

**CMPSC 381**  
**Data Communications and Networks**  
**Spring 2016**  
**Bob Roos**

<http://cs.allegheeny.edu/sites/rroos/cs381s2016>

**Lab 1**

**28 January 2016**

**Due via Bitbucket on Thursday, 4 February, 8 a.m.**

**NOTE THE 8 a.m. DEADLINE!**

**Summary:** Today you will learn a little bit about Wireshark; you'll capture a few packets and do a little bit of analysis of their contents.

**Details:**

1. Create a Bitbucket repository named "*yourlastnamecs381s2016*" (e.g., if your last name is "Fenster" name it "**fenstercs381s2016**") and give me administrative access to it. Ask for help if you have forgotten how to do this (or if you have never done it!) Please use the name I requested—it will make it much easier for me to grade your labs!

Place the uploaded documents for each new lab in a separate folder; name these folders "**lab1**", "**lab2**", etc. Don't bother to create a separate "**labs**" folder.

2. Before beginning the Wireshark portion of the assignment, select another terminal in room 109 that will allow you to remotely log in. The terminals are numbered from **aldenv125** through **aldenv143**. Don't choose your own machine! To do this, type "**ssh aldenv...**" where "**...**" is replaced by the terminal number of the other machine. If you get a message that says "**WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED**", either follow the instructions for fixing the host key or else try a different terminal.

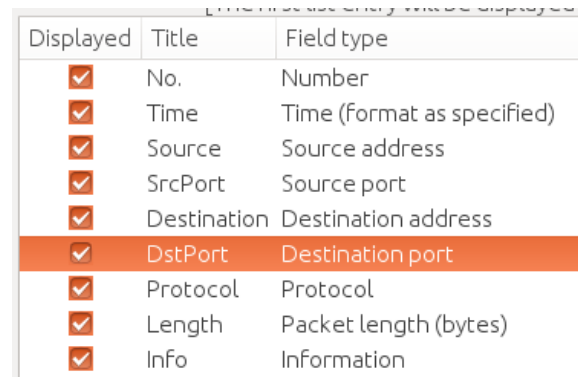
Once you have been able to successfully remotely log on to a different machine, log out from it ("**logout**"). (The next time you remotely log on to it you will be capturing packets.)

3. [**Wireshark Setup.**]

- In a terminal window, type "**wireshark &**" (the "&" isn't essential; it frees up the terminal for other commands). Choose "Edit/Preferences" from the menu and choose "User Interface/Columns" from the sidebar. By using the "Add" button and clicking/dragging in various places, set up the columns as shown in Figure ?? with the column names and order as shown. Make sure it looks like Figure ??, then click "Apply" and "Close". Ask if you can't figure out how to set up the columns.
- In the main Wireshark window, choose the interface that resembles "**p?p?**" (e.g., "**p3p1**", "**p4p1**"). Under "Capture Options", enter the following on the "Capture Filter" line:

(port 12345) or (port 22)

Then click the "Start" button.



The image shows the 'Column Setup' dialog box in Wireshark. It contains a table with three columns: 'Displayed', 'Title', and 'Field type'. Each row represents a column to be displayed in the packet list pane. The 'DstPort' row is highlighted in orange.

Displayed	Title	Field type
<input checked="" type="checkbox"/>	No.	Number
<input checked="" type="checkbox"/>	Time	Time (format as specified)
<input checked="" type="checkbox"/>	Source	Source address
<input checked="" type="checkbox"/>	SrcPort	Source port
<input checked="" type="checkbox"/>	Destination	Destination address
<input checked="" type="checkbox"/>	DstPort	Destination port
<input checked="" type="checkbox"/>	Protocol	Protocol
<input checked="" type="checkbox"/>	Length	Packet length (bytes)
<input checked="" type="checkbox"/>	Info	Information

Figure 1: Wireshark Column Setup

4. In a terminal window, `ssh` to another machine (the one you just successfully tested in part 2). You should see packets appearing in your Wireshark window.
5. On *your* machine (not the remote one), open a new terminal window and type:

```
nc -l 12345
```

On the *remote* machine, type:

```
nc localterminal 12345
```

where *localterminal* is the machine you're sitting at. Alternating between the two windows, type a short dialogue (no more than two or three lines in each window), then terminate the chat with CTRL-D or CTRL-C. Log out of the remote machine. Click the red "Stop capture" button in the Wireshark window, but leave Wireshark open.

6. **[Questions to be answered.]** Create a document using your favorite method (Open Office, L<sup>A</sup>T<sub>E</sub>X, plain text, ... whatever). Ultimately I will ask you to make it a PDF document. At the top, put your name and the Honor Code pledge as described on the syllabus. You'll be pasting information from your Wireshark capture into the document. Number the answers in your document: "6(a)", etc.
  - (a) The `ssh` command that you typed sets up a TCP connection between your local machine and the other machine you chose. This requires a "three-way handshake" as illustrated in Figure 3.39. Which packets in your capture correspond to this handshake? List their sequence numbers (first column) and paste in the text of the lines for those packets. (Right-click on the packet and select "Copy ► Summary (Text)".) See sample document on next page.
  - (b) A TCP connection is closed as shown in Figure 3.40. Which packets in your capture correspond to closing the TCP connection when you log out of your SSH session? List their sequence numbers and paste in the text of the lines for those packets.

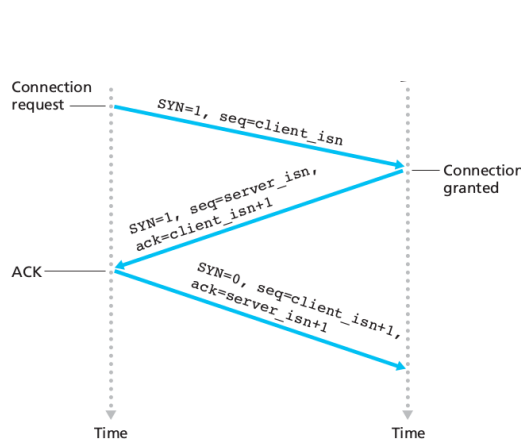


Figure 3.39 ♦ TCP three-way handshake: segment exchange

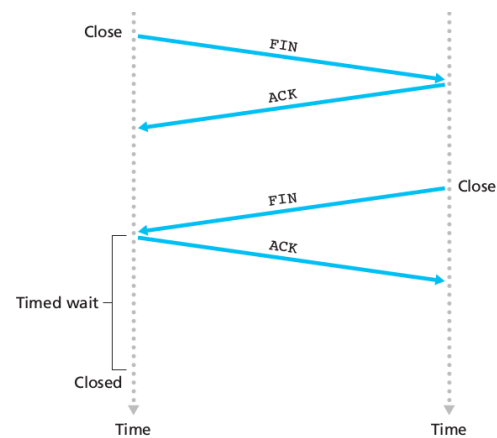


Figure 3.40 ♦ Closing a TCP connection

- (c) The `nc` commands set up a second TCP connection. As you did in part (a), list the packet numbers containing the three-way handshake for your chat and paste in the text summary of those packets. (HINT: look for a message from the remote host to your machine's "italk" port (this is a symbolic name for port 12345)).
- (d) When you terminated the `nc` connection, its TCP connection was closed. As you did in part (b), list the packet numbers and their text summaries for the connection closing.
- (e) The SSH protocol uses encryption. Was any of the data in your "chat" sent in plaintext (unencrypted) form? If so, find a packet containing some unencrypted data and paste in the summary text (as above) and also the unencrypted data (right-click on the packet and select "Copy ► Bytes ► Printable Text Only").

Just to be clear: your document is going to start out looking something like this (except I gave wrong answers!):

```
Bob Roos
Lab 1

This work is mine unless otherwise cited

6(a). TCP Connection for SSH session:

Packet numbers 13, 22, and 55: [NOTE: THESE ARE NOT THE CORRECT ANSWERS!]

13  0.020557000 141.195.226.111 42604 141.195.226.126  ssh  SSHv2114  Client:
Diffie-Hellman Key Exchange Init

22  0.087957000 141.195.226.111 42604 141.195.226.126  ssh  SSHv2438
Encrypted request packet len=372

55  28.928333000 141.195.226.111 42604 141.195.226.126  ssh  SSHv2102
Encrypted request packet len=36

6(b). TCP closing for SSH session:
|
Packet numbers 295, 297, and 315:

... etc. ...
```

7. [Convert your answer file to PDF.] If you created a plain text file, you can convert it to PDF using these commands (obviously using your own last name, not "fenster"):

```
enscript -p temp.ps fensterlab1.txt  
pstopdf temp.ps > fensterlab1.pdf
```

If you used LibreOffice, look for the “File/Export as PDF” menu item.

8. **[Save Your Capture File.]** In Wireshark, use the “File/Save as” menu to save your capture file in the `lab1` folder of your bitbucket repository. Name it “*yourlastnamelab1capture*”. (The default file extension is “`.pcapng`”.)
9. Make sure your answer file (PDF) and your capture file are in your `lab1` folder. Push these into your Bitbucket repository before the 8 a.m. deadline next Thursday. Double-check your repository online to make sure the files made it there!