CS349 : Assignment 2 report , NAME - PIYUSH JAIN, Roll No. - 150101046

Application : Dropbox

Three capture files included which contains three readings taken at three different times. capture1 - 07:00 , capture2 : 18:00, capture3 - 13:00

1. Protocols used by the application at different layers (as seen in traces) :
   - **IP (Network Layer)** : IP pakcet consists of :
     - Version - The Version field indicates the format of the internet header.
     - Header Length - Length of the internet header in 32 bit words, and thus points to the beginning of the data.
     - Type of Service - The Type of Service provides an indication of the abstract parameters of the quality of service desired.
     - Total length - Length of the datagram, measured in octets, including internet header and data. (16 bits)
     - Identification - An identifying value assigned by the sender to aid in assembling the fragments of a datagram(16 bits)
     - Flags - Various Control Flags (3 bits).
     - Fragment offset - This field indicates where in the datagram this fragment belongs. (13 bits).
     - Time to live - Maximum time the datagram is allowed to remain in the internet system. (8 bits).
     - Protocol - Next level protocol used in the data portion of the internet datagram.
     - Header Checksum - A checksum on the header only.
     - Source Address: 32 bits
     - Destination Address: 32 bits

   - **TCP (Transport layer)** : The TCP packet format consists of these fields.
     - Source Port and Destination Port fields (16 bits each) identify the end points of the connection.
     - Sequence Number field (32 bits) specifies the number assigned to the first byte of data in the current message.
     - Acknowledgement Number field (32 bits) contains the value of the next sequence number that the sender of the segment is expecting to receive, if the ACK control bit is set.
     - Data Offset (Header Length) field (variable length) tells how many 32-bit words are contained in the TCP header.
     - Reserved field (6 bits) must be zero. This is for future use.
     - Flags field (6 bits) - URG, ACK, PSH, RST, SYN, FIN
     - Window field (16 bits) specifies the size of the sender's receive window
     - Checksum field (16 bits) indicates whether the header was damaged in transit.
     - Urgent pointer field (16 bits) points to the first urgent data byte in the packet.
     - Options field (variable length) specifies various TCP options.
     - Data field (variable length) contains upper-layer information.
   - **DB-LSP-DISC (Transport Layer)** : Dropbox LAN Sync Discovery Protocol. It sends a UDP broadcast packet in the local network every 30 seconds*. The source and destination port of the packet are set to 17500. This UDP packet has some payload attached to it for identify itself to the receiver. It contains a Javascript object notation. It contains : Text: { “host_int”: 14xxxx52, “version”: [1,8], “displayname”: 14xxxx52,“port”: 17500,“namespaces”: [263xxxx, 152xxxxx, 152*****] }

- **TLSv1.2 (Application Layer)** : Transport Layer Security is a successor of SSL. The basic unit of data is a record. Each record consists of a five-byte record header, followed by data.
    - Record Format : Type (uint8), Version(uint16), Length(uint16)
    - Record Type : Handshake (22, 0x16), Change Cipher Spec (20, 0x14), Alert(21, 0x15), Application Data (23, 0x17)
    - Record Version : The record version is a 16-byte value and is formatted in network order.
    - Record Length : The record length is a 16-byte value and is formatted in network order.

2. Following tables explain the values of various fields for each packet considering an instance of packet of that protocol.

TCP : File - capture1 , Packet serial number - 6

Field	Value	Explanation
Source Port	47306	Port of the source side end point of the packet transfer.
Dst Port	443	Port of the source side end point of the packet transfer.
Sequence Number	0	This is showing the relative sequence number of the packet.
Acknowledge Number	0	This represents the acknowledgement number for the packet received.
Header length	40 Bytes	Length of the attached to the packet.
Flags	0x002 (SYN)	Synchronizes sequence numbers to initiate a connection.
Window Size	29200	The size of the receive window that the sender of this segment is currently willing to receive.
Checksum	0x0053	16-bit for error checking.
Urgent pointer	0	If the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte.
Options	Maximum Segment Size, SAC permitted, Timestamps, No-Operation(NOP), Window Scale	Specifies various TCP options. Options have up to three fields: Option-Kind (1byte),Option-Length (1 byte),Option-Data(variable).

DB-LSP-DISC : File - capture1 , Packet serial number - 185

Field	Value	Explanation
host_int	1209447558677408465567214488653753968 60	The UDP broadcast packet sent by Dropbox in the local network every 30 seconds has some payload attached with it containing these fields. It is destined to the other client on port 17500.
version	[2,0]	
displayname	(NULL)	
port	17500	
namespaces	[2432228944]	

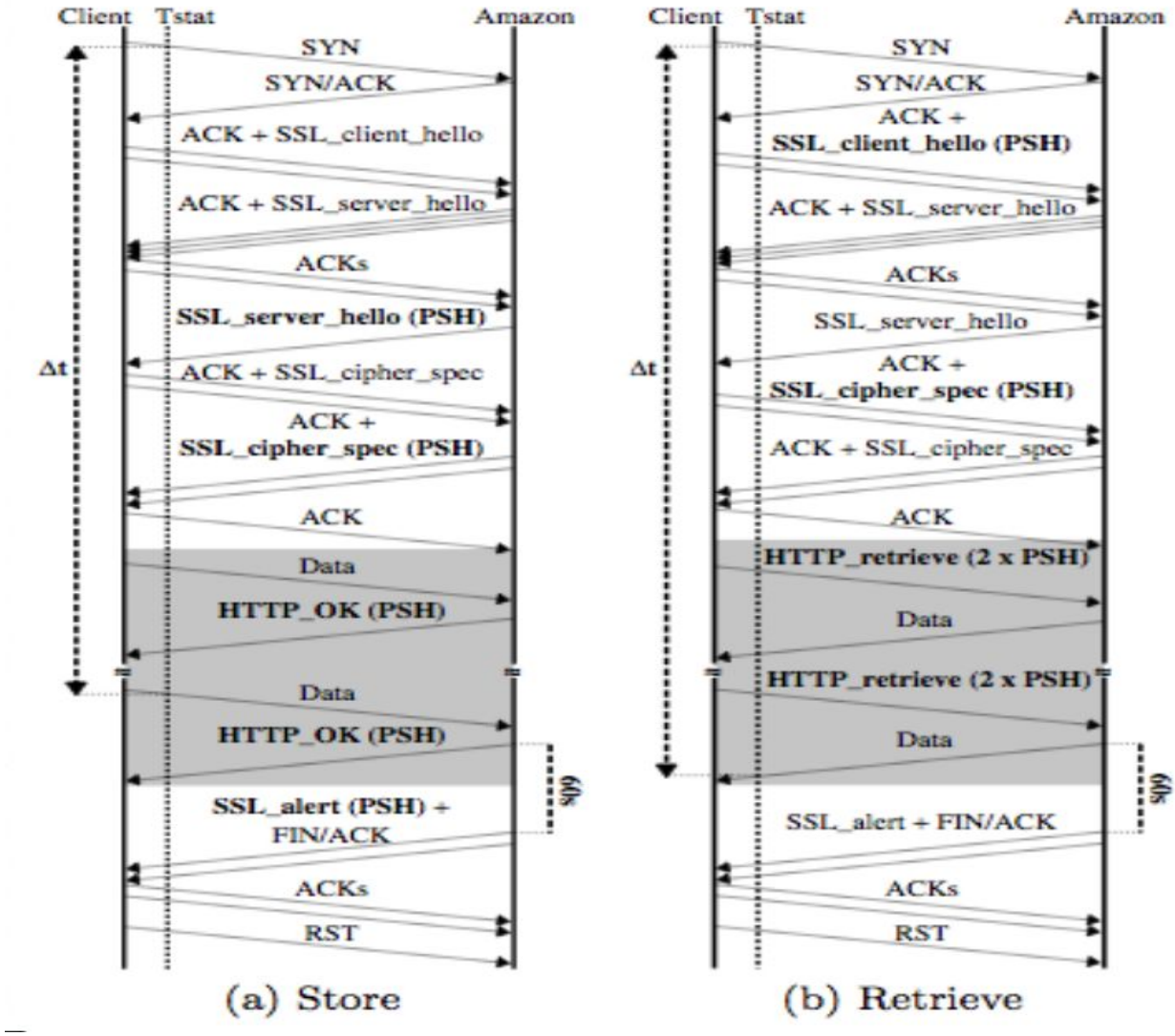
TLSv1.2 : File - capture1 , Packet serial number - 185
Record Layer : Application Data Protocol : http2

Field	Value	Explanation
Content type	Application Data (23)	Type of content being carried by the protocol.
Version	TLS 1.2 (0x0303)	Version of the TLS protocol.
Length	33	Length of the data.
Encrypted Application data	0000000000000002820 4c2d3d4bdb6797f24efdc b250bd3c...	Actual application data.

3. Dropbox uses mainly servers hosted on Amazon datacenters for various types of operation. In dropbox, there are three major operations. Storage of data on cloud, Retrieval of data on client's machine and continuous syncing of data between server and client.

- **Storage/Retrieval** :
    - TCP packet with SYN (0x002) flag is sent to the server. This synchronizes the sequence number to initiate a connection. The server responds back with SYN/ACK.

- Then, TLSv1.2 packet with record layer as Handshake Protocol : Client Hello is sent to the server which is responded back by Server Hello. The corresponding acknowledgements are also exchanged.
- This is followed by TLSv1.2 Change Cipher Spec Message to change the encryption during handshaking to switch to symmetric key encryption between client and server. Server responds correspondingly and finally connection is established to transfer data.
- Data is transferred from client to server (for storage) and server to client (for retrieval).
- After completion of transfer, a TCP packet is sent with FIN (0x011) flag indicating it had finished the transfer. This is responded with a TCP packet containing ACK and the storage/retrieval process is finished.

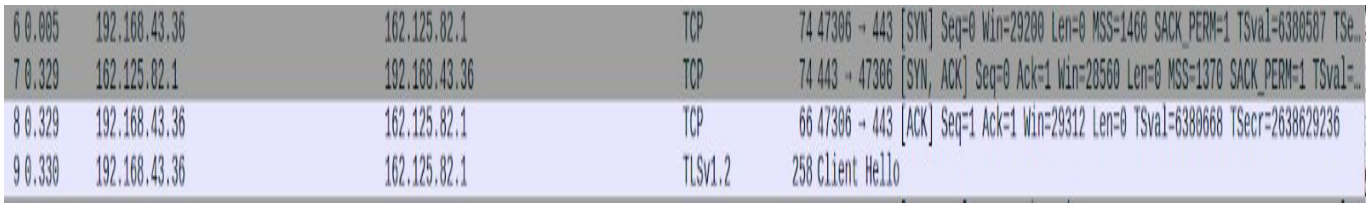


- **Synchronization** - This is done using Dropbox LAN SYNC Discovery Protocol. The DB-LSP DISC provides great sync of files across multiple

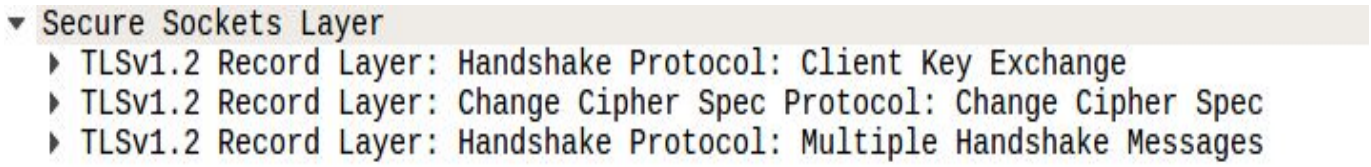
devices, and into the cloud. When dropbox finds that you are on a LAN, it syncs directly between PCs. It sends a UDP broadcast packet in the local network.The source and destination port of the packet are set to 17500. This UDP packet has some payload attached to it for identify itself to the receiver. It seems like a dictionary as defined above.

There are handshaking sequences while establishing a connection.
There is basically a three-way handshake mechanism to establish a TCP connection. There are three messages transmitted (SYN , SYN/ACK, ACK) by TCP to start a TCP session between the dropbox server and client. A sequence of TCP handshaking mechanism is as follows :

- Client sends a TCP SYN packet, which is basically a synchronize packet, to the server. Server receives client's SYN.
- Server sends a SYN/ACK message.(Synchronize/Acknowledgement). Client receives SYN/ACK.
- Client sends ACK which is received by server. TCP socket connection is established between the client and server.



Other than this, TLS also does handshake sequence exchanges before exchanging application data. It sends packets with record layer as Handshake protocol, Change Cipher Spec Protocol and Multiple Handshake Messages.



4.

- **TCP** - Transmission Control Protocol is responsible for synchronization and initiating connection. It sends the SYN (0x002) to synchronize the sequence number and finally sends FIN (0x011) flag indicating finishing of transfer. It is basically responsible for establishing and maintaining a network conversation via which dropbox can exchange data between client and server.
- **TLSv1.2** - It provides secure connection between the server and client. It uses Handshake protocols and Change CIpher Spec Messages to establish

a secure connection. Dropbox uses TLS for transferring actual application data as well with record layer as Application data Protocol.

- **DB-LSP-DISC** - This is the protocol of Dropbox which is mainly responsible for syncing folders across multiple devices connection over a local networks as well as server. For example, if the PC is connected over a LAN, and there are shared dropbox folders across machines, this protocol synchronizes all shared folders across machines and also synchronizes the content with the server.

5.

Parameter	**Value @ 07:00 (capture1)**	**Value @18:00 (capture2)**	**Value @13:00 (capture3)**
Throughput	40k bits/s	9026 bits/s	19k bits/s
RTT	0.325s	0.351s	0.273s
Packet Size	605.5 Bytes (Avg.)	255.5 Bytes (Avg.)	231.5 Bytes (Avg.)
No. of packets lost	6	0	5
Number of TCP and UDP Packets	TCP - 493 UDP - 2	TCP - 374 UDP - 4	TCP - 533 UDP - 4
Number of responses received with respect to one request sent	263/232 = 1.133	163/215 = 0.758	288/249 = 1.156

6. The whole content is being sent from multiple IP addresses.
capture1 : 162.125.82.1, 162.125.34.129
capture2 : 162.125.34.129, 162.125.32.141
capture3 : 162.125.34.129, 162.125.81.1

Hosts use multiple source/locations to facilitate the services. There can be several reasons for existence of multiple IP addresses :

- To compensate for a host that's down at that moment by adding its IP address to another one

- If you have multiple IP networks on the same physical/logical network/vlan it will prevent traffic from being exchanged via the gateway, speeding things up and reducing the load
- In order to use different public IP addresses to avoid firewalls or to avoid being blacklisted in SPAM filters
- In order not to expose commonality between services. E.g. if you host site1.example.com and site2.example.org and you map them on different IPs instead of using CNAMEs there won't be an obvious link between them
- In order to reduce the load on one network adapter (interface) or load balance different request types.