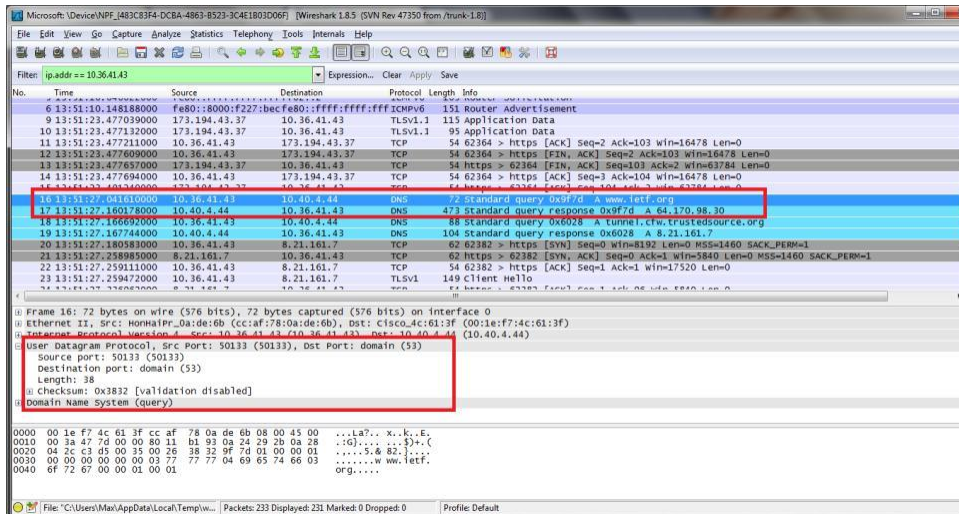


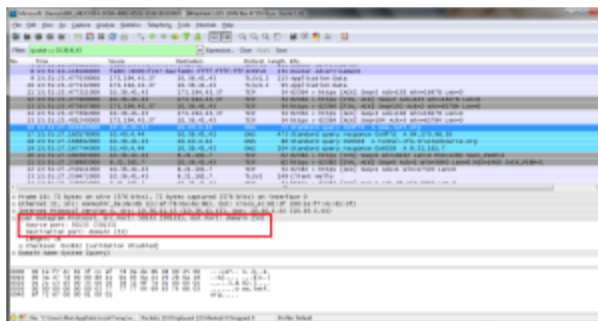
WEEK - 13

Ans1. The DNS query and response messages are sent over UDP.



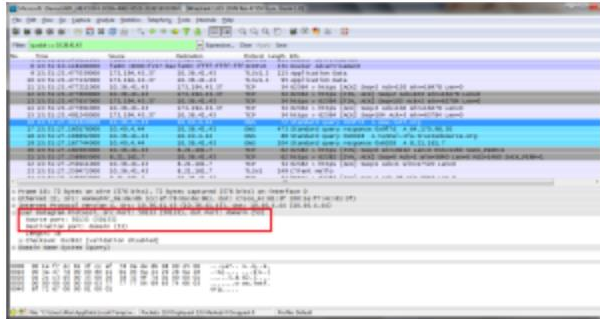
Ans 2.

- The destination port is 53
- The source port is 50133

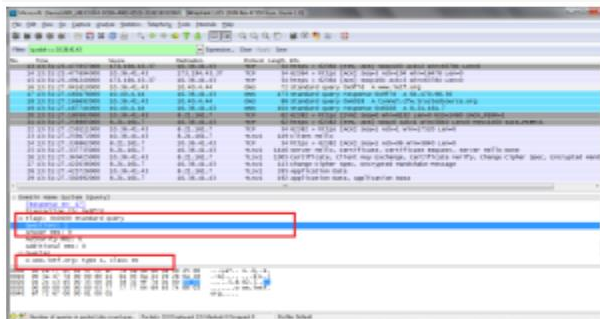


Ans 3. The destination port is 53

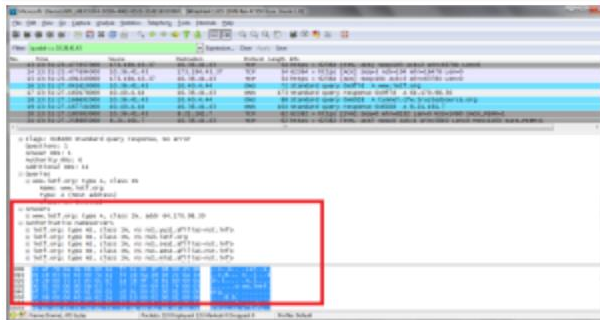
- The source port is 50133



Ans 4. The query message was a type “A” query, but the message did not contain any “answers.”

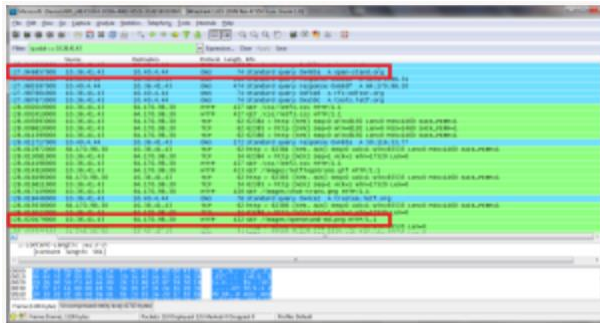


Ans 5. The response message contained one answer to the query which was the sites address [64.170.98.30]. Although it also provided 6 authoritative nameservers, and 11 other responses containing additional information.



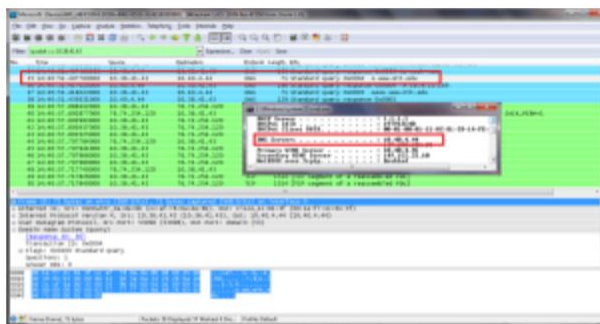
Ans 6. The destination of the SYN packet is 64.170.98.30, the same address that was provided in the DNS response message as the type “A” address of the webpage.

Ans 7. Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made.



12.

- The DNS query message is sent to IP address 10.40.4.44, the same address as my default local DNS server.



13.

- The DNS query message is a type "A" query, containing only one question and not containing any answers.

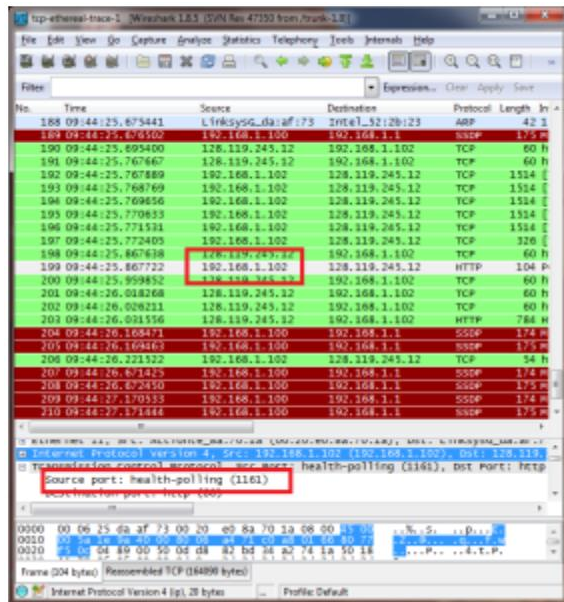
14.

- The response message contains one answer to the aforementioned query which is the type "A" address of <http://www.mit.edu> or 18.9.22.169. It also contained information on 3 authoritative nameservers and 3 additional records.

TCP

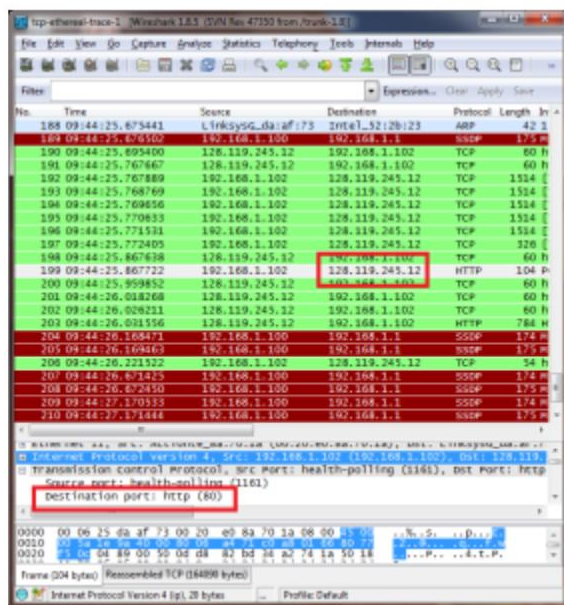
1.

- The source IP address was 192.168.102 using source port 1161.



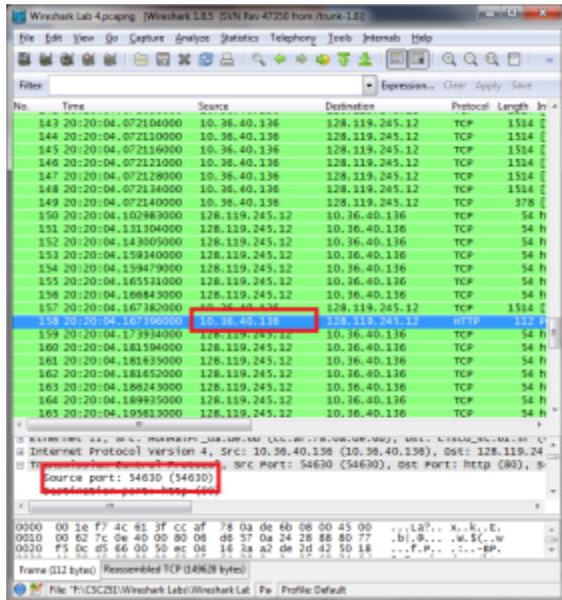
2.

- The destination IP address is 128.119.245.12 receiving on port 80



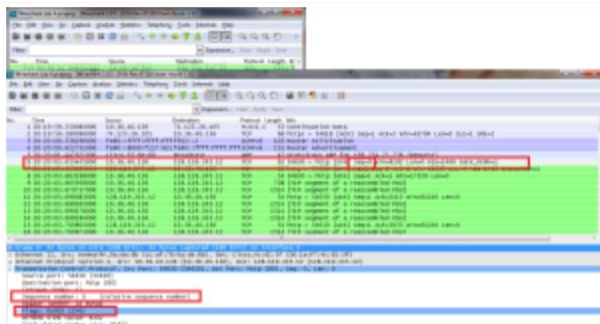
3.

- My IP address source is 10.36.40.136 sending on port 54360.



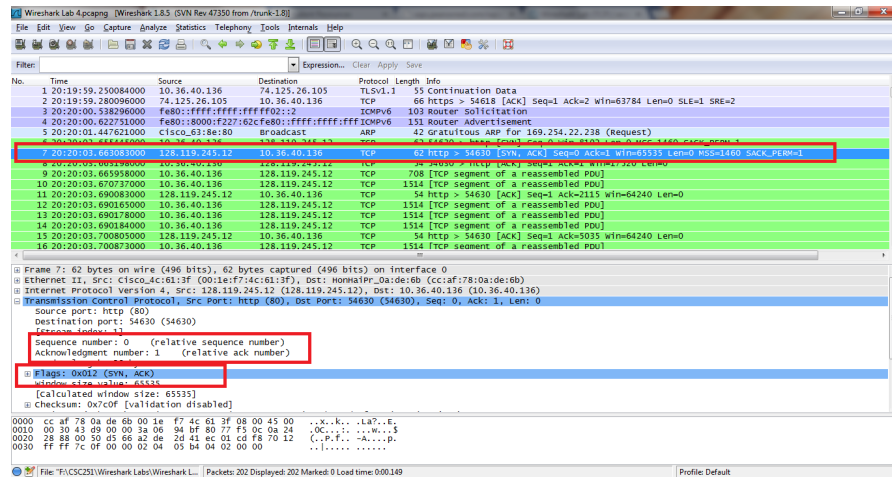
4.

- The sequence number of the segment used to initiate the TCP connection is 0. We can see that the message contains a SYN flag indicating that it is a SYN segment.



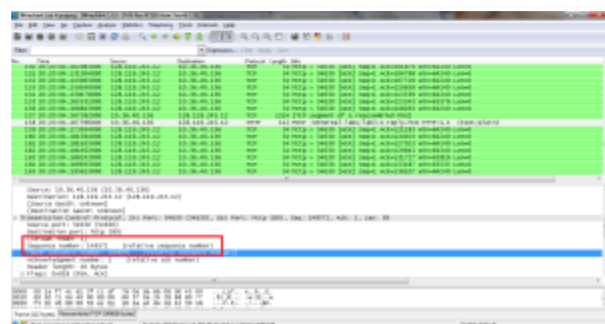
5. The sequence number of the SYNACK segment is 0.

- The value of the acknowledgement field is 1. This value is determined by the initial sequence number + 1.
- The message carries flags that show it to be a SYN ACK message.



6.

- The sequence number of the TCP segment containing the HTTP Post Command is 149571.



7.

