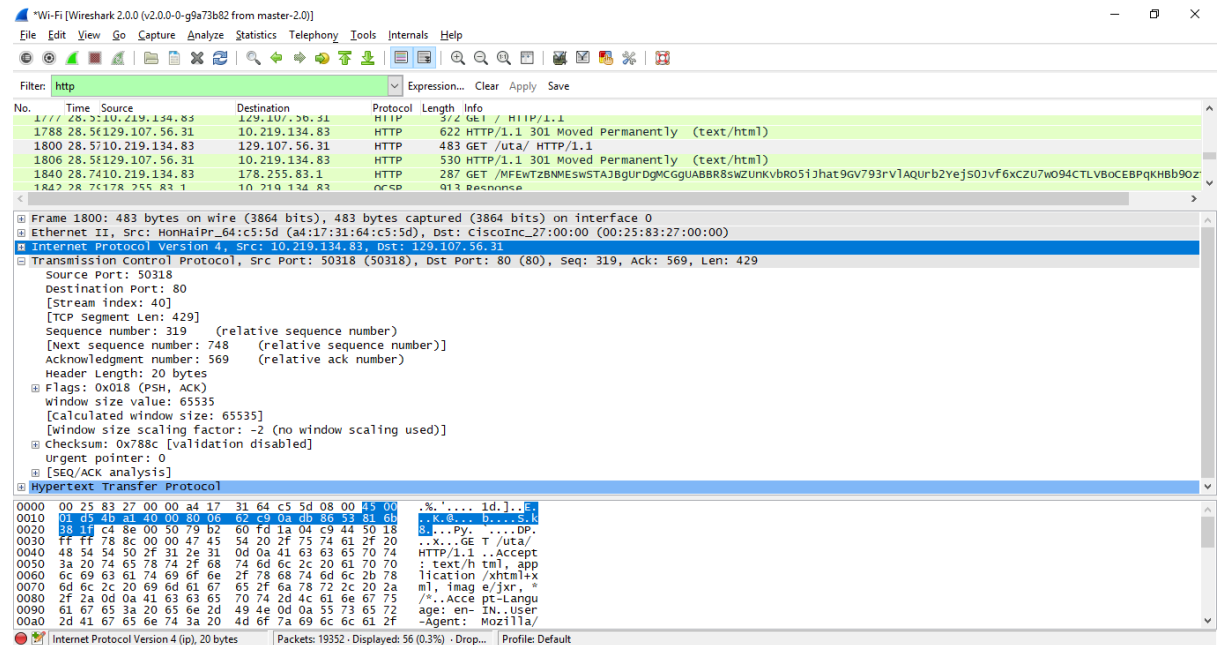


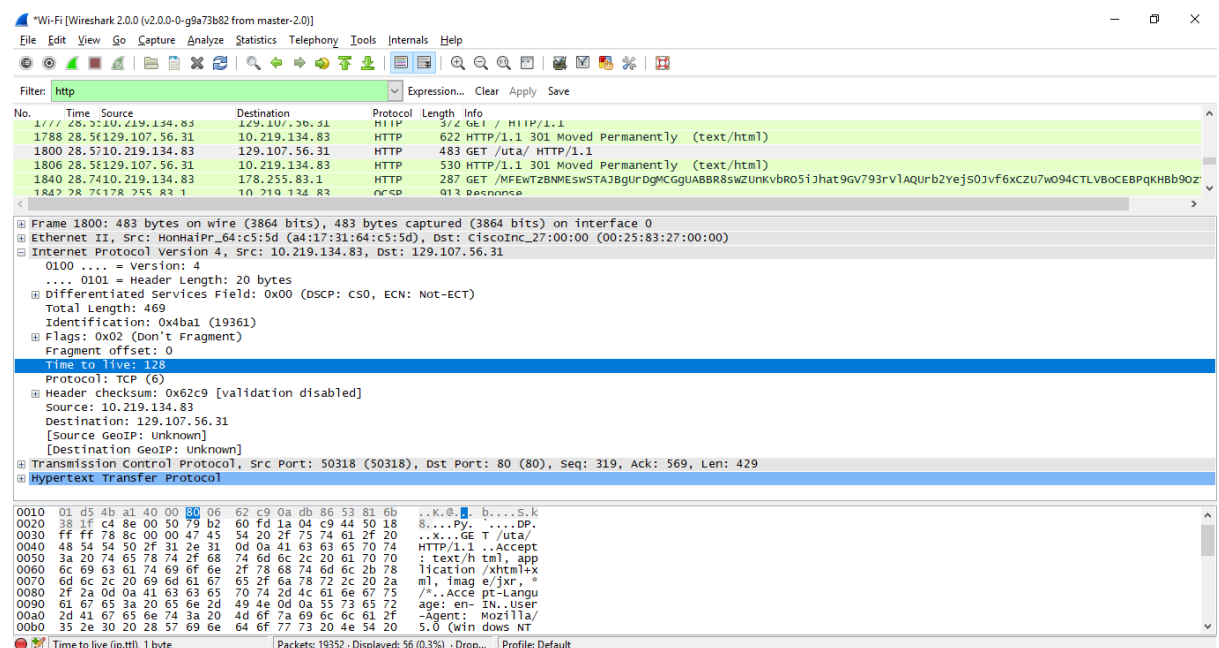
Section 1: HTTP over TCP

Problem Set 1:

1. Source Ip Address and Port is 10.219.134.82 : 50318



2. TTL Value used in Communication is 128



3. IPV4 is used During Communication.

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1778	28.56129.107.56.31	10.219.134.83	10.219.134.83	HTTP	622	HTTP/1.1 301 Moved Permanently (text/html)
1800	28.5710.219.134.83	129.107.56.31	129.107.56.31	HTTP	483	GET /uta/ HTTP/1.1
1806	28.58129.107.56.31	10.219.134.83	10.219.134.83	HTTP	530	HTTP/1.1 301 Moved Permanently (text/html)
1840	28.7410.219.134.83	178.255.83.1	178.255.83.1	HTTP	287	GET /MFEWTZBNMESWSTA3BgurDgMCgGUABBR8sWZUnkvBR051jhat9GV793rV1AqurB2YeJ503vf6XCZU7w094CTLVB0CEBPqKHb90z

Frame 1800: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0

Ethernet II, Src: HonHaiPr_64:c5:5d (a4:17:31:64:c5:5d), Dst: CiscoInc_27:00:00 (00:25:83:27:00:00)

Internet Protocol Version 4, Src: 10.219.134.83, Dst: 129.107.56.31

0100 = Version: 4
 0101 = Header Length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 469
 Identification: 0x4ba1 (19361)
 Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x62c9 [validation disabled]
 Source: 10.219.134.83
 Destination: 129.107.56.31
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 Transmission Control Protocol, Src Port: 50318 (50318), Dst Port: 80 (80), Seq: 319, Ack: 569, Len: 429
 Hypertext Transfer Protocol

0000 00 25 83 27 00 00 a4 17 31 64 c5 5d 08 00 45 00 .%. 1d.]._F
 0010 01 d5 4b a1 40 00 80 06 62 c9 0a db 86 53 81 6b ..K.E...b....S.k
 0020 38 1f c4 8e 00 50 79 b2 60 fd 1a 04 c9 44 50 18 8...Py.DP.
 0030 ff ff 78 8c 00 00 47 45 54 20 2f 75 74 61 2f 20 ..x...GE T /uta/
 0040 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 ..Accept
 0050 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 70 : text/html, app
 0060 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+x
 0070 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72 2c 20 2a ml, image/jxr, "
 0080 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 /*.Acc pt-Langu
 0090 61 67 65 3a 20 65 6e 2d 49 4e 0d 0a 55 73 65 72 age: en- IN..User
 00a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
 00b0 35 2e 30 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (win dows NT)

Internet Protocol Version 4 (ip), 20 bytes

Packets: 19352 · Displayed: 56 (0.3%) · Drop... Profile: Default

4. No Contain in the Option Field

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1778	28.56129.107.56.31	10.219.134.83	10.219.134.83	HTTP	622	HTTP/1.1 301 Moved Permanently (text/html)
1800	28.5710.219.134.83	129.107.56.31	129.107.56.31	HTTP	483	GET /uta/ HTTP/1.1
1806	28.58129.107.56.31	10.219.134.83	10.219.134.83	HTTP	530	HTTP/1.1 301 Moved Permanently (text/html)
1840	28.7410.219.134.83	178.255.83.1	178.255.83.1	HTTP	287	GET /MFEWTZBNMESWSTA3BgurDgMCgGUABBR8sWZUnkvBR051jhat9GV793rV1AqurB2YeJ503vf6XCZU7w094CTLVB0CEBPqKHb90z

Frame 1800: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0

Ethernet II, Src: HonHaiPr_64:c5:5d (a4:17:31:64:c5:5d), Dst: CiscoInc_27:00:00 (00:25:83:27:00:00)

Internet Protocol Version 4, Src: 10.219.134.83, Dst: 129.107.56.31

0100 = Version: 4
 0101 = Header Length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 469
 Identification: 0x4ba1 (19361)
 Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x62c9 [validation disabled]
 Source: 10.219.134.83
 Destination: 129.107.56.31
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 Transmission Control Protocol, Src Port: 50318 (50318), Dst Port: 80 (80), Seq: 319, Ack: 569, Len: 429
 Hypertext Transfer Protocol

0010 01 d5 4b a1 40 00 80 06 62 c9 0a db 86 53 81 6b ..K.E...b....S.k
 0020 38 1f c4 8e 00 50 79 b2 60 fd 1a 04 c9 44 50 18 8...Py.DP.
 0030 ff ff 78 8c 00 00 47 45 54 20 2f 75 74 61 2f 20 ..x...GE T /uta/
 0040 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 ..Accept
 0050 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 70 : text/html, app
 0060 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+x
 0070 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72 2c 20 2a ml, image/jxr, "
 0080 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 /*.Acc pt-Langu
 0090 61 67 65 3a 20 65 6e 2d 49 4e 0d 0a 55 73 65 72 age: en- IN..User
 00a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
 00b0 35 2e 30 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (win dows NT)

Flags (3 bits) (ip.flags), 1 byte

Packets: 19352 · Displayed: 56 (0.3%) · Drop... Profile: Default

5. Packet Fragmented (Don't Fragment)

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1788	28.56129	10.219.134.83	10.219.134.83	HTTP	622	HTTP/1.1 301 Moved Permanently (text/html)
1800	28.5710	10.219.134.83	129.107.56.31	HTTP	483	GET /uta/ HTTP/1.1
1806	28.58129	10.219.134.83	10.219.134.83	HTTP	530	HTTP/1.1 301 Moved Permanently (text/html)
1840	28.7410	10.219.134.83	178.255.83.1	HTTP	287	GET /MFEWTzBNMESwSTA3BgURDgMCgGUABBR8SwZUnkVbR051jhat9Gv793rV1AqurB2YeJ503vF6XCZU7w094CTLVBoCEBPqKHb90Z

Frame 1800: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
 Ethernet II, Src: HONHAIPR_64:c5:5d (a4:17:31:64:c5:5d), Dst: CiscoInc_27:00:00 (00:25:83:27:00:00)
 Internet Protocol Version 4, Src: 10.219.134.83, Dst: 129.107.56.31
 0100 = Version: 4
 0101 = Header Length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 469
 Identification: 0x4ba1 (19361)
 Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x62c9 [validation disabled]
 Source: 10.219.134.83
 Destination: 129.107.56.31
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 Transmission Control Protocol, Src Port: 50318 (50318), Dst Port: 80 (80), Seq: 319, Ack: 569, Len: 429
 Hypertext Transfer Protocol

0010 01 d5 4b a1 00 80 06 62 c9 0a db 86 53 81 6b ..K...b....S.k
 0020 38 1f c4 8e 00 50 79 b2 60 fd 1a 04 c9 44 50 18 8...Py....DP.
 0030 ff ff 78 8c 00 00 47 45 54 20 2f 75 74 61 2f 20 ..x...GE T /uta/
 0040 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1..Accept
 0050 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 70 : text/html, app
 0060 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication/xhtml+xml
 0070 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72 2c 20 2a m1, image/jxr, *
 0080 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 /*.Accept-Language
 0090 61 67 65 3a 20 65 6e 2d 49 4e 0d 0a 55 73 65 72 age: en-IN, User
 00a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
 00b0 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Windows NT
 00c0 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; Win64; x64

Flags (3 bits) (ip.flags), 1 byte Packets: 19352 · Displayed: 56 (0.3%) · Drop... Profile: Default

6. TCP Segment Length: 429

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1788	28.56129	10.219.134.83	10.219.134.83	HTTP	622	HTTP/1.1 301 Moved Permanently (text/html)
1800	28.5710	10.219.134.83	129.107.56.31	HTTP	483	GET /uta/ HTTP/1.1
1806	28.58129	10.219.134.83	10.219.134.83	HTTP	530	HTTP/1.1 301 Moved Permanently (text/html)
1840	28.7410	10.219.134.83	178.255.83.1	HTTP	287	GET /MFEWTzBNMESwSTA3BgURDgMCgGUABBR8SwZUnkVbR051jhat9Gv793rV1AqurB2YeJ503vF6XCZU7w094CTLVBoCEBPqKHb90Z

Frame 1800: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
 Ethernet II, Src: HONHAIPR_64:c5:5d (a4:17:31:64:c5:5d), Dst: CiscoInc_27:00:00 (00:25:83:27:00:00)
 Internet Protocol Version 4, Src: 10.219.134.83, Dst: 129.107.56.31
 Transmission Control Protocol, Src Port: 50318 (50318), Dst Port: 80 (80), Seq: 319, Ack: 569, Len: 429
 Source Port: 50318
 Destination Port: 80
 [Stream index: 40]
 [TCP Segment Len: 429]
 Sequence number: 319 (relative sequence number)
 [Next sequence number: 748 (relative sequence number)]
 Acknowledgment number: 569 (relative ack number)
 Header Length: 20 bytes
 Flags: 0x018 (PSH, ACK)
 Window size value: 65535
 [calculated window size: 65535]
 [window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x88c [validation disabled]
 Urgent pointer: 0
 [Seq/Ack analysis]
 Hypertext Transfer Protocol

0020 38 1f c4 8e 00 50 79 b2 60 fd 1a 04 c9 44 50 18 8...Py....DP.
 0030 ff ff 78 8c 00 00 47 45 54 20 2f 75 74 61 2f 20 ..x...GE T /uta/
 0040 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1..Accept
 0050 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 70 : text/html, app
 0060 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication/xhtml+xml
 0070 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72 2c 20 2a m1, image/jxr, *
 0080 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 /*.Accept-Language
 0090 61 67 65 3a 20 65 6e 2d 49 4e 0d 0a 55 73 65 72 age: en-IN, User
 00a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
 00b0 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Windows NT
 00c0 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; Win64; x64

TCP Segment Len (tcp.len), 1 byte Packets: 19352 · Displayed: 56 (0.3%) · Drop... Profile: Default

7. Sequence Number of TCP Segment is 319

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1788	28.56129.107.56.31	10.219.134.83	HTTP	622	HTTP/1.1 301 Moved Permanently (text/html)	
1800	28.5710.219.134.83	129.107.56.31	HTTP	483	GET /uta/ HTTP/1.1	
1806	28.56129.107.56.31	10.219.134.83	HTTP	530	HTTP/1.1 301 Moved Permanently (text/html)	
1840	28.7410.219.134.83	178.255.83.1	HTTP	287	GET /MFEWTZBNMESWSTA3BgurDgMCgUABBR8SwZUnkvBR051Jhat9GV793rV1AqurB2YeJ50JvF6XCZU7w094CTLVBoCEBPqKHb90Z	

Frame 1800: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
 Ethernet II, Src: HONHaIPr_64:c5:5d (a4:17:31:64:c5:5d), Dst: ciscoInc_27:00:00 (00:25:83:27:00:00)
 Internet Protocol Version 4, Src: 10.219.134.83, Dst: 129.107.56.31
 Transmission Control Protocol, Src Port: 50318 (50318), Dst Port: 80 (80), Seq: 319, Ack: 569, Len: 429
 Source Port: 50318
 Destination Port: 80
 [Stream index: 40]
 [TCP Segment Len: 429]
 Sequence number: 319 (relative sequence number)
 [Next sequence number: 748 (relative sequence number)]
 Acknowledgment number: 569 (relative ack number)
 Header Length: 20 bytes
 Flags: 0x018 (PSH, ACK)
 Window size value: 65535
 [Calculated window size: 65535]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x7886 [validation disabled]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 Hypertext Transfer Protocol

0020 38 1f c4 8e 00 50 79 b2 60 fc 1a 04 c9 44 50 18 8...PZ...DP
 0030 ff ff 78 8c 00 00 47 45 54 20 2f 75 74 61 2f 20 ..X...GE T /uta/
 0040 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 ..Accept
 0050 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 70 :text/html, app
 0060 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /html+x
 0070 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72 2c 20 2a m1, image/jxr, *
 0080 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 /..Accept-Langu
 0090 61 67 65 3a 20 65 6e 2d 49 4e 0d 0a 55 73 65 72 age: en-IN, User
 00a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
 00b0 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (win dows NT
 00c0 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; w1 n64; x64

Sequence number (tcp.seq), 4 bytes Packets: 19352 · Displayed: 56 (0.3%) · Drop... Profile: Default

8. Acknowledgment Number = Tcp segment Length + sequence Number = 748

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1788	28.56129.107.56.31	10.219.134.83	HTTP	622	HTTP/1.1 301 Moved Permanently (text/html)	
1800	28.5710.219.134.83	129.107.56.31	HTTP	483	GET /uta/ HTTP/1.1	
1806	28.56129.107.56.31	10.219.134.83	HTTP	530	HTTP/1.1 301 Moved Permanently (text/html)	
1840	28.7410.219.134.83	178.255.83.1	HTTP	287	GET /MFEWTZBNMESWSTA3BgurDgMCgUABBR8SwZUnkvBR051Jhat9GV793rV1AqurB2YeJ50JvF6XCZU7w094CTLVBoCEBPqKHb90Z	

Frame 1806: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
 Ethernet II, Src: ciscoInc_27:00:00 (00:25:83:27:00:00), Dst: HONHaIPr_64:c5:5d (a4:17:31:64:c5:5d)
 Internet Protocol Version 4, Src: 129.107.56.31, Dst: 10.219.134.83
 Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50318 (50318), Seq: 569, Ack: 748, Len: 476
 Source Port: 80
 Destination Port: 50318
 [Stream index: 40]
 [TCP segment Len: 476]
 Sequence number: 569 (relative sequence number)
 [Next sequence number: 1045 (relative sequence number)]
 Acknowledgment number: 748 (relative ack number)
 Header Length: 20 bytes
 Flags: 0x018 (PSH, ACK)
 Window size value: 4887
 [Calculated window size: 4887]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x6178 [validation disabled]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 Hypertext Transfer Protocol

0020 86 53 00 50 c4 8e 1a 04 c9 44 69 b2 60 3a 50 18 .S.P... ..VADP
 0030 13 1f 61 78 00 00 48 54 54 20 2f 31 2e 31 20 33 ..ak, HT TP/1.1 3
 0040 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 01 Moved Permane
 0050 6e 74 6c 79 0d 0a 44 61 74 65 3a 20 57 65 64 2c ntly..da te: wed,
 0060 20 32 38 20 4d 61 72 20 32 30 31 38 20 30 32 3a 28 Mar 2018 02:
 0070 33 38 3a 34 38 20 47 4d 54 0d 0a 53 65 72 76 65 38:48 gW T..Serve
 0080 72 3a 20 41 70 61 63 68 65 0d 0a 4c 6f 63 61 74 r: Apach e..Locat
 0090 69 6f 6e 3a 20 68 74 74 70 73 3a 2f 2f 77 77 77 ion: htt ps://ww
 00a0 2e 75 74 61 2e 65 64 75 2f 75 74 61 2f 0d 0a 43 .uta.edu /uta/.C
 00b0 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 ontent-L ength: 2
 00c0 33 32 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 32..keep -Alive:

Acknowledgment number (tcp.ack), 4 bytes Packets: 19352 · Displayed: 56 (0.3%) · Drop... Profile: Default

9. PSH flag is used in this packet capture

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list shows a packet from 129.107.56.31 to 10.219.134.83. The packet details pane shows the following information:

- Ethernet II**, Src: CiscoInc_27:00:00 (00:25:83:27:00:00), Dst: HonHaiPr_64:c5:5d (a4:17:31:64:c5:5d)
- Internet Protocol Version 4**, Src: 129.107.56.31, Dst: 10.219.134.83
- Transmission Control Protocol**, Src Port: 80 (80), Dst Port: 50318 (50318), Seq: 569, Ack: 748, Len: 476
 - Source Port: 80
 - Destination Port: 50318
 - [Stream index: 40]
 - [TCP Segment Len: 476]
 - Sequence number: 569 (relative sequence number)
 - [Next sequence number: 1045 (relative sequence number)]
 - Acknowledgment number: 748 (relative ack number)
 - Header Length: 20 bytes
 - Flags: 0x018 (PSH, ACK)**
 - Window size value: 4887
 - [Calculated window size: 4887]
 - [Window size scaling factor: -2 (no window scaling used)]
 - Checksum: 0x6178 [validation disabled]
 - Urgent pointer: 0
 - [Seq/Ack analysis]
- Hypertext Transfer Protocol**
- Line-based text data: text/html**

The packet bytes pane shows the raw data of the packet, including the HTTP GET request and the HTML response body.

10. IP address of UTA.edu = 129.107.56.31 Sending Port No= 80 Receiving Port No. = 50318

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list shows a packet from 129.107.56.31 to 10.219.134.83. The packet details pane shows the following information:

- Ethernet II**, Src: CiscoInc_27:00:00 (00:25:83:27:00:00), Dst: HonHaiPr_64:c5:5d (a4:17:31:64:c5:5d)
- Internet Protocol Version 4**, Src: 129.107.56.31, Dst: 10.219.134.83
- Transmission Control Protocol**, Src Port: 80 (80), Dst Port: 50318 (50318), Seq: 569, Ack: 748, Len: 476
 - Source Port: 80
 - Destination Port: 50318
 - [Stream index: 40]
 - [TCP Segment Len: 476]
 - Sequence number: 569 (relative sequence number)
 - [Next sequence number: 1045 (relative sequence number)]
 - Acknowledgment number: 748 (relative ack number)
 - Header Length: 20 bytes
 - Flags: 0x018 (PSH, ACK)**
 - Window size value: 4887
 - [Calculated window size: 4887]
 - [Window size scaling factor: -2 (no window scaling used)]
 - Checksum: 0x6178 [validation disabled]
 - Urgent pointer: 0
 - [Seq/Ack analysis]
- Hypertext Transfer Protocol**
- Line-based text data: text/html**

The packet bytes pane shows the raw data of the packet, including the HTTP GET request and the HTML response body.

Section 2: Analysing the Connection Parameters in TCP

Problem Set 2:

- Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and youtube.com is trace to 0. The Absolute Sequence number is 43 e5 a7 1b c...

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
50	6.93172	172.217.9.14	10.219.134.83	TCP	60	443 → 64483 [ACK] Seq=377 Ack=770 win=435 Len=0
51	6.9518	8.8.8	10.219.134.83	DNS	133	Standard query response 0xe936 A upload.youtube.com CNAME yt-video-upload.1.google.com A 172.217.
52	6.9510	10.219.134.83	172.217.12.47	TCP	66	64508 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
53	6.964172	172.217.12.47	10.219.134.83	TCP	66	443 → 64508 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=256

Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: HonHaiPr_64:c5:5d (a4:17:31:64:c5:5d), Dst: CiscoInc_27:00:00 (00:25:83:27:00:00)

Internet Protocol Version 4, Src: 10.219.134.83, Dst: 172.217.12.47

Transmission Control Protocol, Src Port: 64508 (64508), Dst Port: 443 (443), Seq: 0, Len: 0

Source Port: 64508

Destination Port: 443

[Stream index: 6]

[TCP segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 0

Header Length: 32 bytes

Flags: 0x002 (SYN)

Window size value: 64240

[calculated window size: 64240]

Checksum: 0x4130 [validation disabled]

Urgent pointer: 0

Options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, No-operation (NOP), No-operation (NOP), SACK permitted

0000 00 25 83 27 00 00 a4 17 31 64 c5 5d 08 00 45 00 .%. '.... 1d.]..E.

0010 00 34 3f 06 40 00 80 06 71 87 0a db 86 53 ac d9 .4?@... q...S..

0020 0c 2f fb fc 01 bb 43 e5 a7 1b 00 00 00 00 80 02 ./... [redacted]

0030 fa f0 41 30 00 00 02 04 05 b4 01 03 03 08 01 01 ..A0.....

0040 04 02 ..

Sequence number (tcp.seq), 4 bytes Packets: 14311 · Displayed: 14311 (100.0%) · ... Profile: Default

- The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
50	6.93172	172.217.9.14	10.219.134.83	TCP	60	443 → 64483 [ACK] Seq=377 Ack=770 win=435 Len=0
51	6.9518	8.8.8	10.219.134.83	DNS	133	Standard query response 0xe936 A upload.youtube.com CNAME yt-video-upload.1.google.com A 172.217.
52	6.9510	10.219.134.83	172.217.12.47	TCP	66	64508 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
53	6.964172	172.217.12.47	10.219.134.83	TCP	66	443 → 64508 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=256

Transmission Control Protocol, Src Port: 64508 (64508), Dst Port: 443 (443), Seq: 0, Len: 0

Source Port: 64508

Destination Port: 443

[Stream index: 6]

[TCP segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 0

Header Length: 32 bytes

Flags: 0x002 (SYN)

000. = 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: 64240

0000 00 25 83 27 00 00 a4 17 31 64 c5 5d 08 00 45 00 .%. '.... 1d.]..E.

0010 00 34 3f 06 40 00 80 06 71 87 0a db 86 53 ac d9 .4?@... q...S..

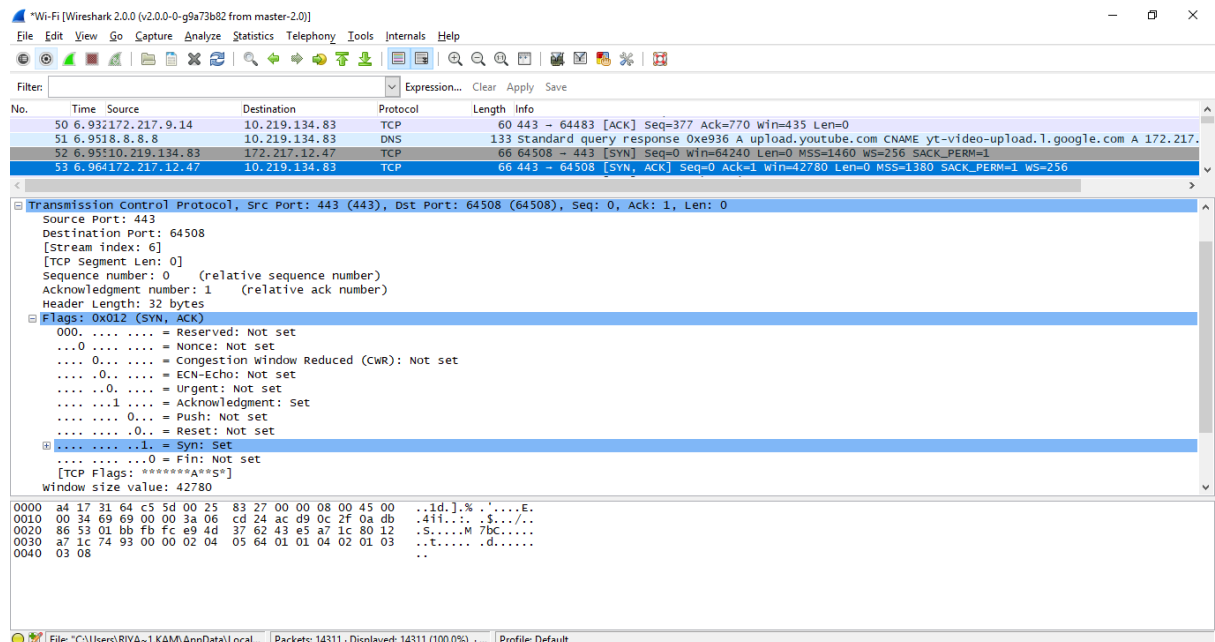
0020 0c 2f fb fc 01 bb 43 e5 a7 1b 00 00 00 00 80 02 ./... [redacted]

0030 fa f0 41 30 00 00 02 04 05 b4 01 03 03 08 01 01 ..A0.....

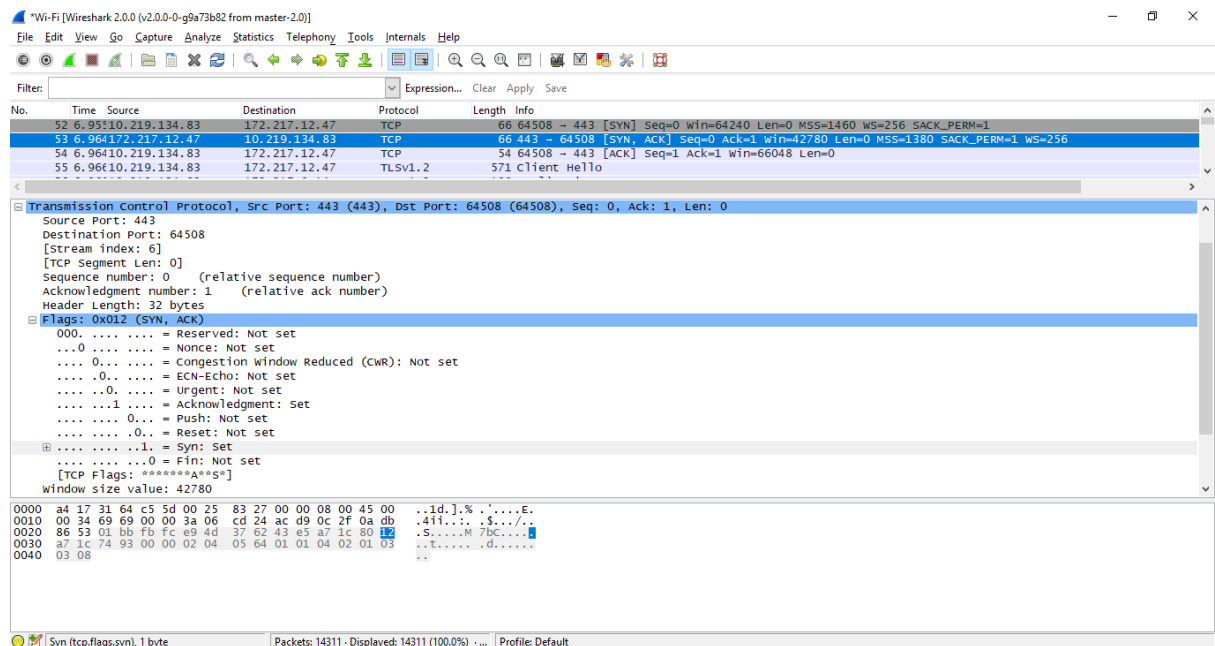
0040 04 02 ..

Sequence number (tcp.seq), 4 bytes Packets: 14311 · Displayed: 14311 (100.0%) · ... Profile: Default

3. Sequence number of the SYNACK segment from youtube.com to the client computer in reply to the SYN has the value of 0 in this trace. The value of the Acknowledgement field in the SYNACK segment is 1.



4. The value of the Acknowledgement field (i.e. Acknowledgement number =1) in the SYNACK segment is determined by youtube.com by adding 1 to the initial sequence number of SYN segment(i.e. Sequence number =0) from the client computer. The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.



Section 3: Analysis of the trace provided

Problem Set 3:

1. Sequence Number is 1415

The screenshot shows a Wireshark packet capture of a TCP segment. The packet list shows a segment with sequence number 1415. The packet details pane shows the following information:

- Frame 140: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
- Ethernet II, Src: Apple_8b:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)
- Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231
- Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 1415, Ack: 56130, Len: 1388
- Source Port: 55790
- Destination Port: 80
- [Stream index: 4]
- [TCP segment Len: 1388]
- Sequence number: 1415 (relative sequence number)
- [Next sequence number: 2803 (relative sequence number)]
- Acknowledgment number: 56130 (relative ack number)
- Header Length: 32 bytes
- Flags: 0x010 (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
-0. = SYN: Not set

The packet bytes pane shows the raw data of the segment, including the sequence number 1415.

2. i. Segment 1: Sequence Number = 1415

The screenshot shows a Wireshark packet capture of a TCP segment. The packet list shows a segment with sequence number 1415. The packet details pane shows the following information:

- Frame 140: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
- Ethernet II, Src: Apple_8b:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)
- Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231
- Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 1415, Ack: 56130, Len: 1388
- Source Port: 55790
- Destination Port: 80
- [Stream index: 4]
- [TCP segment Len: 1388]
- Sequence number: 1415 (relative sequence number)
- [Next sequence number: 2803 (relative sequence number)]
- Acknowledgment number: 56130 (relative ack number)
- Header Length: 32 bytes
- Flags: 0x010 (ACK)
- 000. = Reserved: Not set
- ...0 = Nonce: Not set

The packet bytes pane shows the raw data of the segment, including the sequence number 1415.

Segment 2: Sequence Number = 2803

kayak.pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
138	4.080945	209.105.248.3	172.20.10.2	TCP	74	443 → 55806 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1 TSval=9846119
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 Win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 Win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 Win=77 Len=0 TSval=51237230 TSecr=105870899

Frame 141: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface 0

Ethernet II, Src: Apple_Bb:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)

Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231

Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 2803, Ack: 56130, Len: 135

Source Port: 55790

Destination Port: 80

[Stream index: 4]

[TCP Segment Len: 135]

Sequence number: 2803 (relative sequence number)

[Next sequence number: 2938 (relative sequence number)]

Acknowledgment number: 56130 (relative ack number)

Header Length: 32 bytes

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0. = Nonce: Not set

Sequence number (tcp.seq), 4 bytes

Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

Segment 3: Sequence Number = 2938

kayak.pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
138	4.080945	209.105.248.3	172.20.10.2	TCP	74	443 → 55806 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1 TSval=9846119
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 Win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 Win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 Win=77 Len=0 TSval=51237230 TSecr=105870899

Frame 142: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0

Ethernet II, Src: Apple_Bb:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)

Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231

Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 2938, Ack: 56130, Len: 9

Source Port: 55790

Destination Port: 80

[Stream index: 4]

[TCP Segment Len: 9]

Sequence number: 2938 (relative sequence number)

[Next sequence number: 2947 (relative sequence number)]

Acknowledgment number: 56130 (relative ack number)

Header Length: 32 bytes

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0. = Nonce: Not set

Sequence number (tcp.seq), 4 bytes

Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

Segment 4: Sequence Number = 2947

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
172	4.570189	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
173	4.570191	172.20.10.2	23.235.44.231	TCP	210	[TCP segment of a reassembled PDU]
174	4.570353	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
175	4.570354	172.20.10.2	23.235.44.231	HTTP	175	GET /s/run/recentsearchhistory/gethistory?searchtype=hotel&maxSearchHistoryNum=30&searchHist
176	4.571636	172.20.10.2	23.235.44.231	HTTP	85	POST /s/run/hotelbookmsg HTTP/1.1 (application/x-www-form-urlencoded)
177	4.572121	172.20.10.2	216.58.218.194	TLSv1.2	352	Application Data
178	4.575141	172.20.10.2	172.20.10.1	DNS	74	Standard query 0xcbe2 A www.google.com
179	4.640828	173.194.115.60	172.20.10.2	TCP	74	443 → 55807 [SYN, ACK] Seq=0 Ack=1 win=42540 Len=0 MSS=1400 SACK_PERM=1 TSval=995256744 TSecr=995256744
180	4.640909	172.20.10.2	173.194.115.60	TCP	66	55807 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105871449 TSecr=995256744

Frame 174: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0

Ethernet II, Src: Apple_8b:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)

Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231

Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 2947, Ack: 56939, Len: 1388

Source Port: 55790

Destination Port: 80

[Stream index: 4]

[TCP Segment Len: 1388]

Sequence number: 2947 (relative sequence number)

[Next sequence number: 4335 (relative sequence number)]

Acknowledgment number: 56939 (relative ack number)

Header Length: 32 bytes

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

0020 2c e7 d9 ee 00 50 12 fc 13 cb 3f 57 a8 a2 80 10P...PW...

0030 10 00 7c 84 00 00 01 08 0a 06 4f 78 14 03 0dOX...

0040 d1 7f 47 45 54 20 2f 73 2f 72 75 6e 2f 72 65 63 ...GET /s/run/rec

0050 65 6e 74 73 65 61 72 63 68 68 69 73 74 6f 72 79 entsear chhistory

0060 2f 67 65 74 68 69 73 74 6f 72 79 3f 73 65 61 72 /gethist ory?sear

0070 63 68 54 79 70 65 3d 68 6f 74 65 6c 26 6d 61 78 chtype= otel&max

0080 53 65 61 72 63 68 68 69 73 74 6f 72 79 4e 75 6d searchhl storynum

0090 3d 33 30 26 73 65 61 72 63 68 68 69 73 74 6f 72 =30&sear chHistor

00a0 79 53 75 62 74 79 70 65 3d 20 48 54 54 50 2f 31 ySubtype = HTTP/1

00b0 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 72 6b 61 .1..Host : www.ka

00c0 79 61 6b 2e 63 6f 6d 0d 0a 41 63 63 65 70 74 2d yak.com..Accept-

Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

ii.

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
138	4.080945	209.105.248.3	172.20.10.2	TCP	74	443 → 55806 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1 TSval=98461199 TSecr=98461199
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899

Frame 140: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0

Interface id: 0 (en0)

Encapsulation type: Ethernet (1)

Arrival Time: Nov 6, 2015 14:25:52.121608000 Central America Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1446841552.121608000 seconds

[Time delta from previous captured frame: 0.000484000 seconds]

[Time delta from previous displayed frame: 0.000484000 seconds]

[Time since reference or first frame: 4.081502000 seconds]

Frame Number: 140

Frame Length: 1454 bytes (11632 bits)

Capture Length: 1454 bytes (11632 bits)

[Frame is marked: False]

[Frame is ignored: False]

0000 fa cf 9c 21 5f 64 6c 40 08 8b 6e 80 08 00 45 00 ...|dl@ ..n...E.

0010 05 a0 d5 66 40 00 00 06 65 09 ac 14 0a 02 17 eb ...f@. e.....

0020 2c e7 d9 ee 00 50 12 fc 0d cf 3f 57 a5 79 80 10P...?W.Y...

0030 10 00 36 9a 00 00 01 01 08 0a 06 4f 76 33 03 0d ...6.....Ov3...

0040 d1 4e 50 4f 53 54 20 2f 76 73 2f 70 61 67 65 2f .NPOST /vs/page/

0050 68 6f 74 65 6c 2f 72 63 73 6c 74 73 20 48 54 hotel/re sults HT

0060 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 TP/1.1.. Host: ww

0070 77 2e 6b 61 79 61 6b 2e 63 6f 6d 0d 0a 41 63 63 w.kayak. com..Acc

0080 65 70 74 3a 20 2a 2f 2a 0d 0a 58 2d 52 65 71 75 ept: /?/..X-Requ

0090 65 73 74 65 64 2d 57 69 74 68 3a 20 58 4d 4c 48 ested-wi th: XMLH

00a0 74 74 70 52 65 71 75 65 73 74 0d 0a 41 63 63 65 ttpReque st..Acce

00b0 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-

00c0 75 73 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 us..Acce pt-Encod

00d0 60 6a 67 2a 70 67 7a 60 70 7c 70 64 65 6e 6c 61 3nn...n...dofl3

Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
138	4.080945	209.105.248.3	172.20.10.2	TCP	74	443 → 55806 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1 TSval=9846119
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899

Frame 141: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface 0
 Interface id: 0 (en0)
 Encapsulation type: Ethernet (1)
 Arrival Time: Nov 6, 2015 14:25:52.121609000 central America Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1446841552.121609000 seconds
 [Time delta from previous captured frame: 0.000001000 seconds]
 [Time delta from previous displayed frame: 0.000001000 seconds]
 [Time since reference or first frame: 4.081503000 seconds]
 Frame Number: 141
 Frame Length: 201 bytes (1608 bits)
 Capture Length: 201 bytes (1608 bits)
 [Frame is marked: False]
 [Frame is ignored: False]

0000 Fa cf 9c 21 5f 64 6c 40 08 8b 6e 80 08 00 45 00 ...!dl@..n...E.
 0010 00 bb 82 1d 40 00 40 06 bd 37 ac 14 0a 02 17 eb ...@.@..7.....
 0020 2c e7 d9 ee 00 50 12 fc 13 c2 3f 57 a5 79 80 18P...?W.Y..
 0030 10 00 3f 66 00 00 01 01 08 0a 06 4f 76 33 03 0dOv3..
 0040 d1 4e 62 63 79 32 37 45 70 66 65 75 78 78 50 69 .NBcy27E pfeuxxP
 0050 75 32 65 69 75 39 6a 66 54 72 6d 61 53 52 55 4d u2eiU9Jf TrmaQRUM
 0060 46 33 3b 20 70 31 2e 6d 65 64 2e 74 6f 6b 65 6e F3; pl; n ed.token
 0070 3d 4b 4e 75 56 36 36 6b 4a 77 6c 53 34 34 64 48 =KNUV66k Jw1S44dH
 0080 47 59 79 57 65 4c 65 3b 20 5f 67 61 3d 47 41 31 Gyyweler; _ga=GA1
 0090 2e 32 2e 35 33 39 38 30 39 34 35 36 2e 31 34 34 .2.33980 9456.144
 00a0 36 38 34 31 32 35 39 3b 20 5f 67 61 74 3d 31 3b 6841259; _gat=1;
 00b0 20 5f 67 61 74 5f 55 41 2d 34 32 32 30 39 31 38 _gat_UA -4220918
 00c0 35 2d 38 3d 31 0d 0a 0d 0a 5-8=1....

Time relative to time reference or first frame... Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
138	4.080945	209.105.248.3	172.20.10.2	TCP	74	443 → 55806 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1 TSval=9846119
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899

Frame 142: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
 Interface id: 0 (en0)
 Encapsulation type: Ethernet (1)
 Arrival Time: Nov 6, 2015 14:25:52.121709000 central America Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1446841552.121709000 seconds
 [Time delta from previous captured frame: 0.000100000 seconds]
 [Time delta from previous displayed frame: 0.000100000 seconds]
 [Time since reference or first frame: 4.081603000 seconds]
 Frame Number: 142
 Frame Length: 75 bytes (600 bits)
 Capture Length: 75 bytes (600 bits)
 [Frame is marked: False]
 [Frame is ignored: False]

0000 Fa cf 9c 21 5f 64 6c 40 08 8b 6e 80 08 00 45 00 ...!dl@..n...E.
 0010 00 3d 3b 7b 40 00 40 06 04 58 ac 14 0a 02 17 eb .;{@.@..X.....
 0020 2c e7 d9 ee 00 50 12 fc 13 c2 3f 57 a5 79 80 18P...?W.Y..
 0030 10 00 3f 66 00 00 01 01 08 0a 06 4f 76 33 03 0dOv3..
 0040 d1 4e 61 63 74 69 6f 6e 3d 76 73 .Naction=VS

Frame (75 bytes) Reassembled TCP (1532 bytes)

Time relative to time reference or first frame... Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
167	4.307258	172.20.10.2	23.235.44.231	TCP	66	55789 → 80 [ACK] Seq=4703 Ack=7633 Win=4077 Len=0 TSval=105871118 TSecr=917517986
168	4.335350	209.105.248.3	172.20.10.2	TLSv1	679	Application Data
169	4.335424	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1014 Ack=759 Win=131072 Len=0 TSval=105871146 TSecr=98461224
170	4.346970	209.105.248.3	172.20.10.2	TCP	78	[TCP Dup ACK 168#1] 443 → 55806 [ACK] Seq=759 Ack=1014 Win=131328 Len=0 TSval=98461226 TSecr=
171	4.564246	172.20.10.2	173.194.115.60	TCP	78	55807 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=105871374 TSecr=0 SACK_PERM=1
172	4.570189	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
173	4.570191	172.20.10.2	23.235.44.231	TCP	210	[TCP segment of a reassembled PDU]
174	4.570353	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
175	4.570354	172.20.10.2	23.235.44.231	HTTP	175	GET /s/run/recentsearchhistory/gethistory?searchtype=hotel&maxsearchHistoryNum=30&searchHis

Frame 174: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
 Interface id: 0 (en0)
 Encapsulation type: Ethernet (1)
 Arrival Time: Nov 6, 2015 14:25:52.610459000 Central America Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1446841552.610459000 seconds
 [Time delta from previous captured frame: 0.000162000 seconds]
 [Time delta from previous displayed frame: 0.000162000 seconds]
 [Time since reference or first frame: 4.570353000 seconds]
 Frame Number: 174
 Frame Length: 1454 bytes (11632 bits)
 Capture Length: 1454 bytes (11632 bits)
 [Frame is marked: False]
 [Frame is ignored: False]

0000 Fa cf 9c 21 5f 64 6c 40 08 8b 6e 80 08 00 45 00 ...!_d!@ .n...E.
 0010 05 a0 4e 26 40 00 40 06 ec 49 ac 14 0a 02 17 eb ...N&@.0..I.....
 0020 2c e7 d9 ee 00 50 12 fc 13 cb 3f 57 a8 a2 80 10P...?w....
 0030 10 00 7c 84 00 00 01 01 08 0a 06 4f 78 14 03 0d ...!.....Ox....
 0040 d1 7f 47 45 54 20 2f 73 2f 72 75 6e 2f 72 65 63 ..GET /s/run/rec
 0050 65 6e 74 73 65 61 72 63 68 68 69 73 74 6f 72 79 entsear chistory
 0060 2f 6f 65 74 68 69 73 74 6f 72 79 3f 73 65 61 72 /gethist ory?sear
 0070 63 68 54 79 70 65 63 6d 68 6f 74 65 6c 26 6d 61 78 chType=h otel&max
 0080 53 65 61 72 63 68 48 69 73 74 6f 72 79 4e 75 6d SearchH1 storyNum
 0090 3d 33 30 26 73 65 61 72 63 68 48 69 73 74 6f 72 =30&sear chistor
 00a0 79 53 75 62 74 79 70 65 3d 20 48 54 54 50 2f 31 ysubtype = HTTP/1
 00b0 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6b 61 ..I..Host : www.ka
 00c0 79 61 6b 2e 63 6d 0d 0a 41 63 65 70 74 2d yak.com. .Accept-
 00d0 42 61 6e 73 61 6f 6e 73 7a 65 6e 74 75 73 0d .application/x-w

Time relative to time reference or first frame... Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

From the above observations in the screenshot, below is the details for the Segment Sent Time:

	Segment 1	Segment 2	Segment 3	Segment 4
Segment Sent Time	4.081502000 sec	4.081503000 sec	4.081603000 sec	4.570353000 sec

iii.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
138	4.080945	209.105.248.3	172.20.10.2	TCP	74	443 → 55806 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1 TSval=98461199
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=36130 Ack=2803 Win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=36130 Ack=2938 Win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=36130 Ack=2947 Win=77 Len=0 TSval=51237230 TSecr=105870899

Frame 144: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Interface id: 0 (en0)
 Encapsulation type: Ethernet (1)
 Arrival Time: Nov 6, 2015 14:25:52.175469000 Central America Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1446841552.175469000 seconds
 [Time delta from previous captured frame: 0.052510000 seconds]
 [Time delta from previous displayed frame: 0.052510000 seconds]
 [Time since reference or first frame: 4.135363000 seconds]
 Frame Number: 144
 Frame Length: 66 bytes (528 bits)
 Capture Length: 66 bytes (528 bits)
 [Frame is marked: False]
 [Frame is ignored: False]

0000 6c 40 08 8b 6e 80 fa cf 9c 21 5f 64 08 00 45 00 |@.n...!_d!..E.
 0010 00 34 04 cf 00 00 35 06 8e 0d 17 eb 2c e7 ac 14 .4...S.....
 0020 0a 02 00 50 d9 ee 3f 57 a5 79 12 fc 13 3b 80 10 ...P...?w .y.....
 0030 00 48 45 48 00 00 01 01 08 0a 03 0d d1 6e 06 4f .HEH....n.O
 0040 76 33 V3

Time relative to time reference or first frame... Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

*Above screenshot shows the received time for the 1st Segment only

	Segment 1	Segment 2	Segment 3	Segment 4
Segment Received Time	4.135363000 sec	4.135713000 sec	4.135716000 sec	4.646868000 sec

iv. RTT value for the segments are mentioned below:

	Segment 1	Segment 2	Segment 3	Segment 4
RTT	0.053861 sec	0.05421 sec	0.054113 sec	0.076515 sec

- **Estimated RTT = 0.875 * Estimated RTT + 0.125 * Sample RTT**

For Segment 1:

Estimated RTT = RTT for the first segment = 0.053861 sec (Will be used in segment 2)

For Segment 2:

Estimated RTT = $0.875 * 0.053861 + 0.125 * 0.05421 = 0.05390$ sec (Will be used in segment 3)

For Segment 3:

Estimated RTT = $0.875 * 0.05390 + 0.125 * 0.054113 = 0.05393$ sec (Will be used in segment 4)

For Segment 4:

Estimated RTT = $0.875 * 0.05390 + 0.125 * 0.054113 = 0.05393$ sec (Will be used in next segment)

3. For Length of Segments:

The image shows a Wireshark packet capture of a TCP segment. The packet list pane shows a packet of length 1388 bytes. The packet details pane shows the following information:

- Frame 140: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
- Ethernet II, Src: Apple_8b:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)
- Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231
- Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 1415, Ack: 56130, Len: 1388
- Source Port: 55790
- Destination Port: 80
- [Stream index: 4]
- [TCP Segment Len: 1388]
- Sequence number: 1415 (relative sequence number)
- [Next sequence number: 2803 (relative sequence number)]
- Acknowledgment number: 56130 (relative ack number)
- Header Length: 32 bytes
- EFlags: SYN, FIN, ACK

The packet bytes pane shows the raw data of the TCP segment, starting with 0020 2c e7 d9 ee 00 12 fc 0d cf 3f 57 a5 79 08 10, which corresponds to the sequence number 1415.

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899
147	4.136062	209.105.248.3	172.20.10.2	TLSv1	211	Server Hello, Change Cipher Spec, Encrypted Handshake Message
148	4.136121	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=518 Ack=146 win=131712 Len=0 TSval=105870952 TSecr=98461204
149	4.136418	172.20.10.2	209.105.248.3	TLSv1	72	Change Cipher Spec
150	4.136474	172.20.10.2	209.105.248.3	TLSv1	119	Encrypted Handshake Message
151	4.137150	172.20.10.2	209.105.248.3	TLSv1	503	Application Data
152	4.151176	23.235.44.231	172.20.10.2	TCP	1016	[TCP segment of a reassembled PDU]

Frame 141: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface 0

Ethernet II, Src: Apple_Bb:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)

Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231

Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 2803, Ack: 56130, Len: 135

Source Port: 55790

Destination Port: 80

[Stream index: 4]

[TCP Segment Len: 135]

Sequence number: 2803 (relative sequence number)

[Next sequence number: 2938 (relative sequence number)]

Acknowledgment number: 56130 (relative ack number)

Header Length: 32 bytes

Flags: 0x018 (PSH, ACK)

0020 2c e7 d9 ee 00 50 12 fc 13 3b 3f 57 a5 79 80 18P...?W...
 0030 10 00 9e a8 00 00 01 01 08 0a 06 4f 76 33 03 0dOv3..
 0040 d1 4e 42 63 79 32 37 45 70 66 65 75 78 78 50 69 .NBcy27e pfeuxxP
 0050 75 32 65 69 75 39 6a 66 54 72 6d 61 51 52 55 4d u2efu3ff TrmaQRUM
 0060 46 33 3b 20 70 31 2e 6d 65 64 2e 74 6f 6b 65 6e F3: p1.n ed.token
 0070 3d 4b 4e 75 56 36 36 6b 4a 77 6c 53 34 34 64 48 =KNUV66k Jw1S44dH
 0080 47 59 79 57 65 4c 65 3b 20 5f 67 61 3d 47 41 31 Gyywlee: ga=641
 0090 2e 32 2e 35 39 38 30 39 34 35 36 2e 31 34 34 .2.33080 9456.144
 00a0 36 38 34 31 32 35 39 3b 20 5f 67 61 74 3d 31 3b 6R41259: nat=1

TCP Segment Len (tcp.len), 1 byte Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
140	4.081502	172.20.10.2	23.235.44.231	TCP	1454	[TCP segment of a reassembled PDU]
141	4.081503	172.20.10.2	23.235.44.231	TCP	201	[TCP segment of a reassembled PDU]
142	4.081603	172.20.10.2	23.235.44.231	HTTP	75	POST /vs/page/hotel/results HTTP/1.1 (application/x-www-form-urlencoded)
143	4.082853	172.20.10.2	209.105.248.3	TLSv1	583	Client Hello
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899
147	4.136062	209.105.248.3	172.20.10.2	TLSv1	211	Server Hello, Change Cipher Spec, Encrypted Handshake Message
148	4.136121	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=518 Ack=146 win=131712 Len=0 TSval=105870952 TSecr=98461204
149	4.136418	172.20.10.2	209.105.248.3	TLSv1	72	Change Cipher Spec
150	4.136474	172.20.10.2	209.105.248.3	TLSv1	119	Encrypted Handshake Message
151	4.137150	172.20.10.2	209.105.248.3	TLSv1	503	Application Data
152	4.151176	23.235.44.231	172.20.10.2	TCP	1016	[TCP segment of a reassembled PDU]

Frame 142: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0

Ethernet II, Src: Apple_Bb:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)

Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.235.44.231

Transmission Control Protocol, Src Port: 55790 (55790), Dst Port: 80 (80), Seq: 2938, Ack: 56130, Len: 9

Source Port: 55790

Destination Port: 80

[Stream index: 4]

[TCP Segment Len: 9]

Sequence number: 2938 (relative sequence number)

[Next sequence number: 2947 (relative sequence number)]

Acknowledgment number: 56130 (relative ack number)

Header Length: 32 bytes

Flags: 0x018 (PSH, ACK)

0000 fa cf 9c 21 5f 64 6c 40 08 8b 6e 80 08 00 45 00 ...!d!e...n...E.
 0010 00 3d 3b 7b 40 00 40 06 04 58 ac 14 0a 02 17 eb .;{@.0..X.....
 0020 2c e7 d9 ee 00 50 12 fc 13 32 3f 57 a5 79 80 18P...?W...
 0030 10 00 9e a8 00 00 01 01 08 0a 06 4f 76 33 03 0dOv3..
 0040 d1 4e 61 63 74 69 6f 6e 3d 76 73Naction =vs

Frame (75 bytes) Reassembled TCP (1532 bytes)

TCP Segment Len (tcp.len), 1 byte Packets: 1219 - Displayed: 1219 (100.0%) - Lo... Profile: Default

From the above screenshots for the 4 Segments, we can infer the length of the segments

- Length of Segment 1: 1388
- Length of Segment 2: 135
- Length of Segment 3: 9
- Length of Segment 4: 1388

4. Minimum amount of available buffer space advertised at the receiver: 66

5. No, lack of the receiver buffer space doesn't throttle the sender.

6. Yes, there are 8 retransmitted segments in the trace file. For checking the same, we can apply the filter “tcp.analysis.retransmission” as shown below in the screenshot.

Filter: **tcp.analysis.retransmission**

No.	Time	Source	Destination	Protocol	Length	Info
6	0.025943	172.20.10.2	173.194.115.90	TCP	66	[TCP Retransmission] 55720 → 443 [FIN, ACK] Seq=1 Ack=65 Win=4096 Len=0 TSval=105866879 TSecr=
7	0.025944	172.20.10.2	173.194.115.90	TCP	66	[TCP Retransmission] 55720 → 443 [FIN, ACK] Seq=1 Ack=65 Win=4096 Len=0 TSval=105866879 TSecr=
8	0.058891	173.194.115.90	172.20.10.2	TLSv1.2	129	[TCP Spurious Retransmission] Application Data
9	0.058976	172.20.10.2	173.194.115.90	TCP	78	[TCP Retransmission] 55720 → 443 [FIN, ACK] Seq=1 Ack=65 Win=4096 Len=0 TSval=105866913 TSecr=
15	1.757791	172.20.10.2	104.72.237.125	TCP	394	[TCP Retransmission] 55795 → 80 [PSH, ACK] Seq=1 Ack=1 Win=4096 Len=328 TSval=105868605 TSecr=
163	4.304011	172.20.10.2	209.105.248.3	TCP	503	[TCP Retransmission] 55806 → 443 [PSH, ACK] Seq=577 Ack=146 Win=131712 Len=437 TSval=105871115
226	4.767929	216.58.218.194	172.20.10.2	TCP	112	[TCP Retransmission] 443 → 55496 [PSH, ACK] Seq=682 Ack=287 Win=455 Len=46 TSval=2418025302 TS
1145	10.280426	172.20.10.2	64.6.21.1	TCP	1454	[TCP Retransmission] 55826 → 443 [PSH, ACK] Seq=3459 Ack=4382 Win=65535 Len=1388 TSval=1058769

Frame 66: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: Apple_8b:6e:80 (6c:40:08:8b:6e:80), Dst: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64)
 Internet Protocol Version 4, Src: 172.20.10.2, Dst: 173.194.115.90
 Transmission Control Protocol, Src Port: 55720 (55720), Dst Port: 443 (443), Seq: 1, Ack: 65, Len: 0
 Source Port: 55720
 Destination Port: 443
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Acknowledgment number: 65 (relative ack number)
 Header Length: 32 bytes
 Flags: 0x01 (FIN, ACK)
 Window size value: 4096
 [calculated window size: 4096]
 [window size scaling factor: -1 (unknown)]
 Checksum: 0xa6fd [validation disabled]
 Urgent pointer: 0

0000 fa cf 9c 21 5f 64 6c 40 08 8b 6e 80 00 00 45 00 ... 1 d8 ... n... E.
 0010 00 34 52 53 40 00 00 06 11 3e ac 14 0a 02 ad c2 ... 4 RS B. >
 0020 73 5a 09 a8 01 bb ae 13 2c e8 9c cd dc 91 80 11 s2
 0030 10 00 a6 fd 00 00 01 01 08 0a 06 4f 66 7f 6e 7b 0f.m
 0040 dd 82

Transmission Control Protocol (tcp), 32 bytes | Packets: 1219 - Displayed: 8 (0.7%) - Load ti... | Profile: Default

7. For each of the four packets, in order, the data that is acknowledged is: 0,135,9 and 1388.
 (Subtracting ACK field of 2nd packet from the ACK of the first packet)

Filter: **tcp.analysis.retransmission**

No.	Time	Source	Destination	Protocol	Length	Info
132	4.021118	172.20.10.2	23.235.44.231	TCP	66	55790 → 80 [ACK] Seq=1415 Ack=56130 Win=4057 Len=0 TSval=105870842 TSecr=51237198
136	4.079317	23.235.44.231	172.20.10.2	TCP	66	80 → 55789 [ACK] Seq=5152 Ack=2946 Win=83 Len=0 TSval=917517929 TSecr=105870856
137	4.079650	23.235.44.231	172.20.10.2	TCP	66	80 → 55789 [ACK] Seq=5152 Ack=3138 Win=90 Len=0 TSval=917517929 TSecr=105870856
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=105870899 TSecr=98461199
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 Win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 Win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 Win=77 Len=0 TSval=51237230 TSecr=105870899
148	4.136121	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=518 Ack=146 Win=131712 Len=0 TSval=105870952 TSecr=98461204
154	4.151247	172.20.10.2	23.235.44.231	TCP	66	55789 → 80 [ACK] Seq=3138 Ack=6102 Win=4066 Len=0 TSval=105870967 TSecr=917517947

Frame 144: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64), Dst: Apple_8b:6e:80 (6c:40:08:8b:6e:80)
 Internet Protocol Version 4, Src: 23.235.44.231, Dst: 172.20.10.2
 Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55790 (55790), Seq: 56130, Ack: 2803, Len: 0
 Source Port: 80
 Destination Port: 55790
 [Stream index: 4]
 [TCP Segment Len: 0]
 Sequence number: 56130 (relative sequence number)
 Acknowledgment number: 2803 (relative ack number)
 Header Length: 32 bytes
 Flags: 0x010 (ACK)
 Window size value: 72
 [calculated window size: 72]
 [window size scaling factor: -1 (unknown)]
 Checksum: 0x4548 [validation disabled]
 Urgent pointer: 0

0000 6c 40 08 8b 6e 80 fa cf 9c 21 5f 64 08 00 45 00 1e . . n . . . 1 d . . E .
 0010 00 34 04 cf 00 00 35 06 86 0d 17 eb 2c e7 ac 14 . 4 5
 0020 0a 02 00 50 d9 e8 3f 57 45 79 24 c8 15 80 10 . . . P . . 7 W . y
 0030 00 48 45 48 00 00 01 01 08 0a 03 0d d1 66 06 4f . . H E H h . O
 0040 76 33 v3

Acknowledgment number (tcp.ack), 4 bytes | Packets: 1219 - Displayed: 1219 (100.0%) - Lo... | Profile: Default

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
132	4.021118	172.20.10.2	23.235.44.231	TCP	66	55790 → 80 [ACK] Seq=1415 Ack=56130 win=4057 Len=0 TSval=105870842 TSecr=51237198
136	4.079317	23.235.44.231	172.20.10.2	TCP	66	80 → 55789 [ACK] Seq=5152 Ack=2946 win=85 Len=0 TSval=917517929 TSecr=105870856
137	4.079650	23.235.44.231	172.20.10.2	TCP	66	80 → 55789 [ACK] Seq=5152 Ack=3138 win=90 Len=0 TSval=917517929 TSecr=105870856
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899
148	4.136121	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=518 Ack=146 win=131712 Len=0 TSval=105870952 TSecr=98461204
154	4.151247	172.20.10.2	23.235.44.231	TCP	66	55789 → 80 [ACK] Seq=3138 Ack=6102 win=4066 Len=0 TSval=105870967 TSecr=917517947

Frame 145: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64), Dst: Apple_8b:6e:80 (6c:40:08:8b:6e:80)

Internet Protocol Version 4, Src: 23.235.44.231, Dst: 172.20.10.2

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55790 (55790), Seq: 56130, Ack: 2938, Len: 0

Source Port: 80

Destination Port: 55790

[Stream index: 4]

[TCP segment Len: 0]

Sequence number: 56130 (relative sequence number)

Acknowledgment number: 2938 (relative ack number)

Header Length: 32 bytes

Flags: 0x010 (ACK)

Window size value: 77

[Calculated window size: 77]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x44bc [validation disabled]

Urgent pointer: 0

0000 6c 40 08 8b 6e 80 fa cf 9c 21 5f 64 08 00 45 00 10..n...!..d..E.

0010 00 34 04 d1 00 00 35 06 86 0c 17 eb 2c e7 ac 14 ..4...5.

0020 0a 02 00 50 d9 ee 3f 57 a5 79 12 fc 13 02 80 10 ...P...?W..y...:

0030 00 4d 44 bc 00 00 01 01 08 0a 03 0d d1 6e 06 4f .MD.....n.O

0040 76 33 V3

Acknowledgment number (tcp.ack), 4 bytes | Packets: 1219 - Displayed: 1219 (100.0%) - Lo... | Profile: Default

kayak-pcapng [Wireshark 2.0.0 (v2.0.0-0-g9a73b82 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
132	4.021118	172.20.10.2	23.235.44.231	TCP	66	55790 → 80 [ACK] Seq=1415 Ack=56130 win=4057 Len=0 TSval=105870842 TSecr=51237198
136	4.079317	23.235.44.231	172.20.10.2	TCP	66	80 → 55789 [ACK] Seq=5152 Ack=2946 win=85 Len=0 TSval=917517929 TSecr=105870856
137	4.079650	23.235.44.231	172.20.10.2	TCP	66	80 → 55789 [ACK] Seq=5152 Ack=3138 win=90 Len=0 TSval=917517929 TSecr=105870856
139	4.081018	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=1 Ack=1 win=131840 Len=0 TSval=105870899 TSecr=98461199
144	4.135363	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2803 win=72 Len=0 TSval=51237230 TSecr=105870899
145	4.135713	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2938 win=77 Len=0 TSval=51237230 TSecr=105870899
146	4.135716	23.235.44.231	172.20.10.2	TCP	66	80 → 55790 [ACK] Seq=56130 Ack=2947 win=77 Len=0 TSval=51237230 TSecr=105870899
148	4.136121	172.20.10.2	209.105.248.3	TCP	66	55806 → 443 [ACK] Seq=518 Ack=146 win=131712 Len=0 TSval=105870952 TSecr=98461204
154	4.151247	172.20.10.2	23.235.44.231	TCP	66	55789 → 80 [ACK] Seq=3138 Ack=6102 win=4066 Len=0 TSval=105870967 TSecr=917517947

Frame 146: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: fa:cf:9c:21:5f:64 (fa:cf:9c:21:5f:64), Dst: Apple_8b:6e:80 (6c:40:08:8b:6e:80)

Internet Protocol Version 4, Src: 23.235.44.231, Dst: 172.20.10.2

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55790 (55790), Seq: 56130, Ack: 2947, Len: 0

Source Port: 80

Destination Port: 55790

[Stream index: 4]

[TCP segment Len: 0]

Sequence number: 56130 (relative sequence number)

Acknowledgment number: 2947 (relative ack number)

Header Length: 32 bytes

Flags: 0x010 (ACK)

Window size value: 77

[Calculated window size: 77]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x44b3 [validation disabled]

Urgent pointer: 0

0000 6c 40 08 8b 6e 80 fa cf 9c 21 5f 64 08 00 45 00 10..n...!..d..E.

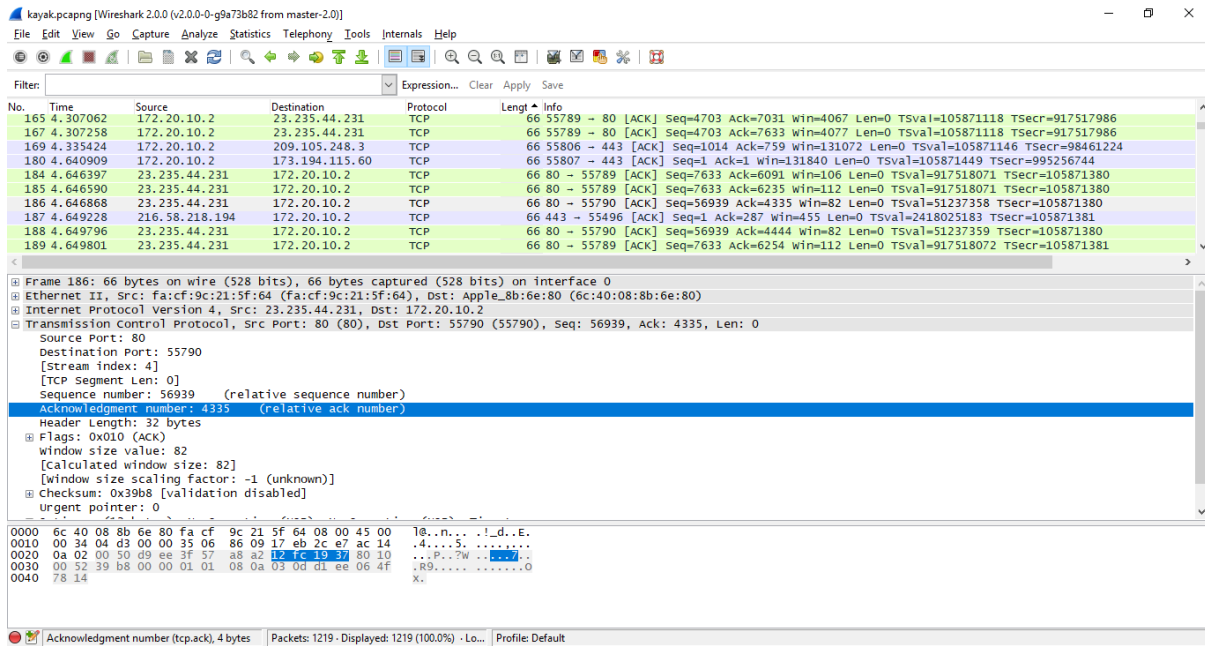
0010 00 34 04 d1 00 00 35 06 86 0b 17 eb 2c e7 ac 14 ..4...5.

0020 0a 02 00 50 d9 ee 3f 57 a5 79 12 fc 13 02 80 10 ...P...?W..y...:

0030 00 4d 44 b3 00 00 01 01 08 0a 03 0d d1 6e 06 4f .MD.....n.O

0040 76 33 V3

Acknowledgment number (tcp.ack), 4 bytes | Packets: 1219 - Displayed: 1219 (100.0%) - Lo... | Profile: Default



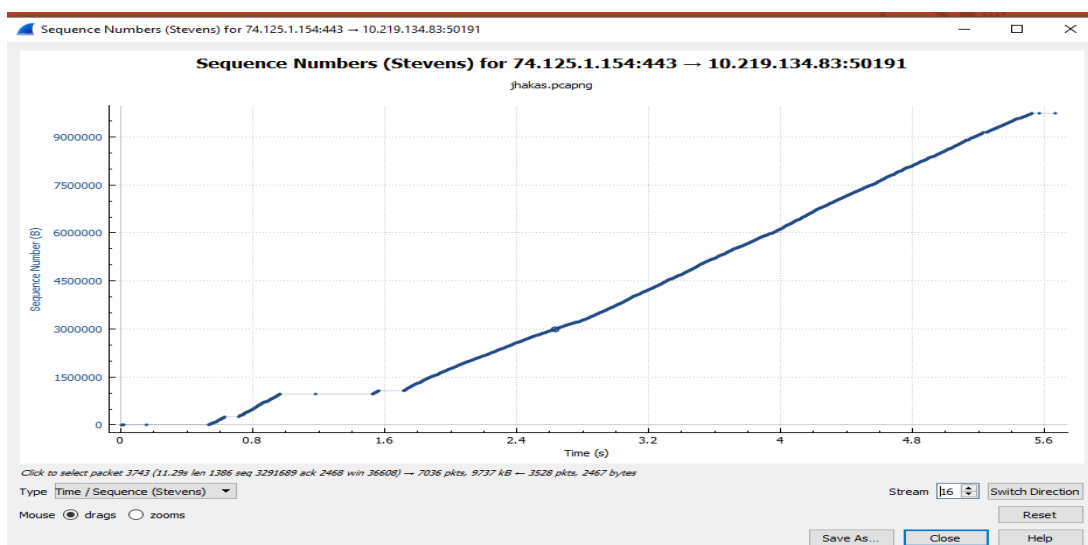
8. Throughput = (Amount of Data Transmitted/Time Incurred)
 = (2920) / (0.565366)
 = 5,164.795 Kb/sec

9. Amount of Data Transmitted can be calculated by subtracting sequence number of the first byte being sent (Packet 140) from the ACK of the last packet (Packet 186)
 i.e. 4335 - 1415 = 2920.
 Time Incurred can be calculated by subtracting the time of the first byte that was sent from the time of the last acknowledgement.
 i.e. 4.646868 - 4.081502 = 0.565366

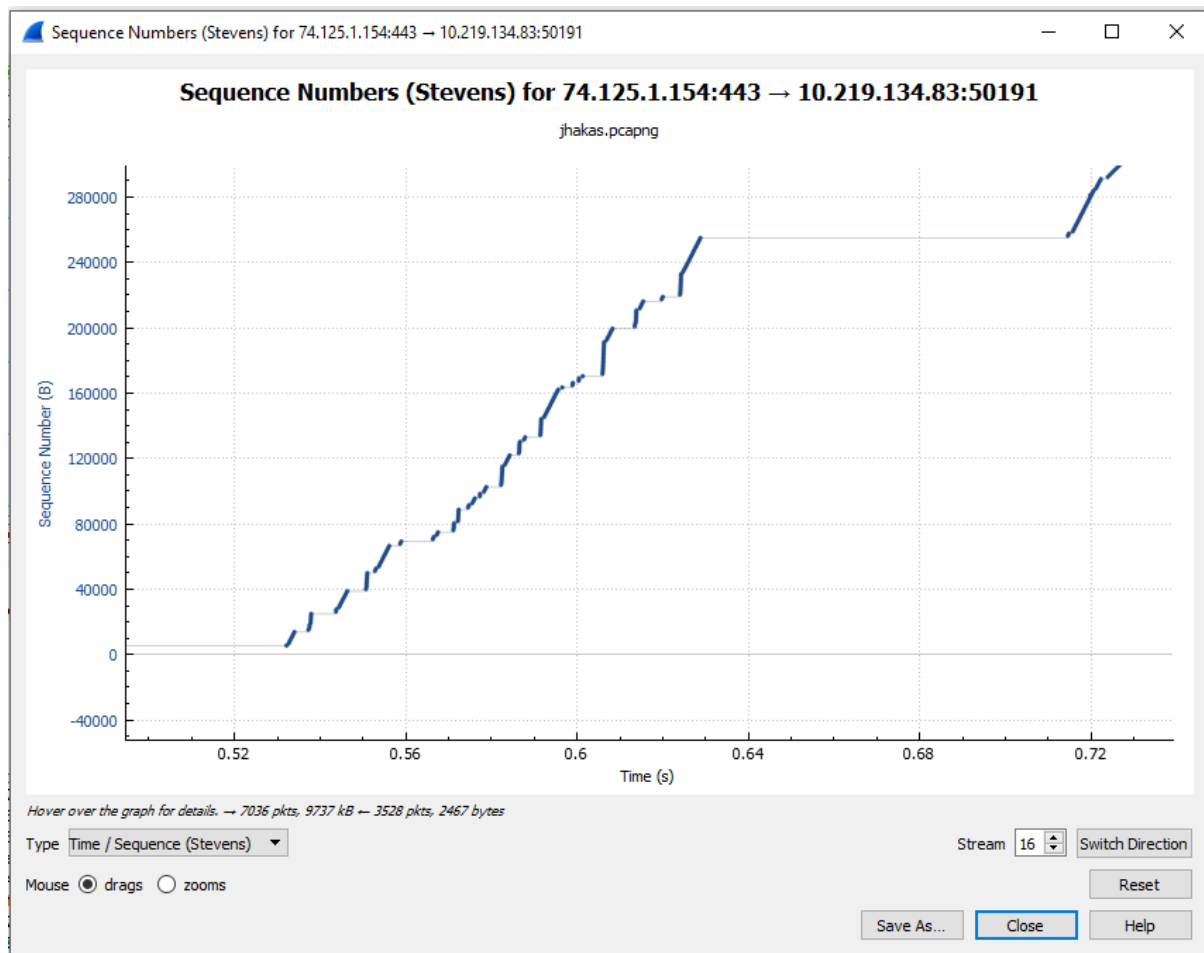
Section 4: TCP congestion control in action

Problem Set 4:

1. Slow Start is 0.01 to 0.075



2. Congestion avoidance is 0.523



- Comments on the ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text can be stated as the idealized behavior of TCP depicts that it is one of the best protocol that can handle internet application using congestion control and slow start mechanism. A huge traffic in the network can congest the network and hence TCP should follow some algorithms like AIMD. This technique is applied so as to drop the size of the window and avoid congestion. There can be various problems like retransmission, time delay or loss mostly based on the application to implement it. Slow start also delays the of application start in some cases.