CMPSC 381
Data Communications and Networks
Fall 2012
Bob Roos

Lab 2
6 September 2012
Due Thursday, 13 September, 1:30 pm,
in your Sakai dropbox

Part 1: Wireshark

Do the first Wireshark lab as described in the handout "WiresharkIntrov6.0.pdf" (should be right next to this document in the "Announcements" section of the Sakai page). Note the following modifications and additions:

- Since Wireshark is already installed, you can skip the section entitled "Getting Wireshark"
- In item number 4 of the section "Taking Wireshark for a Test Run," use the "`eth0`" interface (there is no "Gigabit network Connection" interface listed).
- The biggest changes are in the "What to hand in" section—see below.

Create a document with answers to the following questions:

1. In the HTTP packet containing the "GET" message (see item 9 in the "test run" section), what was the full text of the GET command that was sent to the `gaia.cs.umass.edu` site?
2. Where in the packet description (i.e., what section of the header window in Wireshark, e.g., "Frame," "Ethernet," etc.) is there a mention of "port 80"?
3. What port was used to send the "GET" command (and where is this information located in the header?) From what IP address was the "GET" command sent and what section of the header contains it?
4. What is the IP address of the "`gaia.cs.umass.edu`" site and where is this information shown in the header?
5. In a terminal window, type the command:

   ```
   telnet gaia.cs.umass.edu 80
   ```

   and enter the GET command from question 1 with the following changes:

   - Delete the characters "`\r\n`" from the end of the command
   - Change the "`HTTP/1.1`" to "`HTTP/1.0`"

Hit enter twice. You should see the HTML for the "Congratulations!" message that you got when you visited the site in your brower. If you don't, make sure you followed the instructions above correctly; see me if problems persist.)

Copy the full session (`telnet` command and output all the way through "`Connection closed by foreign host`" from your terminal window into your answers document.

6. Using the "search" feature in Wireshark (either the "Edit/Find packet" menu item or the "magnifying glass" icon in the toolbar), find the packet containing the word "Congratulations!". You'll need to do a "String" search in the "Packet bytes".

   From the packet content window at the very bottom, locate the hexadecimal codes for the letters "`Congr`" and enter them as your answer to this question.

7. How big, in bytes, is the frame you just looked at (the one that has the word "Congratulations")?

8. Go to the "View/Time Display Format" menu item (you have to move your mouse cursor into the Ubuntu toolbar at the top of the screen to make the menus visible) and select "Date and Time of Day" as the format.

   How much time, in seconds, elapsed between sending the "GET" message and receiving the matching "OK" message?

9. Change the "http" filter to "dns". Find DNS packets containing the name "gaia.cs.umass.edu" and copy the portion of the "Answer" field that identifies the IP address and paste it into your answers document. (Right-click on the line containing this information and then choose Copy/Value.)

10. Clear the "http" filter so that all packets are shown. Sort them by packet number and then tell me how many packets there are in your capture and how much time elapsed between the first one and the last one. How many of these were

Congratulations! You are done with Wireshark for this lab.

Problem Set

I did not remember to tell you to bring your books to lab, so if you can't work on these today try them before Tuesday's class. I will work some examples on Tuesday as well, but you should be able to do these just based on reading the book.

> **For this very first, short, problem set I'm requesting that you not collaborate with others in the class. I would like to see how you do on your own. On future problem sets I may let you work with a fellow student. I promise to be very gentle when grading them (and, of course, you can come and talk to me about them . . . but please don't share the answers with others in the class). Again, this is just for this first little problem set so I can begin to assess your skills.**

11. Problem P2, page 71.

12. Problem P6, page 72. Note that questions of the form “where is the first bit?” should be answered relative to the parts of the network, e.g., “the bit is just arriving at host B” or “the bit is somewhere on the link between A and B” or “the bit hasn’t yet left host A” or . . . .

Upload your answers to your Drop box on Sakai. Be sure your name appears *in the document* so that when I print it out I’ll know who owns that document!