CSCE 416 Assignment 3
Wireshark Two-Way Message Application

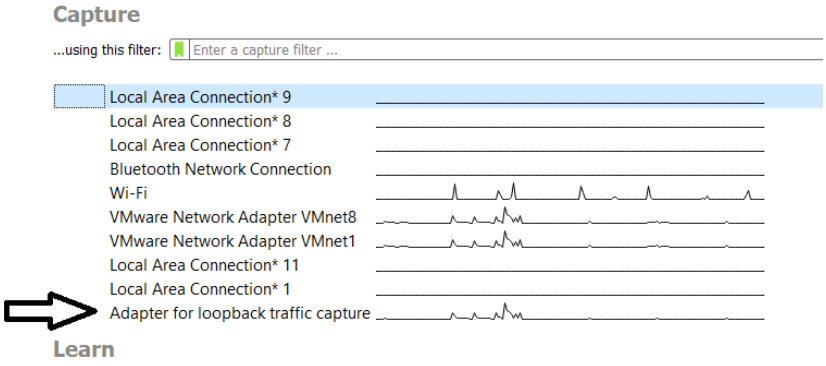
In this assignment we will use Wireshark to inspect the traffic passing between the TwoWayAsyncMesg Client and Server, the given sample code for Assignment 2. You will take various screenshots to demonstrate that you have done this. Wireshark is free to download: You can find Wireshark at (`https://www.wireshark.org/`), for Mac or Windows. For Linux please figure out how to do this for your exact distribution, which should be relatively straightforward. Once Wireshark has been installed, you can begin the assignment. When installing, please be careful to give it enough permissions to monitor traffic for your operating system

Your "deliverables", i.e. what you turn in, will be a sequence of screenshots that you take, a few question answers, and a Wireshark capture file. Please follow these instructions, in order, and submit either a .pdf, .doc, or .docx file. Treat the following section as a *template* for your submission; you can just copy-paste it and fill in the missing pieces.

1 Two-Way Message Application Packet Sniffing with WireShark

1.1 Getting Started

1. Load Wireshark, but do not start capturing packets. Select the "loopback" adapter. See image.



2. Open two command line windows to run the TwoWayAsyncMesg(Client/Server) applications, but do not start them.

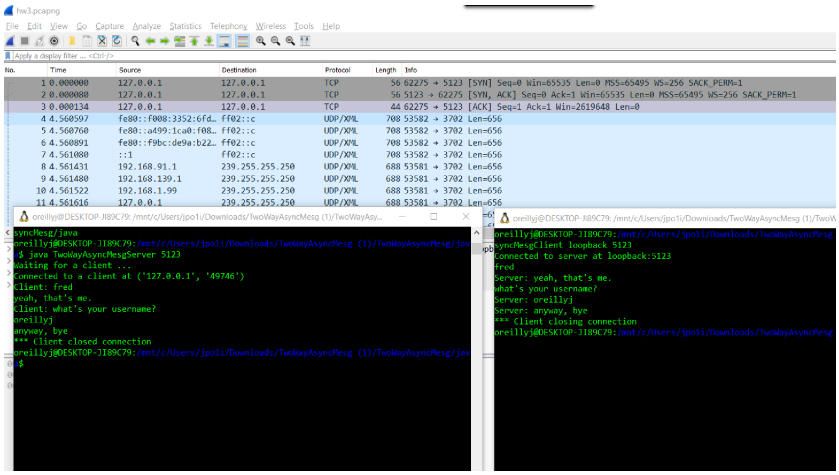
1.2 The Capture

1. Switching back to Wireshark, start capturing by selecting the shark fin in the upper left. You probably see a lot of traffic. We can deal with that later.

2. Start the server on a particular port (> 1024). For template, **Q1. Server was started on port** _____.

3. Connect the client to the server and send a few messages back and forth. *One of your messages should have your name.*

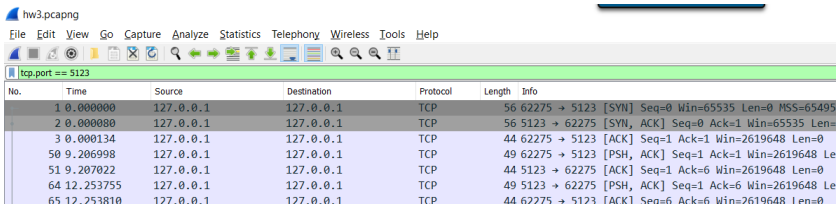
4. Take a whole screenshot of the setup, showing the two screens, the communication, and Wireshark in the background and label in your submission it as **Screenshot 1**, e.g.



5. Switch to Wireshark and Stop capture by pressing the red stop square.

6. Now, to find our packets it may desirable to apply a filter at the top in the filter text box, directly under the capture/stop buttons, type **tcp.port == <what you recorded above>**

7. Find towards the beginning of the packets, and screenshot, the *Three-Way handshake* in Wireshark and record as **Screenshot 2**. You should be looking in the list with the list of packets at the top.



8. Find the TwoWayAsyncMesg**Client**'s source port from the capture. Record this as **Q2. Client's TCP Source port** _____

9. Now, go through the packets and find the one where you send your name. You can Double-click to expand a particular packet and find the payload of the TCP packet. Showing the region having your name, take a screenshot and record as **Screenshot 3**

10. Save your PCAP file (File->Save As) somewhere. You can reload the PCAP file if you want to later.

11. You can explore individual packets. Looking under TCP, you can find a relative and a raw Sequence number. Research why the Sequence numbers don't start at 0, or any fixed number; this will require several sentences. Hint: Maybe make repeated connections with the application until you notice something in Wireshark. **Q3. TCP Sequence numbers don't always start at 0 because ...** Include a screenshot of this part of the Wireshark packet info (for an individual packet) (**Screenshot 4**).

12. Explore the TCP options for the one of the first two packets exchanged and open the TCP options. Take a screenshot containing the Windows Scale Factor, (**Screenshot 5**) and research why it is necessary for some applications. A short paragraph is sufficient, i.e. **Q4. The Window Scale Factor is for ....**.

1.3 Submission

Build a zip file containing

- One .pdf/.doc/.docx file with the three screenshots and the two questions answered.
- Your *filename*.pcapng capture file.

1.4 Grade Breakdown

- 10%: You submitted your assignment on-time and the files are of the right format.
- 8% each: Each of the requested five screenshots
- 5% each: Your answers to the first two questions.
- 15% each: Your answers to the last two, longer questions.
- 10%: your capture file.