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

**Assignment 1 Submission**

**Name:** Siba Smarak Panigrahi

**Roll number:** 18CS10069

**Link of the pcap file:** <https://drive.google.com/file/d/1NgBJ-AerHI_cH8v9aBVbPTpq-ghg75yE/view?usp=sharing>

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

**Q 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**

Ans 1.

|  |
| --- |
| 1. **Application layer:**    1. Multicast Domain Name System (MDNS)    2. Link-local Multicast Name Resolution (LLMNR)    3. Simple Service Discovery Protocol (SSDP)    4. QUIC IETF    5. VSS Monitoring Ethernet trailer    6. NetBIOS Name Service (NBNS)    7. Domain Name System (DNS)    8. Transport Layer Security (TLS)    9. Hypertext Transfer Protocol (HTTP)    10. Online Certificate Status Protocol (OCSP)    11. Dynamic Host Configuration Protocol (DHCP) 2. **Transport layer:**    1. User Datagram Protocol (UDP)    2. Transmission Control Protocol (TCP)    3. Internet Control Message Protocol v6 (ICMPv6) 3. **Network layer:**    1. Internet Protocol Version 6 (IPv6)    2. Internet Protocol Version 4 (IPv4)    3. Address Resolution Protocol (ARP)    4. Internet Group Management Protocol (IGMP)   **Q2. What is the total amount of data being received for the following two cases?**  **a. When you access** [**http://iitkgp.ac.in**](http://iitkgp.ac.in)  **b. When you access** [**https://www.cornell.edu**](https://www.cornell.edu)  **Ans 2. a.** 1644796 bytes (1644k bytes)  **b.** 226856 bytes (226k bytes) |

**Q3. 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.**

**Ans 3.** Total DNS packets observed = **231**

**Ans 3. a.** The <Domain Name, IP> table is given below**. iitkgp.ac.in** and [**www.cornell.edu**](http://www.cornell.edu)are highlighted in the table:

|  |  |
| --- | --- |
| **Domain Name** | **IP Address** |
| adservice.google.com | 216.58.200.194,216.239.34.10,216.239.32.10,216.239.36.10,216.239.38.10 |
| auth.grammarly.com | 35.172.78.238,52.200.32.121,35.168.75.144,205.251.196.197,205.251.198.52,205.251.193.166,205.251.195.67 |
| azwus2-client-s.gateway.messenger.live.com | 52.149.21.60,96.7.49.129,23.61.199.131,84.53.139.129,193.108.88.128 |
| clientservices.googleapis.com | 216.58.196.195,216.239.36.10,216.239.38.10,216.239.34.10,216.239.32.10 |
| data.grammarly.com | 54.174.116.221,52.55.161.123,35.172.197.47,52.86.133.180,34.233.222.28,18.209.122.133,52.203.178.138,34.226.23.237,205.251.197.152,205.251.199.106,205.251.193.250,205.251.194.33 |
| dw8wjz3q0i4gj.cloudfront.net | 54.182.1.130,54.182.1.113,54.182.1.118,54.182.1.26,205.251.196.234,205.251.198.241,205.251.193.16,205.251.195.66 |
| eafddirect.msedge.net | 51.104.24.88,40.90.4.1,64.4.48.1,13.107.160.1,40.90.4.1 |
| erp.iitkgp.ac.in | 203.110.245.60 |
| f-log-extension.grammarly.io | 54.157.175.36,54.145.80.191,54.174.103.60,34.201.155.181,35.172.29.112,54.156.218.23,107.22.49.50,3.226.99.244,205.251.192.112,205.251.197.223,205.251.199.70,205.251.194.153 |
| gate.iitkgp.ac.in | 203.110.245.11 |
| googleads.g.doubleclick.net | 216.58.200.194,216.239.34.10,216.239.32.10,216.239.36.10,216.239.38.10 |
| **iitkgp.ac.in** | **203.110.245.244** |
| iitkgpmail.iitkgp.ac.in | 203.110.245.235 |
| international.iitkgp.ac.in | 203.110.242.133 |
| kgpchronicle.iitkgp.ac.in | 203.110.242.132 |
| mail.google.com | 172.217.27.165,216.239.32.10,216.239.34.10,216.239.36.10,216.239.38.10 |
| mtalk.google.com | 74.125.24.188,216.239.32.10,216.239.34.10,216.239.36.10,216.239.38.10 |
| ns3.cloudflare.com | 162.159.0.33 |
| ocsp.digicert.com | 117.18.237.29,72.21.80.5,72.21.80.6,192.229.254.5,192.229.254.6 |
| p.typekit.net | 104.108.159.40,23.63.110.175,96.17.182.205,23.63.110.149,96.17.182.205,23.63.109.127,104.90.5.30,23.63.110.135,88.221.81.192 |
| platform.bing.com | 13.107.21.200,204.79.197.200,204.79.197.1,204.79.197.2 |
| sec-tws-prod-vip.webex.com | 66.163.35.36 |
| som.iitkgp.ac.in | 203.110.240.154 |
| ssl.google-analytics.com | 216.58.200.200,216.239.32.10,216.239.34.10,216.239.36.10,216.239.38.10 |
| twitter.com | 104.244.42.65 |
| ws.mailtrack.io | 54.171.51.78,108.128.65.19,108.128.74.148,34.251.64.170,34.249.6.34,52.210.126.235,205.251.196.36,205.251.199.238,205.251.193.9,205.251.194.156 |
| www.cep.iitkgp.ac.in | 203.110.245.243 |
| **www.cornell.edu** | **20.42.25.107** |
| www.counsellingcentre.iitkgp.ac.in | 203.110.245.243 |
| www.dak.iitkgp.ernet.in | 203.110.246.11 |
| www.facebook.com | 157.240.198.35,129.134.30.11,185.89.218.11,129.134.31.11,185.89.219.11 |
| www.gian.iitkgp.ac.in | 203.110.245.243 |
| www.google.com | 216.58.221.36,216.239.32.10,216.239.34.10,216.239.36.10,216.239.38.10 |
| www.googleapis.com | 172.217.166.202,172.217.167.42,172.217.166.10,172.217.167.202,172.217.27.170,172.217.167.234,216.58.196.106,216.58.200.170,216.58.200.202,172.217.24.234,216.58.196.202,172.217.161.10,216.239.36.10,216.239.38.10,216.239.34.10,216.239.32.10 |
| www.jeeadv.ac.in | 35.192.176.149,216.239.32.109,216.239.34.109,216.239.36.109,216.239.38.109 |
| www.library.iitkgp.ac.in | 203.110.245.243 |
| www.linkedin.com | 13.107.42.14,13.107.42.1,13.107.42.2 |
| www.msftconnecttest.com | 13.107.4.52 |
| www.nvsp.in | 117.239.183.240 |
| www.pmrf.in | 35.208.145.177 |
| www.rajbhasha.iitkgp.ac.in | 203.110.245.243 |
| www.sric.iitkgp.ac.in | 203.110.245.243 |
| www.tgh.iitkgp.ac.in | 203.110.245.243 |
| www.vidyalakshmi.co.in | 121.240.246.10,113.30.252.95,113.30.143.95,202.162.240.2,128.199.104.2,46.101.116.29,202.162.229.11,113.30.143.241,113.30.252.241 |
| www.youtube.com | 172.217.167.206,172.217.167.238,216.58.200.174,216.58.200.206,216.58.196.206,216.58.221.46,172.217.160.238,172.217.161.14,172.217.166.206,172.217.167.14,172.217.166.14,216.239.32.10,216.239.34.10,216.239.36.10,216.239.38.10 |
| www1.iitkgp.ac.in | 203.110.245.243 |

**Q 3.b. Can you find out the IP of the DNS servers by exploring the DNS packets?**

**Ans 3.b.** **I.** We can find the IP address of the Local Name Server, since the DNS query from the host (our system) is to the Local Name Server (LNS). And, also because our ISP (Internet Service Provider) hard-codes the IP Address of LNS into the system.

**II.** But other than that, we cannot obtain the IP Addresses of other intermediate Name Servers (such as root-name server, authoritative name-server, etc.). This is because the corresponding DNS packets are not captured by Wireshark (as it captures the packets that pass through the host system).

**III.** The IP of LNS (where the DNS query goes from my system) is 192.168.0.1. My system’s IP is 192.168.0.101

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

**a. How many HTTP GET requests do you observe? List down the GET requests.**

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

**Ans 4 a. & b.:**

Total number of GET requests = 19

The table below contains the GET requests, TCP Segments received, HTTP content length and Data received in HTTP Response:

|  |  |  |  |
| --- | --- | --- | --- |
| **GET Requests** | **TCP Segments Received** | **HTTP content length (in bytes)** | **Data received in HTTP Response = Reassembled TCP Segments' Data (in bytes)** |
| GET / HTTP/1.1 | 675 | 932903 | 934075 |
| GET /resources/banners/adm\_vgsom.jpg;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 174 | 239142 | 239321 |
| GET /resources/common\_css/common\_stylesheet.css;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 16 | 19530 | 19706 |
| GET /resources/common\_js/common\_js.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 4 | 2835 | 3024 |
| GET /resources/css/bootstrap.min.css;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 103 | 140990 | 141167 |
| GET /resources/css/font-awesome.css;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 27 | 35319 | 35495 |
| GET /resources/css/home\_style.css;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 8 | 8543 | 8718 |
| GET /resources/css/override.css;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 6 | 6640 | 6815 |
| GET /resources/images/hindi.png;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 3 | 2020 | 2196 |
| GET /resources/images/index.png;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 6 | 5574 | 5750 |
| GET /resources/images/logo.png;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 14 | 17073 | 17250 |
| GET /resources/images/nvsp3.png;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 8 | 8947 | 9123 |
| GET /resources/js/bootstrap.min.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 28 | 36868 | 37058 |
| GET /resources/js/jquery.bootstrap.newsbox.min.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 5 | 5267 | 5456 |
| GET /resources/js/jquery.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 70 | 95791 | 95981 |
| GET /resources/js/navigation.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 3 | 1987 | 2176 |
| GET /resources/js/override.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 7 | 7823 | 8012 |
| GET /resources/page\_js/home\_page.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 5 | 4632 | 4821 |
| GET /resources/page\_js/jquery.tickerNews.min.js;jsessionid=0A31EDF4F52A478ACEEFABCDA4BF76B8 HTTP/1.1 | 4 | 3994 | 4183 |