**M.V.Balaji**

**210905400**

**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: 49892

b. The destination port number: 53

c. The total length of the user datagram: 47

d. The length of the data (UDP Payload): 47-8 (header information) bytes

e. Packet direction: Directed from client to server

f. Application-layer protocol: UDP

g. Checksum calculation: 0xa74d (unverified)

**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?**

• Source: 172.16.59.34

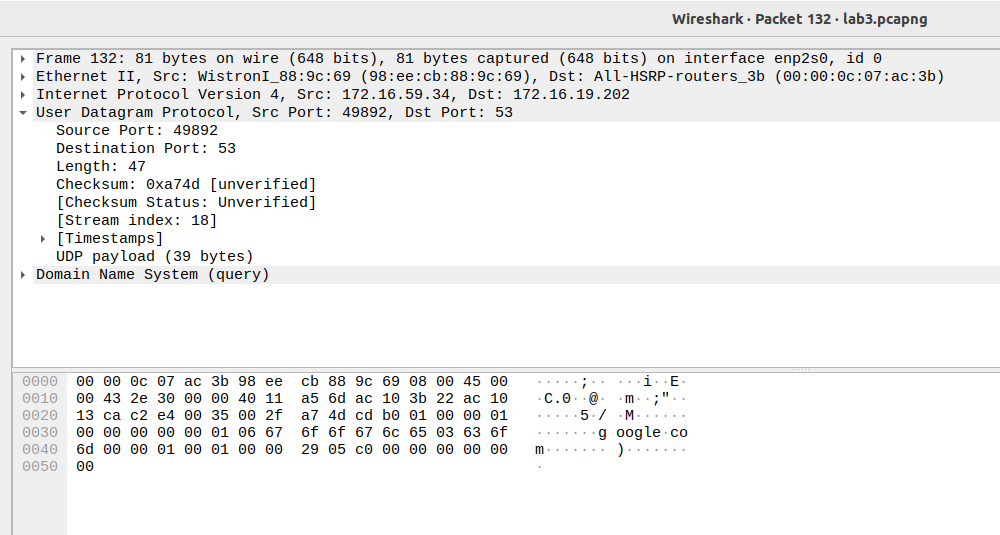
• Destination: 172.16.59.202

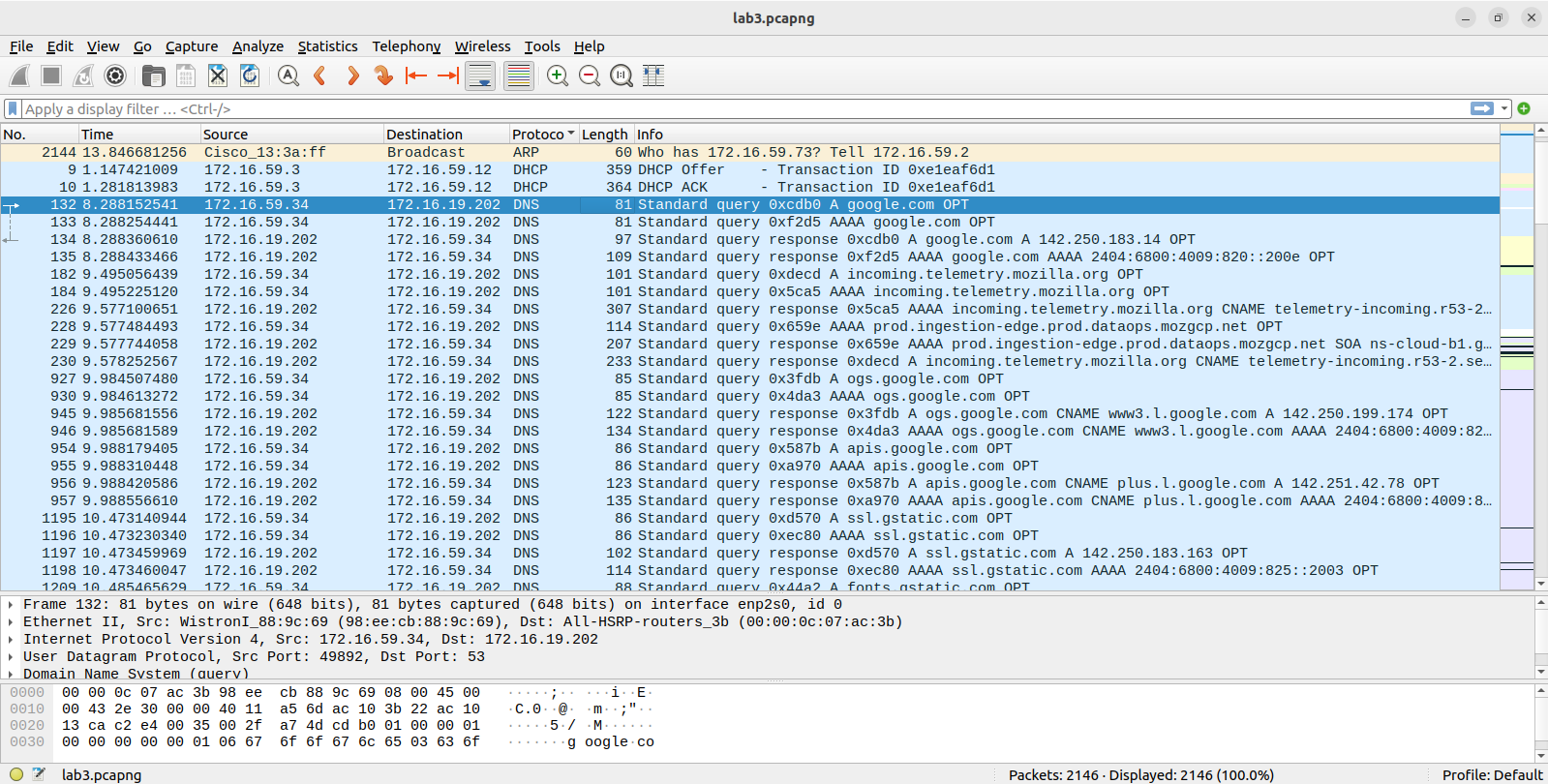
**C. What are the source and destination port numbers in the query message? What are those addresses in the response message? What is the relationship between the two? Which port number is a well-known port number?**

* Source port number: 49892
* Destination port number: 53
* DNS Port 53 is a well known port number

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

Length of 1st Packet:47. It is carrying 39 bytes of payload.





**2B. Analysing TCP packets using Wireshark:**

***Part I: Connection-Establishment Phase***

**Identify the TCP packets used for connection establishment. Note that the last packet used for**

**connection establish may have the application-layer as the source protocol.Using the captured information, answer the following question in your lab report about packets**

**used for connection establishment.**

1. What are the socket addresses for each packet?

* Source:53150 IPAddr:13.225.103.19
* Destination:57764 IPAddr:192.168.168.96

1. What flags are set in each packet?

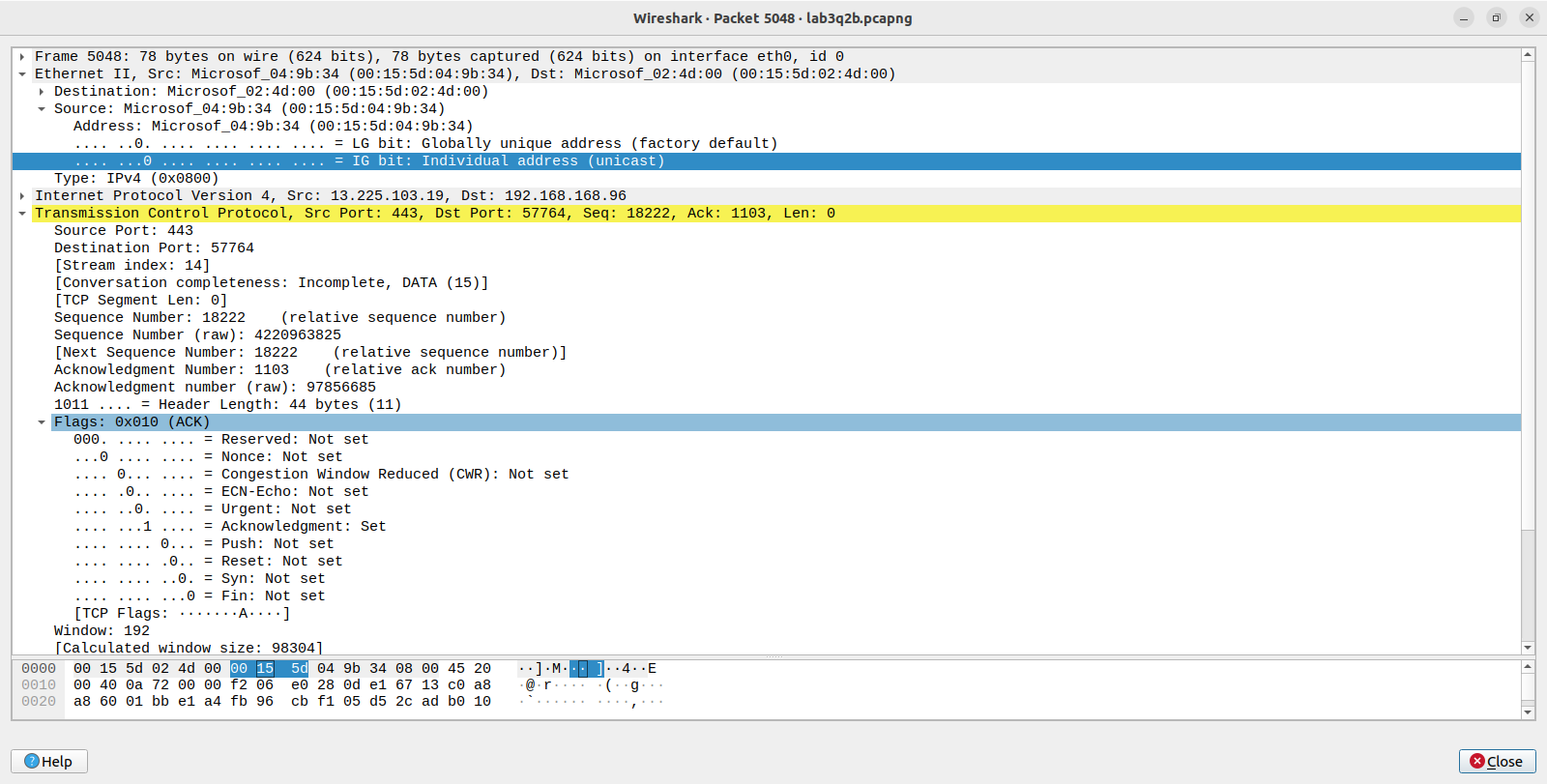
* Flags:0x010(ACK)

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

* Sequence Number:1180
* Acknowledgment:18222

1. What are the window size of each packet?

* 98304

******

***Part II: Data-Transfer Phase***

**The data-transfer phase starts with an HTTP GET request message and ends with an HTTP OK message.Using the captured information, answer the following question in your lab report about packets used for data transfer.**

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

* PSH and ACK

1. How many bytes are transmitted in this packet?

* 293 bytes

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

* 0.005s

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

* 359 bytes are transmitted each packet. The sequence number increases by the number of bytes transmitted, and the acknowledgment number increases by the number of bytes received.

1. 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?

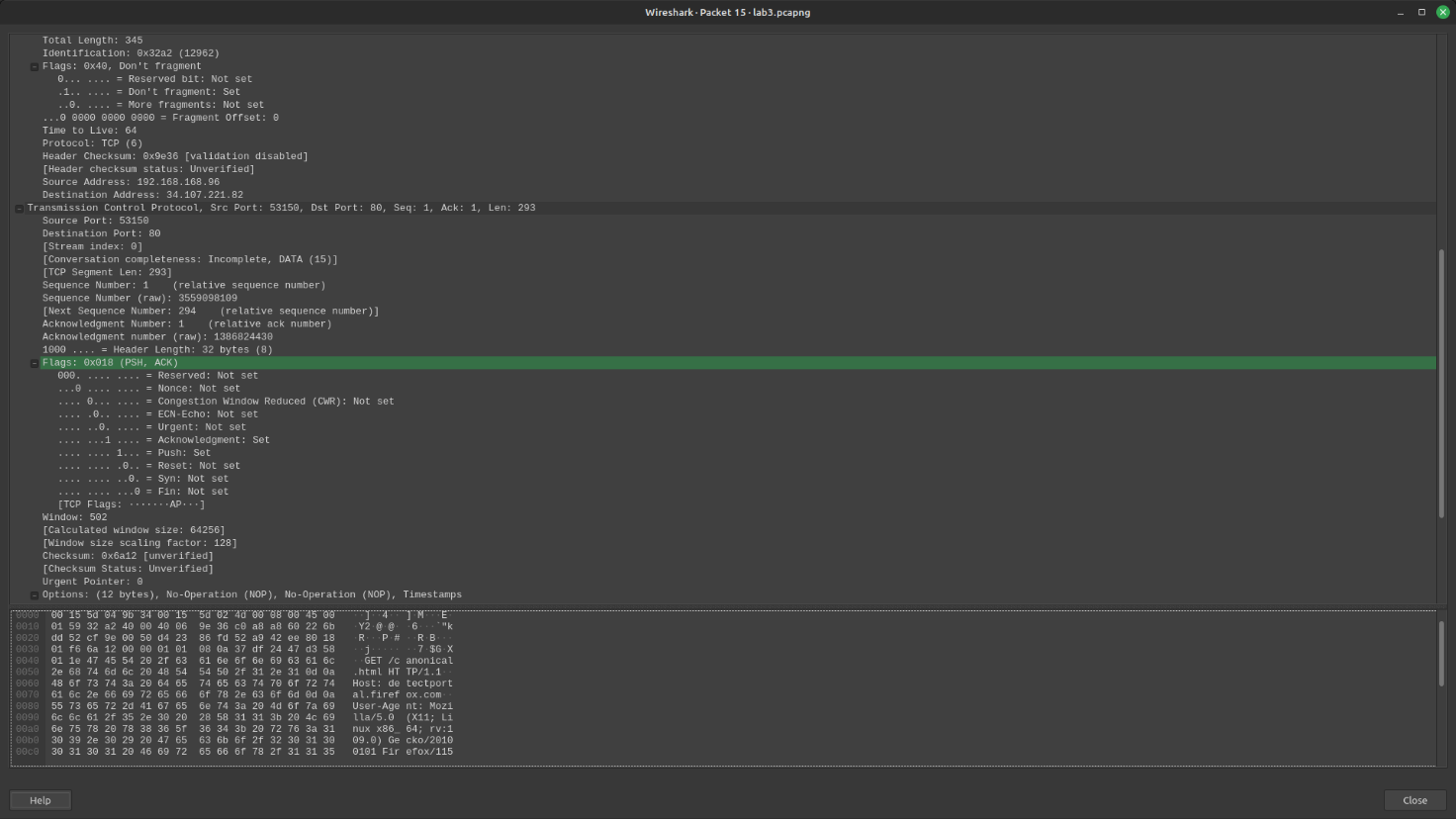
* Original Window Size:64256
* Received Size:128

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

* The client should be able to receive all windows while avoiding any congestion,so flow control is implemented to send a window soze better suited for the client

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

* The HTTP OK message is a feedback about the request OK response indicates that a request has 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. Find the packets used for connection termination.Using the captured information, answer the following question in your lab report about packets used for connection termination.**

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

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

1. Which end point started the connection termination phase?

* Client

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

* FIN and ACK Flag

