Computer Networks Lab

Lab - 2
Pranav Kanire
Roll No - 190010033

January 18, 2021

1 PART-1

1.1 Question 1

The black highlighted packet identifies TCP packets with problems - for example, they could have been delivered out-of-order.

1.2 Question 2

For listing all outgoing http traffic we can put 'http' in the filter bar or to filter out more in a better way we use the 'http.host=="website or it's ip-address"'

1.3 Question 3

UDP stream is fast and has low overhead, hence it is preferred for DNS. A DNS query is a single UDP request from the DNS client followed by a single UDP reply from the server. When a host requests a web page, transmission reliability and completeness must be guaranteed. Therefore, HTTP uses TCP as its transport layer protocol.

2 PART-2

2.1 Question 1

The different protocols that appear in the protocol column in the unfiltered packet-listing window in wireshark GUI are: ARP, DNS, TCP, HTTP.
These are stated using Mozilla Firefox browser and were common in all browsers.
In addtion to these protocols DHCP and ICMP protocols were present in Microsoft Edge also TLS and UDP protocols were there in Google Chrome.

2.2 Question 2

For this we look for the time of arrival of both the packets in the frame section.
(Screenshots for the same are attached separately.)

1. Using Mozilla Firefox browser:
   For HTTP GET message time of arrival is 19:33:01.881517089
   For HTTP OK message time of arrival is 19:33:03.892639110
   The difference of these two times gives:
   03.892639110 - 01.881517089 = **2.011122021 seconds**

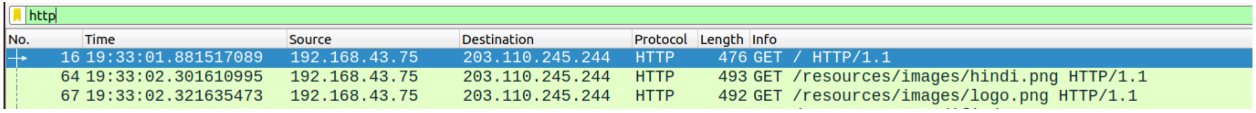
2. Using Microsoft Edge browser:
   For HTTP GET message time of arrival is 20:29:30.314408760
   For HTTP OK message time of arrival is 20:29:31.296629579
   The difference of these two times gives:
   31.296629579 - 30.314408760 = **0.982220819 seconds**

3. Using Google Chrome browser:
   For HTTP GET message time of arrival is 22:52:19.313125363
   For HTTP OK message time of arrival is 22:52:20.655356459
   The difference of these two times gives:
   20.655356459 - 19.313125363 = **1.342231096 seconds**

2.3 Question 3

If we notice the GET request, we have source and destination. Here source is local machine and destination is the web server.

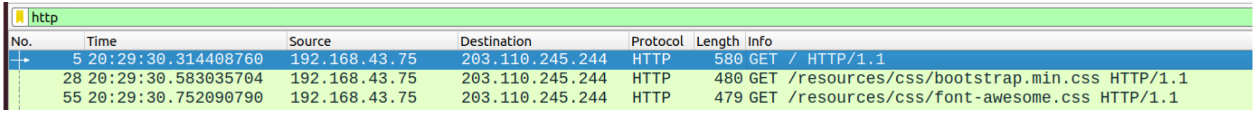
1. Using Mozilla Firefox browser:



http

No.	Time	Source	Destination	Protocol	Length	Info
16	19:33:01.881517089	192.168.43.75	203.110.245.244	HTTP	476	GET / HTTP/1.1
64	19:33:02.301610995	192.168.43.75	203.110.245.244	HTTP	493	GET /resources/images/hindi.png HTTP/1.1
67	19:33:02.321635473	192.168.43.75	203.110.245.244	HTTP	492	GET /resources/images/logo.png HTTP/1.1

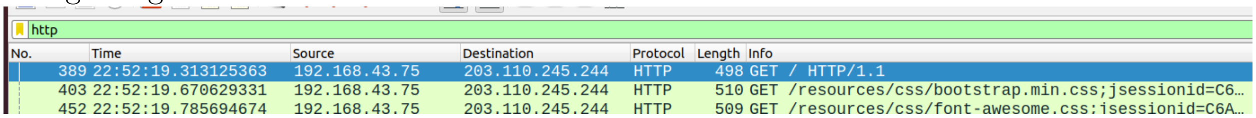
2. Using Microsoft Edge browser:



http

No.	Time	Source	Destination	Protocol	Length	Info
5	20:29:30.314408760	192.168.43.75	203.110.245.244	HTTP	580	GET / HTTP/1.1
28	20:29:30.583035704	192.168.43.75	203.110.245.244	HTTP	480	GET /resources/css/bootstrap.min.css HTTP/1.1
55	20:29:30.752090790	192.168.43.75	203.110.245.244	HTTP	479	GET /resources/css/font-awesome.css HTTP/1.1

3. Using Google Chrome browser:



No.	Time	Source	Destination	Protocol	Length	Info
389	22:52:19.313125363	192.168.43.75	203.110.245.244	HTTP	498	GET / HTTP/1.1
403	22:52:19.670629331	192.168.43.75	203.110.245.244	HTTP	510	GET /resources/css/bootstrap.min.css;jsessionid=C6…
452	22:52:19.785694674	192.168.43.75	203.110.245.244	HTTP	509	GET /resources/css/font-awesome.css:isessionid=C6A…

Since all browsers are in same machine and same URL was achieved in all of them, they have same source and destination.
So IP address of my computer is 192.168.43.75
IP address of visited URL is 203.110.245.244

2.4 Question 4

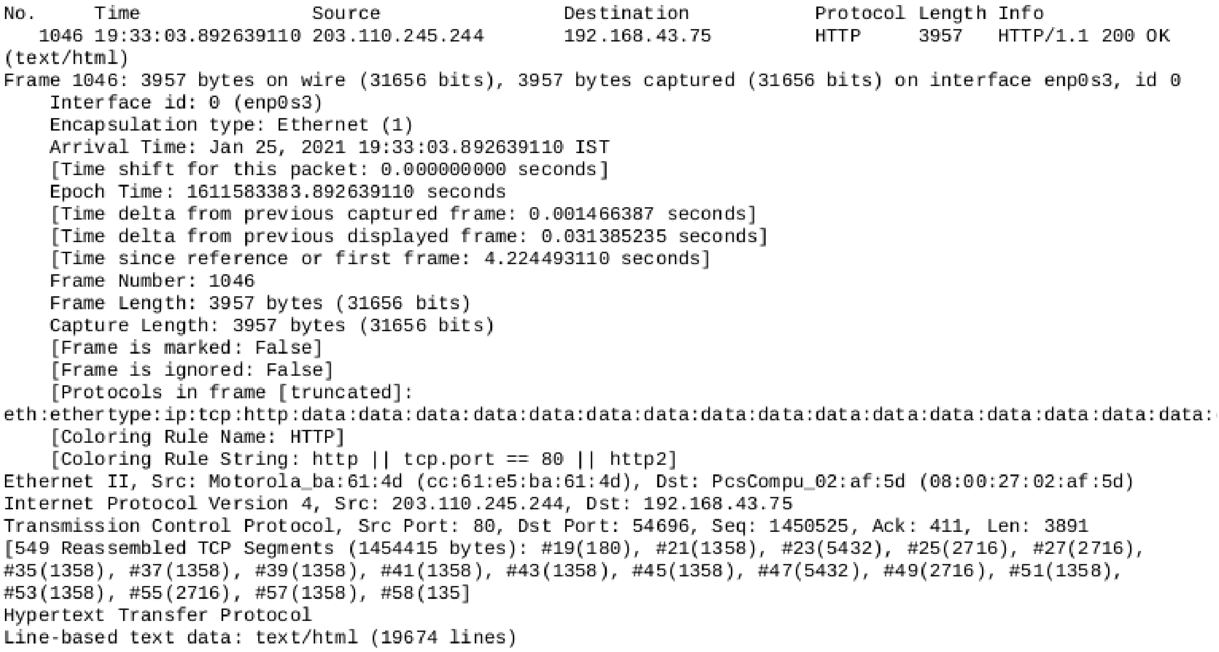
The content of HTTP GET and OK package captured using different browsers is displayed below:
(though screenshots as well as the pdf of these packages of all the browsers is attached separately.)

1. Using Mozilla Firefox browser:

   GET

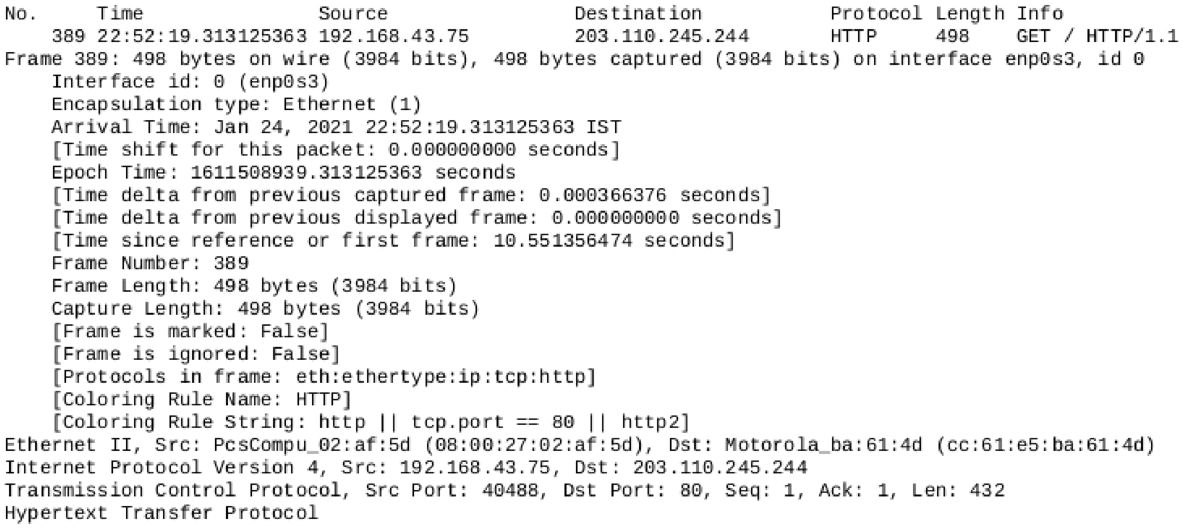
```
No.     Time                   Source                Destination           Protocol Length Info
     16 19:33:01.881517089 192.168.43.75         203.110.245.244       HTTP     476    GET / HTTP/1.1
Frame 16: 476 bytes on wire (3808 bits), 476 bytes captured (3808 bits) on interface enp0s3, id 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 25, 2021 19:33:01.881517089 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611583381.881517089 seconds
    [Time delta from previous captured frame: 0.000271580 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.213371089 seconds]
    Frame Number: 16
    Frame Length: 476 bytes (3808 bits)
    Capture Length: 476 bytes (3808 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PcsCompu_02:af:5d (08:00:27:02:af:5d), Dst: Motorola_ba:61:4d (cc:61:e5:ba:61:4d)
Internet Protocol Version 4, Src: 192.168.43.75, Dst: 203.110.245.244
Transmission Control Protocol, Src Port: 54696, Dst Port: 80, Seq: 1, Ack: 1, Len: 410
Hypertext Transfer Protocol
```

   OK



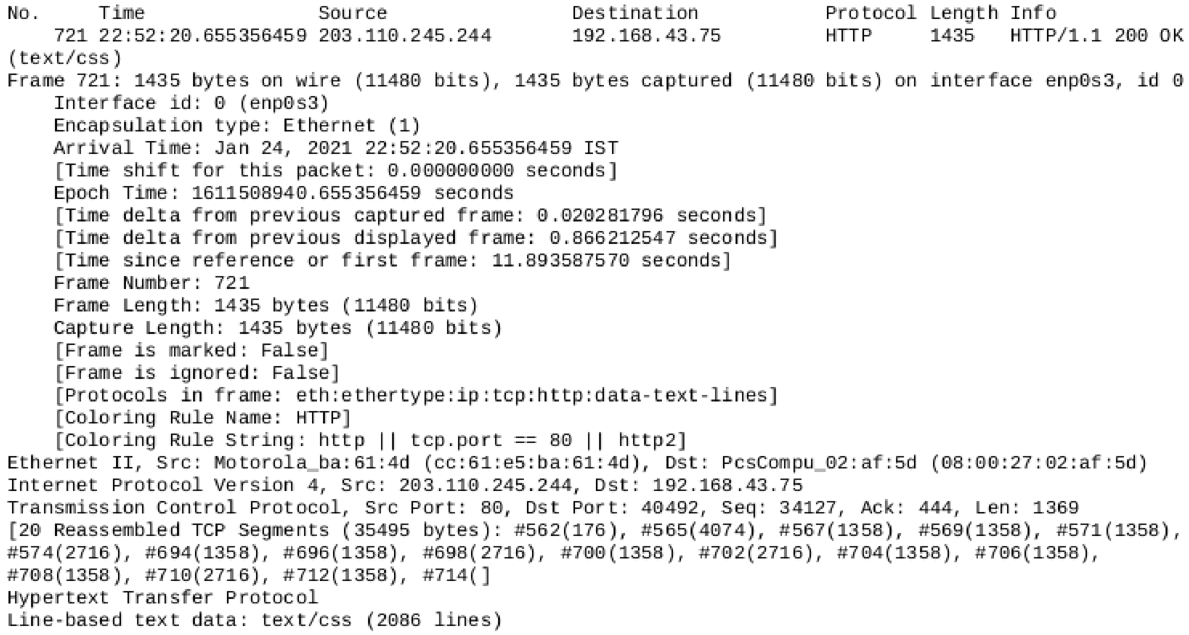
```
No.     Time               Source                Destination           Protocol Length Info
   1046 19:33:03.892639110 203.110.245.244       192.168.43.75         HTTP     3957   HTTP/1.1 200 OK
(text/html)
Frame 1046: 3957 bytes on wire (31656 bits), 3957 bytes captured (31656 bits) on interface enp0s3, id 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 25, 2021 19:33:03.892639110 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611583383.892639110 seconds
    [Time delta from previous captured frame: 0.001466387 seconds]
    [Time delta from previous displayed frame: 0.031385235 seconds]
    [Time since reference or first frame: 4.224493110 seconds]
    Frame Number: 1046
    Frame Length: 3957 bytes (31656 bits)
    Capture Length: 3957 bytes (31656 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame [truncated]:
eth:ethertype:ip:tcp:http:data:data:data:data:data:data:data:data:data:data:data:data:data:data:data:data:
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Motorola_ba:61:4d (cc:61:e5:ba:61:4d), Dst: PcsCompu_02:af:5d (08:00:27:02:af:5d)
Internet Protocol Version 4, Src: 203.110.245.244, Dst: 192.168.43.75
Transmission Control Protocol, Src Port: 80, Dst Port: 54696, Seq: 1450525, Ack: 411, Len: 3891
[549 Reassembled TCP Segments (1454415 bytes): #19(180), #21(1358), #23(5432), #25(2716), #27(2716),
#35(1358), #37(1358), #39(1358), #41(1358), #43(1358), #45(1358), #47(5432), #49(2716), #51(1358),
#53(1358), #55(2716), #57(1358), #58(135]
Hypertext Transfer Protocol
Line-based text data: text/html (19674 lines)
```

2. Using Microsoft Edge browser:
   GET



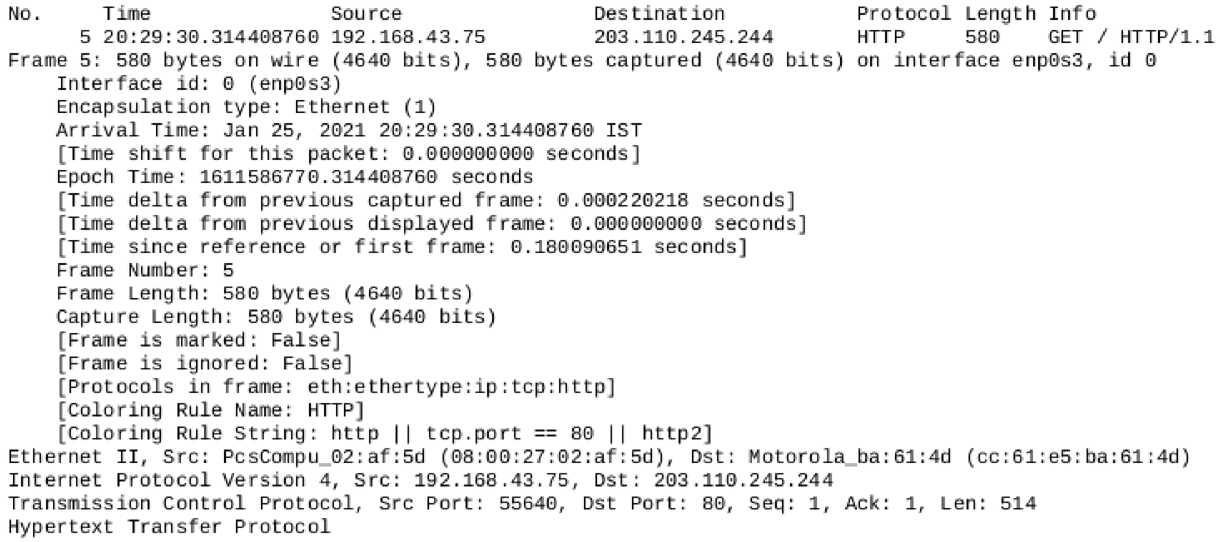
```
No.     Time               Source                Destination           Protocol Length Info
    389 22:52:19.313125363 192.168.43.75         203.110.245.244       HTTP     498    GET / HTTP/1.1
Frame 389: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface enp0s3, id 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2021 22:52:19.313125363 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611508939.313125363 seconds
    [Time delta from previous captured frame: 0.000366376 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 10.551356474 seconds]
    Frame Number: 389
    Frame Length: 498 bytes (3984 bits)
    Capture Length: 498 bytes (3984 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PcsCompu_02:af:5d (08:00:27:02:af:5d), Dst: Motorola_ba:61:4d (cc:61:e5:ba:61:4d)
Internet Protocol Version 4, Src: 192.168.43.75, Dst: 203.110.245.244
Transmission Control Protocol, Src Port: 40488, Dst Port: 80, Seq: 1, Ack: 1, Len: 432
Hypertext Transfer Protocol
```

   OK



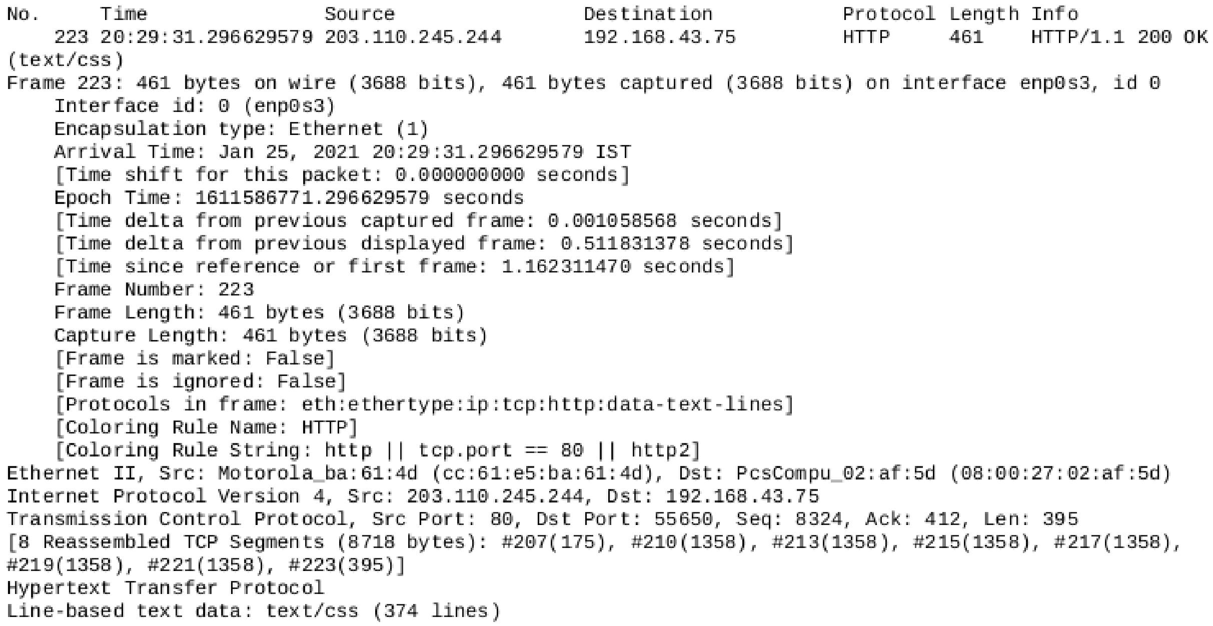
```
No.     Time               Source                Destination           Protocol Length Info
    721 22:52:20.655356459 203.110.245.244       192.168.43.75         HTTP     1435   HTTP/1.1 200 OK 
(text/css)
Frame 721: 1435 bytes on wire (11480 bits), 1435 bytes captured (11480 bits) on interface enp0s3, id 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2021 22:52:20.655356459 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611508940.655356459 seconds
    [Time delta from previous captured frame: 0.020281796 seconds]
    [Time delta from previous displayed frame: 0.866212547 seconds]
    [Time since reference or first frame: 11.893587570 seconds]
    Frame Number: 721
    Frame Length: 1435 bytes (11480 bits)
    Capture Length: 1435 bytes (11480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Motorola_ba:61:4d (cc:61:e5:ba:61:4d), Dst: PcsCompu_02:af:5d (08:00:27:02:af:5d)
Internet Protocol Version 4, Src: 203.110.245.244, Dst: 192.168.43.75
Transmission Control Protocol, Src Port: 80, Dst Port: 40492, Seq: 34127, Ack: 444, Len: 1369
[20 Reassembled TCP Segments (35495 bytes): #562(176), #565(4074), #567(1358), #569(1358), #571(1358), 
#574(2716), #694(1358), #696(1358), #698(2716), #700(1358), #702(2716), #704(1358), #706(1358), 
#708(1358), #710(2716), #712(1358), #714()]
Hypertext Transfer Protocol
Line-based text data: text/css (2086 lines)
```

3. Using Google Chrome browser:
   GET



```
No.     Time               Source                Destination           Protocol Length Info
      5 20:29:30.314408760 192.168.43.75         203.110.245.244       HTTP     580    GET / HTTP/1.1 
Frame 5: 580 bytes on wire (4640 bits), 580 bytes captured (4640 bits) on interface enp0s3, id 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 25, 2021 20:29:30.314408760 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611586770.314408760 seconds
    [Time delta from previous captured frame: 0.000220218 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.180090651 seconds]
    Frame Number: 5
    Frame Length: 580 bytes (4640 bits)
    Capture Length: 580 bytes (4640 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PcsCompu_02:af:5d (08:00:27:02:af:5d), Dst: Motorola_ba:61:4d (cc:61:e5:ba:61:4d)
Internet Protocol Version 4, Src: 192.168.43.75, Dst: 203.110.245.244
Transmission Control Protocol, Src Port: 55640, Dst Port: 80, Seq: 1, Ack: 1, Len: 514
Hypertext Transfer Protocol
```

OK



```
No.     Time               Source                Destination           Protocol Length Info
    223 20:29:31.296629579 203.110.245.244       192.168.43.75         HTTP     461    HTTP/1.1 200 OK
(text/css)
Frame 223: 461 bytes on wire (3688 bits), 461 bytes captured (3688 bits) on interface enp0s3, id 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 25, 2021 20:29:31.296629579 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611586771.296629579 seconds
    [Time delta from previous captured frame: 0.001058568 seconds]
    [Time delta from previous displayed frame: 0.511831378 seconds]
    [Time since reference or first frame: 1.162311470 seconds]
    Frame Number: 223
    Frame Length: 461 bytes (3688 bits)
    Capture Length: 461 bytes (3688 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Motorola_ba:61:4d (cc:61:e5:ba:61:4d), Dst: PcsCompu_02:af:5d (08:00:27:02:af:5d)
Internet Protocol Version 4, Src: 203.110.245.244, Dst: 192.168.43.75
Transmission Control Protocol, Src Port: 80, Dst Port: 55650, Seq: 8324, Ack: 412, Len: 395
[8 Reassembled TCP Segments (8718 bytes): #207(175), #210(1358), #213(1358), #215(1358), #217(1358),
#219(1358), #221(1358), #223(395)]
Hypertext Transfer Protocol
Line-based text data: text/css (374 lines)
```

2.5 Question 4

For this assignment I've used Mozilla Firefox, Google Chrome and Microsoft Edge.
I was able to see HTTP protocol in all of them.
Also all of them had almost same data with some variations. Like some different packets, different protocols, time latency. It was mostly because of background running processes.
Different protocols present in the given browsers is already mentioned in the first question of part-2.
Different packets are resulted due to different background processes.
In the particular case of these captured packets, using the information of time taken between HTTP GET request and HTTP OK packets, I can say that Microsoft Edge was fastest and Mozilla Firefox was slowest.