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: Protocols appearing in wireshark
   1. ARP
   2. Transport layer security protocol
   3. Spanning Tree Protocol
   4. DHCP
   5. DNS
   6. HTTP
   7. ICMP
   8. TCP
   9. UDP

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*.)

   Ans: 0.260406275 sec

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: IP address of gaia.cs.umass.edu 128.119.245.12
   IP address of computer 192.168.94.65

To answer the following two questions, you'll need to select the TCP packet containing the HTTP GET request. The purpose of these next two questions is to familiarize you with using Wireshark's "Details of selected packet window"; see Figure 3. To answer the first question below, then look in the "Details of selected packet" window toggle the triangle for HTTP (your screen should then look similar to Figure 5); for the second question below, you'll need to expand the information on the Transmission Control Protocol (TCP) part of this packet.

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

   Ans: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0

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?

   Ans: Destination Port: 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, and then click OK.
   Ans:

   /home/owner/1st.pcapng 749 total packets, 4 shown

No.

Time

Source

Delta

Destination

Protocol Length Info

551 15:34:17.639249973 128.119.245.12

0.260406275

192.168.94.65

HTTP

492

HTTP/1.1 200 OK

html)

Frame 551: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface eno1, id 0

Ethernet II, Src: HewlettP_09:cb:cf (ec:9b:8b:09:cb:cf), Dst: d8:bb:c1:6b:1b:4a (d8:bb:c1:6b:1b:4a)

Destination: d8:bb:c1:6b:1b:4a (d8:bb:c1:6b:1b:4a)

Address: d8:bb:c1:6b:1b:4a (d8:bb:c1:6b:1b:4a)

.... ..0. .... = LG bit: Globally unique address (factory default)

....0 .... = IG bit: Individual address (unicast)

Source: HewlettP_09:cb:cf (ec:9b:8b:09:cb:cf)

Address: HewlettP_09:cb:cf (ec:9b:8b:09:cb:cf)

.... ..0. .... = LG bit: Globally unique address (factory default)

....0 .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.94.65

0100 .... = Version: 4

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

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 478

Identification: 0xea40 (59968)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 39

Protocol: TCP (6)

Header checksum: 0xd36b [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.94.65

Transmission Control Protocol, Src Port: 80, Dst Port: 50616, Seq: 1, Ack: 391, Len: 438

Source Port: 80

Destination Port: 50616

[Stream index: 10]

[TCP Segment Len: 438]

Sequence number: 1

(relative sequence number)

Sequence number (raw): 2847426419

[Next sequence number: 439

(relative sequence number)]

Acknowledgment number: 391

(relative ack number)

Acknowledgment number (raw): 2974683668

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

Flags: 0x018 (PSH, ACK)

Window size value: 237

[Calculated window size: 30336]

[Window size scaling factor: 128]

Checksum: 0x0526 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[iRTT: 0.258690480 seconds]

[Bytes in flight: 438]

[Bytes sent since last PSH flag: 438]

[Timestamps]

[Time since first frame in this TCP stream: 0.519399143 seconds]

[Time since previous frame in this TCP stream: 0.001436851 seconds]

TCP payload (438 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Wed, 23 Aug 2023 10:04:17 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Wed, 23 Aug 2023 05:59:01 GMT\r\n

ETag: "51-60390cee3bf48"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.260406275 seconds]

[Request in frame: 546]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)

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

- www.washington.edu/
- example.com/
- www.iith.ac.in
- www.youtube.com

Ans:1. http://www.washington.edu/

1: Protocol: ARP, DNS, HTTP, ICMP,OCSP,STP,TCP,TLS,UDP
2: Time required for 1st ack: 0.841338619
3: IP address of www.washington.edu/128.95.155.198
IP address of computer 192.168.94.65

2. example.com/

1: Protocol: ARP, DNS, HTTP, ICMP,OCSP,STP,TCP,TLS,UDP

2 Time required for 1st ack: 0.433122361 sec

3: IP address of example.com/ 93.184.216.34

IP address of computer 192.168.94.65

3. www.iith.ac.in

Website is forcing to use https and we are not able to run the website on http, so we are not able to capture any http packets.

4. www.youtube.com

Website is forcing to use https and we are not able to run the website on http, so we are not able to capture any http packets.

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

Ans: 1. In contrast to example.com which have single req and response, Washington.edu has multiple request and response as multiple resources (js file, text, png) are fetched in washington.edu website.

2. time between request and response time is less in Washington.edu compared to example.com