==

Assignment 1 Submission

Name: Abhinav Bohra

Roll number: 18CS30049

Link of the pcap file: https://drive.google.com/file/d/14ez_QhQvE1Pgr52EqOvJVFwldjpCbpjn/view?usp=sharing

==

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

   a. Application layer – HTTP, DNS, TLS, SSDP, MDNS, NBNS
   b. Transport layer – TCP, UDP, ICMPv6
   c. Network layer – IPv4, IPv6, Address Resolution Protocol (ARP)

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

   a. When you access http://iitkgp.ac.in

Measurement	**Received**
Packets	1165
Bytes	1643315

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

Measurement	**Received**
Packets	2109
Bytes	3054024

3. How many DNS packets have you observed in total? 34

   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 Address**
iitkgpmail.iitkgp.ac.in	203.110.245.235
gate.iitkgp.ac.in	203.110.245.11
iitkgp.ac.in	203.110.245.244
www.cornell.edu	20.42.25.107
clientservices.googleapis.com	2404:6800:4009:813::2003
p.typekit.net	104.120.64.164
fonts.gstatic.com	172.217.24.227
ssl.google-analytics.com	2404:6800:4009:820::2008
settings-win.data.microsoft.com	52.139.168.125
mtalk.google.com	74.125.68.188
accounts.google.com	142.250.183.13
ssl.google-analytics.com	142.250.76.168
encrypted-tbn0.gstatic.com	142.250.67.238
update.googleapis.com	2404:6800:4009:812::2003
caldav.calendar.yahoo.com	119.161.10.11
publicsuffix.org	13.227.185.114
use.typekit.net	49.44.118.43

www.jeeadv.ac.in	35.192.176.149
6120104.global.siteimproveanalytics.io	18.159.119.149
update.googleapis.com	142.250.67.227
www.google.com	142.250.77.36
siteimproveanalytics.com	2606:4700:8d7e:7be7:52ca:10c:e749:3178
f-log-extension.grammarly.io	34.199.54.11
publicsuffix.org	13.227.138.115
caldav.calendar.yahoo.com	2406:2000:98:800::e6
twitter.com	49.44.204.178
data.grammarly.com	34.226.23.237
mip.api.mcafeewebadvisor.com	54.197.194.123
encrypted-tbn0.gstatic.com	2404:6800:4009:814::200e
cdnjs.cloudflare.com	2606:4700::6810:125e
auth.grammarly.com	52.200.32.121
www.facebook.com	2404:6800:4009:80a::2003
webadvisorc.rest.gti.mcafee.com	2606:4700::6810:135e
clientservices.googleapis.com	2404:6800:4009:813::2003
p.typekit.net	104.120.64.164
fonts.gstatic.com	172.217.24.227
ssl.google-analytics.com	2404:6800:4009:820::2008
settings-win.data.microsoft.com	52.139.168.125
mtalk.google.com	74.125.68.188
accounts.google.com	142.250.183.13
ssl.google-analytics.com	142.250.76.168
encrypted-tbn0.gstatic.com	142.250.67.238
update.googleapis.com	2404:6800:4009:812::2003
caldav.calendar.yahoo.com	119.161.10.11
publicsuffix.org	13.227.185.114

b. Can you find out the IP of the DNS servers by exploring the DNS packets?
Yes, we can find out IP of the DNS server by analysing DNS packets. The destination of the packets with Standard Query is the IP address of DNS server. In my case it is 192.168.29.1

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.

Number of HTTP GET requests = 19

List of GET requests: -

Sr. No	Info
1	GET / HTTP/1.1
2	GET /resources/css/bootstrap.min.css;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
3	GET /resources/css/font-awesome.css;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
4	GET/resources/common_css/common_stylesheet.css;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
5	GET /resources/css/home_style.css;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
6	GET /resources/images/hindi.png;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
7	GET /resources/images/logo.png;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
8	GET /resources/css/override.css;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
9	GET /resources/banners/adm_vgsom.jpg;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
10	GET /resources/images/nvsp3.png;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
11	GET /resources/js/jquery.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
12	GET /resources/js/bootstrap.min.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
13	GET /resources/js/override.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
14	GET /resources/js/navigation.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
15	GET/resources/page_js/jquery.tickerNews.min.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
16	GET/resources/js/jquery.bootstrap.newsbox.min.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
17	GET /resources/page_js/home_page.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
18	GET /resources/common_js/common_js.js;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1
19	GET /resources/images/index.png;jsessionid=3485852A0CF9CA3FF866329F433A40A9 HTTP/1.1

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

HTTP GET Request (Sr. No. with respect to above table)	**Total number of TCP segments being received**	**Total amount of data received in the corresponding HTTP Response message (in bytes)**
1	33	44335
2	42	60626
3	3	120
4	2	66
5	12	13923
6	129	185342
7	5	2412
8	602	902938
9	1	0
10	1	0
11	1	0
12	1	0
13	1	0
14	137	196572
15	26	34370
16	1	0
17	48	69968
18	89	124235
19	48	8342