COMPSCI 314 S2C Assignment 2
2011

Department of Computer Science
The University of Auckland

*Carefully review the tutorial document before starting the assignment. This assignment contributes **5%** of your overall course mark. Submit your assignment **as a single PDF file** to **Assignment Drop Box**. Include all **workings** and **explanations**. Marks will be deducted for ambiguous solutions. Zero marks are awarded if the answers contain no explanation. Also, refer to the Departmental policy on cheating and plagiarism. Cut-and-paste without acknowledgment of the source is not acceptable.*

Assignment Drop Box *(https://adb.ec.auckland.ac.nz/adb/).*
Departmental Policy on Cheating on Assignments: *see Assignments page of the course web site.*

Important notes:

If you choose to install Windump and Wireshark on your own computer and carry out the assignment at home, the results may be different from doing it in the Computer Science labs. The sample answers and the marking will be based on results in the labs.

For each question, you must also attach the first page of your actual capture file(s), as proof that you did the work, e.g., screen-shots. You can use File/Export/File in Wireshark to save a text file.

[Total: 50 marks]
[5 marks for each sub-question]

Q1. Packet capturing [20 marks]

Start up Wireshark and choose the Ethernet interface. For this run, make sure to set the maximum packet limit in Capture Options large enough for a complete Ethernet packet.

a) Start capturing packets and let it run for a few minutes. Then stop the capture. What kind of protocols do you see? List and explain at least three of them.
(Hint: See list of protocol abbreviations in Wireshark Help/Supported Protocols)

b) How many packets per second did you observe? Explain how you worked this out and show your calculations.

c) Save the capture file on disk. How big is it? (In Windows properties, that's "Size", not "Size on disk.") Calculate the average data rate in bits/s on the network during the capture. Show your calculations. For each record in the file, the *pcap* format includes 16 bytes of extra information [timestamp and size] as well as the original packet data. After you have done this, look in the Wireshark Statistics/General option to check your answer (there may be a small difference).

d) Now run a capture using Windump for about the same length of time, writing a *pcap* file as explained in the tutorial. Then open up the file with Wireshark. Do you see any differences compared to the previous trace? Are the packets per second and the average data rate about the same as before? (This time, you can just use the Wireshark Statistics/General option to save time.)

Q2. IP packet size distributions [10 marks]

Use a web browser to visit a few HTTP web pages at www.cs.auckland.ac.nz and then a few pages at www.auckland.ac.nz. With Wireshark, capture the full packets that are travelling between you and the web page. (Hint: set an *ether host* capture filter for your own Ethernet address, to avoid being distracted by other traffic.) You only need to visit each page once. Make sure to avoid HTTP status code *304*; this is most likely to happen if you are refreshing the web page. Now look at the size of the packets as indicated by Wireshark.

a) Are there any packet sizes that you observe multiple times? Which ones?

b) Explain why these different sizes exist. Is there any special difference between the two web sites?

Q3. Connections [20 marks]

Make a packet trace like Q1a, but let it run quite a long time, while you are doing other work on the computer, including web browsing, sending and receiving mail, etc. Make sure you set Wireshark to use a large buffer, e.g. 25 MB. You can save the capture file after you stop capturing, and analyse it at any time with Wireshark. Please delete the large capture file when you've submitted the assignment. (Hint: If you are running on a small network at home, you might get more interesting results by starting an application like telephony, radio, streaming or even gaming.)

a) What percentage of the IP packets are UDP and what percentage are TCP? Explain how you worked this out and show your calculations. Your answer does not need to be exact; an approximate answer is OK.

b) Identify at least 3 protocols that run over UDP? What port numbers do they use?

c) Identify at least 3 protocols that run over TCP? What port numbers do they use?

d) Explain in your own words how you can see example of flow control at work in the Wireshark display of your trace file. Which Wireshark feature makes it easy to do this? Include a few actual extracts from the trace to illustrate your answer.