1. What is the duration of the capture file in seconds? What about the start and end time of the capture expressed in hh:mm:ss?

Solution:

The duration for the capture file is 11.862697.

Start time for the capture is : 12:12:54.297846

End time for the capture is : 12:13:06.160543

2. How many protocols do you see in the protocol window? List the names of some of these protocols. You can find information about the protocols from the “protocol” field. You can sort on this field or any other field in the review window. You can also add or delete fields from the list.

Solution:

There are following protocols in the protocol window:

1. TLSv1.3 and TLSv1.2
2. TCP
3. QUIC
4. DNS
5. How many IPv4 conversations do you have in your capture? You can get these if you investigate Statistics -> Conversations.

3. How many IPv4 conversations do you have in your capture? You can get these if you investigate Statistics -> Conversations.

Solution:

We have 28 IPv4 conversation in our capture.

4. What is the IP address of the DNS server you are connecting to? To minimize the search time, you should search for a specific string, in this case “google” since we ended up typing www.google.com in the web browser and it is what the system needs to resolve with DNS to get to the appropriate IP address of the Google server servicing your search request. To find a string within a packet, click on Edit > Find Packet. Under "Find By:" select "string" and enter your search string in the text entry box.

Solution:

The I.P address of the DNS server we are trying to connect is : 10.17.21.2

5. What is the IP address of the Google server? Once you locate DNS query within all captured packets, you will be able to easily find this address as well.

Solution:

The I.P address of the google server is : 142.251.40.196

6. Type udp.port in Apply a Display Filter ... <Ctrl-/>? field and click Enter. List the protocols in the ”Protocol” field that you see.

Solution:

The protocol which we can see while applying udp.port filter is: QUIC. QUIC stand for Quick Internet UDP connection.

7. What is the Checksum field in the UDP header used for and can it be used for reliable data delivery?

Solution:

The checksum field in the UDP header is used to detect errors in the UDP datagram during transmission. While sending datagram, the checksum value is calculated by the sender and include in the UDP header. And when the datagram is received by the destination, it calculates the checksum value and compares it with the checksum value in the UDP header.

The checksum field in the UDP header does not guarantee reliablity. As it cam detect errors in the UDP datagram, it does not provide any mechanisms for recovering lost or

corrupted data as there is no mechanism in the UDP.

8. What is the TOS field in the IP header used for and can it be used for reliable data delivery?

Solution:

The TOS(Type of Service) field in the IP header is used to specify the quality of service(QOS) required for a particular packet as it travels through the network. The TOS field is an 8 -bit field where first 3 bits use dot indicate precedence, 4th bit is used to signal for low delay, 5th bit for high throughput, 6th bit for high reliability, 7th and 8th bit are reserved.

The modern redefinition of the TOS field, is an 8 bit differentiated services field(DS field) which consists of a 6 bit Differentiated Services Code Point(DSCP) field and a 2 bit Explicit Congestion Notification(ECN) field.

However, the TOS field alone is not sufficient to guarantee reliable data delivery. It can help in prioritize the traffic, it does not provide any mechanisms for error detection or correction, nor does it provide any means of recovering lost or corrupted data,]. For reliability, a protocol like TCP is more useful as it provides mechanisms for error detection, retransmission of lost data, and flow control.

9. What is the Sequence Number field in the TCP header used for?

Solution:

The Sequence Number field in the TCP header is used to provide a unique identification number for each byte of data that is transmitted in a TCP connection. The Sequence Number allows the receiver to determine whether data has been lost or corrupted during the transmission. Gaps in the sequence numbers indicate that some data has been lost or corrupted and needs to be retransmitted. The sequence Number plays a key role I. Ensuring that the data is received in the correct order. The Sequence Number field along with Acknowledgement Number field helps in implementing reliable data delivery.

10. What is the timestamp field in the UDP header used for?

Solution:

The timestamp field in the UDP header is used to show the conversation timestamp. It shows the time since the first frame and the time since the previous frame. It is used to get the conversation timestamp for each conversation separately. It can be helpful in spotting large delays. The general time column will tell us the time for each packet regardless it is a part of single stream or not but the timestamp added by the Wireshark is providing that information for each UDP connection separately.

11. Elaborate how the router uses TCP acknowledgment for reliable packet delivery?

Solution:

TCP(Transmission Control Protocol) is a connection-oriented protocol that provides reliable packet delivery. It use the “Acknowledgement” to ensure that the packets are delivered successfully from the sender to receiver. When. A sender sends a packet, it sets a timer to wait for an acknowledgement from the receiver. If the sender doesn’t receive the acknowledgement within the specified time, it assumes that was lost or damaged and retransmit it.

In TCP the sender sends packet to the receiver and the sender starts a timer and waits for an acknowledgement form the receiver. The receiver receives the packet and send an acknowledgement(ACK) back to the sender. The sender receives the ACK and stops the timer. If the sender doesn’t receive an ACK within a specified timeout period then it assumes that the packet was lost or damaged and therefore retransmit it. This mechanism ensures the reliable delivery.

In TCP we have sequence number which ensure that the packets are delivered I the correct order as each packet is assigned a unique sequence number by the sender, and the receiver uses this to reassemble the packets in the correct order.

So in this way it ensures the reliable packet delivery.