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

**Assignment 1 Submission**

Name: **Itish Agarwal**

Roll number: **18CS30021**

Link of the pcap file: <https://drive.google.com/file/d/1LlKYimBJhqdwngrSU1nx5B-TXsz1S5xz/view?usp=sharing>

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

**QUESTION 1**

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

**a**. Application layer

**b**. Transport layer

**c**. Network layer

**ANSWER 1**

Different protocols observed at the following layers of protocol stack are:

1. **Application layer:**
2. HyperText Transfer Protocol (HTTP)
3. Domain Name System (DNS)
4. Simple Service Discovery Protocol (SSDP)
5. Transport Layer Security (TLSv1.2, TLSv1.3)
6. Multicast Domain Name System (MDNS)
7. **Transport layer:**
8. Transmission Control Protocol (TCP)
9. User Datagram Protocol (UDP)
10. **Network layer:**
11. Address Resolution Protocol (ARP)
12. Internet Control Message Protocol (ICMP, ICMPv6)
13. Internet Group Management Protocol (IGMPv3)
14. Internet Protocol v4 (IPv4)

**QUESTION 2**

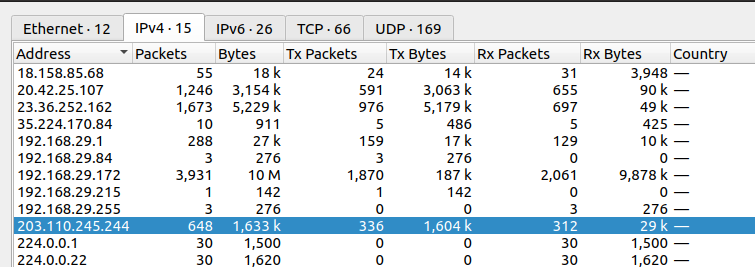
What is the total amount of data being received for the following two cases?

1. When you access ​ <http://iitkgp.ac.in>
2. When you access ​ <https://www.cornell.edu>

**ANSWER 2**

1. **On accessing** [**http://iitkgp.ac.in**](http://iitkgp.ac.in)**:**

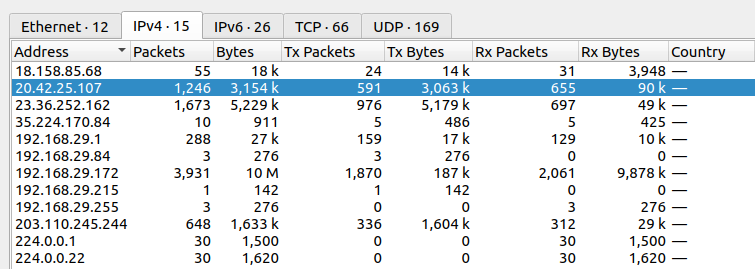
**(highlighted row in the table)**

****

1. IP address of the iitkgp server : **203.110.245.244**
2. Total number of packets being received: **336**
3. Total amount of data being received : **1604 kb (1.6 mb)**

**b. On accessing** <https://www.cornell.edu>**:**

**(highlighted row in the table)**

****

1. IP address of the cornell.edu server: **20.42.25.107**
2. Total number of packets being received: **591**
3. Total amount of data being received: **3063 kb (3 mb)**

**QUESTION 3**

How many DNS packets have you observed in total?

1. 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

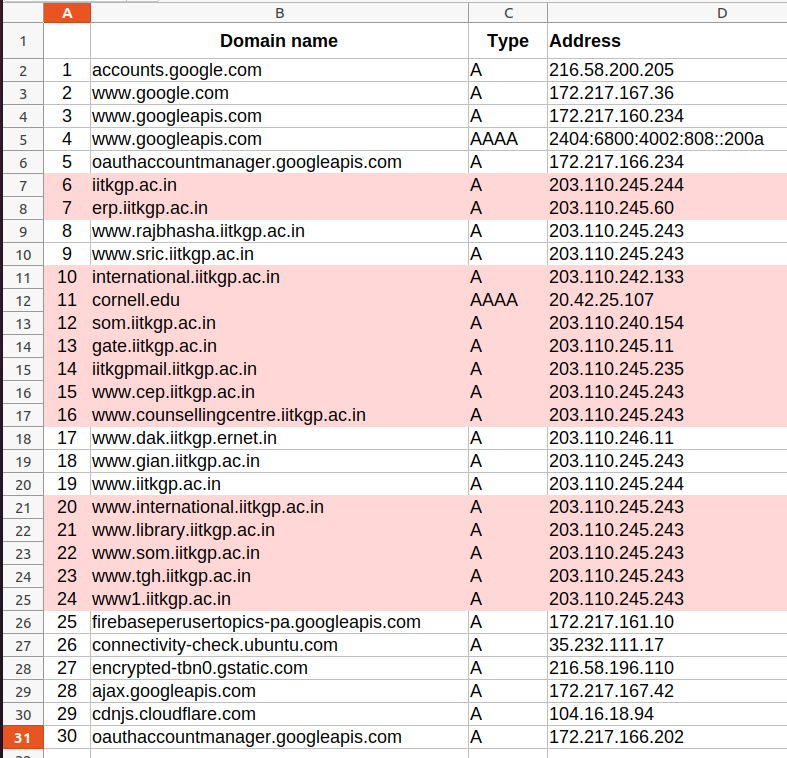
query, and the IP address will be the address that is being returned against

The corresponding query.

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

**ANSWER 3**

1. Table:



**Observations:**

1. There were a lot of dns packets received (total **252**) but most of them were third priority (like other processes running in the background or cache).
2. The top priority servers (ie, of iitkgp and cornell.edu) are highlighted in the table above.

**b**. **YES**, we can find the ip address of the DNS packets by exploring

the **Standard Query response**. It is the address of the source of

the standard query response, which in my case is **192.168.29.1.**

**QUESTION 4**

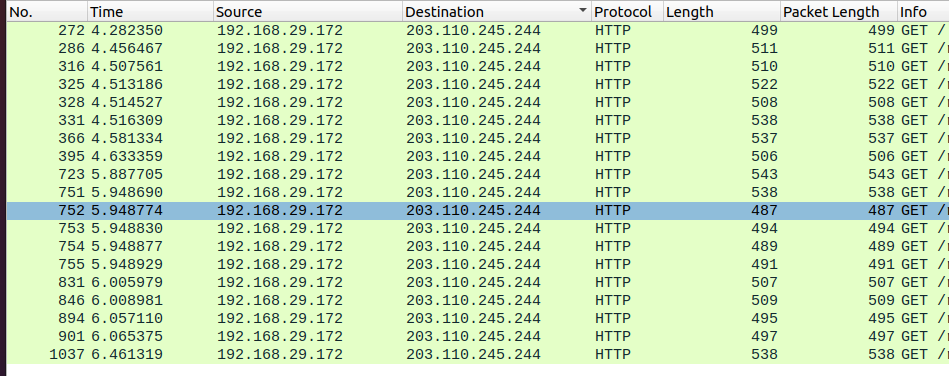
Answer the following when you access the site ​ [http://iitkgp.ac.in​](about:blank):

1. How many HTTP GET requests do you observe? List down the GET requests.
2. 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.

**ANSWER 4**

1. On accessing the site<http://iitkgp.ac.in>:



Number of HTTP GET requests observed: **19**

1. **For each of the 19 HTTP GET requests above**

In the table below, we have:

Number of TCP segments being received and the amount of data being received.

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Sr .No (of request)** | **Number of TCP segments** | **Amount of data received(in bytes)** |
| 1 | 272 | 140 | 932903 |
| 2 | 286 | 27 | 140990 |
| 3 | 316 | 11 | 35319 |
| 4 | 325 | 7 | 19530 |
| 5 | 328 | 7 | 8543 |
| 6 | 331 | 2 | 2020 |
| 7 | 366 | 4 | 17073 |
| 8 | 395 | 2 | 6640 |
| 9 | 723 | 52 | 239142 |
| 10 | 751 | 3 | 8947 |
| 11 | 752 | 14 | 95791 |
| 12 | 753 | 7 | 36868 |
| 13 | 754 | 7 | 7823 |
| 14 | 755 | 2 | 1987 |
| 15 | 831 | 2 | 3994 |
| 16 | 846 | 2 | 5267 |
| 17 | 894 | 3 | 4632 |
| 18 | 901 | 3 | 2835 |
| 19 | 1037 | 2 | 5574 |