===

Assignment 1 Submission
Name : Patel Devarshi Chandrakant
Roll No. : 18CS10040
Link of the pcap file :
https://drive.google.com/file/d/1t6MT7meMb6qeDlgGYb7VThyD5KmUMd4b/view?usp=sharing

===

Answers:

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

a. Application layer

Solution: HTTP(HyperText Transfer Protocol)
DNS(Domain Name System)
SSDP(Simple Service Discovery Protocol)
MDNS(Multicast DNS)
TLS(Transport Layer Security)

b. Transport layer

Solution: TCP(Transmission Control Protocol)
UDP(User Datagram Protocol)

c. Network layer

Solution: IPv6(Internet Protocol version 6)
IPv4(Internet Protocol version 4)
ICMPv6(Internet Control Message Protocol)
IGMP(Internet Group Management Protocol)
ARP(Address Resolution Protocol)

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

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

Solution: i) IP address : 203.110.245.244.
ii) Total No of packets received is 1150.
iii) Total amount of data received is 1652kBytes (1.61MB).

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

Solution: i) IP address : 20.42.25.107.
ii) Total No of packets received is 1323.
iii) Total amount of data received is 1913kBytes (1.86MB).

---

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

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.

Table :

Sr.No.	Domain name	Type	IP Address
1	www3.l.google.com	A	172.217.166.46
2	www.gstatic.com	A	216.58.203.35
3	ssl.gstatic.com	A	142.250.77.67
4	plus.l.google.com	A	142.250.76.174
5	play.google.com	A	142.250.67.238
6	lh5.googleusercontent.com	A	172.217.174.65
7	sb.l.google.com	A	172.217.167.174
8	googlemail.l.google.com	A	172.217.174.229
9	www.facebook.com	A	157.240.16.35
10	www.linkedin.com	A	13.107.42.14

11	www.jeeadv.ac.in	A	35.192.176.149
12	mtalk.google.com	A	172.217.194.188
13	iitkgp.ac.in	A	203.110.245.244
14	connectivity-check.ubuntu.com	A	35.232.111.17
15	www.cornell.edu	A	20.42.25.107
16	use.typekit.net	A	43.250.166.121
17	ajax.googleapis.com	A	142.250.76.170
18	cdnjs.cloudflare.com	A	104.16.18.94
19	embanner.univcomm.cornell.edu	A	20.42.25.107
20	media.univcomm.cornell.edu	A	20.42.25.107
21	ssl.google-analytics.com	A	142.250.183.136
22	siteimproveanalytics.com	A	172.64.197.24
23	stats.g.doubleclick.net	A	74.125.24.156
24	p.typekit.net	A	23.15.195.45
25	6120104.global.siteimproveanalytics.io	A	18.158.85.68
26	plugin.rocketreach.co	A	54.245.66.78
27	extension-api.hunter.io	A	104.22.11.67

Note: There were several cname in the intermediate steps that were not mentioned here.

b. Can you find out the IP of the DNS servers by exploring the DNS packets?
Solution: Yes. We can filter the DNS queries out of the total queries and look at the query response dns packet. By looking at the source of the response we can find out the IP of the DNS servers . It is 192.168.1.1.

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.

Solution: 19 HTTP GET requests are observed. The list is as follows :

Sr.No.	Time	Source	Destination	Length	Info
540	15.042598	192.168.1.8	203.110.245.244	541	GET / HTTP/1.1
642	15.294594	192.168.1.8	203.110.245.244	467	GET /resources/css/bootstrap.min.css HTTP/1.1
758	15.380428	192.168.1.8	203.110.245.244	466	GET /resources/css/font-awesome.css HTTP/1.1
847	15.410403	192.168.1.8	203.110.245.244	478	GET /resources/common_css/common_stylesheet.css HTTP/1.1
848	15.4112	192.168.1.8	203.110.245.244	464	GET /resources/css/home_style.css HTTP/1.1
873	15.41826	192.168.1.8	203.110.245.244	483	GET /resources/images/hindi.png HTTP/1.1
1268	15.556537	192.168.1.8	203.110.245.244	482	GET /resources/images/logo.png HTTP/1.1
1310	15.576775	192.168.1.8	203.110.245.244	462	GET /resources/css/override.css HTTP/1.1
1904	15.818992	192.168.1.8	203.110.245.244	488	GET /resources/banners/adm_vgsom.jpg HTTP/1.1
1982	15.8624	192.168.1.8	203.110.245.244	483	GET /resources/images/nvsp3.png HTTP/1.1
2007	15.871642	192.168.1.8	203.110.245.244	443	GET /resources/js/jquery.js HTTP/1.1
2008	15.871753	192.168.1.8	203.110.245.244	450	GET /resources/js/bootstrap.min.js HTTP/1.1
2009	15.871843	192.168.1.8	203.110.245.244	445	GET /resources/js/override.js HTTP/1.1
2051	15.916466	192.168.1.8	203.110.245.244	447	GET /resources/js/navigation.js HTTP/1.1
2073	15.940995	192.168.1.8	203.110.245.244	463	GET /resources/page_js/jquery.tickerNews.min.js HTTP/1.1

2084	15.944894	192.168.1.8	203.110.245.244	465	GET /resources/js/jquery.bootstrap.newsbox.min.js HTTP/1.1
2187	15.999097	192.168.1.8	203.110.245.244	451	GET /resources/page_js/home_page.js HTTP/1.1
2194	16.003091	192.168.1.8	203.110.245.244	453	GET /resources/common_js/common_js.js HTTP/1.1
2481	16.961448	192.168.1.8	203.110.245.244	483	GET /resources/images/index.png HTTP/1.1

b. For each of the HTTP GET requests as 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.

Solution :

Sr. No.	Time	Info	TCP Segments	File Data(bytes)	Total Data(bytes)
540	15.042598	GET / HTTP/1.1	647	928899	929995
642	15.294594	GET /resources/css/bootstrap.min.css HTTP/1.1	99	140990	141167
758	15.380428	GET /resources/css/font-awesome.css HTTP/1.1	26	35319	35495
847	15.410403	GET /resources/common_css/common_stylesheet.css HTTP/1.1	15	19530	19706
848	15.4112	GET /resources/css/home_style.css HTTP/1.1	7	8543	8718
873	15.41826	GET /resources/images/hindi.png HTTP/1.1	3	2020	2196
1268	15.556537	GET /resources/images/logo.png HTTP/1.1	13	17073	17250

1310	15.576775	GET /resources/css/override.css HTTP/1.1	6	6640	6815
1904	15.818992	GET /resources/banners/adm_vgsom.jpg HTTP/1.1	168	239142	239321
1982	15.8624	GET /resources/images/nvsp3.png HTTP/1.1	8	8947	9123
2007	15.871642	GET /resources/js/jquery.js HTTP/1.1	68	95791	95981
2008	15.871753	GET /resources/js/bootstrap.min.js HTTP/1.1	27	36868	37058
2009	15.871843	GET /resources/js/override.js HTTP/1.1	7	7823	8012
2051	15.916466	GET /resources/js/navigation.js HTTP/1.1	3	1987	2176
2073	15.940995	GET /resources/page_js/jquery.tickerNews.min.js HTTP/1.1	4	3994	4183
2084	15.944894	GET /resources/js/jquery.bootstrap.newsbox.min.js HTTP/1.1	5	5267	5456
2187	15.999097	GET /resources/page_js/home_page.js HTTP/1.1	5	4632	4821
2194	16.003091	GET /resources/common_js/common_js.js HTTP/1.1	3	2835	3024
2481	16.961448	GET /resources/images/index.png HTTP/1.1	5	5574	5750

Note : Here the file data as well as total data (including headers) is mentioned.