CS349:NETWORKS LAB

ASSIGNMENT 2

Partha Pratim Malakar
170101043

Application:Dropbox

Traces:
https://drive.google.com/drive/folders/1iZ6OoSqUZUe8P0BEDe2kJ_neoFGMgXe4?usp=sharing

Question1.

Protocol by application at different layer:

A)TCP protocol(Transport layer protocol):

Source Port:Sender's connection endpoint . size 16bit.
Destination Port:Receiver's connection endpoint.size 16bit.
Sequence Number:TCP assigns a number to each byte of a data stream.Sequence Number is the byte number of the first byte of the segment in the TCP stream .It is a 32 bit field.If SYN flag is set, then sequence number is 0.
Acknowledgement Number: It's a 32 bit field.If the ACK flag is set then the value of this field is the next sequence number that the sender is expecting.
Header Length: It's a 4 bit field.It tells the number of 32 bit words in the TCP header.
Flags: It's a 9 bit field.It says about the TCP flag bits-(NS,CWR,ECE,URG,ACK,PSH,RST,SYN,FIN).
Window Size Value: This 16 bit field gives the size of the receiver window.It gives the number of byte receiver is willing to accept.
Checksum: This is a 16bit bit field used in error checking of header,the Payload and a Pseudo-Header.
Urgent Pointer: This 16 bit field pointer points to the last byte of the urgent data if the URG flag is set.Else it is 0.
Options: This field has no fixed length though length should be divisible by 32.It indicates TCP options like MSS,Window Scaling,Nop ,Selective Acknowledgements.
TCP Payload: This field says size of the data portion of the packet.

***B)*IP Protocol(Network Layer protocol):**

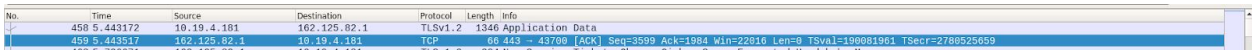
Version: This 4 bit field says about the Ip version.
Header Length: Ip header length .Its max size 24 byte and min size 20 byte.
DSCP: Differentiated Services Code Point.6 bit field. this is Type of Service.
ECN: Explicit Congestion Notification. It carries information about the congestion seen in the route.It is a 2 bit field.

Total Length: It is a 2 byte field that specifies the length of the IP packet that includes the IP header and the user data.Therefore it is the total length of the datagram.
Identification: It is a 2 byte field .If IP packet is fragmented during the transmission, all the fragments contain the same identification number to identify original IP packet they belong to.
Flags: It is a 3 bit field.It says about Ip flags-DF(do not fragment) ,MF (more to follow).
Fragment Offset: The fragment offset field is measured in units of eight-byte blocks. It is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero.
Time To Live: It is the upper limit of routers.
Protocol: This field Tells the next level protocol name.It is 6 for TCP and 17 for UDP.
Header CheckSum:16 bit field used for error checking of header.
Source: This 32 bit field shows the IP of the source host.
Destination: This 32 bit field shows the IP of the destination host**.**

***C*)TLSv1.2(Transport Layer):**
Version:shows The TLS version.
Length : The record length is a 16-byte value.

D)Ethernet II(Link Layer Protocol):
Destination: Destination host MAC(Media Access Control) Address.It's a 6 octet field.
Source: Source Host MAC(Media Access Control) Address.It's a 6 octet field.
Type: Higher Layer protocol name.

Question2.



A)TCP protocol(Transport layer protocol):
A Port number specifies a specified running process in a host.A port is always associated with an Ip and a protocol.
Source Port:443
Destination Port:43700
Sequence Number:3599. It means the first byte of the TCP packet(or segment) has byte number 3599.
Acknowledgement Number:1984. It means source of this packet wants a packet from destination with sequence
Header Length:8 It means TCP header has 8 32 bit words.
Flags:0x010(ACK) It means acknowledgement flag.
Window Size Value:172 It announces the number of bytes still free in the receiver buffer.
Checksum:0x1b32
Urgent Pointer:0 It means the URG flag is not set.

B)IP Protocol(Network Layer protocol):

Version:4 The protocol is Ipv4.
Header Length:5 Ip header length is 20 byte.
Differentiated Service Codepoint:CS0
Total Length:52 Total size of IP packet including user data and Ip header is 52 byte.
Identification:0x84c5
Flags:reserved bit=not set
Dont fragment =not set Means fragmentation can be done.
More fragment =not set Means packet is not fragmented.
Fragment offset =0 Means it is the first fragment of the packet or the packet is not fragmented.
Time To Live:62 The limit of routers for the packet is 62.
Protocol:TCP it means TCP protocol will be used in transport layer.
Header CheckSum: 0xf4b8 The error-checking of the header
Source:162.125.82.1 Source IP address.
Destination:10.19.4.181 Destination IP address.

C)TLSv1.2(Transport Layer protocol):

Content Type:Application data(23) Type of data carried by TLSv1.2
Version:TLS 1.2 Version of Transport Layer Security(TLS) protocol
Length :1275 Length of data
Encrypted Application Data:00000000000000002642f885e9a730c672aa34a9a7b5a7bca

D)Ethernet II(Link Layer Protocol):

Destination :LcfcHefe_e0:75:cd (54:e1:ad:e0:75:cd) MAC address of destination.
Source:Cisco_74:60:43 (ec:44:76:74:60:43) MAC address of source.
Type:IPv4 (0x0800) IPv4 is used in the next higher layer that is Network Layer.

Question3.

Functionalities*:Uploading a large file to dropbox and downloading a large file from Dropbox.*

TCP Protocol:

TCP protocol used in Transport Layer.*Application* uses TCP for initializing the connection the client sent 'SYN' packet to initialize connection.The ACK(acknowledgement) packets uses TCP protocol.After completing data transfer(uploading/downloading) the packet with FIN flag use TCP protocol.

Reasons for using TCP:

i)It's a reliable,connection oriented transport protocol that facilitates the exchange of messages between computing devices in a network.
ii)It is the most common protocol in networks that use the Internet Protocol (IP).Together they are referred to as TCP/IP.
iii)TCP is said to be connection-oriented because before sending data through TCP,the two hosts must ‘handshake’ with each other.

iv) TCP connection is point-to-point, means data transfer takes between a single sender and a single receiver.
v)TCP provides full duplex service. If there is a TCP connection between Process A on one host and Process B on another host, data can flow from Process A to Process B at the same time from Process B to Process A.
vi)TCP also provides high error rate handling,good failure recovery,Low data overhead.

TLSv1.2:

Application uses TLSv1.2 during TLS handshake .Also the packets that contain 'application data' use TLSv1.2.

Reasons for using TLSv1.2

i)It is a Transport Layer Security protocol designed for providing privacy and data security for communication over a network.
ii)TLS protects websites from attacks.
iii)It provides
Encryption: hides the data being transferred from third parties.
Authentication: ensures that the parties exchanging information are who they claim to be.
Integrity: verifies that the data has not been forged or tampered with.

IPv4 Protocol:

All packets of the application use this protocol in network layer for communication between source host and server.

Reasons for Using IPv4:

i)It is used in network layer.
ii)IPv4 is a connectionless protocol used for packet-switched networks.
iii)It provides a logical connection between network devices by providing identification for each device.

Ethernet II:It is used in data link layer.It uses the underlying Ethernet physical layer transport mechanisms.a data unit on an Ethernet link transports an Ethernet frame as its payload.

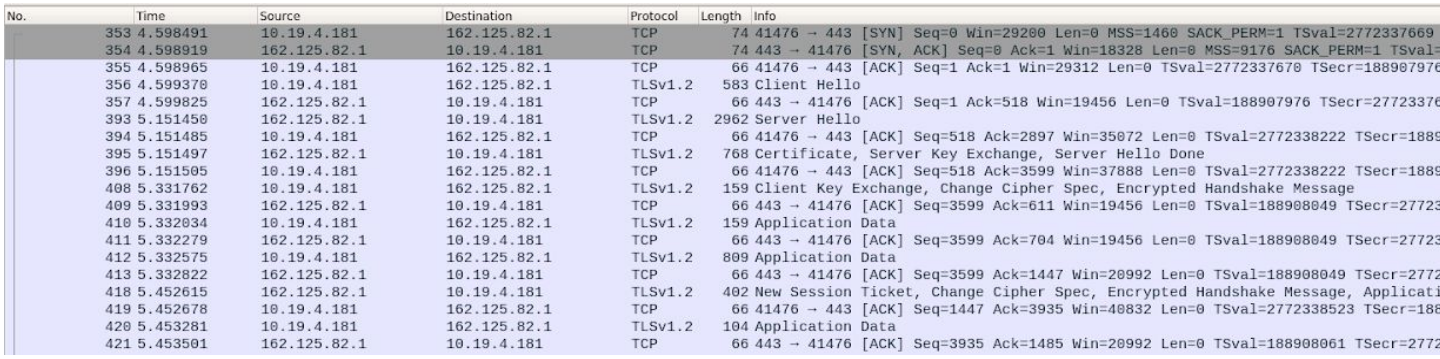
All packets of the application use this protocol in data link layer .

Question4.

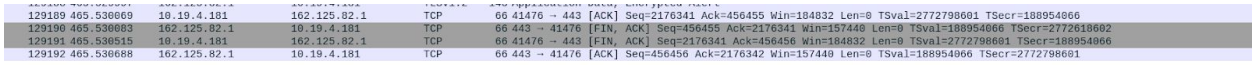
Functionalities: Uploading large files to dropbox and downloading large files from Dropbox.

i)My computer ,as a client initializes the connection with dropbox servers by sending a packet with TCP protocol and flag SYN(synchronize).The server replies to this by sending a TCP packet with flags SYN(synchronize) and ACK(acknowledgement).Then the client replies with a ACK packet using TCP protocol.
ii)Then Client sent 'Client Hello' message Using TLSv1.2 protocol.It contains “random bytes” used to generate a cryptographic key, which TLS version client supports ,the cipher suites the client understands and signature algorithms.
iii)After that server sends ACK.Then server sent 'server hello message'.It contains the cipher suite selected for encryption,session ID and random byte string.

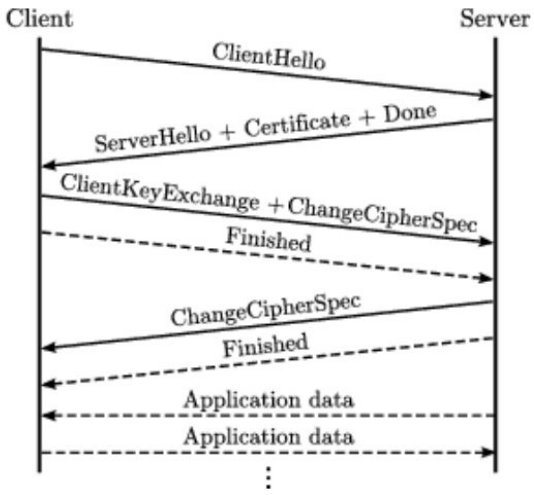
iv)This followed by client ACK.then server sends a message using TLSv1.2 protocol with 'Certificate,Server Key Exchange , Server Hello Done' .It includes info about the company who issued the certificates, the actual public key that represents the certificate, Server's public key, the signature algorithm etc.
v)The client verifies the certificate,acknowledged this packet and then sends another packet using TLSv1.2 protocol with info 'Client key Exchange,Change Cipher Spec,Encrypted handshake message' . It icontains client's public key to Server, a random byte string that enables both the client and the server to compute the secret key to be used for encrypting subsequent messages.
vi)The server sent 'new session ticket ,change cipher spec,encrypted handshake message' using TLSv1.2.
vii)After that data transmissions start with packets info 'application data'.They use TLSv1.2 protocols.The ACK messages use TCP protocol.
viii)The end of transfer can be identified by the 'FIN,ACK' packet. Although sometimes only 'FIN,ACK' packet don't appear.



No.	Time	Source	Destination	Protocol	Length	Info
353	4.598491	10.19.4.181	162.125.82.1	TCP	74	41476 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2772337669
354	4.598919	162.125.82.1	10.19.4.181	TCP	74	443 → 41476 [SYN, ACK] Seq=0 Ack=1 Win=18328 Len=0 MSS=9176 SACK_PERM=1 TSval=
355	4.598965	10.19.4.181	162.125.82.1	TCP	66	41476 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2772337670 TSecr=188907976
356	4.599370	10.19.4.181	162.125.82.1	TLSv1.2	583	Client Hello
357	4.599825	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [ACK] Seq=1 Ack=518 Win=19456 Len=0 TSval=188907976 TSecr=2772337
393	5.151450	162.125.82.1	10.19.4.181	TLSv1.2	2962	Server Hello
394	5.151485	10.19.4.181	162.125.82.1	TCP	66	41476 → 443 [ACK] Seq=518 Ack=2897 Win=35072 Len=0 TSval=2772338222 TSecr=1889
395	5.151497	162.125.82.1	10.19.4.181	TLSv1.2	768	Certificate, Server Key Exchange, Server Hello Done
396	5.151505	10.19.4.181	162.125.82.1	TCP	66	41476 → 443 [ACK] Seq=518 Ack=3599 Win=37888 Len=0 TSval=2772338222 TSecr=1889
408	5.331762	10.19.4.181	162.125.82.1	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
409	5.331993	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [ACK] Seq=3599 Ack=611 Win=19456 Len=0 TSval=188908049 TSecr=27723
410	5.332034	10.19.4.181	162.125.82.1	TLSv1.2	159	Application Data
411	5.332279	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [ACK] Seq=3599 Ack=704 Win=19456 Len=0 TSval=188908049 TSecr=27723
412	5.332575	10.19.4.181	162.125.82.1	TLSv1.2	809	Application Data
413	5.332822	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [ACK] Seq=3599 Ack=1447 Win=20992 Len=0 TSval=188908049 TSecr=2772
418	5.452615	162.125.82.1	10.19.4.181	TLSv1.2	402	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Applicati
419	5.452678	10.19.4.181	162.125.82.1	TCP	66	41476 → 443 [ACK] Seq=1447 Ack=3935 Win=40832 Len=0 TSval=2772338523 TSecr=188
420	5.453281	10.19.4.181	162.125.82.1	TLSv1.2	104	Application Data
421	5.453501	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [ACK] Seq=3935 Ack=1485 Win=20992 Len=0 TSval=188908061 TSecr=2772



129189	465.530069	10.19.4.181	162.125.82.1	TCP	66	41476 → 443 [ACK] Seq=2176341 Ack=456455 Win=184832 Len=0 TSval=2772798601 TSecr=188954066
129190	465.530083	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [FIN, ACK] Seq=456455 Ack=2176341 Win=157440 Len=0 TSval=188954066 TSecr=2772618602
129191	465.530515	10.19.4.181	162.125.82.1	TCP	66	41476 → 443 [FIN, ACK] Seq=2176341 Ack=456456 Win=184832 Len=0 TSval=2772798601 TSecr=188954066
129192	465.530688	162.125.82.1	10.19.4.181	TCP	66	443 → 41476 [ACK] Seq=456456 Ack=2176342 Win=157440 Len=0 TSval=188954066 TSecr=2772798601



There are handshaking sequences of messages in the application.It is called TLS handshake.I Explained it in steps ii) to v).

Question5:

Capture 1(2:30 pm)(uploading large file to dropbox using hostel ethernet)
Capture 2(6:10 pm) (downloading large file from dropbox using hostel ethernet)
Capture 3(8:00 am)(uploading large file to dropbox using mobile hotspot)

Perimeters	**capture1**	**capture2**	**capture3**
Throughput(Bytes/s)	309k	1051k	331k
RTT(s)	.003608	0.001174	0.0029
Packet size(Byte)	1115	1234	960
Loss packet	0	4	22
UDP packets	4310	2631	23
TCP packets	118688	216637	50396
Number of responses received with respect to one request sent	0.2280	1.2377	0.47841

Question6:

Capture 1(2:30 pm)*(uploading large file to dropbox using hostel ethernet)*:src=10.19.4.181(My host ip)
Capture 2(6:10 pm) *(downloading large file from dropbox using hostel ethernet)*:src =162.125.82.1, 162.125.82.6
Capture 3(8:00 am)*(uploading large file to dropbox using mobile hotspot)*:src =192.168.43.74

i)A host Ip address changes with change in network.That's why it is different while using ethernet and mobile hotspot.
ii)Even with the same network, if a host ip is dynamic(or not static) it may change over time.Multiple Ip's in a host helps in preventing traffic and load balancing.

iii)Websites like dropbox use round robin DNS which helps in load balancing .Due to round robin DNS ips of websites don't remain constant and changes in a round robin fashion.Also for security reasons,websites use multiple ips.