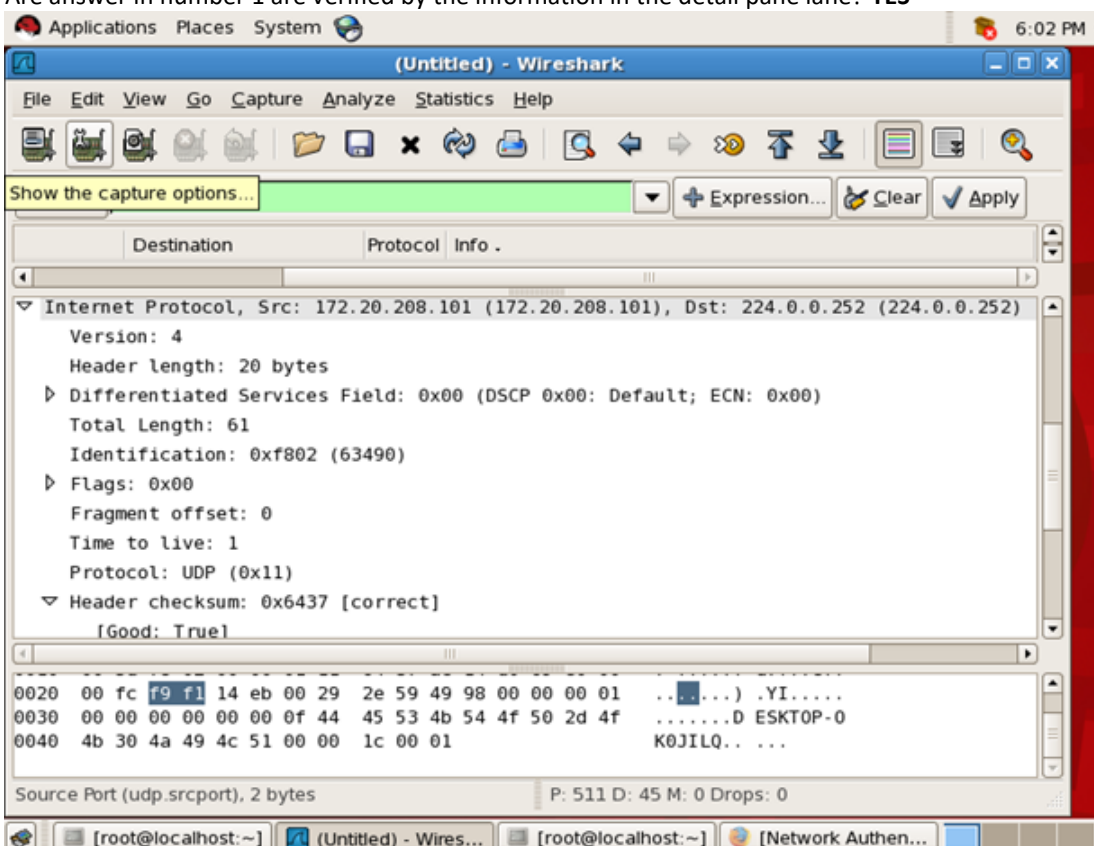


Report for Lab 3-1: UDP

Name: Soham Desai		Student ID: 202003021	Date: 21/03/2022
1	a. Source port number: 63985	b. Destination port number: hostman(5355)	
	c. Total length of user diagram 41	d. Length of data 33	
	e. Is the packet from client or server? Both	f. Application layer protocol: UDP	
	g. Is checksum calculated? Yes		
2	Are answer in number 1 are verified by the information in the detail pane lane? YES		
			
3	Source and destination IP addresses in the query message: fe80::ad7f:681f:79ac:cf3f(source) ff02::1:3(destination) Source and destination IP addresses in the response) message: 63985(source)		

	<p>hostman(5355) (destination)</p> <p>Relation between IP addresses: Source IP address: the IP packet field containing the IP address of the workstation from which it came. Destination IP address: the IP packet field containing the IP address of the workstation to which it is addressed.</p>
4	<p>Source and destination port number in the query message: 63985 (source) hostman(5355) (destination)</p> <p>Source and destination port number in the response message: fe80::ad7f:681f:79ac:cf3f(source) ff02::1:3(destination)</p> <p>Relation between port numbers: Source port number: the port number field containing the port number of the workstation from which packet is sent. Destination port number: the port number field containing the port number of the workstation to which it is a packet is received.</p> <p>Which port number is well-known? 0 - 1023</p>
5	<p>The length of the first UDP packet: 76</p> <p>How many bytes of payload are carried by the first UDP packet? total length - header length = 76-20 = 56</p>
6	<p>Number of bytes in the DNS message:4</p> <p>Does the count agree with the answer to question 5? No</p>
7	<p>Is the checksum calculated for the first UDP packet? Yes</p> <p>Value of the checksum: 0xc43e</p>

Report for LAB 3-2: TCP

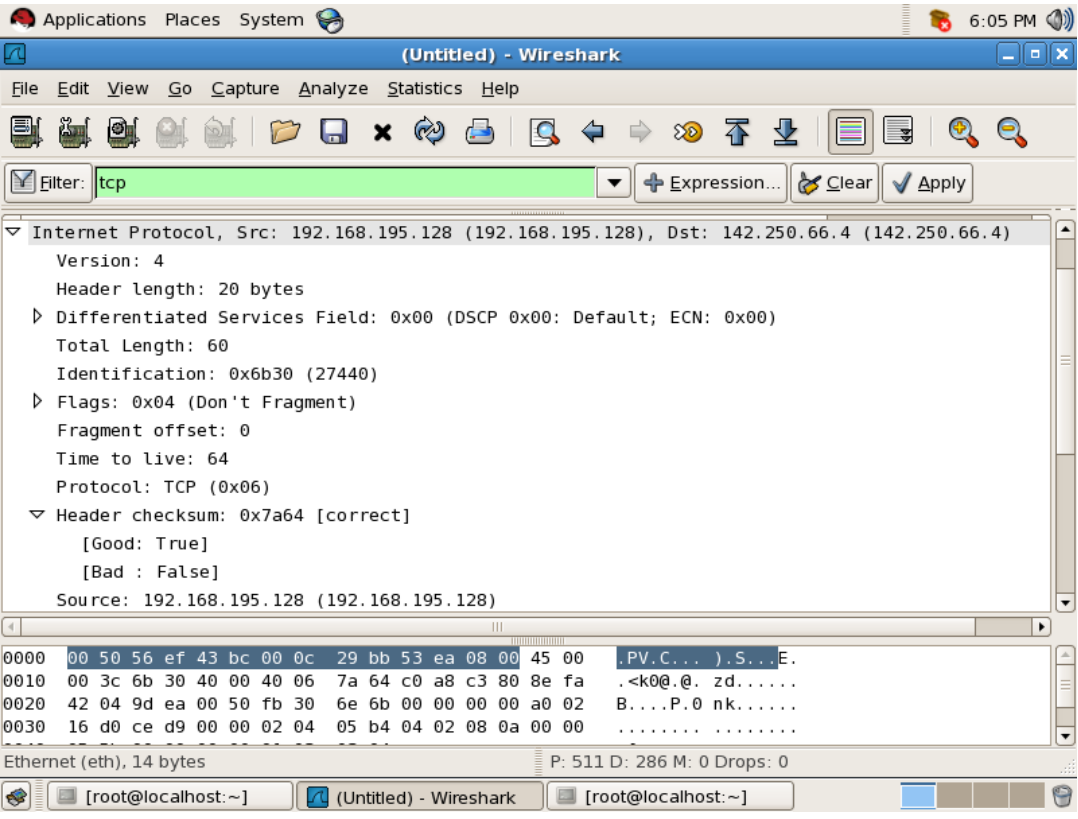
Name: Soham Desai	Student ID: 202003021	Date: 21/03/2022
--------------------------	------------------------------	-------------------------

Part I	
1	Socket addresses: Source: 142.168.195.128 Destination: 142.250.66.4
2	Set flags: PSH and ACK
3	Sequence number and acknowledgement number: 2805 and 893
4	Window size: 5840

Part II	
1	Set flag in HTTP GET message: ACK, PSH
2	Number of bytes transmitted by the HTTP GET message: 235
3	Acknowledgement frequency: $22.831829570\text{ s} - 22.826527150 = 0.00530242\text{ s} = 5.30242\text{ ms}$ Corresponding rule: An acknowledgement be sent for at least every other full-size segment, and that no more than 500ms expire before any segment is acknowledged.
4	Number of bytes transmitted by each packet: 60 Relation to sequence and acknowledgement Number: 1:1
5	Original window sizes: 5840 Are these numbers expected? Yes How window sizes change? The window size keeps increasing as long as the receiver sends acknowledgments for all our segments or when the window size hits a certain maximum limit. When the receiver doesn't send an acknowledgment within a certain time period (called the round-trip time) then the window size will be reduced.

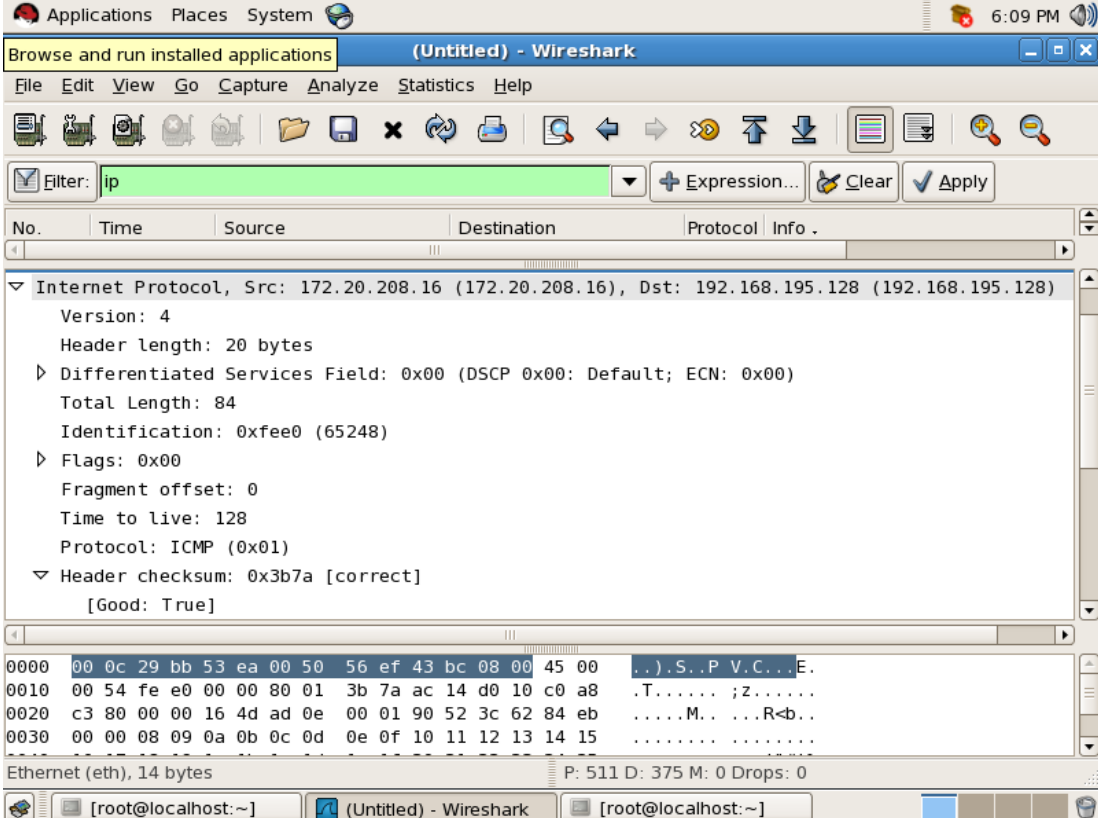
6	<p>How the window size is used in flow control?</p> <p>Flow control is accomplished by the receiver sending back a window to the sender. The size of this window, called the receive window, tells the sender how much data to send. Often, when the client is saturated, it might not be able to send back a receive window to the sender to signal it to slow down transmission.</p>
7	<p>Purpose of the HTTP OK message:</p> <p>The request has succeeded. The meaning of the success depends on the HTTP method:</p> <p>GET: The resource has been fetched and is transmitted in the message body.</p> <p>HEAD: The entity headers are in the message body.</p> <p>PUT or POST: The resource describing the result of the action is transmitted in the message body.</p> <p>TRACE: The message body contains the request message as received by the server.</p>

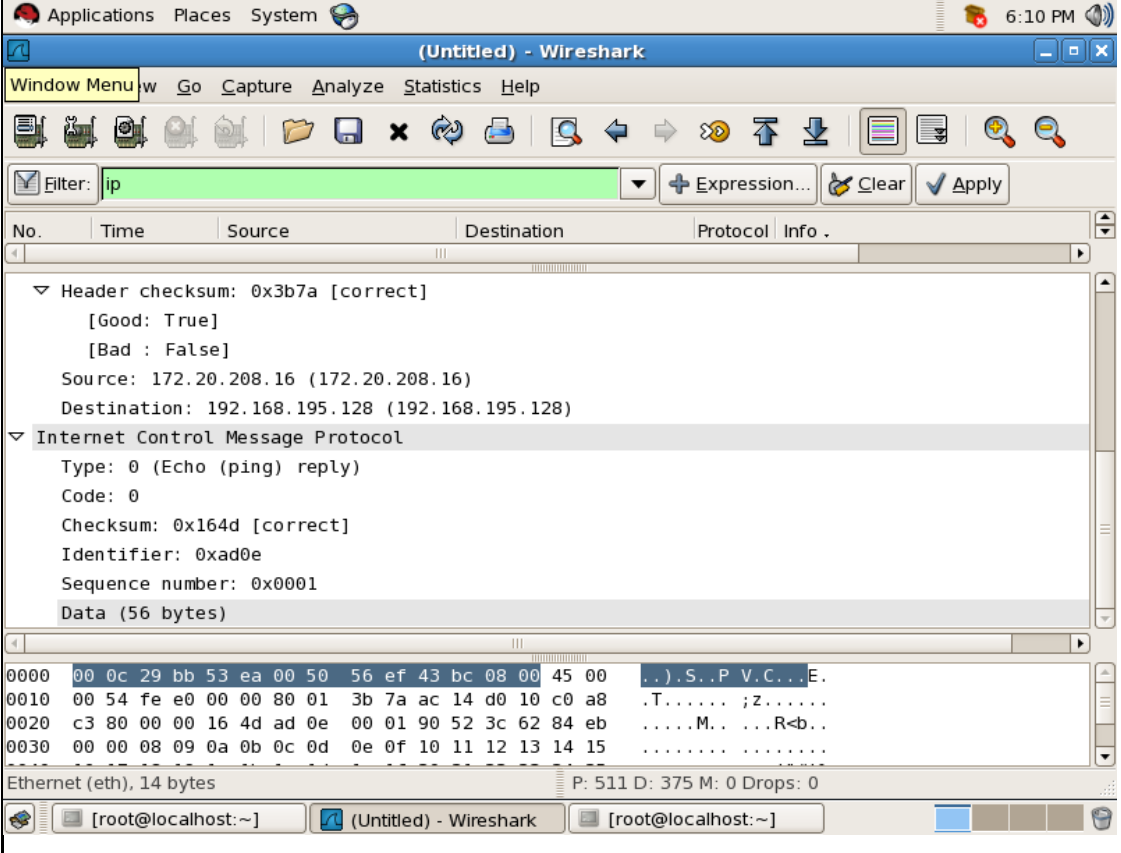
Part III	
1	Number of TCP segments exchanged for connection termination: N/A
2	Which end point started the connection termination phase? N/A
3	Flags sets in each of the segments used for connection termination: N/A

Part IV		
1	a. Source port number: 40426	b. Destination port number: http (80)
	c. Sequence number: 2805	d. Acknowledgment number: 897
	e. Header length: 40 Bytes	f. Set flags: ACK and PSH
	g. Window size: 5840	h. Urgent pointer: 0
2	<p>Are answer in the question number 1 verified by the information in the detail pane lane? Yes</p> 	
3	<p>Does any of the TCP packet headers carry options? Yes</p> <p>Explain</p> <p>TCP options fields are at the end of the header and they are multiple of 8 bits. If any of bits remains from options, they can be filled by padding, with zeros. This options are MSS, Window Scaling, Selective Acknowledgements, Timestamps and Nop. The size of this field is changable according tot the used options. Generally these options are used during the 3-way handshake but others can be use during normal TCP session.</p>	

4	Size of a TCP packet with no option: 157 Size of a TCP packet with options: 169
5	Is window size in any of the TCP packet zero? Explain: When a client (or server – but it is usually the client) advertises a zero value for its window size, this indicates that the TCP receive buffer is full and it cannot receive any more data. It may have a stuck processor or be busy with some other task, which can cause the TCP to receive buffer to fill. Zero Windows can also be caused by a problem within the application, where the TCP buffer is not being retrieved.

Report for Lab 4-1: IP

Name: Soham Desai		Student ID: 202003021	Date: 21/03/2022
1	a. IP version:4	b. Header length:20 bytes	
		Number of bytes in the header:20	
	c. Service type: Differentiated	d. Total length:84	
	e. Identification: 0xfe0 (65248)	f. Flags:0x00	
	g. Fragmentation offset: 0	h. TTL:128	
	i. Upper layer protocol: ICMP(0x11)	j. Checksum:0x3b7a [correct]	
	k. Source IP address:172.20.208.16	l. Destination IP address:192.168.195.128	
2	Are answers to question 1 verified by the information in the packet detail pane? Yes		
			

	
3	<p>If the checksum in the packet detail pane is marked correct, can we conclude that the IP payload is not corrupted?</p> <p>Explain.</p> <p>YES, IPv4 has a header checksum. It only covers the header, so any corruption of the IP payload is not detected. Due to each router having to update the TTL field, the checksum has to be recomputed at each hop.</p>
4	<p>Is the datagram fragmented?</p> <p>Explain.</p> <p>NO, Since the don't fragment flag is set, the datagram is not fragmented.</p>
5	<p>Does source or destination address belong to one of the special addresses?</p> <p>If yes which one?</p> <p>YES, they are ipv4 addresses and are also called the loopback addresses</p>
6	<p>Number of bytes of data in the IP payload:</p> <p>total length - header length = 84-20 = 64</p>