Lab Assignment 1 for ECE671
Posted: 01/22/19
Due: 01/31/19

Step 1:

Download and install Wireshark on your laptop/desktop from here: http://www.wireshark.org/

Step 2:

Read the following page to make sure you have capture privileges: http://wiki.wireshark.org/CaptureSetup/CapturePrivileges

Run Wireshark

Tip for MacOS: Run following instruction in Terminal.
sudo /Applications/Wireshark.app/Contents/MacOS/Wireshark
Step 3:

Go to menu “Capture” -> “Options”, or click the little black gear icon (the fourth one from left) on toolbar.

Select the interface you are using to connect to the Internet. (In the example above it, it would be “Wi-Fi:en0”)

Hit “Start” to start capturing traffic.

Step 4:

While continuing to capture traffic start your browser and direct it to http://www.mmsys2019.org/ (128.119.44.21)

Step 5:

Stop capturing by clicking the red square in toolbar.
Step 6:

Filter the packets that belong to the http session between your host and the UMass web server.

Enter `http && ip.addr==128.119.44.21` in the “Filter” field of Wireshark as shown below. This IP address can be found using `ping [domain name]` in your Terminal or CMD, if you are interested in trying some other website.

Step 7:

Take a screenshot of this result. How many packets were transmitted from the UMass web server to your client in this session?
Step 8:

Please try to capture the packets while visiting the website using “Incognito/Private” mode of your browser. What is the difference compared to previous result? What do you think is the possible reason for this?