Download wireshark from [http://www.wireshark.org](http://www.wireshark.org/). Select all installation options. (Note: These files are about 20 MB and may take a long time to download on a slow link.) You may also download the documentation.

**1. Upload the tcp-syn-attack.cap file and answer the following 10 questions (10 points each):**

1. **Is this a two-way conversation? Yes**
2. **Are there any ACK's? Yes**
3. **How long is the data portion of each packet? Why?**
4. **Why is the sequence number zero (seq=0) in every packet?**
5. **Why do the port numbers change in every packet?**
6. **Look at the "Time" column in the summary pane. Explain the various options it supports?**
7. **Click the "View" menu and select "Time Display Format". "Seconds since beginning of capture" is checked. Select "Seconds since Previous Captured Packet". How frequently are these packets being sent?**
8. **Where in the protocol tree pane would you find the protocol "Type" field?**
9. **Look in the flags section of the transport layer (Transmission Control Protocol" in the protocol tree section for one of the packets. What flags are set?**
10. **How does a SYN attack deny service?**

If you are getting stuck with the assignment, here are a few links that may be useful:

YouTube videos:

<https://www.youtube.com/watch?v=NHLTa29iovU>

<https://www.youtube.com/watch?v=nQyWWWDl_5c> (This is perhaps what is most relevant for Lab 2)