COMPSCI 314 S1T Assignment 1
2008

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 in* ***PDF*** *format 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 on Assignments.*

Assignment Drop Box *(https://adb.ec.auckland.ac.nz/adb/).*
Departmental Policy on Cheating on Assignments *(http://www.cs.auckland.ac.nz/CheatingPolicy.php)*

Important: For the questions **Q1(d), Q2, Q3 and Q4(b)**, you must also attach one or two pages of your actual capture files for each question, as proof that you did the work, e.g., output screen-shots. You can use File/Export/File in Wireshark to save a text file.

[Total: 50 marks]

Q1. Packet capturing [10 marks]

Go to Capture Options in Wireshark, and check '*Limit each packet to…*'.

a) What is the smallest and largest size limit you can set?

b) Explain why Wireshark imposes a lower and higher limit.

c) Explain one advantage and one disadvantage of setting a small size limit

d) Start capturing packets and stay *idle* 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)

Q2. IP packet size distributions [10 marks]

Use a web browser to visit a few HTTP web pages, e.g., www.cs.auckland.ac.nz. Capture the full packets that are travelling between you and the web page. You only need to visit once to capture all the packets. Make sure to avoid HTTP status code *304*; this is most likely to happen if you are refreshing the web page.

a) List at least two frequently observed packet sizes, e.g. a small size and a large size.

b) Explain why these two different sizes exist. What is the difference in contents of the two sizes of packet?

Q3. Packet trace file [20 marks]

Use a web browser to download two files **`BigFile1`** and **`BigFile2`** from the 314 webpage *Assignments* section. Make sure to capture only packets belonging to the file download (i.e. set a host IP filter). Save the packets separately into a capture file for each download.
(Hints: See Packet Length in Wireshark Statistics Menu. Make sure you set Wireshark to use a large buffer, e.g. 25 MB. Please delete the large files when you've submitted the assignment. These files are probably too large to test from home.)

a) Assuming the two files are the *user-data*, and observing from the frame level, list and explain the overheads (extra bytes per **user datagram**) involved in layer 2, layer 3 and layer 4 (Ethernet, IP and TCP).

b) Based on your answer (a) and the packet sizes seen by Wireshark, calculate the efficiency *ratio* of your user-data to total data transmitted in both directions. In other words, approximately what percentage of the total transmission should be user-data?

c) Based on your answer (b), comment on the overhead effects for transmitting small versus large packet size. Which is more efficient?

d) Comment on the size of the actual downloaded files (BigFile1 and BigFile2) compared with the total sizes indicated by your capture files. Why are they different?

Q4. Transport layer [10 marks]

TCP and UDP are the most widely used protocols in the transport layer. However, they are very different. For example, TCP provides end-to-end reliable transmission, while UDP does not. Often, TCP carries HTTP traffic and together they often contribute more than 90% of total volume in our network.

a) Assuming that all of your HTTP traffic is carried by TCP; would you be able to visit web pages such as www.google.com if a network administrator blocks all UDP traffic? Justify your answer.

b) Often we use the term *TCP stream*, or simply a *connection* to represent data transmission between two end points. Technically, there can be many connections at the same time. List the fields/attributes used to identify a *single* stream. In other words, what makes a series of packet transmissions belong to the same connection?
(Hint: Use your web browser as in Q2. In the Wireshark capture window, right-click on a packet and use the 'Follow TCP stream' option.)