**============================================================**

**Assignment 1 (Part A) Submission**

**Name: Bratin Mondal**

**Roll Number: 21CS10016**

**Link of the pcap file:**

[**https://drive.google.com/file/d/18GhIYapGIlchZ3nXl\_a1jm6R4oL9uRCh/view?usp=sharing**](https://drive.google.com/file/d/18GhIYapGIlchZ3nXl_a1jm6R4oL9uRCh/view?usp=sharing)

**============================================================**

1. **How many packets do you see for the following protocols?**
   1. **TCP and UDP together**
   2. **IPv4 and IPv6?**

Answer:

1. TCP packets: 27949  
   UDP packets: 1537  
   Total: 29486
2. IPv4: 29485

IPv6: 1

1. **What is the total amount of data being received for the following two cases?**
   1. **When you access** [**http://iitkgp.ac.in**](http://iitkgp.ac.in/)
   2. **When you access** [**https://www.cornell.edu**](https://www.cornell.edu/)

Answer:

1. 22868159 bytes
2. 3460269 bytes
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.**
   2. **Can you find out the IP of the DNS servers by exploring the DNS packets?**

Answer:

Total DNS packets observed in total: 1088

|  |  |
| --- | --- |
| **Domain Name** | **IP** |
| **connectivity-check.ubuntu.com** | 2620:2d:4000:1::23,  2001:67c:1562::24,  2001:67c:1562::23,  2620:2d:4000:1::22,  2620:2d:4000:1::2b,  2620:2d:4000:1::2a,  185.125.190.49,  185.125.190.48,  35.232.111.17,  185.125.190.17,  34.122.121.32,  35.224.170.84,  91.189.91.49,  91.189.91.48,  185.125.190.18 |
| **detectportal.firefox.com** | 2600:1901:0:38d7::,  34.107.221.82 |
| **contile.services.mozilla.com** | 34.117.237.239 |
| **spocs.getpocket.com** | 54.81.18.32,  3.231.97.13,  44.215.47.169,  44.205.134.14 |
| **example.org** | 2606:2800:220:1:248:1893:25c8:1946,  93.184.216.34 |
| **ipv4only.arpa** | 192.0.0.171,  192.0.0.170 |
| **content-signature-2.cdn.mozilla.net** | 2600:1901:0:92a9::,  34.160.144.191 |
| **www.facebook.com** | 163.70.143.35,  2a03:2880:f188:84:face:b00c:0:25de |
| **www.wikipedia.org** | 103.102.166.224,  2001:df2:e500:ed1a::1 |
| **www.youtube.com** | 2404:6800:4002:817::200e,  2404:6800:4002:815::200e,  2404:6800:4002:814::200e,  2404:6800:4002:816::200e,  142.250.194.78,  142.250.192.206,  142.250.193.238,  142.250.192.238,  142.250.206.174,  142.250.194.110,  142.250.206.110,  142.250.193.14,  142.250.193.46,  142.250.194.14,  142.250.194.174,  142.250.193.206,  142.250.194.142,  142.250.206.142,  142.250.194.206,  142.250.194.46 |
| **getpocket.com** | 108.159.61.6,  108.159.61.85,  108.159.61.102,  108.159.61.86 |
| **www.reddit.com** | 199.232.101.140 |
| **twitter.com** | 104.244.42.65,  104.244.42.129,  104.244.42.193,  104.244.42.1 |
| **r3.o.lencr.org** | 2600:140f:3::170f:8a9f,  2600:140f:3::170f:8ad7,  184.84.233.67,  184.84.233.97 |
| **img-getpocket.cdn.mozilla.net** | 34.120.237.76,  2600:1901:0:e988:: |
| **firefox.settings.services.mozilla.co**  **m** | 34.149.100.209 |
| **scroll.in** | 142.93.213.69 |
| **www.tastingtable.com** | 18.66.78.24,  18.66.78.97,  18.66.78.3,  18.66.78.19 |
| **www.inverse.com** | 18.66.78.24,  18.66.78.97,  18.66.78.3,  18.66.78.19 |
| **www.cnbc.com** | 104.123.210.231 |
| **www.lonelyplanet.com** | 13.35.191.51,  13.35.191.35,  13.35.191.57,  13.35.191.81 |
| **www.theguardian.com** | 151.101.153.111,  2a04:4e42:24::367 |
| **push.services.mozilla.com** | 34.107.243.93 |
| **safebrowsing.googleapis.com** | 142.250.192.74,  2404:6800:4002:82b::200a |
| **iitkgp.ac.in** | 172.16.3.10 |
| **www.vox.com** | 151.101.153.52 |
| **www.gq-magazine.co.uk** | 199.232.22.133,  2a04:4e42:42::645 |
| **www.nytimes.com** | 151.101.153.164 |
| **www.fastcompany.com** | 151.101.153.54 |
| **incoming.telemetry.mozilla.org** | 34.120.208.123 |
| **ocsp.r2m02.amazontrust.com** | 18.67.196.194 |
| **ocsp.pki.goog** | 142.250.194.131,  2404:6800:4002:81c::2003 |
| **daily.jstor.org** | 23.185.0.2 |
| **thewire.in** | 2606:4700:3031::ac43:b808,  2606:4700:3035::6815:5404,  172.67.184.8,  104.21.84.4 |
| **www.smithsonianmag.com** | 172.67.5.56,  104.22.7.9,  104.22.6.9 |
| **www.outlooktraveller.com** | 2606:4700::6812:5ac6,  2606:4700::6812:5bc6,  2606:4700::6812:5dc6,  2606:4700::6812:5cc6,  2606:4700::6812:5ec6,  104.18.92.198,  104.18.93.198,  104.18.91.198,  104.18.90.198,  104.18.94.198 |
| **bigthink.com** | 172.67.14.204,  104.22.59.144,  104.22.58.144,  2606:4700:10::ac43:ecc,  2606:4700:10::6816:3a90,  2606:4700:10::6816:3b90 |
| **contile-**  **images.services.mozilla.com** | 34.120.115.102 |
| **www.livestrong.com** | 23.57.238.18 |
| **www.technologyreview.com.** | 192.0.66.184 |
| **tastecooking.com** | 23.185.0.2,  2620:12a:8000::2,  2620:12a:8001::2 |
| **cdnjs.cloudflare.com** | 2606:4700::6811:180e,  2606:4700::6811:190e,  104.17.24.14,  104.17.25.14 |
| **code.jquery.com** | 151.101.130.137,  151.101.194.137,  151.101.66.137,  151.101.2.137, 2a04:4e42:600::649,  2a04:4e42:200::649,  2a04:4e42:400::649,  2a04:4e42::649,  151.101.2.137,  151.101.194.137,  151.101.130.137,  151.101.66.137,  151.101.194.137,  151.101.2.137,  151.101.66.137,  151.101.130.137,  2a04:4e42:600::649,  2a04:4e42:200::649,  2a04:4e42::649,  2a04:4e42:400::649 |
| **connect.facebook.net** | 163.70.143.4,  2a03:2880:f0a4:115:face:b00c:0:3 |
| **status.geotrust.com** | 152.195.38.76 |
| **cdn.jsdelivr.net** | 199.232.21.229,  2a04:4e42:42::485 |
| **firefox-api-proxy.cdn.mozilla.net** | 34.149.97.1,  2600:1901:0:74e4:: |
| **fonts.googleapis.com** | 142.251.42.10,  2404:6800:4002:820::200a |
| **shavar.services.mozilla.com** | 34.213.155.5,  52.24.152.80,  44.239.151.67 |
| **www.smithsonianmag.com.cdn.clo**  **udflare.net** | 2606:4700:10::6816:709,  2606:4700:10::ac43:538,  2606:4700:10::6816:609,  2606:4700:10::6816:709,  2606:4700:10::ac43:538,  2606:4700:10::6816:609 |
| **telemetry-incoming.r53-**  **2.services.mozilla.com** | 34.120.208.123 |
| **services.addons.mozilla.org** | 3.160.188.15,  3.160.188.45,  3.160.188.61,  3.160.188.95 |
| **www.wired.com** | 151.101.154.194 |
| **e1483.j.akamaiedge.net** | 104.123.217.133,  104.85.119.162 |
| **jnn-pa.googleapis.com** | 142.250.194.10,  142.250.206.170,  142.250.182.170,  142.250.193.234,  142.250.77.234,  142.250.194.138,  142.250.194.42,  142.250.193.10,  142.250.194.106,  142.250.192.234,  142.250.193.74,  142.250.206.138,  142.250.193.42,  142.250.206.106,  142.250.194.74,  142.250.193.202,  2404:6800:4009:831::200a,  2404:6800:4009:82a::200a,  2404:6800:4009:828::200a,  2404:6800:4009:830::200a |
| **www.google.com** | 2404:6800:4009:821::2004,  142.250.183.36 |
| **i.ytimg.com** | 172.217.167.246,  216.58.196.214,  172.217.27.182,  142.250.193.54,  142.250.192.182,  172.217.166.246,  142.250.77.246,  142.250.182.182,  142.250.193.22,  142.250.193.246,  142.250.193.214,  142.250.192.246,  142.250.77.214,  142.250.193.86,  172.217.167.214,  172.217.166.22,  2404:6800:4009:82b::2016,  2404:6800:4009:827::2016,  2404:6800:4009:823::2016,  2404:6800:4009:829::2016 |
| **www.mozilla.org** | 18.164.190.188 |
| **yt3.ggpht.com** | 216.58.200.193 |
| **photos-**  **ugc.l.googleusercontent.com** | 2404:6800:4009:81e::2001 |
| **www.cornell.edu** | 13.107.246.72,  13.107.213.72,  2620:1ec:bdf::72,  2620:1ec:46::72 |
| **www.amazon.in** | 18.164.192.103,  2405:8a00:1b:686::3bda,  2405:8a00:1b:688::3bda |
| **s.click.aliexpress.com** | 23.57.234.242 |
| **fonts.gstatic.com** | 2404:6800:4002:822::2003,  216.58.196.195 |
| **scontent.xx.fbcdn.net** | 2a03:2880:f0a4:115:face:b00c:0:3 |
| **googleads.g.doubleclick.net** | 142.250.70.98,  2404:6800:4002:825::2002 |
| **platform.twitter.com** | 2606:2800:248:2f:1d8a:787:dc7:17df,  192.229.237.25 |
| **static.doubleclick.net** | 172.217.160.198,  2404:6800:4002:817::2006 |
| **nytimes.map.fastly.net** | 199.232.21.164 |
| **syndication.twitter.com** | 104.244.42.8 |
| **www.linkedin.com** | 3.107.42.14 |
| **www.instagram.com** | 163.70.143.174,  2a03:2880:f288:e4:face:b00c:0:4420 |
| **gateoffice.iitkgp.ac.in** | 203.110.245.11 |
| **som.iitkgp.ac.in** | 10.43.1.6 |
| **pbs.twimg.com** | 199.232.20.159 |
| **dualstack.twimg.twitter.map.fastly.**  **net** | 2a04:4e42:42::159 |
| **play.google.com** | 142.250.193.78,  2404:6800:4002:81b::200e,  172.217.167.14 |
| **abs-0.twimg.com** | 104.244.43.131 |
| **apna.iitkgp.ac.in** | 10.3.100.171 |
| **library.iitkgp.ac.in** | 10.18.24.7 |
| **www.counsellingcentre.iitkgp.ac.in** | 203.110.245.243 |
| **oldish.iitkgp.ac.in** | 10.3.100.102 |
| **www.tgh.iitkgp.ac.in** | 203.110.245.243 |
| **mail.google.com** | 142.250.193.37,  2404:6800:4002:815::2005 |
| **iitkgpmail.iitkgp.ac.in** | 10.3.100.244 |
| **www.nvsp.in** | 61.0.172.246 |
| **www.vidyalakshmi.co.in** | 121.240.246.10 |
| **www.pmrf.in** | 13.234.100.116,  13.200.123.229, 65.0.79.182 |
| **abs.twimg.com** | 152.199.43.83 |
| **cs510.wpc.edgecastcdn.net** | 2606:2800:247:9376:8aa7:779e:f6d9:de02 |
| **www.ncwwomenhelpline.in** | 18.164.202.59,  18.164.202.99,  18.164.202.108,  18.164.202.24 |
| **www.g20.org** | 189.9.176.149 |
| **erp.iitkgp.ac.in** | 10.57.7.12,  10.57.7.11 |
| **dualstack.guardian.map.fastly.net** | 2a04:4e42:42::367 |
| **scontent-bom2-1.xx.fbcdn.net** | 163.70.143.4,  2a03:2880:f0a4:3:face:b00c:0:3 |
| **star-mini.c10r.facebook.com** | 163.70.143.35,  2a03:2880:f188:84:face:b00c:0:25de,  163.70.144.35,  2a03:2880:f188:84:face:b00c:0:25de |
| **static.xx.fbcdn.net** | 163.70.143.4 |
| **scontent-bom1-1.xx.fbcdn.net** | 157.240.16.20,  2a03:2880:f02f:13:face:b00c:0:3 |
| **h2.condenast.map.fastly.net** | 151.101.154.194 |
| **external-bom1-1.xx.fbcdn.net** | 157.240.16.20 |
| **scontent-bom1-2.xx.fbcdn.net** | 31.13.79.26,  2a03:2880:f02f:11b:face:b00c:0:3 |
| **video-bom2-1.xx.fbcdn.net** | 163.70.143.22,  2a03:2880:f0a4:17:face:b00c:0:1823 |
| **video-bom1-2.xx.fbcdn.net** | 2a03:2880:f02f:114:face:b00c:0:1823,  31.13.79.20 |
| **aus5.mozilla.org** | 35.244.181.201 |
| **versioncheck-**  **bg.addons.mozilla.org** | 34.160.90.233 |
| **normandy.cdn.mozilla.net** | 35.201.103.21 |
| **a1887.dscq.akamai.net** | 180.149.59.136, 180.149.59.144,  2405:8a00:14:1::b495:3b90,  2405:8a00:14:1::b495:3b88 |
| **classify-client.services.mozilla.com** | 34.98.75.36 |
| **z-p42-**  **instagram.c10r.instagram.com** | 163.70.143.174,  2a03:2880:f288:e4:face:b00c:0:4420 |
| **cornell-edge-**  **ekhkdhg5czdmb2bf.z01.azurefd.net** | 13.107.213.72,  13.107.246.72 |
| **part-0044.t-0009.t-msedge.net** | 2620:1ec:46::72,  2620:1ec:bdf::72 |
| **use.typekit.net** | 180.149.59.145,  180.149.59.147 |
| **www.googletagmanager.com** | 172.217.161.8,  2404:6800:4009:802::2008 |
| **ajax.googleapis.com** | 142.250.207.202,  2404:6800:4002:81e::200a |
| **media.univcomm.cornell.edu** | 13.107.246.72,  13.107.213.72,  2620:1ec:bdf::72,  2620:1ec:46::72 |
| **a1988.dscg1.akamai.net** | 2600:140f:6::1739:4bd0,  2600:140f:6::1739:4bc2 |
| **ssl.google-analytics.com** | 142.250.76.168,  2404:6800:4009:806::2008 |
| **siteimproveanalytics.com** | 104.21.50.150,  172.67.163.237,  2606:4700:3030::ac43:a3ed,  2606:4700:3035::6815:3296 |
| **www.google-analytics.com** | 142.250.206.142,  2001:4860:4802:34::178,  2001:4860:4802:38::178,  2001:4860:4802:36::178,  2001:4860:4802:32::178 |
| **p.typekit.net** | 49.44.116.86,  49.44.116.78 |
| **a1874.dscg1.akamai.net** | 2600:140f:6::172c:b12,  2600:140f:6::172c:b1a |
| **cdnsecakmi.kaltura.com** | 23.35.94.115 |
| **6120104.global.siteimproveanalytic**  **s.io** | 13.49.88.20,  51.20.213.244 |
| **ocsp.r2m03.amazontrust.com** | 13.35.189.111 |
| **stats.g.doubleclick.net** | 172.217.194.157, 172.217.194.156,  172.217.194.154, 172.217.194.155,  2404:6800:4003:c02::9c,  2404:6800:4003:c02::9b,  2404:6800:4003:c02::9a,  2404:6800:4003:c02::9d |

1. Determining the IP address of the Local DNS is feasible as DNS queries from my machine are directed to it.  
   The Local DNS IP is 172.16.1.166
2. **Answer the following when you access the site** [**http://iitkgp.ac.in**](http://iitkgp.ac.in/)**.**
   1. **How many HTTP GET requests do you observe? List down the GET requests.**
   2. **For each of the HTTP GET requests 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:

1. 7 HTTP GET requests are observed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Serial**  **Number** | **Source** | **Destination** | **Length (bytes)** | **Information** |
| 329 | 10.145.238.72 | 172.16.3.10 | 461 | **GET / HTTP/1.1** |
| 2525 | 10.145.238.72 | 172.16.3.10 | 436 | **GET /assets/images/about-iitk-video.jpg HTTP/1.1** |
| 2685 | 10.145.238.72 | 172.16.3.10 | 492 | **GET / HTTP/1.1** |
| 7646 | 10.145.238.72 | 172.16.3.10 | 410 | **GET / HTTP/1.1** |
| 9481 | 10.145.238.72 | 172.16.3.10 | 436 | **GET /assets/images/about-iitk-video.jpg HTTP/1.1** |
| 9553 | 10.145.238.72 | 172.16.3.10 | 438 | **GET /assets/images/about-iitk-video.jpg HTTP/1.1** |
| 10045 | 10.145.238.72 | 172.16.3.10 | 494 | **GET / HTTP/1.1** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial**  **Number** | **Information** | **The total number of TCP segments being received** | **The total amount of data being received in the corresponding HTTP Response message** |
| 329 | **GET / HTTP/1.1** | 157 | 432289 bytes |
| 2525 | **GET /assets/images/about-iitk-video.jpg HTTP/1.1** | 7 | 19690 bytes |
| 2685 | **GET / HTTP/1.1** | 66 | 181012 bytes |
| 7646 | **GET / HTTP/1.1** | 106 | 316876 bytes |
| 9481 | **GET /assets/images/about-iitk-video.jpg HTTP/1.1** | 7 | 19690 bytes |
| 9553 | **GET /assets/images/about-iitk-video.jpg HTTP/1.1** | 8 | 19690 bytes |
| 10045 | **GET / HTTP/1.1** | 84 | 241568 bytes |