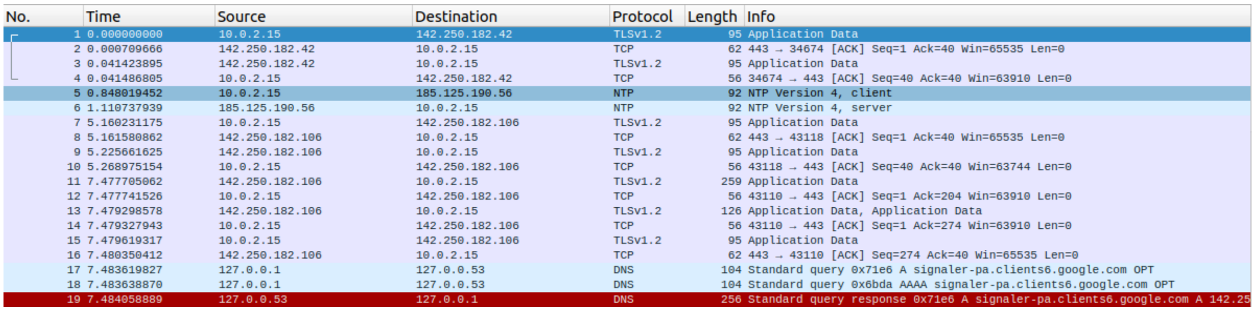
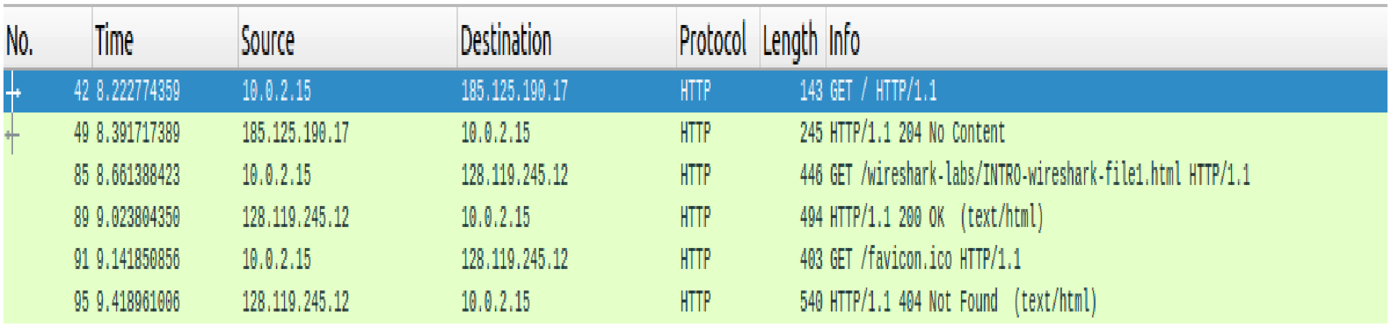
1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP,TLSv1.2, etc?

Ans: I got all of them TCP, QUIC, HTTP, DNS, UDP, TLSv1.2 And other than this i got OCSP



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	142.250.182.42	TLSv1.2	95	Application Data
2	0.000709666	142.250.182.42	10.0.2.15	TCP	62	443 → 34674 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.041423895	142.250.182.42	10.0.2.15	TLSv1.2	95	Application Data
4	0.041486805	10.0.2.15	142.250.182.42	TCP	56	34674 → 443 [ACK] Seq=40 Ack=40 Win=63910 Len=0
5	0.848019452	10.0.2.15	185.125.190.56	NTP	92	NTP Version 4, client
6	1.110737939	185.125.190.56	10.0.2.15	NTP	92	NTP Version 4, server
7	5.160231175	10.0.2.15	142.250.182.106	TLSv1.2	95	Application Data
8	5.161580862	142.250.182.106	10.0.2.15	TCP	62	443 → 43118 [ACK] Seq=1 Ack=40 Win=65535 Len=0
9	5.225661625	142.250.182.106	10.0.2.15	TLSv1.2	95	Application Data
10	5.268975154	10.0.2.15	142.250.182.106	TCP	56	43118 → 443 [ACK] Seq=40 Ack=40 Win=63744 Len=0
11	7.477705062	142.250.182.106	10.0.2.15	TLSv1.2	259	Application Data
12	7.477741526	10.0.2.15	142.250.182.106	TCP	56	43110 → 443 [ACK] Seq=1 Ack=204 Win=63910 Len=0
13	7.479298578	142.250.182.106	10.0.2.15	TLSv1.2	126	Application Data, Application Data
14	7.479327943	10.0.2.15	142.250.182.106	TCP	56	43110 → 443 [ACK] Seq=1 Ack=274 Win=63910 Len=0
15	7.479619317	10.0.2.15	142.250.182.106	TLSv1.2	95	Application Data
16	7.480350412	142.250.182.106	10.0.2.15	TCP	62	443 → 43110 [ACK] Seq=274 Ack=40 Win=65535 Len=0
17	7.483619827	127.0.0.1	127.0.0.53	DNS	104	Standard query 0x71e6 A signaler-pa.clients6.google.com OPT
18	7.483638870	127.0.0.1	127.0.0.53	DNS	104	Standard query 0x6bda AAAA signaler-pa.clients6.google.com OPT
19	7.484058889	127.0.0.53	127.0.0.1	DNS	256	Standard query response 0x71e6 A signaler-pa.clients6.google.com A 142.25

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. (If you want to display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



No.	Time	Source	Destination	Protocol	Length	Info
42	8.222774359	10.0.2.15	185.125.190.17	HTTP	143	GET / HTTP/1.1
49	8.391717389	185.125.190.17	10.0.2.15	HTTP	245	HTTP/1.1 204 No Content
85	8.661388423	10.0.2.15	128.119.245.12	HTTP	446	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
89	9.023804350	128.119.245.12	10.0.2.15	HTTP	494	HTTP/1.1 200 OK (text/html)
91	9.141850856	10.0.2.15	128.119.245.12	HTTP	403	GET /favicon.ico HTTP/1.1
95	9.418961006	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 404 Not Found (text/html)

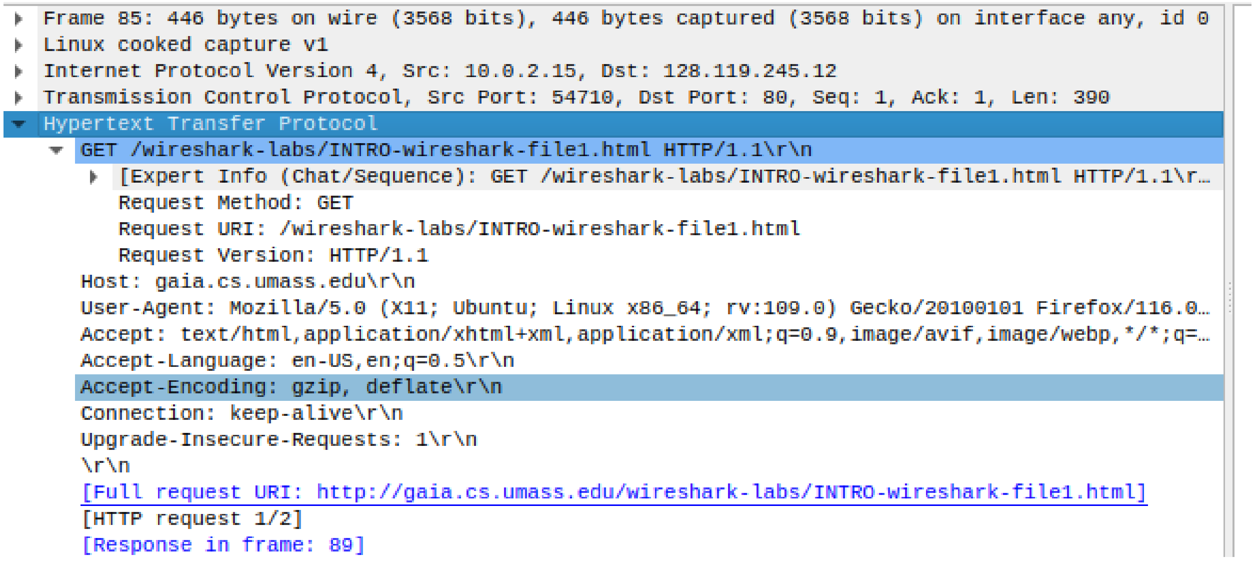
Ans: Time taken = 9.0238-8.6613 = 0.5767

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET Message?

Ans:
address of the gaia.cs.umass.edu 128.119.245.12
Source address is the 10.0.2.15

4. Expand the information on the HTTP message in the Wireshark “Details of selected packet” window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the “User-Agent:” field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are using.]

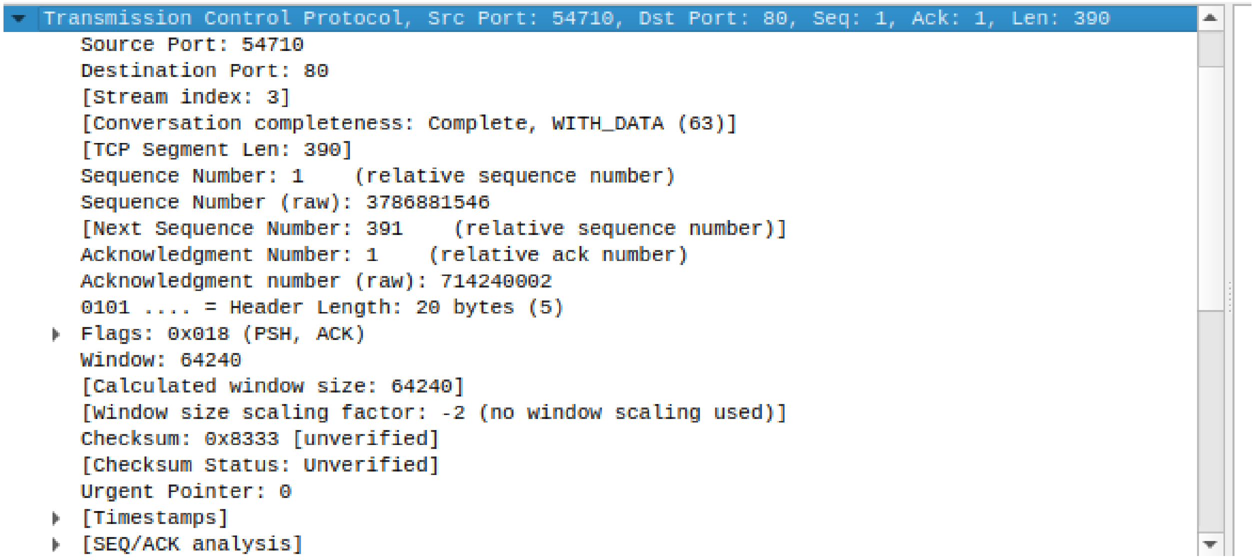
● Firefox, Safari, Microsoft Internet Edge, Other



```
Frame 85: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54710, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
Hypertext Transfer Protocol
   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r…
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0…
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=…
   Accept-Language: en-US,en;q=0.5\r\n
   Accept-Encoding: gzip, deflate\r\n
   Connection: keep-alive\r\n
   Upgrade-Insecure-Requests: 1\r\n
   \r\n
   [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
   [HTTP request 1/2]
   [Response in frame: 89]
```

Here user agent is Mozilla

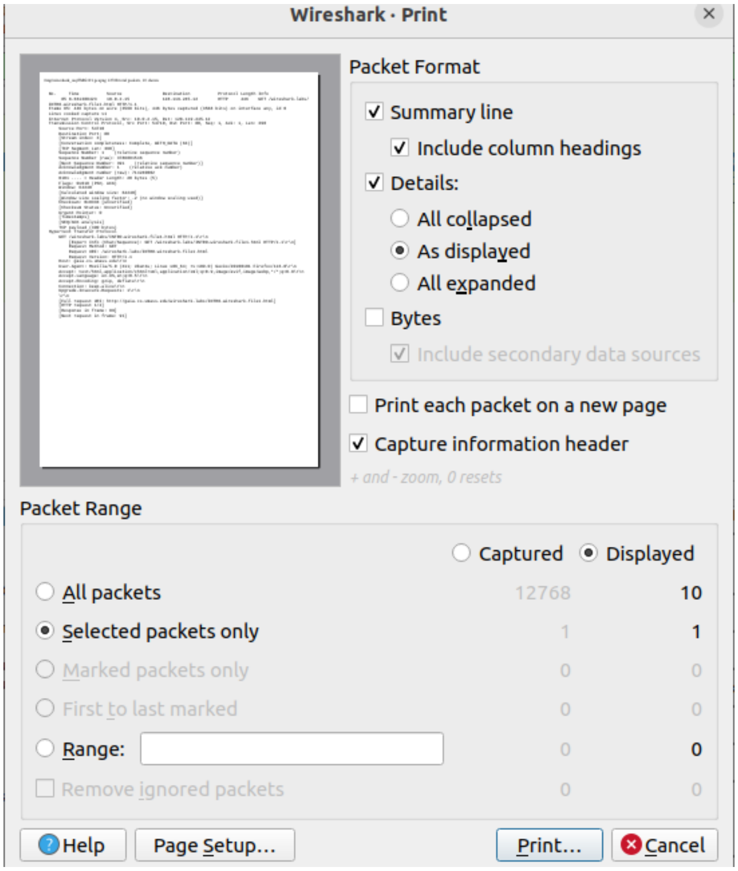
5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark “Details of selected packet” window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following “Dest Port:” for the TCP segment containing the HTTP request) to which this HTTP request is being sent?



```
▼ Transmission Control Protocol, Src Port: 54710, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
      Source Port: 54710
      Destination Port: 80
      [Stream index: 3]
      [Conversation completeness: Complete, WITH_DATA (63)]
      [TCP Segment Len: 390]
      Sequence Number: 1    (relative sequence number)
      Sequence Number (raw): 3786881546
      [Next Sequence Number: 391    (relative sequence number)]
      Acknowledgment Number: 1    (relative ack number)
      Acknowledgment number (raw): 714240002
      0101 .... = Header Length: 20 bytes (5)
   ▸ Flags: 0x018 (PSH, ACK)
      Window: 64240
      [Calculated window size: 64240]
      [Window size scaling factor: -2 (no window scaling used)]
      Checksum: 0x8333 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
   ▸ [Timestamps]
   ▸ [SEQ/ACK analysis]
```

Here Destination port is 80

6. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons,



Wireshark · Print

Packet Format

☑ Summary line
☑ Include column headings
☑ Details:
○ All collapsed
● As displayed
○ All expanded
□ Bytes
☑ Include secondary data sources
□ Print each packet on a new page
☑ Capture information header

+ and - zoom, 0 resets

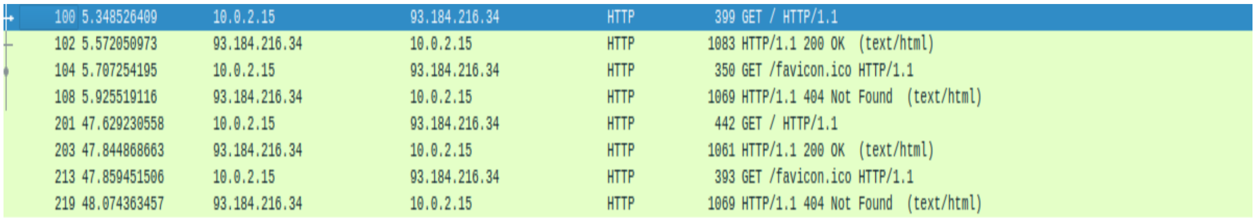
Packet Range

	○ Captured	● Displayed
○ All packets	12768	10
● Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove ignored packets	0	0

and then click OK.

7. Answer Q1-Q3 again by visiting the following links from your web browser. Save each visit as a separate pcap file.

o example.com/

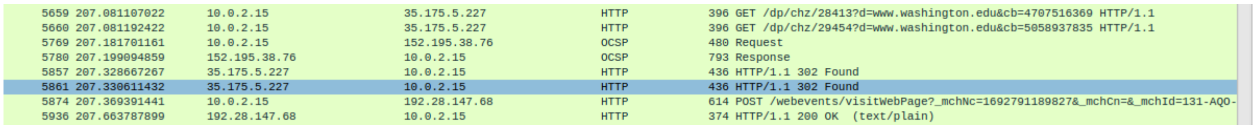


```
100 5.348526409    10.0.2.15        93.184.216.34    HTTP     399 GET / HTTP/1.1
102 5.572050973    93.184.216.34    10.0.2.15        HTTP    1083 HTTP/1.1 200 OK  (text/html)
104 5.707254195    10.0.2.15        93.184.216.34    HTTP     350 GET /favicon.ico HTTP/1.1
108 5.925519116    93.184.216.34    10.0.2.15        HTTP    1069 HTTP/1.1 404 Not Found  (text/html)
201 47.629230558   10.0.2.15        93.184.216.34    HTTP     442 GET / HTTP/1.1
203 47.844868663   93.184.216.34    10.0.2.15        HTTP    1061 HTTP/1.1 200 OK  (text/html)
213 47.859451506   10.0.2.15        93.184.216.34    HTTP     393 GET /favicon.ico HTTP/1.1
219 48.074363457   93.184.216.34    10.0.2.15        HTTP    1069 HTTP/1.1 404 Not Found  (text/html)
```

Time taken is 0.273 sec

www.washington.edu/

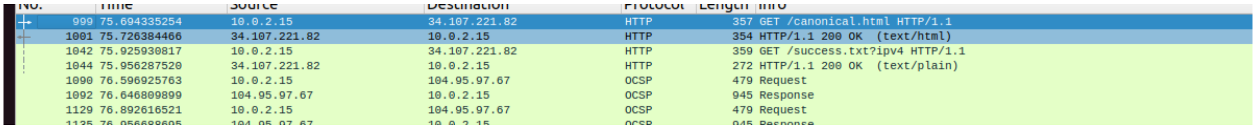
Time taken 0.8 sec



```
5659 207.081107022   10.0.2.15        35.175.5.227     HTTP    396 GET /dp/chz/28413?d=www.washington.edu&cb=4707516369 HTTP/1.1
5660 207.081192422   10.0.2.15        35.175.5.227     HTTP    396 GET /dp/chz/29454?d=www.washington.edu&cb=5058937835 HTTP/1.1
5769 207.181701161   10.0.2.15        152.195.38.76    OCSP    480 Request
5780 207.199094859   152.195.38.76    10.0.2.15        OCSP    793 Response
5857 207.328667267   35.175.5.227     10.0.2.15        HTTP    436 HTTP/1.1 302 Found
5861 207.330611432   35.175.5.227     10.0.2.15        HTTP    436 HTTP/1.1 302 Found
5874 207.369391441   10.0.2.15        192.28.147.68    HTTP    614 POST /webevents/visitWebPage?_mchNc=1692791189827&_mchCn=&_mchId=131-AQO-
5936 207.663787899   192.28.147.68    10.0.2.15        HTTP    374 HTTP/1.1 200 OK  (text/plain)
```

www.iith.ac.in

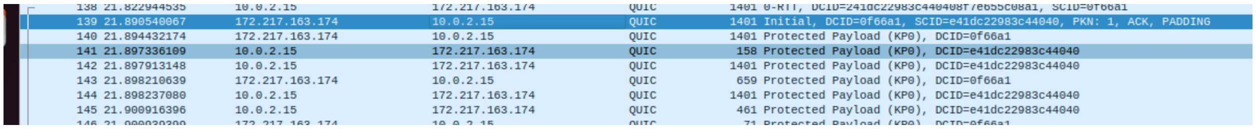
Time taken is 0.03 sec



```
No.  Time           Source           Destination      Protocol Length Info
 999 75.694335254   10.0.2.15        34.107.221.82    HTTP     357 GET /canonical.html HTTP/1.1
1001 75.726384466   34.107.221.82    10.0.2.15        HTTP     354 HTTP/1.1 200 OK  (text/html)
1042 75.925930817   10.0.2.15        34.107.221.82    HTTP     359 GET /success.txt?ipv4 HTTP/1.1
1044 75.956287520   34.107.221.82    10.0.2.15        HTTP     272 HTTP/1.1 200 OK  (text/plain)
1090 76.596925763   10.0.2.15        104.95.97.67     OCSP     479 Request
1092 76.646809899   104.95.97.67     10.0.2.15        OCSP     945 Response
1129 76.892616521   10.0.2.15        104.95.97.67     OCSP     479 Request
1135 76.956688605   104.95.97.67     10.0.2.15        OCSP     945 Response
```

o www.youtube.com

Because youtube work on quic protocol



```
138 21.822944535   10.0.2.15         172.217.163.174   QUIC   1401 0-RTT, DCID=241dc22983c440408f7e655c08a1, SCID=0f66a1
139 21.890540067   172.217.163.174   10.0.2.15         QUIC   1401 Initial, DCID=0f66a1, SCID=e41dc22983c44040, PKN: 1, ACK, PADDING
140 21.894432174   172.217.163.174   10.0.2.15         QUIC   1401 Protected Payload (KP0), DCID=0f66a1
141 21.897336109   10.0.2.15         172.217.163.174   QUIC    158 Protected Payload (KP0), DCID=e41dc22983c44040
142 21.897913148   10.0.2.15         172.217.163.174   QUIC   1401 Protected Payload (KP0), DCID=e41dc22983c44040
143 21.898210639   172.217.163.174   10.0.2.15         QUIC    659 Protected Payload (KP0), DCID=0f66a1
144 21.898237080   10.0.2.15         172.217.163.174   QUIC   1401 Protected Payload (KP0), DCID=e41dc22983c44040
145 21.900916396   10.0.2.15         172.217.163.174   QUIC    461 Protected Payload (KP0), DCID=e41dc22983c44040
146 21.900930390   172.217.163.174   10.0.2.15         QUIC     71 Protected Payload (KP0), DCID=0f66a1
```

8. Compare and contrast what you observed in Wireshark and in your browser when you visited the above four websites.

I can understand how many packets are coming and going for single webpage and web browser are very abstract for user.