**Lab: 3.7.10 – Using Wireshark To Capture Network Traffic Template**

Answer following questions as part of your homework delivery. Go to the end of the document for submission details:

1. What is the duration of your capture in seconds? What about the start and end time of the

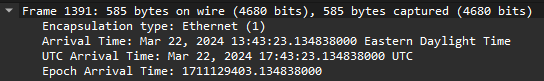
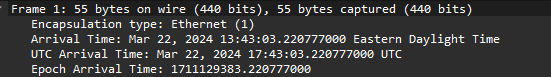
capture expressed in hh:mm:ss?

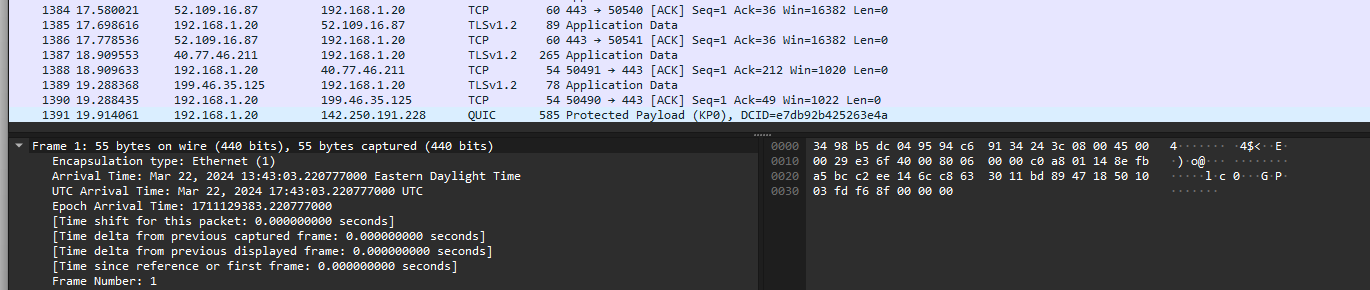
**(Take a Screenshot of this screen)**

**Start Time: 13:43:03**

**End Time: 13:43:23**

**Total Packet Capture Time: 19.914061**





\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. How many protocols do you see in the protocol window? Name some of these for me? You can get these info from the “protocol” field. You can sort on this or any other field in the window.

You can also add or delete fields from the list.

I see 11 protocols listed: TCP, TLSv1.2, QUIC, MDNS and DNS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. How many IPv4 or IPv6 conversations do you have in your capture? You can get these if you investigate

Statistics -> Conversations.

IPv4- 32 conversations

IPv6- 2 Conversations

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

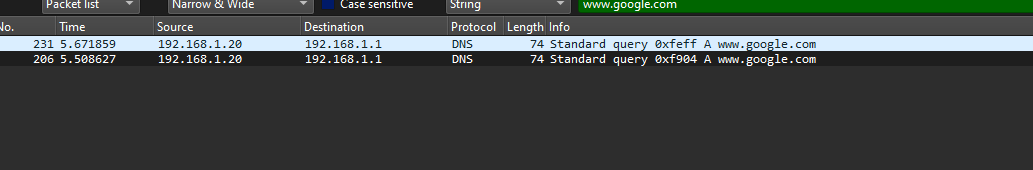
we ended up typing www.google.com in the web browser and it is what the system needs to

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.

My DNS IP is showing as my router. My current PC is connected to a switch, to another wireless switch, and then to my ISP modem (Spectrum)



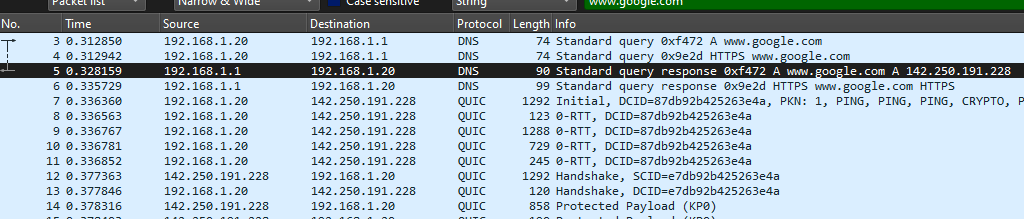
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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 is well.

142.250.191.228



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Type udp.port in *Apply a display filter … <Ctrl-/>?* field and click Enter.

List protocols in ”Protocol” field that you see now.

DNS, DHCPv6, QUIC, NBNS, MDNS, UDP

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now type udp.port in *Apply a display filter … <Ctrl-/>?* field and click Enter.

List protocols in ”Protocol” field that you see now.

DNS, DHCPv6, QUIC, NBNS, MDNS, UDP

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

The checksum header is used to ensure the UDP header is not corrupted. They cannot be used for reliable data deliver.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

This appears to be the same question, but if its referring to the actual state information then it is the packets set state for the acknowledgement of whether the header is corrupt or not. The checksum cannot be used for reliable data delivery in the sense of ensuring the packet reaches the destination, but can be used to ensure the header isn’t corrupt.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

TOS assigns the priority of the IP packet causing it to be forwarded before or after other packets depending on the other packets priority level.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

The sequence number identifies which packet number is being sent for reassembly later and verification that all packets have been received by end device.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. What is timestamp field in UDP header used for?

The timestamp field gives you the time since the first frame was sent and the time since the last frame was sent.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Routers use TCP acknowledgment to identify that they have received a specific packet in the sequence of packets being sent. If the packet is requested to be acknowledged 3 times then the sender will resend that packet known as fast recovery.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please return your completed assignments using Canvas.

The following documents are required as part of your submission.

* **This answer Template completed**
* **Wireshark Capture Assignment1 wireshark.pcap**

**Both files must be uploaded to receive full credit for this assignment.**