CMPSC 381
Data Communications and Networks
Spring 2016
Bob Roos
`http://cs.allegheny.edu/sites/rroos/cs381s2016`

Lab 6
3 March 2016
Due via Bitbucket on Thursday, 10 March, 8 a.m.
NOTE THE 8 a.m. DEADLINE!

Summary: Learn more about Wireshark; look more closely at TCP

Details: There are a number of features of Wireshark that make it easier to analyze network traffic; the first part of today's lab examines just a few of these. In the second part, we look at three components of TCP: sequence numbers, acknowledgements, and RTTs. You will capture some packets and answer questions about them.

1. **[Learning Features of Wireshark.]** When investigating TCP it is nice to be able to tailor the output on the capture screen to suit your needs.

   To get started, run Wireshark, capturing on the interface named "`p?p?`" (e.g., "`p4p1`") and using the filter "`tcp`". In Chrome (or another browser), visit the following websites:

   ```
   www.stanford.edu
   www.tsinghua.edu.cn
   www.ethz.ch
   ```

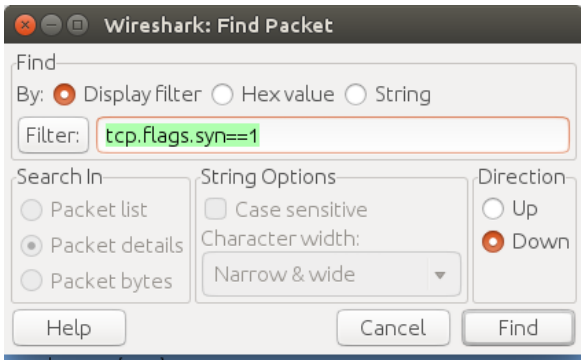
   Just wait long enough for the pages to finish loading—don't spend any time clicking on anything. When a page is finished loading, navigate to the next site in the list. When you have visited all three, stop the capture in Wireshark.

   [To hand in:] Save your capture file in your `lab6` directory as "*yourname*`-capture.pcapng`". It will probably be many thousands of lines long.

   (a) **[Eliminate unnecessary columns.]** We are really only interested in "No.", "Time", "Source", "Destination," "Protocol," "Length," and "Info." Use the "View/Displayed Columns" menu item to make sure only these columns are visible.

   (b) **[Set Name Resolution.]** We want the source and destination to be displayed as IP addresses (this may already be the default setting for you, so maybe you can skip this step). In the "View/Name Resolution" menu, make sure that "Enable for Network Layer" is UNCHECKED.

   (c) **[Find the first "`SYN`" packet.]** We can search for packets in several ways. If you click on the "magnifying glass" (same as CTRL-F or "Edit/Find Packet"), you can search on specific fields of the TCP segments. Do the following:



You should now be at the first packet containing a "`SYN`" flag. You can move forward or backward in the search using CTRL-N ("next") or CTRL-B ("back"); these are also accessible through the Edit menu.

(d) **[Filter out one "conversation".]** You probably have many segments containing "`SYN`." To limit the view to only the ones in a given connection session, right-click on a SYN segment and choose "Conversation Filter/TCP". Now only the packets related to this connection are visible. ("Follow TCP stream" appears to do the same thing, but it also pops up a window containing the stream contents.)

NOTE: to undo the effect of a filter, click the "Clear" button in the Filter bar just below the main menu bar.

(e) **[Change the Time Display.]** We are more interested in the times BETWEEN packets than the actual clock time. Go to the "View" menu and select "Time Display Format/Seconds Since Previous Displayed Packet."

(f) **[To hand in.]** Set up your window to show ONLY the packets for the *first* connection to Stanford University. (How do you know which ones are for Stanford? Can you use `dig` to figure it out?) The columns shown should be the ones listed above, and the Time column should be set to display as described above.

Use the SHIFT-PrtScn button to select the first dozen or so lines, including the top of the window containing the "Filter:" information and save this image in your `lab6` folder. It's okay if part of the "Info" field is cut off. Rename it "*yourname*-`stanford.png`".

(g) **[To hand in.]** Repeat the previous part, but for the *first* connection to Tsinghua University; name the screenshot "*yourname*-`tsinghua.png`".

2. **[Examining TCP.]** In your capture file from part 1, locate any of the TCP conversations with ETHZürich. Filter so that only these packets show and take a screen shot of the first dozen or so packets, starting with the initial `SYN` and including the "Filter:" line below the tool bar. Save it in your `lab6` folder as "*yourname*-`eth.png`".

(a) Open a text document and put your name and the honor code pledge at the top.

Starting with the first packet AFTER the three-way handshake in the conversation from the previous question, describe the next 8 packets in the conversation showing the direction of the packet, the sequence number of the packet, the acknowledgement number, and the length of the data in the packet. Example:

```
3582  localhost ---> ETH  seq = 1, ack = 1, len = 414
3777  ETH ---> localhost  seq = 1, ack = 415, len = 1448
       ... etc. (6 more) ...
```

Explain, using words and simple arithmetic, how the `seq`, `ack`, and `len` numbers are related in this collection of packets.

(b) Clear the filter, then filter the capture on all packets that contain a `SYN` (same syntax you used for the "Find" in part 1). Choose any three "handshakes," *one from each of the three websites you were asked to visit in part 1*, and for each one list the sequence numbers of the handshake, the source and destination hosts, and the "initial Round Trip Time," or "iRTT" (this is the elapsed time between sending the initial `SYN` segment and receipt of the matching `SYN/ACK` statement).

Which of the three sites had the shortest iRTT? Which had the longest? Do the numbers make sense?

[**Submit your work.**] Make sure you have the following in your `lab6` folder:

- your "`...-capture.pcapng`" file
- your "`...-stanford.png`" image
- your "`...-tsinghua.png`" image
- your "`...-eth.png`" image
- a PDF of your answers to the questions in part 2, with your name and the standard pledge line ("This work is mine unless otherwise cited").

Upload this folder to your Bitbucket repository by the lab deadline.

Make sure your name and the honor code pledge appear at the top of your answer document.