CSL317 Computer Networks Assignment – WireShark

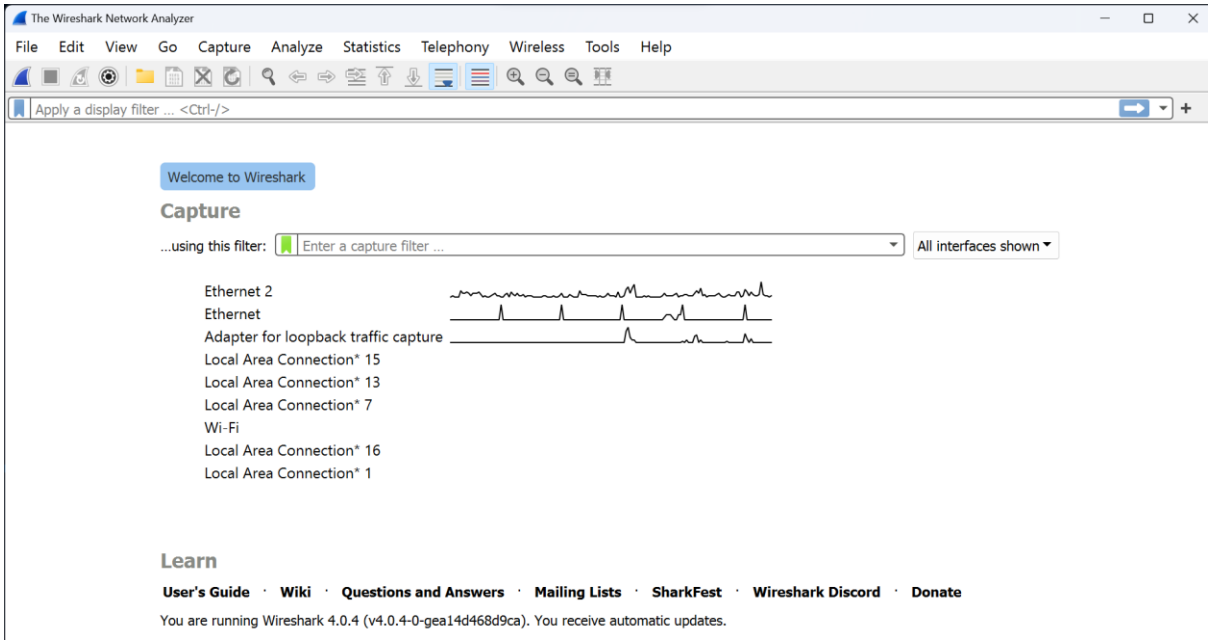
Name: Dweeja Reddy Devi

Enrollment Number: BT20CSE032

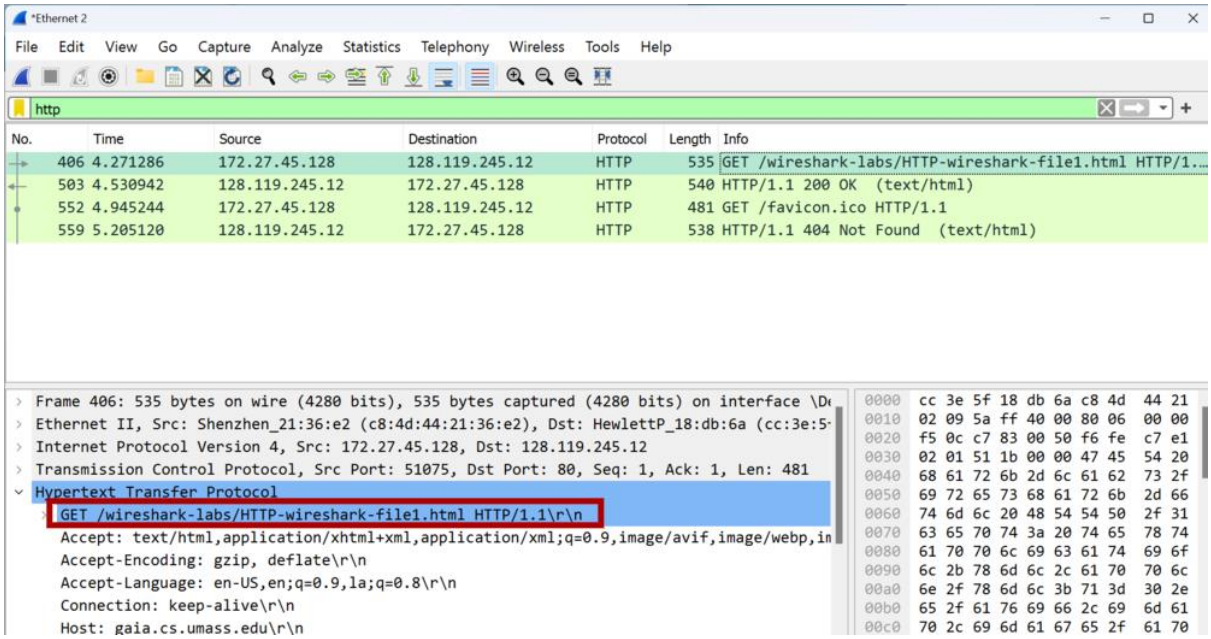
HTTP Assignment

Begin Wireshark packet capture and enter the following to your browser "http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html" Your browser should display the very simple, one-line HTML file. Now Stop Wireshark packet capture. By looking at the information in the HTTP GET and response messages, answer the following questions:

Wireshark Interface showing the networks available (both wired and wireless):

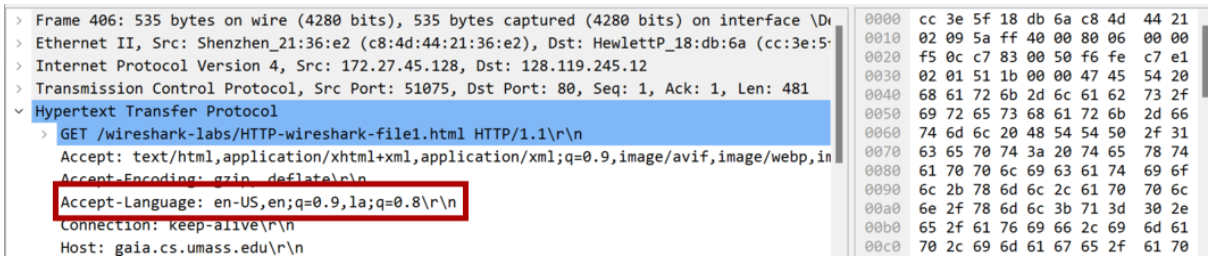


1. Is your browser running HTTP version 1.0 or 1.1?
   My browser is running the HTTP version **1.1** which can be seen from the GET message of HTTP protocol



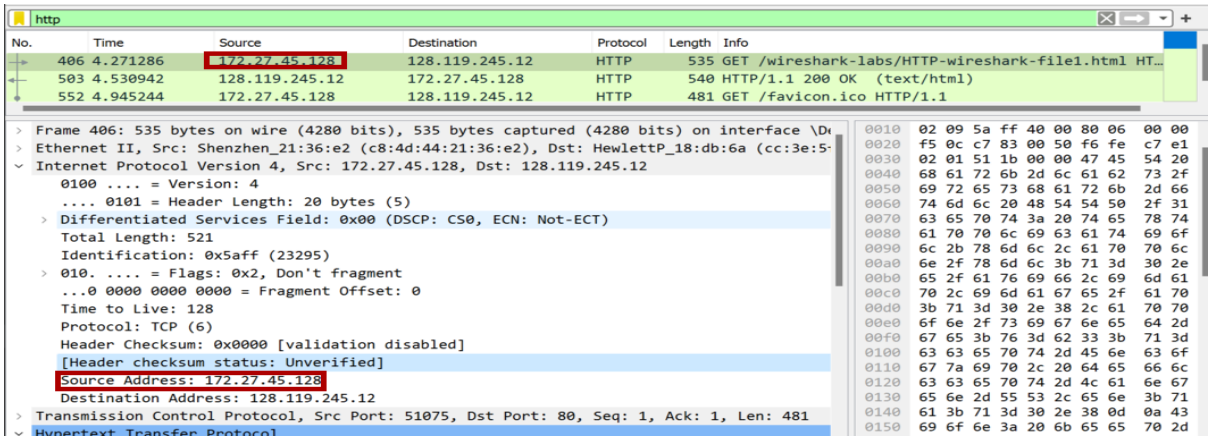
2.What languages (if any) does your browser indicate that it can accept to the server?

Accept-Languages are: **en-US, en, q=0.9,la;q=0.8**



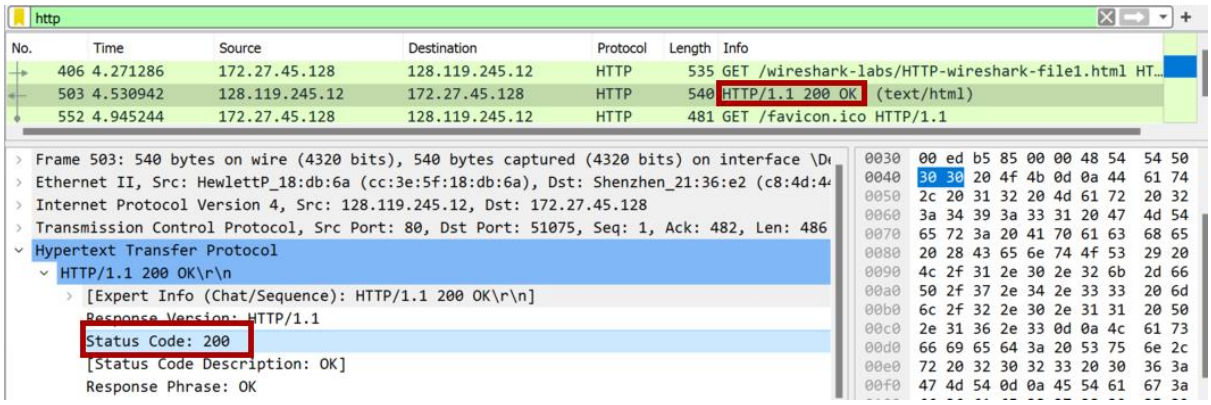
3.What is the IP address of your computer?

My Computer IP address: **172.27.45.128**



4. What is the status code returned from the server to your browser?

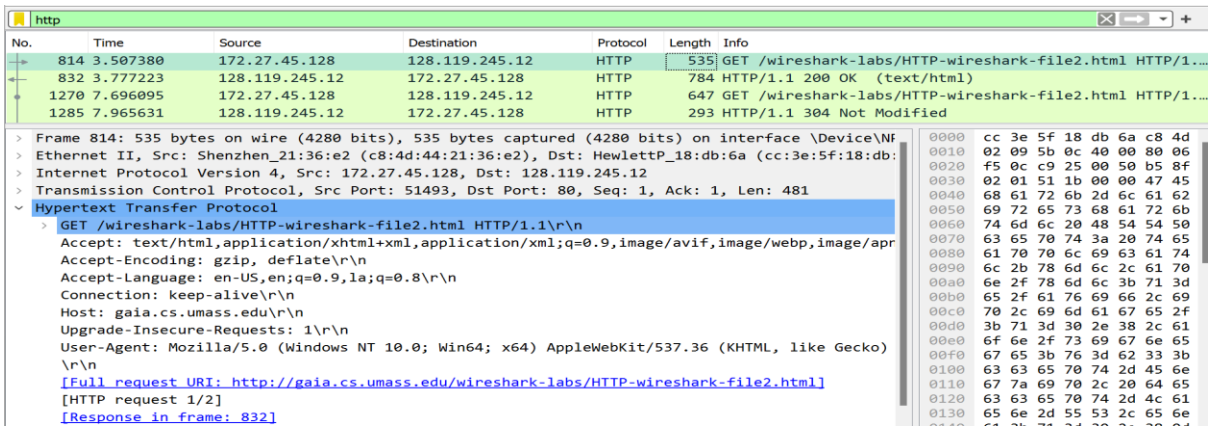
The status code returned is **200 OK** indicates that request has been succeeded i.e resource is fetched and is transmitted in the message body.



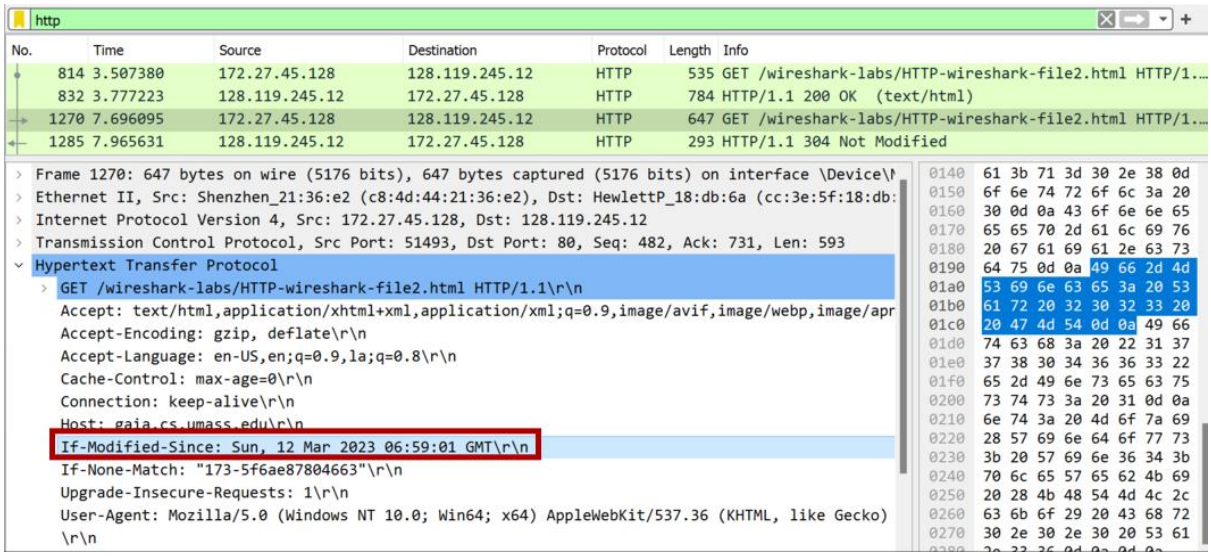
Start up the Wireshark packet sniffer. Enter the following URL into your browser(make sure your browser's cache is empty) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html . Your browser should display a very simple five-line HTML file.Quickly enter the same URL into your browser again (or simply select the refresh button on your browser).Stop Wireshark packet capture.

5. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

There is **no if-modified-since** line in the first HTTP GET request because the file was requested on the browser for the first time not yet modified

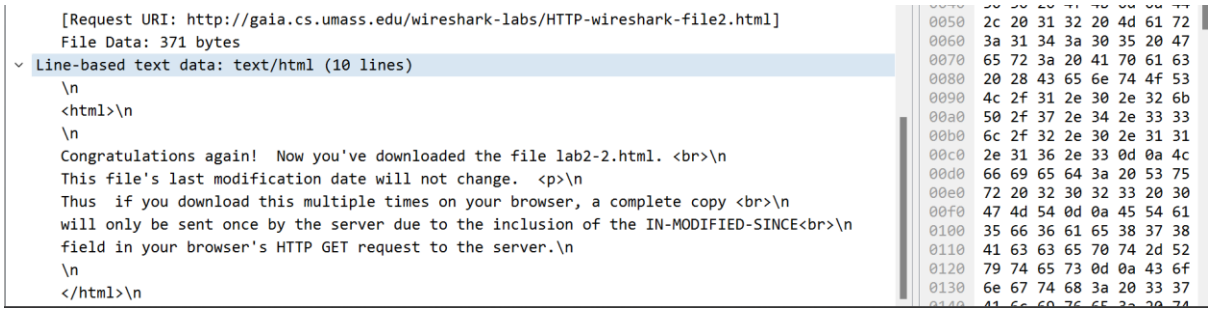


After refreshing, there will be a if-modified-since line because chrome will ping the server for each file regardless of whether or not they are already cached.

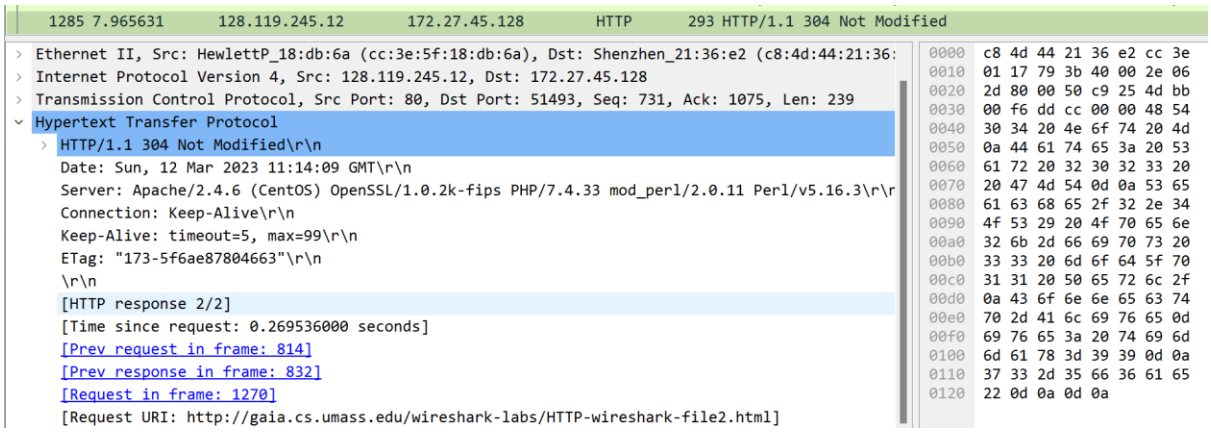


6. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

The contents of the file are returned for the first time.



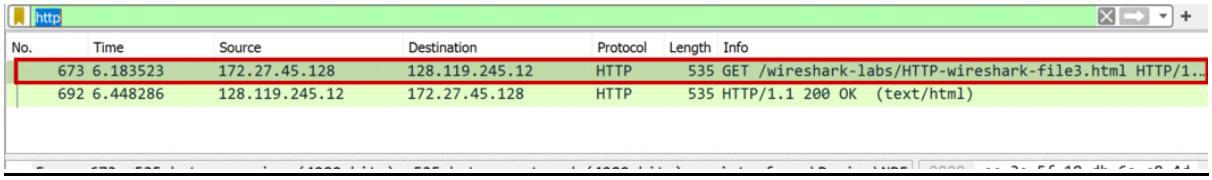
After refreshing, there will be no data returned as earlier response got cached.



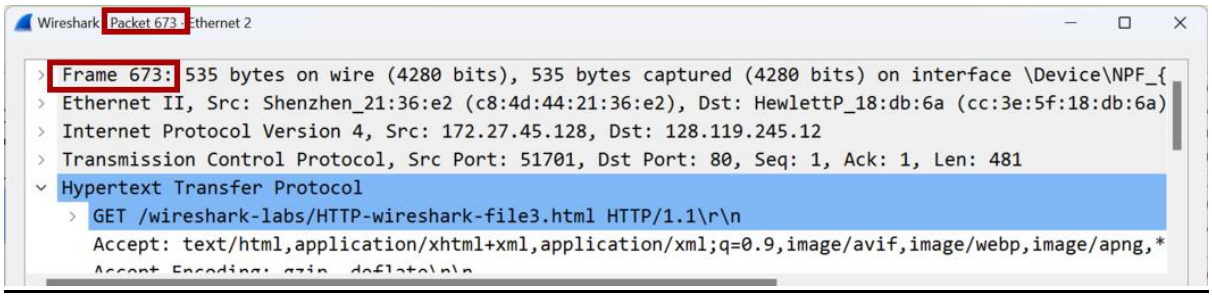
Start up the Wireshark packet sniffer. Enter the following URL into your browser(make sure your browser's cache is empty) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html .Your browser should display the lengthy US Bill of Rights. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

7. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Browser sent **1** HTTP GET request

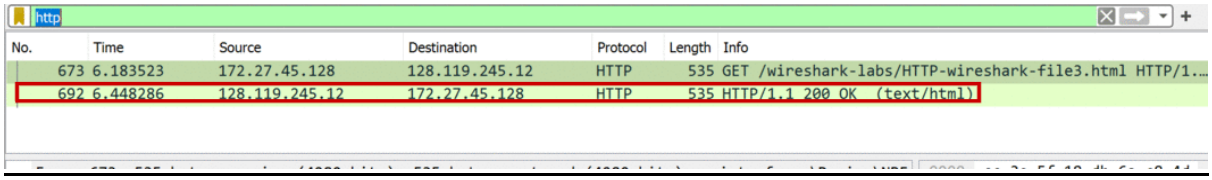


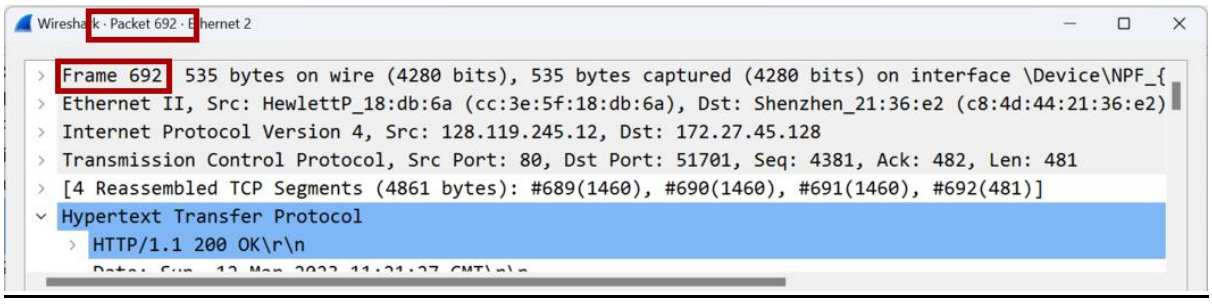
Packet number **673** contains the GET message for the Bill or Rights



8. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Packet number **692** in trace contains the status code.

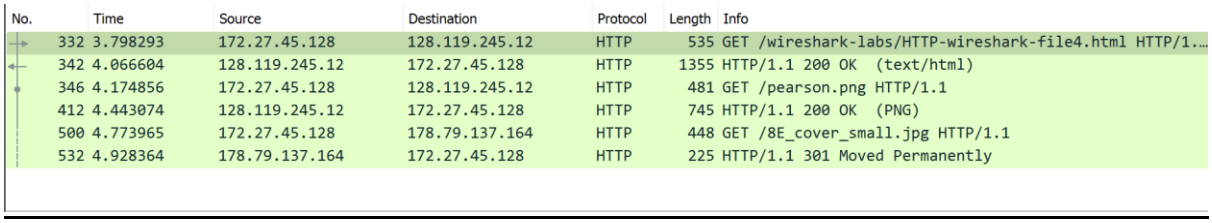




Start up the Wireshark packet sniffer. Enter the following URL into your browser (make sure your browser's cache is empty) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html Your browser should display a short HTML file with two images. Stop Wireshark packet capture

9. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

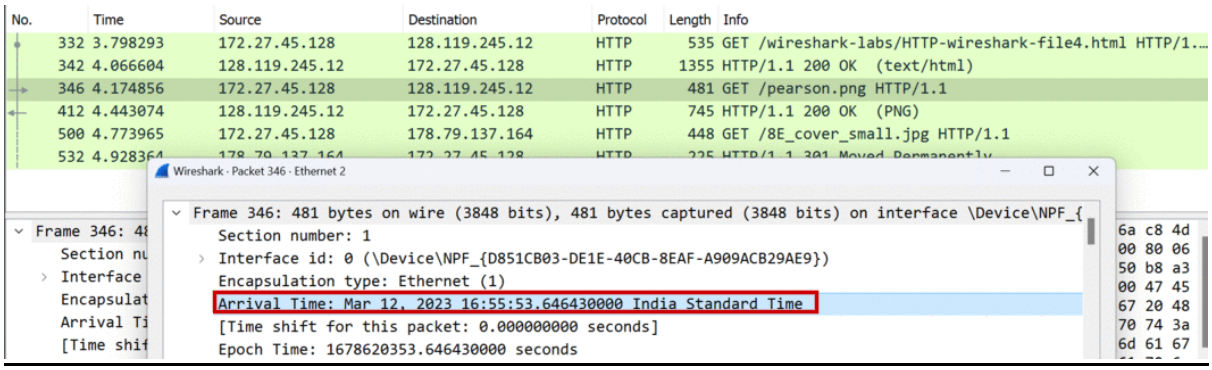
Browser sent **3** HTTP GET requests to the IP address **128.119.245.12**

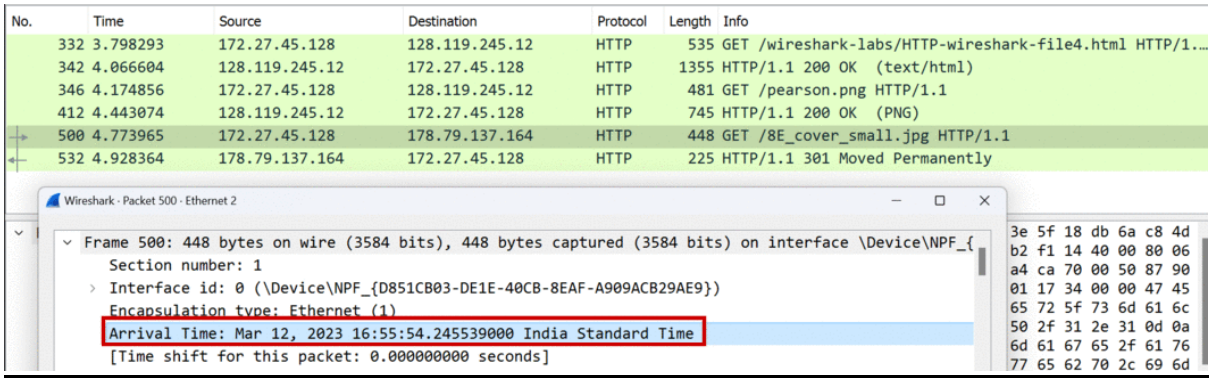


No.	Time	Source	Destination	Protocol	Length	Info
332	3.798293	172.27.45.128	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.…
342	4.066604	128.119.245.12	172.27.45.128	HTTP	1355	HTTP/1.1 200 OK (text/html)
346	4.174856	172.27.45.128	128.119.245.12	HTTP	481	GET /pearson.png HTTP/1.1
412	4.443074	128.119.245.12	172.27.45.128	HTTP	745	HTTP/1.1 200 OK (PNG)
500	4.773965	172.27.45.128	178.79.137.164	HTTP	448	GET /8E_cover_small.jpg HTTP/1.1
532	4.928364	178.79.137.164	172.27.45.128	HTTP	225	HTTP/1.1 301 Moved Permanently

10.Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

The images were downloaded **serially** and it can be explained by their packet arrival times. Both the times are different, hence cannot be parallel.





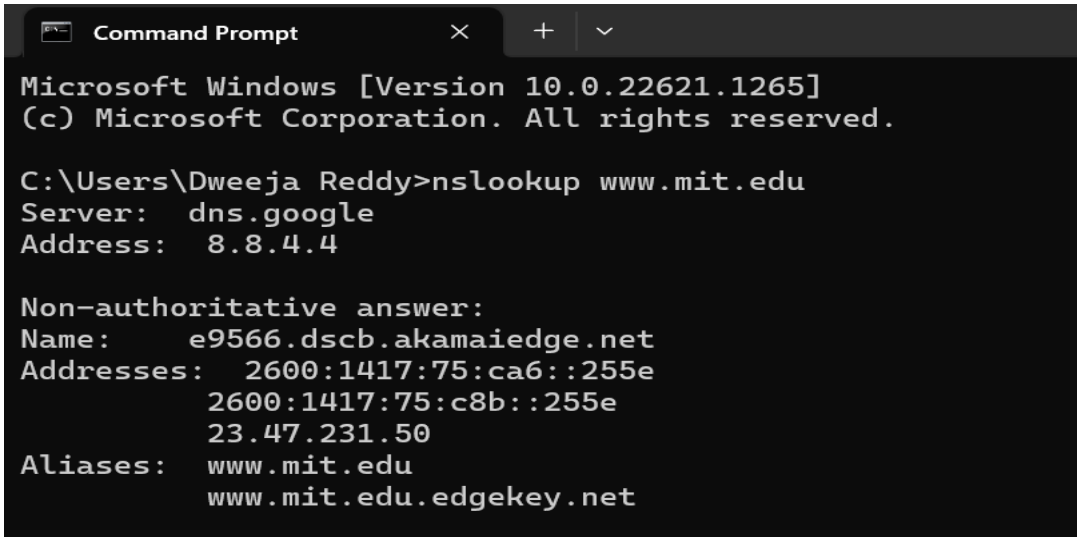
DNS Assignment

nslookup: nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top - leveldomain DNS server, an authoritative DNS server, or an intermediate DNS server. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

1.Run 'nslookup www.mit.edu' on your command prompt and what will be the name and IP address of the DNS server that provides the answer?

Name: e9566.dscb.akamaiedge.net

IP Address: 23.47.231.50



2.Run 'nslookup –type=NS mit.edu' on your command prompt and what will be the host names of the authoritative DNS for mit.edu.

mit.edu nameserver = asia1.akam.net

mit.edu nameserver = ns1-37.akam.net

mit.edu nameserver = eur5.akam.net

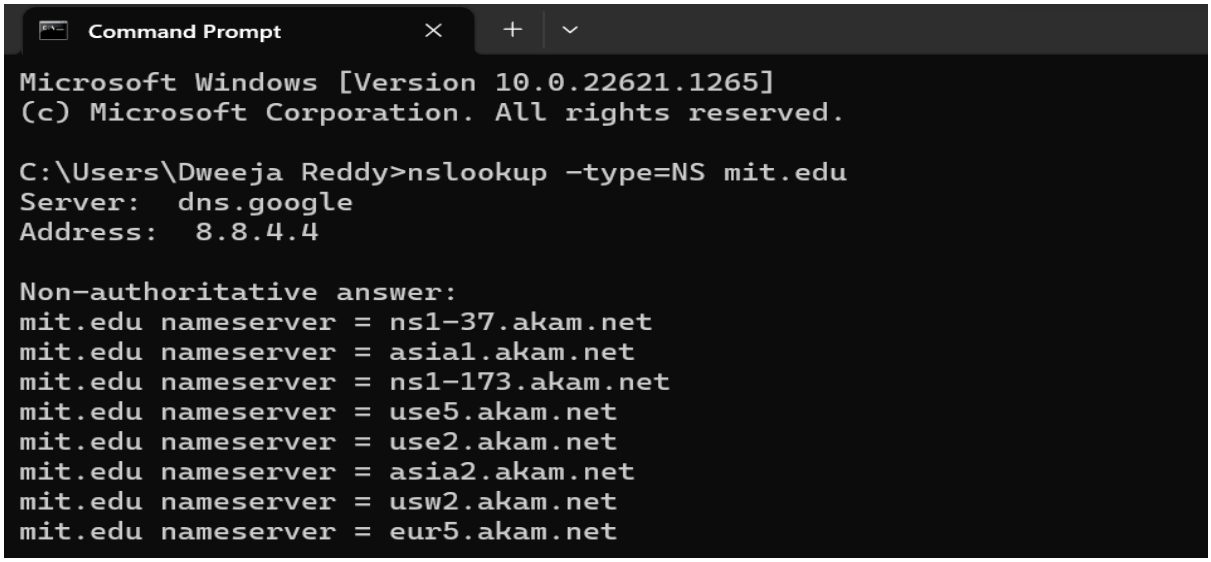
mit.edu nameserver = asia2.akam.net

mit.edu nameserver = ns1-173.akam.net

mit.edu nameserver = use2.akam.net

mit.edu nameserver = use5.akam.net

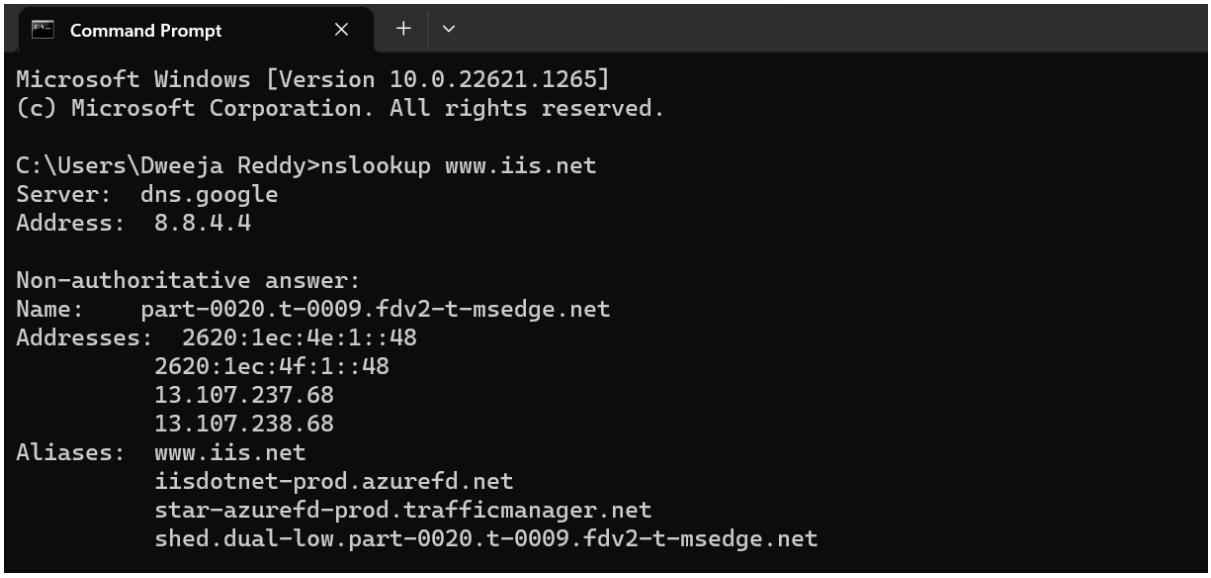
mit.edu nameserver = usw2.akam.net



3.Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

I took www.iis.net as Asian webserver to test nslookup.

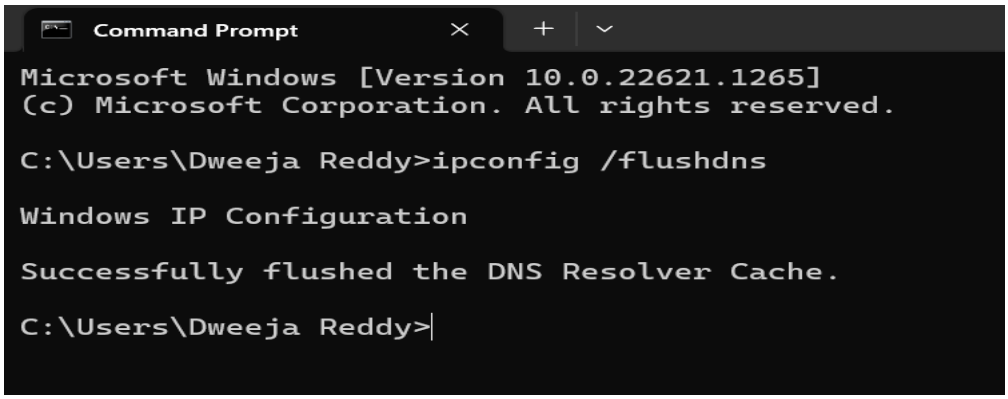
IP address of that server: 13.107.238.68

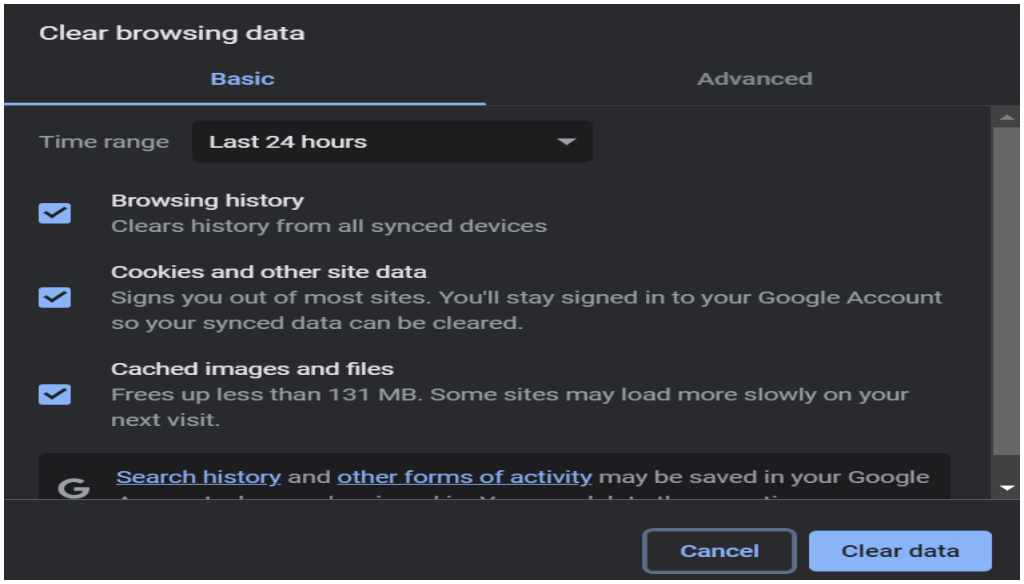


ipconfig: ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. ipconfig can be used to show your current TCP/IP information, including your

address, DNS server addresses, adapter type and so on. For example, you can get all this information about your host simply by entering ‘ipconfig \all’ into the Command Prompt. ‘ipconfig /displaydns’ -->Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter ‘ipconfig /flushdns’ Flushing the DNS cache clears all entries and reloads the entries from the hosts file. Now that we are familiar with nslookup and ipconfig, firstly now capture the DNS packets that are generated by ordinary Websurfing activity.

- Use ipconfig to empty the DNS cache in your host.
- Open your browser and empty your browser cache.
- Open Wireshark and enter “ip.addr == ” into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: http://www.ietf.org
- Stop packet capture.



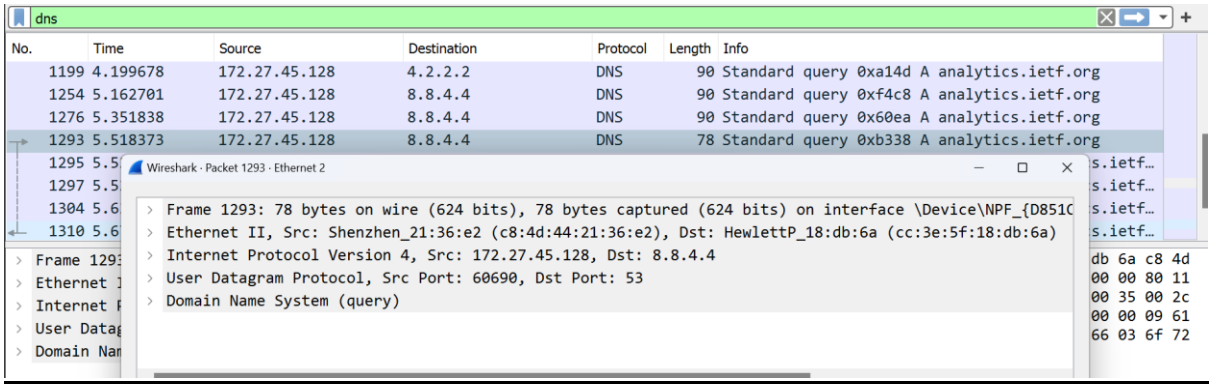


```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::122b:66b2:be99:2c84%56
   IPv4 Address. . . . . . . . . . . : 172.27.45.128
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : fe80::2a3b:82ff:fe2a:7ab5%56
                                       172.27.32.1
```

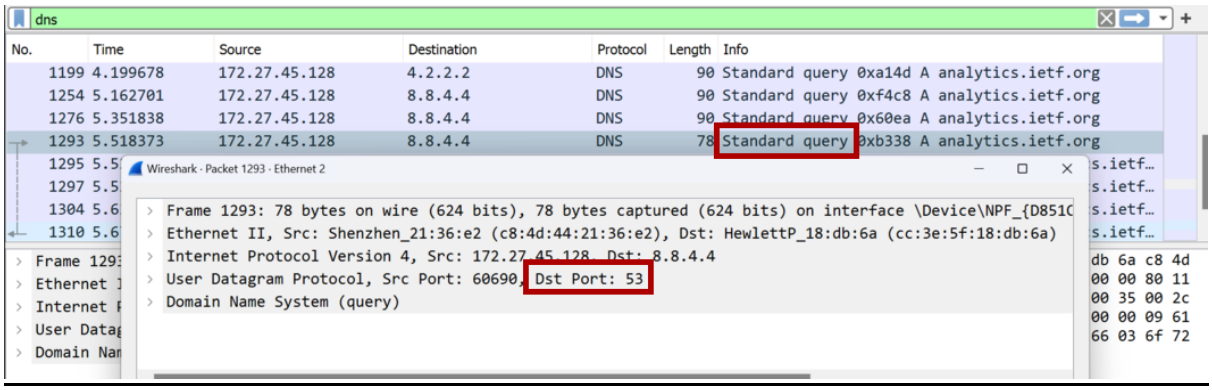
4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

<u>These are sent over **UDP**</u>

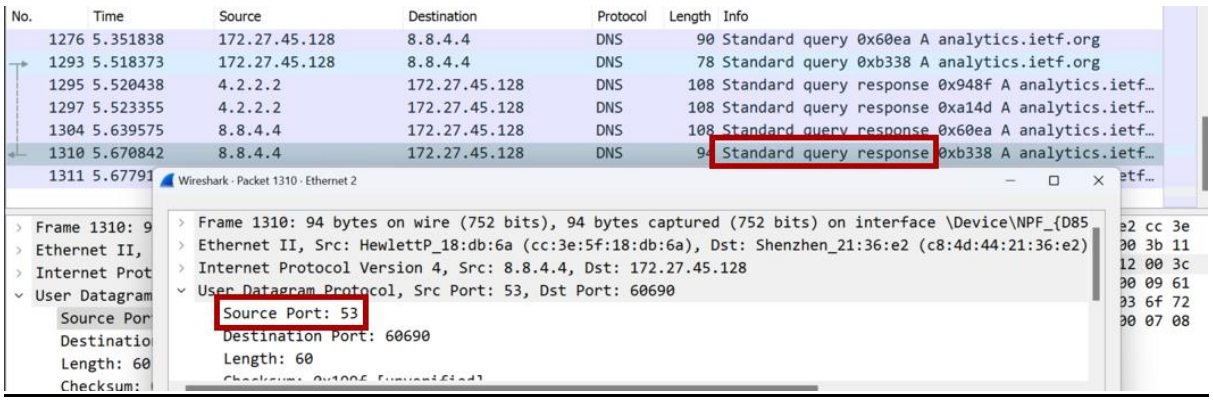


5. What is the destination port for the DNS query message? What is the source port of the DNS response message?

<u>Destination port for DNS query : **53**</u>

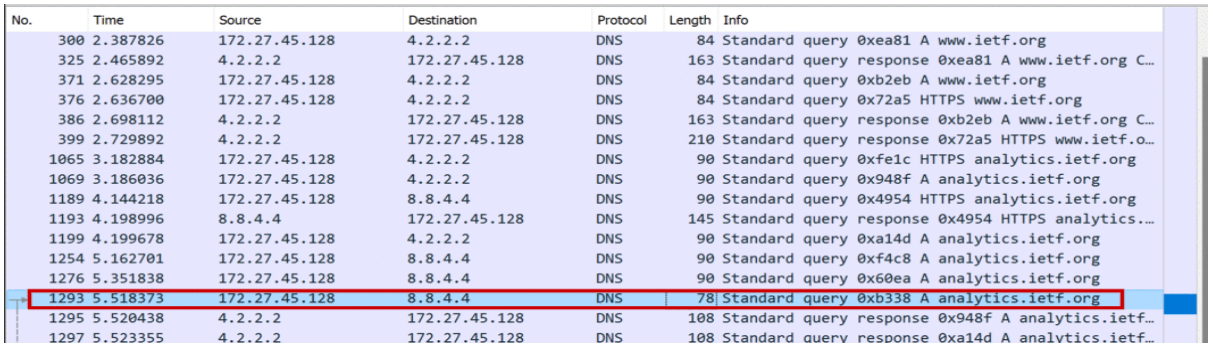


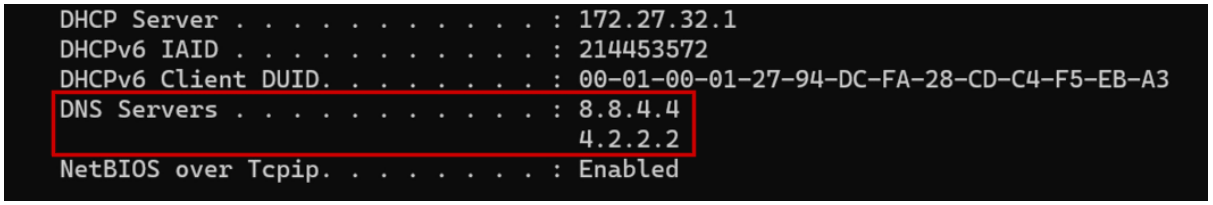
Source port for DNS response : **53**



6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

DNS query message is sent to the IP address: **8.8.4.4** which is also one of the DNS servers IP addresses





TCP Assignment

● Start up your web browser. Go the http://gaia.cs.umass.edu/wiresharklabs/alice.txt and retrieve an ASCII copy of Alice in Wonderland. Store this file somewhere on your computer.

● Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wiresharkfile1.html.

● Use the Browse button in this form to enter the name of the file (full path name) on your computer containing Alice in Wonderland (or do so manually). Don't yet press the "Upload alice.txt file" button.

● Now start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we'll not need to select any options here).

● Returning to your browser, press the "Upload alice.txt file" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.

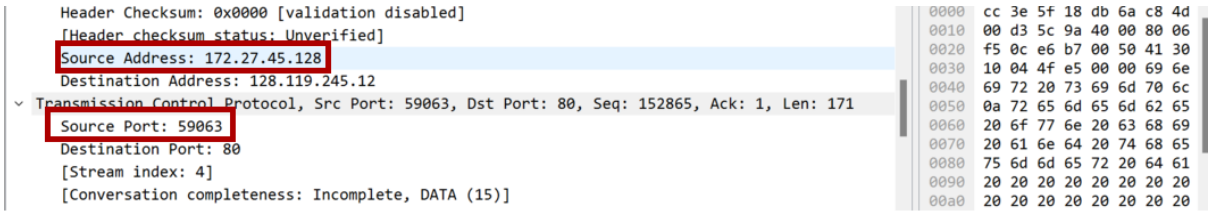
● Stop Wireshark packet capture.

● Before analyzing the behavior of the TCP connection in detail, let's take a high level view of the trace. First, filter the packets displayed in the Wireshark window by entering "tcp"

1.What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

Source IP address: **172.27.45.128**

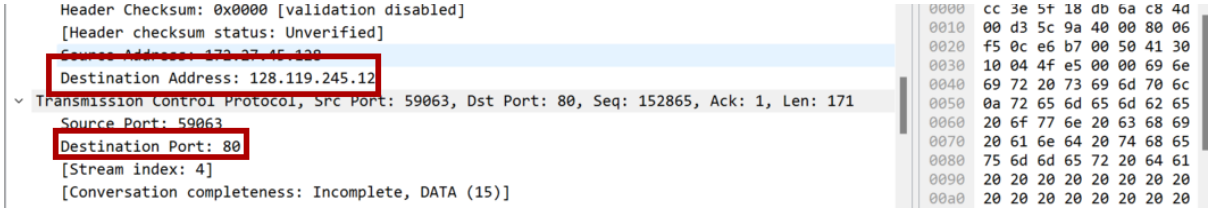
Source Port: **59063**



2.What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Destination IP address: **128.119.245.12**

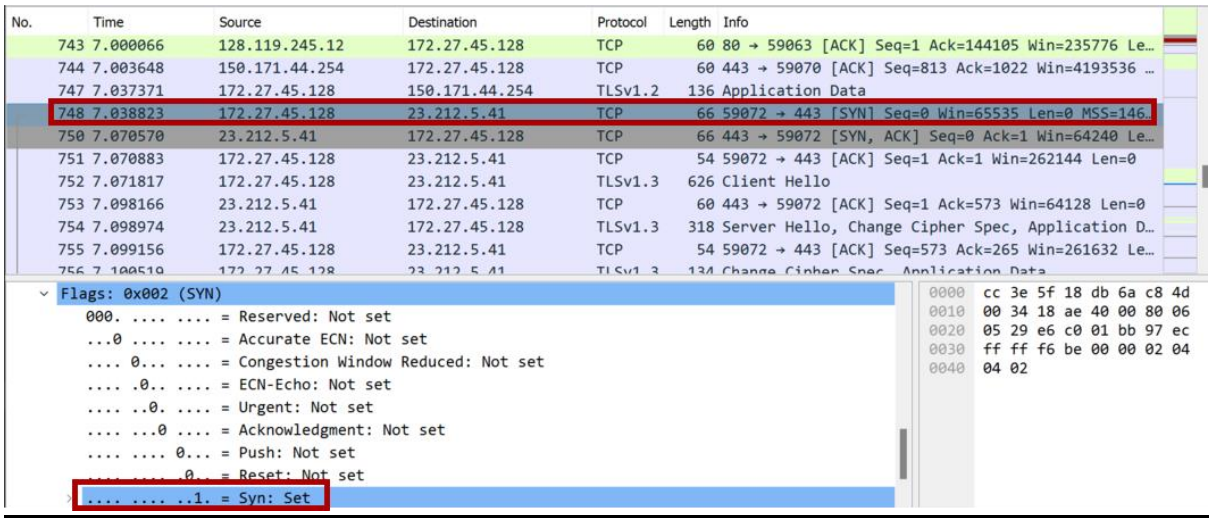
Destination Port: **80**



3.What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is **0**.

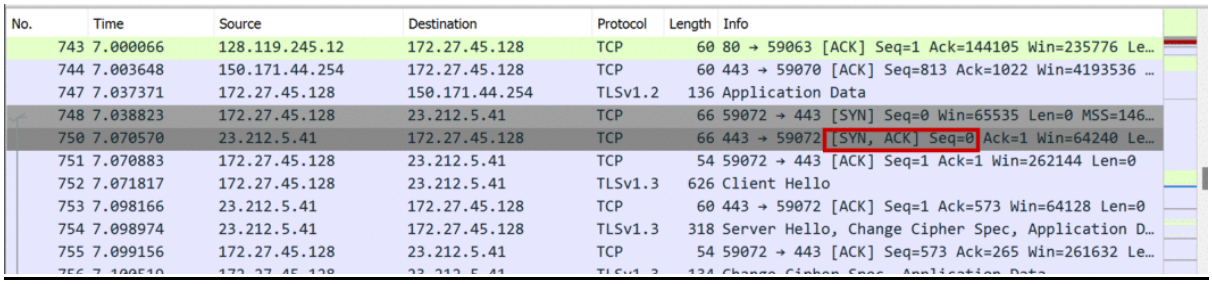
Segment can be identified as a SYN segment if **SYN flag is set to 1**.



4. Answer the following:

a. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?

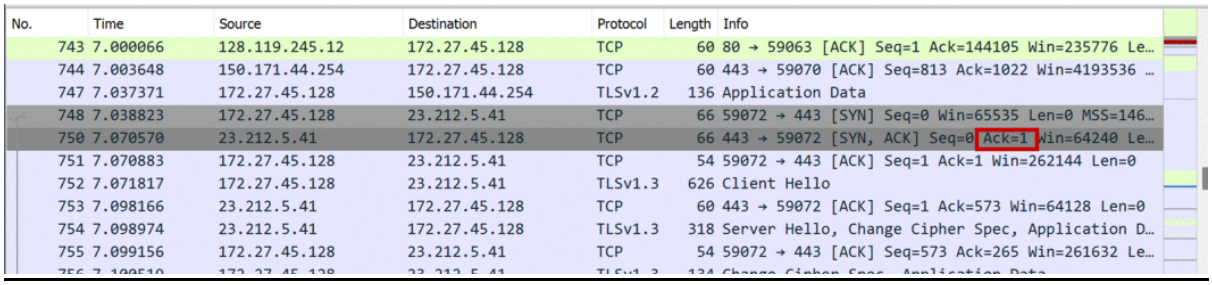
Sequence number of the SYNACK segment from gaia.cs.umass.edu to the client computer in reply to the SYN is **0** in this trace



No.	Time	Source	Destination	Protocol	Length	Info
743	7.000066	128.119.245.12	172.27.45.128	TCP	60	80 → 59063 [ACK] Seq=1 Ack=144105 Win=235776 Le…
744	7.003648	150.171.44.254	172.27.45.128	TCP	60	443 → 59070 [ACK] Seq=813 Ack=1022 Win=4193536 …
747	7.037371	172.27.45.128	150.171.44.254	TLSv1.2	136	Application Data
748	7.038823	172.27.45.128	23.212.5.41	TCP	66	59072 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=146…
750	7.070570	23.212.5.41	172.27.45.128	TCP	66	443 → 59072 [SYN, ACK] Seq=0 Ack=1 Win=64240 Le…
751	7.070883	172.27.45.128	23.212.5.41	TCP	54	59072 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
752	7.071817	172.27.45.128	23.212.5.41	TLSv1.3	626	Client Hello
753	7.098166	23.212.5.41	172.27.45.128	TCP	60	443 → 59072 [ACK] Seq=1 Ack=573 Win=64128 Len=0
754	7.098974	23.212.5.41	172.27.45.128	TLSv1.3	318	Server Hello, Change Cipher Spec, Application D…
755	7.099156	172.27.45.128	23.212.5.41	TCP	54	59072 → 443 [ACK] Seq=573 Ack=265 Win=261632 Le…

b.What is the value of the Acknowledgement field in the SYNACK segment?

The value of the Acknowledgement field in the SYNACK segment is 1.

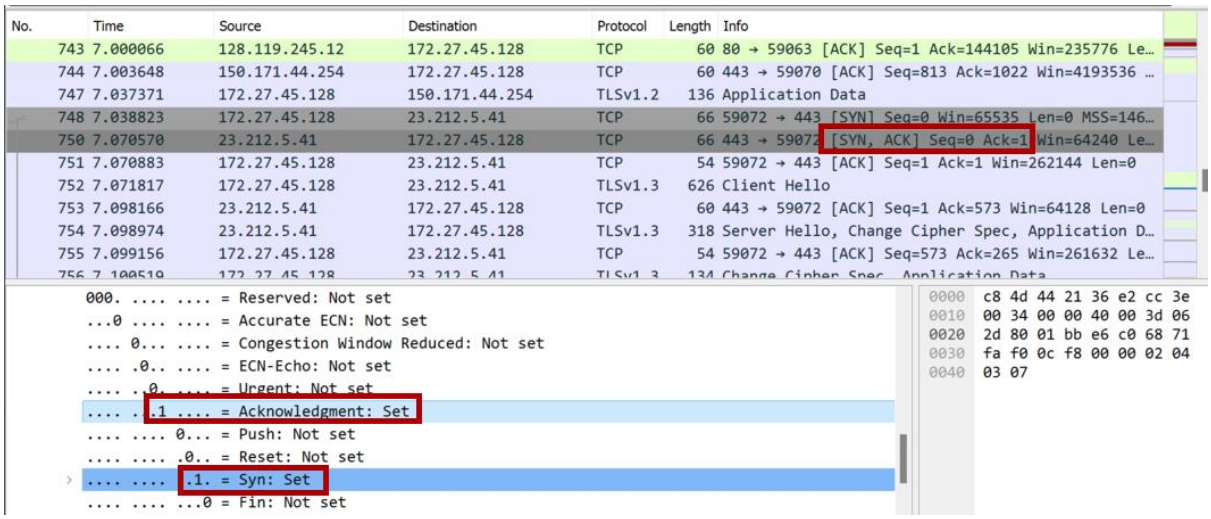


No.	Time	Source	Destination	Protocol	Length	Info
743	7.000066	128.119.245.12	172.27.45.128	TCP	60	80 → 59063 [ACK] Seq=1 Ack=144105 Win=235776 Le…
744	7.003648	150.171.44.254	172.27.45.128	TCP	60	443 → 59070 [ACK] Seq=813 Ack=1022 Win=4193536 …
747	7.037371	172.27.45.128	150.171.44.254	TLSv1.2	136	Application Data
748	7.038823	172.27.45.128	23.212.5.41	TCP	66	59072 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=146…
750	7.070570	23.212.5.41	172.27.45.128	TCP	66	443 → 59072 [SYN, ACK] Seq=0 Ack=1 Win=64240 Le…
751	7.070883	172.27.45.128	23.212.5.41	TCP	54	59072 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
752	7.071817	172.27.45.128	23.212.5.41	TLSv1.3	626	Client Hello
753	7.098166	23.212.5.41	172.27.45.128	TCP	60	443 → 59072 [ACK] Seq=1 Ack=573 Win=64128 Len=0
754	7.098974	23.212.5.41	172.27.45.128	TLSv1.3	318	Server Hello, Change Cipher Spec, Application D…
755	7.099156	172.27.45.128	23.212.5.41	TCP	54	59072 → 443 [ACK] Seq=573 Ack=265 Win=261632 Le…

c.How did gaia.cs.umass.edu determine that value?

The value of the ACKnowledgement field in the SYNACK segment is determined by gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer (i.e. the sequence number of the SYN segment initiated by the client computer is 0.)

d. What is it in the segment that identifies the segment as a SYNACK segment?



No.	Time	Source	Destination	Protocol	Length	Info
743	7.000066	128.119.245.12	172.27.45.128	TCP	60	80 → 59063 [ACK] Seq=1 Ack=144105 Win=235776 Le…
744	7.003648	150.171.44.254	172.27.45.128	TCP	60	443 → 59070 [ACK] Seq=813 Ack=1022 Win=4193536 …
747	7.037371	172.27.45.128	150.171.44.254	TLSv1.2	136	Application Data
748	7.038823	172.27.45.128	23.212.5.41	TCP	66	59072 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=146…
750	7.070570	23.212.5.41	172.27.45.128	TCP	66	443 → 59072 [SYN, ACK] Seq=0 Ack=1 Win=64240 Le…
751	7.070883	172.27.45.128	23.212.5.41	TCP	54	59072 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
752	7.071817	172.27.45.128	23.212.5.41	TLSv1.3	626	Client Hello
753	7.098166	23.212.5.41	172.27.45.128	TCP	60	443 → 59072 [ACK] Seq=1 Ack=573 Win=64128 Len=0
754	7.098974	23.212.5.41	172.27.45.128	TLSv1.3	318	Server Hello, Change Cipher Spec, Application D…
755	7.099156	172.27.45.128	23.212.5.41	TCP	54	59072 → 443 [ACK] Seq=573 Ack=265 Win=261632 Le…

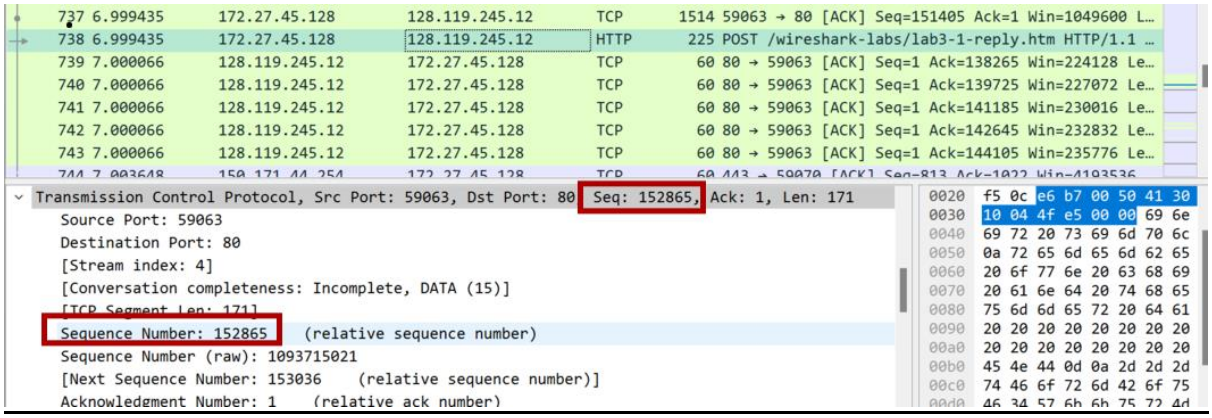
```
000. .... .... = Reserved: Not set
...0 .... .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
```

```
0000  c8 4d 44 21 36 e2 cc 3e
0010  00 34 00 00 40 00 3d 06
0020  2d 80 01 bb e6 c0 68 71
0030  fa f0 0c f8 00 00 02 04
0040  03 07
```

The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.

5. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

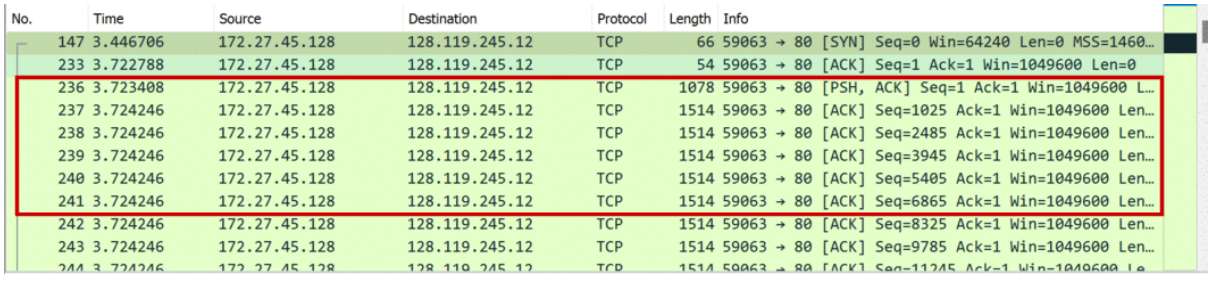
Sequence number of the TCP segment containing the HTTP POST command is **152865**



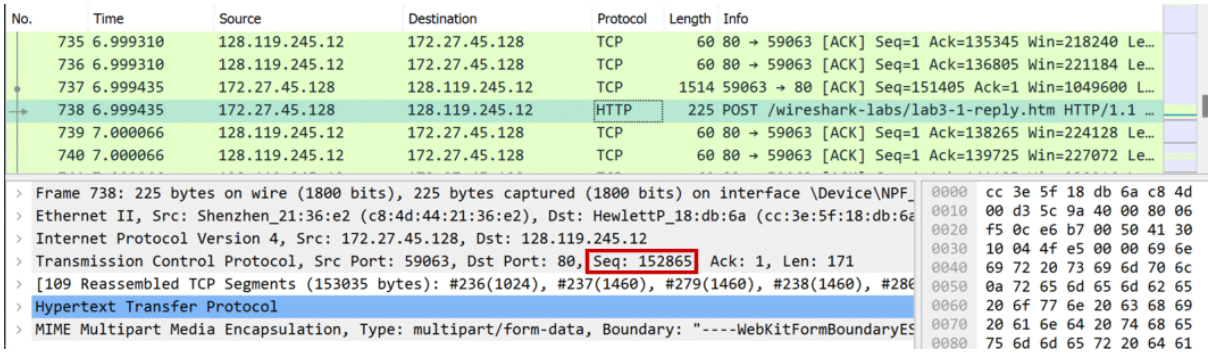
6. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection:

a. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)?

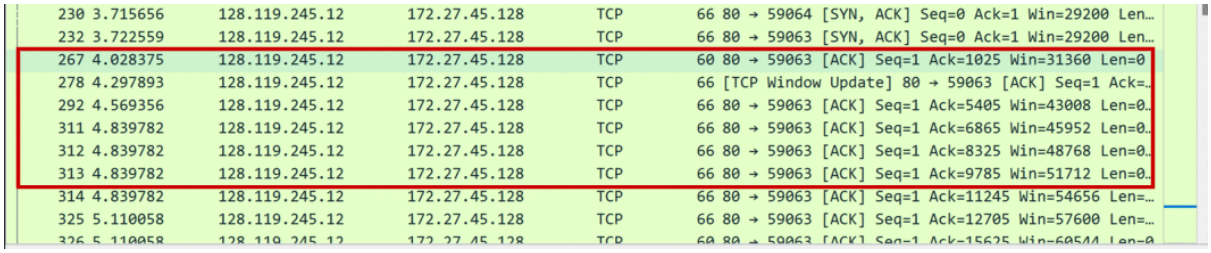
The sequence numbers of first six segments in TCP are **1,1025,2485,3945,5405,6865**



The sequence number of the segment containing HTTP POST is **152865**



Coressponding arrival times are shown below:



b. At what time was each segment sent? And when was the ACK for each segment received?

Packet Number	Sent Time	Received Time	RTT
1	3.723408	4.028375	0.304967
2	3.724246	4.297893	0.573647
3	3.724246	4.569356	0.845110
4	3.724246	4.839782	1.115536
5	3.724246	4.839782	1.115536
6	3.724246	4.839782	1.115536

c.What is the EstimatedRTT value after the receipt of each ACK? (*Use the EstimatedRTT equation. Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation).

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

Initially, Estimated RTT = 0. 304967

Step 1 value 0.875*0.304967 + 0.125*0.573647 = 0.338552

Step 2 value 0.875*0.338552 + 0.125*0.845110 = 0.401872

Step 3 value 0.875*0.401872 + 0.125*1.115536 = 0.491080

Step 4 value 0.875*0.491080 + 0.125*1.115536 = 0.569137

Step 5 value 0.875*0.569137 + 0.125*1.115536 = **0.637437**

d.What is the length of each of the first six TCP segments?

Lengths are **1078,1514,1514,1514,1514,1514**

e. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

The alice.txt on the hard drive is of size **152,136 bytes**

Download time is

7.269500 (last TCP segment) - 3. 723408(last ACK) = 3.546092 second.

Throughput for the TCP connection is computed as 152,136/3.546092

= **42902.4402** bytes/second.

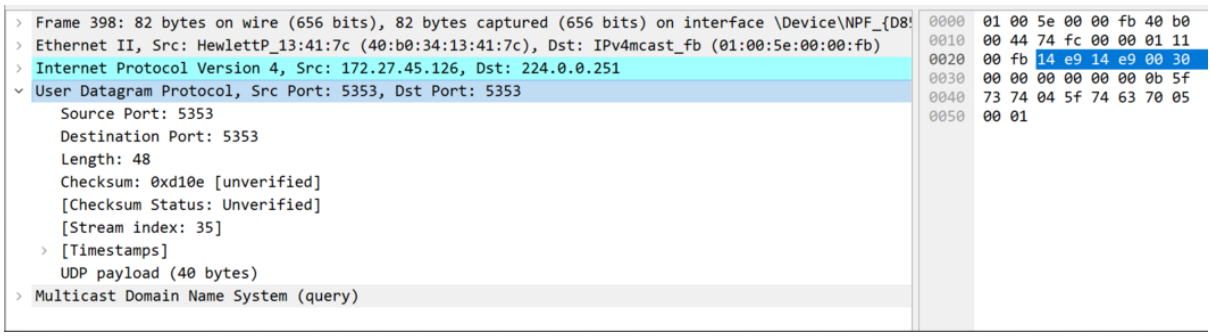
UDP Assignment

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It's also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window.

Use the packet trace that you have captured and answer the following questions, by opening the Wireshark captured packet file.

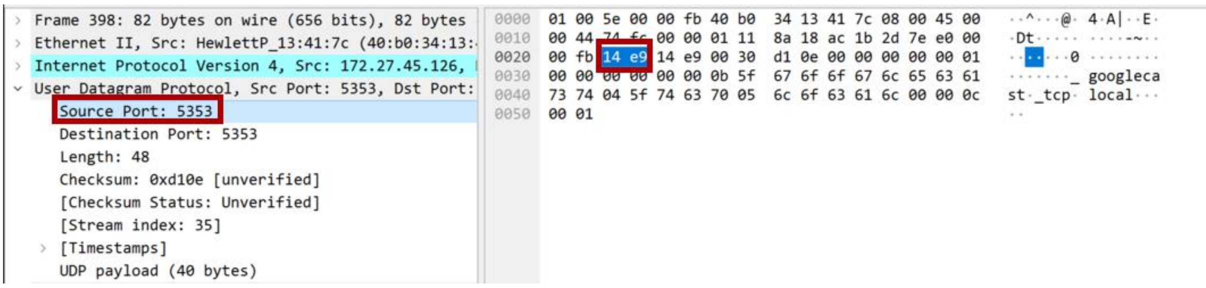
1.Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields. (Answer these questions directly from what you observe in the packet trace.)

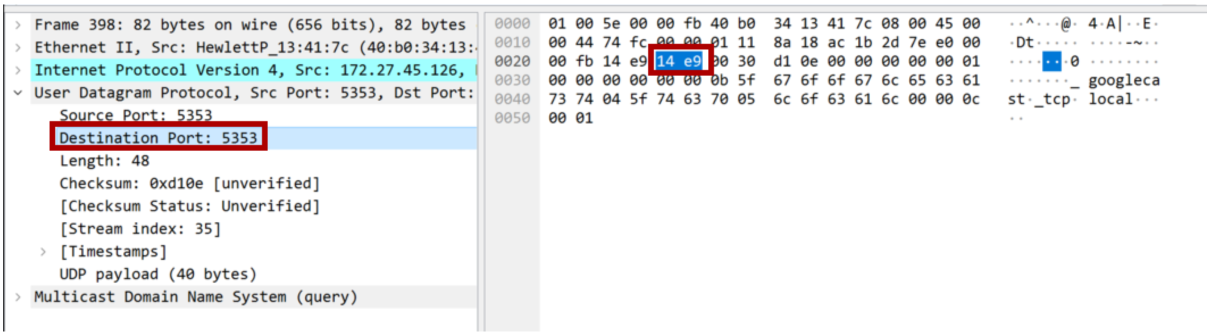
There are four fields – **Source Port, Destination Port, Length and checksum**

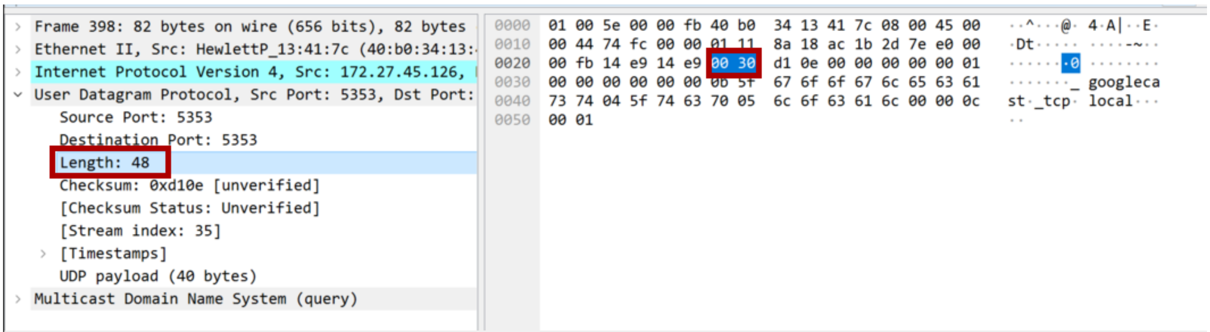


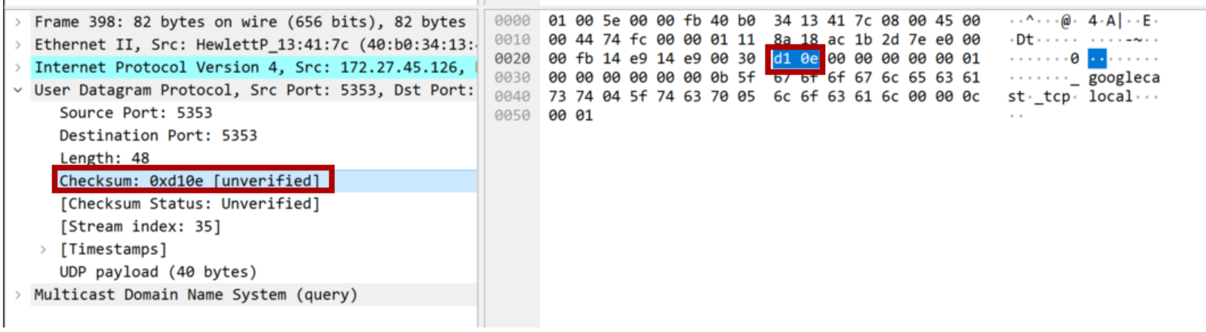
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Each UDP header is of length **2 bytes** which can be understood from the hex values beside.

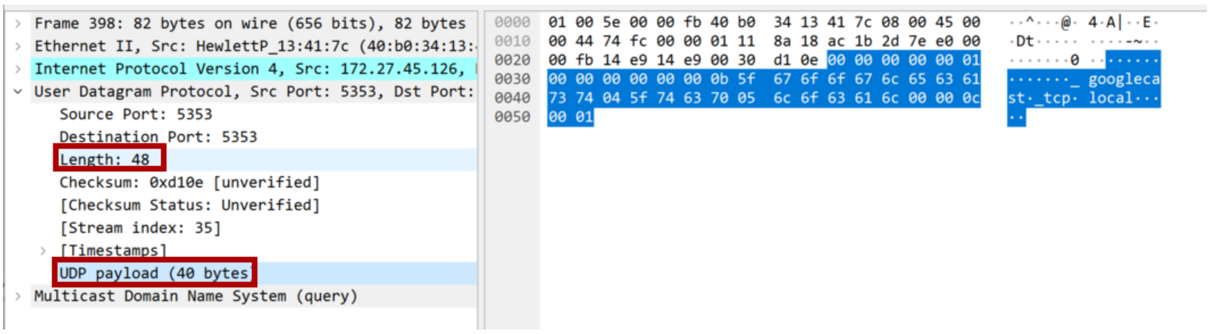








3.The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.



Length field has value as 48.

It is the length in bytes for the UDP segment (header + data).

Header will be of 2*4 = 8 Bytes.

Hence payload will be of 48-8 = 40 Bytes which can be seen from above picture.

4. What is the maximum number of bytes that can be included in a UDP payload?

Source port field is 16 bits.

Therefore 2^16-1 - header bytes(8) = **65527** can be included in the payload.

5. What is the largest possible source port number?

Largest possible source port number is **2^16-1 = 65535**

6. What is the protocol number for UDP?

Protocol number for UDP is **17** (0x11 in hexadecimal)