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

**Assignment 1 (Part A) Submission**

Name: Barun Parua

Roll number: 21CS10014

Link of the pcap file: [21CS10014.pcapng](https://drive.google.com/file/d/18nBMn7egtbHEp0OEuKDE4IISIE3H5Xto/view?usp=sharing)

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

**Questions**

For reference, the total number of packets is 6900.

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

**a. TCP and UDP together:** TCP - 6334, UDP - 383, Total - 6717 (using statistics page)

**b. IPv4 and IPv6?:** IPv4 - 6679, IPv6 - 58, Total - 6737 (using statistics page)

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

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

1707699 bytes (setting ip.src == 172.16.3.10 and ip.dst == 10.117.166.55)

**b. When you access** <https://www.cornell.edu>

43705 bytes (setting ip.src == 13.107.246.72 and ip.dst ==10.117.166.55 and filtering all packets after 100s time to get for cornell, might be inaccurate as it is https website)

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

There are 142 DNS packets in total (71 queries and 71 responses).

**a. Create a 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.**

We check each DNS response and get the IP addresses. The table is given below.

| **Domain Name** | **IP Address(es)** |
| --- | --- |
| *6120104.global.siteimproveanalytics.io* | 13.51.8.45 |
| *aad.cs.dds.microsoft.com* | 52.152.90.172 |
| *accounts.google.com* | 216.239.32.10, 216.239.34.10, 216.239.38.10, 2001:4860:4802:38::a, 2001:4860:4802:34::a, 2001:4860:4802:32::a, 2001:4860:4802:36::a |
| *api-d.dropbox.com* | 162.125.8.20 |
| *assets.msn.com* | 180.149.52.200, 180.149.52.217, 180.149.52.209, 180.149.52.219, 180.149.52.216, 180.149.52.218, 180.149.52.202 |
| *beacons.gcp.gvt2.com* | 172.217.166.35 |
| *browser.pipe.aria.microsoft.com* | 52.178.17.2 |
| *catalog.gamepass.com* | 49.44.131.147, 49.44.131.145 |
| *client.wns.windows.com* | 20.198.119.143 |
| *clients2.google.com* | 142.250.194.14 |
| *clients4.google.com* | 142.250.182.238, 172.217.167.46, 142.250.194.14 |
| *clientservices.googleapis.com* | 142.250.183.35 |
| *config.teams.microsoft.com* | 52.113.194.132 |
| *connect.facebook.net* | 163.70.143.4 |
| *content-autofill.googleapis.com* | 142.250.194.138, 142.250.207.234, 172.217.166.234, 142.250.195.10 |
| *ctldl.windowsupdate.com* | 180.149.59.224, 180.149.59.200 |
| *cu1pehnsmps01.servicebus.windows.net* | 104.208.16.0 |
| *darkreader.org* | 185.199.109.153, 185.199.108.153, 185.199.110.153, 185.199.111.153 |
| *default.exp-tas.com* | 13.107.5.93 |
| *ecs.office.com* | 52.113.194.132 |
| *gateway.facebook.com* | 163.70.143.11 |
| *history.google.com* | 142.251.175.100, 142.251.175.101, 142.251.175.102, 142.251.175.113, 142.251.175.139 |
| ***iitkgp.ac.in*** | 172.16.3.10 |
| *inputsuggestions.msdxcdn.microsoft.com* | 13.107.246.7213.107.213.72 |
| *jnn-pa.googleapis.com* | 142.250.206.170, 142.250.192.170, 142.250.193.42, 142.250.193.10 |
| *lh3.google.com* | 142.250.206.174 |
| *lh3.googleusercontent.com* | 142.250.70.65 |
| *login.live.com* | 20.190.146.34, 20.190.146.36, 20.190.146.39, 20.190.146.33, 20.190.146.37, 20.190.146.38, 40.126.18.32, 40.126.18.33 |
| *login.microsoftonline.com* | 40.126.17.135 |
| *mtalk.google.com* | 74.125.24.188 |
| *ogs.google.com* | 172.217.166.206 |
| *outlook.office365.com* | 52.98.58.50, 52.98.58.34, 52.98.123.194, 40.99.9.66 |
| *p.typekit.net* | 180.149.59.145, 180.149.59.136 |
| *platform.twitter.com* | 192.229.237.25 |
| *play.google.com* | 142.250.206.174 |
| *pool.ntp.org* | 162.159.200.1, 162.159.200.123, 95.216.144.266, 144.24.146.96 |
| *prd-mcafee-mosaic-pub.azurewebsites.net* | 104.40.53.219 |
| *safebrowsing.google.com* | 142.250.199.174 |
| *safebrowsing.googleapis.com* | *142.250.183.170* |
| *scontent-bom2-1.xx.fbcdn.net* | 163.70.143.4, 157.240.16.20 |
| *scontent-bom2-1.xx.fbcdn.net* | 31.13.79.26 |
| *scontent.xx.fbcdn.net* | 31.13.79.26 |
| *server.events.data.microsoft.com* | 20.42.73.26 |
| *ssl.google-analytics.com* | 142.250.193.200, 142.250.182.174 |
| *ssl.gstatic.com* | 172.217.166.195 |
| *stats.g.doubleclick.net* | 74.125.68.155, 74.125.68.154 |
| *substrate.office.com* | 52.98.57.162, 52.98.123.194, 52.98.57.114, 40.99.9.178, 52.98.59.18, 52.98.123.178 |
| *syndication.twitter.com* | 104.244.42.136 |
| *www.bing.com* | 180.149.52.201, 180.149.52.202, 180.149.52.210, 180.149.52.211, 180.149.52.208, 180.149.52.203, 180.149.52.218, 180.149.52.219 |
| ***www.cornell.edu*** | 13.107.246.72, 13.107.213.72 |
| *www.dropbox.com* | 162.125.81.18 |
| *www.facebook.com* | 163.70.143.35, 31.13.79.35 |
| *www.google.com* | 142.250.76.196, 142.250.194.142, 142.250.70.110 |
| *www.googleapis.com, cloudsearch.googleapis.com, optimizationguide-pa.googleapis.com* | 142.250.183.74, 142.250.183.106, 142.250.192.74, 142.250.192.10, 142.250.76.202, 142.251.42.74, 142.250.192.138, 142.251.42.42,142.250.183.42, 142.250.192.106, 142.250.192.42, 142.250.67.170, 142.250.67.138, 172.217.166.74, 172.217.174.234, 172.217.160.170 |
| *www.googletagmanger.com* | 142.250.194.136 |
| *www.youtube.com* | 142.250.182.206, 142.250.183.174, 142.250.77.78, 172.217.174.78, 142.251.42.46, 142.250.77.46, 142.250.183.206, 142.250.183.142, 142.250.66.14, 172.217.166.174, 142.251.42.78, 172.217.160.206, 142.250.192.46, 142.250.182.238, 142.250.183.14 |

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

Yes, we can find IP of the DNS servers by exploring the packets. In the "Queries" or "Answers" sections in DNS packets we can find the IP addresses. The "A" (Address of IPv4) or "AAAA" (Address of IPv6) fields in the "Answers" section contain the resolved domain's IP address.

However, some websites operate securely using the HTTPS or other protocols and in those cases, the actual IP addresses are hidden as the DNS queries and responses themselves are not visible. Even if we can track them using some Wireshark settings, they might be encrypted so we cannot get their actual addresses easily.

**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.**

We can see 2 HTTP GET requests from the site http://iitkgp.ac.in (We determine it using the HTTP filter, and then from there, checking which ones are GET requests with host iitkgp.ac.in). The packet numbers are 1642 and 2025.

Both of the two GET requests are of the form “GET / HTTP/1.1\r\n”.

**b. For each of the HTTP GET requests you see above, find out (ii) the total number of TCP segments being received, and (ii) the total amount of data being received in the corresponding HTTP Response message.**

Response 1 (Packet 2016):

Data Received - 432540 bytes in chunks of 8192 octets

TCP segments received - 298 (433543 bytes)

Response 2 (Packet 3171):

Data Received - 432540 bytes in chunks of 8192 octets

TCP segments received - 298 (433400 bytes)

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