Assignment 1 (Part A) Submission

Name: Tanishq Prasad

Roll number: 21CS30054

Link of the pcap file:
https://drive.google.com/file/d/1nEs4Hq9zbtEOL7i7i6mbIFkP79YenWn8/view?usp=drive_link

1)

a) TCP = 16321 packets
UDP = 384 packets
In Total = 16705 packets
(by using tcp and udp as filters, respectively)

b) IPv4 = 16705
IPv6 = 0
(by using ip and ipv6 as filters, respectively)

2)

a) http://iitkgp.ac.in/ had the IP address as - 172.16.3.10 (by using dns.resp.name=="iitkgp.ac.in" filter)
Packets received = 7870
The total amount of data = 12257711 bytes

b) https://www.cornell.edu/ had two IP addresses (by looking at IPv4 DNS packets and looking at the answers of the query response, specifically by packet no. 16508)

1) 13.107.246.72
   - Packets received = 2
   - The total amount of data = 148 bytes
2) 13.107.213.72
   - Packets received = 15
   - The total amount of data = 1374 bytes

3) Total DNS packets = 332 (by using dns as filter)

a) The table is attached as screenshots:- (Statistics -> Resolved Addresses -> Pop-up window (Select hosts))

Address	Name
180.149.59.144	a1887.dscq.akamai.net
180.149.59.136	a1887.dscq.akamai.net
184.84.233.97	a1887.dscq.akamai.net
184.84.233.67	a1887.dscq.akamai.net
2405:8a00:14:1::b495:3b88	a1887.dscq.akamai.net
2405:8a00:14:1::b495:3b90	a1887.dscq.akamai.net
180.149.59.145	a1988.dscg1.akamai.net
180.149.59.147	a1988.dscg1.akamai.net
2405:8a00:14:1::b495:3b93	a1988.dscg1.akamai.net
2405:8a00:14:1::b495:3b91	a1988.dscg1.akamai.net
104.244.43.131	abs-zero.twimg.com
216.58.196.202	ajax.googleapis.com
2404:6800:4009:820::200a	ajax.googleapis.com
34.107.243.93	autopush.prod.mozaws.net
104.17.24.14	cdnjs.cloudflare.com
104.17.25.14	cdnjs.cloudflare.com
2606:4700::6811:190e	cdnjs.cloudflare.com
2606:4700::6811:180e	cdnjs.cloudflare.com
151.101.66.137	code.jquery.com
151.101.194.137	code.jquery.com
151.101.2.137	code.jquery.com
151.101.130.137	code.jquery.com
2a04:4e42:400::649	code.jquery.com
2a04:4e42::649	code.jquery.com
2a04:4e42:600::649	code.jquery.com
2a04:4e42:200::649	code.jquery.com
34.117.237.239	contile.services.mozilla.com
192.229.237.25	cs491.wac.edgecastcdn.net
2606:2800:248:2f:1d8a:787:dc7:17df	cs491.wac.edgecastcdn.net
192.229.237.101	cs505.wac.edgecastcdn.net

Address	Name
2606:2800:248:1707:10d3:19d0:1ba2:1a23	cs505.wac.edgecastcdn.net
152.199.43.83	cs510.wpc.edgecastcdn.net
2606:2800:247:9376:8aa7:779e:f6d9:de02	cs510.wpc.edgecastcdn.net
185.199.108.153	darkreader.org
185.199.109.153	darkreader.org
185.199.110.153	darkreader.org
185.199.111.153	darkreader.org
23.205.218.112	e4350.g.akamaiedge.net
93.184.216.34	example.org
2606:2800:220:1:248:1893:25c8:1946	example.org
2404:6800:4002:816::200a	fonts.googleapis.com
142.250.194.163	fonts.gstatic.com
2404:6800:4002:80a::2003	fonts.gstatic.com
152.195.38.76	fp2e7a.wpc.phicdn.net
142.250.183.118	i.ytimg.com
142.251.42.86	i.ytimg.com
216.58.203.54	i.ytimg.com
142.250.71.118	i.ytimg.com
142.250.182.214	i.ytimg.com
142.250.192.22	i.ytimg.com
172.217.166.54	i.ytimg.com
142.250.192.54	i.ytimg.com
142.250.77.54	i.ytimg.com
142.250.192.86	i.ytimg.com
142.250.77.86	i.ytimg.com
142.250.192.118	i.ytimg.com
142.250.183.86	i.ytimg.com
142.250.192.150	i.ytimg.com
142.251.42.54	i.ytimg.com
142.250.76.182	i.ytimg.com

Address	Name
2404:6800:4009:81a::2016	i.ytimg.com
2404:6800:4009:822::2016	i.ytimg.com
2404:6800:4009:823::2016	i.ytimg.com
2404:6800:4009:80f::2016	i.ytimg.com
192.0.0.171	ipv4only.arpa
192.0.0.170	ipv4only.arpa
142.250.77.74	jnn-pa.googleapis.com
142.250.70.42	jnn-pa.googleapis.com
142.250.70.74	jnn-pa.googleapis.com
142.250.183.138	jnn-pa.googleapis.com
142.251.42.106	jnn-pa.googleapis.com
142.250.70.106	jnn-pa.googleapis.com
142.250.183.170	jnn-pa.googleapis.com
142.250.71.106	jnn-pa.googleapis.com
142.250.182.202	jnn-pa.googleapis.com
172.217.174.74	jnn-pa.googleapis.com
142.250.183.202	jnn-pa.googleapis.com
142.250.182.234	jnn-pa.googleapis.com
142.250.66.10	jnn-pa.googleapis.com
142.250.199.138	jnn-pa.googleapis.com
142.250.183.10	jnn-pa.googleapis.com
142.250.199.170	jnn-pa.googleapis.com
2404:6800:4009:826::200a	jnn-pa.googleapis.com
2404:6800:4009:824::200a	jnn-pa.googleapis.com
2404:6800:4009:825::200a	jnn-pa.googleapis.com
151.101.153.229	jsdelivr.map.fastly.net
2a04:4e42:42::485	jsdelivr.map.fastly.net
13.107.246.72	part-0044.t-0009.t-msedge.net
13.107.213.72	part-0044.t-0009.t-msedge.net
2620:1ec:bdf::72	part-0044.t-0009.t-msedge.net

Address	Name
142.250.182.193	photos-ugc.l.googleusercontent.com
2404:6800:4009:81e::2001	photos-ugc.l.googleusercontent.com
142.250.192.227	pki-goog.l.google.com
2404:6800:4009:82b::2003	pki-goog.l.google.com
34.160.144.191	prod.content-signature-chains.prod.webservices.mozgcp.net
2600:1901:0:92a9::	prod.content-signature-chains.prod.webservices.mozgcp.net
34.107.221.82	prod.detectportal.prod.cloudops.mozgcp.net
2600:1901:0:38d7::	prod.detectportal.prod.cloudops.mozgcp.net
34.149.100.209	prod.remote-settings.prod.webservices.mozgcp.net
95.216.195.133	redirect.archlinux.org
2a01:4f9:c010:2636::1	redirect.archlinux.org
142.250.206.138	safebrowsing.googleapis.com
2404:6800:4002:813::200a	safebrowsing.googleapis.com
157.240.16.20	scontent-bom1-1.xx.fbcdn.net
2a03:2880:f02f:13:face:b00c:0:3	scontent-bom1-1.xx.fbcdn.net
31.13.79.26	scontent-bom1-2.xx.fbcdn.net
2a03:2880:f02f:11b:face:b00c:0:3	scontent-bom1-2.xx.fbcdn.net
163.70.143.4	scontent.xx.fbcdn.net
2a03:2880:f0a4:3:face:b00c:0:3	scontent.xx.fbcdn.net
163.70.144.35	star-mini.c10r.facebook.com
2a03:2880:f188:181:face:b00c:0:25de	star-mini.c10r.facebook.com
104.244.42.136	syndication.twitter.com
34.120.208.123	telemetry-incoming.r53-2.services.mozilla.com
142.250.193.36	www.google.com
2404:6800:4009:82d::2004	www.google.com
172.16.3.10	www.iitkgp.ac.in
142.250.70.46	youtube-ui.l.google.com
142.250.70.78	youtube-ui.l.google.com
142.250.183.142	youtube-ui.l.google.com
142.251.42.110	youtube-ui.l.google.com

142.250.70.110	youtube-ui.l.google.com
142.250.183.174	youtube-ui.l.google.com
142.250.71.110	youtube-ui.l.google.com
142.250.182.206	youtube-ui.l.google.com
142.250.183.206	youtube-ui.l.google.com
142.250.182.238	youtube-ui.l.google.com
142.250.66.14	youtube-ui.l.google.com
142.250.199.142	youtube-ui.l.google.com
142.250.77.46	youtube-ui.l.google.com
142.250.183.14	youtube-ui.l.google.com
142.250.199.174	youtube-ui.l.google.com
142.250.77.78	youtube-ui.l.google.com
2404:6800:4009:81a::200e	youtube-ui.l.google.com
2404:6800:4009:813::200e	youtube-ui.l.google.com
2404:6800:4009:80d::200e	youtube-ui.l.google.com
2404:6800:4009:80a::200e	youtube-ui.l.google.com

b) Yes, we can find the IP of the DNS servers by looking at the Source of DNS query responses or the Destination of the DNS queries.
It was seen that 172.16.1.166 was the only one.

4) While accessing http://iitkgp.ac.in/ :-

a) 5 HTTP GET requests were observed (filter :- http and ip.dst_host=="172.16.3.10")

No.	Time	Source	Destination	Protocol	Length	Info
311	6.620785	10.145.70.96	172.16.3.10	HTTP	455	GET / HTTP/1.1
1162	7.740987	10.145.70.96	172.16.3.10	HTTP	486	GET / HTTP/1.1
3590	8.959595	10.145.70.96	172.16.3.10	HTTP	430	GET /assets/images/about-iitk-video.jpg HTTP/1.1
7761	11.493623	10.145.70.96	172.16.3.10	HTTP	455	GET / HTTP/1.1
9750	12.901402	10.145.70.96	172.16.3.10	HTTP	486	GET / HTTP/1.1

b) By exploring the packets and looking at the description of their response packets

Packet No.	Response Packet No.	TCP Segments	Total Data (in bytes)
311	932	293	433222
1162	5241	300	433214
3590	4454	14	19691
7761	No Response	0	0
9750	No Response	0	0

Information for the last two HTTP GET packets

```
▸ Frame 7761: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits)
▸ Ethernet II, Src: AzureWav_f4:fd:1d (48:e7:da:f4:fd:1d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
▸ Internet Protocol Version 4, Src: 10.145.70.96, Dst: 172.16.3.10
▸ Transmission Control Protocol, Src Port: 58008, Dst Port: 80, Seq: 810, Ack: 866437, Len: 389
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: iitkgp.ac.in\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  ▾ Cookie: ci_session=selc16ku6fn6rr8f63kdq3j3uonf2u1g\r\n
      Cookie pair: ci_session=selc16ku6fn6rr8f63kdq3j3uonf2u1g
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://iitkgp.ac.in/]
    [HTTP request 3/3]
    [Prev request in frame: 1162]
```

```
▸ Frame 9750: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits)
▸ Ethernet II, Src: AzureWav_f4:fd:1d (48:e7:da:f4:fd:1d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
▸ Internet Protocol Version 4, Src: 10.145.70.96, Dst: 172.16.3.10
▸ Transmission Control Protocol, Src Port: 58020, Dst Port: 80, Seq: 365, Ack: 19692, Len: 420
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: iitkgp.ac.in\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://iitkgp.ac.in/\r\n
    Connection: keep-alive\r\n
  ▾ Cookie: ci_session=selc16ku6fn6rr8f63kdq3j3uonf2u1g\r\n
      Cookie pair: ci_session=selc16ku6fn6rr8f63kdq3j3uonf2u1g
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://iitkgp.ac.in/]
    [HTTP request 2/2]
    [Prev request in frame: 3590]
```