Homework 2 - Wireshark

- This is an individual assignment, and worth 20 points.
- The due date is on Tuesday, September 20, 2:30 (Sec 01) / 5:30 (Sec 76).
- Follow the naming convention (e.g., Homework2-ImG.docx). If you do not follow the convention, I will deduct 1.
- Use "http.cap" (source: https://wiki.wireshark.org/SampleCaptures#Sample_Captures).

1. In the first TCP packet, what is the MAC address of the destination?

   - MAC address: fe:ff:20:00:01:00

2. What are the absolute sequence and acknowledgement numbers of the ACK packet observed during the three-way handshake?

   - Absolute sequence number:

     [SYN, ACK] SEQ = 290218379 ACK = 951057940

   - Absolute acknowledgement number:
     [ACK] SEQ = 951057940 ACK = 290218380

3. What ports are used for the TCP communication during the three-way handshake? List the ports that the client (source) and the server (destination) used.

   - The port # (client used): 3372
   - The port # (server used): 80

4. What are the MSSs (Maximum Segment Size) exchanged during the three-way handshake?

   - The client's MSS: 1460
   - The server's MSS: 1380

5. What are the Window Sizes exchanged during the three-way handshake?
   - The client's Window Size in the SYN packet:8760
   - The server's Window Size in the SYN/ACK packet: 5840

6. Answer the questions using the packets 13 and 17.

1) Domain name to be resolved: pools.arcor-ip.net
2) CNAME record (a):
3) CNAME record (b):
4) A record:
5) The two IP addresses of the A record:

7. List the hostnames the client accessed in this capture.