Homework 2 - Wireshark

- This is an individual assignment, and worth 20 points.
- The due date is on Tuesday, September 21, 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: 951057940
   - Absolute acknowledgement number: 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 bytes
   - The server's MSS: 1380 bytes

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

   1) Domain name to be resolved: pagead2.googlesyndication.com
   2) CNAME record (a): pagead2.google.com
   3) CNAME record (b): pagead2.google.akadns.com
   4) A record: pagead2.google.akadns.com
   5) The two IP addresses of the A record: 216.239.59.104; 216.239.59.99

6. List the host(s) the client accessed in this capture.

   pagead2.googlesyndication.com

   www.ethereal.com