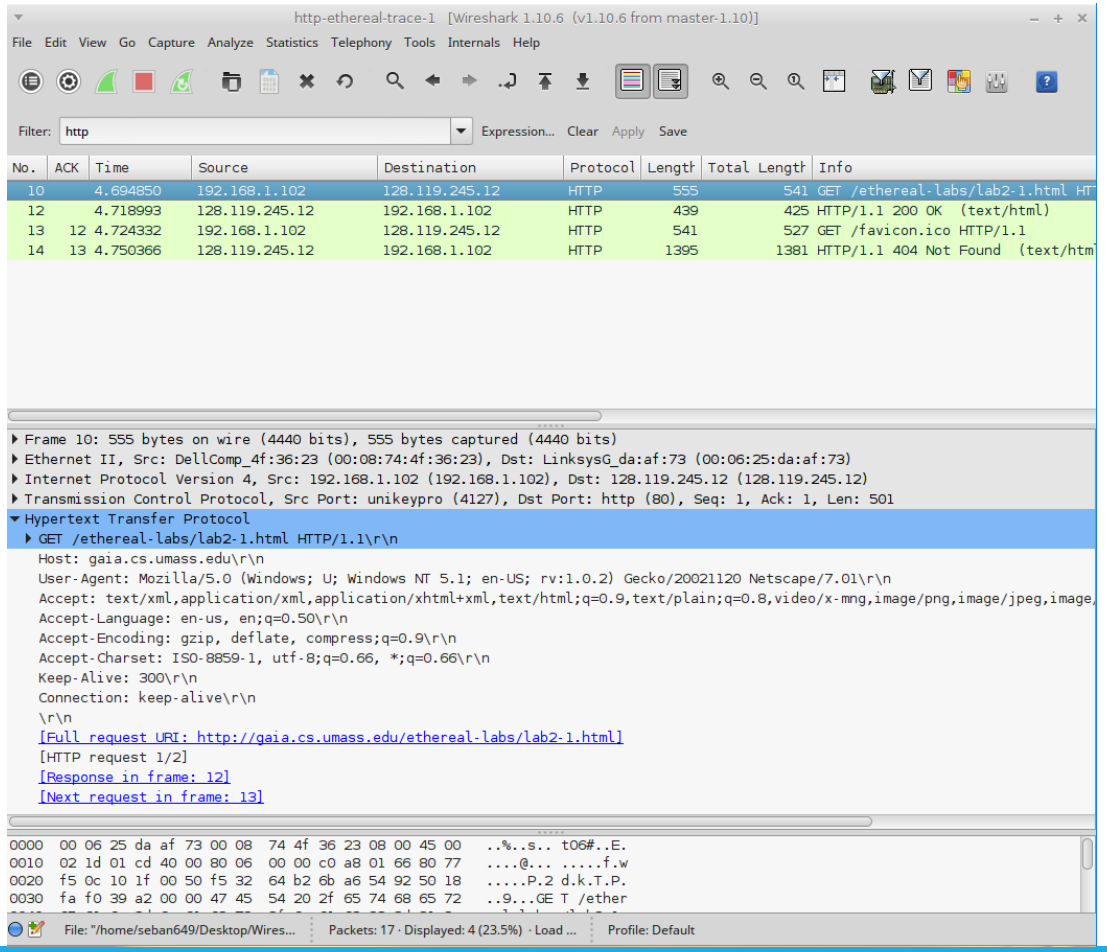
Example

HTTP
- Request type

TCP
- Port

IP
- IP Address

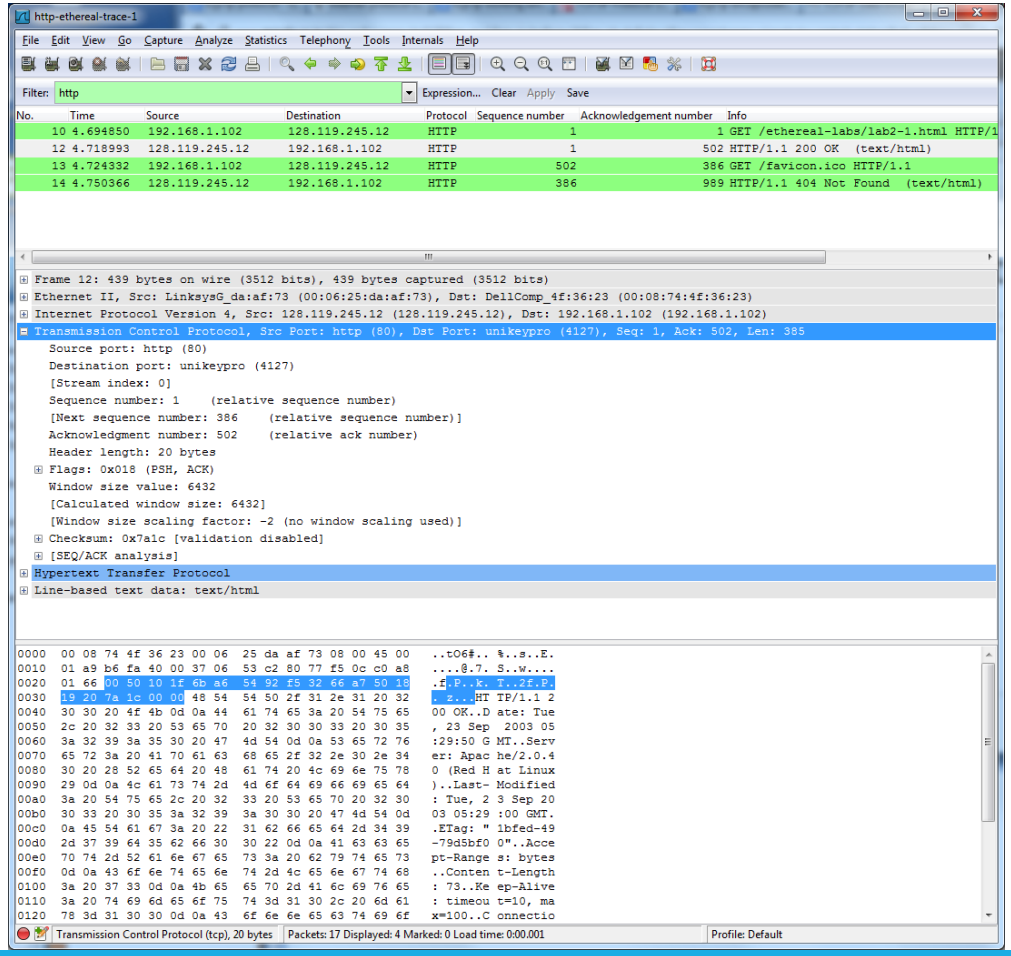
Ethernet
- MAC Address



TCP Headers

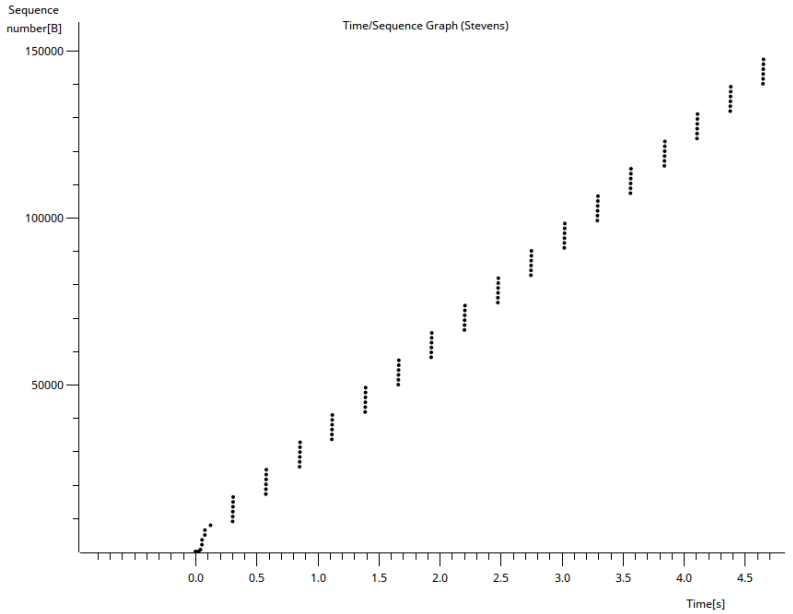
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

TCP Header


http-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol Sequence number Acknowledgement number Info
10 4.694850 192.168.1.102 128.119.245.12 HTTP 1 1 GET /ethereal-labs/lab2-1.html HTTP/1
12 4.718993 128.119.245.12 192.168.1.102 HTTP 1 502 HTTP/1.1 200 OK (text/html)
13 4.724332 192.168.1.102 128.119.245.12 HTTP 502 386 GET /favicon.ico HTTP/1.1
14 4.750366 128.119.245.12 192.168.1.102 HTTP 386 989 HTTP/1.1 404 Not Found (text/html)
Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: unikeypro (4127), Seq: 1, Ack: 502, Len: 385
Source port: http (80)
Destination port: unikeypro (4127)
[Stream index: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 386 (relative sequence number)]
Acknowledgment number: 502 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 6432
[Calculated window size: 6432]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x7a1c [validation disabled]
[SEQ/ACK analysis]
Hypertext Transfer Protocol
Line-based text data: text/html
0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ..tO6#.. %..s..E.
0010 01 a9 b6 fa 40 00 37 06 53 c2 80 77 f5 0c c0 a8 ....@.7. S..w....
0020 01 66 00 50 10 1f 6b a6 54 92 f5 32 66 a7 50 18 .f.P..k. T..2f.P.
0030 19 20 7a 1c 00 00 48 54 54 50 2f 31 2e 31 20 32 . z...HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK..D ate: Tue
0050 2c 20 32 33 20 53 65 70 20 32 30 30 33 20 30 35 , 23 Sep 2003 05
0060 3a 32 39 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76 :29:50 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4
0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux
0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)..Last- Modified
00a0 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30 : Tue, 2 3 Sep 20
00b0 30 33 20 30 35 3a 32 39 3a 30 30 20 47 4d 54 0d 03 05:29 :00 GMT.
00c0 0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39 .ETag: " 1bfed-49
00d0 2d 37 39 64 35 62 66 30 30 22 0d 0a 41 63 63 65 -79d5bf0 0"..Acce
00e0 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 pt-Range s: bytes
00f0 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 ..Conten t-Length
0100 3a 20 37 33 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 : 73..Ke ep-Alive
0110 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61 : timeou t=10, ma
0120 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f x=100..C onnectio
Transmission Control Protocol (tcp), 20 bytes
Packets: 17 Displayed: 4 Marked: 0 Load time: 0:00.001
Profile: Default

TCP Time-Sequence Graph

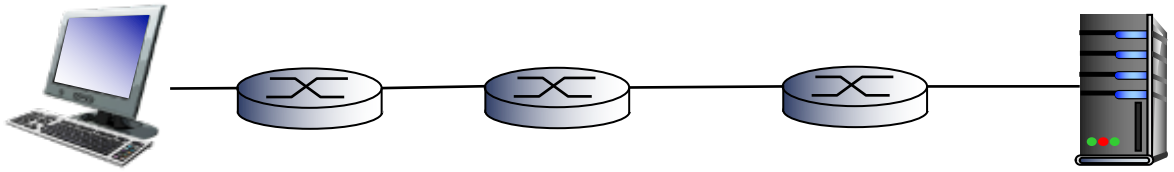
1. Open trace file
2. Filter by entering *tcp*
3. Select tcp segement
4. Choose:
   Statistics->
   TCP Stream Graph->
   Time-Sequnce Graph (Stevens)



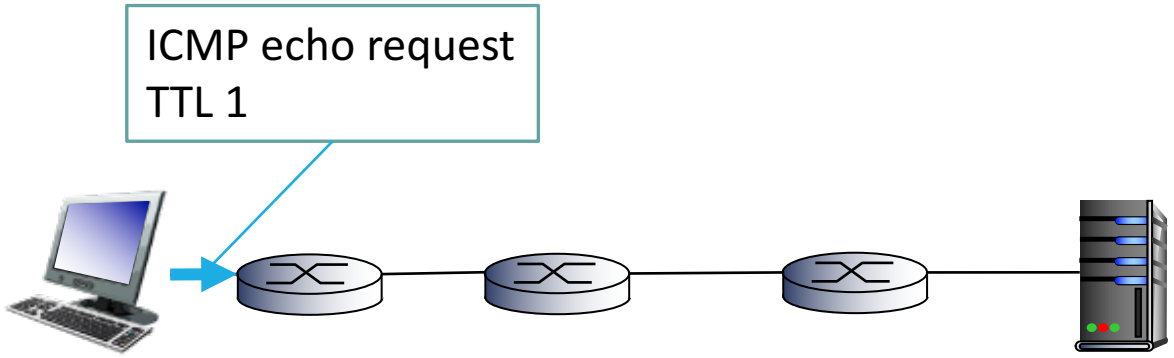
IP Headers

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

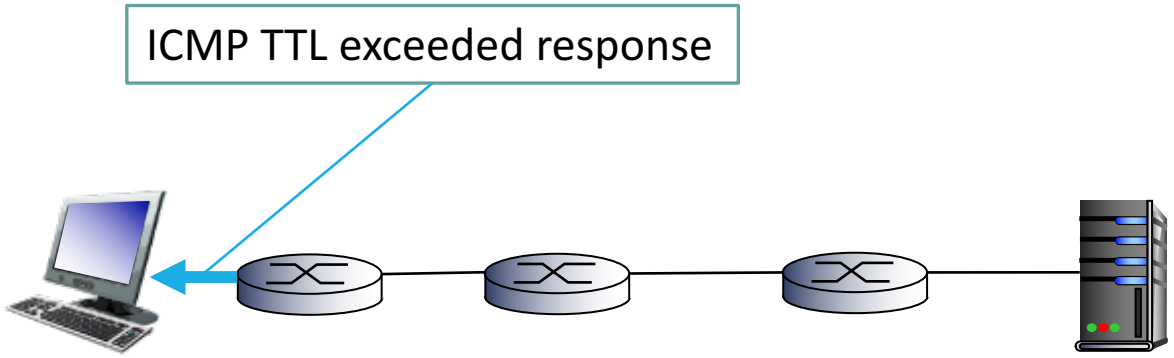
Traceroute



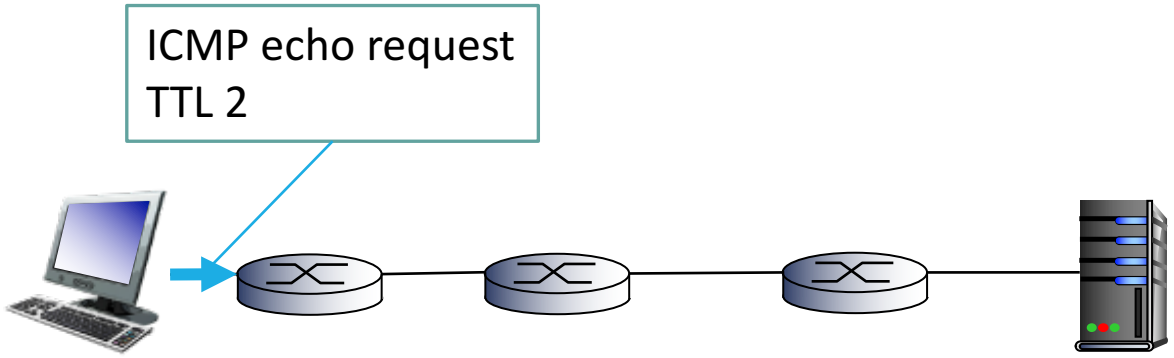
Traceroute



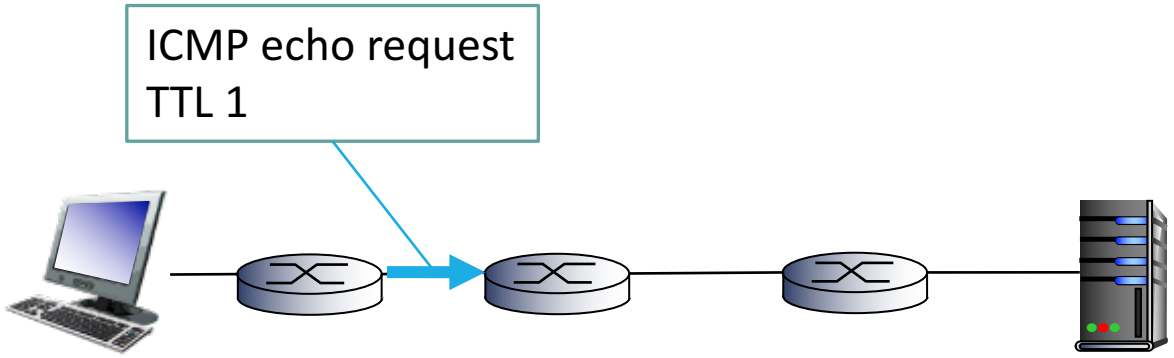
Traceroute



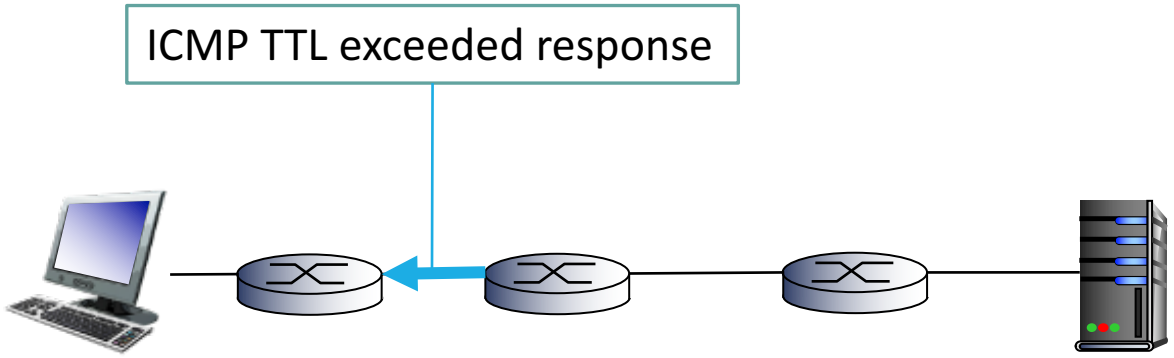
Traceroute



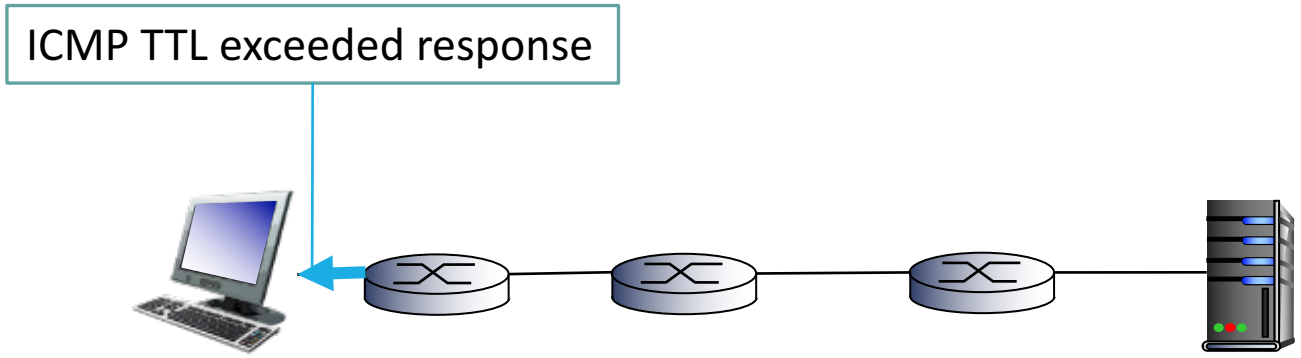
Traceroute



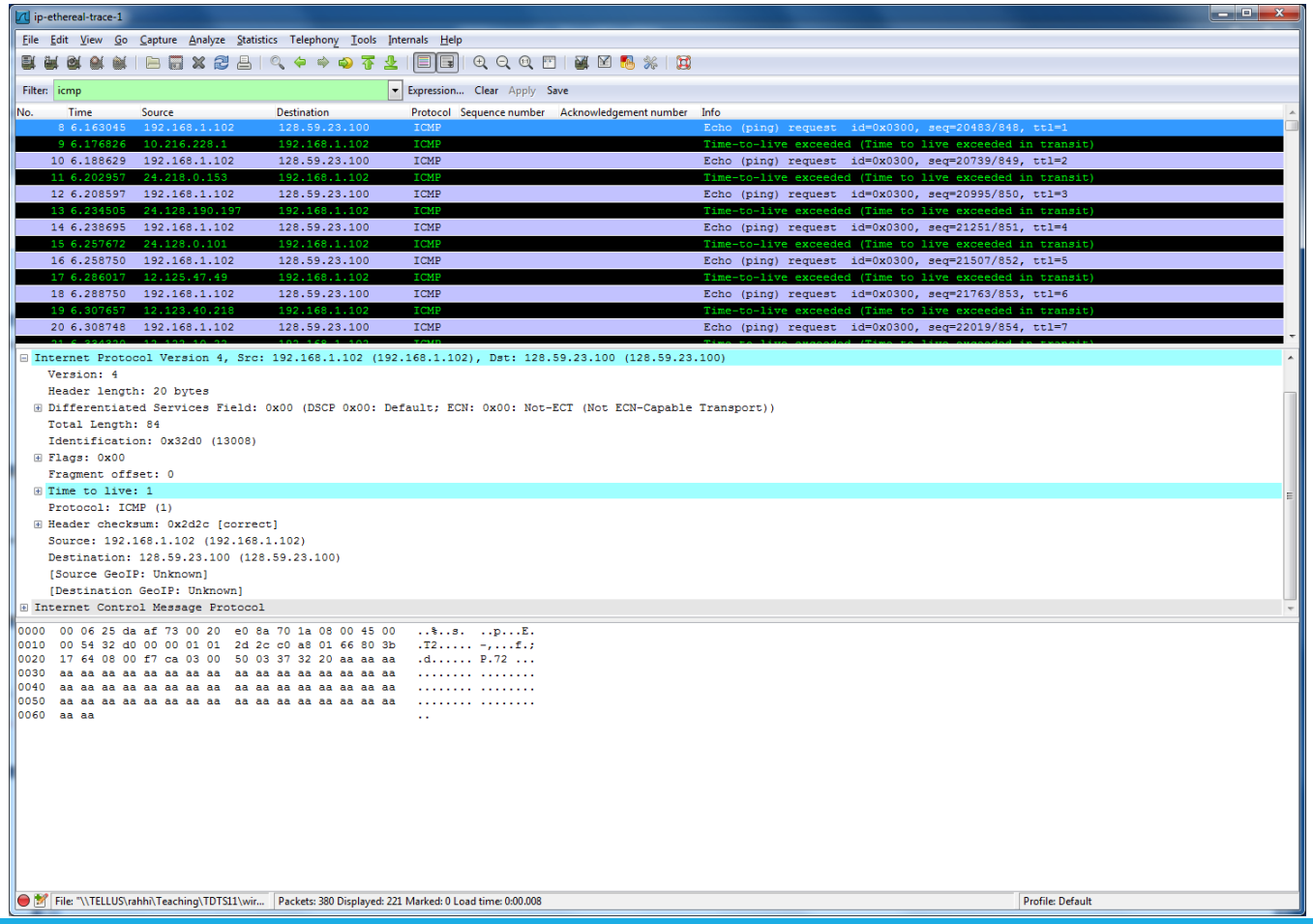
Traceroute



Traceroute



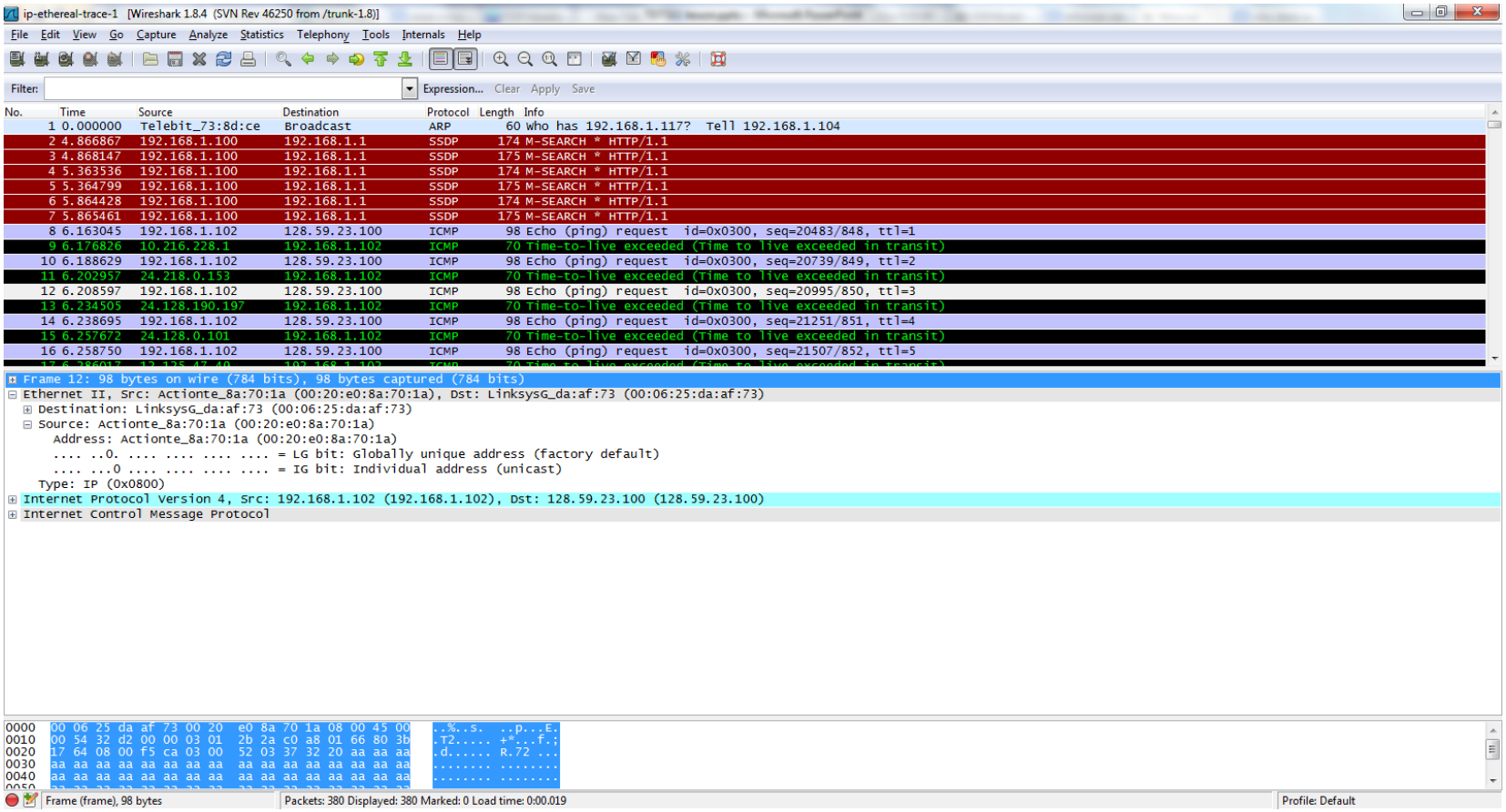
IP Headers


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply Save
No. Time Source Destination Protocol Sequence number Acknowledgement number Info
8 6.163045 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=20483/848, ttl=1
9 6.176826 10.216.228.1 192.168.1.102 ICMP Time-to-live exceeded (Time to live exceeded in transit)
10 6.188629 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=20739/849, ttl=2
11 6.202957 24.218.0.153 192.168.1.102 ICMP Time-to-live exceeded (Time to live exceeded in transit)
12 6.208597 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=20995/850, ttl=3
13 6.234505 24.128.190.197 192.168.1.102 ICMP Time-to-live exceeded (Time to live exceeded in transit)
14 6.238695 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=21251/851, ttl=4
15 6.257672 24.128.0.101 192.168.1.102 ICMP Time-to-live exceeded (Time to live exceeded in transit)
16 6.258750 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=21507/852, ttl=5
17 6.286017 12.125.47.49 192.168.1.102 ICMP Time-to-live exceeded (Time to live exceeded in transit)
18 6.288750 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=21763/853, ttl=6
19 6.307657 12.123.40.218 192.168.1.102 ICMP Time-to-live exceeded (Time to live exceeded in transit)
20 6.308748 192.168.1.102 128.59.23.100 ICMP Echo (ping) request id=0x0300, seq=22019/854, ttl=7
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 84
Identification: 0x32d0 (13008)
Flags: 0x00
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2d2c [correct]
Source: 192.168.1.102 (192.168.1.102)
Destination: 128.59.23.100 (128.59.23.100)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%..s. ..p...E.
0010 00 54 32 d0 00 00 01 01 2d 2c c0 a8 01 66 80 3b .T2..... -,...f.;
0020 17 64 08 00 f7 ca 03 00 50 03 37 32 20 aa aa aa .d...... P.72 ...
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0060 aa aa ..
File: "\\TELLUS\rahhi\Teaching\TDTS11\wir... Packets: 380 Displayed: 221 Marked: 0 Load time: 0:00.008
Profile: Default

Ethernet Headers & Trailers

Layer	Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46–1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64(68)–1518(1522) octets →						
Layer 1 Ethernet packet & IPG	← 72(76)–1526(1530) octets →								← 12 oct. →

Ethernet Headers & Trailers



Handy things

- Mark packets: ctrl + M (“selects” packets)
- Disable checksum error coloring from:
  - Views->Coloring rules
- Apply filter by right clicking the value from an item and select:
  - Apply as Filter->Selected

Assignments

Assignment 1: "Wireshark lab: Getting started + HTTP" (1+ time slot, plus own work…)

- Two parts: **wireshark** and **questions**

Assignment 2: "Wireshark lab: TCP" (1+ time slots, plus own work…)

- Two parts: **wireshark** and **questions**

Assignment 3: "Wireshark lab: IP" (1+ time slot, plus own work…)

- Two parts: **wireshark** and **questions**

Assignment 4: "Web analysis" (4+ to 5+ time slots, plus own work…)

Questions