Indian Institute of Technology Bombay

Department of Electrical Engineering

Handout 21 EE 706 Communication Networks

Assignment 5 : **0 points** (Optional) March 23, 2010

This is an optional assignment which does not need to be turned in.

- Wireshark is a free software which captures network traffic and displays it in human readable form. The objective of this assignment is to learn how to use Wireshark to observe the behavior of real-world protocols.
- **Wireshark installation:**
  - Follow the instructions at `http://www.wireshark.org` for installation on Microsoft Windows.
  - For installing on Linux, type "`sudo apt-get install wireshark`" on Ubuntu and "`sudo yum install wireshark`" on Fedora. Alternatively, you can install the `wireshark` and `wireshark-common` packages using Synaptic Package Manager. Note that you need administrator priviledges to do this.
- **Running Wireshark**
  - On Windows, find the Wireshark application in the Start Menu and run as administrator.
  - On Linux, type "`sudo wireshark`" in a terminal window.
- **Using Wireshark**
  - To capture the packets heard by your network card, select `Interfaces` in the `Capture` menu of Wireshark. Select the network card which is connected to the LAN from the list of interfaces. On Linux it will be `eth0` if you are connected to Ethernet LAN and `wlan0` if you are connected to wireless LAN. On Windows, you will need to find which interface is connected to the LAN using the Network and Sharing Center dialog.
  - Click `Start` from the `Capture` menu to start seeing the packets heard by your network card. The top part of the Wireshark window shows list of captured packets. The middle part of the window shows the packet details of selected packet. The bottom part shows bytes of selected packet. You can select any packet in the top window by clicking on it.
  - To stop the capturing process click `Stop` in the `Capture` menu.
  - Look at the different sources, destinations, protocol types and information in the packets captured.
  - Find the IP address of the interface you have chosen to perform network capture from the `Interfaces` dialog in the `Capture` menu. Select a packet whose source is that IP address. Find the MAC address of the interface by looking at the packet contents. You may have to start a browser to initiate some traffic. Cross check this MAC address by obtaining the MAC address through `ifconfig` in Linux and the Network and Sharing Center in Windows.

- Find out the manufacturer of your network interface by checking the box under `Edit`→`Preferences`→`Name Resolution`→`Enable MAC Name Resolution`. This will cause the first 24 bits of the MAC address to be decoded as a string which has the manufacturer's name.
- To display traffic belonging to a particular protocol (for example, TCP) enter that protocol name in the `Filter` text field and click on `Apply` button. To display traffic belonging to all protocols click on `Clear` button.
- Ping any other machine on the LAN like 10.107.1.1 using "`ping -c 5 10.107.1.1`". Start the capture before pinging and stop it after ping completes. Enter the string `ICMP` in the `Filter` text field to isolate the ping packets (ping uses the Internet Control Message Protocol (ICMP)). By looking at the source MAC address in the ping reply packets, find out the manufacturer of the other machine's network card.
- Disconnect the LAN cable from your computer and start a Wireshark capture. Reconnect the cable and see what are the protocols used by your computer to reconnect to the network.