

Bryan Arnold

CSE 3300

10/24/18

Programming Assignment 2

Part 1: UDP

- 1) There is a total of 4 headers in this UDP packet: Source Port, Destination Port, Length, and Checksum:

The image shows a Wireshark packet capture of a network interface. The filter is set to 'udp'. The packet list shows several UDP packets. The selected packet is packet 8, which is a UDP packet from 137.99.81.214 to 172.217.6.206, length 1074, len=1032. The packet details pane shows the following structure:

- Frame 8: 1074 bytes on wire (8592 bits), 1074 bytes captured (8592 bits) on interface 0
- Ethernet II, Src: AsustekC_3f:a4:6d (ac:9e:17:3f:a4:6d), Dst: Cisco1c:f2:80 (00:26:ca:1c:f2:80)
- Internet Protocol Version 4, Src: 137.99.81.214, Dst: 172.217.6.206
- User Datagram Protocol, Src Port: 62767, Dst Port: 443
- Source Port: 62767
- Destination Port: 443
- Length: 1040
- Checksum: 0xb5f1 [unverified]
- [Checksum status: unverified]
- [Stream index: 0]
- Data (1032 bytes)
- Data: 0cf0d75dd83fc0e0230e1b0e2574f513c2f2434dbf25411a...
- [Length: 1032]

Handwritten red annotations are present:

- A red circle is drawn around the 'User Datagram Protocol' section in the packet details pane.
- A red arrow points from the text 'UDP Headers' to the circled section.
- The text 'UDP Headers' is written in red cursive script.

The packet bytes pane shows the raw data of the packet, with the first 8 bytes (0020 06 ce 15 2f 01 bb 04 10) highlighted in blue.

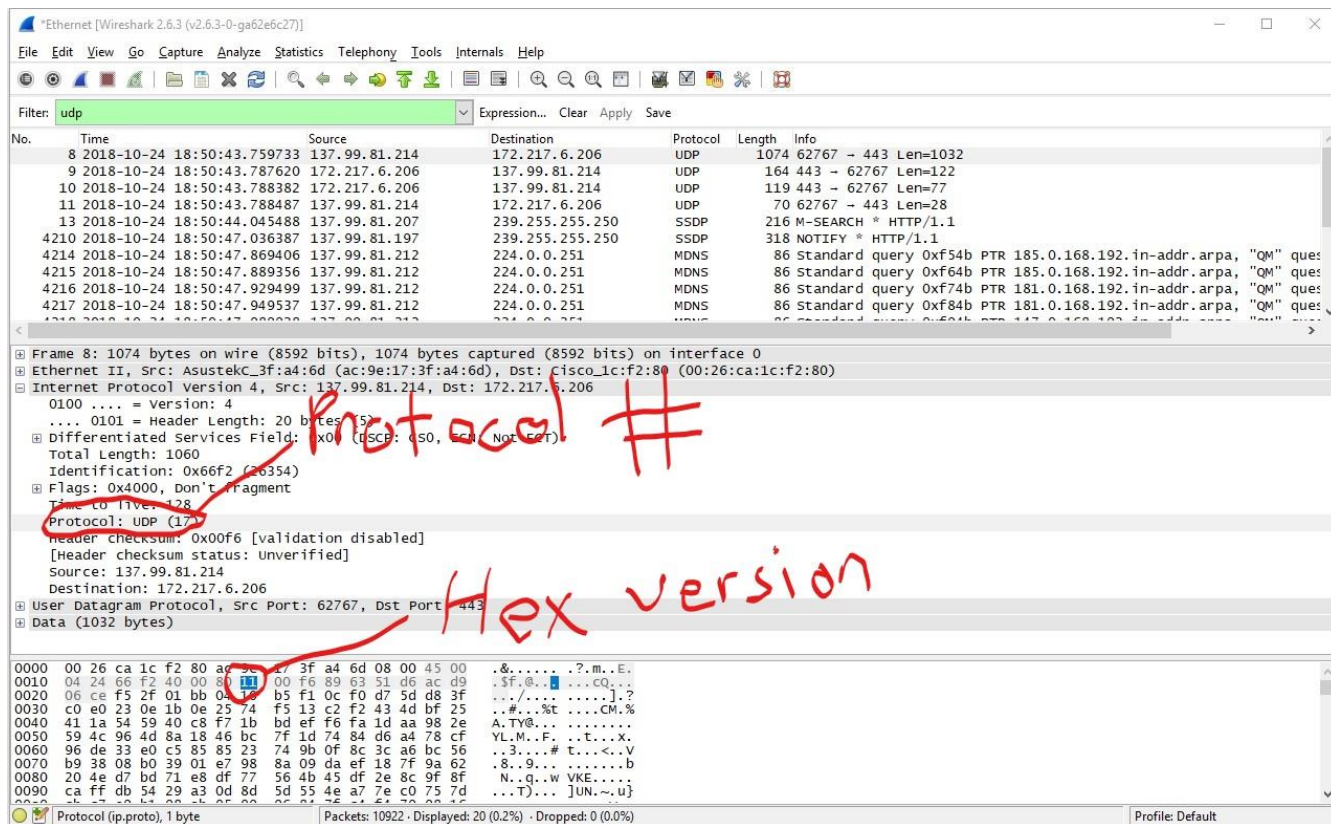
- 2) Each UDP header field is 2 bytes long:

The image shows a Wireshark packet capture of a UDP packet. The packet list shows a packet of length 1074 bytes. The packet details pane shows the following structure:

- Frame 8: 1074 bytes on wire (8592 bits), 1074 bytes captured (8592 bits) on interface 0
- Ethernet II, Src: AsustekC_3f:a4:6d (ac:9e:17:3f:a4:6d), Dst: Cisco1c:f2:80 (00:26:ca:1c:f2:80)
- Internet Protocol Version 4, Src: 137.99.81.214, Dst: 172.217.6.206
- User Datagram Protocol, Src Port: 62767, Dst Port: 443
- Data (1032 bytes)

A handwritten red note is written over the packet details pane: $1032 + 8 = 1040 \text{ bytes}$. The packet bytes pane shows the raw data in hexadecimal and ASCII.

- 4) The maximum number of bytes that can be sent in a UDP packet is 2^{16} bytes. But, since there needs to be 8 reserve bytes for the headers, there is a maximum payload size of $2^{16} - 8 = 65527$ bytes.
- 5) The largest port number corresponds to the maximum payload size not including the header bytes, so the largest port number is 65535.
- 6) The protocol for UDP is indicated by 17 and the hexadecimal notation of this value can be found below as 0x11:

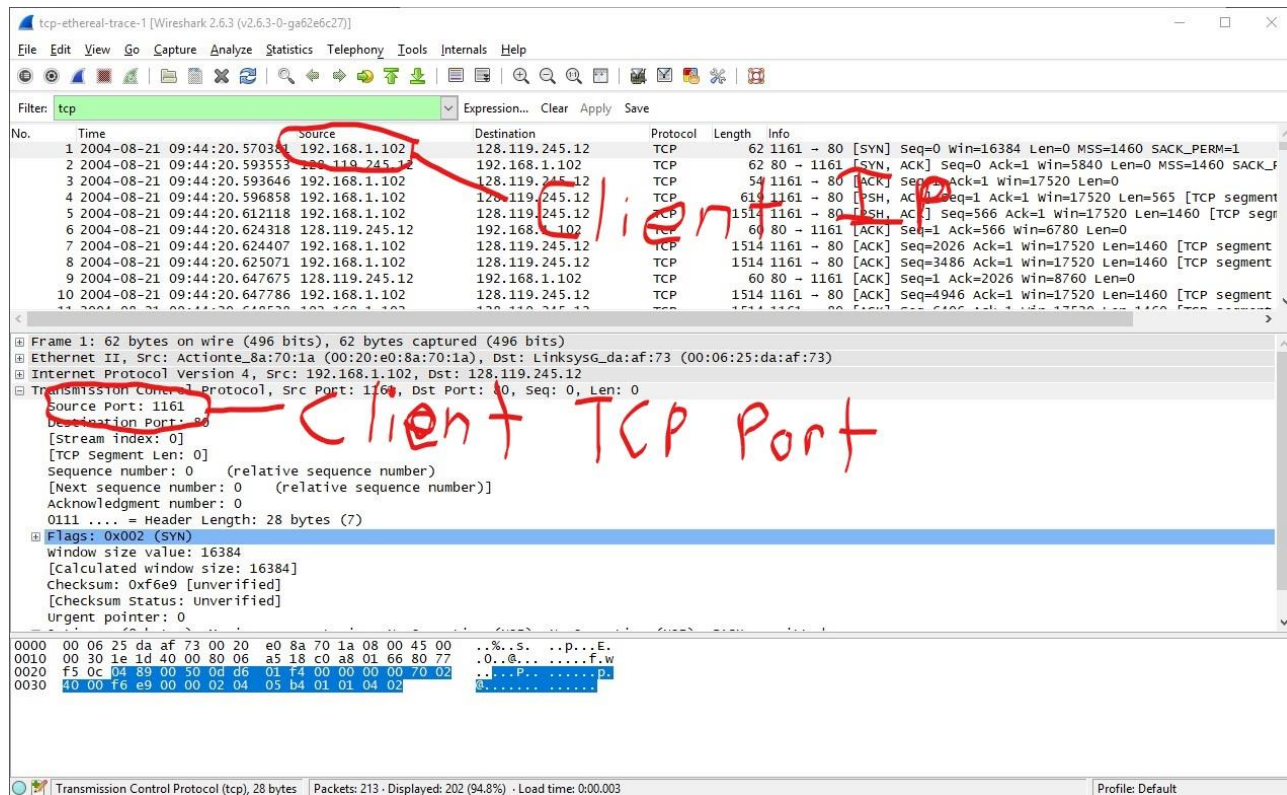


- 7) The relationship between these two UDP packets is the port numbers. The Source Port of the UDP packet that sent the packet is the Destination Port of the receiving message UDP packet. Hence, the Destination Port for the packet that sent the message is the Source Port of the receiving message packet:

Sending Message Packet:

Part 2: TCP Bulk Transfer

- 1) The IP address of the client computer is 192.168.1.102 and the TCP port number is 1161:



- 2) The IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP port number is 80:

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|--|
| 1 | 2004-08-21 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 -> 80 [SYN] Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 2004-08-21 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 -> 1161 [SYN, ACK] Seq=0 Ack=1 win=580 Len=0 MSS=1460 SACK_P |
| 3 | 2004-08-21 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 -> 80 [ACK] Seq=1 Ack=1 win=17520 Len=0 |
| 4 | 2004-08-21 09:44:20.596858 | 128.119.245.12 | 128.119.245.12 | TCP | 619 | 1161 -> 80 [RST, ACK] Seq=1 Ack=1 win=17520 Len=565 [TCP segment |
| 5 | 2004-08-21 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 -> 80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460 [TCP segm |
| 6 | 2004-08-21 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 -> 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0 |
| 7 | 2004-08-21 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 -> 80 [ACK] Seq=2026 Ack=1 win=17520 Len=1460 [TCP segment |
| 8 | 2004-08-21 09:44:20.625071 | 128.119.245.12 | 128.119.245.12 | TCP | 1514 | 1161 -> 80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460 [TCP segment |
| 9 | 2004-08-21 09:44:20.647675 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 -> 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0 |
| 10 | 2004-08-21 09:44:20.647786 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 -> 80 [ACK] Seq=4946 Ack=1 win=17520 Len=1460 [TCP segment |

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_ga:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0

0111 = Header Length: 28 bytes (7)

Flags: 0x002 (SYN)

Window size value: 16384

[Calculated window size: 16384]

Checksum: 0xf6e9 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ...S...P...E.

0010 00 30 1e 1d 40 00 80 06 a5 18 c0 a8 01 66 80 77 ...@...f.w

0020 f5 0c 04 89 00 30 0d d6 01 f4 00 00 00 00 70 02 ...P...P.

0030 40 00 f6 e9 00 00 02 04 05 b4 01 01 04 02 ...A.....

Transmission Control Protocol (tcp), 28 bytes | Packets: 213 · Displayed: 202 (94.8%) · Load time: 0:00.003 | Profile: Default

- 3) The IP address of my client computer is 137.99.81.214 and the TCP port number is 51417:

Ethernet [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|--|
| 25 | 2018-10-24 19:55:27.786811 | 137.99.81.214 | 128.119.245.12 | TCP | 54 | 51404 -> 80 [FIN, ACK] Seq=1 Ack=1 win=256 Len=0 |
| 26 | 2018-10-24 19:55:27.786944 | 137.99.81.214 | 128.119.245.12 | TCP | 66 | 51417 -> 80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SACK_PEF |
| 27 | 2018-10-24 19:55:27.787045 | 137.99.81.214 | 128.119.245.12 | TCP | 66 | 51418 -> 80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SACK_PEF |
| 28 | 2018-10-24 19:55:27.792130 | 128.119.245.12 | 137.99.81.214 | TCP | 60 | 80 -> 51404 [ACK] Seq=1 Ack=2 win=229 Len=0 |
| 29 | 2018-10-24 19:55:27.792131 | 128.119.245.12 | 137.99.81.214 | TCP | 60 | 80 -> 51403 [ACK] Seq=1 Ack=2 win=229 Len=0 |
| 30 | 2018-10-24 19:55:27.792131 | 128.119.245.12 | 137.99.81.214 | TCP | 66 | 80 -> 51417 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PEF |
| 31 | 2018-10-24 19:55:27.792205 | 137.99.81.214 | 128.119.245.12 | TCP | 54 | 51417 -> 80 [ACK] Seq=1 Ack=1 win=65536 Len=0 |
| 32 | 2018-10-24 19:55:27.792573 | 137.99.81.214 | 128.119.245.12 | TCP | 714 | 51417 -> 80 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=660 [TCP segment |
| 33 | 2018-10-24 19:55:27.792659 | 137.99.81.214 | 128.119.245.12 | TCP | 1514 | 51417 -> 80 [ACK] Seq=661 Ack=1 win=65536 Len=1460 [TCP segment |
| 34 | 2018-10-24 19:55:27.792664 | 137.99.81.214 | 128.119.245.12 | TCP | 1514 | 51417 -> 80 [ACK] Seq=2121 Ack=1 win=65536 Len=1460 [TCP segment |

Frame 26: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: Asustekc_3f:a4:6d (ac:9e:17:3f:a4:6d), Dst: Cisco_lc:f2:80 (00:26:ca:1c:f2:80)

Internet Protocol Version 4, Src: 137.99.81.214, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 51417, Dst Port: 80, Seq: 0, Len: 0

Source Port: 51417

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0

1000 = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)

Window size value: 64240

[Calculated window size: 64240]

Checksum: 0xf341 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

0000 00 26 ca 1c f2 80 ac 9e 17 3f a4 6d 08 00 45 00 ...&.....P...E.

0010 00 34 34 ce 40 00 80 06 75 38 89 63 51 d6 80 77 ...44.@...u8.CQ..W

0020 f5 0c c8 d9 00 50 82 32 e4 c3 00 00 00 00 80 02 ...P.2

0030 fa f0 f3 41 00 00 02 04 05 b4 01 03 03 08 01 01 ...A.....

0040 04 02 ..

File: "C:\Users\bryan\AppData\Local\Temp\..." | Packets: 256 · Displayed: 225 (87.9%) · Dropped: 0 (0.0%) | Profile: Default

- 4) The sequence number of the top SYN packet is for the initiation of a connection to the destination computer. In this specific trace, the sequence number value is 0. The segment that indicates that this packet is a SYN one, is in the Flags section of the protocol information. It is 1 in this case, to indicate the packet is a SYN:

The image shows a Wireshark packet capture of a TCP SYN packet. The packet list at the top shows a packet from 192.168.1.102 to 128.119.245.12 with sequence number 0. The packet details pane shows the TCP flags section with the Syn flag set to 1. Handwritten red annotations include "Sequence Value" with an arrow pointing to the sequence number field, and "Syn Flag = 1" with an arrow pointing to the Syn flag field. The packet bytes pane shows the raw data of the packet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|--|
| 213 | 2004-08-21 09:44:28.165938 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1162 → 80 [RST] Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 206 | 2004-08-21 09:44:26.221522 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [ACK] Seq=164091 Ack=731 win=16790 Len=0 |
| 203 | 2004-08-21 09:44:26.031556 | 128.119.245.12 | 192.168.1.102 | TCP | 784 | 80 → 1161 [PSH, ACK] Seq=1 Ack=164091 win=62780 Len=730 |
| 202 | 2004-08-21 09:44:26.026211 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=164091 win=62780 Len=0 |
| 201 | 2004-08-21 09:44:26.018268 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=164041 win=62780 Len=0 |
| 200 | 2004-08-21 09:44:25.959852 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=162309 win=62780 Len=0 |
| 199 | 2004-08-21 09:44:25.867722 | 192.168.1.102 | 128.119.245.12 | TCP | 104 | 1161 → 80 [PSH, ACK] Seq=164041 Ack=1 win=17520 Len=50 |
| 198 | 2004-08-21 09:44:25.867638 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=159389 win=62780 Len=0 |
| 197 | 2004-08-21 09:44:25.772405 | 192.168.1.102 | 128.119.245.12 | TCP | 326 | 1161 → 80 [PSH, ACK] Seq=163769 Ack=1 win=17520 Len=272 |
| 196 | 2004-08-21 09:44:25.771531 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=162309 Ack=1 win=17520 Len=1460 |

Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
0111 = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
...0 = Reserved: Not set
...0 = Nonce: Not set
...0 = Congestion Window Reduced (CWR): Not set
...0 = ECN-Echo: Not set
...0 = Urgent: Not set
...0 = Acknowledgment: Not set
...0 = Push: Not set
...0 = Reset: Not set
...1 = Syn: Set
...0 = Fin: Not set
[TCP Flags:S.]
window size value: 16384
[calculated window size: 16384]
checksum: over? (unverified)

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%..S. ...p...E.
0010 00 30 1e 9e 40 00 80 06 1d 4b c0 a8 01 66 c7 02 .0...@...K...F..
0020 35 ce 04 8a 02 77 0d f3 82 b9 00 00 00 00 70 02 5...W.p..
0030 40 00 ec 92 00 00 02 04 05 b4 01 01 04 02 @.....

- 5) The value of Acknowledgement field in the SYNACK segment is 1. The destination server determines this value by adding on 1 to the initial sequence value of the SYN segment sent earlier. The segment that determines that the segment is a SYNACK one is in the flags section in the protocol information. Both the Acknowledgement and Syn flags are equal 1, which means the packet is flagged to be a SYNACK:

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|--|
| 3 | 2004-08-21 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 2 | 2004-08-21 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=1 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 1 | 2004-08-21 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 SACK_PERM=1 |
| 212 | 2004-08-21 09:44:27.674161 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 211 | 2004-08-21 09:44:27.673233 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 210 | 2004-08-21 09:44:27.171444 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 209 | 2004-08-21 09:44:27.170533 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 208 | 2004-08-21 09:44:26.672450 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 207 | 2004-08-21 09:44:26.671425 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 205 | 2004-08-21 09:44:26.169463 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 204 | 2004-08-21 09:44:26.168471 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |

Sequence number: 0 (relative sequence number)
 [Next sequence number: 0 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 0111 = Header Length: 28 bytes (7)
 [Flags: 0x012 (SYN, ACK)]
 000. = Reserved: Not set
 ...0 = Nonce: Not set
0... = Congestion Window Reduced (CWR): Not set
0... = ECN-Echo: Not set
0... = Urgent: Not set
1... = Acknowledgment: Set
0... = Push: Not set
0... = Reset: Not set
1... = Syn: Set
0... = Fin: Not set
 [TCP Flags:A..S.]
 window size value: 5840
 [calculated window size: 5840]
 [checksum: 0x774d, unverified]

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00 ...p...%.s..E.
 0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c c0 a8 ..0..8.7..6.w...
 0020 01 66 00 50 04 89 34 a2 74 19 0d d6 01 f5 70 12 .f.P..4..t....p
 0030 16 d0 77 4d 00 00 02 04 05 b4 01 01 04 02 ...WM.....

Acknowledgment (tcp.flags.ack), 1 byte Packets: 213 · Displayed: 213 (100.0%) · Load time: 0:00.002 Profile: Default

- 6) The 4th packet in the trace is the packet that contains the HTTP POST. The sequence value for this segment is 1:

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|--|
| 1 | 2004-08-21 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN, Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 2004-08-21 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 3 | 2004-08-21 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 win=17520 Len=0 |
| 4 | 2004-08-21 09:44:20.596858 | 192.168.1.102 | 128.119.245.12 | TCP | 619 | 1161 → 80 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=565 [TCP segment of a |
| 5 | 2004-08-21 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460 [TCP segment |
| 6 | 2004-08-21 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0 |
| 7 | 2004-08-21 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=2026 Ack=1 win=17520 Len=1460 [TCP segment of a |
| 8 | 2004-08-21 09:44:20.625071 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460 [TCP segment of a |
| 9 | 2004-08-21 09:44:20.647675 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0 |
| 10 | 2004-08-21 09:44:20.647786 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 win=17520 Len=1460 [TCP segment of a |
| 11 | 2004-08-21 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460 [TCP segment of a |
| 12 | 2004-08-21 09:44:20.694466 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=3486 win=11680 Len=0 |
| 13 | 2004-08-21 09:44:20.694566 | 192.168.1.102 | 128.119.245.12 | TCP | 1201 | 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 win=17520 Len=1147 [TCP segment |
| 14 | 2004-08-21 09:44:20.739499 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0 |
| 15 | 2004-08-21 09:44:20.787680 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0 |
| 16 | 2004-08-21 09:44:20.838183 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0 |
| 17 | 2004-08-21 09:44:20.875188 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0 |

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 565]

Sequence number: 1 (relative sequence number)

[Next sequence number: 566 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p...E.

0010 02 5d 1e 21 40 00 80 06 a2 e7 c0 a8 01 06 80 77 .].8...:..f.w

0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18 ...P...4..t..

0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 Dp...PO ST /ethe

0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 real-lab s/lab3-1

0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f -reply.h tm HTTP/

0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 1.., Hos t: gdl

0070 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 55 73 cs.unass -edu.Us

0080 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill

0090 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 a/S.O (w indows;

File: "C:\Users\bryan\Desktop\tcp-ethereal-t... Packets: 213 - Displayed: 213 (100.0%) - Load time: 0:00.002 Profile: Default

HTTP Post

- 7) The first six segments in the HTTP POST are packet numbers 4, 5, 7, 8, 10, and 11. The corresponding ACK segments of these segments are packets numbers 6, 9, 12, 14, 15, and 16 respectively.

(Segments 1-6):

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62efc27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| Time | Source | Destination | Protocol | Length | Info |
|-----------------|----------------|----------------|----------|--------|---|
| 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN] Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 win=17520 Len=0 |
| 09:44:20.596858 | 192.168.1.102 | 128.119.245.12 | TCP | 619 | 1161 → 80 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=565 [TCP segment of a reassembled |
| 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460 [TCP segment of a reassemb |
| 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0 |
| 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=2026 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.625071 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.647765 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0 |
| 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.694466 | 128.119.245.12 | 192.168.1.102 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.694566 | 192.168.1.102 | 128.119.245.12 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=3486 win=11680 Len=0 |
| 09:44:20.739499 | 128.119.245.12 | 192.168.1.102 | TCP | 1201 | 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 win=17520 Len=1147 [TCP segment of a reassemb |
| 09:44:20.787680 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0 |
| 09:44:20.838183 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0 |
| 09:44:20.875188 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0 |

Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_g_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 566, Ack: 1, Len: 1460

Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence number: 566 (relative sequence number)
[Next sequence number: 2026 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p...E.
0010 05 dc 1e 22 40 00 80 06 9f 67 c0 a8 01 66 80 77@...g...f.w
0020 f5 0c 04 89 00 50 0d d6 04 2a 34 a2 74 1a 50 18P...4.t.P.
0030 44 70 3b e5 00 00 43 6f 6e 74 65 6e 74 2d 54 79 Dp:...Co ntent-Ty
0040 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f pe: mult ipart/fo
0050 72 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 rm-data; boundar
0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d y-----
0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----265
0080 30 30 31 39 31 36 39 31 35 37 32 34 0d 0a 43 6f 00191691 5724..Co
0090 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 36 ntent-Le ngth: 16

File: "C:\Users\bryan\Desktop\tcp-ethereal-tr... Packets: 213 · Displayed: 213 (100.0%) · Load time: 0:00.002 Profile: Default

Segment's 1-6

(ACK segments of segments 1-6):

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62efc27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| Time | Source | Destination | Protocol | Length | Info |
|-----------------|----------------|----------------|----------|--------|---|
| 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN] Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 win=17520 Len=0 |
| 09:44:20.596858 | 192.168.1.102 | 128.119.245.12 | TCP | 619 | 1161 → 80 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=565 [TCP segment of a reassembled |
| 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460 [TCP segment of a reassemb |
| 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0 |
| 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=2026 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.625071 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.647765 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0 |
| 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.694466 | 128.119.245.12 | 192.168.1.102 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 09:44:20.694566 | 192.168.1.102 | 128.119.245.12 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=3486 win=11680 Len=0 |
| 09:44:20.739499 | 128.119.245.12 | 192.168.1.102 | TCP | 1201 | 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 win=17520 Len=1147 [TCP segment of a reassemb |
| 09:44:20.787680 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0 |
| 09:44:20.838183 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0 |
| 09:44:20.875188 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0 |

Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_g_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 566, Ack: 1, Len: 1460

Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence number: 566 (relative sequence number)
[Next sequence number: 2026 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p...E.
0010 05 dc 1e 22 40 00 80 06 9f 67 c0 a8 01 66 80 77@...g...f.w
0020 f5 0c 04 89 00 50 0d d6 04 2a 34 a2 74 1a 50 18P...4.t.P.
0030 44 70 3b e5 00 00 43 6f 6e 74 65 6e 74 2d 54 79 Dp:...Co ntent-Ty
0040 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f pe: mult ipart/fo
0050 72 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 rm-data; boundar
0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d y-----
0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----265
0080 30 30 31 39 31 36 39 31 35 37 32 34 0d 0a 43 6f 00191691 5724..Co
0090 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 36 ntent-Le ngth: 16

File: "C:\Users\bryan\Desktop\tcp-ethereal-tr... Packets: 213 · Displayed: 213 (100.0%) · Load time: 0:00.002 Profile: Default

ACK's 1-6

Segment 1 Seq = 1, Segment 2 Seq = 566, Segment 3 Seq = 2026, Segment 4 Seq = 3486, Segment 5 Seq = 4946, Segment Seq 6 = 6406.

Here are the times of when the segments were sent, the ACK was received back, and the RTT time:

Segment 1: Sent = 0.026477s, ACK received = 0.053937s, RTT = 0.02746s
Segment 2: Sent = 0.041737s, ACK received = 0.077294s, RTT = 0.035557s
Segment 3: Sent = 0.054026s, ACK received = 0.124085s, RTT = 0.070059s
Segment 4: Sent = 0.054690s, ACK received = 0.169118s, RTT = 0.11443s
Segment 5: Sent = 0.077405s, ACK received = 0.217299s, RTT = 0.13989s
Segment 6: Sent = 0.078157s, ACK received = 0.267802s, RTT = 0.18964s

Now, here are the calculations for each EstimatedRTT:

Segment 1 EstimatedRTT = RTT Segment 1 = 0.02746 seconds

Segment 2 EstimatedRTT = $0.875 * \text{Segment 1 EstimatedRTT} + 0.125 * \text{RTT}$
Segment 2 = 0.0285 seconds

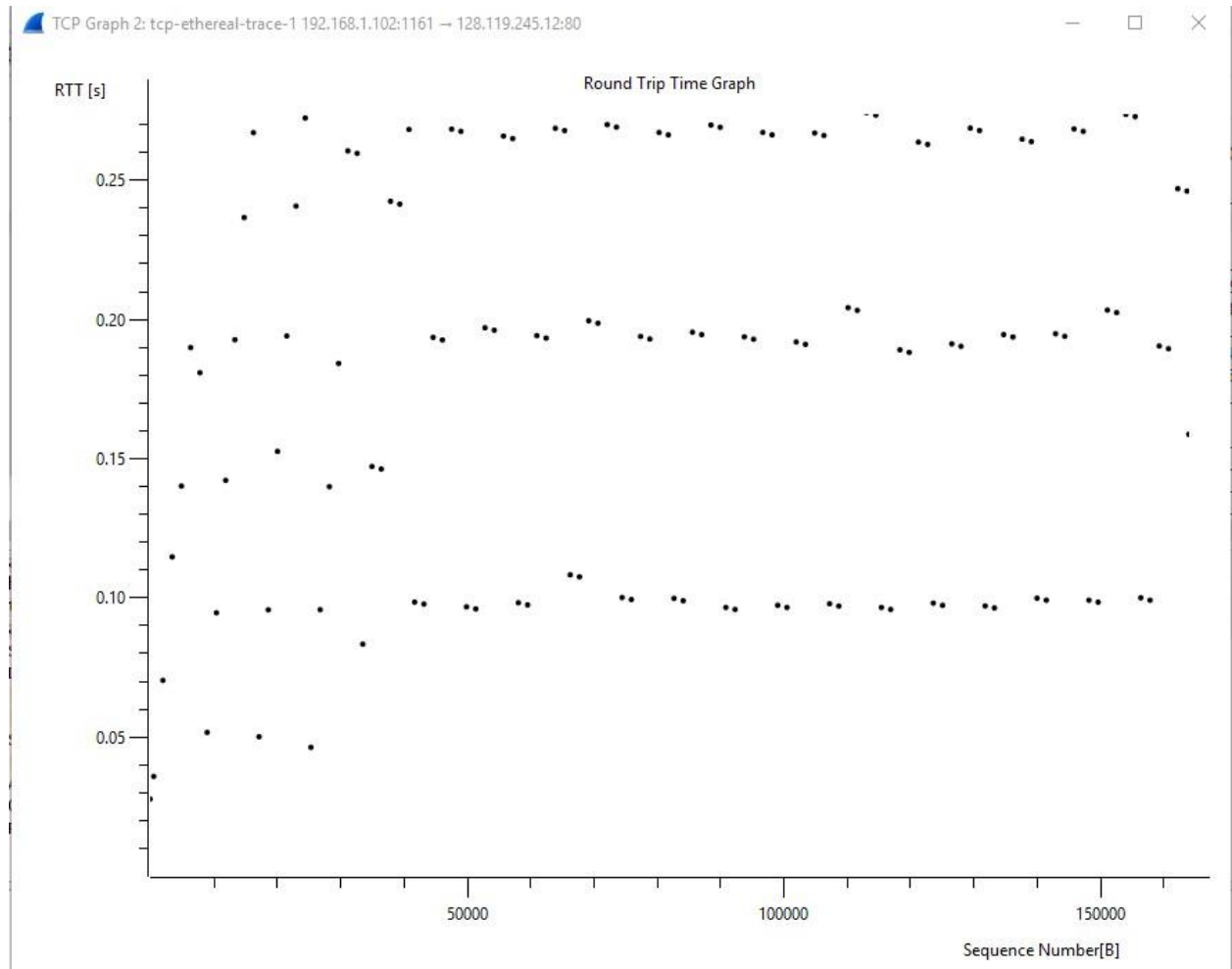
Segment 3 EstimatedRTT = $0.875 * \text{Segment 2 EstimatedRTT} + 0.125 * \text{RTT}$
Segment 3 = 0.0337

Segment 4 EstimatedRTT = $0.875 * \text{Segment 3 EstimatedRTT} + 0.125 * \text{RTT}$
Segment 4 = 0.0438

Segment 5 EstimatedRTT = $0.875 * \text{Segment 4 EstimatedRTT} + 0.125 * \text{RTT}$
Segment 5 = 0.0558

Segment 6 EstimatedRTT = $0.875 * \text{Segment 5 EstimatedRTT} + 0.125 * \text{RTT}$
Segment 6 = 0.0725

(Graph of TCP Segments and ACKS)



- 8) The Lengths of the first 6 TCP segments are 565, 1460, 1460, 1460, 1460, and 1460 respectively:

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

1-6 Lengths

| Time | Source | Destination | Protocol | Length | Info |
|-----------------------|----------------|----------------|----------|--------|---|
| 08-21 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN, Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 08-21 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 08-21 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 win=17520 Len=0 |
| 08-21 09:44:20.596858 | 192.168.1.102 | 128.119.245.12 | TCP | 619 | 1161 → 80 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=565 [TCP segment of a reassembled |
| 08-21 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460 [TCP segment of a reassemb |
| 08-21 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0 |
| 08-21 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=2026 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 08-21 09:44:20.625071 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 08-21 09:44:20.647675 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0 |
| 08-21 09:44:20.647786 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 08-21 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460 [TCP segment of a reassembled |
| 08-21 09:44:20.694466 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=3486 win=11680 Len=0 |
| 08-21 09:44:20.694566 | 192.168.1.102 | 128.119.245.12 | TCP | 1201 | 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 win=17520 Len=1147 [TCP segment of a reassemb |
| 08-21 09:44:20.739499 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0 |
| 08-21 09:44:20.787680 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0 |
| 08-21 09:44:20.838183 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0 |
| 08-21 09:44:20.875188 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0 |

- 9) The minimum buffer space that the destination computer advertises usually is seen in the very first acknowledgement response from the server. This would be in the first

ACK segments in the trace, and the minimum buffer space is 5840 bytes. The sender is never throttled in this trace for a lack of receiving buffer:

The image shows a Wireshark packet capture analysis. The top pane displays a list of 17 TCP segments. The bottom pane shows the details of a selected segment (No. 16), which is an ACK segment. The 'Flags' field is highlighted with a red circle, and a handwritten red note 'Min receive buffer' is written next to it. The 'window size value' is 5840, and the 'calculated window size' is also 5840. The bottom status bar indicates 'Packets: 213 · Displayed: 213 (100.0%) · Load time: 0:00.003'.

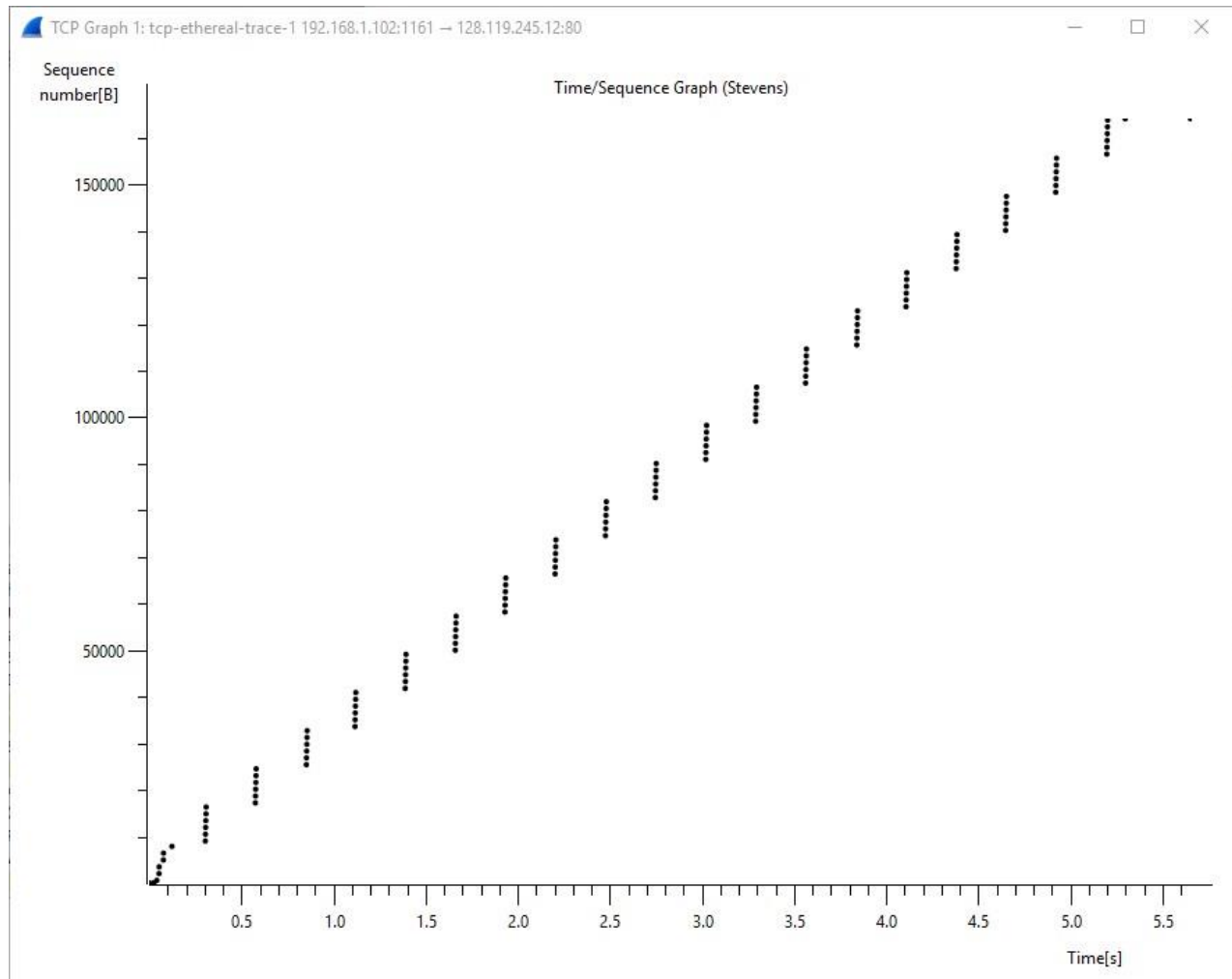
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|---|
| 1 | 2004-08-21 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN] Seq=0 win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 2004-08-21 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 3 | 2004-08-21 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 win=17520 Len=0 |
| 4 | 2004-08-21 09:44:20.596858 | 192.168.1.102 | 128.119.245.12 | TCP | 619 | 1161 → 80 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=565 [TCP segment of a ...] |
| 5 | 2004-08-21 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [PSH, ACK] Seq=566 Ack=1 win=17520 Len=1460 [TCP segment of a ...] |
| 6 | 2004-08-21 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0 |
| 7 | 2004-08-21 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=2026 Ack=1 win=17520 Len=1460 [TCP segment of a ...] |
| 8 | 2004-08-21 09:44:20.625071 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=3486 Ack=1 win=17520 Len=1460 [TCP segment of a ...] |
| 9 | 2004-08-21 09:44:20.647675 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0 |
| 10 | 2004-08-21 09:44:20.647786 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 win=17520 Len=1460 [TCP segment of a ...] |
| 11 | 2004-08-21 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 win=17520 Len=1460 [TCP segment of a ...] |
| 12 | 2004-08-21 09:44:20.694466 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=3486 win=11680 Len=0 |
| 13 | 2004-08-21 09:44:20.694566 | 128.119.245.12 | 128.119.245.12 | TCP | 1201 | 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 win=17520 Len=1147 [TCP segment of a ...] |
| 14 | 2004-08-21 09:44:20.739499 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0 |
| 15 | 2004-08-21 09:44:20.787680 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0 |
| 16 | 2004-08-21 09:44:20.838183 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0 |
| 17 | 2004-08-21 09:44:20.875188 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=9013 win=23360 Len=0 |

Destination Port: 1161
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative acknowledgment number)
0111 = Header Length: 28 bytes (C)
Flags: 0x012 (SYN, ACK)
window size value: 5840
[Calculated window size: 5840]
Checksum: 0x774d [unverified]
[Checksum Status: Unverified]
urgent pointer: 0
Options: (8 bytes), Maximum segment size, No-operation (NOP), No-operation (NOP), SACK permitted
[seq/ack analysis]

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00 ...p...%.s..E.
0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c c0 a8 .0.0.7..6.w....
0020 01 66 00 50 04 89 34 a2 74 19 0d 06 01 f5 70 12 .f.p..4.t.....p.
0030 16 c0 77 4d 00 00 02 04 05 b4 01 01 04 02 77 4d 00 00 02 04 05 b4 01 01 04 02 77 4d 00 00 02 04 05 b4 01 01 04 02

The window size value from the TCP header ... Packets: 213 · Displayed: 213 (100.0%) · Load time: 0:00.003 Profile: Default

- 10) None of the segments in the trace were retransmitted. By using the Time-Sequence-Graph for the entire trace, also given to us in the homework pdf, we can see the sequence numbers from the source increasing linearly with time. In order for a segment to be retransmitted, the segment must have a smaller sequence value than the segments next to it (which doesn't happen):



- 11) The amount of data that is usually received in an ACK is the difference of the sequence numbers of two ACKs. For instance, sequence number 566 for one ACK and then 2026 for the next ACK results in a total of 1460 acknowledged data. If you look closely at the data being acknowledged, sometimes the receiver is ACKing every other segment. For instance, segment 80 of the trace acknowledged 2920 bytes instead of 1460 bytes like it should have:

tcp-ethereal-trace-1 [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|---------------|----------------|----------|--------|--|
| 63 | 2004-08-21 09:44:21.960491 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=41781 Ack=1 win=17520 Len= |
| 64 | 2004-08-21 09:44:21.961205 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=43241 Ack=1 win=17520 Len= |
| 65 | 2004-08-21 09:44:21.962064 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=44701 Ack=1 win=17520 Len= |
| 66 | 2004-08-21 09:44:21.962975 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=46161 Ack=1 win=17520 Len= |
| 67 | 2004-08-21 09:44:21.963771 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=47621 Ack=1 win=17520 Len= |
| 10 | 2004-08-21 09:44:20.647786 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 win=17520 Len= |
| 72 | 2004-08-21 09:44:22.232115 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=49973 Ack=1 win=17520 Len= |
| 73 | 2004-08-21 09:44:22.232855 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=51433 Ack=1 win=17520 Len= |
| 74 | 2004-08-21 09:44:22.233696 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=52893 Ack=1 win=17520 Len= |
| 75 | 2004-08-21 09:44:22.234579 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=54353 Ack=1 win=17520 Len= |
| 76 | 2004-08-21 09:44:22.235635 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=55813 Ack=1 win=17520 Len= |
| 81 | 2004-08-21 09:44:22.501480 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=58165 Ack=1 win=17520 Len= |
| 82 | 2004-08-21 09:44:22.502260 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=59625 Ack=1 win=17520 Len= |
| 83 | 2004-08-21 09:44:22.503138 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=61085 Ack=1 win=17520 Len= |
| 84 | 2004-08-21 09:44:22.504017 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=62545 Ack=1 win=17520 Len= |
| 85 | 2004-08-21 09:44:22.505151 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=64005 Ack=1 win=17520 Len= |
| 11 | 2004-08-21 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 win=17520 Len= |

[TCP segment Len: 1460]
Sequence number: 61085 (relative sequence number)
[Next sequence number: 62545 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
[Flags: 0x010 (ACK)]
window size value: 17520
[calculated window size: 17520]
[window size scaling factor: -2 (no window scaling used)]
checksum: 0xa312 [unverified]
[checksum status: unverified]
urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1460 bytes)

```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  ..%.s. .p...E.
0010 05 dc 1e 4e 40 00 80 06 9f 3b c0 a8 01 66 80 77  ...NB... ;...f.w
0020 f5 0c 04 89 00 50 0d d6 f0 91 34 a2 74 1a 50 10  ....P... .4.t.P.
0030 44 70 a3 12 00 00 0d 0a 0d 0a 20 20 60 49 20 64  Dp..... ; 'I d
0040 6f 6e 27 74 20 73 65 65 2c 27 20 73 61 69 64 20  on't see, said
0050 74 68 65 20 43 61 74 65 72 70 69 6c 6c 61 72 2e  the cate rpillar.
0060 0d 0a 0d 0a 20 20 60 49 27 6d 20 61 66 72 61 69  .... I'm afrai
0070 64 20 49 20 63 61 6e 27 74 20 70 75 74 20 69 74  d I can't put it
0080 20 6d 6f 72 65 20 63 6c 65 61 72 6c 79 2c 27 20  more cl early,
0090 41 6c 69 63 65 20 72 65 70 6c 69 65 64 20 76 65  Alice re plied ve
00a0 72 70 6d 6f 72 65 20 63 6c 65 61 72 6c 79 2c 27 20  more cl early,

```

File: "C:\Users\bryan\Desktop\tcp-ethereal-t... Packets: 213 · Displayed: 213 (100.0%) · Load time: 0:00.003 Profile: Default

12) To find the throughput of the TCP connection, we need to know the total data sent and the time from the first ACK segment to the last ACK segment of the trace. To find the total amount of data transmitted, we need to look at sequence number of the very first ACK segment, and the sequence number of the very last ACK segment of the trace. This packet corresponds to packet 4 and 202. Sequence value for packet 4 is 1, and the sequence value for packet 202 is 164091. $164091 - 1 = 16490$ gives us the total bytes transmitted. Now, we also need to look at the time the first ACK was received, and the last ACK. Looking at packets 4 and 202 again, we get $5.455830 - 0.026477 = 5.4294$ seconds for the data to transmit. Finally, to get the total throughput, we do $16490 \text{ bytes} / 5.4294 \text{ seconds} = \text{roughly } 30.2 \text{ KBps}$:

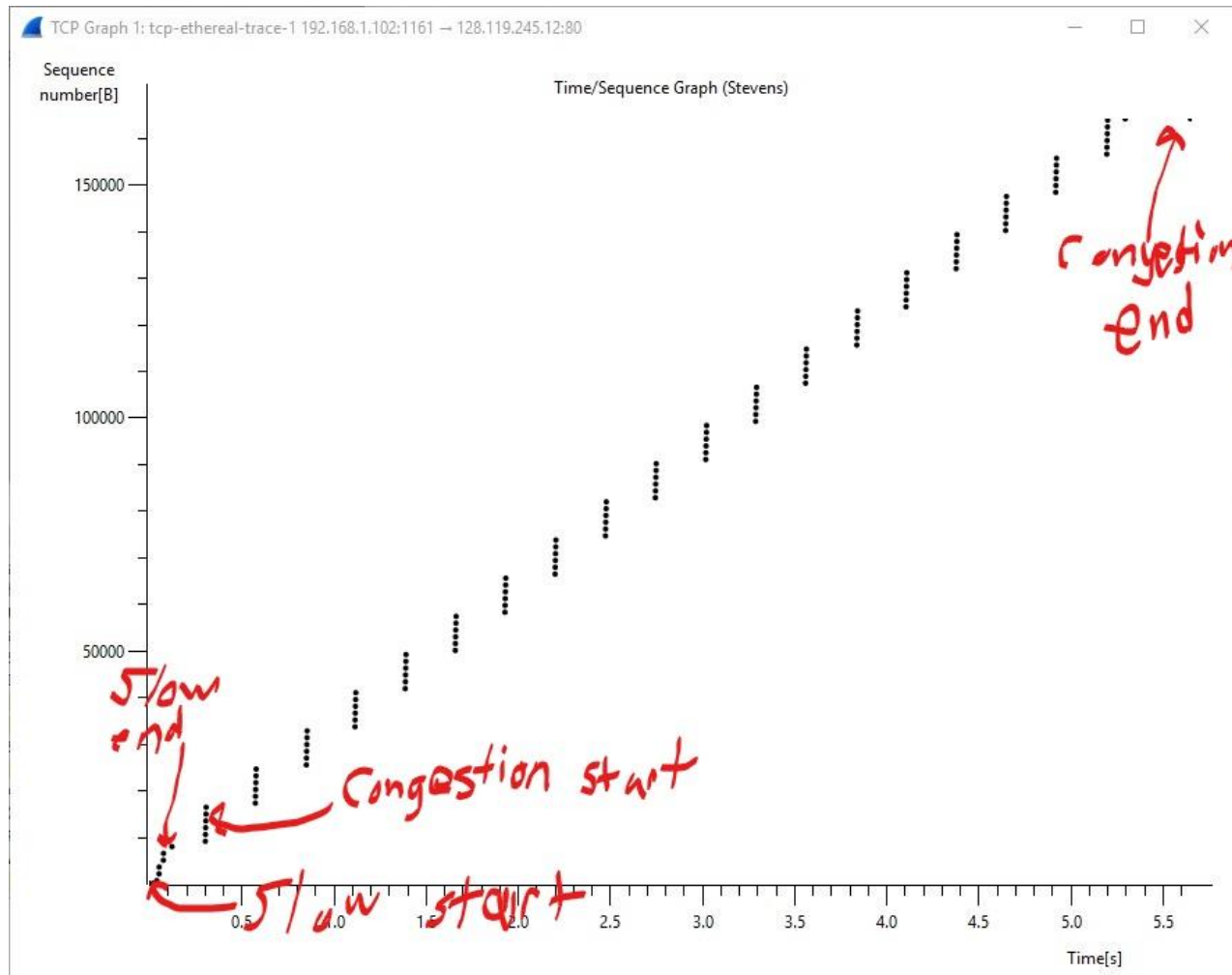
Segment 1 (packet 4) sequence and time:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|---|
| 1 | 2004-08-21 09:44:20.570381 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 2004-08-21 09:44:20.593553 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 3 | 2004-08-21 09:44:20.593646 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 4 | 2004-08-21 09:44:20.596858 | 192.168.1.102 | 128.119.245.12 | TCP | 619 | 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=563 [TCP segment of a |
| 5 | 2004-08-21 09:44:20.612118 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a |
| 6 | 2004-08-21 09:44:20.624318 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0 |
| 7 | 2004-08-21 09:44:20.624407 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a |
| 8 | 2004-08-21 09:44:20.625071 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a |
| 9 | 2004-08-21 09:44:20.647675 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0 |
| 10 | 2004-08-21 09:44:20.647786 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a |
| 11 | 2004-08-21 09:44:20.648538 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a |
| 12 | 2004-08-21 09:44:20.694466 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0 |
| 13 | 2004-08-21 09:44:20.694566 | 192.168.1.102 | 128.119.245.12 | TCP | 1201 | 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment |
| 14 | 2004-08-21 09:44:20.739499 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0 |
| 15 | 2004-08-21 09:44:20.787680 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0 |
| 16 | 2004-08-21 09:44:20.838183 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0 |
| 17 | 2004-08-21 09:44:20.875188 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0 |

Last ACK segment (packet 202) size and time:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|----------------|----------------|----------|--------|--|
| 195 | 2004-08-21 09:44:25.770633 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=160849 Ack=1 Win=17520 Len=1460 [TCP segment of |
| 196 | 2004-08-21 09:44:25.771531 | 192.168.1.102 | 128.119.245.12 | TCP | 1514 | 1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520 Len=1460 [TCP segment of |
| 197 | 2004-08-21 09:44:25.772405 | 192.168.1.102 | 128.119.245.12 | TCP | 326 | 1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=17520 Len=272 [TCP segment |
| 198 | 2004-08-21 09:44:25.867638 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780 Len=0 |
| 199 | 2004-08-21 09:44:25.867722 | 192.168.1.102 | 128.119.245.12 | HTTP | 104 | POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain) |
| 200 | 2004-08-21 09:44:25.959852 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0 |
| 201 | 2004-08-21 09:44:26.018268 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0 |
| 202 | 2004-08-21 09:44:26.026211 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0 |
| 203 | 2004-08-21 09:44:26.031556 | 128.119.245.12 | 192.168.1.102 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 204 | 2004-08-21 09:44:26.168471 | 192.168.1.100 | 192.168.1.1 | SSDP | 174 | M-SEARCH * HTTP/1.1 |
| 205 | 2004-08-21 09:44:26.169463 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 206 | 2004-08-21 09:44:26.221522 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0 |
| 207 | 2004-08-21 09:44:26.671425 | 192.168.1.100 | 192.168.1.1 | SSDP | 174 | M-SEARCH * HTTP/1.1 |
| 208 | 2004-08-21 09:44:26.672450 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 209 | 2004-08-21 09:44:27.170533 | 192.168.1.100 | 192.168.1.1 | SSDP | 174 | M-SEARCH * HTTP/1.1 |
| 210 | 2004-08-21 09:44:27.171444 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |

- 13) From the graph, we can see that the slow start phase begins when the HTTP POST command is sent, so the very first sequence number of the graph. This slow start ends when the very last sequence number in the first cluster is received an ACK. This indicates the start of the congestion avoidance phase. As seen in the graph, the clusters of sequences are spaced out from one another in their clusters, as well as other clusters, hence it is trying to avoid congestion. This phase ends when the trace stops. In terms of how the measured data compares to the aggressive nature of idealized TCP, too much traffic could interrupt the transmission of data. Idealized TCP has no packet loss, but due to the congestion in the data, it can happen, making it not match idealized TCP. Overall, the data measured here is fairly good match to idealized TCP:



- 14) For a file I transferred to the destination server, the same ways of telling when the slow start phase and congestion avoidance phase are the same as the previous. The measured data in this TCP trace was much quicker than the previous one. The overall transmission was a lot faster and the amount of sequences clustered together was much bigger than the previous as well. This was significantly quicker and a much more aggressive transmission of data, which aligns more with how idealized TCP should be. Hence, the file I sent is much better fit to idealized TCP.

