Lab#2

Exercise 1-1: (2 pts/each)

1. Download and install Wireshark https://www.wireshark.org/
2. Go to (Edit →) Preferences → Name Resolution → and Check the box "Resolve transport names" and "Resolve network (IP) addresses"
3. Open your browser and clear the cache (Chrome: Settings → Privacy and security → Clear browsing data) (Firefox: Preferences/Options → See the upper-right corner for "Find in Preferences/Options" → Enter "clear data" → Click the "Clear Data" button)
4. Select Capture → Options → your network interface (most likely Wi-Fi) → Start
5. Use the browser (the one the cache was cleared in the previous step) and connect to http://www.bradley.edu/
6. After you see the Bradley University homepage, wait for a few seconds, and then select Capture → Stop
7. Select File → Save → enter file name "bradley_capture" (leave the suffix as .pcapng)
8. Now go to the main interface of the Wireshark and apply a display filter by entering "http" in the filter
9. Locate the HTTP request with payload "GET / HTTP/1.1" and your device's host name/IP address as the Source

   Question 1: What is the IP address of www.bradley.edu?

   Question 2: Do you see www.bradley.edu in the captured data frame? If not, what do you see?

   Question 3: What is the size of this data frame?

   Question 4: In the same data frame, how many bytes are transmitted in the application layer (HTTP)?

Exercise 1-2: (2 pts/each)

1. Repeat the above steps 3 and 4 in Exercise 1-1
2. Connect to `http://daemon.bradley.edu/`
3. After you see the page, wait a few seconds, and then select Capture → Stop

4. Select File → Save → enter file name "daemon_capture" (leave the suffix as .pcapng)
5. **NOTE:** do not close the page yet. You'll use the same page again in the next exercise
6. Apply the "http" filter.
7. Locate the data frame with Destination "daemon.bradley.edu" and the Info "GET / HTTP/1.1". Use mouse's right-click on this data frame and select "Follow" → "HTTP Stream".

   Question 5: How many "GET"' requests are there to fetch the whole content (including text, images, etc) in this page?

   Question 6: What does it mean when receiving "HTTP/1.1 200 OK"?

1-3: (2 pts/each)

1. This time, **DO NOT** repeat step 3 in Exercise 1-1. Only do step 4 in 1-1
2. **Reload** the webpage in Exercise 1-2
3. Once you see the page, wait a few seconds, and select Capture → Stop
4. Select File → Save → enter file name "daemon_no_mod" (leave the suffix as .pcapng)
5. Now look for the "GET" requests again

   Question 7: How many "GET" requests are required to fetch the content in this page?

   Question 8: What can you observe (in terms of differences) from the exercises 1-2 and 1-3?

Upload your answers for the above questions and also the three capture files.
2 pts/each for the capture files.