Homework 2 - Wireshark

- This is an individual assignment, and worth 20 points.
- The due date is 2:30 (Sec 01) / 5:30 (Sec 76) on Thursday, September 10.
- 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 handshaking?
   - Absolute sequence number: 951057940
   - Absolute acknowledgement number: 290218380

3. What ports are used for the TCP communication during the three-way handshaking? 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 exchanged during the three-way handshaking?
   - The client's MSS: 1460
   - The server's MSS: 1380

5. Answer the questions using the packets 13 and 17. In the DNS queries, identify the domain name to which the IP addresses should be resolved. Find the CNAME and A records from the DNS Answers. Find the IP addresses from the DNS Answers. To answer this question, you should understand CNAME and A records in DNS.
   A helpful site is: https://www.web24.com.au/tutorials/cname-records-used

   1) Domain name: pagead2.googlesyndication.com
   2) CNAME record (a): pagead2.google.com
   3) CNAME record (b): pagead.google.akadns.net

   4) A record (not a record): pagead.google.akadns.net
   5) The two IP addresses of the A record: 216.239.59.104 and 216.239.59.99

   Note: An A record is mapped to a IP address. A CNAME (Canonical Name, alias) points to another domain name rather than an IP address.