

COL-334/672 (COMPUTER NETWORKS)

ASSIGNMENT 1

1 NETWORKING TOOLS

- a. IP address of the machine (basically the IP address of the interface connected to WiFi or Ethernet) can be found directly by using **ipconfig** command in windows.

On connecting to different Internet service providers (ISPs) or even different devices the IP address of the interface is changed as this IP address is not of our pc but is the IP address of the network we are connected to.

IP address using Airtel Broadband: 169.254.48.17

```
Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2401:4900:5d15:acf4:ec0e:67cd:ee2d:3011
Temporary IPv6 Address. . . . . : 2401:4900:5d15:acf4:4dfb:f323:5a57:72e7
Link-local IPv6 Address . . . . . : fe80::ec0e:67cd:ee2d:3011%14
Autoconfiguration IPv4 Address. . : 169.254.48.17
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : fe80::5877:9aff:fecf:45b9%14
```

Ip address using Airtel Mobile Hotspot: 169.254.185.83

```
Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2402:3a80:1bd4:9b81:d8e6:68f:adf9:b953
Temporary IPv6 Address. . . . . : 2402:3a80:1bd4:9b81:fd82:6696:13d9:fe59
Link-local IPv6 Address . . . . . : fe80::d8e6:68f:adf9:b953%14
Autoconfiguration IPv4 Address. . : 169.254.185.83
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : fe80::60af:9fff:fee9:6e0c%14
```

- b. IP address associated with www.google.com and www.facebook.com can be found using **nslookup** command in windows.

IP address of www.google.com using Default server: 172.217.161.4

IP address of www.facebook.com using Default server: 157.240.16.35

```
C:\Users\HARIKESH>nslookup
Default Server: UnKnown
Address: 2401:4900:5d15:acf4::dc

> www.google.com
Server: UnKnown
Address: 2401:4900:5d15:acf4::dc

Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4002:807::2004
172.217.161.4

> www.facebook.com
Server: UnKnown
Address: 2401:4900:5d15:acf4::dc

Non-authoritative answer:
Name: star-mini.c10r.facebook.com
Addresses: 2a03:2880:f12f:83:face:b00c:0:25de
157.240.16.35
Aliases: www.facebook.com
```

Now on using some Open DNS servers from the web the IP address of both of these domain names changes. One important thing to note is that we get response from these open servers only i.e. if we try to obtain IP address of these sites using any private server we will not get any response.

IP address of www.google.com using dns.google.com server: 142.250.182.164

IP address of www.facebook.com using dns.opendns.com server: 157.240.198.35

IP address of www.facebook.com if we try it using some private server: No response

```
C:\Users\HARIKESH>nslookup www.google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     www.google.com
Addresses: 2404:6800:4002:81e::2004
          142.250.182.164

C:\Users\HARIKESH>nslookup www.facebook.com 253.112.112.112
Server:  UnKnown
Address: 253.112.112.112

*** UnKnown can't find www.facebook.com: No response from server

C:\Users\HARIKESH>nslookup www.facebook.com 208.67.220.220
Server:  dns.opendns.com
Address: 208.67.220.220

Non-authoritative answer:
Name:     star-mini.c10r.facebook.com
Addresses: 2a03:2880:f144:82:face:b00c:0:25de
          157.240.198.35
Aliases:  www.facebook.com
```

- c. For ping the IP address of www.iitd.ac.in we can directly use the **ping** command in windows. Directly using **>>ping www.iitd.ac.in** gives us the required results.
- Using the command with -l flag **>>ping -l 230 www.iitd.ac.in** changes the packet size to 230 bytes and the default size is 32 bytes.
- Using the command with -i flag **>>ping -i 150 www.iitd.ac.in** changes the TTL values and one important thing to note is that the TTL value shown after executing the command is the TTL value of the packets received and is thus not controlled by us but is defined by server while the TTL value we are setting is the TTL values of packets sent.

For finding the maximum size of the ping packet that we can send on www.iitd.ac.in we just start increasing the size of packets using -l flag and then narrow down the range and try to find the exact ping packet size in bytes that we are able to send and it is nearly 35000 bytes and it varies every time but is closely near 35000 bytes. (One of these results is shown in the figure below).

Does this packet size same for all other domains? Simply no, because as we try to increase size of ping packets of www.google.com and www.facebook.com we see that the max size of ping packet that we can send on www.google.com and www.facebook.com is very much less than that of www.iitd.ac.in. One of the reasons why the maximum ping packet size changes with different domains is that these are the ethernet protocols and can depend on the domains itself like what maximum data flow they are allowing.

Pinging the IP address of www.iitd.ac.in with different packet sizes, TTL values

```
C:\Users\HARIKESH>ping www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: bytes=32 time=50ms TTL=50
Reply from 103.27.9.24: bytes=32 time=219ms TTL=50
Reply from 103.27.9.24: bytes=32 time=278ms TTL=50
Reply from 103.27.9.24: bytes=32 time=62ms TTL=50
```

```
Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 278ms, Average = 152ms
```

```
C:\Users\HARIKESH>ping -l 230 www.iitd.ac.in
```

```
Pinging www.iitd.ac.in [103.27.9.24] with 230 bytes of data:
Reply from 103.27.9.24: bytes=230 time=63ms TTL=50
Reply from 103.27.9.24: bytes=230 time=494ms TTL=50
Reply from 103.27.9.24: bytes=230 time=35ms TTL=50
Reply from 103.27.9.24: bytes=230 time=79ms TTL=50
```

```
Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 494ms, Average = 167ms
```

```
C:\Users\HARIKESH>ping -i 150 www.iitd.ac.in
```

```
Pinging www.iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: bytes=32 time=879ms TTL=50
Reply from 103.27.9.24: bytes=32 time=947ms TTL=50
Reply from 103.27.9.24: bytes=32 time=439ms TTL=50
Reply from 103.27.9.24: bytes=32 time=43ms TTL=50
```

```
Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 947ms, Average = 577ms
```

I Finding the maximum ping packet size that can be sent on www.iitd.ac.in (actually range)

II Comparing the maximum packet size with different other domains like www.google.com

```
C:\Users\HARIKESH>ping 35500 www.iitd.ac.in
Bad parameter www.iitd.ac.in.
```

```
C:\Users\HARIKESH>ping -l 35500 www.iitd.ac.in
```

```
Pinging www.iitd.ac.in [103.27.9.24] with 35500 bytes of data:
Reply from 103.27.9.24: bytes=35500 time=205ms TTL=50
Reply from 103.27.9.24: bytes=35500 time=154ms TTL=50
Reply from 103.27.9.24: bytes=35500 time=168ms TTL=50
Reply from 103.27.9.24: bytes=35500 time=724ms TTL=50
```

```
Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 154ms, Maximum = 724ms, Average = 312ms
```

```
C:\Users\HARIKESH>ping -l 36000 www.iitd.ac.in
```

```
Pinging www.iitd.ac.in [103.27.9.24] with 36000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 103.27.9.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\HARIKESH>ping -l 2000 www.google.com
```

```
Pinging www.google.com [2404:6800:4002:81e::2004] with 2000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 2404:6800:4002:81e::2004:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

d. Tracerouting of www.iitd.ac.in can be done in windows using **tracert** command.

One of my ISP was blocking packets on the path to www.iitd.ac.in hence i have tracerouted www.iitd.ac.in using only 1 ISP provider while ran traceroute on www.google.com using other both ISP providers.

If some paths default to IPV6 we can force tracerout to use IPV4 using -4 flag in the command and vice-verca. In case of www.iitd.ac.in it was by default all IPV4 hence I used this in www.google.com

Running tracert on www.iitd.ac.in with default conditions

```
C:\Users\HARIKESH>tracert www.iitd.ac.in

Tracing route to www.iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  0  *          *          *          Request timed out.
  1  233 ms    325 ms    127 ms    192.168.29.10
  2  60 ms     30 ms     29 ms     192.168.28.157
  3  69 ms     33 ms     38 ms     192.168.31.3
  4  40 ms     33 ms     40 ms     192.168.31.9
  5  25 ms     29 ms     34 ms     192.168.31.49
  6  *          *          *          Request timed out.
  7  45 ms     68 ms     46 ms     nsg-corporate-157.38.187.122.airtel.in [122.187.38.157]
  8  40 ms     43 ms     111 ms    182.79.153.83
  9  65 ms     38 ms     52 ms     115.110.232.173.static.Delhi.vsnl.net.in [115.110.232.173]
 10  *          *          *          Request timed out.
 11  44 ms     61 ms     79 ms     14.140.210.22.static-Delhi-vsnl.net.in [14.140.210.22]
 12  38 ms     45 ms     52 ms     10.119.234.161
 13  100 ms    55 ms     54 ms     10.119.233.65
 14  59 ms     37 ms     66 ms     10.119.233.66
 15  51 ms     40 ms     46 ms     103.27.9.24
 16  54 ms     36 ms     41 ms     103.27.9.24
 17  56 ms     39 ms     38 ms     103.27.9.24

Trace complete.
```

I Running tracert on www.google.com using Airtel(ISP) Broadband

II Running tracert on www.google.com using Airtel Mobile hotspot

```
C:\Users\HARIKESH>tracert www.google.com

Tracing route to www.google.com [142.250.194.100]
over a maximum of 30 hops:

  0  *          *          *          Request timed out.
  1  143 ms    212 ms    207 ms    192.168.29.10
  2  49 ms     33 ms     87 ms     192.168.28.73
  3  55 ms     30 ms     44 ms     192.168.31.25
  4  45 ms     54 ms     65 ms     192.168.31.27
  5  69 ms     34 ms     60 ms     192.168.31.33
  6  *          *          *          Request timed out.
  7  59 ms     417 ms    55 ms     nsg-corporate-157.38.187.122.airtel.in [122.187.38.157]
  8  119 ms    60 ms     66 ms     116.119.61.251
  9  59 ms     45 ms     52 ms     142.250.161.56
 10  92 ms     61 ms     97 ms     142.251.66.171
 11  68 ms     41 ms     66 ms     142.251.52.225
 12  174 ms    265 ms    66 ms     dell2s04-in-f4.1e100.net [142.250.194.100]

Trace complete.

C:\Users\HARIKESH>tracert -4 www.google.com

Tracing route to www.google.com [2404:6800:4007:81c::2004]
over a maximum of 30 hops:

  0  1 ms      1 ms      1 ms      2401:4900:5d12:8d00::99
  1  *          *          *          Request timed out.
  2  79 ms     195 ms    43 ms     2401:4900:c:893::1
  3  *          *          *          Request timed out.
  4  51 ms     37 ms     48 ms     2404:a800:1a00:800::25
  5  66 ms     56 ms     79 ms     2404:a800::207
  6  *          *          *          Request timed out.
  7  100 ms    69 ms     70 ms     2404:6800:811c::1
  8  74 ms     *          74 ms     2001:4860:0:9e::1
  9  61 ms     67 ms     63 ms     2001:4860:0:9e::4
 10  165 ms    92 ms     80 ms     2001:4860::9:4001:67bc
 11  98 ms     100 ms    91 ms     2001:4860::9:4001:163c
 12  102 ms    90 ms     88 ms     2001:4860:0:1::5663
 13  98 ms     88 ms     105 ms    maa05s21-in-x04.1e100.net [2404:6800:4007:81c::2004]

Trace complete.
```

Running tracer on www.google.com by forcing it to use IPV4 only

Command Used: **tracert -4 www.google.com**

```
C:\Users\HARIKESH>tracert www.google.com

Tracing route to www.google.com [2404:6800:4007:81c::2004]
over a maximum of 30 hops:

  1  1 ms  1 ms  1 ms  2401:4900:5d12:8d00::99
  2  *      *      *      Request timed out.
  3  79 ms  195 ms  43 ms  2401:4900:c:893::1
  4  *      *      *      Request timed out.
  5  51 ms  37 ms  48 ms  2404:a800:1a00:800::25
  6  66 ms  56 ms  79 ms  2404:a800::207
  7  *      *      *      Request timed out.
  8  100 ms  69 ms  70 ms  2404:6800:811e::1
  9  74 ms  *      74 ms  2001:4860:0:9e::1
 10  61 ms  67 ms  63 ms  2001:4860:0:9e::4
 11  165 ms  92 ms  80 ms  2001:4860::9:4001:67bc
 12  98 ms  100 ms  91 ms  2001:4860::9:4001:163c
 13  107 ms  90 ms  88 ms  2001:4860:0:1:5663
 14  98 ms  88 ms  105 ms  maa05s21-in-x04.1e100.net [2404:6800:4007:81c::2004]

Trace complete.

C:\Users\HARIKESH>tracert -4 www.google.com

Tracing route to www.google.com [142.250.194.100]
over a maximum of 30 hops:

  1  3 ms  2 ms  2 ms  192.168.252.109
  2  52 ms  464 ms  154 ms  192.168.29.10
  3  114 ms  30 ms  44 ms  192.168.28.101
  4  52 ms  45 ms  42 ms  192.168.31.10
  5  75 ms  29 ms  40 ms  192.168.31.3
  6  41 ms  39 ms  55 ms  192.168.31.33
  7  *      *      *      Request timed out.
  8  44 ms  36 ms  48 ms  ns-g-corporate-157.38.187.122.airtel.in [122.187.38.157]
  9  63 ms  91 ms  66 ms  116.119.73.32
 10  70 ms  48 ms  68 ms  142.250.161.56
 11  51 ms  51 ms  46 ms  142.251.66.171
 12  69 ms  450 ms  50 ms  142.251.52.225
 13  75 ms  66 ms  64 ms  del12s04-in-f4.1e100.net [142.250.194.100]

Trace complete.
```


2 PACKET ANALYSIS

Installed wireshark and analysed protocols being used along with flushing the local DNS cache and clearing the Browser cache.

Captured packets while visiting <http://apache.org> using wireshark

- a. Applied a dns filter on the packet trace and DNS request response time is the time to get response from the main domain i.e. apache.org and in total there are 4 such authoritative name servers and on an average all will take approx. same time to get responded. So, time taken for responding dns request response i.e. dns.time == 0.244309000 seconds.

The screenshot shows a Wireshark capture of DNS traffic. The packet list pane displays a series of packets, with the selected packet being a DNS query for 'apache.org'. The packet details pane shows the query structure, including the question section with 'apache.org. type AAAA, class IN, addr 2a04:4e42::644'. The packet bytes pane shows the raw data of the packet, including the query and response sections.

No.	Time	Source	Destination	Protocol	Length	Info
25	2.408875	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	90	Standard query 0x6312 A apache.org
26	2.409120	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	90	Standard query 0x6fd1 AAAA apache.org
27	2.538835	192.168.43.242	192.168.43.1	DNS	70	Standard query 0x6312 A apache.org
28	2.538847	192.168.43.242	192.168.43.1	DNS	70	Standard query 0x6fd1 AAAA apache.org
29	2.729353	192.168.43.1	192.168.43.242	DNS	86	Standard query response 0x6312 A apache.org A 151.101.2.132
30	2.739571	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	106	Standard query response 0x6312 A apache.org A 151.101.2.132
32	2.778320	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	255	Standard query response 0x6fd1 AAAA apache.org AAAA 2a04:4e42::644 NS ns-1139.awsdns-14.org NS ns-1955.awsdns-52.co.uk NS ns-303.awsdns-37.com NS ns-558.awsdns-05.net
34	2.783156	192.168.43.1	192.168.43.242	DNS	235	Standard query response 0x6fd1 AAAA apache.org AAAA 2a04:4e42::644 NS ns-1139.awsdns-14.org NS ns-1955.awsdns-52.co.uk NS ns-303.awsdns-37.com
60	2.998709	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	100	Standard query 0x79e7 A fonts.googleapis.com
61	2.999408	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	100	Standard query 0xfbb8 AAAA fonts.googleapis.com
65	3.004567	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	97	Standard query 0x5c3a A www.apachecon.com
66	3.004568	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	94	Standard query 0x4cde A cse.google.com
67	3.004939	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	97	Standard query 0x964c AAAA www.apachecon.com
68	3.005055	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	94	Standard query 0x1487 AAAA cse.google.com
72	3.053079	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	116	Standard query response 0x79e7 A fonts.googleapis.com A 142.250.196.10

Authority RRs: 4
Additional RRs: 0
Queries: 0
Answers: 0
Authoritative nameservers: 0
Request In: 28
[Time: 0.244309000 seconds]

- b. Applied an http filter and total number of http requests made while visiting <http://apache.org> are approximately 52.

Any webpage consist of a lot of files, images, and for accessing each and every file browser asserts a query which is bacially an http request to get the data. All these images, adds, videos and chunks of data are retrieved when the web browser is accessed through http requests and then the response of original query is sent back along with the data obtained here.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
39	2.862285	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	512	GET / HTTP/1.1
59	2.993715	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	740	HTTP/1.1 200 OK (text/html)
71	3.008775	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	415	GET /css/min.bootstrap.css HTTP/1.1
83	3.083585	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	408	GET /css/styles.css HTTP/1.1
86	3.084394	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	462	GET /img/support-apache.jpg HTTP/1.1
87	3.084558	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	466	GET /img/asf-estd-1999-logo.jpg HTTP/1.1
111	3.112878	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	499	GET /img/trillions-and-trillions/apache-everywhere-thumbnail.jpg HTTP/1.1
112	3.112881	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	491	GET /img/trillions-and-trillions/why-apache-thumbnail.jpg HTTP/1.1
125	3.212838	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	221	HTTP/1.1 200 OK (text/css)
141	3.217206	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	401	GET /js/jquery-2.1.1.min.js HTTP/1.1
172	3.248801	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	221	HTTP/1.1 200 OK (text/css)
175	3.252281	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	394	GET /js/bootstrap.js HTTP/1.1
186	3.254866	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	1416	HTTP/1.1 200 OK (JPEG JFIF image)
192	3.257815	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	394	GET /js/slideshow.js HTTP/1.1
256	3.325787	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	794	HTTP/1.1 200 OK (JPEG JFIF image)
262	3.329356	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	505	GET /img/trillions-and-trillions/trillions-and-trillions-thumbnail.jpg HTTP/1.1
266	3.334402	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	945	HTTP/1.1 200 OK (JPEG JFIF image)
268	3.337710	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	499	GET /img/trillions-and-trillions/apache-innovation-thumbnail.jpg HTTP/1.1
314	3.370333	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	460	HTTP/1.1 200 OK (JPEG JFIF image)
316	3.372161	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	459	GET /img/2020-report.jpg HTTP/1.1
324	3.387236	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	724	HTTP/1.1 200 OK (application/javascript)
332	3.391866	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	457	GET /img/community.jpg HTTP/1.1
344	3.407927	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	913	HTTP/1.1 200 OK (application/javascript)
359	3.409064	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	599	HTTP/1.1 200 OK (application/javascript)
361	3.411630	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	462	GET /img/the-apache-way.jpg HTTP/1.1
362	3.412408	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	457	GET /img/ApacheCon.jpg HTTP/1.1
421	3.469615	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	883	HTTP/1.1 200 OK (JPEG JFIF image)
424	3.469615	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	1423	HTTP/1.1 200 OK (JPEG JFIF image)
432	3.472924	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	467	GET /logos/res/camel/default.png HTTP/1.1
433	3.473523	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	467	GET /logos/res/http/default.png HTTP/1.1
502	3.526900	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	298	HTTP/1.1 200 OK (JPEG JFIF image)
508	3.529673	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	491	GET /foundation/press/kit/poweredby/Apache_PoweredBy.svg HTTP/1.1
668	3.711856	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	610	HTTP/1.1 200 OK (JPEG JFIF image)
678	3.714645	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	467	GET /fonts/glyphicons-halflings-regular.woff2 HTTP/1.1
736	3.755694	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	864	HTTP/1.1 200 OK (PNG)
748	3.759450	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	465	GET /logos/res/hop/default.png HTTP/1.1
757	3.766720	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	673	HTTP/1.1 200 OK (PNG)

Frame 20: 512 bytes on wire (A096 bits) 512 bytes captured (A096 bits) on interface \Device\NPF{53FCE5CF-D6FE-A55D-B348-D085A8FF1831} id 0

Transmission Control Protocol (tcp), 20 bytes

Packets: 2360 - Displayed: 52 (2.2%) - Dropped: 0 (0.0%) Profile: Default

17:59 22-08-2021

- c. Now, we have to find the total time taken to download the entire webpage . This is actually the time between the first dns request made and last content object received i.e. last image, objects were approached which are basically http requests. So, time taken is $7.232613 - 2.408875 = 4.8237$ seconds.

748	3.759450	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	465	GET /logos/res/hop/default.png HTTP/1.1
757	3.766720	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	673	HTTP/1.1 200 OK (PNG)
776	3.770704	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	468	GET /logos/res/flagon/default.png HTTP/1.1
781	3.778726	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP/X...	544	HTTP/1.1 200 OK
790	3.782188	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	469	GET /logos/res/datalab/default.png HTTP/1.1
802	3.784935	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	591	HTTP/1.1 200 OK (JPEG JFIF image)
816	3.818788	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	454	HTTP/1.1 200 OK (JPEG JFIF image)
828	3.819561	2401:4900:5d13:1a48...	2a04:6800:4007:814:...	HTTP	426	GET /cse-js?cx=005703438322411770421:5mgshgrgx2u HTTP/1.1
872	3.894047	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	384	HTTP/1.1 200 OK (font/woff2)
981	4.190078	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	1456	HTTP/1.1 200 OK (PNG)
994	4.228862	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	1219	HTTP/1.1 200 OK (PNG)
1003	4.263911	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	987	HTTP/1.1 200 OK (PNG)
1078	4.384143	2404:6800:4007:814:...	2401:4900:5d13:1a48...	HTTP	670	HTTP/1.1 404 Not Found (text/html)
2344	7.055514	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	460	GET /favicons/favicon.ico HTTP/1.1
2349	7.142349	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	832	HTTP/1.1 200 OK (PNG)
2351	7.146079	2401:4900:5d13:1a48...	2a04:4e42::644	HTTP	466	GET /favicons/favicon-32x32.png HTTP/1.1
2355	7.232613	2a04:4e42::644	2401:4900:5d13:1a48...	HTTP	124	HTTP/1.1 200 OK (PNG)

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
25	2.408875	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	90	Standard query 0x6312 A apache.org
26	2.409120	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	90	Standard query 0x6fd1 AAAA apache.org
27	2.538835	192.168.43.242	192.168.43.1	DNS	70	Standard query 0x6312 A apache.org
28	2.538847	192.168.43.242	192.168.43.1	DNS	70	Standard query 0x6fd1 AAAA apache.org
29	2.729353	192.168.43.1	192.168.43.242	DNS	86	Standard query response 0x6312 A apache.org A 151.101.2.132
30	2.739571	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	106	Standard query response 0x6fd1 A apache.org A 151.101.2.132
32	2.778320	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	255	Standard query response 0x6fd1 AAAA apache.org AAAA 2a04:4e42::644 NS ns-1139.awsdns-14.org NS ns-1955.awsdns-52.co.uk NS ns-3...
34	2.783156	192.168.43.1	192.168.43.242	DNS	235	Standard query response 0x6fd1 AAAA apache.org AAAA 2a04:4e42::644 NS ns-1139.awsdns-14.org NS ns-1955.awsdns-52.co.uk NS ns-3...
60	2.998709	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	100	Standard query 0x79e7 A fonts.googleapis.com
61	2.999408	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	100	Standard query 0xfbb8 AAAA fonts.googleapis.com
65	3.004567	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	97	Standard query 0x5c3a A www.apachecon.com
66	3.004568	2401:4900:5d13:1a48...	2401:4900:5d13:1a48...	DNS	94	Standard query 0x4cde A cse.google.com

d. Now, we will be running packet trace for <http://www.cse.iitd.ac.in> and then will be filtering it for http.

Total http requests obtained are 2 and there is no other http traffic.

In case of <http://apache.org> we were getting more http traffic as compared to <http://www.cse.iitd.ac.in> this tells us that the former webpage is more structured i.e. contains more files, images and is complex compared to the latter.

