CSIS 330 -Lab 3: Using Wireshark To Capture Network Traffic Answer Template

1. Objectives

Capture and Analyze UDP Data in Wireshark

1. Background / Scenario

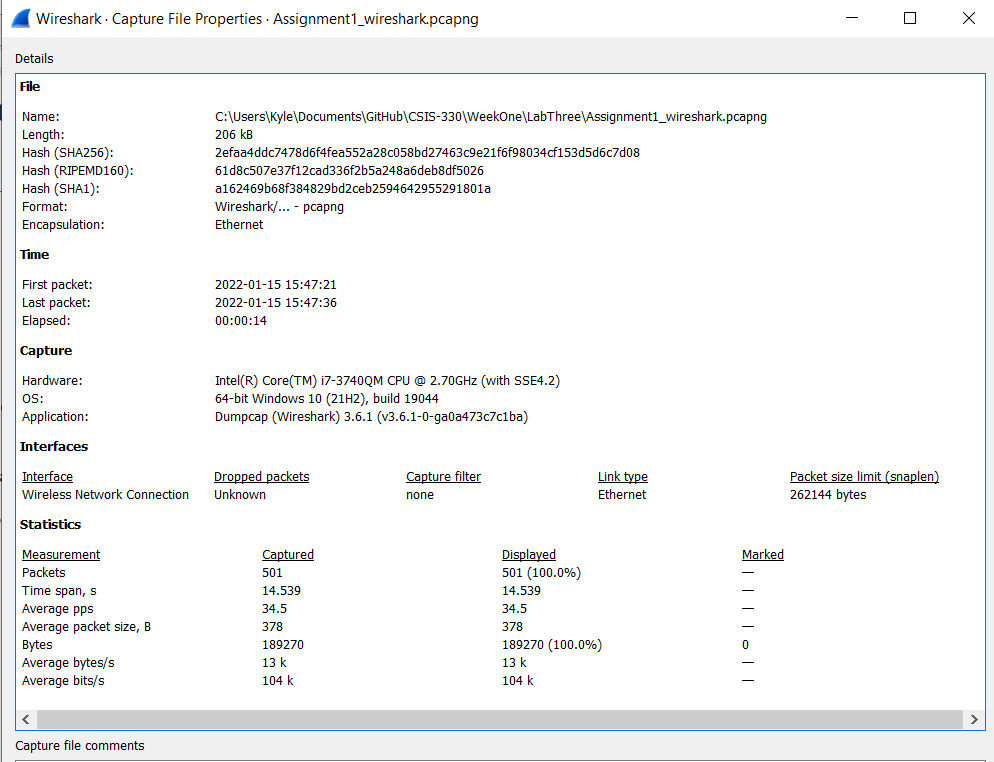
**Wireshark is a Packet Sniffer.**

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)**

duration: 14.538755 seconds



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

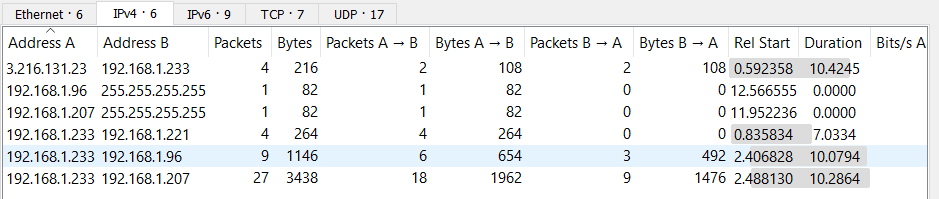
2. How many protocols do you see in the protocol window? Name some of these for me? You can get these info from the “protocol” field. You can sort on this or any other field in the window.

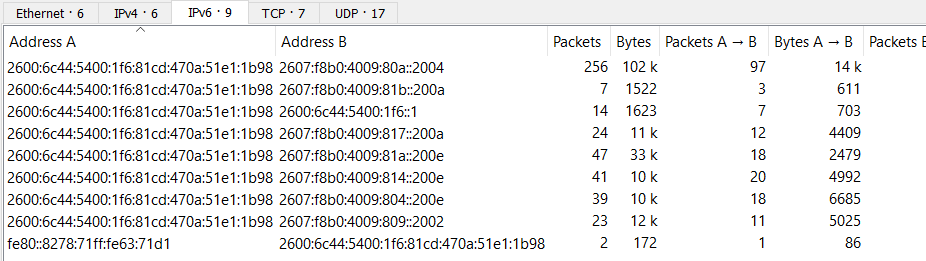
You can also add or delete fields from the list.

7 protocols: ARP, DNS, ICMPv6, QUIC, TCP, TLSv1.2, UDP

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

Statistics -> Conversations.

6 IPv4 conversations:  


9 IPv6 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.

IP Address: 2600:6c44:5400:1f6::1

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.

Google IP Address: 2607:f8b0:4009:80a::2004

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

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

\_\_DNS, QUIC, 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, QUIC, UDP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Checksum is used to identify and validate the integrity of the packet. It CAN be used for reliable data delivery.

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

Checksum field is used to identify and validate the integrity of the packet. It CAN be used for reliable data delivery.

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

TOS is used to classify IP packets in the request so that routers can make decisions about what path the packets should take across the network. It CAN be used for reliable data delivery.

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

Sequence Number is counter that keeps track of every byte sent out by a host.

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

Timestamp field is used for time synchronization and tracks the time at which a packet was forwarded through a network device, measuring network delays and monitoring performance.

https://www.marvell.com/content/dam/marvell/en/public-collateral/switching/marvell-switching-zen-art-of-network-timestamping-white-paper-2018-02.pdf

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

TCP will break down its queued application data into segments and retransmit each segment until an acknowledgement has been received.

Please return your completed assignments using Blackboard.

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.**