Networking Lab

Assignment 2

Name: Aditya Vardhan Gara Roll number: 170101003

Question 1:

Application Layer:

HTTP: HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents fetched, for instance text, layout description, images, videos, scripts and more. Here the http requests are exchanged between my system and googleuser_content server with IP 35.222.85.5 before opening my website.The HTTP protocol is a frame of width 153 bytes.

DNS: Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. DNS helps Internet users and network devices discover websites using human-readable hostnames, instead of numeric IP addresses. DNS protocols are exchanged between my system and my DNS server and is of packet widh 75 bytes.

MDNS: In computer networking, the multicast DNS (mDNS) protocol resolves hostnames to IP addresses within small networks that do not include a local name server. MDNS protocol is observed with frame width of 221 bytes.

TLSv1.3 & TLSv1.2: Transport Layer Security (**TLS**) protocol is used to secure the web (and much more!), providing encryption and ensuring the authenticity of every HTTPS website and API. It is the first major overhaul of the protocol, bringing significant security and performance improvements. TLS is an industry standard designed to protect the privacy of information communicated over the Internet. The TLS protocol allows client/server applications to detect the following security risks like Message tampering. TLSv1.2 protocol is observed with frame width of 160 bytes where as TLSv1.3 protocol is of frame width 1424 bytes.

Transport Layer:

TCP: Transmission Control Protocol is a connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network.TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. It allows one computer to talk to another computer via the Internet through compiling packets of data and sending them to the right location. TCP is a transport layer protocol. In my network sniffing TCP protocol observed with packet width of 1424 bytes with TCP payload(data) of 1358 bytes.

UDP: User Datagram Protocol is an alternative communications protocol to TCP used primarily for establishing low-latency and loss-tolerating connections between applications on the internet. Numerous key Internet applications use UDP, including: the DNS, where queries must be fast and only consist of a single request followed by a single reply packet, the Simple Network Management Protocol (SNMP), the Routing Information Protocol (RIP) and the Dynamic Host Configuration Protocol (DHCP). TCP and UDP are transport layer protocols and as such exist at layer 4 of the OSI model above the Network Layer and below the Session Layer. It was observed that UDP protocol is of frame width 1053 bytes.

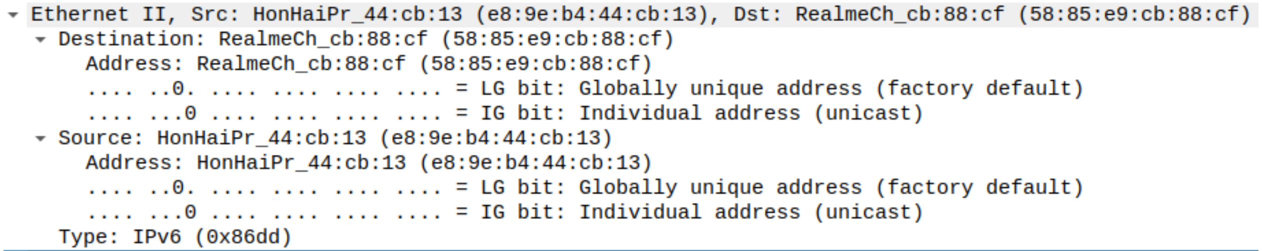
Networking Layer:

Ipv4: IPv4 is one of the core protocols of standards-based inter-networking methods in the Internet. It is a connectionless protocol for use on packet-switched networks. The header consists of 14 fields, of which **13 are required.** They are – **Version** is always equal to 4, **Internet Header Length** (IHL) has 4 bits which is the number of 32-bit words in header, Differentiated Services Code Point (DSCP) used in QoS, Explicit Congestion Notification (ECN) allows end-to-end notification of network congestion without dropping packets, **Total Length** is 16-bit field which defines the entire packet size in bytes, **identification** field is primarily used for uniquely identifying the group of fragments of a single IP datagram, **flags** bit is used to control or identify fragments (0th bit: Reserved and is always 0; 1st bit: Don't Fragment(DF); 2nd bit: More Fragments (MF)), **Fragment Offset** specifies the offset of a particular fragment, **Time To Live** (TTL) helps prevent datagrams from persisting on network forever, **Protocol** defines the protocol used in the data portion of the IP datagram, **Header Checksum** is used for error-checking of the header, **Source address & Destination** address is the IPv4 address of the sender and receiver of the packet respectively.

ARP : The address resolution protocol (arp) is a protocol used by the Internet Protocol (IP)to map IP network addresses to the hardware addresses used by a data link protocol.The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.

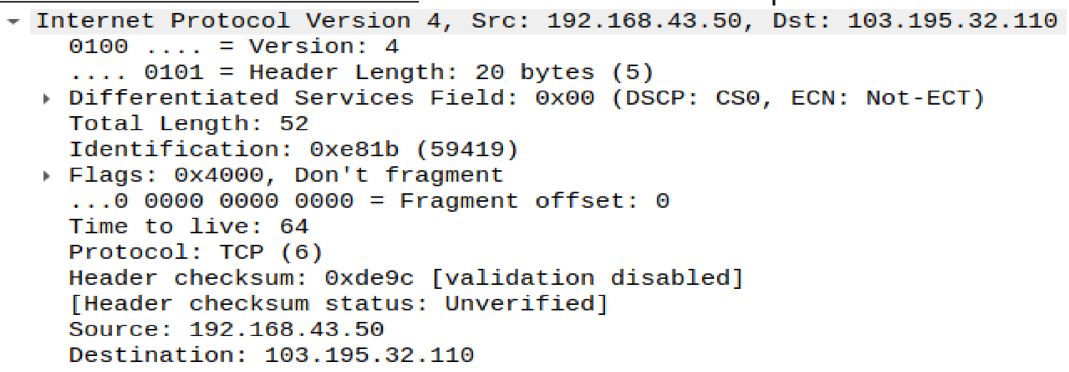
Question 2:

Ethernet II: The Ethernet fields of the captured frame are shown. It shows the *destination and source MAC*(Media Access control) addresses of the devices communicating with each other. Here Source address is my PC's address.The *LG bit* (or UL bit) and the IG bit second least and least significant bit in the most significant byte of each MAC address.The IG bit distinguishes whether the MAC address is an individual or group address.An IG bit of 0 indicates unicast MAC address, whereas 1 indicates **multicast or broadcast address. The LG on the other hand distinguishes** vendor **assigned(0) and administratively assigned** MAC addresses(1). Hence we see 0 in **both cases implying unicast and** vendor assigned. Both are Globally unique addresses not local addresses. Type indicates the network protocol used here Ipv4.



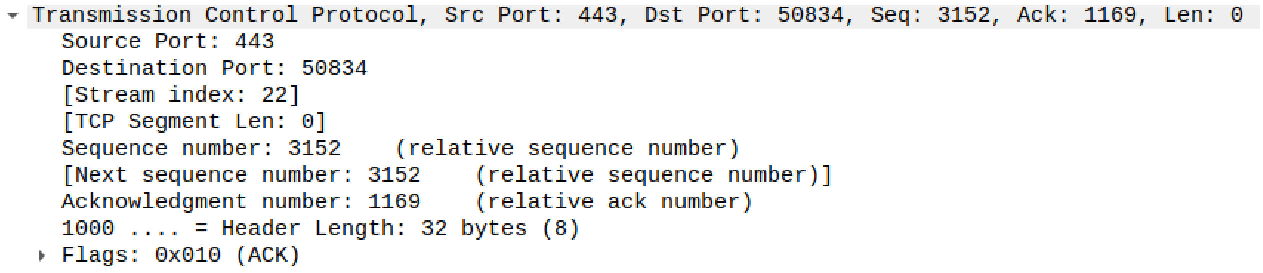
```
▾ Ethernet II, Src: HonHaiPr_44:cb:13 (e8:9e:b4:44:cb:13), Dst: RealmeCh_cb:88:cf (58:85:e9:cb:88:cf)
  ▾ Destination: RealmeCh_cb:88:cf (58:85:e9:cb:88:cf)
      Address: RealmeCh_cb:88:cf (58:85:e9:cb:88:cf)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: HonHaiPr_44:cb:13 (e8:9e:b4:44:cb:13)
      Address: HonHaiPr_44:cb:13 (e8:9e:b4:44:cb:13)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
```

Internet Protocol version 4: The IPV4 fields of the captured frames are shown. It shows the source and destination IP addresses.Version is 4 as we are using IPv4. Header Length is length of the internet header in 32 bit words. Hence here we have 5 32-bit words i.e 20 bytes. Total length of the datagram is 52 bytes.The flag set is don't fragment which instructs all the nodes through which the packet passes to not fragment the packet(don't fragment bit set as 1) Fragment offset 0 as packet not fragmented. Time to Live is 64 seconds. Protocol of the data unit in it is TCP(6 is TCP protocol number). The packet is sent from from my PC (192.168.43.50) to the Dailymotion server (103.195.32.110). Header checksum shows that checksum validation is disabled.



```
▾ Internet Protocol Version 4, Src: 192.168.43.50, Dst: 103.195.32.110
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xe81b (59419)
  ▸ Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xde9c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.43.50
    Destination: 103.195.32.110
```

__Transmission Control Protocol :__ The TCP fields of the captured frame are shown. It shows the source and destination ports TCP Stream index(to uniquely identify a TCP stream), Segment length(TCP Payload length.here 272 bytes). Sequence and Acknowledgment number are relative, i.e, relative to the first seen segment for the conversation. Header Length as 32 bytes. Flags are set as 018 implying PSH and ACK only.Scaling factor to increase TCP receive window exponentially. Checksum value is not verified. nitial Round Trip Time (iRTT) value is calculated when the first two packets of a TCP handshake are seen. TCP payload is the data to be transmitted over network. There is no urgent data in packet as Urgent pointer is 0.



```
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 50834, Seq: 3152, Ack: 1169, Len: 0
    Source Port: 443
    Destination Port: 50834
    [Stream index: 22]
    [TCP Segment Len: 0]
    Sequence number: 3152    (relative sequence number)
    [Next sequence number: 3152    (relative sequence number)]
    Acknowledgment number: 1169    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
```

__user datagram Protocol :__ The UDP fields of the captured frame are shown in the figure. The source and destination ports are displayed. Length of datagram is 42 bytes. The checksum is also displayed which is not verified.

__Domain Name System :__ The identification field is 0x77dd7, which is used to identify the query. The flags field has also been updated. No. of questions is 1. There are no answer resource records(RR), no authority RRs, no Additional Rrs.

__Hypertext Transfer Protocol :__ I have not observed any HTTP packets but observed SSDP packets using HTTP format for transferring messages.

<u>Transport Layer Security :</u> The Transport layer security fields of the captured frame are shown. TLSv1.2 is the protocol used. **Version** used is TLS 1.0. The **content type** 22 is handshake messaging protocol which we are using here. **Client Hello Protocol** is used as the handshaking protocol. TLSv1.2 is observed with packet width of 160 bytes.

Question 3:

Dailymotion is a videosharing platform in web application that can allow to play and upload videos across multiple mobile and desktop based devices. Managing load traffic and keeping the data secured become two most important things to be taken care of, concerning the services. Protocols used by Dailymotion include TCP, TSL(SSL).

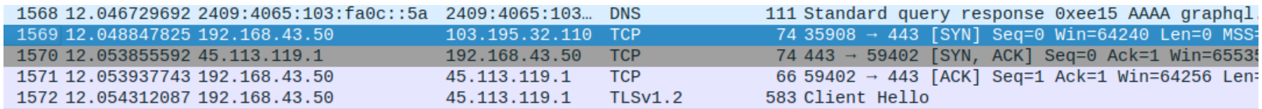
SECURITY -- (TLS/SSL) : Video content encrypted at rest can be done through Advanced Encryption Standard (AES). AES comes in three different key sizes: 128, 192 and 256 bits. Basically, AES transforms the key and some data (plaintext) into something random, known as ciphertext. To draw meaning out of the ciphertext, AES and the same key used to transform it are required to convert it back into plaintext. Dailymotion uses security protocols like SSL and TLS for encryption and security.

RELIABLE TRANSFER -- (TCP) TCP is a transport layer protocol used by applications that require guaranteed delivery. It is a sliding window protocol that provides handling for both timeouts and retransmissions.TCP establishes a full duplex virtual connection between two endpoints(which makes the transfer reliable). It is interoperable, i.e., it allows cross-platform communications among heterogeneous networks.It is a scalable, client-server architecture. This allows networks to be added without disrupting the current services. It assigns an IP address to each computer on the network, thus making each device to be identifiable over the network. It assigns each site a domain name. It provides name and address resolution services. I didnt obsered any UDP protocols in the transport layer while running the Dailymotion application That way it only needs to download files from your local network, which is much faster.

Question 4:

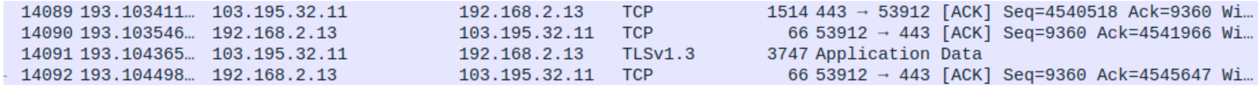
Dailymotion is a web based video sharing platform. Dailymotion lets you to upload and download videos in the website. Testing series of protocols occured in opening, playing and uploading videos in Dailymotion.

Connecting Dailymotion: We can see series of protocols when we started connecting to the Dailymotion website. The request is sent to the IP adress we got from th DNS and connection is established.



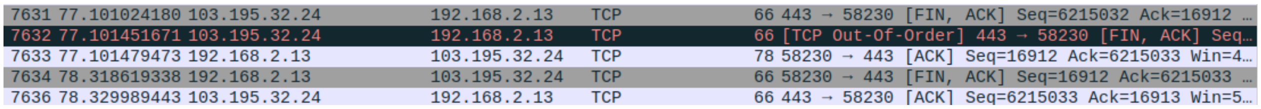
```
1568 12.046729692 2409:4065:103:fa0c::5a  2409:4065:103…  DNS       111 Standard query response 0xee15 AAAA graphql.
1569 12.048847825 192.168.43.50           103.195.32.110  TCP        74 35908 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
1570 12.053855592 45.113.119.1            192.168.43.50   TCP        74 443 → 59402 [SYN, ACK] Seq=0 Ack=1 Win=65535
1571 12.053937743 192.168.43.50           45.113.119.1    TCP        66 59402 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=
1572 12.054312087 192.168.43.50           45.113.119.1    TLSv1.2   583 Client Hello
```

Playing and pausing video: *We can see both series of protocols while playing* and pausing the streaming video.After certain time of pause connection closing acknowledgement is sent which iploes again connection acknowledgement is needed for resuming the video.



```
14089 193.103411…  103.195.32.11          192.168.2.13    TCP        1514 443 → 53912 [ACK] Seq=4540518 Ack=9360 Wi…
14090 193.103546…  192.168.2.13           103.195.32.11   TCP          66 53912 → 443 [ACK] Seq=9360 Ack=4541966 Wi…
14091 193.104365…  103.195.32.11          192.168.2.13    TLSv1.3    3747 Application Data
14092 193.104498…  192.168.2.13           103.195.32.11   TCP          66 53912 → 443 [ACK] Seq=9360 Ack=4545647 Wi…
```

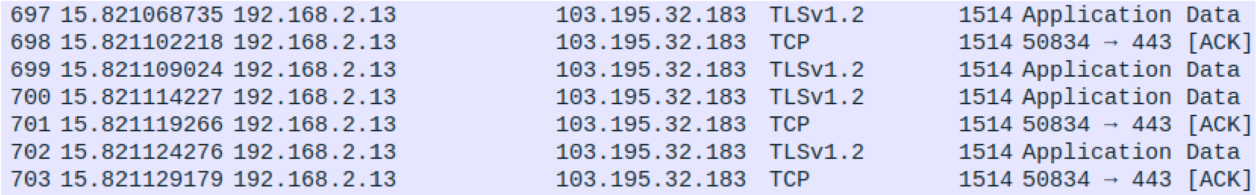
while playing



```
7631 77.101024180 103.195.32.24        192.168.2.13    TCP        66 443 → 58230 [FIN, ACK] Seq=6215032 Ack=16912 …
7632 77.101451671 103.195.32.24        192.168.2.13    TCP        66 [TCP Out-Of-Order] 443 → 58230 [FIN, ACK] Seq…
7633 77.101479473 192.168.2.13         103.195.32.24   TCP        78 58230 → 443 [ACK] Seq=16912 Ack=6215033 Win=4…
7634 78.318619338 192.168.2.13         103.195.32.24   TCP        66 58230 → 443 [FIN, ACK] Seq=16912 Ack=6215033 …
7636 78.329989443 103.195.32.24        192.168.2.13    TCP        66 443 → 58230 [ACK] Seq=6215033 Ack=16913 Win=5…
```

during pause

Uploading Video: We can see the encryption technology used in uploading the video into dailymotion website. TLSv1.2 is used as security protocol for encryption.

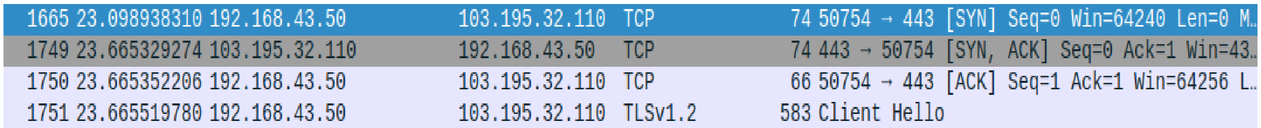


```
697 15.821068735 192.168.2.13          103.195.32.183  TLSv1.2      1514 Application Data
698 15.821102218 192.168.2.13          103.195.32.183  TCP          1514 50834 → 443 [ACK]
699 15.821109024 192.168.2.13          103.195.32.183  TLSv1.2      1514 Application Data
700 15.821114227 192.168.2.13          103.195.32.183  TLSv1.2      1514 Application Data
701 15.821119266 192.168.2.13          103.195.32.183  TCP          1514 50834 → 443 [ACK]
702 15.821124276 192.168.2.13          103.195.32.183  TLSv1.2      1514 Application Data
703 15.821129179 192.168.2.13          103.195.32.183  TCP          1514 50834 → 443 [ACK]
```

Handshaking Sequence:

TCP Connection Establishment Handshake: A three-way handshake/TCP handshake is a method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins. In the first step(SYN), client wants to establish a connectionwith server, so it sends a segment with SYN(Synchronise Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with. In second step(SYN+ACK) server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with. In the third and final step(ACK) client acknowledges the response of server and they both establish a reliable connection with which they will start actual data transfer. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex TCP communication is established.

TCP Connection Termination Handshake: A TCP connection is normally terminating using a special procedure where each side independently closes its end of the link. It normally begins with one of the application processes signalling to its TCP layer that the session is no longer needed. That device sends a FIN(finish) message, serves as a connection termination request to the other device, while also possibly carrying data like a regular segment to tell the other device that it wants to end the connection, which is acknowledged by the device receiving the FIN to indicate that it was received.When the responding device is ready, it too sends a FIN that is acknowledged; after waiting a period of time for the ACK to be received, the session is closed. The connection as a whole is not considered terminated until both sides have finished the shut down procedure by sending a FIN and receiving an ACK.Thus, termination isn't a three-way handshake like establishment: it is a pair of two-way handshakes.



```
1665 23.098938310 192.168.43.50      103.195.32.110  TCP          74 50754 → 443 [SYN] Seq=0 Win=64240 Len=0 M…
1749 23.665329274 103.195.32.110     192.168.43.50   TCP          74 443 → 50754 [SYN, ACK] Seq=0 Ack=1 Win=43…
1750 23.665352206 192.168.43.50      103.195.32.110  TCP          66 50754 → 443 [ACK] Seq=1 Ack=1 Win=64256 L…
1751 23.665519780 192.168.43.50      103.195.32.110  TLSv1.2     583 Client Hello
```

Question 6: *Dailymotion* is a video sharing technolgy which lets you to download or upload a video. On using the website for several times it was observed that multiple IPs are used by the website. This might happen due to several reasons while managing the load traffic. The basic need/ want of any website is that it should satisfy all its request and it should never go offline. Generally websites are build more than one server, that serves a copy of the same web page. Each server has a different IP address. If one of these servers is down, then the client software just picks the next address in the list and tries again. I observed Dailymotion website used various IPs 103.195.32.30, 103.195.32.26, 103.195.32.36 while using. It is also observed that some IPs are specific for certain tasks such as 103.195.32.36 is observed in all TLSv1.3 protocols.

Question 5:

	Throughput bytes/sec	RTT sec	Avg. Packet size bytes	Packet loss %	UDP packets	TCP packets	Avg. respons/req
Sample 1	2.2k	0.012	569	0	0	800	0.27
Sample 2	6.5k	0.0085	474	0	0	650	0.32
Sample 3	7.2 k	0.0013	481	0	16	1041	0.48
Sample 4	8.3 k	0.0142	504	0	0	254	0.18

RTT is found by taking average of values obtained after using "**tcp.analysis.ack_rtt**" as a filter. Throughput, Packet Sizes and no. of packets were found from "Statistics-> Capture Filter Properties" menu. No. of Responses per request = Packets from B to A / Packets from A to B calculated from "Statistics->conversations" after applying the filter, here A-> y browser and B-> Dailymotion site.

Drive link for Traces:

https://drive.google.com/drive/folders/1RwksIrl_mbcFlybJF3wFlScSwaCUvYyJ?usp=sharing