=====================================

Assignment 1 (Part A) Submission

Name: Prasanna Paithankar

Roll number: 21CS30065

Link of the pcap file: <https://drive.google.com/file/d/11V27bAD8dOMC93wPsW5tbIxOB_eWiamp/view?usp=sharing>

=====================================

1. How many packets do you see for the following protocols?

a. TCP and UDP together

TCP: 15856

UDP: 298

Total: 16154

b. IPv4 and IPv6?

IPv4: 16154

IPv6: 0

2. What is the total amount of data being received for the following two cases?

a. When you access <http://iitkgp.ac.in> : 10540183 bytes

b. When you access https://www.cornell.edu : 3606690 bytes

3. How many DNS packets have you observed in total?

Ans. 210 packets.

a. Create a <Domain Name, IP> table by exploring the queries and the answers in

those DNS packets. The Domain Name will be the domain for which you see a

query, and the IP address will be the address that is being returned against the

corresponding query.

Ans. Use tshark -r [pcap filename] -z host -q > hostadd.txt

|  |  |
| --- | --- |
| **IP** | **Domain** |
| 151.101.194.137 | code.jquery.com |
| 163.70.143.4 | scontent-bom2-1.xx.fbcdn.net |
| 91.189.91.48 | connectivity-check.ubuntu.com |
| 104.17.25.14 | cdnjs.cloudflare.com |
| 142.250.77.206 | youtube-ui.l.google.com |
| 142.250.207.238 | youtube-ui.l.google.com |
| 172.217.167.22 | i.ytimg.com |
| 91.189.91.49 | connectivity-check.ubuntu.com |
| 172.217.27.202 | content-autofill.googleapis.com |
| 31.13.79.26 | scontent-bom1-2.xx.fbcdn.net |
| 216.239.36.178 | www-alv.google-analytics.com |
| 216.239.32.178 | www-alv.google-analytics.com |
| 142.250.77.246 | i.ytimg.com |
| 142.251.42.42 | content-autofill.googleapis.com |
| 172.217.194.154 | stats.g.doubleclick.net |
| 142.250.193.54 | i.ytimg.com |
| 142.250.193.246 | i.ytimg.com |
| 192.229.237.25 | cs491.wac.edgecastcdn.net |
| 142.250.193.67 | update.googleapis.com |
| 35.224.170.84 | connectivity-check.ubuntu.com |
| 142.250.67.202 | content-autofill.googleapis.com |
| 172.217.166.206 | youtube-ui.l.google.com |
| 152.199.43.83 | cs510.wpc.edgecastcdn.net |
| 216.58.196.206 | youtube-ui.l.google.com |
| 172.217.194.155 | stats.g.doubleclick.net |
| 142.250.183.10 | optimizationguide-pa.googleapis.com |
| 142.250.183.138 | optimizationguide-pa.googleapis.com |
| 142.250.183.74 | content-autofill.googleapis.com |
| 142.250.199.138 | ajax.googleapis.com |
| 142.250.193.42 | jnn-pa.googleapis.com |
| 142.250.193.234 | jnn-pa.googleapis.com |
| 180.149.59.145 | a1874.dscg1.akamai.net |
| 185.125.190.17 | connectivity-check.ubuntu.com |
| 142.250.192.238 | youtube-ui.l.google.com |
| 142.250.194.206 | youtube-ui.l.google.com |
| 172.217.194.156 | stats.g.doubleclick.net |
| 172.217.166.246 | i.ytimg.com |
| 185.125.190.18 | connectivity-check.ubuntu.com |
| 104.244.43.131 | abs-zero.twimg.com |
| 172.217.194.157 | stats.g.doubleclick.net |
| 172.217.160.202 | optimizationguide-pa.googleapis.com |
| 172.217.166.42 | optimizationguide-pa.googleapis.com |
| 172.217.166.170 | content-autofill.googleapis.com |
| 172.64.192.27 | siteimproveanalytics.com |
| 180.149.59.147 | a1988.dscg1.akamai.net |
| 142.250.182.182 | i.ytimg.com |
| 142.250.206.118 | i.ytimg.com |
| 163.70.143.35 | star-mini.c10r.facebook.com |
| 142.250.194.131 | fonts.gstatic.com |
| 142.250.76.202 | content-autofill.googleapis.com |
| 172.217.167.206 | youtube-ui.l.google.com |
| 51.21.125.30 | ana-collector-alb-eu-iron-829160369.eu-north-1.elb.amazonaws.co |
| 142.250.182.170 | jnn-pa.googleapis.com |
| 142.250.182.234 | optimizationguide-pa.googleapis.com |
| 142.250.194.106 | jnn-pa.googleapis.com |
| 142.250.194.42 | jnn-pa.googleapis.com |
| 142.250.192.74 | content-autofill.googleapis.com |
| 142.250.192.10 | content-autofill.googleapis.com |
| 142.250.192.138 | content-autofill.googleapis.com |
| 142.250.192.202 | jnn-pa.googleapis.com |
| 142.251.42.72 | ssl.google-analytics.com |
| 142.250.206.170 | jnn-pa.googleapis.com |
| 142.250.206.106 | jnn-pa.googleapis.com |
| 142.250.77.238 | youtube-ui.l.google.com |
| 104.244.42.8 | syndication.twitter.com |
| 104.244.42.200 | syndication.twitter.com |
| 104.244.42.136 | syndication.twitter.com |
| 104.244.42.72 | syndication.twitter.com |
| 142.250.183.129 | photos-ugc.l.googleusercontent.com |
| 142.250.195.14 | youtube-ui.l.google.com |
| 142.250.207.206 | youtube-ui.l.google.com |
| 13.51.8.45 ana- | collector-alb-eu-iron-829160369.eu-north-1.elb.amazonaws.co |
| 172.217.167.246 | i.ytimg.com |
| 142.250.207.232 | www.googletagmanager.com |
| 216.239.38.178 | www-alv.google-analytics.com |
| 216.239.34.178 | www-alv.google-analytics.com |
| 142.250.77.214 | i.ytimg.com |
| 13.107.213.72 | part-0044.t-0009.t-msedge.net |
| 142.251.42.74 | content-autofill.googleapis.com |
| 172.64.193.27 | siteimproveanalytics.com |
| 142.250.193.214 | i.ytimg.com |
| 142.250.193.86 | i.ytimg.com |
| 142.250.193.22 | i.ytimg.com |
| 142.250.192.230 | static.doubleclick.net |
| 185.125.190.48 | connectivity-check.ubuntu.com |
| 142.250.71.106 | content-autofill.googleapis.com |
| 142.250.67.234 | content-autofill.googleapis.com |
| 142.250.77.202 | jnn-pa.googleapis.com |
| 180.149.59.138 | a1874.dscg1.akamai.net |
| 142.251.175.84 | accounts.google.com |
| 192.229.237.96 | cs672.wac.edgecastcdn.net |
| 142.250.183.170 | safebrowsing.googleapis.com |
| 142.250.183.106 | content-autofill.googleapis.com |
| 142.250.193.74 | jnn-pa.googleapis.com |
| 142.250.193.202 | jnn-pa.googleapis.com |
| 142.250.193.10 | jnn-pa.googleapis.com |
| 104.17.24.14 | cdnjs.cloudflare.com |
| 185.125.190.49 | connectivity-check.ubuntu.com |
| 172.217.160.194 | googleads.g.doubleclick.net |
| 142.250.193.36 | www.google.com |
| 157.240.16.20 | scontent-bom1-1.xx.fbcdn.net |
| 172.16.3.10 | www.iitkgp.ac.in |
| 142.250.182.174 | youtube-ui.l.google.com |
| 142.250.194.238 | youtube-ui.l.google.com |
| 142.250.192.206 | youtube-ui.l.google.com |
| 34.122.121.32 | connectivity-check.ubuntu.com |
| 23.205.218.112 | e4350.g.akamaiedge.net |
| 216.58.200.214 | i.ytimg.com |
| 35.232.111.17 | connectivity-check.ubuntu.com |
| 172.217.166.74 | content-autofill.googleapis.com |
| 13.107.246.72 | part-0044.t-0009.t-msedge.net |
| 172.217.27.174 | youtube-ui.l.google.com |
| 142.250.192.246 | i.ytimg.com |
| 142.250.192.182 | i.ytimg.com |
| 151.101.153.229 | jsdelivr.map.fastly.net |
| 142.250.206.150 | i.ytimg.com |
| 142.250.194.35 | www.gstatic.com |
| 151.101.2.137 | code.jquery.com |
| 172.217.161.14 | youtube-ui.l.google.com |
| 172.217.167.46 | play.google.com |
| 151.101.66.137 | code.jquery.com |
| 216.58.221.46 | youtube-ui.l.google.com |
| 151.101.130.137 | code.jquery.com |
| 142.250.182.202 | optimizationguide-pa.googleapis.com |
| 142.250.194.10 | jnn-pa.googleapis.com |
| 142.250.192.234 | jnn-pa.googleapis.com |
| 142.250.194.74 | jnn-pa.googleapis.com |
| 142.250.192.42 | content-autofill.googleapis.com |
| 142.250.192.106 | content-autofill.googleapis.com |
| 142.250.206.138 | jnn-pa.googleapis.com |

b. Can you find out the IP of the DNS servers by exploring the DNS packets?

Ans: Yes. It can be found by noting the Destination in Standard query or the Source in Standard query response. For my analysed pcap file it is 172.16.1.166

4. Answer the following when you access the site http://iitkgp.ac.in

a. How many HTTP GET requests do you observe? List down the GET requests.

Ans. Only 1 HTTP GET request to <http://connectivity-check.ubuntu.com/>

b. For each of the HTTP GET requests you see above, find out

(ii) The total number of TCP segments being received

Ans. 1

(ii) The total amount of data being received in the corresponding HTTP Response message.

Ans. TCP segment length is 189 bytes (also 20 bytes for IPv4 header and total 255 bytes of frame).