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

Assignment 1 Submission

Name: **Sriyash Poddar**

Roll number: **18CS30040**

Link of the pcap file: [**https://drive.google.com/file/d/1ERFW3aYmmFU\_wzkeOcgUxUqFaugVJ3HP/view?usp=sharing**](https://drive.google.com/file/d/1ERFW3aYmmFU_wzkeOcgUxUqFaugVJ3HP/view?usp=sharing)

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

## Q1. What are the different protocols you observe at the following layers of the protocol stack?

#### Application Layer

1. Hypertext Transfer Protocol (HTTP)
2. Transport Layer Security (TLS)
3. Domain Name System (DNS)
4. Simple Service Discovery Protocol (SSDP)
5. Multicast Domain Name System
6. QUIC IETF

#### Transport Layer

1. User Datagram Protocol (UDP)
2. Transmission Control Protocol (TCP)

#### Network Layer

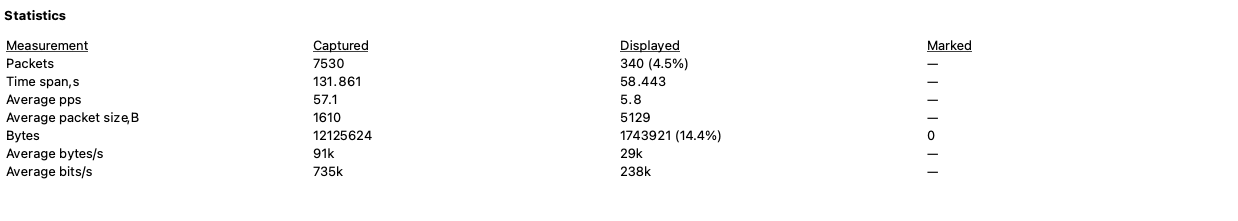
1. Internet Protocol v4 (IPv4)
2. Internet Protocol v6 (IPv6)
3. Address Resolution Protocol (ARP)
4. Internet Control Message Protocol version 6 (ICMPv6)

## Q2. What is the total amount of data being received for the following two cases?

### On accessing <http://iitkgp.ac.in>

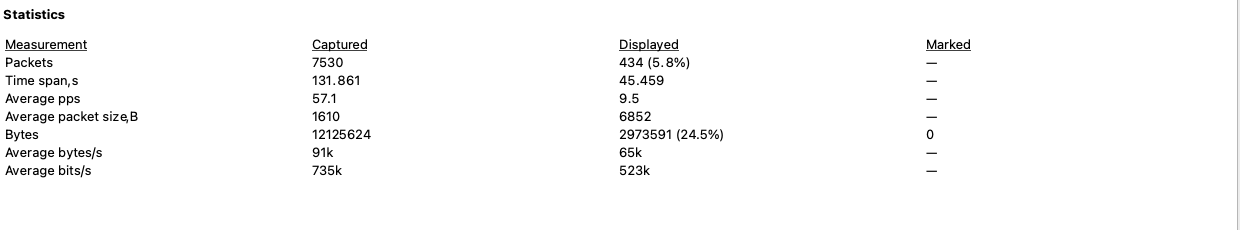
1. The total number of packets received is **340**
2. The size of data received is **1776069 bytes (1.74 MB)**
3. To check, filter by: **ip.src == 203.110.245.244**

(Considering those packets that we receive)



### On accessing <https://www.cornell.edu> :

1. The total number of packets received is **434**
2. Size of data received is **2973591 bytes (2.97 MB)**
3. To check, filter by: **ip.src == 20.42.25.107**



## 

## Q3. How many DNS packets have you observed in total?

* There are **357** DNS packets

### Create a <DOMAIN, IP> table

|  |  |  |
| --- | --- | --- |
| Domain name | Type | Address |
| clientservices.googleapis.com | A | 172.217.167.131 |
| clientservices.googleapis.com | AAAA | 2404:6800:4002:80f::2003 |
| accounts.google.com | A | 172.217.163.173 |
| accounts.google.com | AAAA | 2404:6800:4002:809::200d |
| cdn.mxpnl.com | A | 35.186.235.23 |
| cdn.mxpnl.com | AAAA | 2600:1901:0:bc29:: |
| d24n15hnbwhuhn.cloudfront.net | A | 54.230.222.105 |
| www.google.com | A | 172.217.167.228 |
| www.google.com | AAAA | 2404:6800:4007:80e::2004 |
| beacons3.gvt2.com | A | 172.217.26.163 |
| www.googleapis.com | A | 172.217.166.234 |
| www.googleapis.com | AAAA | 2404:6800:4002:812::200a |
| ws.mailtrack.io | A | 54.171.51.78 |
| d27xxe7juh1us6.cloudfront.net | A | 52.85.125.75 |
| api-js.mixpanel.com | A | 107.178.240.159 |
| oauthaccountmanager.googleapis.com | A | 142.250.67.74 |
| oauthaccountmanager.googleapis.com | AAAA | 2404:6800:4007:812::200a |
| www.gstatic.com | A | 172.217.163.195 |
| www.gstatic.com | AAAA | 2404:6800:4002:807::2003 |
| encrypted-tbn0.gstatic.com | AAAA | 2404:6800:4007:80b::200e |
| encrypted-tbn0.gstatic.com | A | 172.217.161.14 |
| s-usc1c-nss-266.firebaseio.com | A | 35.201.97.85 |
| s-usc1c-nss-266.firebaseio.com | AAAA | 2600:1901:0:94b6:: |
| securetoken.googleapis.com | A | 172.217.166.202 |
| securetoken.googleapis.com | AAAA | 2404:6800:4007:809::200a |
| www.iitkgp.ac.in | A | 203.110.245.244 |
| www.rajbhasha.iitkgp.ac.in | A | 203.110.245.243 |
| api.amplitude.com | A | 44.238.7.162 |
| www.sric.iitkgp.ac.in | A | 203.110.245.243 |
| erp.iitkgp.ac.in | A | 203.110.245.60 |
| som.iitkgp.ac.in | A | 203.110.240.154 |
| international.iitkgp.ac.in | A | 203.110.242.133 |
| twitter.com | A | 104.244.42.1 |
| gate.iitkgp.ac.in | A | 203.110.245.11 |
| iitkgpmail.iitkgp.ac.in | A | 203.110.245.235 |
| www.cep.iitkgp.ac.in | A | 203.110.245.243 |
| www.counsellingcentre.iitkgp.ac.in | A | 203.110.245.243 |
| www.dak.iitkgp.ernet.in | A | 203.110.246.11 |
| www.gian.iitkgp.ac.in | A | 203.110.245.243 |
| www.international.iitkgp.ac.in | A | 203.110.245.243 |
| www.library.iitkgp.ac.in | A | 203.110.245.243 |
| www.som.iitkgp.ac.in | A | 203.110.245.243 |
| www.tgh.iitkgp.ac.in | A | 203.110.245.243 |
| www.vidyalakshmi.co.in | A | 121.240.246.10 |
| www1.iitkgp.ac.in | A | 203.110.245.243 |
| www.weavatools.com | A | 54.230.41.51 |
| auth.grammarly.com | A | 35.168.75.144 |
| f-log-extension.grammarly.io | A | 52.205.211.154 |
| update.googleapis.com | A | 172.217.166.195 |
| update.googleapis.com | AAAA | 2404:6800:4002:808::2003 |
| ssl.gstatic.com | AAAA | 2404:6800:4002:807::2003 |
| ssl.gstatic.com | A | 172.217.31.195 |
| remotedesktop-pa.googleapis.com | A | 172.217.167.42 |
| remotedesktop-pa.googleapis.com | AAAA | 2404:6800:4002:80e::200a |
| beacons4.gvt2.com | A | 216.239.32.116 |
| storage.googleapis.com | AAAA | 2404:6800:4007:808::2010 |
| storage.googleapis.com | A | 172.217.163.176 |
| erp.iitkgp.ac.in | A | 203.110.245.59 |
| www.google.com | A | 172.217.167.228 |
| www.google.com | AAAA | 2404:6800:4007:80e::2004 |
| encrypted-tbn0.gstatic.com | AAAA | 2404:6800:4007:80b::200e |
| encrypted-tbn0.gstatic.com | A | 172.217.161.14 |
| ajax.googleapis.com | AAAA | 2404:6800:4002:805::200a |
| ajax.googleapis.com | A | 172.217.167.234 |
| oauthaccountmanager.googleapis.com | A | 142.250.67.74 |
| oauthaccountmanager.googleapis.com | AAAA | 2404:6800:4007:80e::200a |
| cdnjs.cloudflare.com | A | 104.16.18.94 |
| cdnjs.cloudflare.com | AAAA | 2606:4700::6810:135e |
| siteimproveanalytics.com | A | 172.64.197.24 |
| siteimproveanalytics.com | AAAA | 2606:4700:8d9e:7be7:52d7:c:e749:3178 |
| f-log-extension.grammarly.io | A | 54.145.80.191 |
| connectivity-check.ubuntu.com | A | 35.232.111.17 |
| beacons3.gvt2.com | A | 172.217.166.227 |

* Omitted CNAME records as they indicate aliases.

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

The DNS queries are sent to the **IP 192.168.29.1**

## Q4 Answer the following when you access the site [iitkgp.ac.in](http://iitkgp.ac.in)

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

* There are **22 GET requests**
* To check GET requests, filter by **ip.dst == 203.110.245.244 and http.request.method == GET**

|  |  |  |  |
| --- | --- | --- | --- |
| Source | * Destination | * Protocol | * Info |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET / HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/css/bootstrap.min.css;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/css/font-awesome.css;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/common\_css/common\_stylesheet.css;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/css/home\_style.css;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/images/hindi.png;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/images/logo.png;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/css/override.css;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/banners/adm\_vgsom.jpg;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/images/nvsp3.png;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/js/jquery.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/js/bootstrap.min.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/js/override.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/js/navigation.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/page\_js/jquery.tickerNews.min.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/js/jquery.bootstrap.newsbox.min.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/page\_js/home\_page.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/common\_js/common\_js.js;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/fonts/glyphicons-halflings-regular.woff2 HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/images/footer\_bg.jpg HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/fonts/fontawesome-webfont.woff2?v=4.5.0 HTTP/1.1 |
| 192.168.29.230 | 203.110.245.244 | HTTP | GET /resources/images/index.png;jsessionid=55A8F1BB9E52D9E457183776CB43BA7F HTTP/1.1 |

### 

### For each GET request, show total number of TCP segments and data received in the corresponding HTTP response message

|  |  |  |
| --- | --- | --- |
| Request | No. of TCP Segments | HTTP Content Length (bytes) |
| GET / HTTP/1.1 | 143 | 932903 |
| GET /resources/css/bootstrap.min.css;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 33 | 140990 |
| GET /resources/css/font-awesome.css;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 11 | 35319 |
| GET /resources/common\_css/common\_stylesheet.css;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 7 | 19530 |
| GET /resources/css/home\_style.css;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 2 | 8543 |
| GET /resources/images/hindi.png;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 2 | 2020 |
| GET /resources/images/logo.png;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 5 | 17073 |
| GET /resources/css/override.css;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 3 | 6640 |
| GET /resources/fonts/glyphicons-halflings-regular.woff2 HTTP/1.1 | 4 | 18028 |
| GET /resources/banners/adm\_vgsom.jpg;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 44 | 239142 |
| GET /resources/images/nvsp3.png;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 3 | 8947 |
| GET /resources/js/jquery.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 13 | 95791 |
| GET /resources/js/bootstrap.min.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 8 | 36868 |
| GET /resources/js/override.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 4 | 7823 |
| GET /resources/js/navigation.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 2 | 1987 |
| GET /resources/page\_js/jquery.tickerNews.min.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 3 | 3994 |
| GET /resources/js/jquery.bootstrap.newsbox.min.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 3 | 5267 |
| GET /resources/page\_js/home\_page.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 3 | 4632 |
| GET /resources/common\_js/common\_js.js;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 2 | 2835 |
| GET /resources/fonts/fontawesome-webfont.woff2?v=4.5.0 HTTP/1.1 | 8 | 66624 |
| GET /resources/images/footer\_bg.jpg HTTP/1.1 | 10 | 55972 |
| GET /resources/images/index.png;jsessionid=944552E5F9E0E045F8035DB1B96EC01E HTTP/1.1 | 2 | 5574 |