בס״ד

Name: Daniel Attali I.D.: 328780879 Date: 30/10/2024

**Advanced Computer Networks – רשתות מחשבים מתקדם**

**Laboratory 01 - Wireshark Exercise:**

Credit: Laura Chappell, Wireshark Workbook

This laboratory allows a review of the principles learnt in the “Introduction to Telecom” course. For this laboratory, we advise downloading the last version of Wireshark. You can also follow the installation instructions from p. 12 of “computer networks” from Barak Gonen, Omer Rosenbaum, and Shlomi Hod for a complete and working installation of the required applications for this course.

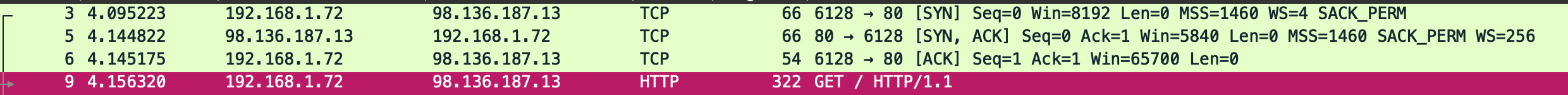
For each question, try to use the right filter to get the answer.

Important note:

For each question, **add explanation of what you did + screenshot**, to get maximal score.

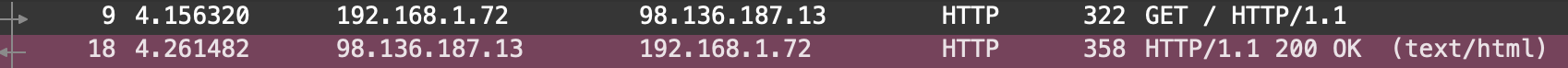
Good Luck 😊

Classwork:

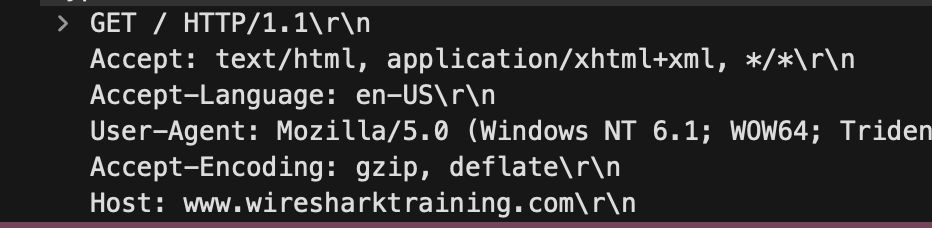
1. What is the IP address of the DNS/HTTP client in the trace file *wwb001-http.pcapng*? I filtered the type of protocol to DNS and searched for the first DNS query 192.168.1.72
2. What is the IP address of the DNS server? I found the DNS query response packet 192.168.1.254
3. What DNS response time is seen in the trace file? 0.256…, the delta of the DNS query and the answer we get 0.256… - 0 = 0.256…
4. Do you think that this trace was taken (captured) closer to the HTTP client or closer to the HTTP server? Closer to the Client since the trace was recorded on the client since when we look at the 3-way-handshaks before the first HTTP request, we see that the time that the first packet (SYN) was recorded at 4.095 and the second (SYN, ACK) was 4.145 and the third (ACK) was at 4.1451 we see that the difference between 2 & 3 (2 times the distance to the client) is smaller than the 1 & 2 (2 times the distance to the server) telling us that we are closer to the client. And since the time difference between 2 & 3 is so close we can safely assume the trace was captured on the client.

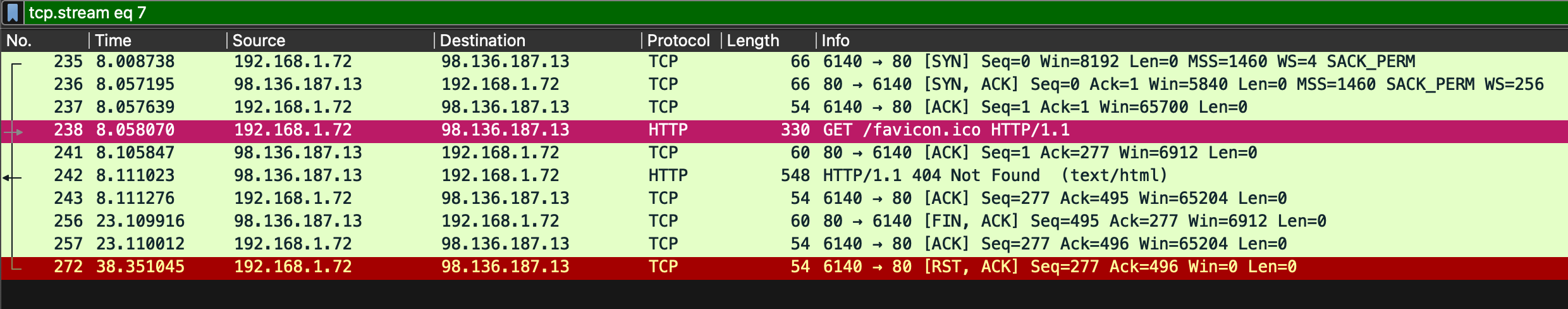
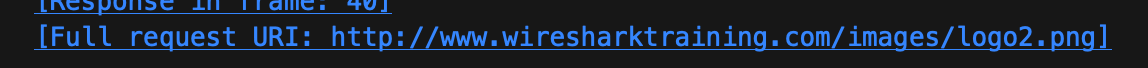
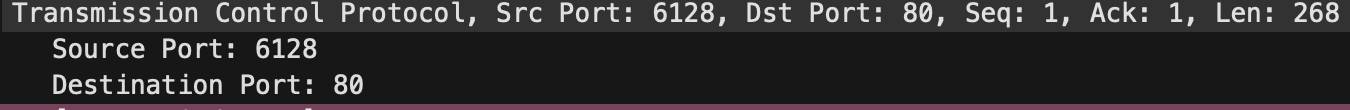
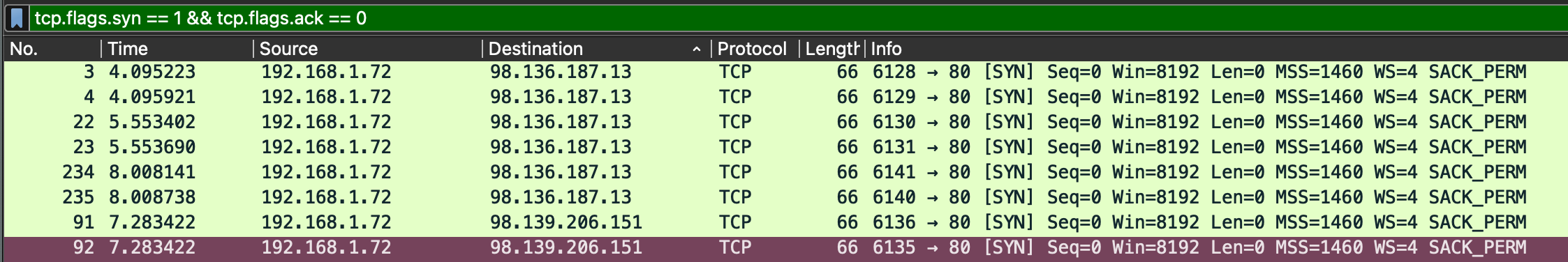
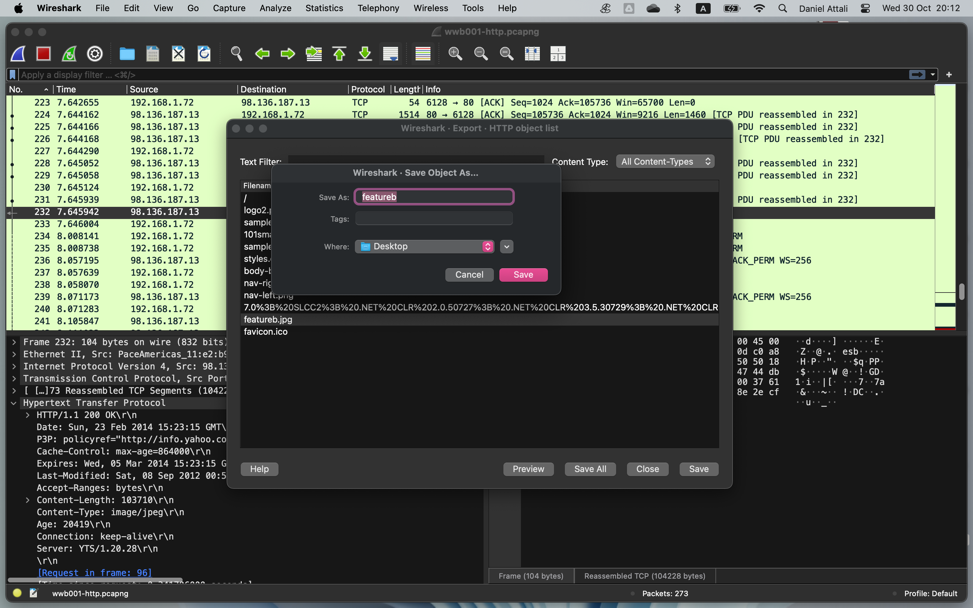
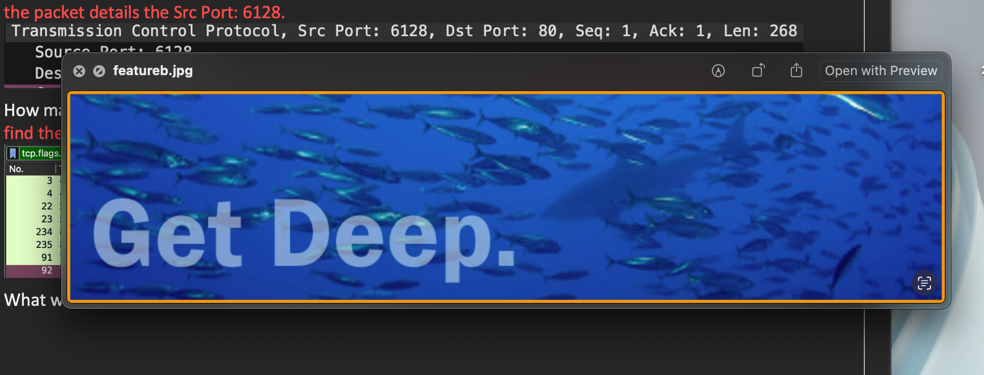
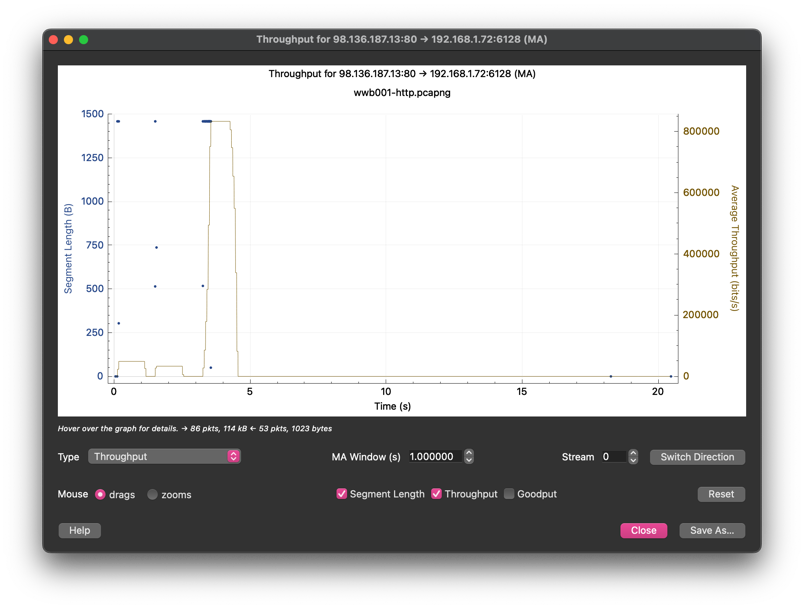
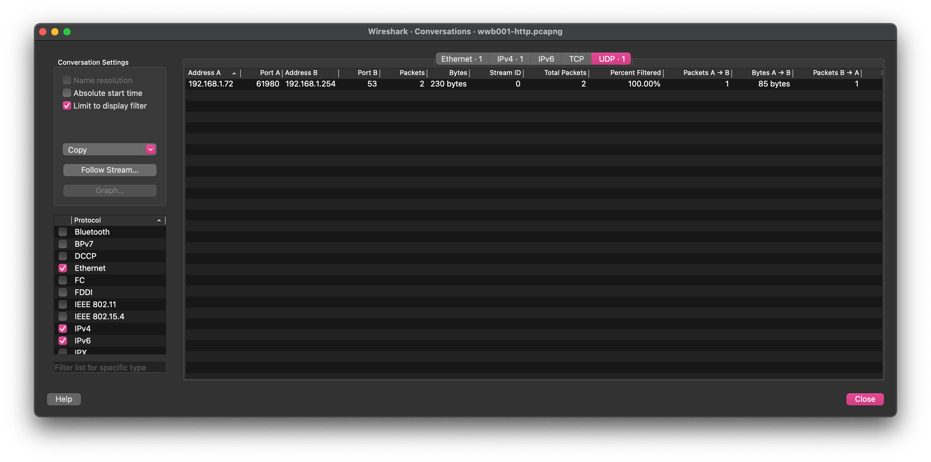
Homework:

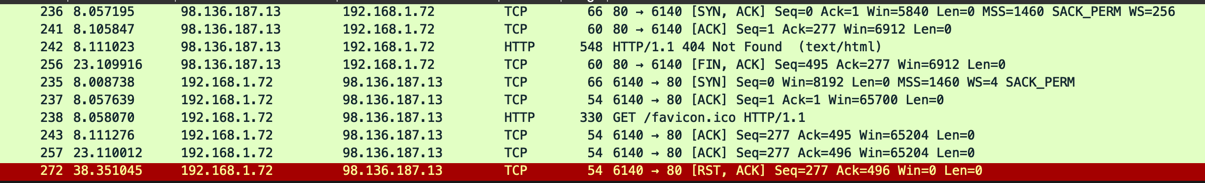
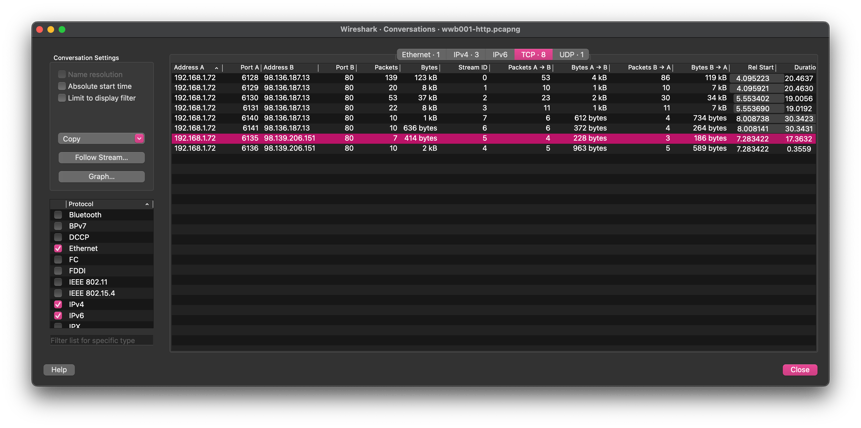
1. What are the IP addresses of the HTTP servers to which the client successfully connected?

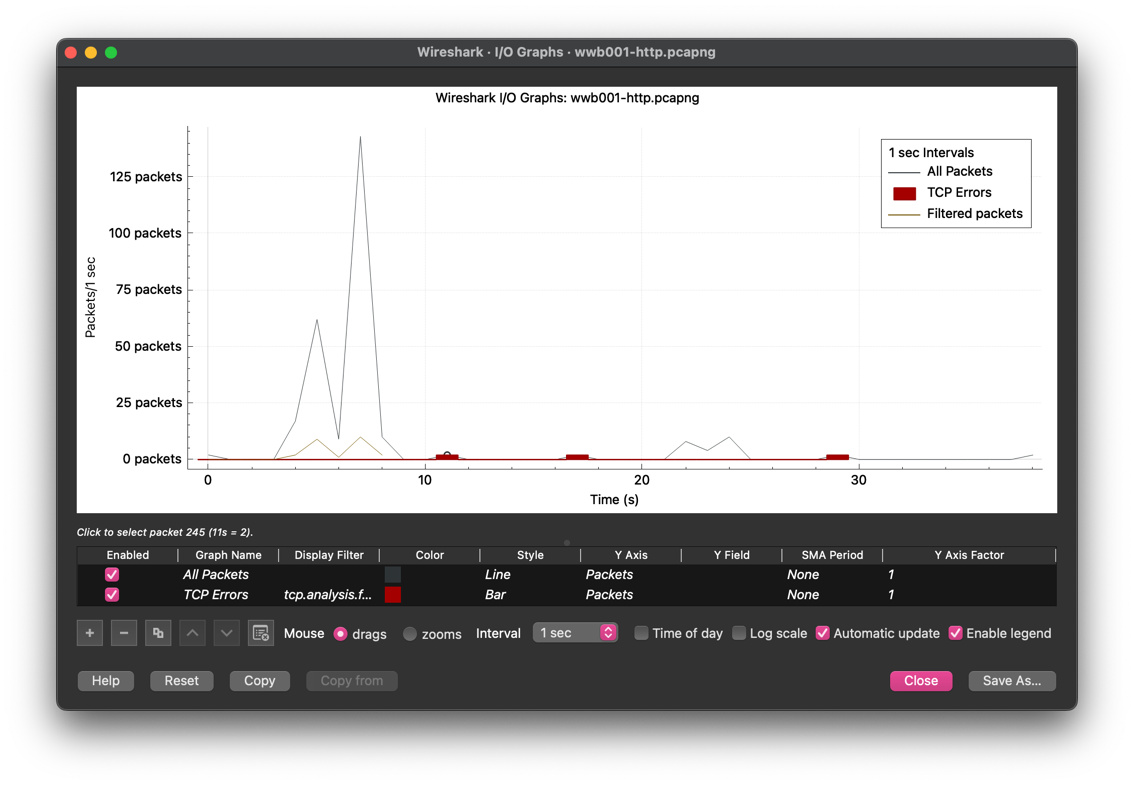
I filtered for the HTTP packets and found the IP Address of the destination server is 98.136.187.13

1. What are the HTTP host names of the target HTTP servers? I searched in the packet details to get the headers of the HTTP request According to the GET request the host is [www.wiresharktraining.com](http://www.wiresharktraining.com)



1. What HTTP error response(s) are seen in this trace file? I searched for one of the HTTP requests the where in the 404 in the response. 
2. What requested web object could not be found on the HTTP server? I searched up the request of the HTTP that got us the 404 response and then followed the stream up and the object that could not be found is “/favicon.ico”
3. What Uniform Resource Identifier (URI) does the client request first in this trace file? The first I found is the request of an image, I found it in the packet details. The URI is “images/logo2.png”
4. What TCP port numbers did the client open to communicate with the HTTP server? According to the packet details the Src Port: 6128.
5. How many TCP SYN packets did the client send to the HTTP servers? After applying the filter to find the TCP SYN packets, and I have found 8 (which is telling us that there is 8 TCP streams).
6. What words are seen in the featureb.jpg image? The text displayed is “Get Deep”, File > Export Objects and exported to file the packet 232 which had the desired image. 
7. What is the average throughput rate (bits per second) in this trace file? I search in Statistic > TCP Stream Graph > Throughputs and found this graph.
8. How many UDP streams are in the trace file? I apply the UDP filter, then in Statistics > Conversations > UDP tab and count the total and I see 1 stream. 
9. What is the purpose of TCP stream 7? Same idea in the Conversations > TCP found the 7th, so in the filter I typed “tcp.stream eq 7” and found the following trace. And according to the trace the steam was to get the “/favicon.ico” which is the displayed icon for the website in the browser and the response was “404 not found” so the stream was terminated.



1. How many times does the packets per second rate reach over 125 in this trace file? Going to Statistics > IO Graph. And getting the following graph I get only once. 

The End