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

Assignment 1 (Part A) Submission

Name: Apoorv Kumar

Roll number: 21CS10008

Link of the pcap file: <https://drive.google.com/file/d/1d3R_v19Fhlao2MF8EjNXT0NrIAusvjBh/view?usp=sharing>

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

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

a. TCP and UDP together

8603 packets (TCP: 8216 packets and UDP: 387 packets)

b. IPv4 and IPv6?

IPv4: 8603 packets

IPv6: 0 packet

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

a. When you access http://iitkgp.ac.in (got it’s IP address: 172.16.3.10)

933 kB

b. When you access https://www.cornell.edu (got it’s IP address: 13.107.246.68)

43 kB

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

309 DNS 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.

| **Domain Name** | **IP** |
| --- | --- |
| [**a1874.dscgl.akamai.net**](http://a1874.dscgl.akamai.net) | 180.149.59.138 |
| [**a1874.dscg1.akamai.net**](http://a1874.dscg1.akamai.net) | 180.149.59.145 |
| [**a1988.dscg1.akamai.net**](http://a1988.dscg1.akamai.net) | 180.149.59.147 |
| [**ana-collector-alb-eu-iron-829160369.eu-north-1.elb.amazonaws.co**](http://ana-collector-alb-eu-iron-829160369.eu-north-1.elb.amazonaws.co) | 51.21.125.30 |
| [**ana-collector-alb-eu-iron-829160369.eu-north-1.elb.amazonaws.co**](http://ana-collector-alb-eu-iron-829160369.eu-north-1.elb.amazonaws.co) | 13.51.8.45 |
| [**apac-in-courier-4.push-apple.com.akadns.net**](http://apac-in-courier-4.push-apple.com.akadns.net) | 17.57.145.119 |
| [**apac-in-courier-4.push-apple.com.akadns.net**](http://apac-in-courier-4.push-apple.com.akadns.net) | 17.57.145.120 |
| [**apac-in-courier-4.push-apple.com.akadns.net**](http://apac-in-courier-4.push-apple.com.akadns.net) | 17.57.145.118 |
| [**apna.litkgp.ac.in**](http://apna.litkgp.ac.in) | 10.3.100.171 |
| [**apse1-wps-prod.apple.com**](http://apse1-wps-prod.apple.com) | 17.8.131.124 |
| [**apsel-wps-prod.apple.com**](http://apsel-wps-prod.apple.com) | 17.8.131.163 |
| [**apsel-wps-prod.apple.com**](http://apsel-wps-prod.apple.com) | 17.8.131.15 |
| [**beta.iitkgp.ac.in**](http://beta.iitkgp.ac.in) | 10.3.100.102 |
| [**cdnjs.cloudflare.com**](http://cdnjs.cloudflare.com) | 104.17.24.14 |
| [**cdnjs.cloudflare.com**](http://cdnjs.cloudflare.com) | 104.17.25.14 |
| [**cdnjs.cloudflare.com**](http://cdnjs.cloudflare.com) | 2606:4700::6811:180e |
| [**cdnjs.cloudflare.com**](http://cdnjs.cloudflare.com) | 2606:4700::6811:190e |
| [**code.jquery.com**](http://code.jquery.com) | 151.101.66.137 |
| [**code.jquery.com**](http://code.jquery.com) | 151.101.2.137 |
| [**code.jquery.com**](http://code.jquery.com) | 151.101.194.137 |
| [**code.jquery.com**](http://code.jquery.com) | 151.101.130.137 |
| [**code.jquery.com**](http://code.jquery.com) | 2a04:442::649 |
| [**code.jquery.com**](http://code.jquery.com) | 2a04:442:200::649 |
| [**code.jquery.com**](http://code.jquery.com) | 2a04:442:600::649 |
| [**code.jquery.com**](http://code.jquery.com) | 2a04:442:400::649 |
| [**cs491.wac.edgecastcdn.net**](http://cs491.wac.edgecastcdn.net) | 192.229.237.25 |
| [**cs491.wac.edgecastcdn.net**](http://cs491.wac.edgecastcdn.net) | 2606:2800:248:2f:1d8a:787:dc7:17df |
| [**e4350.g.akamaiedge.net**](http://e4350.g.akamaiedge.net) | 23.201.133.134 |
| [**e9959.dsce9.akamaiedge.net**](http://e9959.dsce9.akamaiedge.net) | 23.32.176.130 |
| [**erp.iitkgp.ac.in**](http://erp.iitkgp.ac.in) | 10.57.7.11 |
| [**erp.iitkgp.ac.in**](http://erp.iitkgp.ac.in) | 10.57.7.12 |
| [**gateoffice.itkgp.ac.in**](http://gateoffice.itkgp.ac.in) | 203.110.245.11 |
| [**gateway.fe2.apple-dns.net**](http://gateway.fe2.apple-dns.net) | 17.248.239.65 |
| [**googleads.g.doubleclick.net**](http://googleads.g.doubleclick.net) | 142.250.194.194 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.70.118 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.70.86 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.70.54 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.192.118 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.192.86 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.192.22 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.192.54 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.192.150 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.199.182 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.183.86 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.183.54 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.183.118 |
| [**i.ytimg.com**](http://i.ytimg.com) | 172.217.167.182 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.251.42.22 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.251.42.118 |
| [**i.ytimg.com**](http://i.ytimg.com) | 142.250.67.182 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.76.202 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 216.58.203.42 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 172.217.166.170 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 172.217.166.74 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.77.42 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.192.138 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.192.106 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.192.10 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.192.42 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.192.74 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.183.74 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.250.183.106 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.251.42.42 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 172.217.174.74 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 142.251.42.74 |
| [**jnn-pa.googleapis.com**](http://jnn-pa.googleapis.com) | 172.217.27.202 |
| [**jsdelivr.map.fastly.net**](http://jsdelivr.map.fastly.net) | 199.232.21.229 |
| [**jsdelivr.map.fastly.net**](http://jsdelivr.map.fastly.net) | 2a04:442:42::485 |
| [**I-0005.I-dc-msedge.net**](http://i-0005.i-dc-msedge.net) | 13.107.43.14 |
| [**I-0005.I-dc-msedge.net**](http://i-0005.i-dc-msedge.net) | 2620:1ec:22::14 |
| [**library.itkgp.ac.in**](http://library.itkgp.ac.in) | 10.18.24.7 |
| [**mail.google.com**](http://mail.google.com) | 142.250.182.165 |
| [**mail.google.com**](http://mail.google.com) | 2404:6800:4002:815::2005 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.7 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.103 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.39 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.100 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.36 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.132 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.40 |
| [**mask.apple-dns.net**](http://mask.apple-dns.net) | 17.248.162.8 |
| [**ncwwomenhelpline.in**](http://ncwwomenhelpline.in) | 18.164.202.59 |
| [**ncwwomenhelpline.in**](http://ncwwomenhelpline.in) | 18.164.202.24 |
| [**ncwwomenhelpline.in**](http://ncwwomenhelpline.in) | 18.164.202.108 |
| [**ncwwomenhelpline.in**](http://ncwwomenhelpline.in) | 18.164.202.99 |
| [**nvsp.in**](http://nvsp.in) | 61.0.172.246 |
| [**ocsp2.g.aaplimg.com**](http://ocsp2.g.aaplimg.com) | 17.253.18.196 |
| [**ocsp2.g.aaplimg.com**](http://ocsp2.g.aaplimg.com) | 17.253.18.195 |
| [**part-0040.t-0009.t-msedge.net**](http://part-0040.t-0009.t-msedge.net) | 13.107.246.68 |
| [**part-0040.t-0009.t-msedge.net**](http://part-0040.t-0009.t-msedge.net) | 13.107.213.68 |
| [**pki-goog.l.google.com**](http://pki-goog.l.google.com) | 142.250.194.131 |
| [**pki-goog.l.google.com**](http://pki-goog.l.google.com) | 142.250.193.195 |
| [**play.google.com**](http://play.google.com) | 172.217.166.14 |
| [**proxy-ssl-geo.webflow.com**](http://proxy-ssl-geo.webflow.com) | 65.0.79.182 |
| [**proxy-ssl-geo.webflow.com**](http://proxy-ssl-geo.webflow.com) | 13.200.123.229 |
| [**proxy-ssl-geo.webflow.com**](http://proxy-ssl-geo.webflow.com) | 13.234.100.116 |
| [**proxy1.iitkgp.ac.in**](http://proxy1.iitkgp.ac.in) | 10.3.100.244 |
| [**quota.fe.apple-dns.net**](http://quota.fe.apple-dns.net) | 17.248.239.66 |
| [**safebrowsing.g.aaplimg.com**](http://safebrowsing.g.aaplimg.com) | 17.253.61.217 |
| [**safebrowsing.g.aaplimg.com**](http://safebrowsing.g.aaplimg.com) | 17.253.85.207 |
| [**safebrowsing.g.aaplimg.com**](http://safebrowsing.g.aaplimg.com) | 17.253.61.215 |
| [**safebrowsing.g.aaplimg.com**](http://safebrowsing.g.aaplimg.com) | 17.253.61.219 |
| [**scontent-cdg4-3.xx.fbcdn.net**](http://scontent-cdg4-3.xx.fbcdn.net) | 163.70.128.23 |
| [**scontent.xx.fbcdn.net**](http://scontent.xx.fbcdn.net) | 163.70.144.20 |
| [**scontent.xx.fbcdn.net**](http://scontent.xx.fbcdn.net) | 163.70.143.4 |
| [**scontent.xx.fbcdn.net**](http://scontent.xx.fbcdn.net) | 2a03:2880:f0a4:3:face:b00c:0:3 |
| [**smoot-searchv2-aaps1b.v.aaplimg.com**](http://smoot-searchv2-aaps1b.v.aaplimg.com) | 13.127.122.28 |
| [**som.iitkgp.ac.in**](http://som.iitkgp.ac.in) | 10.43.1.6 |
| [**ssl.google-analytics.com**](http://ssl.google-analytics.com) | 142.251.42.8 |
| [**star-mini.c10r.facebook.com**](http://star-mini.c10r.facebook.com) | 163.70.144.35 |
| [**star-mini.c10r.facebook.com**](http://star-mini.c10r.facebook.com) | 2a03:2880:188:84:face:b00c:0:25de |
| [**static.doubleclick.net**](http://static.doubleclick.net) | 172.217.167.166 |
| [**stats.g.doubleclick.net**](http://stats.g.doubleclick.net) | 142.251.10.155 |
| [**stats.g.doubleclick.net**](http://stats.g.doubleclick.net) | 142.251.10.156 |
| [**stats.g.doubleclick.net**](http://stats.g.doubleclick.net) | 142.251.10.157 |
| [**stats.g.doubleclick.net**](http://stats.g.doubleclick.net) | 142.251.10.154 |
| [**syndication.twitter.com**](http://syndication.twitter.com) | 104.244.42.72 |
| [**twitter.com**](http://twitter.com) | 104.244.42.1 |
| [**twitter.com**](http://twitter.com) | 104.244.42.193 |
| [**twitter.com**](http://twitter.com) | 104.244.42.129 |
| [**twitter.com**](http://twitter.com) | 104.244.42.65 |
| [**www.g20.org**](http://www.g20.org) | 189.9.176.149 |
| [**www.google-analytics.com**](http://www.google-analytics.com) | 142.250.206.142 |
| [**www.google.com**](http://www.google.com) | 142.250.199.132 |
| [**www.googletagmanager.com**](http://www.googletagmanager.com) | 172.217.166.8 |
| [**www.iitkgp.ac.in**](http://www.iitkgp.ac.in) | 172.16.3.10 |
| [**www.pgdba.iitkgp.ac.in**](http://www.pgdba.iitkgp.ac.in) | 203.110.245.243 |
| [**www.vidyalakshmi.co.in**](http://www.vidyalakshmi.co.in) | 121.240.246.10 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.66.14 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.251.42.46 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.251.42.78 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 172.217.174.78 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 172.217.27.206 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.71.110 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.182.238 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.182.206 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 172.217.166.46 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.77.78 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.77.46 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.199.142 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.183.174 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.183.142 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.183.14 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 142.250.183.206 |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 2404:6800:4002:814::200e |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 2404:6800:4002:816::200e |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 2404:6800:4002:815::200e |
| [**youtube-ui.l.google.com**](http://youtube-ui.l.google.com) | 2404:6800:4002:813::200e |
| [**z-p42-instagram.c10r.instagram.com**](http://z-p42-instagram.c10r.instagram.com) | 163.70.144.174 |
| [**z-p42-instagram.c10r.instagram.com**](http://z-p42-instagram.c10r.instagram.com) | 2a03:2880:288:12:face:b00c:0:4420 |

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

By exploring the DNS packets, it’s possible to find the IP address of the local DNS server that the host system is using, but finding the IP addresses of other intermediate DNS servers seems challenging, since Wireshark only captures the packets that pass through the host system.

In this case, the IP address of the local DNS server that the host is using 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.

2 HTTP GET requests (with request URI: http://iitkgp.ac.in/)

| **No.** | **Source** | **Destination** | **Protocol** | **Length** | **Info** |
| --- | --- | --- | --- | --- | --- |
| **400** | 10.145.247.76 | 172.16.3.10 | HTTP | 441 | GET / HTTP/1.1 |
| **1010** | 10.145.247.76 | 172.16.3.10 | HTTP | 525 | GET / HTTP/1.1 |

b. For each of the HTTP GET requests you see above, find out (i) the total number

of TCP segments being received, and (ii) the total amount of data being received

in the corresponding HTTP Response message.

| **No.** | **Source** | **Destination** | **Protocol** | **Info** | **Total no. of TCP segments received** | **Total amount of data received** |
| --- | --- | --- | --- | --- | --- | --- |
| **400** | 10.145.247.76 | 172.16.3.10 | HTTP | GET / HTTP/1.1 | 301 | 453230 bytes |
| **1010** | 10.145.247.76 | 172.16.3.10 | HTTP | GET / HTTP/1.1 | 302 | 453146 bytes |