

# CS-349 Networks Lab

## Assignment – 2

By- ABHINAV GUPTA (150123001)

Drive link for traces: [https://drive.google.com/open?id=1ugelOuniObiCyt\\_k\\_oIBLZXGBpujazeRa](https://drive.google.com/open?id=1ugelOuniObiCyt_k_oIBLZXGBpujazeRa)

Nomenclature of trace files: pp (play-pause trace), up(upload trace), d(download trace)

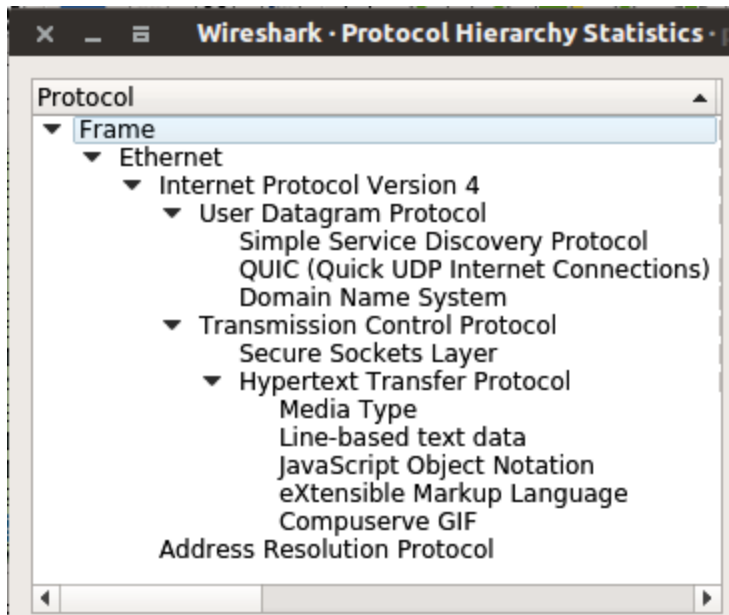
My main source of internet for all readings was Airtel No-Proxy Hotspot.

Second Alternate Readings are from Hostel Room IP.

Dailymotion Videos were downloaded from this website while performing tasks - " en.savefrom.net "

(9am-pp1 trace file used while answering first 2 questions)

**Ans-1:** All the protocols used by the application at different layers are listed below:



In the obtained protocols, **HTTP** protocol works in Application Layer, **SSL** in presentation layer and all other work in transport Layer.

**Flags and options** explained below:

- **Source port:** This is the port number associated with the sender side
- **Destination port:** Port number associated with the recipient side
- **Sequence number:** These are the unique values that are used to ensure reliable delivery of data.
- **Acknowledgement number:** Response from the receiver side as part of the confirmation process that the packet was successfully received.
- **Data offset:** This indicates where the data packet begins and the length of the TCP header.
- **Flags:** There are various types of flag bits present. They initiate connection, carry data, and tear down connections. Their functionality is as follows:
- **SYN (synchronize):** Packets that are used to initiate a connection that is commonly known as the handshake process.
- **ACK (acknowledgement):** These packets are used to confirm that the data packets have been received, and this also confirms the initiation and tear down of the connections.
- **RST (reset):** These packets signify that the connection you were trying to create has been shut down or may be the application we were trying to communicate with is not accepting connections.
- **FIN (finish):** These packets indicate that the connection is being torn down after the successful delivery of data packets.
- **PSH (push):** These packets indicate that the incoming data should be passed on directly to the application instead of getting buffered.
- **URG (urgent):** Marked packets indicate that the data that the packet is carrying should be processed immediately by the TCP stack and the urgent pointer field should be examined if it is set.
- **CWR (Congestion Window Reduced):** These packets are used by the sender to inform the receiver that the buffer is getting overfilled, and because of congestion, both the parties should slow down the transmission process to avoid any packet loss that might happen.
- **Window size:** This field in the header indicates the amount of data that the sender can send.
- **Checksum:** To cross check the contents of the TCP segments.
- **Urgent pointer:** This field tells us about the value that the urgent pointer contains. It specifically indicates the sequence number of the octet that lies before the data.
- **Options:** This field has three parts: length of the option, options being used, options in use. One of the important options **Maximum Segment Size (MSS)** is also part of this field.
- **Data:** The last part in the TCP header is the real data that travels around

## TCP:

```
▶ Frame 6: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
▶ Ethernet II, Src: XiaomiCo_c2:d1:a1 (38:a4:ed:c2:d1:a1), Dst: Tp-LinkT_7f:8a:65 (d4:6e:0e:7f:8a:65)
▶ Internet Protocol Version 4, Src: 5.63.145.102, Dst: 192.168.43.20
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 43338, Seq: 5553, Ack: 1, Len: 1388
  Source Port: 80
  Destination Port: 43338
  [Stream index: 0]
  [TCP Segment Len: 1388]
  Sequence number: 5553 (relative sequence number)
  [Next sequence number: 6941 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....1... = Acknowledgment: Set
    ....0... = Push: Not set
    ....0... = Reset: Not set
    ....0... = Syn: Not set
    ....0... = Fin: Not set
    [TCP Flags: .....A....]
  Window size value: 125
  [Calculated window size: 125]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x32dd [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
  TCP payload (1388 bytes)
```

## HTTP:

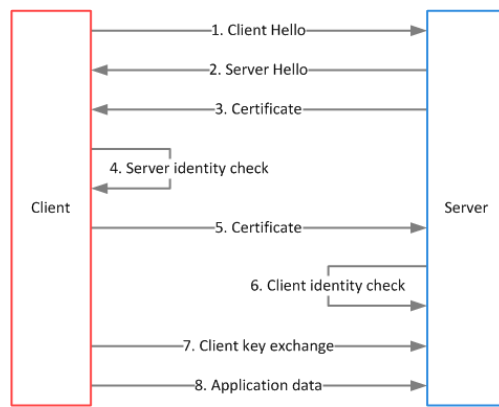
The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, and hypermedia information systems. HTTP functions as a request-response protocol in the client-server computing model.

```
▶ Internet Protocol Version 4, Src: 192.168.43.20, Dst: 54.68.212.98
▶ Transmission Control Protocol, Src Port: 48076, Dst Port: 80, Seq: 1, Ack: 1, Len: 1193
▼ Hypertext Transfer Protocol
  ▶ [truncated]GET /iframe/8613/?che=523918803&c=%7B%22bid%22%3A%22dailymotion%22%2C%22loc%22%3A%22http%3A%2F%2Fwww.dailymotion.com%2Fvid
    Host: d.agkn.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.167 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Referer: http://www.dailymotion.com/video/x68pyo4\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  ▶ [truncated]Cookie: aa=0001%3AJp9NG8isNWX00P5ftjHVDQLgE2Wy%2F6SaJBen0z%2F%2BWPWEghumYxnZHLqfpNnhKd1%2BoB3oSecHgHSbrr7l6qXiCJDx9ei%2Faou
    \r\n
  [Full request URI [truncated]: http://d.agkn.com/iframe/8613/?che=523918803&c=%7B%22bid%22%3A%22dailymotion%22%2C%22loc%22%3A%22http%3
  [HTTP request 1/1]
```

## TLSv1.2:

Transport Layer Security (TLS) – and its predecessor, Secure Sockets Layer (SSL), which is now prohibited from use by the Internet Engineering Task Force (IETF) – are cryptographic protocols that provide communications security over a computer network.

```
▶ Frame 28: 729 bytes on wire (5832 bits), 729 bytes captured (5832 bits) on interface 0
▶ Ethernet II, Src: XiaomiCo_c2:d1:a1 (38:a4:ed:c2:d1:a1), Dst: Tp-LinkT_7f:8a:65 (d4:6e:0e:7f:8a:65)
▶ Internet Protocol Version 4, Src: 35.190.84.46, Dst: 192.168.43.20
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 48460, Seq: 98, Ack: 1, Len: 663
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 528
    Encrypted Application Data: 00000000000000006325a066d13cd25d8d655287dfba3b7dc4...
  ▶ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
```



## DNS:

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

```

Frame 7: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: Tp-LinkT_7f:8a:65 (d4:6e:0e:7f:8a:65), Dst: XiaomiCo_c2:d1:a1 (38:a4:ed:c2:d1:a1)
Internet Protocol Version 4, Src: 192.168.43.20, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 58900, Dst Port: 53
  Source Port: 58900
  Destination Port: 53
  Length: 37
  Checksum: 0x858b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  Domain Name System (query)
    [Response In: 15]
    Transaction ID: 0x165c
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
  
```

## QUIC:

QUIC supports a set of multiplexed connections between two endpoints over User Datagram Protocol (UDP), and was designed to provide security protection equivalent to TLS/SSL, along with reduced connection and transport latency, and bandwidth estimation in each direction to avoid congestion.

## SSDP:

The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet Protocol Suite for advertisement and discovery of network services and presence information. It accomplishes this without assistance of server-based configuration mechanisms, such as the Dynamic Host Configuration Protocol (DHCP) or the Domain Name System (DNS), and without special static configuration of a network host.

```

Frame 3853: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
Ethernet II, Src: Tp-LinkT_7f:8a:65 (d4:6e:0e:7f:8a:65), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.43.20, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 46939, Dst Port: 1900
  Simple Service Discovery Protocol
    M-SEARCH * HTTP/1.1\r\n
      HOST: 239.255.255.250:1900\r\n
      MAN: "ssdp:discover"\r\n
      MX: 1\r\n
      ST: urn:dial-multiscreen-org:service:dial:1\r\n
      USER-AGENT: Google Chrome/64.0.3282.167 Linux\r\n
      \r\n
      [Full request URI: http://239.255.255.250:1900*]
      [HTTP request 4/4]
      [Prev request in frame: 3820]
  
```

## ARP:

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

## Ans-2: Main Protocols are

### TCP: Protocol Number (6)

Ethernet-Address,	Source addr.:	Tp-LinkT_7f:8a:65 ( <b>d4:6e:0e:7f:8a:65</b> ),	
	Destination addr.:	XiaomiCo_c2:d1:a1 ( <b>38:a4:ed:c2:d1:a1</b> )	
	Type:	IPv4 ( <b>0x0800</b> )	
Internet Protocol Version 4,	Source IP:	<b>192.168.43.20</b> ,	Destination IP: <b>188.65.124.58</b>
Transmission Control Protocol,	Source Port:	<b>44400</b> ,	Destination Port: <b>80</b> ,
Sequence No.: <b>402</b> ,	Acknowledgement No.:	<b>1</b> ,	Packet Length: <b>1388</b>

### HTTP:

Ethernet-Address, Source addr.: Tp-LinkT\_7f:8a:65 (**d4:6e:0e:7f:8a:65**),  
Destination addr.: XiaomiCo\_c2:d1:a1 (**38:a4:ed:c2:d1:a1**)  
Type: IPv4 (**0x0800**)  
Internet Protocol Version 4, Source IP: **192.168.43.20**, Destination IP: **151.101.38.2**  
Transmission Control Protocol, Source Port: **44144**, Destination Port: **80**,  
Sequence No.: **2777**, Acknowledgement No.: **1**, Packet Length: **180**

### TLSv1.2:

Ethernet-Address, Source addr.: XiaomiCo\_c2:d1:a1 (**38:a4:ed:c2:d1:a1**)  
Destination addr.: Tp-LinkT\_7f:8a:65 (**d4:6e:0e:7f:8a:65**)  
Type: IPv4 (**0x0800**)  
Internet Protocol Version 4, Source IP: **35.190.84.46**, Destination IP: **192.168.43.20**  
Transmission Control Protocol, Source Port: **443**, Destination Port: **48460**,  
Sequence No.: **4827**, Acknowledgement No.: **47**, Packet Length: **97**

### SSDP:

Ethernet-Address, Source addr.: Tp-LinkT\_7f:8a:65 (**d4:6e:0e:7f:8a:65**),  
Destination addr.: IPv4mcast\_7f:ff:fa(**01:00:5e:7f:ff:fa**)  
Type: IPv4 (**0x0800**)  
Internet Protocol Version 4, Source IP: **192.168.43.20**, Destination IP: **239.255.255.250**  
Transmission Control Protocol, Source Port: **41016**, Destination Port: **1900** ,  
Sequence No.: **93**, Acknowledgement No.: **170**, Packet Length: **1360**

## Ans-3: Series of Events:

Whenever we load a website or something, host to IP lookup is triggered using DNS protocol (UDP). We may also have some ARP packets due to our ethernet/wifi connection's broadcast messages .A http request is fired up and nodes are created for intercommunication.In the transport layer TCP helps in establishing a correct communication through **three-way handshake** which ensured that both client and server are ready.New data packets are sent and acknowledged time to time through tcp protocol. TCP helps in correct teardown.MP4 protocol is sent at-last when upload is successful.

**Yes, there are TCP Handshaking sequences in the applications as explained below:**

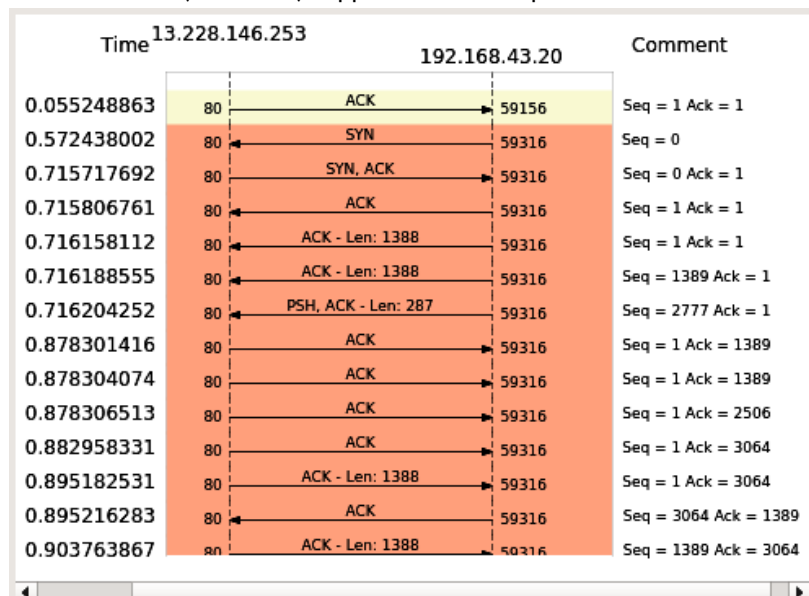
In TCP, the two parties keep track of what they have sent by using a Sequence number. Effectively it ends up being a running byte count of everything that was sent. The receiving party can use the opposite speaker's sequence number to acknowledge what it has received.

But the sequence number doesn't start at 0. It starts at the ISN (Initial Sequence Number), which is a randomly chosen value. And since TCP is a bi-directional communication, both parties can "speak", and therefore both must randomly generate an ISN as their starting Sequence Number. Which in turn means, both parties need to notify the other party of their starting ISN.

So you end up with this sequence of events for a start of a TCP conversation between "Host-A" and "Host-B":

"Host-A" ----> "Host-B" SYNchronize with my Initial Sequence Number of X  
"Host-A" <--- "Host-B" I received your syn, I ACKnowledge that I am ready for [X+1]  
"Host-A" <--- "Host-B" SYNchronize with my Initial Sequence Number of Y  
"Host-A" ----> "Host-B" I received your syn, I ACKnowledge that I am ready for [Y+1]  
Notice, four events are occurring:

In actuality though, the middle two events (#2 and #3) happen in the same packet.



(Fig. 1)

What makes a packet a SYN or ACK is simply a binary flag turned on or off inside each TCP header, so there is nothing preventing both of these flags from being enabled on the same packet.

```

▼ Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... ....0 = Push: Not set
.... ....0 = Reset: Not set
.... ....0 = Syn: Not set
.... ....0 = Fin: Not set
[TCP Flags: .....A....]

```

(Fig 2)

#### Ans-4:

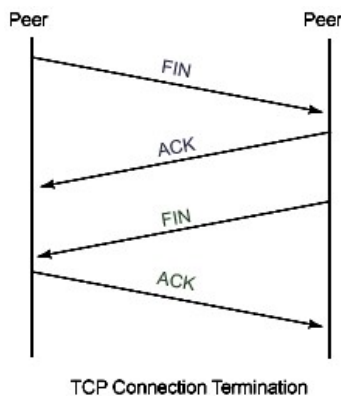
##### How the transactions works:

Firstly whenever we load a website or something, host to IP lookup is triggered using DNS protocol (UDP). We may also have some ARP packets due to our ethernet/wifi connection's broadcast messages.

The HTTP protocol can be likened to a conversation based on a series of questions and answers, which we refer to respectively as HTTP requests and HTTP responses.

The contents of HTTP requests and responses are easy to read and understand, being near to plain English in their syntax.

A http request is fired up and nodes are created for intercommunication. In the transport layer TCP helps in establishing a correct communication through **three-way handshake** which ensured that both client and server are ready. Then when each and every segment of video loads on **dailymotion.com**, new data packets are sent and acknowledged time to time through tcp protocol. TCP helps in correct teardown of the process by the following sequence of packets:



The TCP/IP protocol is designed such that each computer or device in a network has a unique "IP Address" (Internet Protocol Address) and each IP address can open and communicate over up to 65535 different "ports" for sending and receiving data to or from any other network device. The IP Address uniquely identifies the computer or device on the network and a "Port Number" identifies a specific connection between one computer or device and another (i.e between two IP Addresses). A TCP/IP "port" can be thought of as a private two-way communications line where the port number is used to identify a unique connection between two devices. The concept is very similar to any other type of port on your PC (serial, parallel, etc) except that instead of having a physical connection, the TCP/IP protocol creates a "virtual IP port" and the network hardware and software is responsible for routing data in and out of each virtual IP port.

The Transmission Control Protocol provides a considerable number of services to the IP layer and the upper layers. Most importantly, it provides a connection-oriented protocol to the upper layers that enable an application to be sure that a datagram sent out over the network was received in its entirety. In this role, TCP acts as a message-validation protocol providing reliable communications. If a datagram is corrupted or lost, it is usually TCP (not the applications in the higher layers) that handles the retransmission.

**Ans-5:** Data is collected according to "Play and Pause traces". Data is collected after putting filter in each file with ip's of dailymotion got from **Statistics->Resolved Addresses**. As the list is different for different file so exact filter is not possible.

All the below stats are extracted from pp1 (play-pause 1) files from each time of day.

**RTT:-** Got from TCP Syn/Ack Packet (as there's no general method for it)

**# of UDP/TCP:** Got from protocol hierarchy

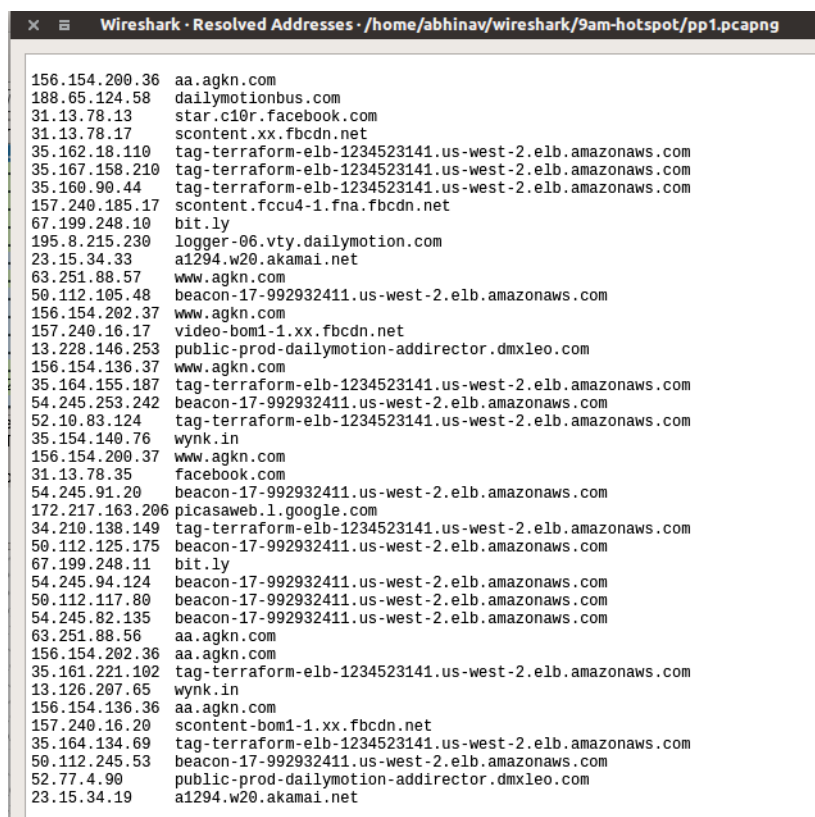
	09:00 hrs	13:00 hrs	18:00 hrs
Throughput	37,468.65 Bytes/sec	88116.05 Bytes/sec	75837.3 Bytes/sec

RTT	.343034614 sec	.287104089 sec	.173759512 sec
Packet Size	658.5 Bytes	830.5 Bytes	808.5 Bytes
No. of Packets Lost	1	28	1
UDP Packets	59	4	25
TCP Packets	2240	2900	2304
No. of responses received per request sent	1.2	1.0	1.4

## Ans-6:

Packets from “**dailymotion.com**” come from different-different servers across the world. Few IP’s of the content providers are listed below:

IP’s with “dailymotion” in their hostname correspond to servers of “dailymotion.com”.



IP Address	Hostname
156.154.200.36	aa.agkn.com
188.65.124.58	dailymotionbus.com
31.13.78.13	star.c10r.facebook.com
31.13.78.17	scontent.xx.fbcdn.net
35.162.18.110	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
35.167.158.210	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
35.160.90.44	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
157.240.185.17	scontent.fccu4-1.fna.fbcdn.net
67.199.248.10	bit.ly
195.8.215.230	logger-06.vty.dailymotion.com
23.15.34.33	a1294.w20.akamai.net
63.251.88.57	www.agkn.com
50.112.105.48	beacon-17-992932411.us-west-2.elb.amazonaws.com
156.154.202.37	www.agkn.com
157.240.16.17	video-bom1-1.xx.fbcdn.net
13.228.146.253	public-prod-dailymotion-addirector.dmxleo.com
156.154.136.37	www.agkn.com
35.164.155.187	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
54.245.253.242	beacon-17-992932411.us-west-2.elb.amazonaws.com
52.10.83.124	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
35.154.140.76	wynk.in
156.154.200.37	www.agkn.com
31.13.78.35	facebook.com
54.245.91.20	beacon-17-992932411.us-west-2.elb.amazonaws.com
172.217.163.206	picasaweb.l.google.com
34.210.138.149	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
50.112.125.175	beacon-17-992932411.us-west-2.elb.amazonaws.com
67.199.248.11	bit.ly
54.245.94.124	beacon-17-992932411.us-west-2.elb.amazonaws.com
50.112.117.80	beacon-17-992932411.us-west-2.elb.amazonaws.com
54.245.82.135	beacon-17-992932411.us-west-2.elb.amazonaws.com
63.251.88.56	aa.agkn.com
156.154.202.36	aa.agkn.com
35.161.221.102	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
13.126.207.65	wynk.in
156.154.136.36	aa.agkn.com
157.240.16.20	scontent-bom1-1.xx.fbcdn.net
35.164.134.69	tag-terraform-elb-1234523141.us-west-2.elb.amazonaws.com
50.112.245.53	beacon-17-992932411.us-west-2.elb.amazonaws.com
52.77.4.90	public-prod-dailymotion-addirector.dmxleo.com
23.15.34.19	a1294.w20.akamai.net

**Listing few of them:** 103.195.32.1 ,103.195.32.14 ,151.101.38.2 ,188.65.124.58, 188.65.124.64, 195.8.215.226 , 195.8.215.171, 195.8.215.136, 13.228.146.253

Multiple sources exist maybe because of the following reasons:

- **Load Balancing** - Distributing network traffic across a server
- **Geographic location** - Ideal scenario is for a server to be as close as possible to the customer or end user
- **Maintenance backup**
- **Price**
- **As a caution for unwanted fault in the network lines of few servers.**