CS3210: Computer Networks Lab
Final Exam, 24th April 2014
Part 2 (2 Hours)

For this part of the exam, the duration is 2 hours.

In the answer sheet, the answers must be STRICTLY in the order of the questions. Mark Q1, Q2 etc. clearly, and answer the subsections also STRICTLY in the order given below.

Question A: Network Commands

Perform the tasks in the order. Do task X before moving to task X+1.

1. Write down the ifconfig command to set your machine's IP address to 10.6.16.x (where x is your roll number if you are from the 2011 batch. If you are not from the batch, ask us for a unique number).
2. There is a gateway which can carry the network traffic to outside the department. Its IP address is 10.6.16.254. Write the route command(s) to set your routing so that all traffic to machines outside the department goes through this gateway.
3. Our department has a DNS server numbered 10.6.0.11. Write a command to see if you can reach the DNS server.
4. You want all the DNS requests to be resolved by 10.6.0.11. How will you set up your DNS configuration? Which file(s) will you have to modify and what entries will you make in those files?
5. Write the command to find out the IP address of ftp.iitm.ac.in
6. Write the command to find the number of hops between your host and ftp.iitm.ac.in
7. Assume that your machine is running a Ubuntu-like OS. What are the steps that you take for installing a new package on your machine? Specify all the relevant details, including which version of Ubuntu, which host you get the updates from, which files you modify etc. Do not worry about dependencies.
8. Write a command to install a package called libssl-dev from the Ubuntu repository of the institute.

Question B: Socket Program

In this problem, you are expected to use both UDP and TCPs. Write a program to do the following:

1. Make a UDP connection to 10.6.11.28 on port 1500 and send your roll number (as cs1xbxxx – watch out, all lower case).
2. You will get a response from the server with a port number (above 7500 but less than 8900).
3. Open a TCP connection to the same server (10.6.11.28) on the port

number you received. On that connection, send your roll number once more.

4. You will get a string which is of utmost 100 characters.

You should write a single program to achieve this. No scripting, no system calls to call two different programs, just one .c program.

Create a text file <rollnumber_prob2.txt> with the following,in the order specified:

<roll number>
<port number you got back>
<your IP address>
<unique string that you got from the TCP server>

Question C: Sleuthing

In this question, you are expected to analyze a pcap file (made available on moodle). Use wireshark (and any other program that you write or a package that you think is useful) for this problem.

Prof. Schizo Phrenic suspects that one of the students, Tweety Bird, is upset about the networks lab question paper. Tweety wants to take revenge and has access to something that can wreck Prof. Phrenic's car: the secret recipe. The TAs are worried that Tweety may try to pass on the recipe.

The TAs have been monitoring Tweety's activity for some time, but haven't found anything suspicious– until now. Today an unexpected laptop briefly appeared on the network. The TAs hypothesize it may have been someone in the DCF, because no strangers were seen in the lab. Tweety's computer, (**192.168.1.158**) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

"We have a packet capture of the activity," said the TAs, "but we can't figure out what's going on. Can you help?"

You are the forensic investigator. Your mission is to figure out who Tweety was IM-ing, what she sent, and recover evidence including:

1. How many packets were captured?

2. How many of the packets were TCP packets?
3. What is the IP address of Tweety's buddy?
4. What is the screen name of Tweety?
5. What is the screen name of Tweety's IM buddy?
6. What was the first comment in the captured IM conversation?
7. What is the name of the file Tweety transferred?
8. What is the secret recipe?

Write the questions, along with your answers in a single text file <rollnumber_prob3.txt>. In the same file, also write briefly what was your strategy to get the answer.

Deliverable:

You should upload a single tarball with
1. One C file with the program for problem 2
2. <rollnumber_prob2.txt>
3. <rollnumber_prob3.txt>