



**NAME :: IBRAR BABAR**

**ROLL NO. :: 19P-0104**

**CN LAB WORK :: 5 (WIRESHARK)**

**SECTION (B)**

❖ (UDP)

www.daraz.pk						
udp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.10	47.107.60.190	UDP	146	6881 → 18342 Len=104
2	0.220957	192.168.100.10	142.250.181.132	UDP	278	54857 → 443 Len=236
3	0.480449	142.250.181.132	192.168.100.10	UDP	73	443 → 54857 Len=31
4	0.496730	192.168.100.10	142.250.181.132	UDP	75	54857 → 443 Len=33
5	0.497589	47.107.60.190	192.168.100.10	UDP	317	18342 → 6881 Len=275
6	0.497589	142.250.181.132	192.168.100.10	UDP	113	443 → 54857 Len=71
7	0.497589	142.250.181.132	192.168.100.10	UDP	68	443 → 54857 Len=26
8	0.497881	192.168.100.10	142.250.181.132	UDP	80	54857 → 443 Len=38
9	0.513781	192.168.100.10	142.250.181.132	UDP	75	54857 → 443 Len=33
11	1.254755	142.250.181.132	192.168.100.10	UDP	68	443 → 54857 Len=26
12	1.438361	192.168.100.10	192.168.100.1	DNS	72	Standard query 0xa0a8 A
43	1.705228	192.168.100.1	192.168.100.10	DNS	550	Standard query response
172	2.800442	192.168.100.17	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
175	2.802576	192.168.100.17	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
260	3.338697	192.168.100.10	192.168.100.1	DNS	80	Standard query 0xd66a A
308	3.475807	192.168.100.1	192.168.100.10	DNS	399	Standard query response
312	3.680754	192.168.100.10	192.168.100.1	DNS	72	Standard query 0x879d A
343	3.853698	192.168.100.1	192.168.100.10	DNS	381	Standard query response
367	4.026310	192.168.100.10	192.168.100.1	DNS	71	Standard query 0x81e2 A
383	4.470120	192.168.100.1	192.168.100.10	DNS	549	Standard query response
402	5.009045	192.168.100.10	111.92.81.122	UDP	146	6881 → 31675 Len=104
505	5.497991	111.92.81.122	192.168.100.10	UDP	317	31675 → 6881 Len=275
509	5.596761	192.168.100.10	192.168.100.1	DNS	78	Standard query 0xe03b A
523	5.642271	192.168.100.1	192.168.100.10	DNS	397	Standard query response
963	8.828913	192.168.100.10	192.168.100.1	DNS	72	Standard query 0x6721 A
967	9.286863	192.168.100.1	192.168.100.10	DNS	319	Standard query response

### Q#1(UDP)-Answer

The header only contains 5 fields: the source port, destination port, length, checksum and UDP payload.



Wireshark · Packet 505 · Wi-Fi

- > Frame 505: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface
- > Ethernet II, Src: HuaweiTe\_9a:18:b7 (70:7b:e8:9a:18:b7), Dst: IntelCor\_4c:d8:8a
- > Internet Protocol Version 4, Src: 111.92.81.122, Dst: 192.168.100.10
- ▼ User Datagram Protocol, Src Port: 31675, Dst Port: 6881
  - Source Port: 31675
  - Destination Port: 6881
  - Length: 283
  - Checksum: 0xbf67 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 7]
  - > [Timestamps]
  - UDP payload (275 bytes)

0020	64 0a 7b bb 1a e1 01 1b	bf 67	64 31 3a 72 64 32	d { . . . . .	gd1:rd2
0030	3a 69 64 32 30 3a 38 38	38 38 38 38 38 38 a8 cc		:id20:88 888888 . .	
0040	0f 4a 77 17 51 90 61 50	87 e5 35 3a 6e 6f 64 65		.Jw.Q.aP . .5:node	
0050	73 32 30 38 3a 38 38 38	38 38 38 38 38 e6 ac d3		s208:888 88888 . . .	
0060	9f 19 82 b8 2e a3 fa 9a	55 b2 8d 9b 59 14 e9 38		. . . . . U . . . Y . . 8	

## Q#2(UDP)-Answer

Each of the UDP header fields is 2 bytes long.



Wireshark · Packet 505 · Wi-Fi

- > Internet Protocol Version 4, Src: 111.92.81.122, Dst: 192.168.100.10
- ▼ User Datagram Protocol, Src Port: 31675, Dst Port: 6881
  - Source Port: 31675
  - Destination Port: 6881
  - Length: 283
  - Checksum: 0xbf67 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 7]
  - > [Timestamps]
  - UDP payload (275 bytes)
- > Data (275 bytes)

0020	64 0a 7b bb 1a e1 01 1b	bf 67	64 31 3a 72 64 32	d { . . . . .	gd1:rd2
0030	3a 69 64 32 30 3a 38 38	38 38 38 38 38 38 a8 cc		:id20:88 888888 . .	

## Q#3-Answer

The value in the length field, in the example below it is 46, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.

### Q#4(UDP)-Answer


The maximum number of bytes that can be in the payload is  $2^{16}$  - the bytes already being used by the header field (8). Therefore, the maximum payload is  $65535 - 8 = 65527$  bytes.

### Q#5(UDP)-Answer

The largest possible source port number is  $2^{16}$  or 65535.

### Q#6(UDP)-Answer

The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.

 Wireshark · Packet 505 · Wi-Fi

```
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 303
Identification: 0x0000 (0)
▼ Flags: 0x40, Don't fragment
  0... .... = Reserved bit: Not set
  .1... .... = Don't fragment: Set
  ..0. .... = More fragments: Not set
Fragment Offset: 0
Time to Live: 52
Protocol: UDP (17)
Header Checksum: 0x6035 [validation disabled]
```

0010	01 2f 00 00 40 00 34 11	60 35 6f 5c 51 7a c0 a8	./..@.4. `5o\Qz..
0020	64 0a 7b bb 1a e1 01 1b	bf 67 64 31 3a 72 64 32	d.{.....gd1:rd2
0030	3a 69 64 32 30 3a 38 38	38 38 38 38 38 38 a8 cc	:id20:88 888888..
0040	0f 4a 77 17 51 90 61 50	87 e5 35 3a 6e 6f 64 65	·Jw·Q·aP ..5:node
0050	73 32 30 38 3a 38 38 38	38 38 38 38 38 e6 ac d3	s208:888 88888..
0060	9f 19 82 b8 2e a3 fa 9a	55 b2 8d 9b 59 14 e9 38	.....U...Y..8
0070	38 38 38 38 38 38 e6	ac d3 9f 19 82 b8 2e a3	88888888.....

### Q#7(UDP)-Answer

UDP Sent by my host.

.....0..... = IG bit: Individual address (unicast)	
Type: IPv4 (0x0800)	
> Internet Protocol Version 4, Src: 111.92.81.122, Dst: 192.168.100.10	
▼ User Datagram Protocol, Src Port: 31675, Dst Port: 6881	
Source Port: 31675	
Destination Port: 6881	
Length: 283	
Checksum: 0xbf67 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 7]	
> [Timestamps]	
UDP payload (275 bytes)	
0020	64 0a 7b bb 1a e1 01 1b bf 67 64 31 3a 72 64 32 d1:rd2
0030	3a 69 64 32 30 3a 38 38 38 38 38 38 38 a8 cc :id20:88 888888..
0040	0f 4a 77 17 51 90 61 50 87 e5 35 3a 6e 6f 64 65 ·Jw·Q·aP ··5:node
0050	73 32 30 38 3a 38 38 38 38 38 38 38 e6 ac d3 s208:888 88888..
0060	9f 19 82 b8 2e a3 fa 9a 55 b2 8d 9b 59 14 e9 38 ..... U···Y··8

## UDP Reply to Host.

.....0..... = IG bit: Individual address (unicast)	
Type: IPv4 (0x0800)	
> Internet Protocol Version 4, Src: 111.92.81.122, Dst: 192.168.100.10	
▼ User Datagram Protocol, Src Port: 31675, Dst Port: 6881	
Source Port: 31675	
Destination Port: 6881	
Length: 283	
Checksum: 0xbf67 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 7]	
> [Timestamps]	
UDP payload (275 bytes)	
0020	64 0a 7b bb 1a e1 01 1b bf 67 64 31 3a 72 64 32 d1:rd2
0030	3a 69 64 32 30 3a 38 38 38 38 38 38 38 a8 cc :id20:88 888888..
0040	0f 4a 77 17 51 90 61 50 87 e5 35 3a 6e 6f 64 65 ·Jw·Q·aP ··5:node
0050	73 32 30 38 3a 38 38 38 38 38 38 38 e6 ac d3 s208:888 88888..
0060	9f 19 82 b8 2e a3 fa 9a 55 b2 8d 9b 59 14 e9 38 ..... U···Y··8

The relationship between port numbers is that the source port on the send message is the destination port of the receive message. The destination port for the send message is also the source port for the receive message.

## ❖ (TCP)

The File name (TCP\_home\_work.txt) is attached.

← → ↻ ⚠ Not secure | [gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html](http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html)

Upload page for TCP Wireshark Lab

Computer Networking: A Top Down Approach, 6th edition

Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII file and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

TCP\_home\_work.txt

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to upload the file to the server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating that the file has been uploaded and that the analysis has begun.

No.	Time	Source	Destination	Protocol	Length	Info
236	4.999686	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
237	4.999686	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
238	5.000512	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
239	5.001909	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
240	5.002221	192.168.100.10	163.125.211.35	UDP	146	6881 → 9430 Le
241	5.007288	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
242	5.010690	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
243	5.012637	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
244	5.013396	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
245	5.013396	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
246	5.014246	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
247	5.017006	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
248	5.066519	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [AC
249	5.067734	128.119.245.12	192.168.100.10	HTTP	831	HTTP/1.1 200 C
250	5.113598	192.168.100.10	128.119.245.12	TCP	54	61826 → 80 [AC
251	5.287276	192.168.100.10	172.217.19.3	QUIC	1292	Initial, DCID=
252	5.287759	192.168.100.10	172.217.19.3	QUIC	119	0-RTT, DCID=a2
253	5.288201	192.168.100.10	172.217.19.3	QUIC	470	0-RTT, DCID=a2
254	5.370941	172.217.19.3	192.168.100.10	QUIC	1292	Initial, SCID=
255	5.456026	172.217.19.3	192.168.100.10	QUIC	1292	Protected Payl
256	5.456532	172.217.19.3	192.168.100.10	QUIC	664	Protected Payl
257	5.457233	192.168.100.10	172.217.19.3	QUIC	121	Handshake, DCI
258	5.457632	192.168.100.10	172.217.19.3	QUIC	75	Protected Payl
259	5.466603	172.217.19.3	192.168.100.10	QUIC	68	Protected Payl
260	5.470565	172.217.19.3	192.168.100.10	QUIC	67	Protected Payl
261	5.503868	192.168.100.10	172.217.19.3	QUIC	75	Protected Payl
262	5.524539	172.217.19.3	192.168.100.10	QUIC	146	Protected Payl
263	5.551874	192.168.100.10	172.217.19.3	QUIC	75	Protected Payl
264	5.569968	172.217.19.3	192.168.100.10	QUIC	652	Protected Payl
265	5.570586	192.168.100.10	172.217.19.3	QUIC	77	Protected Payl
266	5.573723	172.217.19.3	192.168.100.10	QUIC	67	Protected Payl
267	5.599705	192.168.100.10	172.217.19.3	QUIC	75	Protected Payl
268	5.635942	172.217.19.3	192.168.100.10	QUIC	67	Protected Payl

← → ↻ ⚠ Not secure | [gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm](https://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm)

Congratulations!

You've now transferred a copy of `alice.txt` from your computer to `gaia.cs.umass.edu`. You should now stop Wireshark (stop capturing packets)!

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
227	4.957818	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=122845 Win=218240 Len=0
228	4.967677	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=124257 Win=221184 Len=0
229	4.974543	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=125669 Win=224128 Len=0
230	4.974820	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=127081 Win=227072 Len=0
231	4.985786	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=128493 Win=230016 Len=0
232	4.997036	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=129905 Win=232832 Len=0
233	4.997651	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=131317 Win=235776 Len=0
234	4.999197	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=132729 Win=238720 Len=0
235	4.999686	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=134141 Win=241664 Len=0
236	4.999686	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=135553 Win=244608 Len=0
237	4.999686	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=136965 Win=247424 Len=0
238	5.000512	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=138377 Win=250368 Len=0
239	5.001909	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=139789 Win=253312 Len=0
241	5.007288	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=142613 Win=258944 Len=0
242	5.010690	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=144025 Win=261888 Len=0
243	5.012637	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=145437 Win=264832 Len=0
244	5.013396	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=146849 Win=267776 Len=0
245	5.013396	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=148261 Win=270592 Len=0
> Frame 242: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DEF338A6-703C-4D0F-8F17-12A2AB889FD} > Ethernet II, Src: HuaweiTe_9a:18:b7 (70:7b:e8:9a:18:b7), Dst: IntelCor_4c:d8:8a (f4:06:69:4c:d8:8a) > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.100.10 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 40 Identification: 0x1f48 (8008) > Flags: 0x40, Don't fragment						
0000	f4 06 69 4c d8 8a 70 7b e8 9a 18 b7 08 00 45 00	..iL..p{ .....E.				
0010	00 28 1f 48 40 00 33 06 8e 51 80 77 f5 0c c0 a8	.(.H@.3. .Q.w....				
0020	64 0a 00 50 f1 82 08 61 fe 91 6c 66 46 ee 50 10	d..P...a ..lF.P.				
0030	07 fe 61 85 00 00	..a...				

The answers below are based on the trace file tcp-ethereal-trace-1 in

<http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>



## Q#1(TCP)-Answer

Client computer (source) IP address: 192.168.1.102

TCP port number: 1161

tcp-ethereal-trace-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
182	4.921916	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=151197 Ack=1 Win=17520
183	4.922820	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=152657 Ack=1 Win=17520
184	4.923863	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=154117 Ack=1 Win=17520
185	4.924667	192.168.1.102	128.119.245.12	TCP	946	1161 → 80 [PSH, ACK] Seq=155577 Ack=1 Win=
186	5.019189	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=151197 Win=62780
187	5.104175	Intel_52:2b:23	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
188	5.105060	LinksysG_da:af:73	Intel_52:2b:23	ARP	42	192.168.1.1 is at 00:06:25:da:af:73
189	5.106121	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
190	5.125019	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=154117 Win=62780
191	5.197286	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=156469 Win=62780
192	5.197508	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=156469 Ack=1 Win=17520
193	5.198388	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=157929 Ack=1 Win=17520
194	5.199275	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=159389 Ack=1 Win=17520
195	5.200252	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=160849 Ack=1 Win=17520
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)

> Frame 203: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits)

> Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)

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

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 730

Source Port: 80

Destination Port: 1161

[Stream index: 0]

0020 01 66 00 50 04 89 34 a2 74 1a 0d d8 82 ef 50 18 .f.P..4.t....P.

0030 f5 3c a9 20 00 00 48 54 54 50 2f 31 2e 31 20 32 .<...HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK..D ate: Sat

0050 2c 20 32 31 20 41 75 67 20 32 30 30 34 20 31 33 , 21 Aug 2004 13

0060 3a 34 34 3a 32 30 20 47 4d 54 0d 0a 53 65 72 76 :44:20 G MT..Serv



## Q#2(TCP)-Answer

Destination computer: gaia.cs.umass.edu IP address: 128.119.245.12

TCP port number: 80

tcp-ethereal-trace-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
182	4.921916	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=151197 Acl
183	4.922820	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=152657 Acl
184	4.923863	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=154117 Acl
185	4.924667	192.168.1.102	128.119.245.12	TCP	946	1161 → 80 [PSH, ACK] Seq=15557
186	5.019189	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1511
187	5.104175	Intel_52:2b:23	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192
188	5.105060	LinksysG_da:af:73	Intel_52:2b:23	ARP	42	192.168.1.1 is at 00:06:25:da
189	5.106121	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
190	5.125019	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1541
191	5.197286	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1564
192	5.197508	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=156469 Acl
193	5.198388	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=157929 Acl
194	5.199275	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=159389 Acl
195	5.200252	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=160849 Acl
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 Acl
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=16376
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1591
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-rep
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1621
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1646
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=1646

< >

> 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: 164041, Ack: 1, Len: 50

Source Port: 1161

Destination Port: 80

[Stream index: 0]

< >

0020 f5 0c 04 89 00 50 0d d8 82 bd 34 a2 74 1a 50 18 .....P...4.t.P.

0030 44 70 9f 0f 00 00 0d 0a 2d 2d 2d 2d 2d 2d 2d Dp.....

0040 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----

0050 2d 2d 2d 2d 2d 32 36 35 30 30 31 39 31 36 39 31 -----265 00191691

## Q#3(TCP)-Answer

My IP address source is 192.168.100.10 sending on port 61826.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
197	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=134141 Ack=1 Win=0 Len=0
198	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=135553 Ack=1 Win=0 Len=0
199	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=136965 Ack=1 Win=0 Len=0
200	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=138377 Ack=1 Win=0 Len=0
201	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=139789 Ack=1 Win=0 Len=0
202	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=141201 Ack=1 Win=0 Len=0
203	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=142613 Ack=1 Win=0 Len=0
204	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=144025 Ack=1 Win=0 Len=0
205	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=145437 Ack=1 Win=0 Len=0
206	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [PSH, ACK] Seq=146849 Ack=1 Win=0 Len=0
207	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=148261 Ack=1 Win=0 Len=0
208	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=149673 Ack=1 Win=0 Len=0
209	4.742169	192.168.100.10	128.119.245.12	TCP	1466	61826 → 80 [ACK] Seq=151085 Ack=1 Win=0 Len=0
210	4.820802	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=93193 Win=0 Len=0
211	4.820907	192.168.100.10	128.119.245.12	HTTP	604	POST /wireshark-labs/lab3-1-reply.htm
212	4.870554	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=96017 Win=0 Len=0
213	4.871929	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=98841 Win=0 Len=0
214	4.881689	128.119.245.12	192.168.100.10	TCP	54	80 → 61826 [ACK] Seq=1 Ack=101665 Win=0 Len=0

Wireshark · Packet 211 · Wi-Fi

> Frame 211: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) on interface \Device\NPF\_{DEF338A6-703...}

> Ethernet II, Src: IntelCor\_4c:d8:8a (f4:06:69:4c:d8:8a), Dst: HuaweiTe\_9a:18:b7 (70:7b:e8:9a:18:b7)

> Internet Protocol Version 4, Src: 192.168.100.10, Dst: 128.119.245.12

▼ Transmission Control Protocol, Src Port: 61826, Dst Port: 80, Seq: 152497, Ack: 1, Len: 550

Source Port: 61826

Destination Port: 80

[Stream index: 2]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 550]

Sequence Number: 152497 (relative sequence number)

Sequence Number (raw): 1818650630

<

0000	70 7b e8 9a 18 b7 f4 06	69 4c d8 8a 08 00 45 00	p{.....iL....E..
0010	02 4e bf 93 40 00 80 06	9e df c0 a8 64 0a 80 77	.N.:@... ..d..w
0020	f5 0c f1 82 00 50 6c 66	68 06 08 61 fe 91 50 18	.....Plf h..a..P..
0030	01 03 df 78 00 00 65 72	73 65 6c 66 20 61 20 67	...x...er self a g

## Q#4(TCP)-Answer

The sequence number of the segment used to initiate the TCP connection is 0. We can see that the message contains a SYN flag indicating that it is a SYN segment.

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

tcp-etnereai-trace-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=1

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

✓ Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0

Source Port: 80  
Destination Port: 1161  
[Stream index: 0]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 883061785  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 232129013  
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.]

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 . . @ . 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 . . w M . . . . .

## Q#5(TCP)-Answer

- The sequence number of the SYNACK segment is 0.
- The value of the acknowledgement field is 1. This value is determined by the initial sequence number +1.
- The message carries flags that show it to be a SYN ACK message.

tcp-ethereal-trace-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=1 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1 Len=585
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=1 Len=1480
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=0 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=1 Len=1480

Destination Port: 1161  
[Stream index: 0]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 883061785  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 232129013  
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.]

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 . . @ . 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 . w M . . . . .

## Q#6(TCP)-Answer

The sequence number of the TCP segment containing the HTTP Post Command is 164041.

tcp-ethereal-trace-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
194	5.199275	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=159389 A
195	5.200252	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=160849 A
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 A
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=163
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=15
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-r
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=16
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=16
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=16
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
204	5.598090	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
205	5.599082	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 A

> Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 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: 164041, Ack: 1, Len: 50

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 50]

Sequence Number: 164041 (relative sequence number)

Sequence Number (raw): 232293053

[Next Sequence Number: 164091 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 883061786

0101 .... = Header Length: 20 bytes (5)

<

0020	f5 0c 04 89 00 50 0d d8 82 bd 34 a2 74 1a 50 18	.....P...4.t.P.
0030	44 70 9f 0f 00 00 0d 0a 2d 2d 2d 2d 2d 2d 2d	Dp.....
0040	2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	-----
0050	2d 2d 2d 2d 2d 32 36 35 30 30 31 39 31 36 39 31	-----265 00191691

Frame (104 bytes) Reassembled TCP (164090 bytes)

Sequence Number (tcp.seq), 4 bytes

## Q#7(TCP)-Answer

The sending time and the received time of ACKs are tabulated in the following table.

	Sent time	ACK received time	RTT (seconds)
Segment 1	0.026477	0.053937	0.02746
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.11443
Segment 5	0.077405	0.217299	0.13989
Segment 6	0.078157	0.267802	0.18964

No..	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	1161 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
2	0.023172	128.119.245.12	192.168.1.102	TCP	http > 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.023265	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	HTTP	POST /etherbase-labs/lab3-1-reply.htm HTTP/1.1
5	0.041737	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
6	0.053937	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
8	0.054690	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
9	0.077294	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
11	0.078157	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
12	0.124085	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
14	0.169118	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
19	0.305813	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
20	0.306643	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic

# Frame 11 (1514 bytes on wire, 1514 bytes captured)  
# Ethernet II, Src: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Dst: 192.168.1.1 (00:06:25:da:af:73)  
# Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)  
# Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: http (80), Seq: 6406, Ack: 1, Len: 1460  
# Hypertext Transfer Protocol

```

0000  00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  ..%.s.  ..p...E.
0010  05 dc 1e 26 40 00 80 06 9f 63 c0 a8 01 66 80 77  ...68... .C...f.w
0020  f5 0c 04 89 00 50 0d d6 1a fa 34 a2 74 1a 50 10  ....P..  ..4.t.P.
0030  44 70 95 83 00 00 20 55 6e 69 74 65 64 20 53 74  Dp.... U nited St

```

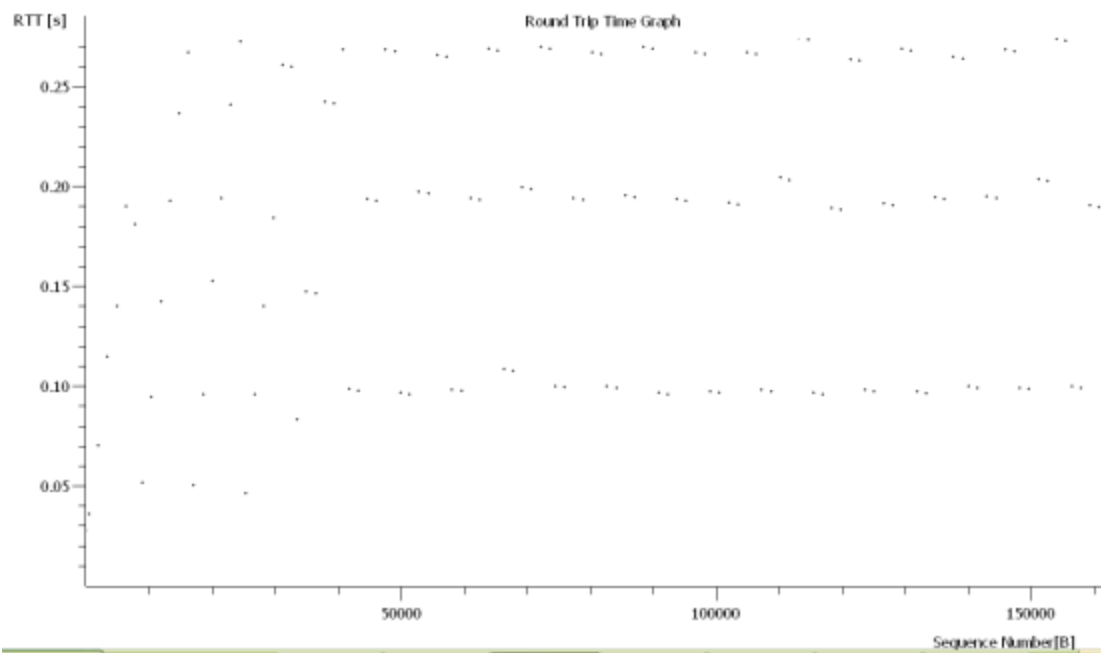
No..	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	1161 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
2	0.023172	128.119.245.12	192.168.1.102	TCP	http > 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.023265	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	HTTP	POST /etherbase-labs/lab3-1-reply.htm HTTP/1.1
5	0.041737	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
6	0.053937	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
8	0.054690	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
9	0.077294	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
11	0.078157	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
12	0.124085	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
14	0.169118	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
19	0.305813	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic
20	0.306643	192.168.1.102	128.119.245.12	HTTP	Continuation or non-HTTP traffic

# Frame 16 (60 bytes on wire, 60 bytes captured)  
# Ethernet II, Src: 192.168.1.1 (00:06:25:da:af:73), Dst: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)  
# Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)  
# Transmission Control Protocol, Src Port: http (80), Dst Port: 1161 (1161), Seq: 1, Ack: 7866, Len: 0

```

0000  00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00  ...p... %.s..E.
0010  00 28 58 77 40 00 37 06 b3 c6 80 77 f5 0c c0 a8  .Cw8.7.  ...w....
0020  01 66 00 50 04 89 34 a2 74 1a 0d d6 20 ae 50 10  .F.P..4.  t... .P.
0030  4f d8 4c 50 00 00 93 c0 00 00 63 ed             O.LP....  ..C.

```





## Q#8(TCP)-Answer

The Length of the first TCP segment (containing the HTTP POST): 565 bytes Length of each of the other five TCP segments: 730 bytes (MSS).

tcp-capture-nalce-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
191	5.197286	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=156469
192	5.197508	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=156469 Ack=1
193	5.198388	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=157929 Ack=1
194	5.199275	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=159389 Ack=1
195	5.200252	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=160849 Ack=1
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 Ack=1
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=163769
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=159389
199	5.297341	128.119.245.12	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)

> Frame 203: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits)

> Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)

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

> Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 730

> Hypertext Transfer Protocol

> Line-based text data: text/html (11 lines)

```
0020  01 66 00 50 04 89 34 a2 74 1a 0d d8 82 ef 50 18  ·f·P··4· t····P·
0030  f5 3c a9 20 00 00 48 54 54 50 2f 31 2e 31 20 32  ·<· ··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74  00 OK··D ate: Sat
0050  2c 20 32 31 20 41 75 67 20 32 30 30 34 20 31 33  , 21 Aug  2004 13
0060  3a 34 34 3a 32 30 20 47 4d 54 0d 0a 53 65 72 76  :44:20 G MT··Serv
0070  65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34  er: Apac he/2.0.4
0080  30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78  0 (Red H at Linux
0090  29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64  )··Last- Modified
00a0  3a 20 53 61 74 2c 20 32 31 20 41 75 67 20 32 30  : Sat, 2 1 Aug 20
00b0  30 34 20 30 31 3a 34 38 3a 31 34 20 47 4d 54 0d  04 01:48 :14 GMT·
00c0  0a 45 54 61 67 3a 20 22 31 62 38 63 32 2d 31 61  ·ETag: " 1b8c2-1a
00d0  30 2d 33 35 37 37 62 33 38 30 22 0d 0a 41 63 63  0-3577b3 80"··Acc
00e0  65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65  ept-Rang es: byte
00f0  73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74  s··Conte nt-Lengt
0100  68 3a 20 34 31 36 0d 0a 4b 65 65 70 2d 41 6c 69  h: 416·· Keep-Ali
0110  76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20  ve: time out=10,
```

## Q#9(TCP)-Answer

The minimum amount of buffer space (receiver window) advertised at gaia.cs.umass.edu for the entire trace is 5840 bytes, which shows in the first acknowledgement from the server. The minimum amount of available buffer space is listed as 65535. The sender is never throttled because we never reach full capacity of the window.

tcp-entire-trace-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP s
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TC
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP se
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP se
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP se
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP se
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [T
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP se
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460 [TCP s
20	0.306692	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=11933 Ack=1 Win=17520 Len=1460 [TCP s
21	0.307571	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=13393 Ack=1 Win=17520 Len=1460 [TCP s
22	0.308699	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=14853 Ack=1 Win=17520 Len=1460 [TCP s
23	0.309553	192.168.1.102	128.119.245.12	TCP	946	1161 → 80 [PSH, ACK] Seq=16313 Ack=1 Win=17520 Len=892 [T

## Q#10(TCP)-Answer

No, no segments were ever retransmitted. This is shown by the fact that an old Acknowledgement number was never resent in order to re-request former packets.

### **Q#11(TCP)-Answer**

The acknowledged sequence numbers of the ACKs are listed as follows.

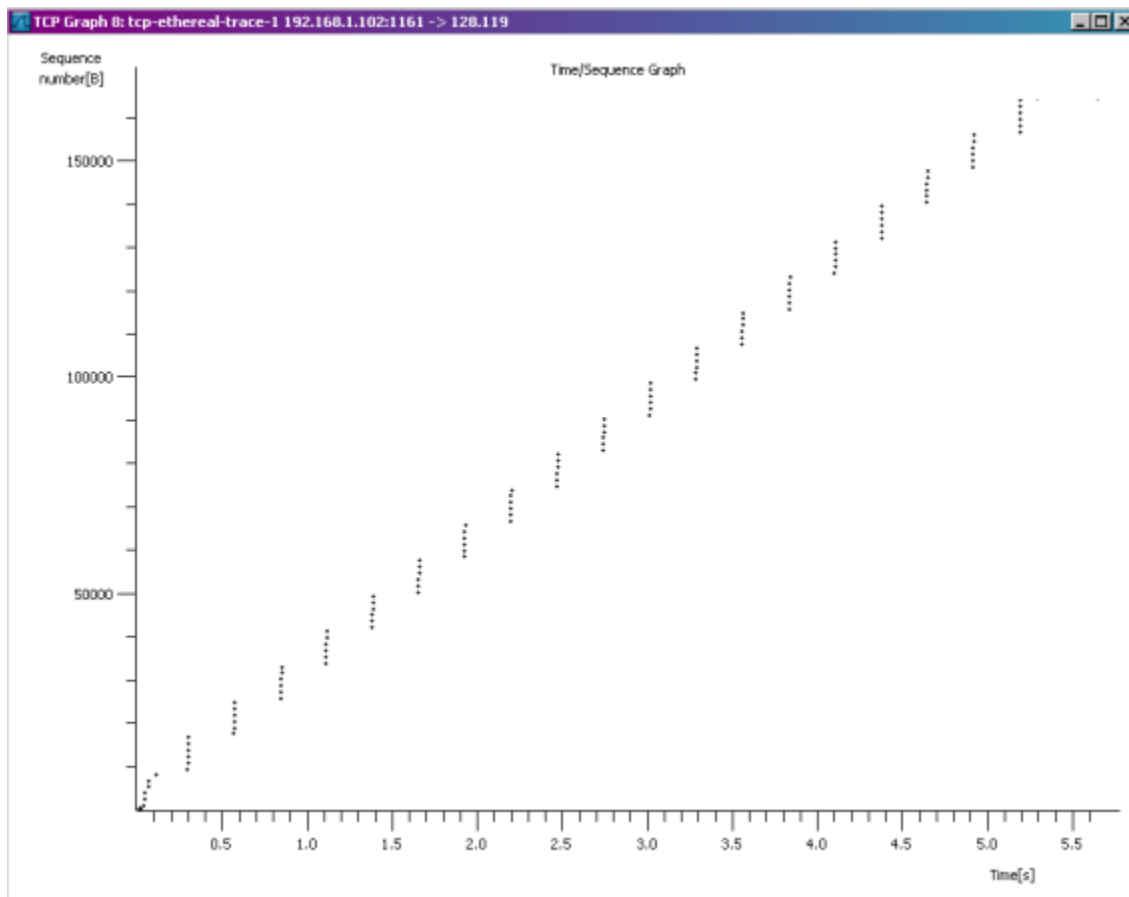
	acknowledged sequence number	acknowledged data
ACK 1	566	566
ACK 2	2026	1460
ACK 3	3486	1460
ACK 4	4946	1460
ACK 5	6406	1460
ACK 6	7866	1460
ACK 7	9013	1147
ACK 8	10473	1460
ACK 9	11933	1460
ACK 10	13393	1460
ACK 11	14853	1460
ACK 12	16313	1460

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. By inspecting the amount of acknowledged data by each ACK, there are cases where the receiver is ACKing every other segment.

### **Q#12(TCP)-Answer**

The throughput can be calculated by using the value of the last ack(149,629)- the first sequence number(1) divided by the time since first frame (1.6) = 93517.6 bps.

## Q#13-14-(TCP)-Answer



The TCP slowstart phase begins at just above seq number 5000, and ends just before sequence number 10000. Congestion avoidance takes over at 10000.

