NAME: Deepesh V. Patil **MIS:** 112215055 Assignment - 2 (Group – 2)

Application: 3. OneDrive (Desktop App)

Q1. List of all the protocols used by the application (layer wise).

LAYER	PROTOCOL	USES
Transport Layer	TCP	For the transmission of data between the client and the server using 3-way handshake.
Transport Layer	TLSv1.3	Used to provide encryption to the data that is being transmitted over HTTPS.
Transport Layer	TLSv1.2	Also used for data encryption but is less effective than TLSv1.3

The TCP protocol allows an application to communicate with other computing devices/hosts. The TCP packet consists of the following layers:

- Source Port (Holds the port no. of the port number of the transmitting application).
- Dest. Port (Holds the port no. Of the receiver).
- Sequence Number (This ensures that the data is received in proper order by the receiver).
- Acknowledgement Number (contains the upcoming sequence number)
- Data Offset (stores the starting point of the data payload and stores the size of the TCP header).
- Flags (used to regulate the communication. Eg. SYN, ACK, FIN, RST PSH, etc.).
- Checksum (Reveals if the header was damaged while communicating)
- Urgent Pointer (points to the first byte of the urgent data of the packet).
- Options (points to different options of the TCP protocol like Max Segment Size (MSS), Timestamp, etc.)
- Payload (The actual data to be sent by the packet).

The TLSv1.3 packet has two major parts i.e. the header and the payload. The header contains the following:

- Content Type (Indicates the type of data (Alert, Normal Packet, Handshake, etc.)
- Protocol Version (stores the version of TLS Protocol)
- Record Length (stores the entire length of the packet)

The payload part may contain any of the following depending on the content.

- Handshake (contains the messages required to perform a successful handshake between the client and the server)
- Alert (contains messages such as warnings and errors)
- Application Data (contains encrypted data such as HTTP request and response, SMTP messages, etc.)

Here are the values of 5 different packets:

PACKET NO.	DEST. IP ADDR.	PACKET LENGTH	ETH. DEST. ADDRESS	PROTOCOL TYPE	PORT NO.
953	40.79.189.59	734	7c:5a:1c:c8:ec:56	TLSv1.3	443
1003	40.79.189.59	800	7c:5a:1c:c8:ec:56	TLSv1.3	443
1042	40.79.189.59	54	7c:5a:1c:c8:ec:56	TCP	443
1053	40.79.189.59	1494	7c:5a:1c:c8:ec:56	TCP	443
169458	40.79.189.59	89	7c:5a:1c:c8:ec:56	TLSv1.3	443

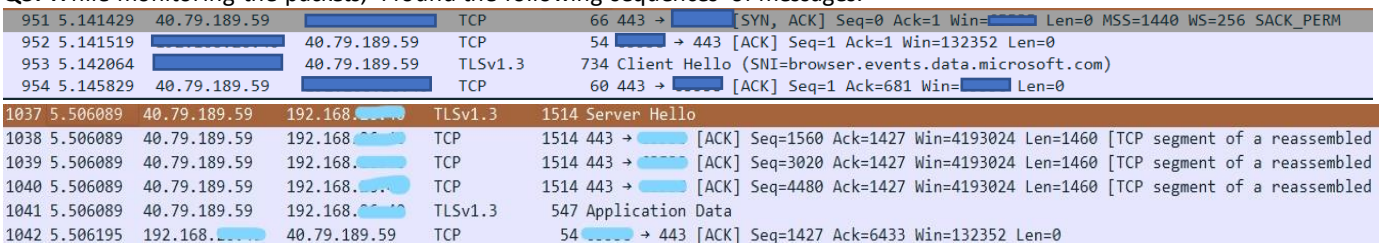
In the above table, we can see that the destination port and the destination ethernet address is the same as well as its IP address.

Q2. The application has various functionalities such as file & folder storage, syncing, sharing, backup and recovery options, security, etc.

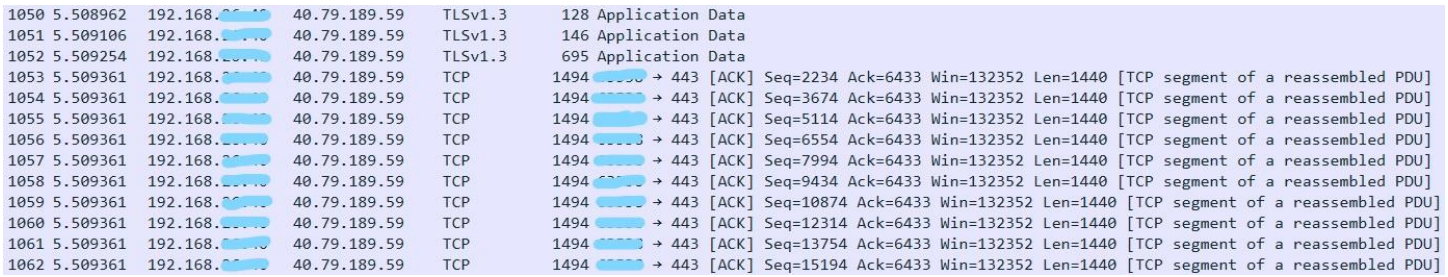
PROTOCOL	FUNCTIONS
HTTPS	File Sharing, File Syncing, File Security, data integrity
TCP/IP	the 3-way handshake, sharing data between client and host
TLSv1.3	Encryption of data

The HTTPS protocol is used because of its capability of data encryption and integrity, and it also holds various digital certificates received from trusted CAs. HTTPS is also supported by most of the web browsers, which allows the OneDrive to run on most of the devices.
Since OneDrive is a cloud storage application, TCP/IP protocols are most suited for communication over internet. The TCP/IP also provides reliable data delivery, and the sequence and the acknowledgement method ensures that the correct order is maintained when the data is received. Just like HTTPS, the TCP/IP is also widely supported various devices.
Like HTTPS, the TLS protocol is also trusted and is certifies of authenticated CAs. It provides features like encryption, authentication, data integrity and preventions from eavesdropping.

Q3. While monitoring the packets, I found the following sequences of messages.

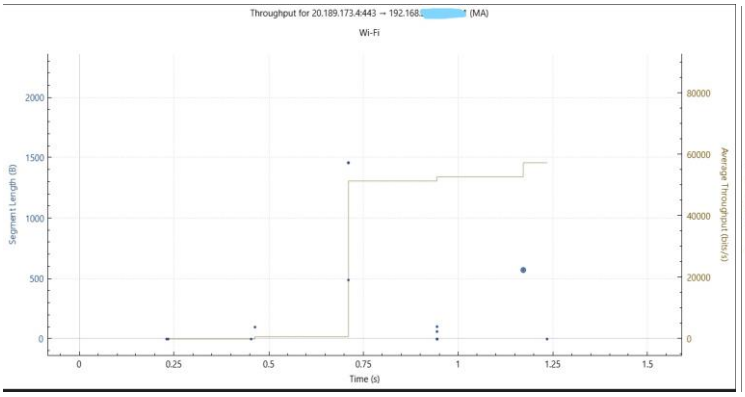


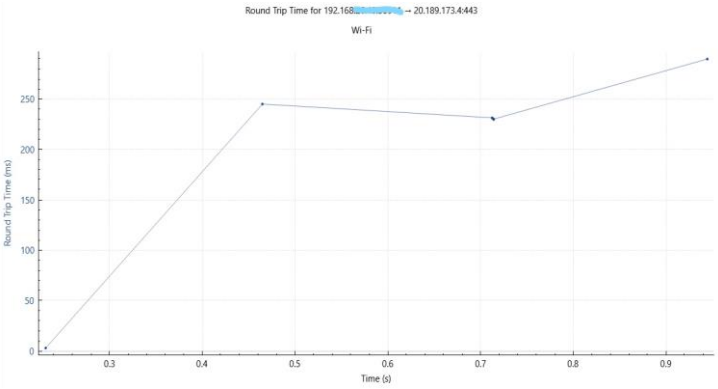
In the above images, there is a handshake sequence, as we can see that the client is sending a “Client hello” message in the packet no. 953. We can also see that we are getting a response from the server ”Server Hello". The above packets took place while creating a new folder.
The below shown sequence was sniffed while downloading a file from OneDrive. It does not contain any handshaking sequence.

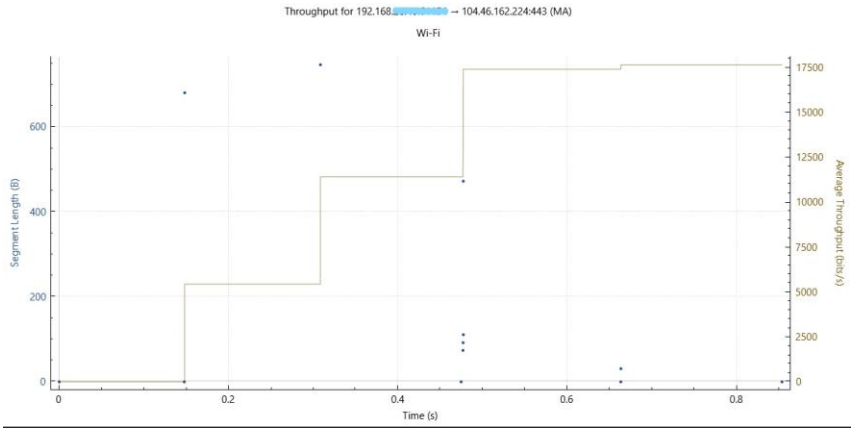


The presence of a handshaking sequence depends on factors such as nature of operation and the protocols used. In the first operation of creating a new folder in OneDrive, since the change was being made in the cloud server, the handshaking sequence was required. However, while downloading a file, since there were no changes to be made in the cloud server, the handshake was not necessary.

Q4. Some of the screenshots of the graph is attached below, and the statistical data is shown in the attached files namely 'Morning_Data.txt', 'Afternoon_Data.txt' and Night_data.txt'. The required values are mentioned at the end of the particular '.txt' files.







Q5. The IP address of the application changes frequently depending on the time the operations are performed. This is because the server has multiple IP addresses, among which one of the addresses is assigned to one or a few clients. One of the advantages of this is that it prevents data packet loss, by handling the congestion, i.e. if an IP address has a lot of network traffic, a new IP address is assigned to communicate with other clients. This also ease of administration and security by not being easily able to track the packets.

Here is a list of all the IP addresses along with time captured used by OneDrive:

- 20.189.173.4 (Morning)
- 20.189.173.11 (Afternoon)
- 104.46.162.224 (Evening)
- 40.79.189.59 (Night)