Analyzing UDP datagrams using wireshark

A. In the packet list pane, select the first DNS packet. In the packet detail pane, select the User Datagram Protocol. The UDP hexdump will be highlighted in the packet byte lane. Using the hexdump, Answer the following:

a. the source port number.

47291

b. the destination port number.

53

c. the total length of the user datagram.

60

d. the length of the data.

40

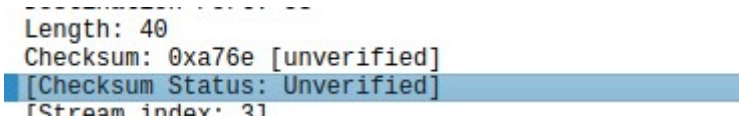
e. whether the packet is directed from a client to a server or vice versa.

Client to server

f. the application-layer protocol.

User datagram protocol

g. whether a checksum is calculated for this packet or not.



B. What are the source and destination IP addresses in the DNS query message? What are those addresses in the response message? What is the relationship between the two?

In the response HTTP message, the address are the opposite i.e. source becomes the destination and the previous destination becomes the source.

C. What are the source and destination port numbers in the query message? What are those addresses in the response message? What is the relationship between the two? Which port number is a well-known port number?

QUERY: src: 47291 dst: 53
RESPONSE: src: 53 dst:47291
53 is the standard port for DNS

D. What is the length of the first packet? How many bytes of payload are carried by the first packet?

Length: 40
UDP Payload: 202 bytes

FLAGS:

SYN, SYN-ACK, ACK

1. What are the socket addresses for each packet?
    SYN: Source: 10.86.2.232:54980 Destination: 8.8.4.4:443
    SYN-ACK: Source: 8.8.4.4:443 Destination: 10.86.2.232:54980
    ACK: Source: 8.8.4.4:443 Destination: 10.86.2.232:54980

2. What flags are set in each packet?
    0X002 : SYN flag is set
    0x022: SYN and ACK flags are set
    0x018: ACK flag is set

3. What are the sequence number and acknowledgment number of each packet?

    SYN:
        Sequence Number: 3791519344 acknowledgment Number: 0
    SYN-ACK:
        Sequence Number: 3897095971 acknowledgment Number: 3791519345
    ACK:
        Sequence Number: 3987100586 acknowledgment Number: 3971307332

4. What are the window size of each packet?
    SYN: 74220
    SYN-ACK: 75445
    ACK: 81850

Part II: Data-Transfer Phase
The data-transfer phase starts with an HTTP GET request message and ends with an HTTP OK message.

1. What TCP flags are set in the first data-transfer packet (HTTP GET message)?
    ACK and PUSH flags

2. How many bytes are transmitted in this packet?
    87 bytes

3. How often does the receiver generate an acknowledgment? To which acknowledgment rule (defined in Page 200 in the textbook) does your answer correspond to?

0.053926

corresponds to NO CONNECTION ESTABLISHMENT(no delay)

4. How many bytes are transmitted in each packet? How are the sequence and acknowledgment numbers related to number of bytes transmitted?

87 bytes transmitted in GET request, 154 bytes recieved in response.

Sequence numbers increases as number of bytes transmitted increase.

5. What are the original window sizes that are set by the client and the server? Are these numbers expected? How do they change as more segments are received by the client?

```
Window: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
```

Window size will increase as long as hardware supports it to reduce congestion.

6. Explain how the window size is used in flow control?

Sender can only send bytes that can fit in the reciever's buffer then must wait till the bytes have been acknowledged to prevent congestion in turn improving flow control.

7. What is the purpose of the HTTP OK message in the data transfer phase?

OK mesage means that the request succeeded

Part III: Connection Termination Phase

The data-transfer phase is followed by the connection termination phase. Note that some packets used in the connection-termination phase may have the source or sink protocol at the application layer.

1. How many TCP segments are exchanged for this phase?

4 segments are exchanged in the connection termination phase. (FIN, ACK, FIN, ACK)

2. Which end point started the connection termination phase?

Browser(sends first fin flag)

3. What flags are set in each of segments used for connection termination?

Segment 1 Client sends FIN flag to server to initiate termination indicating end of data sending process

Segment 2 : Server sends ACK flag to client to acknowledge FIN flag reception

Segment 3 (Server to Client):FIN flag

Segment 4 (Client to Server): ACK flag to indicate completion of termination process