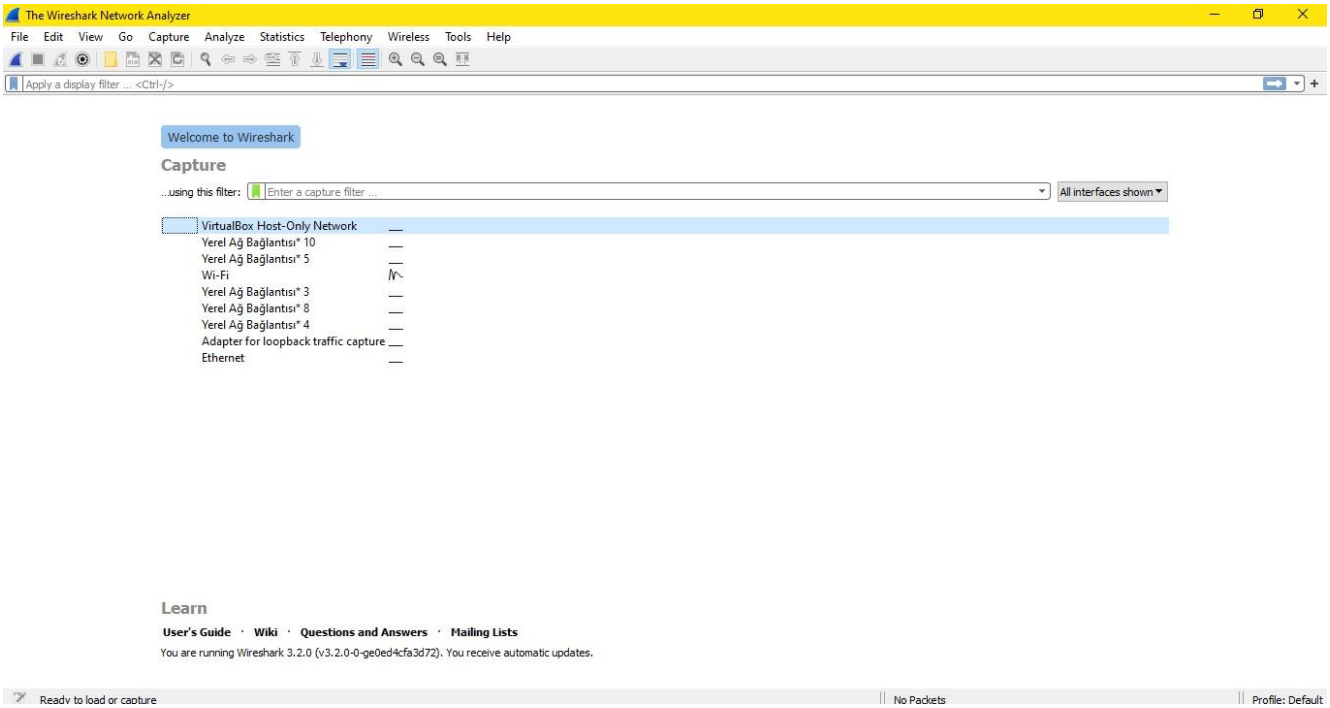
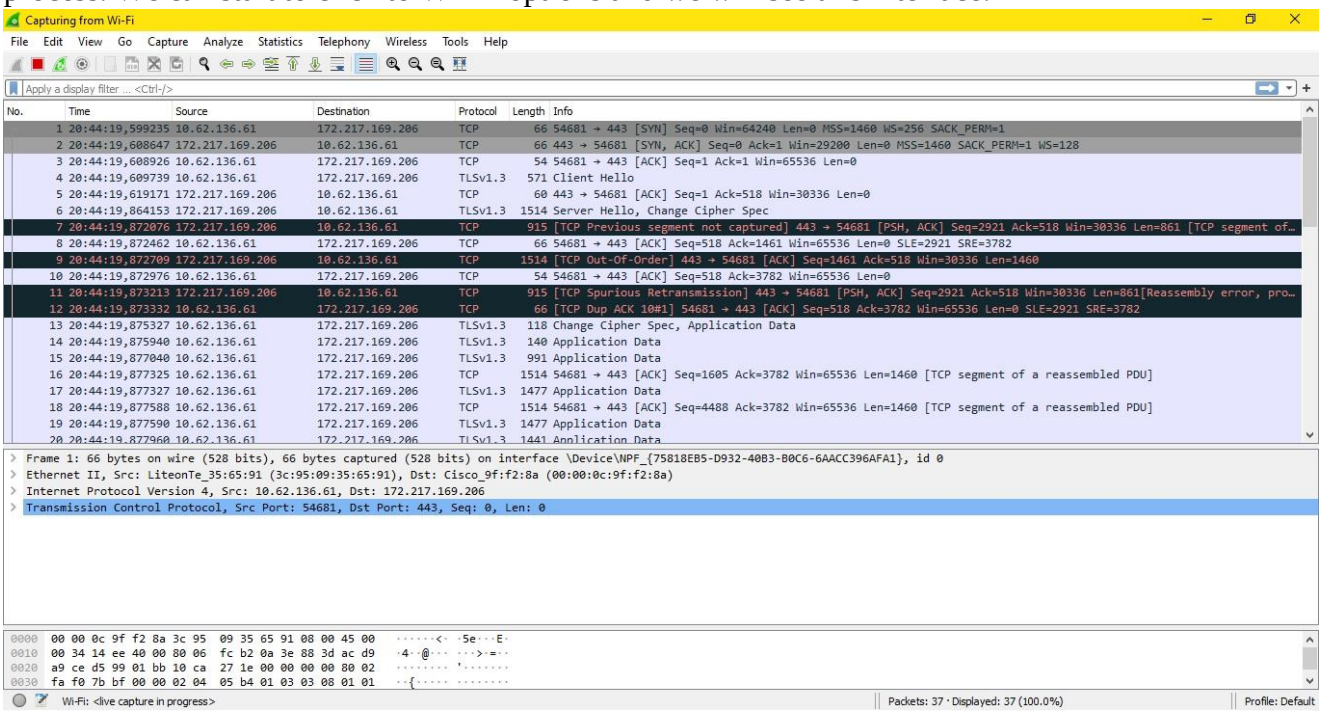
ASSIGNMENT I

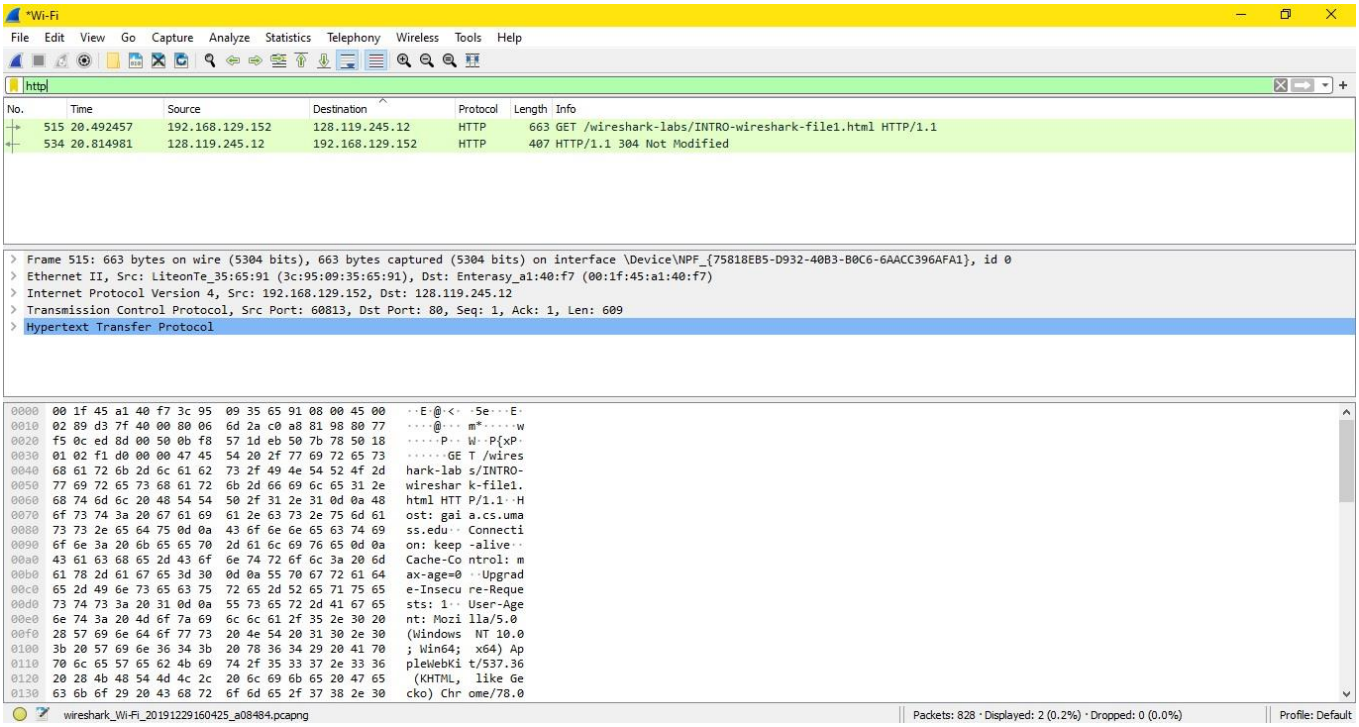
In first step, we opened the any internet browser. After, we opened also Wireshark program.



After the opening Wireshark, we saw the Wireshark's interface. We can start to capture process. We can start to click to WI-FI options and we will see this interface.



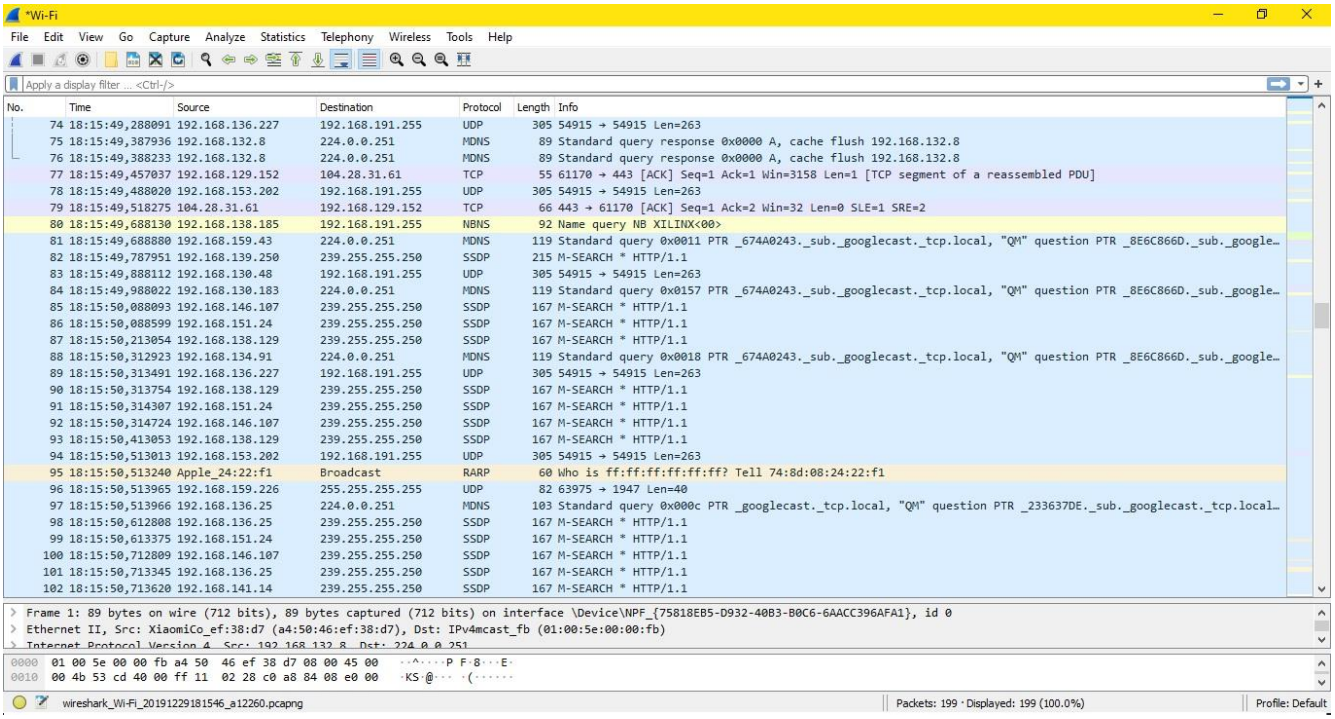
After that process, we can visit http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html this website and we started to capture again. After capture process, we can filter to HHTP protocol. We can see in image process which we did.

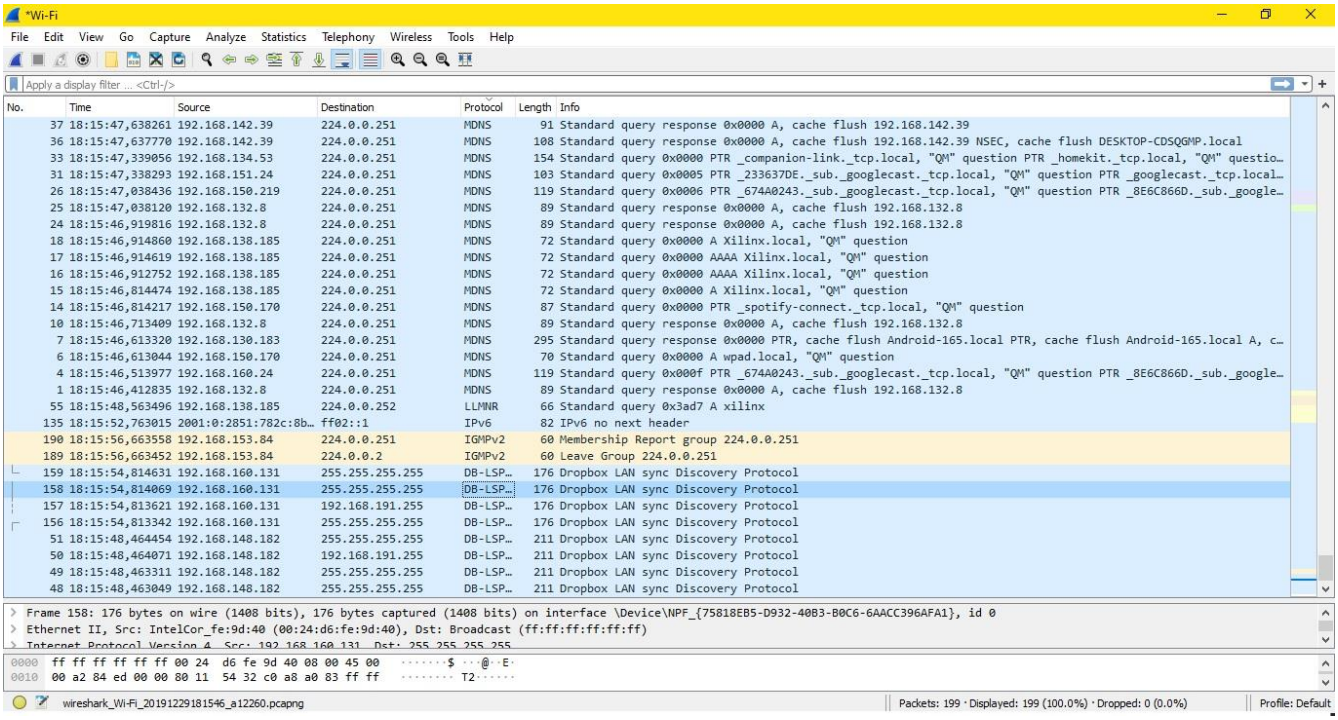


Answers of Questions

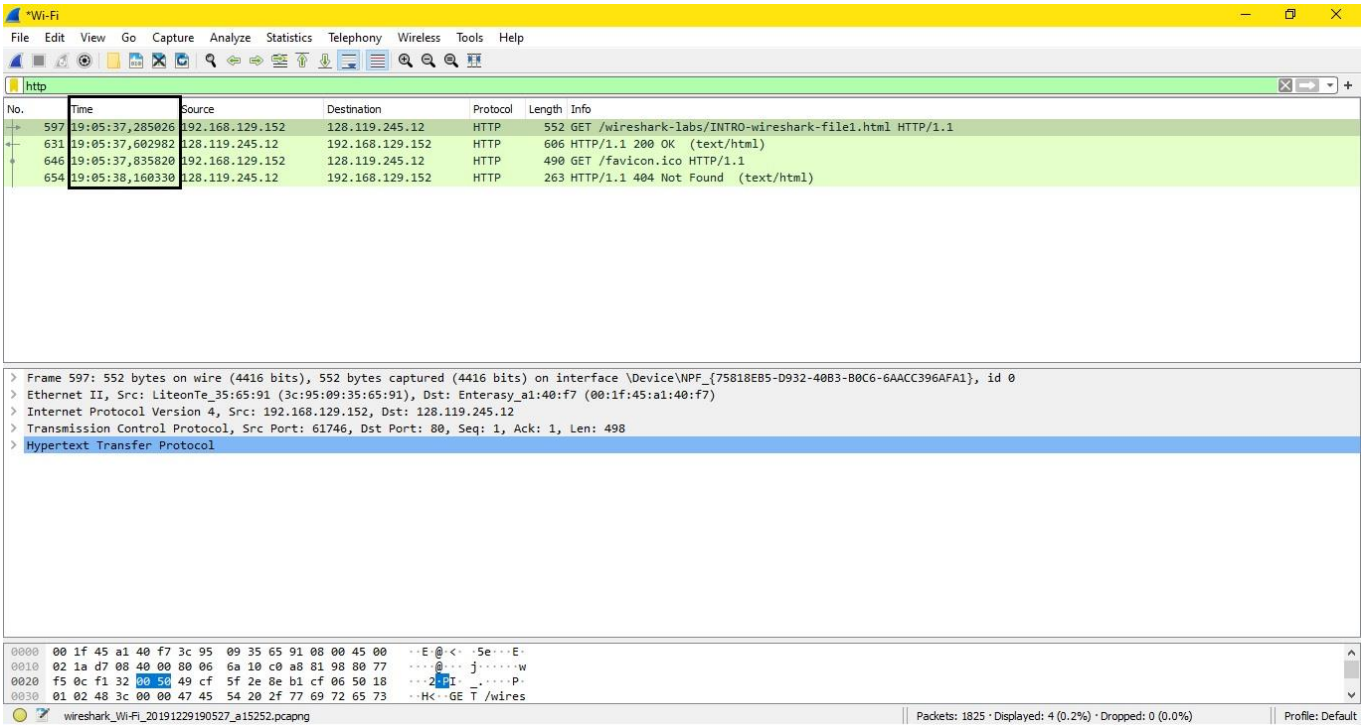
1) We can list 10 different protocols.

MDNS / LLMNR / IPv6 / IGMPv2 / DB-LSP / UDP / TCP / NBNS / SSDP / RARP

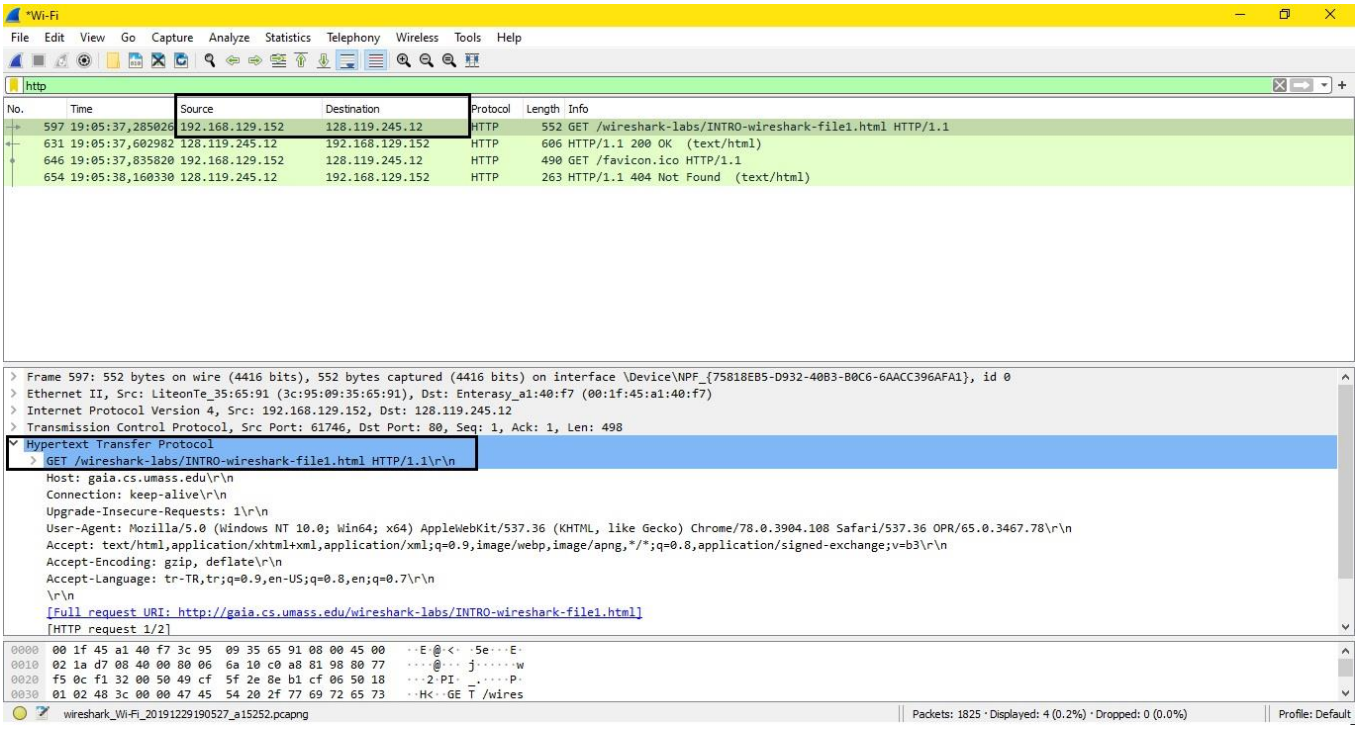




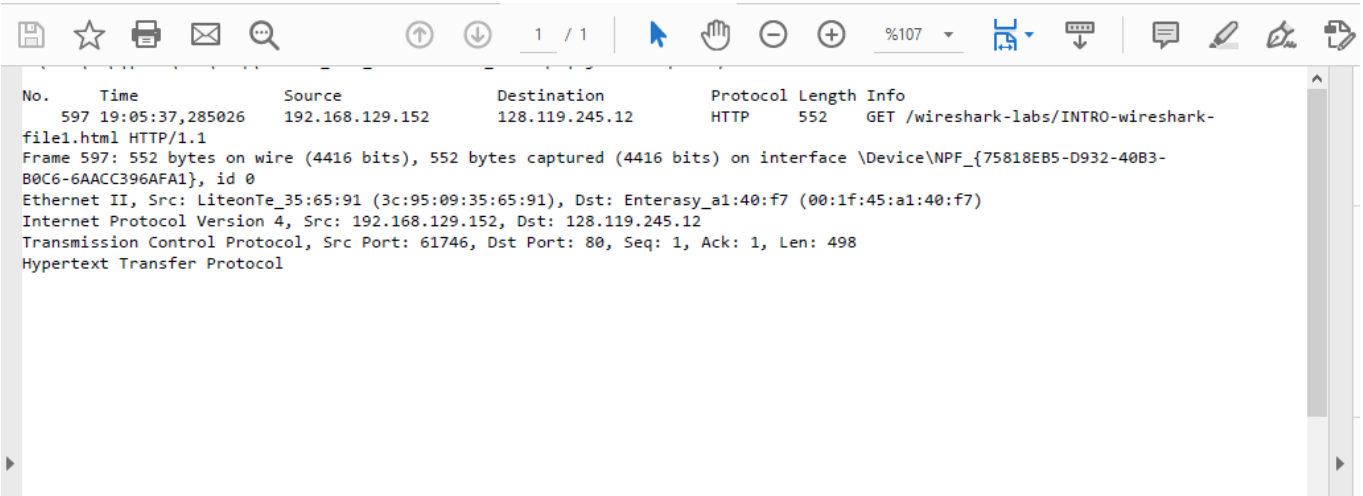
2) In the marked area, we can see time of sending.



3) We can see internet addresses of website and my computer internet address.



4) We printed “Print as displayed” process.



```
No.     Time                Source                Destination           Protocol Length Info
    597 19:05:37,285026     192.168.129.152       128.119.245.12        HTTP     552    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 597: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{75818EB5-D932-40B3-
B0C6-6AACC396AFA1}, id 0
Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Enterasy_a1:40:f7 (00:1f:45:a1:40:f7)
Internet Protocol Version 4, Src: 192.168.129.152, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61746, Dst Port: 80, Seq: 1, Ack: 1, Len: 498
Hypertext Transfer Protocol
```

ASSINGMENT II

1. The Basic HTTP GET/response interaction

We did same processes in Assignment I. This is printed form.

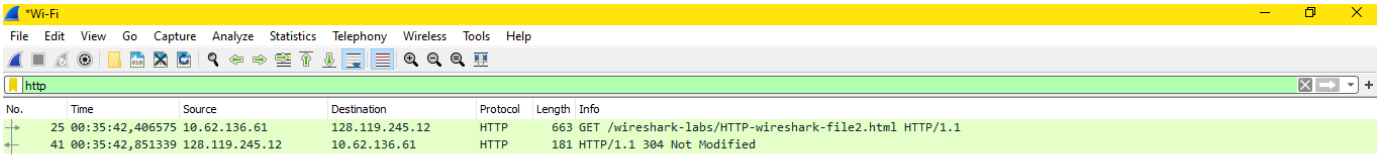
```
No.     Time              Source              Destination         Protocol Length Info
    245 00:10:53,403778   10.62.136.61        128.119.245.12      HTTP     551    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 245: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{75818EB5-D932-40B3-
B0C6-6AACC396AFA1}, id 0
Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Cisco_9f:f2:8a (00:00:0c:9f:f2:8a)
Internet Protocol Version 4, Src: 10.62.136.61, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55573, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
    Source Port: 55573
    Destination Port: 80
    [Stream index: 12]
    [TCP Segment Len: 497]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 4251117732
    [Next sequence number: 498    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1019213120
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0x2feb [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (497 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
OPR/65.0.3467.78\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
```

Answers of Questions

1- My browser running version 1.1 of HHTP. We can see screnshot of packet list.
2- Tr-TR, tr;q=0.9, en-US;q=0.8; en;q=0.7\r\n
3- My computer ip: 192.168.129.152
   gaia.cs.umass.edu's ip : 128.119.245.12
4- ?
5- ?
6- Header lenght : 20 bytes / TCP Payload 497 bytes
7- ?

2. The HTTP CONDITIONAL GET/response interaction

We implemented the steps and we reached these two situation.




```
No.     Time                Source                Destination           Protocol Length Info
     25 00:35:42,406575     10.62.136.61          128.119.245.12        HTTP     663    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 25: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits) on interface \Device\NPF_{75818EB5-D932-40B3-
B0C6-6AACC396AFA1}, id 0
Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Cisco_9f:f2:8a (00:00:0c:9f:f2:8a)
Internet Protocol Version 4, Src: 10.62.136.61, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52796, Dst Port: 80, Seq: 1, Ack: 1, Len: 609
Hypertext Transfer Protocol
No.     Time                Source                Destination           Protocol Length Info
     41 00:35:42,851339     128.119.245.12        10.62.136.61          HTTP     181    HTTP/1.1 304 Not Modified
Frame 41: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface \Device\NPF_{75818EB5-D932-40B3-
B0C6-6AACC396AFA1}, id 0
Ethernet II, Src: Cisco_1f:67:00 (a0:e0:af:1f:67:00), Dst: LiteonTe_35:65:91 (3c:95:09:35:65:91)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.62.136.61
Transmission Control Protocol, Src Port: 80, Dst Port: 52796, Seq: 1, Ack: 610, Len: 127
```

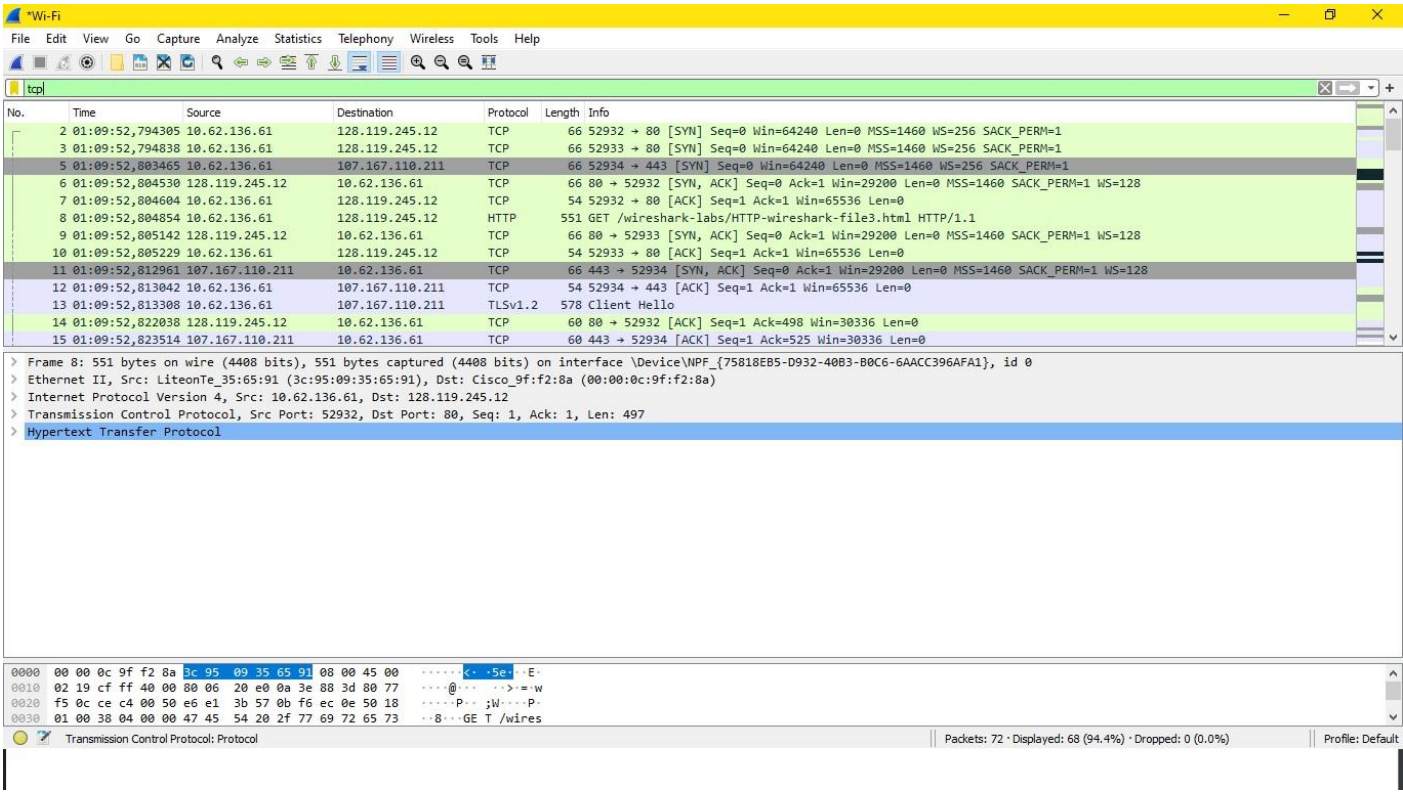
Answers of Questions

8) There is no IF-MODIFIED-SINCE line

9) No. There is a mistake but i cannot find it.

10 and 11) There is no IF-MODIFIED-SINCE line and no response text from server.

3. Retrieving Long Documents



Answers of Questions

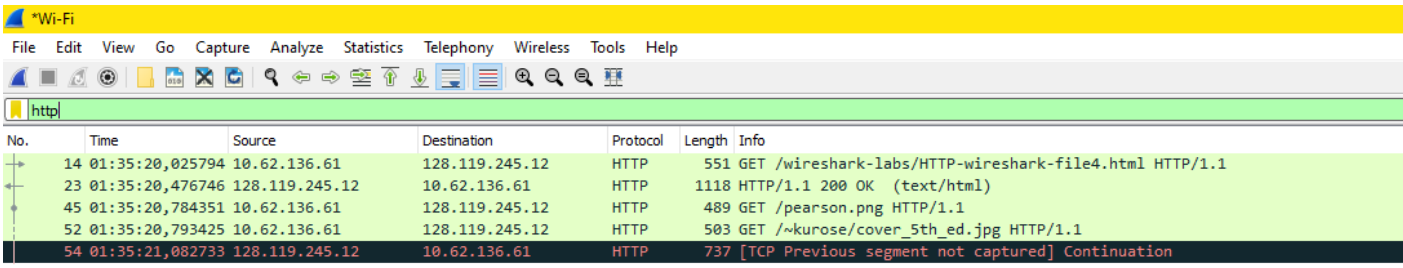
12) One http GET request sent. (no:8)

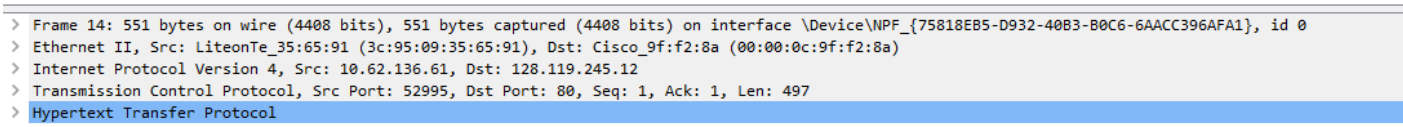
13) ?

14) ?

15) There is no TCP segment of a reassembled PDU.

4. HTML Documents with Embedded Objects



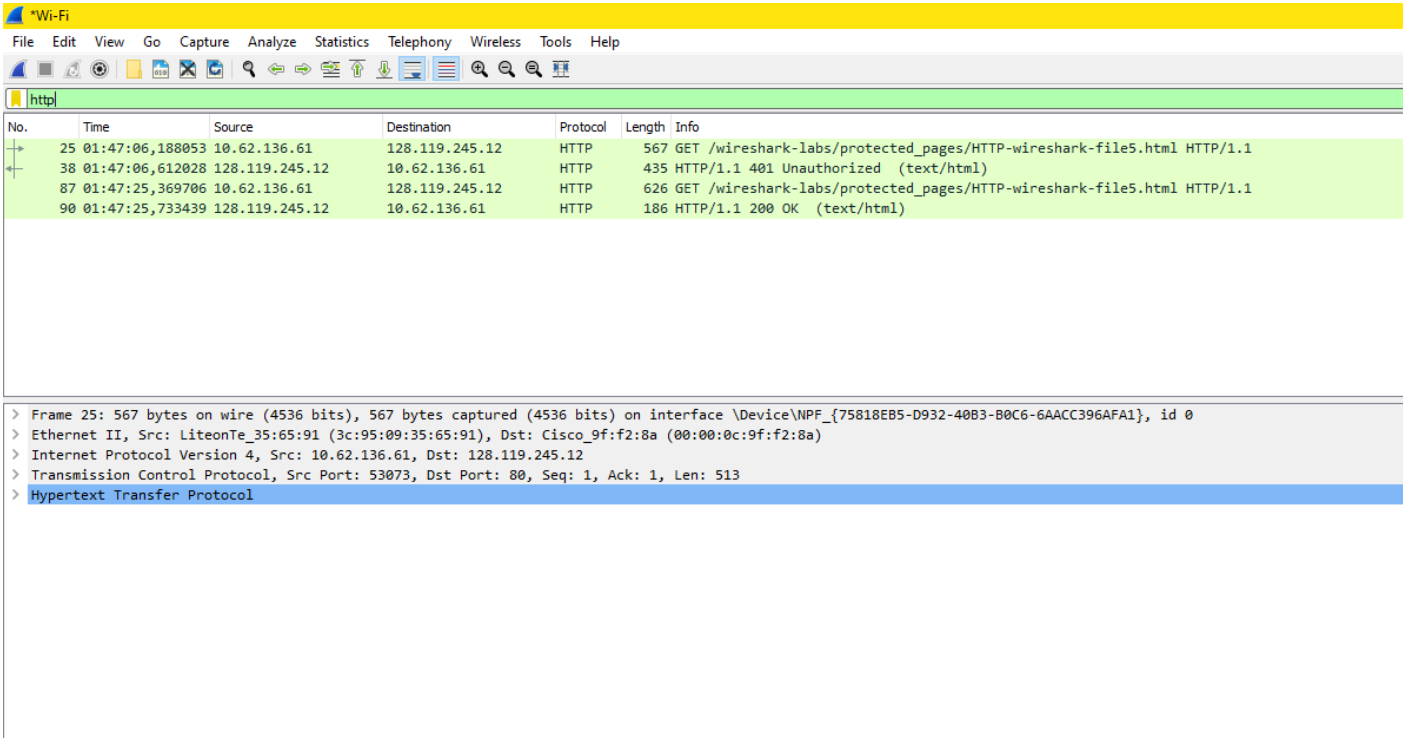


Answers of Questions

16) There is no any HTTP GET request message. There are 3 GET message request and these are 14,45 and 52.

17) My browser downloaded serially. I did not see any delay.

5. HTTP Authentication



Answers of Questions

18) I could not find the http HTTP GET message from Wireshark.

19) ?

ASSIGNMENT III

1. Capturing a bulk TCP transfer from your computer to a remote server

First of all, we visited to http://gaia.cs.umass.edu/wiresharklabs/alice.txt this website and after that, we visited http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html this website. After, as we can see in the assignment file, we saw this.

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 copy of Alice and Wonderland from http://gaia.cs.umass.edu/wireshark-labs/alice.txt and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

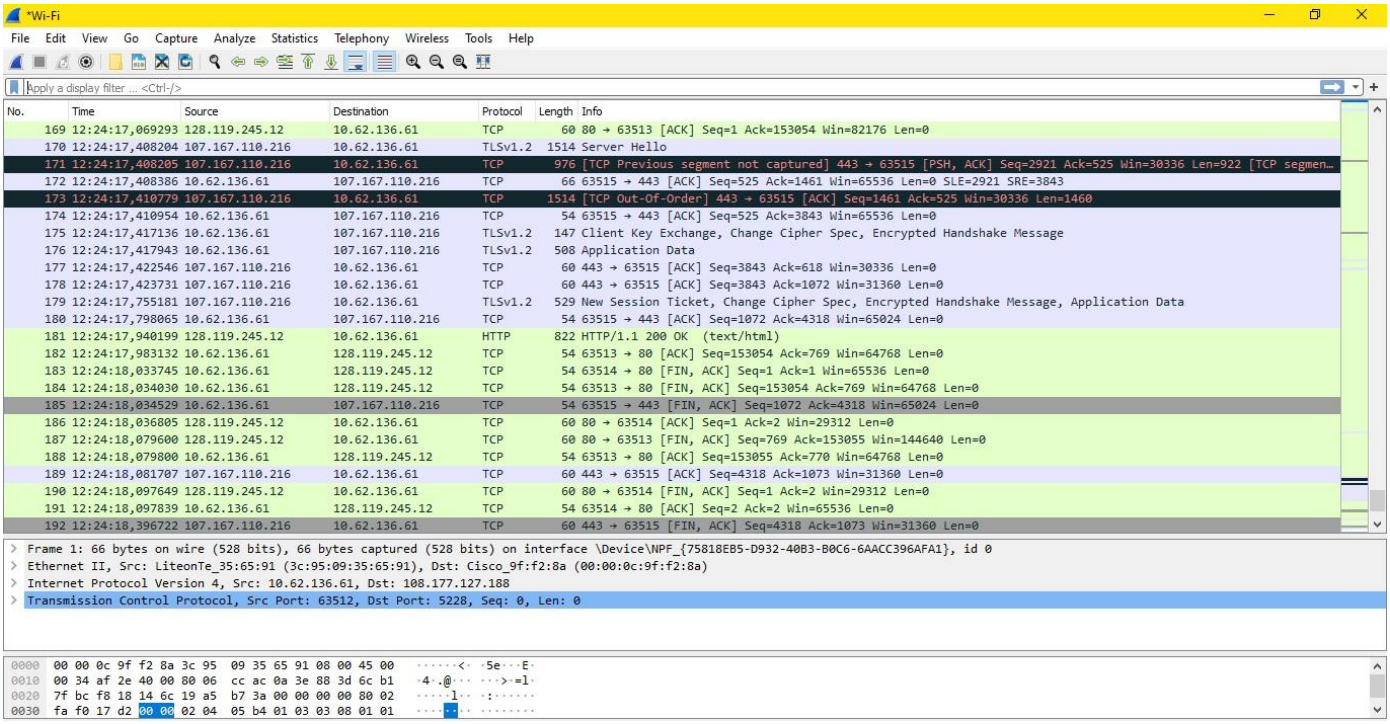
Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

Dosya Seç Dosya seçilmedi

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to gaia.cs.umass.edu!!

Upload alice.txt file

After this step, we used browse button and we selected story of alice text file which we already downloaded. After, we started captured process with Wireshark and we reached this situation.



2. A first look at the captured trace

Answers of Questions

1-2-3) We could reached to this situation after we implement the steps which given from pdf.
We can see IP addresses source and destination.

```
No.     Time                Source              Destination         Protocol Length Info
      1 16:44:20,570381     192.168.1.102       128.119.245.12      TCP      62     1161 → 80 [SYN] Seq=0 Win=16384 Len=0
MSS=1460 SACK_PERM=1
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: 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: 0, Len: 0
```

We can see port numbers.

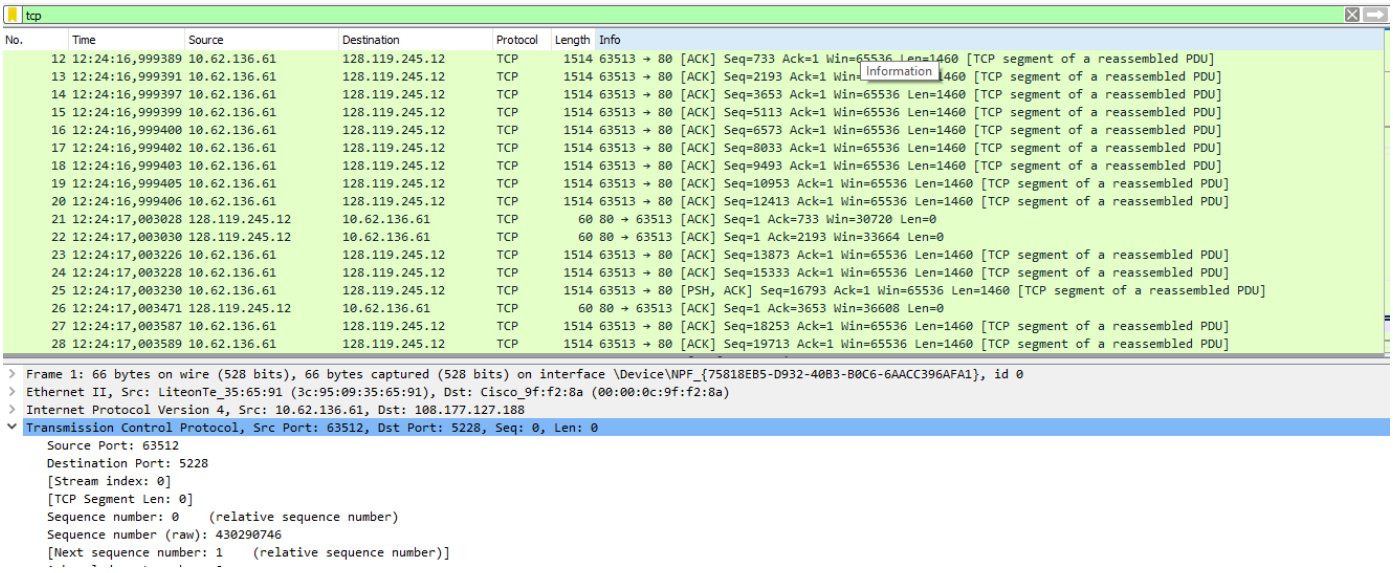
	Time	Source	Destination	Protocol	Length	Info
1	16:44:20,570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	16:44:20,593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	16:44:20,593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	16:44:20,596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	16:44:20,612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	16:44:20,624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	16:44:20,624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	16:44:20,625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	16:44:20,647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	16:44:20,647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	16:44:20,648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
12	16:44:20,694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	16:44:20,694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]

```
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 232129012
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x002 (SYN)
    Window size value: 16384
    [Calculated window size: 16384]
    Checksum: 0xf6e9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

3. TCP Basics

Answers of Question

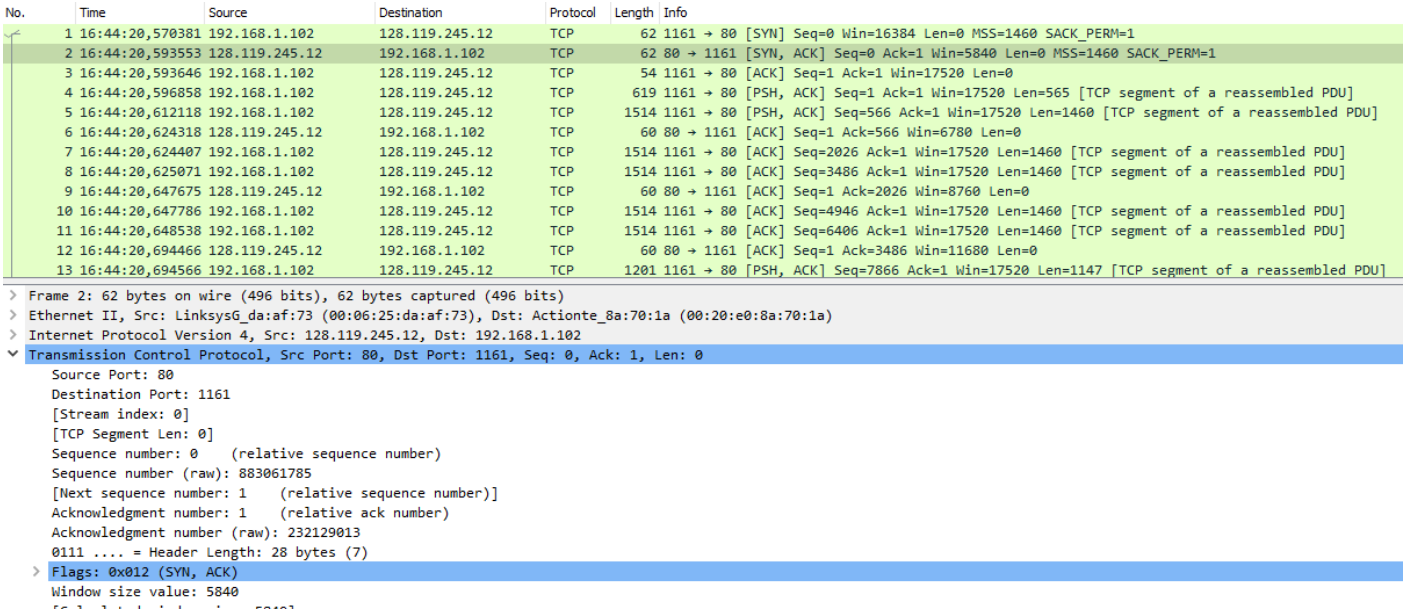
4) We can see sequence number of trace. Its 0.



No.	Time	Source	Destination	Protocol	Length	Info
12	12:24:16,999389	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=733 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
13	12:24:16,999391	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=2193 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
14	12:24:16,999397	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=3653 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
15	12:24:16,999399	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=5113 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
16	12:24:16,999400	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=6573 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
17	12:24:16,999402	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=8033 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
18	12:24:16,999403	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=9493 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
19	12:24:16,999405	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=10953 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
20	12:24:16,999406	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=12413 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
21	12:24:17,003028	128.119.245.12	10.62.136.61	TCP	60	80 → 63513 [ACK] Seq=1 Ack=733 Win=30720 Len=0
22	12:24:17,003030	128.119.245.12	10.62.136.61	TCP	60	80 → 63513 [ACK] Seq=1 Ack=2193 Win=33664 Len=0
23	12:24:17,003226	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=13873 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
24	12:24:17,003228	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=15333 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
25	12:24:17,003230	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [PSH, ACK] Seq=16793 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
26	12:24:17,003471	128.119.245.12	10.62.136.61	TCP	60	80 → 63513 [ACK] Seq=1 Ack=3653 Win=36608 Len=0
27	12:24:17,003587	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=18253 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
28	12:24:17,003589	10.62.136.61	128.119.245.12	TCP	1514	63513 → 80 [ACK] Seq=19713 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{75818EB5-D932-40B3-B0C6-6AACC396AFA1}, id 0
> Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Cisco_9f:f2:8a (00:00:0c:9f:f2:8a)
> Internet Protocol Version 4, Src: 10.62.136.61, Dst: 108.177.127.188
v Transmission Control Protocol, Src Port: 63512, Dst Port: 5228, Seq: 0, Len: 0
    Source Port: 63512
    Destination Port: 5228
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 430290746
    [Next sequence number: 1    (relative sequence number)]
```

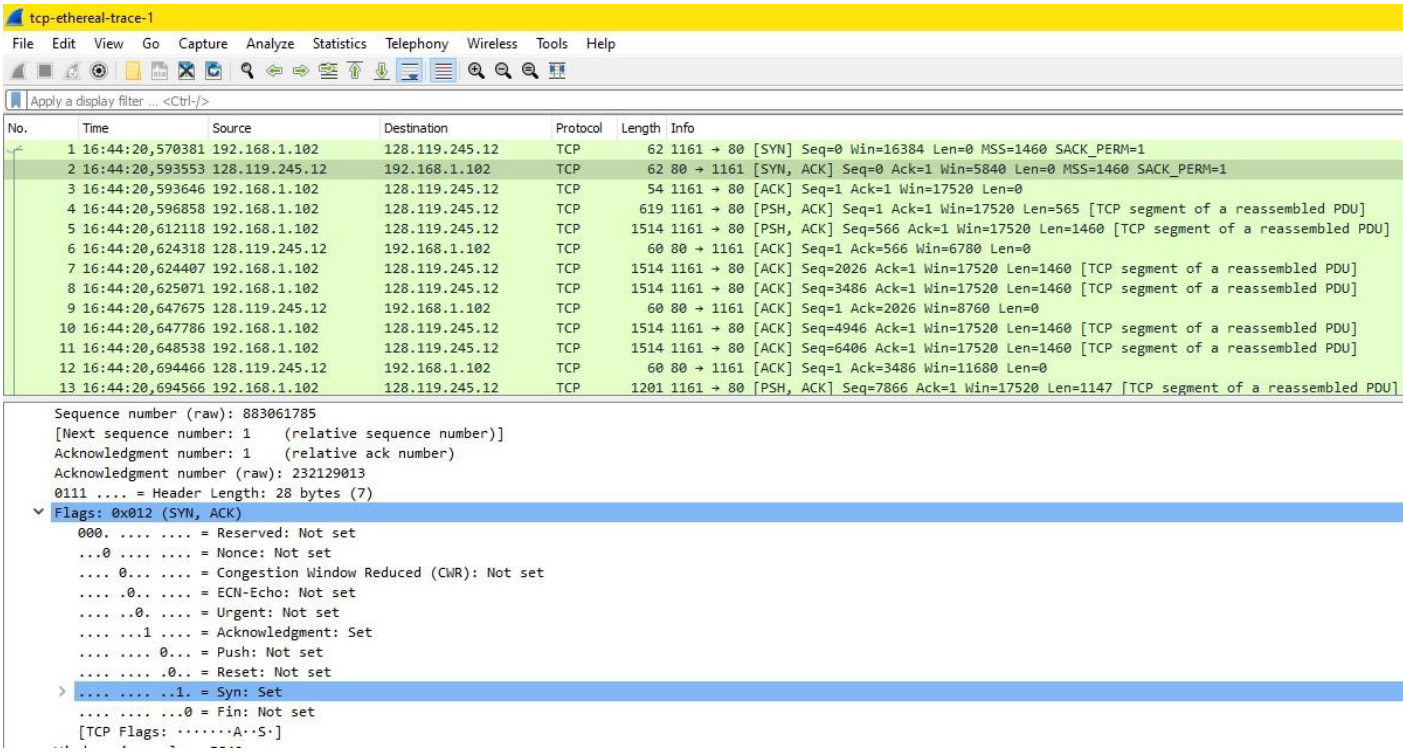
5) Sequence number of SYNACK segment is 1.



No.	Time	Source	Destination	Protocol	Length	Info
1	16:44:20,570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	16:44:20,593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	16:44:20,593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	16:44:20,596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	16:44:20,612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	16:44:20,624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	16:44:20,624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	16:44:20,625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	16:44:20,647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	16:44:20,647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	16:44:20,648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
12	16:44:20,694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	16:44:20,694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]

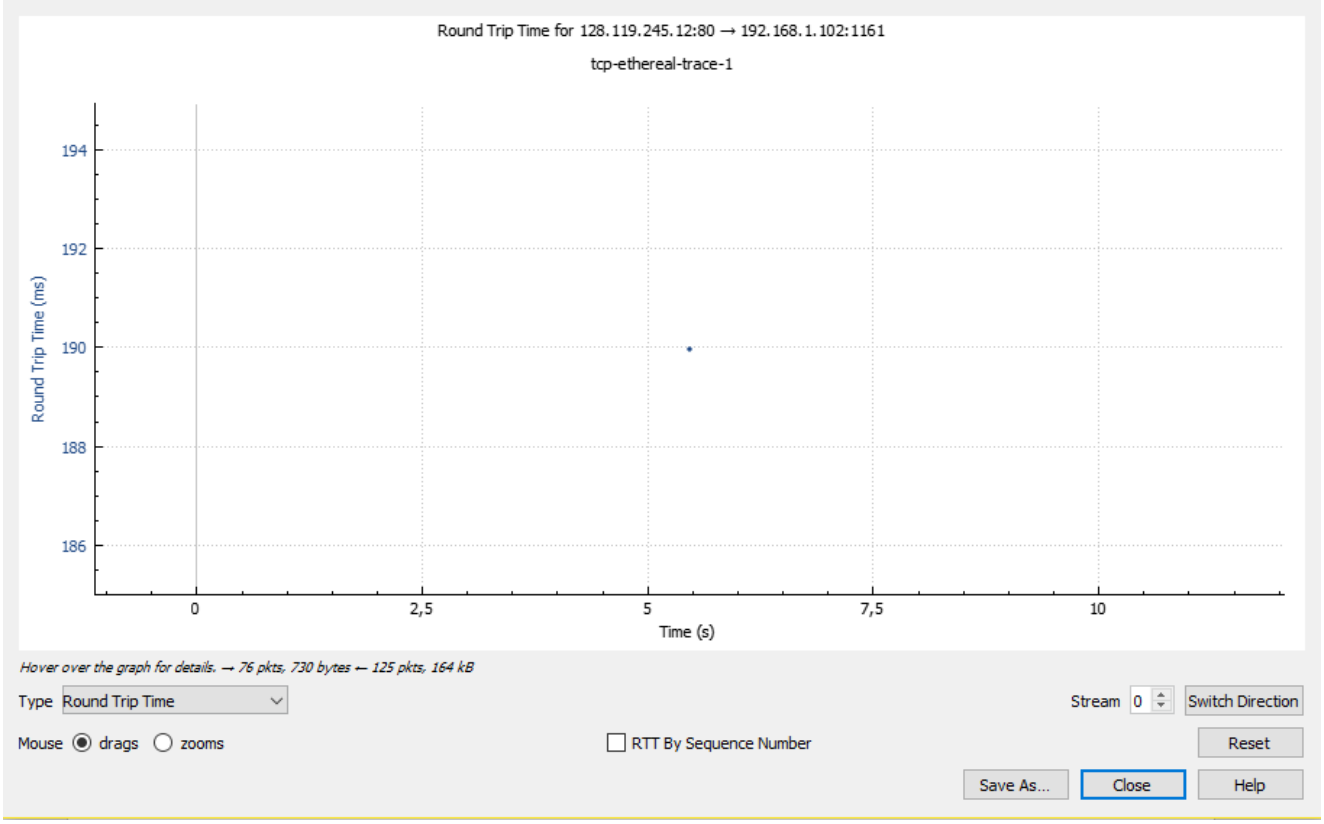
```
> Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [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)
    Window size value: 5840
```

6) We can see details of sequence number of the TCP segment containing the HTTP POST Command.



No.	Time	Source	Destination	Protocol	Length	Info
1	16:44:20,570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	16:44:20,593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	16:44:20,593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	16:44:20,596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	16:44:20,612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	16:44:20,624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	16:44:20,624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	16:44:20,625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	16:44:20,647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	16:44:20,647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	16:44:20,648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
12	16:44:20,694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	16:44:20,694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]

7) I could not to find solution of answer. I can add the graph of Round Trip Time but there may be mistake.



8) 62+62+54+619+1514+60 = 2371 bytes

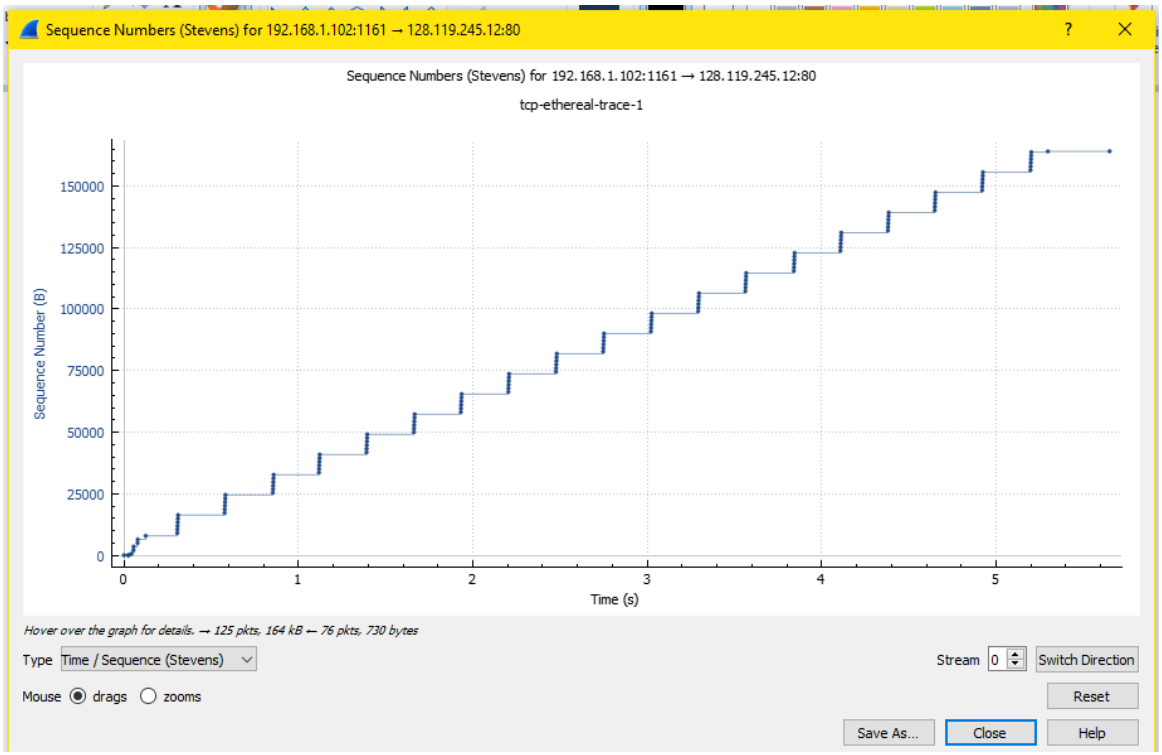
No.	Time	Source	Destination	Protocol	Length	Info
1	16:44:20,570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	16:44:20,593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	16:44:20,593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	16:44:20,596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a
5	16:44:20,612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of
6	16:44:20,624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	16:44:20,624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a r
8	16:44:20,625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a r
9	16:44:20,647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	16:44:20,647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a r
11	16:44:20,648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a r
12	16:44:20,694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	16:44:20,694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment o

```
> 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
v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 730
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 730]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 883061786
    [Next sequence number: 731    (relative sequence number)]
    Acknowledgment number: 164091    (relative ack number)
    Acknowledgment number (raw): 232293103
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 00   · ··p··· %··s··E·
0010  03 02 58 bc 40 00 37 06  b0 a7 80 77 f5 0c c0 a8   ··X·@·7· ···w····
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
```

9) ?

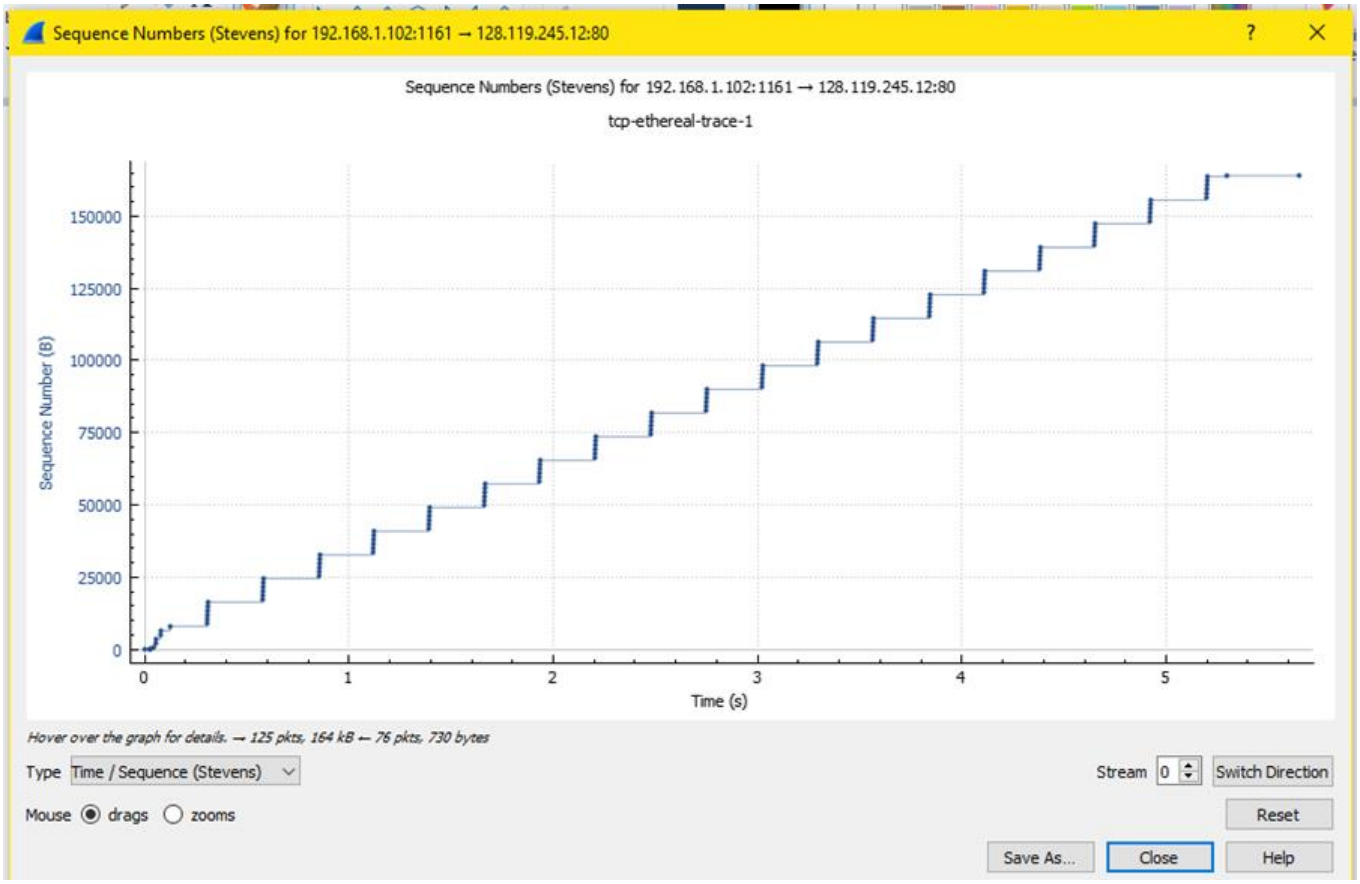
10) Time Sequence-Graph (Stevens)



11) ?

12)?

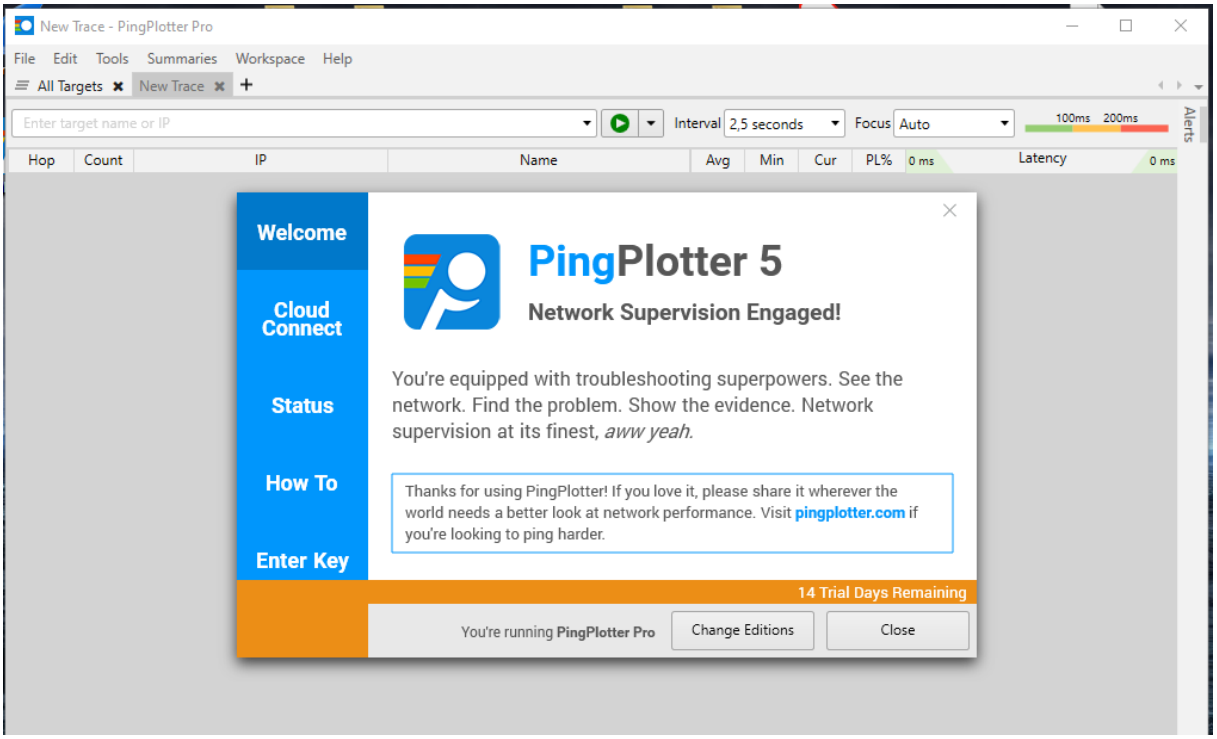
13 and 14) Question ask same graph. Time-Sequence-Graph(Stevens)



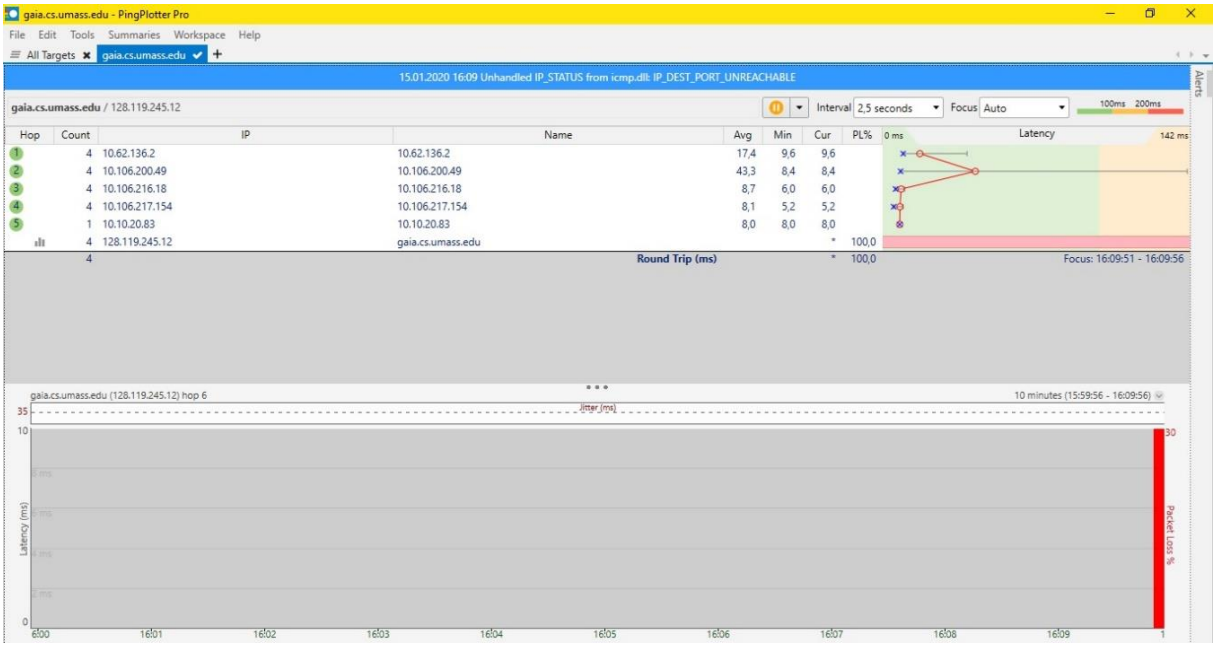
ASSIGNMENT IV

1. Capturing packets from an execution of traceroute

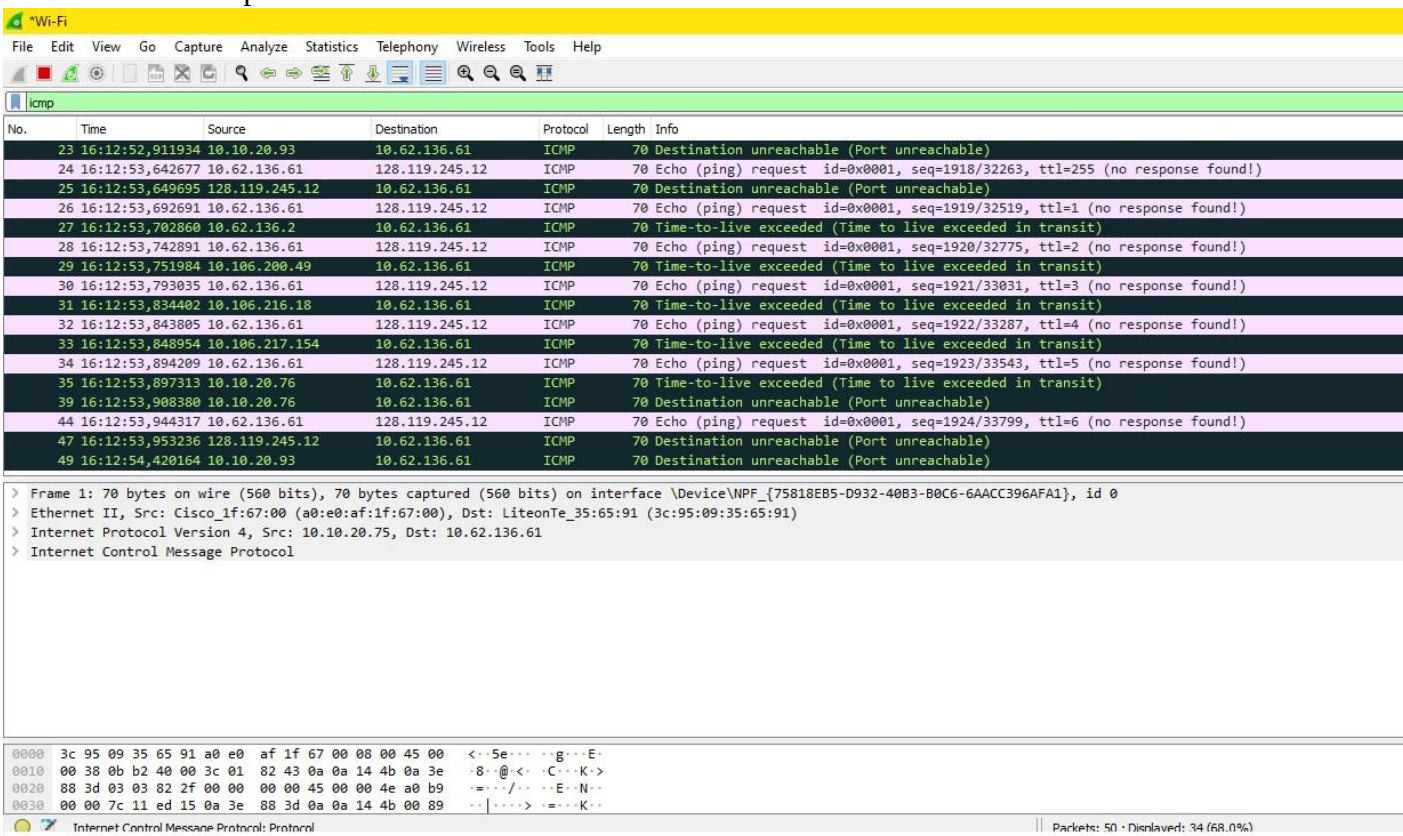
First step is downloaded the PingPlotter program.



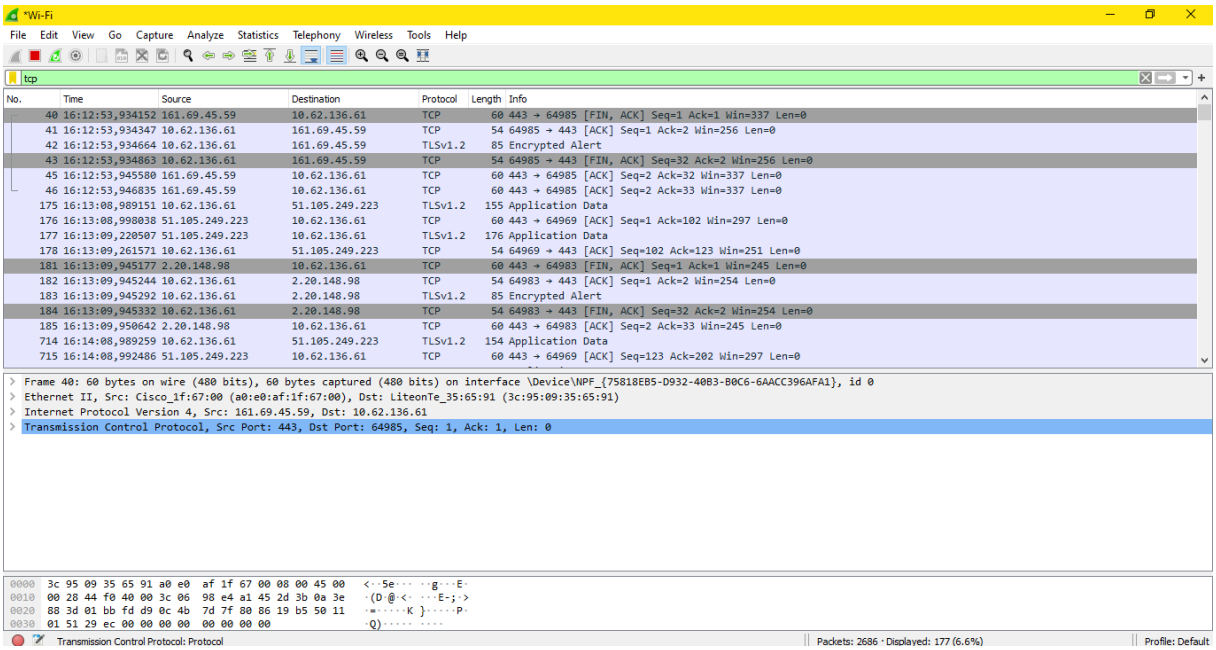
After, we can go to aia.cs.umass.edu



We can see ICMP protocol list



Also, we captured and listed the TCP protocols.



Answers of Questions

1) IP of my computer: 192.168.129.152

IP of aia.cs.umass.edu: 128.119.245.12

2) ?

3) Header lenght is 20 bytes.

4) Data is not fragmented.

5) According to identification, Time to live and Header checksum can change.

6) ?

7)

```
> Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Cisco_9f:f2:8a (00:00:0c:9f:f2:8a)
> Internet Protocol Version 4, Src: 10.62.136.61, Dst: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2ebf [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1918 (0x077e)
    Sequence number (LE): 32263 (0x7e07)
  > [No response seen]
  > Data (28 bytes)
```

Important Note:

There are no answers of questions 8-9-10-11-12-13-14-15 in the assignment file.

Because i could not find and solve it. I did not want to copy and paste the answers from internet. So, this is the last page and last form of my assignment.