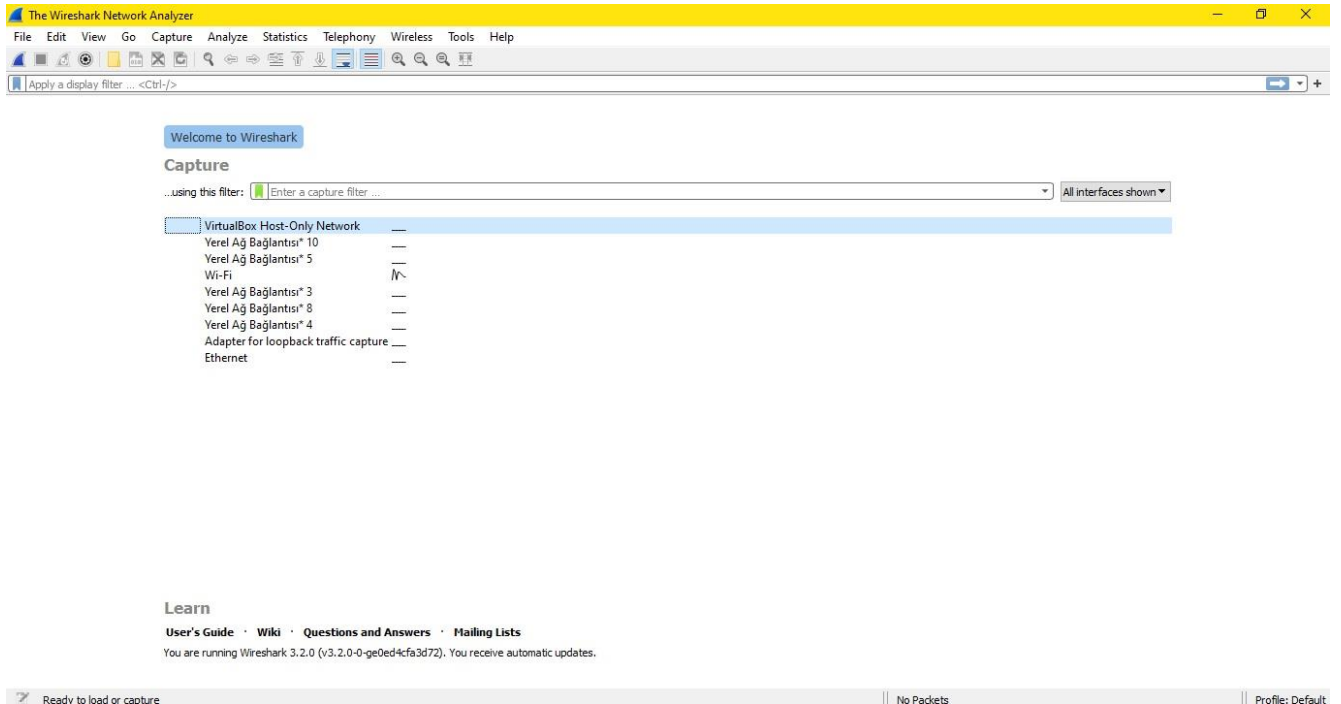
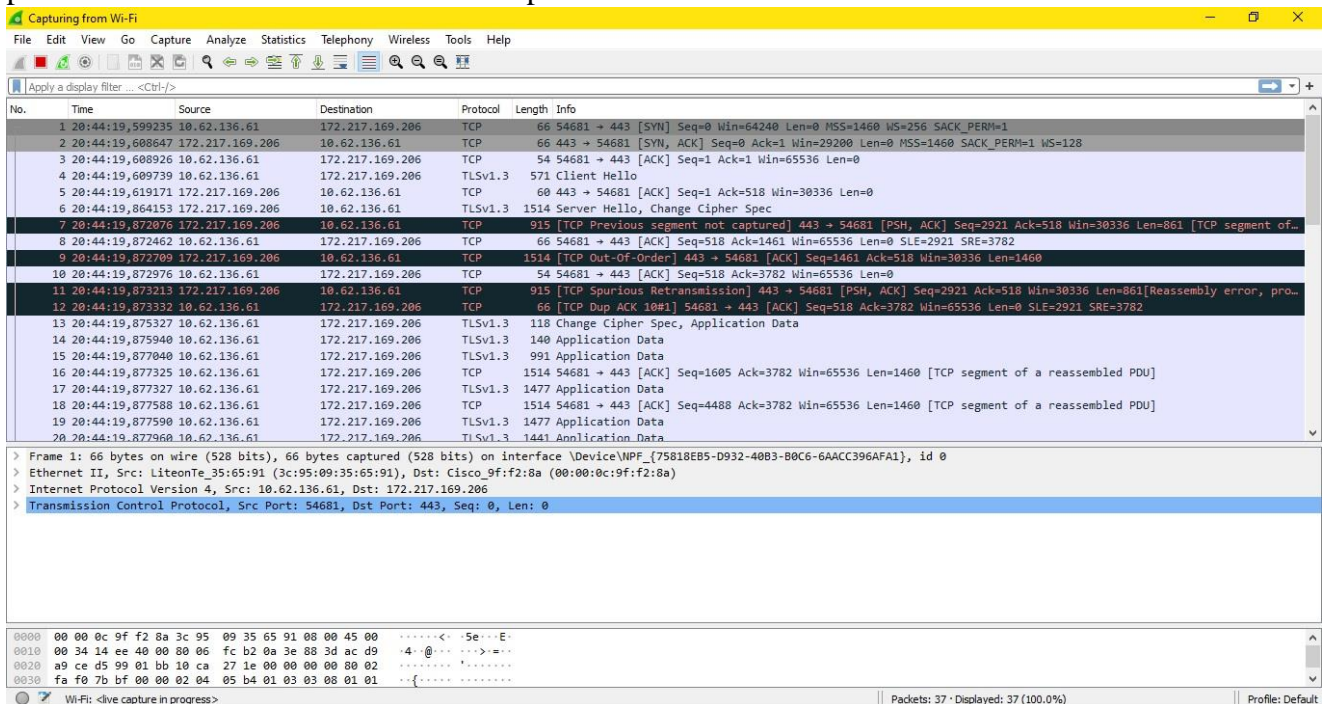


ASSIGNMENT I

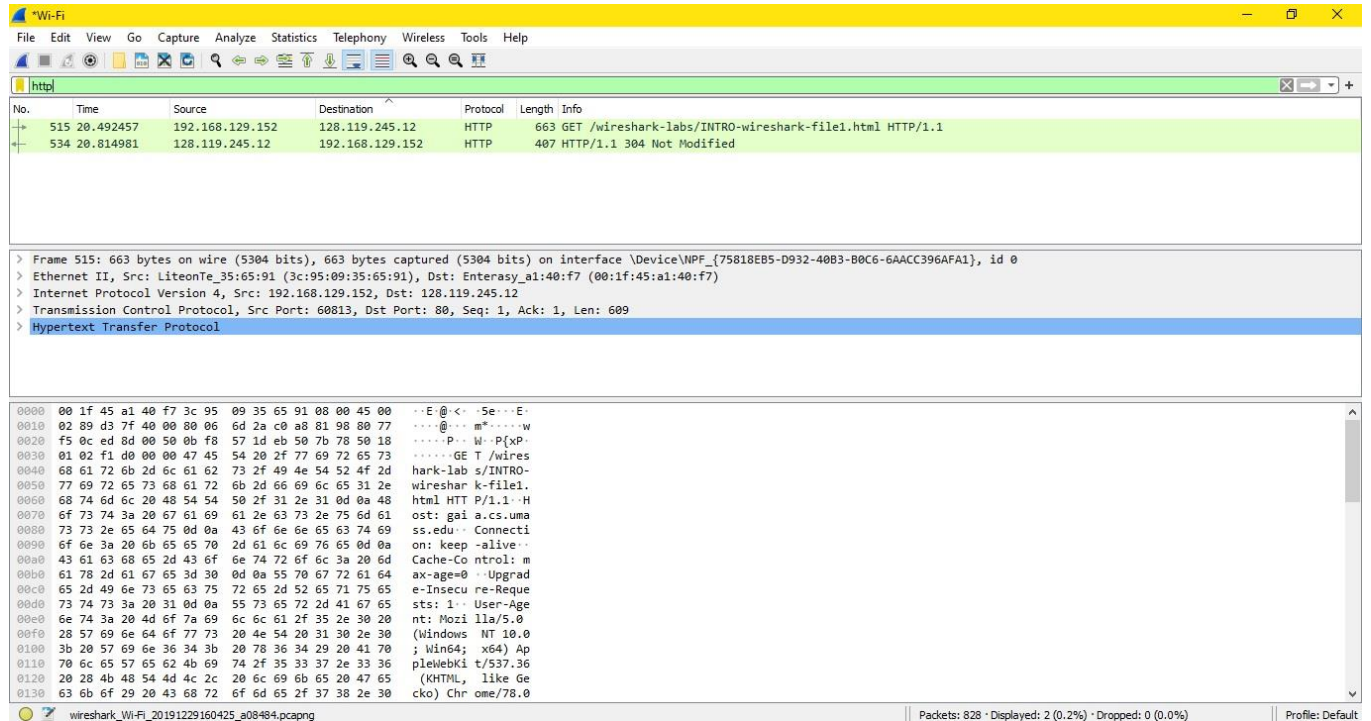
In first step, we opened the any internet browser. After, we opened also Wireshark program.



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.



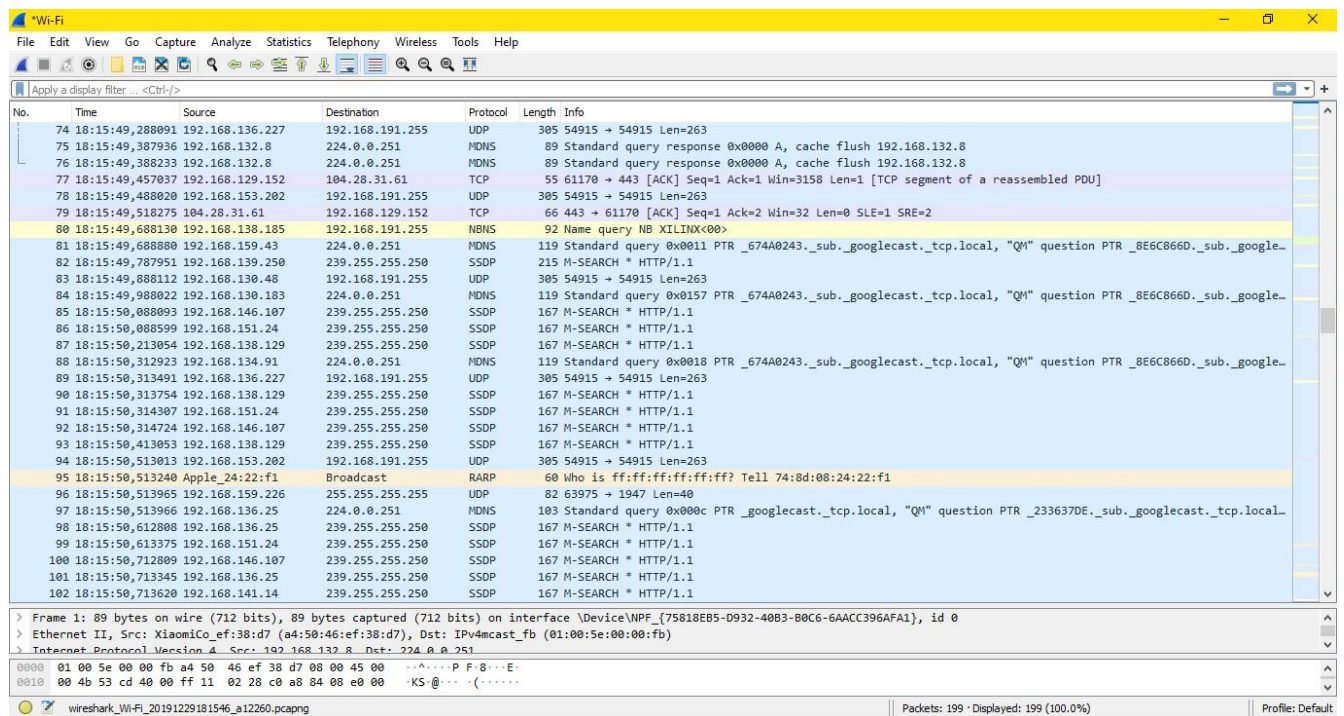
After that process, we can visit <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> this website and we started to capture again. After capture process, we can filter to HTTP protocol. We can see in image process which we did.



Answers of Questions

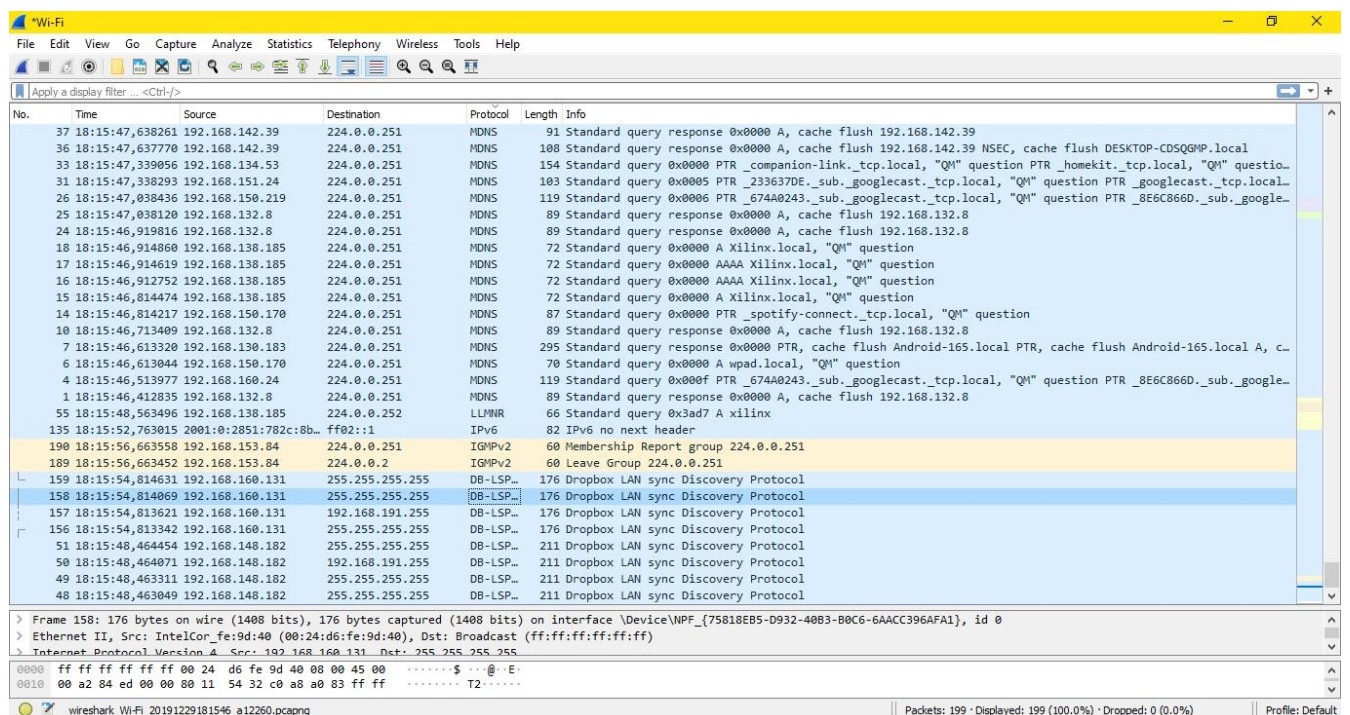
1) We can list 10 different protocols.

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



The screenshot shows a Wireshark packet capture on a Wi-Fi interface. The packet list on the left contains 102 packets. The packet details pane on the right shows the structure of a selected packet (No. 80), which is a Name query (PTR) for a Googlecast service. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

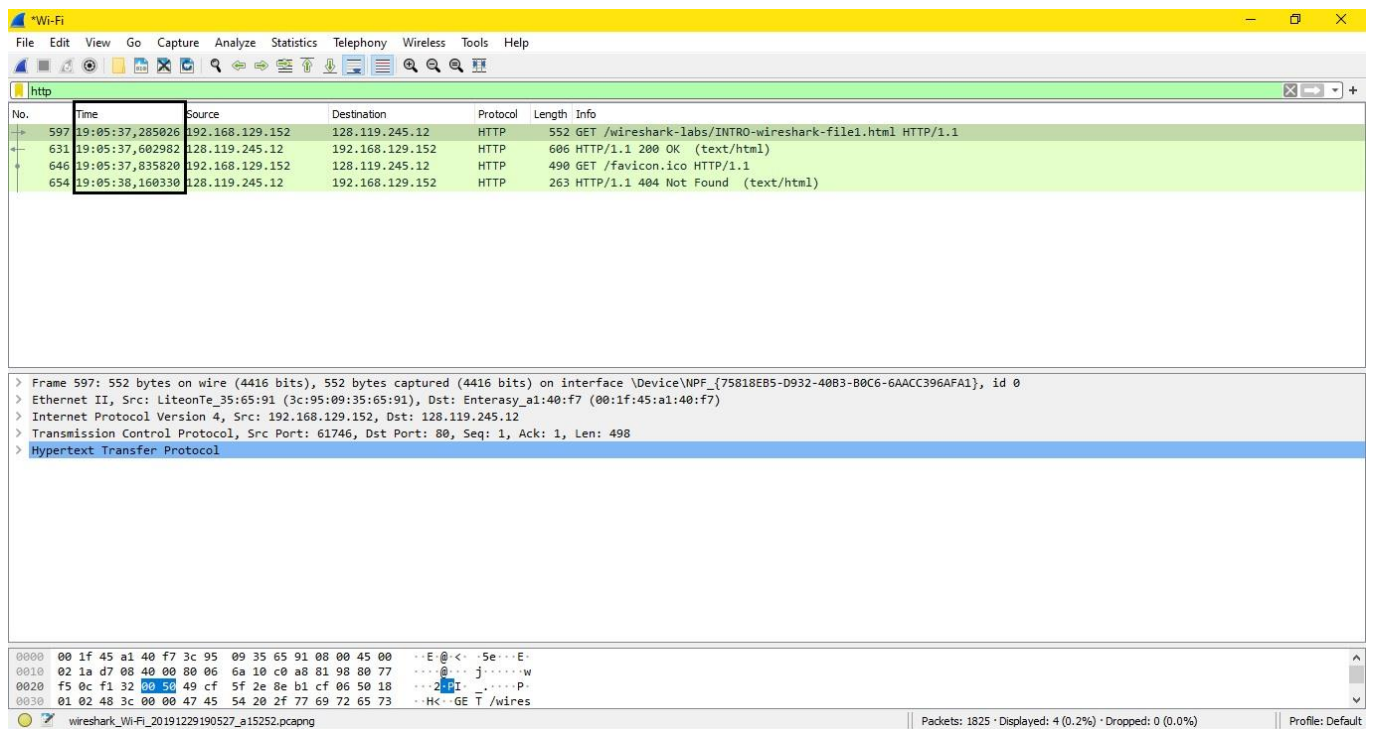
No.	Time	Source	Destination	Protocol	Length	Info
74	18:15:49,288091	192.168.136.227	192.168.191.255	UDP	305	54915 → 54915 Len=263
75	18:15:49,387936	192.168.132.8	224.0.0.251	MDNS	89	Standard query response 0x0000 A, cache flush 192.168.132.8
76	18:15:49,388233	192.168.132.8	224.0.0.251	MDNS	89	Standard query response 0x0000 A, cache flush 192.168.132.8
77	18:15:49,457037	192.168.129.152	104.28.31.61	TCP	55	61170 → 443 [ACK] Seq=1 Ack=1 Win=3158 Len=1 [TCP segment of a reassembled PDU]
78	18:15:49,480820	192.168.153.202	192.168.191.255	UDP	305	54915 → 54915 Len=263
79	18:15:49,518275	104.28.31.61	192.168.129.152	TCP	66	443 → 61170 [ACK] Seq=1 Ack=2 Len=0 SLE=1 SRE=2
80	18:15:49,688130	192.168.138.185	192.168.191.255	NBNS	92	Name query NB XILINX<00>
81	18:15:49,688880	192.168.159.43	224.0.0.251	MDNS	119	Standard query 0x0011 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._google...
82	18:15:49,787951	192.168.139.250	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
83	18:15:49,888112	192.168.130.48	192.168.191.255	UDP	305	54915 → 54915 Len=263
84	18:15:49,988022	192.168.130.183	224.0.0.251	MDNS	119	Standard query 0x0157 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._google...
85	18:15:50,088093	192.168.146.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
86	18:15:50,088599	192.168.151.24	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
87	18:15:50,213054	192.168.138.129	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
88	18:15:50,312923	192.168.134.91	224.0.0.251	MDNS	119	Standard query 0x0018 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._google...
89	18:15:50,313491	192.168.136.227	192.168.191.255	UDP	305	54915 → 54915 Len=263
90	18:15:50,313754	192.168.138.129	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
91	18:15:50,314307	192.168.151.24	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
92	18:15:50,314724	192.168.146.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
93	18:15:50,413053	192.168.138.129	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
94	18:15:50,513013	192.168.153.202	192.168.191.255	UDP	305	54915 → 54915 Len=263
95	18:15:50,513240	Apple, 24:22:f1	Broadcast	RARP	60	who is ff:ff:ff:ff:ff:ff? Tell 74:8d:08:24:22:f1
96	18:15:50,513965	192.168.159.226	255.255.255.255	UDP	82	63975 → 1947 Len=40
97	18:15:50,513966	192.168.136.25	224.0.0.251	MDNS	103	Standard query 0x000c PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local...
98	18:15:50,612808	192.168.136.25	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
99	18:15:50,613375	192.168.151.24	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
100	18:15:50,712809	192.168.146.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
101	18:15:50,713345	192.168.136.25	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
102	18:15:50,713620	192.168.141.14	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1



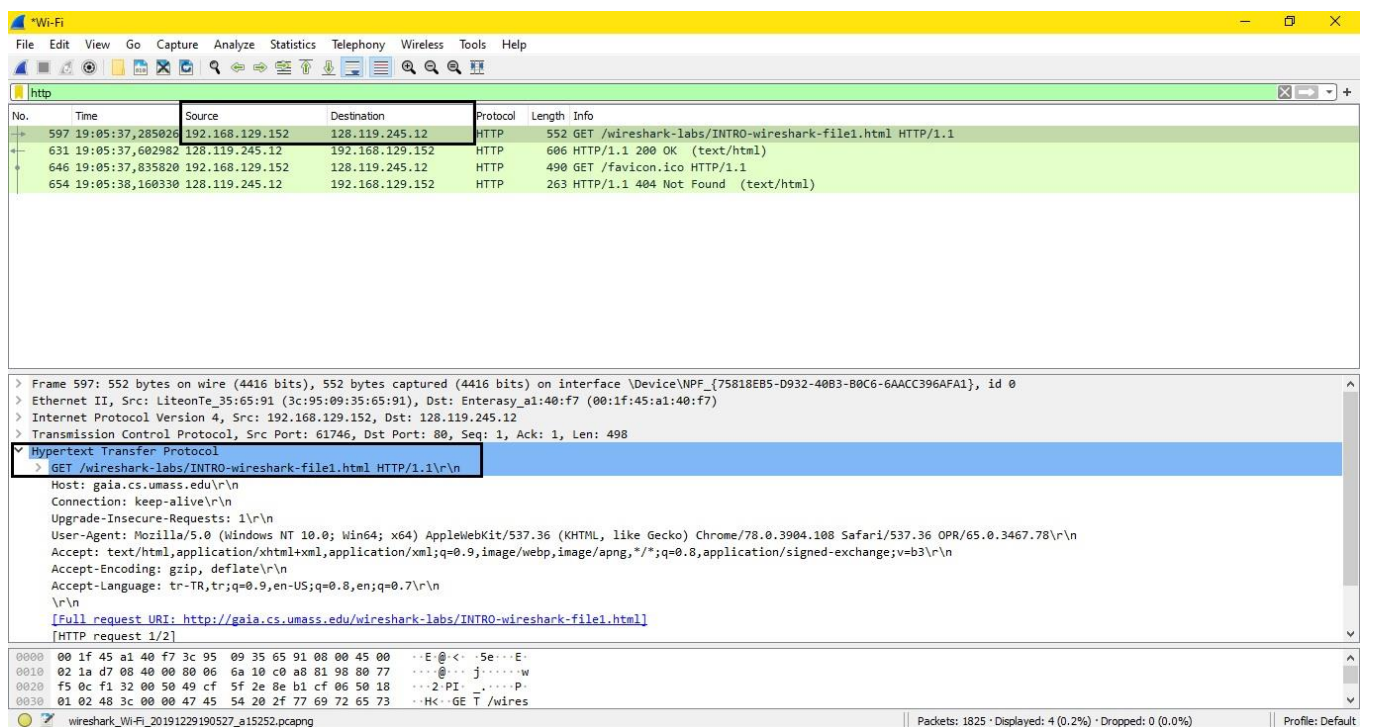
The screenshot shows a Wireshark packet capture on a Wi-Fi interface. The packet list on the left contains 102 packets. The packet details pane on the right shows the structure of a selected packet (No. 80), which is a Name query (PTR) for a Googlecast service. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
37	18:15:47,638261	192.168.142.39	224.0.0.251	MDNS	91	Standard query response 0x0000 A, cache flush 192.168.142.39
36	18:15:47,637770	192.168.142.39	224.0.0.251	MDNS	108	Standard query response 0x0000 A, cache flush 192.168.142.39 NSEC, cache flush DESKTOP-CD5QMP.local
33	18:15:47,339056	192.168.134.53	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" questio...
31	18:15:47,338293	192.168.151.24	224.0.0.251	MDNS	103	Standard query 0x0005 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local...
26	18:15:47,038436	192.168.150.219	224.0.0.251	MDNS	119	Standard query 0x0006 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._google...
25	18:15:47,038120	192.168.132.8	224.0.0.251	MDNS	89	Standard query response 0x0000 A, cache flush 192.168.132.8
24	18:15:46,919816	192.168.132.8	224.0.0.251	MDNS	89	Standard query response 0x0000 A, cache flush 192.168.132.8
18	18:15:46,914860	192.168.138.185	224.0.0.251	MDNS	72	Standard query 0x0000 A Xilinx.local, "QM" question
17	18:15:46,914619	192.168.138.185	224.0.0.251	MDNS	72	Standard query 0x0000 AAAA Xilinx.local, "QM" question
16	18:15:46,912752	192.168.138.185	224.0.0.251	MDNS	72	Standard query 0x0000 AAAA Xilinx.local, "QM" question
15	18:15:46,814474	192.168.138.185	224.0.0.251	MDNS	72	Standard query 0x0000 A Xilinx.local, "QM" question
14	18:15:46,814217	192.168.138.185	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
10	18:15:46,713409	192.168.132.8	224.0.0.251	MDNS	89	Standard query response 0x0000 A, cache flush 192.168.132.8
7	18:15:46,613320	192.168.130.183	224.0.0.251	MDNS	295	Standard query response 0x0000 PTR, cache flush Android-165.local PTR, cache flush Android-165.local A, c...
6	18:15:46,613044	192.168.150.170	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
4	18:15:46,513977	192.168.160.24	224.0.0.251	MDNS	119	Standard query 0x000f PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._google...
1	18:15:46,412835	192.168.132.8	224.0.0.251	MDNS	89	Standard query response 0x0000 A, cache flush 192.168.132.8
55	18:15:48,563496	192.168.138.185	224.0.0.252	LLMNR	66	Standard query 0x3ad7 A xilinx
135	18:15:52,763015	2001:0:2051:782c:8b...	ff02::1	IPv6	82	IPv6 no next header
190	18:15:56,663558	192.168.153.84	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
189	18:15:56,663452	192.168.153.84	224.0.0.2	IGMPv2	60	Leave Group 224.0.0.251
159	18:15:54,814631	192.168.160.131	255.255.255.255	DB-LSP	176	Dropbox LAN sync Discovery Protocol
158	18:15:54,814069	192.168.160.131	255.255.255.255	DB-LSP	176	Dropbox LAN sync Discovery Protocol
157	18:15:54,813621	192.168.160.131	192.168.191.255	DB-LSP	176	Dropbox LAN sync Discovery Protocol
156	18:15:54,813342	192.168.160.131	255.255.255.255	DB-LSP	176	Dropbox LAN sync Discovery Protocol
151	18:15:48,464454	192.168.148.182	255.255.255.255	DB-LSP	211	Dropbox LAN sync Discovery Protocol
50	18:15:48,464071	192.168.148.182	192.168.191.255	DB-LSP	211	Dropbox LAN sync Discovery Protocol
49	18:15:48,463311	192.168.148.182	255.255.255.255	DB-LSP	211	Dropbox LAN sync Discovery Protocol
48	18:15:48,463049	192.168.148.182	255.255.255.255	DB-LSP	211	Dropbox LAN sync Discovery Protocol

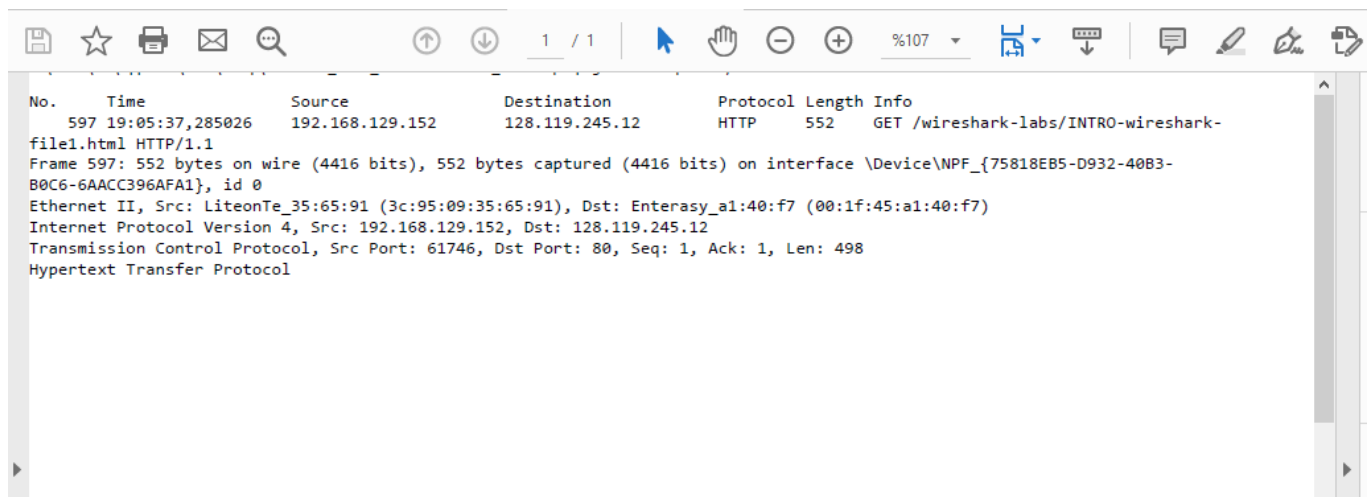
2) In the marked area, we can see time of sending.



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



4) We printed “Print as displayed” process.



ASSINGMENT II

1. The Basic HTTP GET/response interaction

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

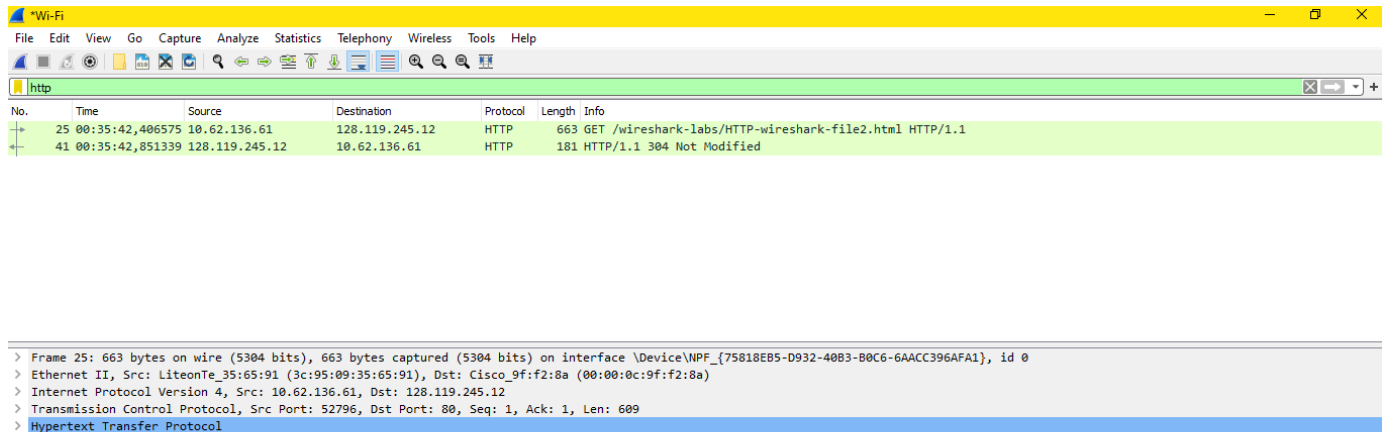
No.	Time	Source	Destination	Protocol	Length	Info
245	00:10:53.403778	10.62.136.61	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1						
Frame 245: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{75818EB5-D932-40B3-B0C6-6AACC396AFA1}, 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 HHTTP. We can see screenshot 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

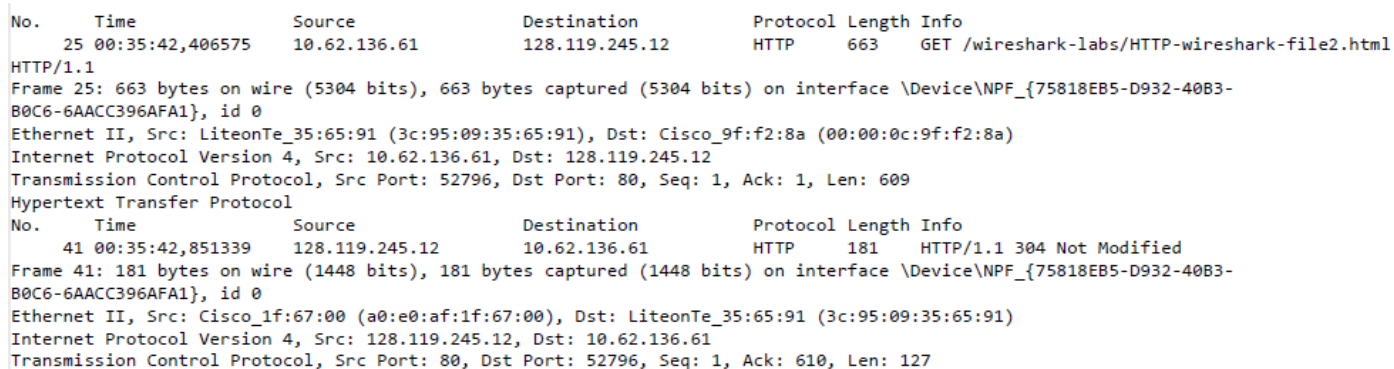
We implemented the steps and we reached these two situation.



The image shows a Wireshark capture of an HTTP interaction. The packet list pane shows two packets: a GET request (No. 25) and a 304 Not Modified response (No. 41). The packet details pane shows the structure of the selected packet (No. 41), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

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
41	00:35:42,851339	128.119.245.12	10.62.136.61	HTTP	181	HTTP/1.1 304 Not Modified

> 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



The image shows a Wireshark capture of an HTTP interaction. The packet list pane shows two packets: a GET request (No. 25) and a 304 Not Modified response (No. 41). The packet details pane shows the structure of the selected packet (No. 41), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

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
41	00:35:42,851339	128.119.245.12	10.62.136.61	HTTP	181	HTTP/1.1 304 Not Modified

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

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

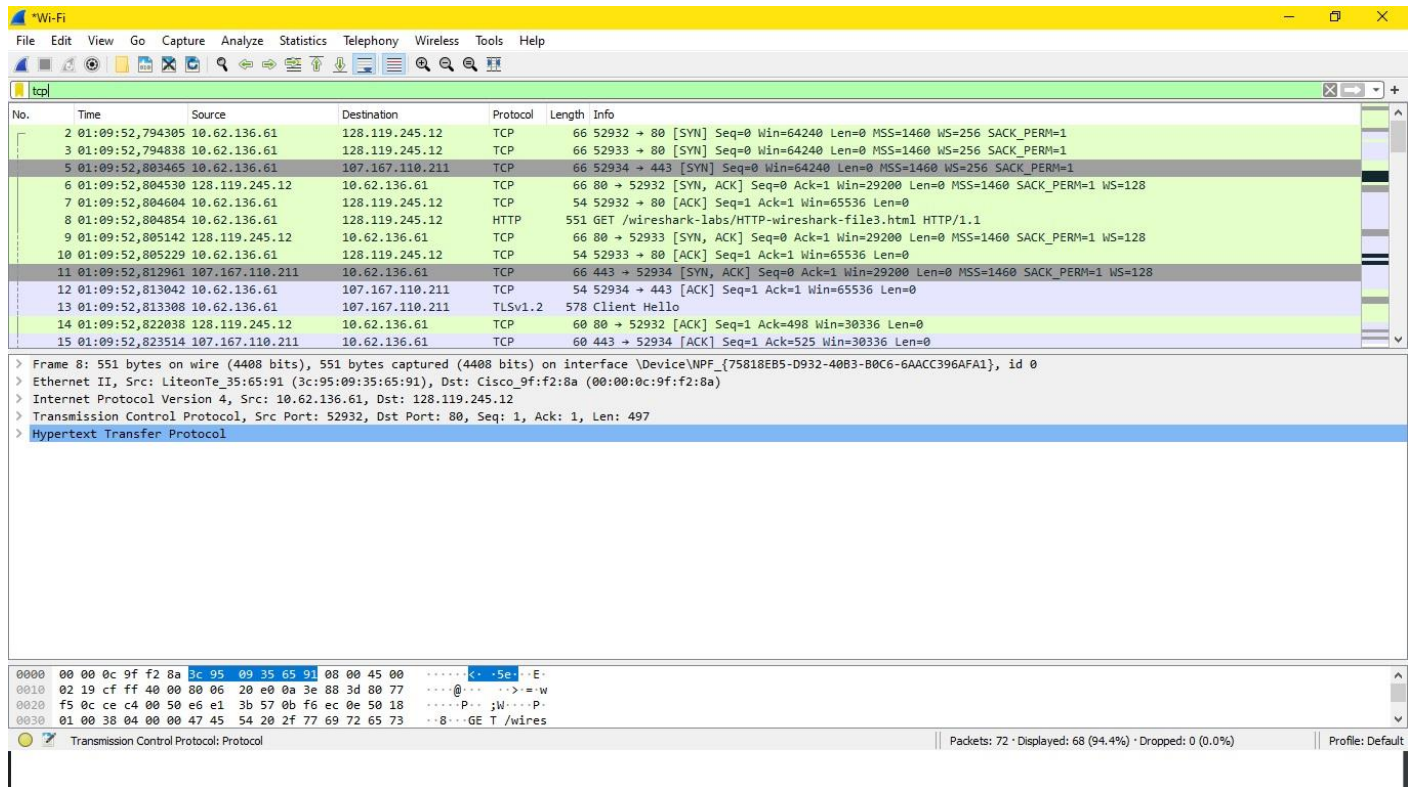
Answers of Questions

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.

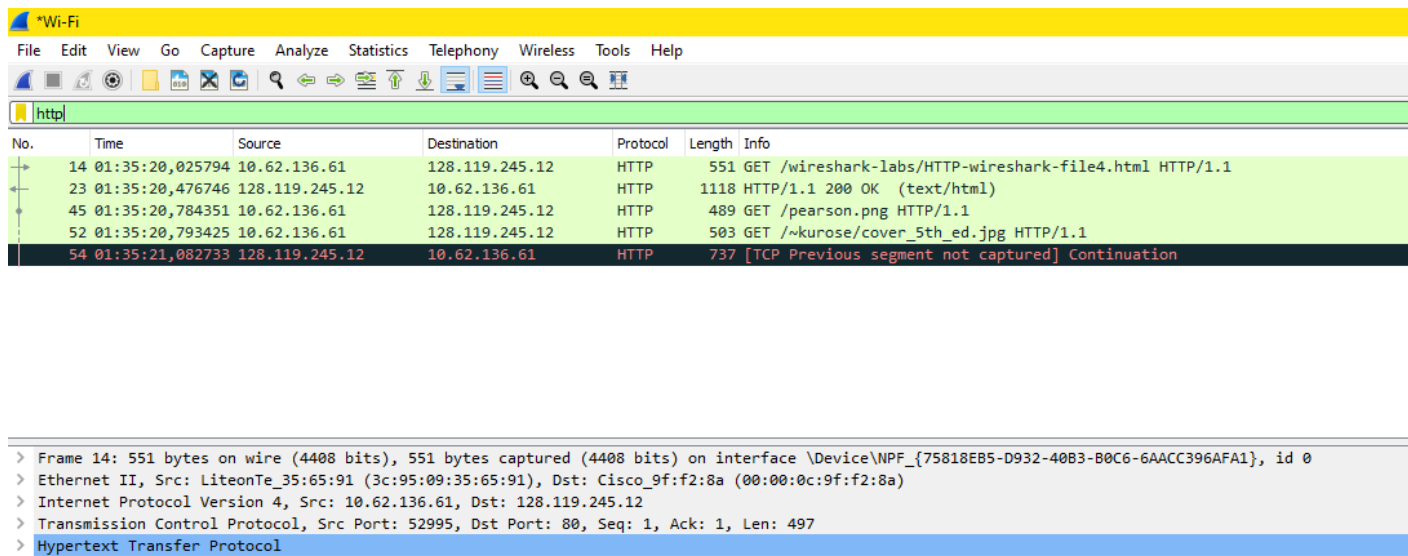
3. Retrieving Long Documents



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



The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first column is 'No.', the second is 'Time', the third is 'Source', the fourth is 'Destination', the fifth is 'Protocol', and the sixth is 'Length Info'. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length Info
14	01:35:20,025794	10.62.136.61	128.119.245.12	HTTP	551 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
23	01:35:20,476746	128.119.245.12	10.62.136.61	HTTP	1118 HTTP/1.1 200 OK (text/html)
45	01:35:20,784351	10.62.136.61	128.119.245.12	HTTP	489 GET /pearson.png HTTP/1.1
52	01:35:20,793425	10.62.136.61	128.119.245.12	HTTP	503 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
54	01:35:21,082733	128.119.245.12	10.62.136.61	HTTP	737 [TCP Previous segment not captured] Continuation

Below the packet list, the details pane shows the selected packet (No. 14) and its details:

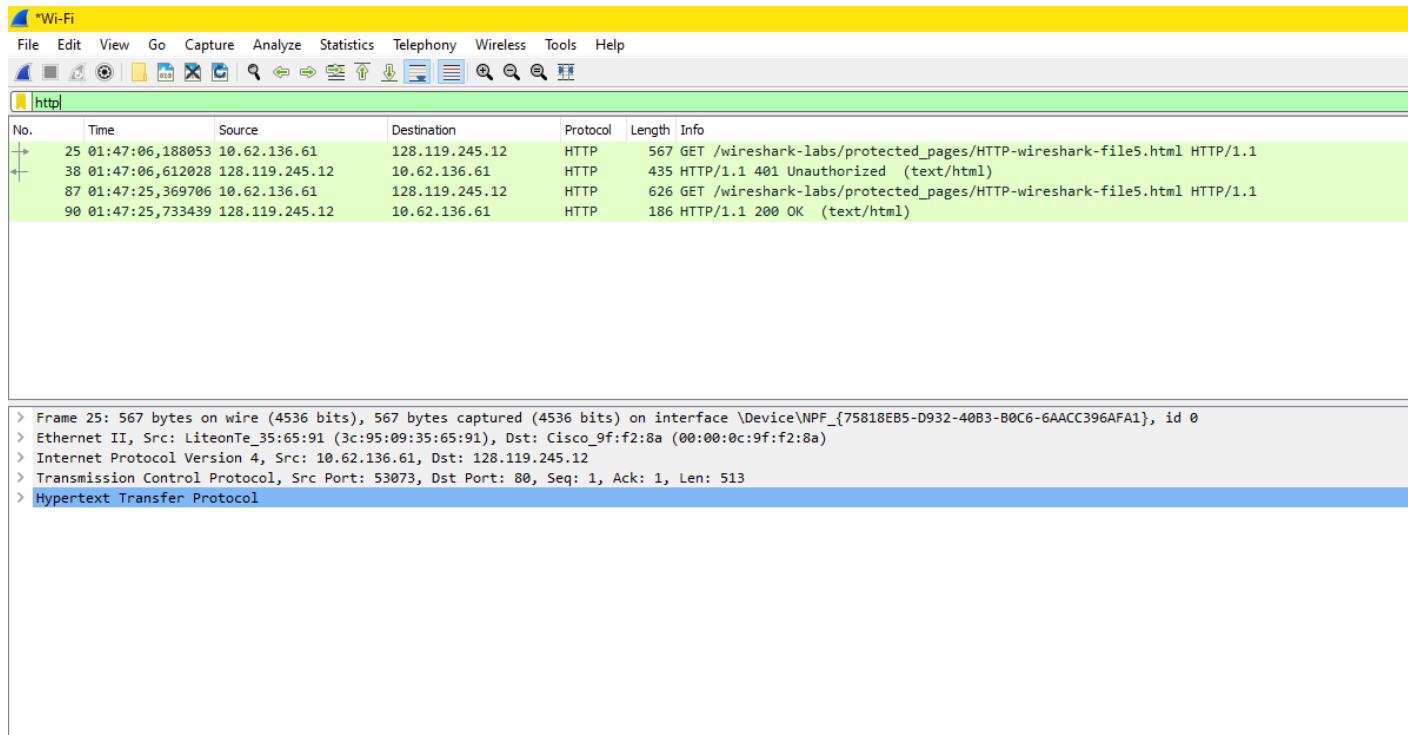
- > Frame 14: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{75818EB5-D932-40B3-B0C6-6AACC396AFA1}, id 0
- > Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Cisco_9f:f2:8a (00:00:0c:9f:f2:8a)
- > Internet Protocol Version 4, Src: 10.62.136.61, Dst: 128.119.245.12
- > Transmission Control Protocol, Src Port: 52995, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
- > Hypertext Transfer Protocol

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.

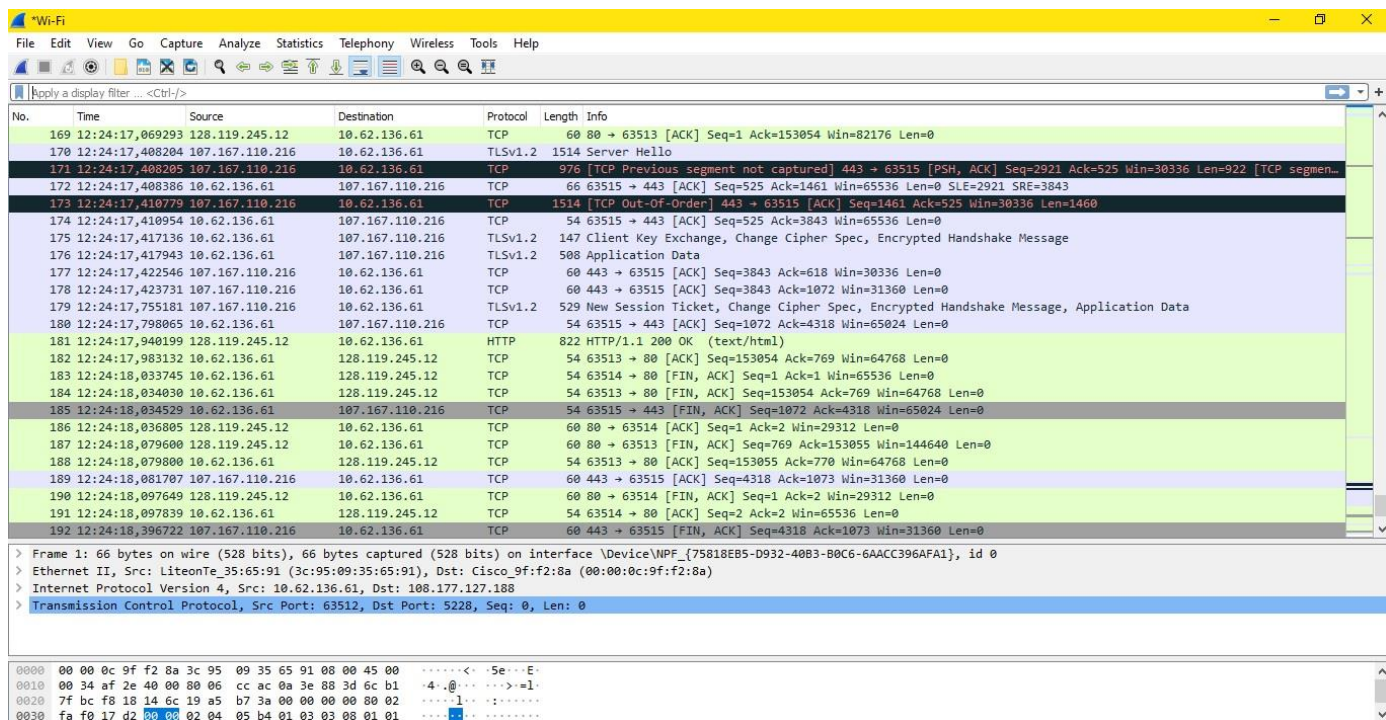
Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

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

> Options: (0 bytes) -> Window segment size -> No Sequence (NOP) -> No Sequence (NOP) -> SACK permitted

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]

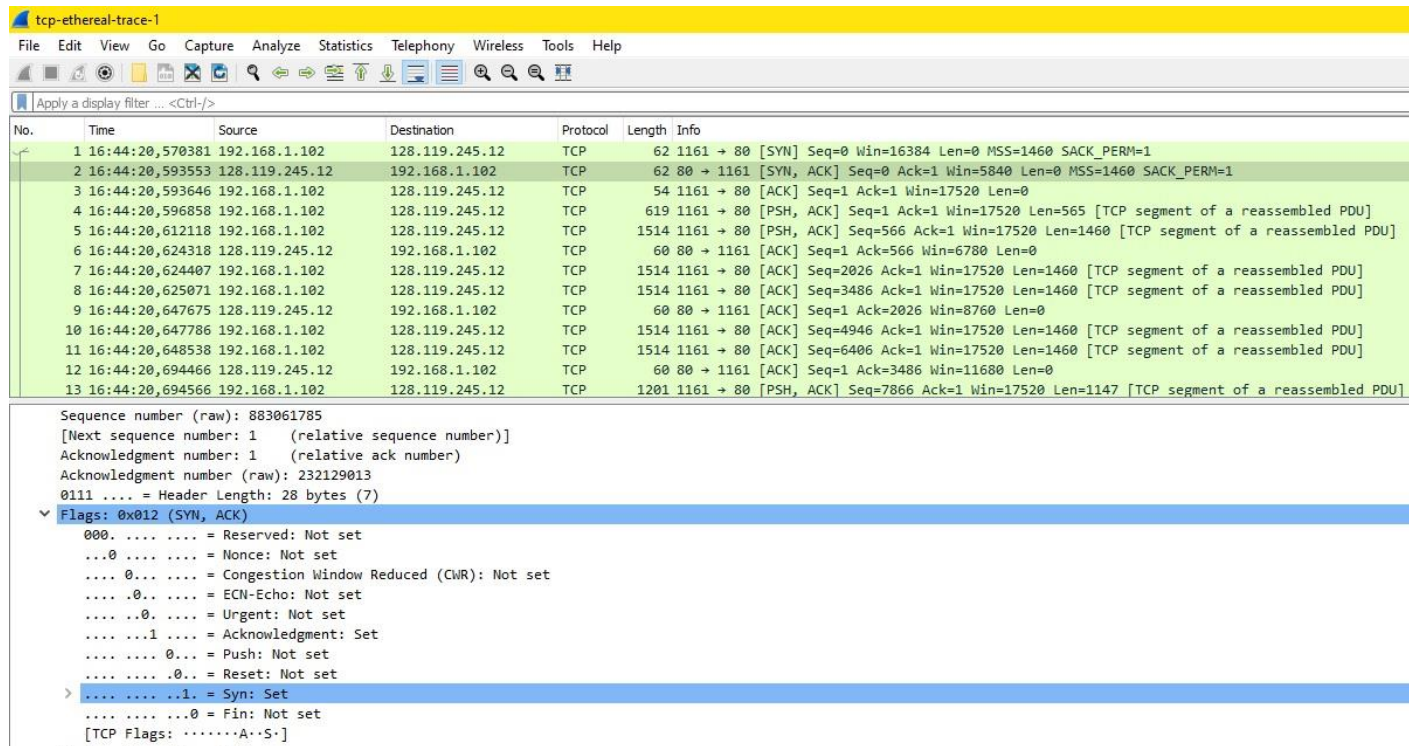
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{75818EB5-D932-40B3-B0C6-6AACC396AFA1}, id 0
> Ethernet II, Src: LiteonTe_35:65:91 (3c:95:09:35:65:91), Dst: Cisco_9f:f2:8a (00:00:0c:9f:f2:8a)
> Internet Protocol Version 4, Src: 10.62.136.61, Dst: 108.177.127.188
▼ 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
▼ 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.

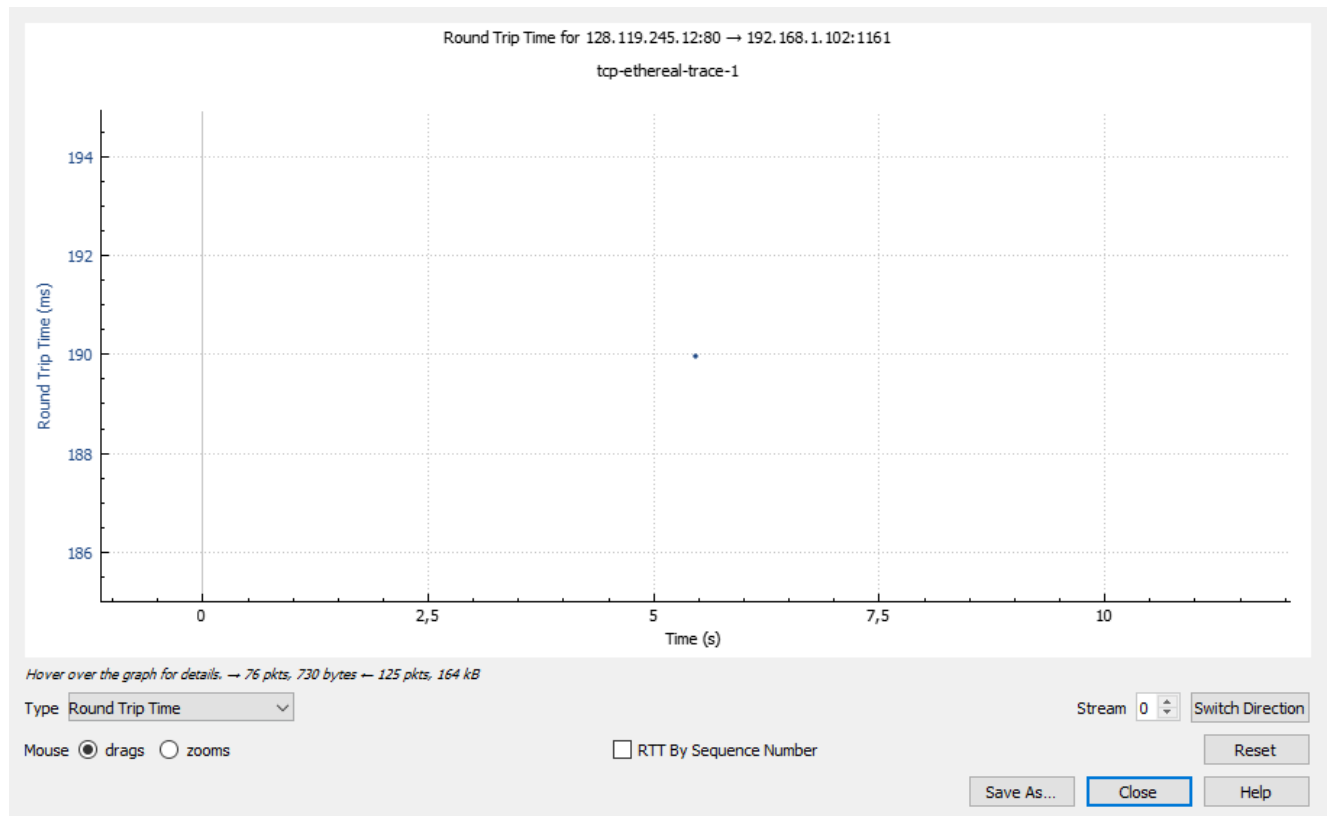


The image shows a Wireshark packet capture window titled 'tcp-ethereal-trace-1'. The packet list shows 13 packets. Packet 12 is selected, showing details for a TCP segment. The details pane shows the sequence number (raw) as 883061785, the next sequence number as 1 (relative), and the acknowledgment number as 1 (relative). The flags are 0x012 (SYN, ACK). The details pane also shows the sequence number (raw) as 232129013 and the header length as 28 bytes (7).

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]

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.]

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 r
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 c

> 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]

[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)

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...%...E.

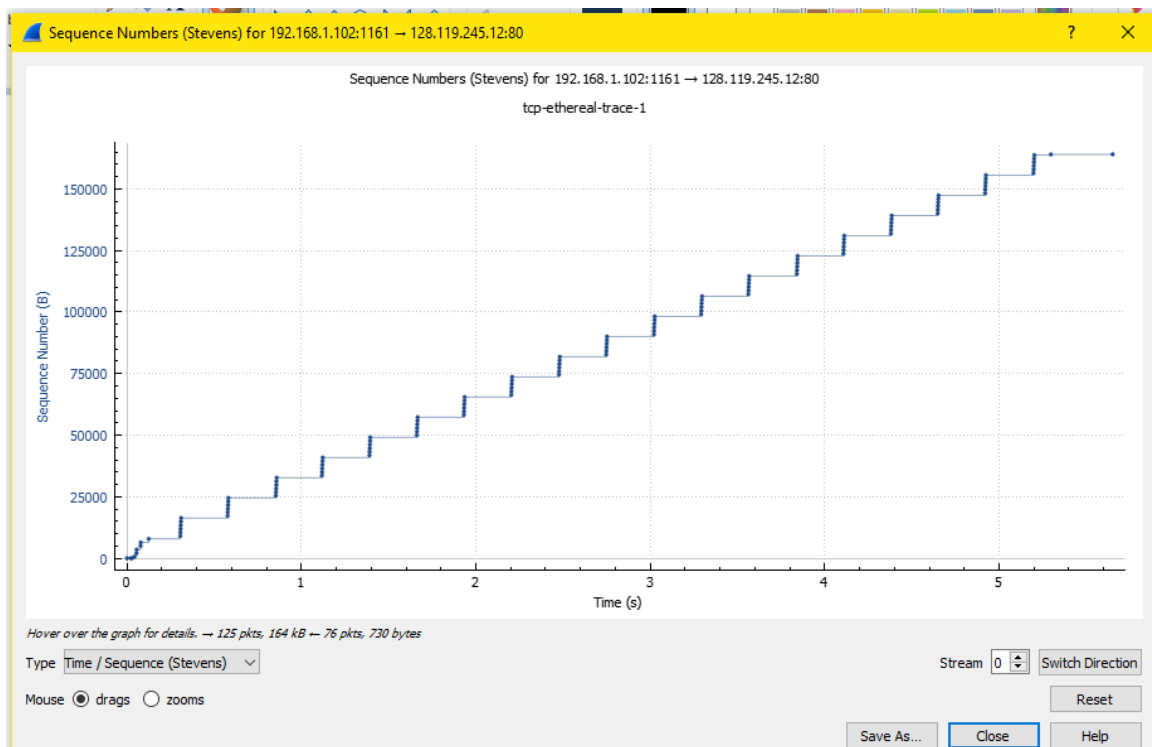
0010 03 02 58 bc 40 00 37 06 b0 a7 80 77 f5 0c c0 a8 ...X.@.7...w...

0020 01 66 00 50 04 89 34 a2 74 1a 0d d8 82 ef 50 18 ...f.P.44.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) ?

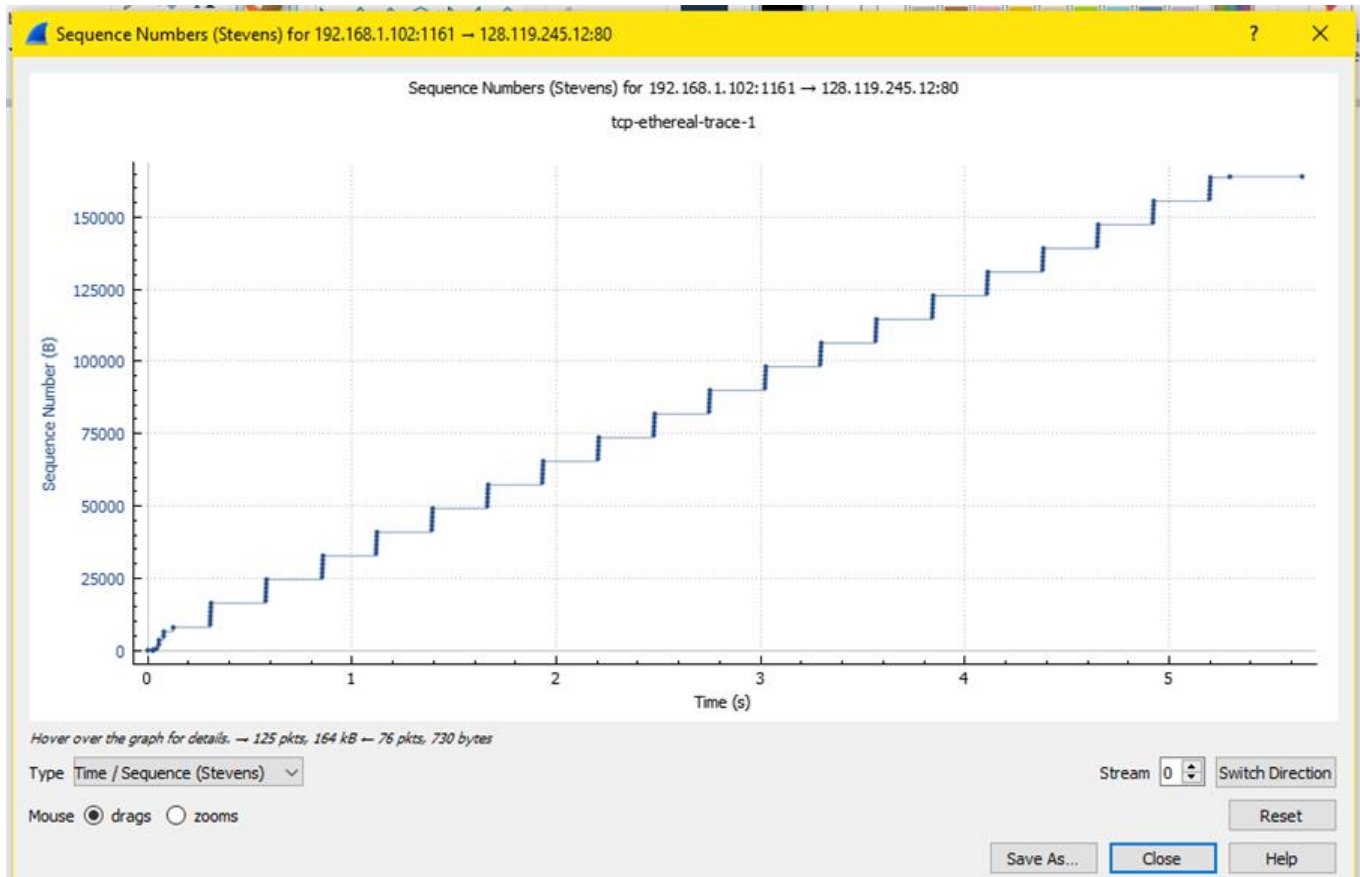
10) Time Sequence-Graph (Stevens)



11) ?

12)?

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



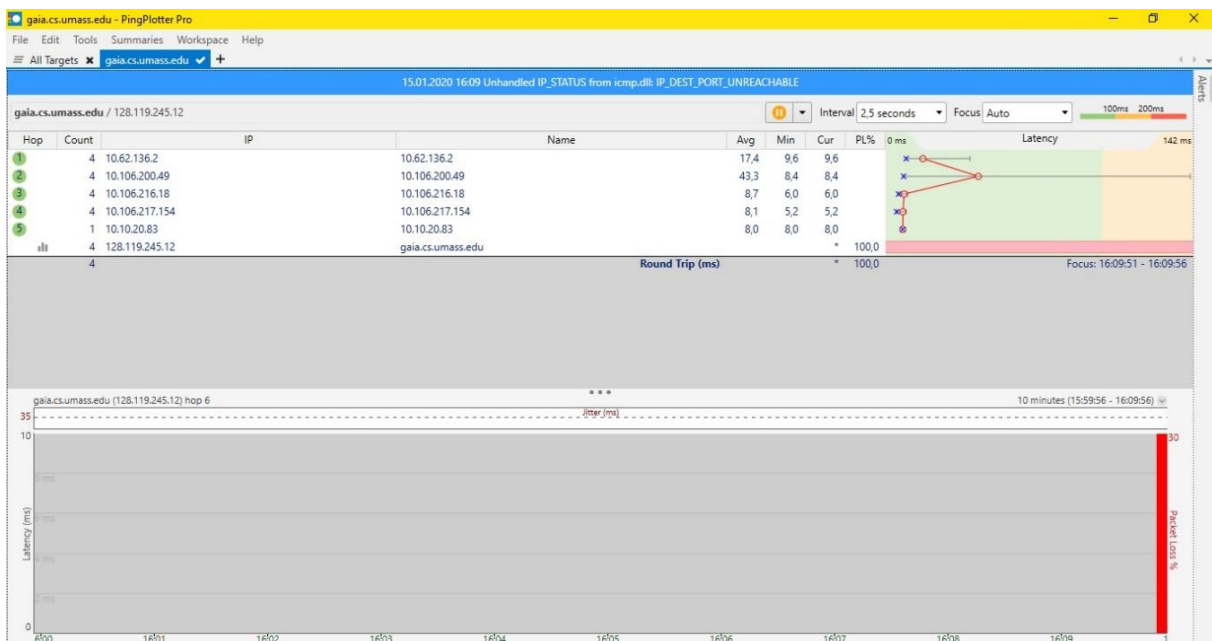
ASSIGNMENT IV

1. Capturing packets from an execution of traceroute

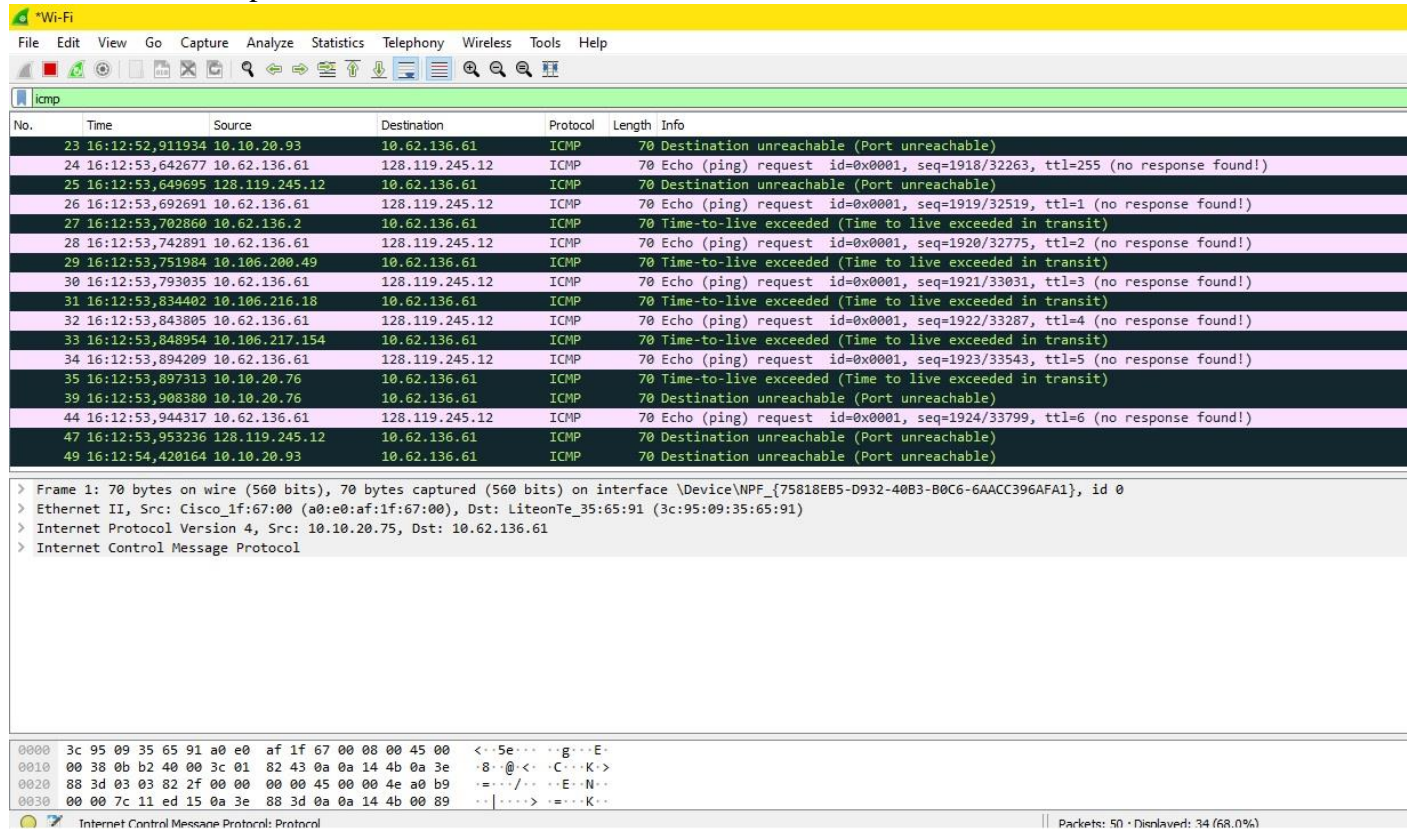
First step is downloaded the PingPlotter program.



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



We can see ICMP protocol list



The image shows a Wireshark capture of ICMP traffic. The top pane displays a list of 49 ICMP packets. The middle pane shows the details of the selected packet (No. 49), including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
23	16:12:52,911934	10.10.20.93	10.62.136.61	ICMP	70	Destination unreachable (Port unreachable)
24	16:12:53,642677	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1918/32263, ttl=255 (no response found!)
25	16:12:53,649695	128.119.245.12	10.62.136.61	ICMP	70	Destination unreachable (Port unreachable)
26	16:12:53,692691	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1919/32519, ttl=1 (no response found!)
27	16:12:53,702860	10.62.136.2	10.62.136.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	16:12:53,742891	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1920/32775, ttl=2 (no response found!)
29	16:12:53,751984	10.106.200.49	10.62.136.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	16:12:53,793035	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1921/33031, ttl=3 (no response found!)
31	16:12:53,834402	10.106.216.18	10.62.136.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	16:12:53,843805	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1922/33287, ttl=4 (no response found!)
33	16:12:53,848954	10.106.217.154	10.62.136.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	16:12:53,894209	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1923/33543, ttl=5 (no response found!)
35	16:12:53,897313	10.10.20.76	10.62.136.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
39	16:12:53,908380	10.10.20.76	10.62.136.61	ICMP	70	Destination unreachable (Port unreachable)
44	16:12:53,944317	10.62.136.61	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=1924/33799, ttl=6 (no response found!)
47	16:12:53,953236	128.119.245.12	10.62.136.61	ICMP	70	Destination unreachable (Port unreachable)
49	16:12:54,420164	10.10.20.93	10.62.136.61	ICMP	70	Destination unreachable (Port unreachable)

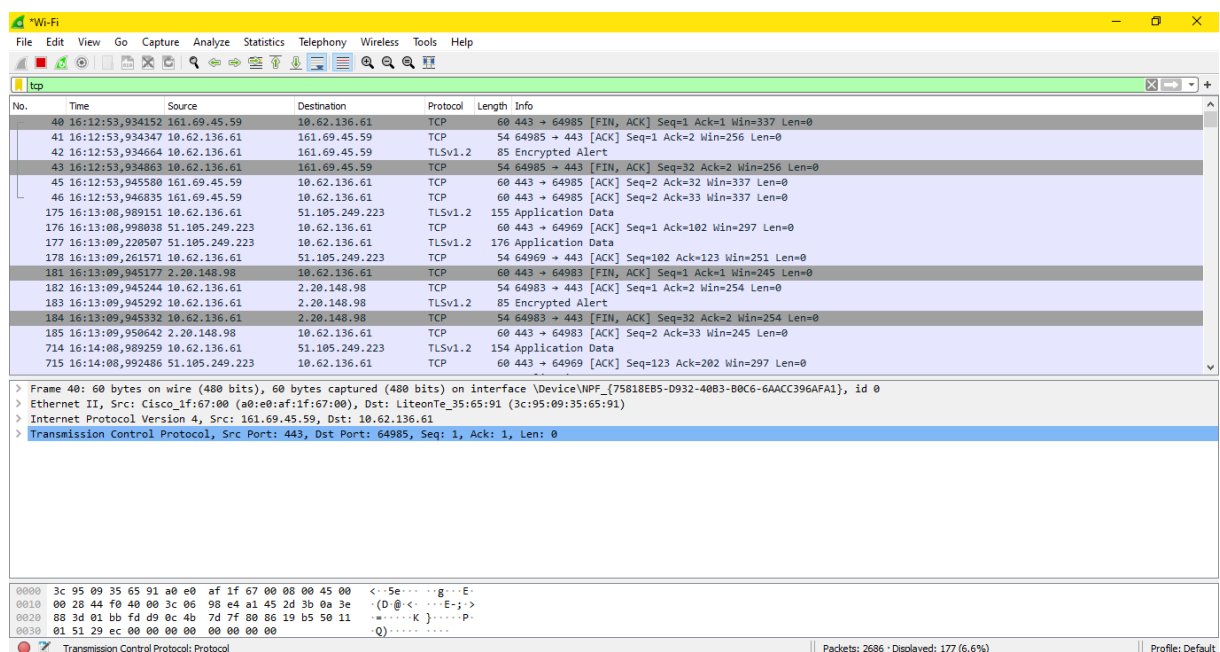
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{75818EB5-D932-40B3-B0C6-6AACC396AFA1}, id 0
> Ethernet II, Src: Cisco_1f:67:00 (a0:e0:af:1f:67:00), Dst: LiteonTe_35:65:91 (3c:95:09:35:65:91)
> Internet Protocol Version 4, Src: 10.10.20.75, Dst: 10.62.136.61
> Internet Control Message Protocol

0000 3c 95 09 35 65 91 a0 e0 af 1f 67 00 08 00 45 00 <...5e... ..g...E-
0010 00 38 0b b2 40 00 3c 01 82 43 0a 0a 14 4b 0a 3e .8..@.<...C...K>
0020 88 3d 03 03 82 2f 00 00 00 00 45 00 00 4e a0 b9 .-.../-...E..N..
0030 00 00 7c 11 ed 15 0a 3e 88 3d 0a 0a 14 4b 00 89 ..|....>...=...K..

Internet Control Message Protocol: Protocol

Packets: 50 · Displayed: 34 (68.0%)

Also, we captured and listed the TCP protocols.



The image shows a Wireshark capture of TCP traffic. The top pane displays a list of 21 TCP packets. The middle pane shows the details of the selected packet (No. 40), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
40	16:12:53,934152	161.69.45.59	10.62.136.61	TCP	60	443 → 64985 [FIN, ACK] Seq=1 Ack=1 Win=337 Len=0
41	16:12:53,934347	10.62.136.61	161.69.45.59	TCP	54	64985 → 443 [ACK] Seq=1 Ack=2 Win=256 Len=0
42	16:12:53,934664	10.62.136.61	161.69.45.59	TLSv1.2	85	Encrypted Alert
43	16:12:53,934863	10.62.136.61	161.69.45.59	TCP	54	64985 → 443 [FIN, ACK] Seq=32 Ack=2 Win=256 Len=0
45	16:12:53,945500	161.69.45.59	10.62.136.61	TCP	60	443 → 64985 [ACK] Seq=2 Ack=32 Win=337 Len=0
46	16:12:53,946835	161.69.45.59	10.62.136.61	TCP	60	443 → 64985 [ACK] Seq=2 Ack=33 Win=337 Len=0
176	16:13:00,989151	10.62.136.61	51.105.249.223	TLSv1.2	155	Application Data
176	16:13:00,990038	51.105.249.223	10.62.136.61	TCP	60	443 → 64969 [ACK] Seq=1 Ack=102 Win=297 Len=0
177	16:13:00,220507	51.105.249.223	10.62.136.61	TLSv1.2	176	Application Data
178	16:13:00,261571	10.62.136.61	51.105.249.223	TCP	54	64969 → 443 [ACK] Seq=102 Ack=123 Win=251 Len=0
181	16:13:00,945177	2.20.148.98	10.62.136.61	TCP	60	443 → 64983 [FIN, ACK] Seq=1 Ack=1 Win=245 Len=0
182	16:13:00,945244	10.62.136.61	2.20.148.98	TCP	54	64983 → 443 [ACK] Seq=1 Ack=2 Win=254 Len=0
183	16:13:00,945292	10.62.136.61	2.20.148.98	TLSv1.2	85	Encrypted Alert
184	16:13:00,945332	10.62.136.61	2.20.148.98	TCP	54	64983 → 443 [FIN, ACK] Seq=32 Ack=2 Win=254 Len=0
185	16:13:00,950642	2.20.148.98	10.62.136.61	TCP	60	443 → 64983 [ACK] Seq=2 Ack=33 Win=245 Len=0
714	16:14:00,989259	10.62.136.61	51.105.249.223	TLSv1.2	154	Application Data
715	16:14:00,992486	51.105.249.223	10.62.136.61	TCP	60	443 → 64969 [ACK] Seq=123 Ack=202 Win=297 Len=0

> Frame 40: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 161.69.45.59, Dst: 10.62.136.61
> Transmission Control Protocol, Src Port: 443, Dst Port: 64985, Seq: 1, Ack: 1, Len: 0

0000 3c 95 09 35 65 91 a0 e0 af 1f 67 00 08 00 45 00 <...5e... ..g...E-
0010 00 28 44 f0 40 00 3c 06 98 e4 a1 45 2d 3b 0a 3e .(D.@.<...E-;>
0020 88 3d 01 bb fd 09 0c 4b 7d 7f 00 06 19 b5 50 11 .-...K }.....P-
0030 01 51 29 cc 00 00 00 00 00 00 00 00 00 00 00 00 Q).....

Transmission Control Protocol: Protocol

Packets: 2686 · Displayed: 177 (6.6%)

Profile: Default

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 length 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
▼ 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.