ITP 125 - Lab 05

Deadline

1 minute before the next scheduled lecture.

Objective

Learn a bit about network sniffing and what protocols look on the lower level.

Setup

If you wish to run Wireshark at home, you can easily install it on Windows or OSX. Go to the following site and download Wireshark:

<http://www.wireshark.org/>

Windows:

In order to get Wireshark working on Windows, you will need to install WinPcap. In general, the Wireshark installation will help you install that. If for any reason that doesn’t happen, you can download WinPcap from the following site:

<http://www.winpcap.org/install/default.htm>

OSX:

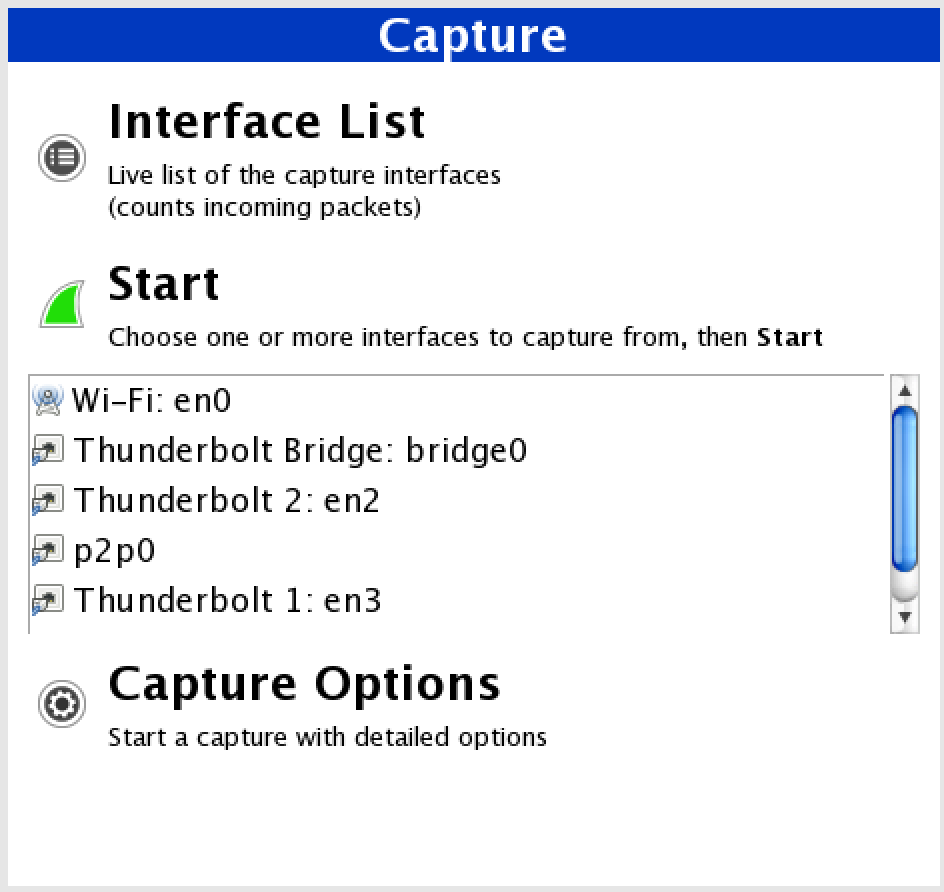
In order to get Wireshark to work on OSX, you will need to install XQuartz:

<http://xquartz.macosforge.org/landing/>

There maybe a chance you will need to install Xcode as well (unlikely), but if you do you can get it from the following:

Procedure

1. Open a command prompt in Windows by doing the following:  
     
   Press key 🡪 “Search Programs and files” 🡪 type in: cmd.exe
2. When a command prompts opens type the following command:  
     
   > ping www.usc.edu  
     
   **Note the IP address that you see.** You will be using it later
3. Start up Wireshark. Under the section titled ‘Capture’ select the network card that you with to listen to. Once you have that selected, click ‘Start’



1. Let Wireshark run, and open up a web browser. Goto [www.usc.edu](http://www.usc.edu).
2. Go back into Wireshark and notice all the traffic that it is capturing. There is too much to look through so we need to filter out the results. In order to do that click in the ‘Filter’ box and type in the following ‘dns’:



This will only show traffic involving DNS (i.e. converting an IP address to domain name)

1. In order to see the TCP three-way handshake you need to add some custom filters.

SYN:

tcp[13]==02

SYN/ACK:

tcp[13]==12

ACK:

tcp.seq == 1 && tcp.ack == 1 && tcp.len == 0 && !(tcp.flags.push == 1)

Try it out and see if you notice the three-way handshake when you talked with the USC servers.

1. Now if you wish to view the web content that was running over the network, type in the filter box ‘http’

You will see all the web traffic that was sent, but it isn’t very human readable. So in order to fix that click on File 🡪 Export Objects 🡪 HTTP

1. If you wish to filter out traffic by a particular IP address type in the following in the filter box:  
     
   ip.addr == **<USC IP address from the >**  
   Replace <USC IP address from the ping> with the results you found from step 1.

Questions

1. You will notice that if you’re doing this lab on a LAN (not a wireless LAN), that you cannot see the traffic of other people. Wireshark only picks up the traffic from your own machine. Look at the two following network devices:

<http://en.wikipedia.org/wiki/Ethernet_hub>

<http://en.wikipedia.org/wiki/Ethernet_switch>

<http://lmgtfy.com/?q=hub+vs+switch>

What is the difference between the two network devices? If you cannot see the traffic of other people on the LAN, which network device do you think the room is using?

**A hub is just a connection device that connects multiple devices together into one connection. A switch is a device that forwards incoming packets to the correct device. The room is most likely using a switch.**

1. If you can, try out Wireshark on a wireless network. Are you able to see the traffic of others?

**No, you can still only see your own packets.**

1. What is VoIP? How is it helpful? Any security concerns with it from your research? Can you find any attacks against VoIP? Does USC use it?

**VoIP is Voice over IP, essentially Skype. If you can intercept the set-up of a VoIP session, you can effectively join in as a member of the conversation without others knowing.**

Submission

Answer the questions above and name the file **lab04.docx,** then encrypt the file using **7zip or Keka**, and. Upload the file to your **itp125 folder** on the web hosting.

Set the password to the all the files to be: **noticemesenpai**

Make sure you can see the file by publicly accessing the URL using any web browser of your choosing.