COMPSCI 314 S2T Assignment 1
2009

Department of Computer Science
The University of Auckland

*This assignment contributes to **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 **Q2, Q3 and Q4**, 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]

Notes: This assignment is intended to help you understand the way that packets flow across a network, and how various protocols fit on top of one another. *Carefully review the tutorial document before starting the assignment*. It is recommended that you perform the work in one of the Computer Science labs. Some people may prefer to install Wireshark on their own computer and work at home, but the results could be less interesting.

Q1. Packet capturing [10 marks]

a) Go to Capture Options in Wireshark and find '*Name Resolution*' (bottom right). Briefly describe and explain the following options:
- *Enable MAC name resolution*
- *Enable network name resolution*
- *Enable transport name resolution*

b) Explain why a filter is useful.

c) What filter string would you use to filter out packets of 'UDP, and TCP port 80, and at least 1200 bytes of TCP segment size, and IP address 2001:4860:b005::68' ? (hint: look at 'Expression' button)

d) Will your filter display some packets?
If yes, what packet type is displayed? If no, give a better filter example.

Q2. IP packet observation [10 marks]

Use a web browser to visit at least two HTTP web servers, e.g. www.cs.auckland.ac.nz and www.google.com. 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. Also, it is best to clear the browser cache before starting.

a) You should observe some DNS packets. Which field in each IP/UDP packet for DNS identifies the corresponding request/response?

b) Did the system use IPv4, IPv6, or a mixture? Can you explain why? (If you want to test for IPv6 access, try http://ipv6.google.com)
Also, list at least two frequently observed packet sizes, e.g. a small size and a large size. Explain why these two different sizes exist, e.g. what is the difference in contents of the two sizes?

c) Explore the details of the first HTTP request packet. What 'TCP option' have you observed? What TCP segment length is used by your computer and the web server?

d) Which TCP flag field is mostly set to 'true' (value 1)?

Q3. ICMP packet observation [10 marks]

Start Wireshark capturing and send ICMP messages through the Windows command prompt. Type: ping www.cs.auckland.ac.nz -4 -l 1000

a) Which field in the ICMP packet identifies the corresponding request/reply? How does ping know to match the corresponding packets?

b) What is the size of ICMP packet (ICMP header and payload)? What value is the first byte of the payload?

c) What is the length limit (-l option) before the packet is fragmented in the network? Try higher and lower values until you find it. How did Wireshark find whether the packet was fragmented?

d) Try sending fragmented ICMP packets to different servers (such as www.auckland.ac.nz, www.google.com). Describe and explain your observation.

Q4. Packet trace file [20 marks]

Use a web browser to download a file '**BigFile3**' from the 314 webpage *Assignment* section, while capturing with Wireshark. Make sure to capture only packets belonging to the file download (i.e. set a filter). You should right-click on one of the packets and use the 'Follow TCP stream' to ensure you are only observing the downloaded file. Save the captured packets to a trace file (e.g. name it '**BigFile3-down**').

a) Calculate the performance in megabytes per second (MB/s) (use the Wireshark Summary menu)

b) Consider '**BigFile3**' to be the *user-data.* Observing from the frame level with Wireshark, each datagram contains four parts: three kinds of overhead (extra bytes) per datagram and a section of user-data. List and explain the overheads for each protocol layer (Ethernet, IP and TCP). How does their position in the datagram correspond to the numbered protocol layers mentioned in the course Introduction?

c) Calculate the efficiency *ratio* of your *user-data* to data transmitted by the hardware. In other words, approximately what percentage of the total transmission is *user-data*? Use the following formula: efficiency-ratio = file-size / captured-frames

d) Can we improve the efficiency-ratio if the *user-data* segment size is changed to smaller, or larger? Explain with some examples.

Use Wireshark to open the file '**BigFile3**' itself. Compare with the capture file '**BigFile3-down**'.

e) Both transactions used TCP, however they are quite different. Can you identify some of the differences? Use the Statistics menu (e.g. Summary, Packet length, Port type, etc) to support your answer. What kind of traffic do you think was carried in '**BigFile3**'?
