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. [Sample answer does not include this.]

[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)

[*Note to markers: There is no single correct answer.* Examples:
ARP - Address resolution protocol, how IPv4 hosts find the MAC address of other IPv4 hosts.
NBNS - NetBIOS Name Service, how Microsoft networking looks up names of other hosts. NetBIOS is Microsoft's Network Basic Input/Output System.
ICMPv6 - the IPv6 version of ICMP, Internet Control Message Protocol, used for messages managing the IPv6 protocol itself.]

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

[There are 381 packets in the trace and the end timestamp is 39.23s. Therefore there were 381/39.23 = 9.71 packets per second.]

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).

[File size is 47658 bytes. The pcap overhead for 381 packets is 381*16 = 6096 bytes, so the real data size is 47658-6096 = 41562 bytes. So the data rate is 41562/39.23 = 1059.4 bytes/s = 8475.5 bits/s = 0.008 Mbits/s. Wireshark calculates almost the same values, 9.713 packets/s and 1058.9 bytes/s.]

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.)

[The trace is pretty similar, just a different set of packets. Packets per second is 8.675 and data rate is 1151.7 bytes/s or 0.009 Mb/s.]

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?

[On CS site, 74 and 1514 are frequent, on Uni site, 54 and 1514 are frequent.]

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

[The short ones are TCP ACKs in IPv6 and IPv4 respectively. The long ones are

maximum MTUs on Ethernet. IPv6 payload is 1440 and IPv4 payload is 1460. The CS site supports IPv6 and the Uni doesn't.]

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.

[After stopping the capture, apply the filter expression 'udp' and use the Statistics/Protocol Hierarchy option. Then clear the filter and repeat for 'tcp'.
We see 1947 UDP packets and 4964 TCP packets and the total is 8938 packets. Therefore we have 1947/8938 = 21.8% UDP and 4964/8938 = 55.5% UDP. *Alternatively take the UDP and TCP percentage values for IPv4 and IPv6 in the Protocol Hierarchy option and add them.*]

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

[At Uni we can see, for example: DNS/UDP port 53, NBNS/UDP port 137, BROWSER/UDP port 137. At home we could see, for example, Skype over UDP (and TCP), unregistered ports, RealAudio over RDT/UDP, unregistered ports. *Note to markers: any 3 correctly described examples will do.*]

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

[At Uni, for example: HTTP/TCP port 80, HTTPS/TCP port 443, SMB/TCP port 445, LANMAN/TCP port 139. At home we could see, for example, Skype over TCP (and UDP), unregistered ports. *Note to markers: any 3 correctly described examples will do.*]

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.

[You right-click on a packet and use the 'Follow TCP stream' option. When you look at a TCP stream, you can see the sequence numbers and data going one way, and the sequence numbers and ACKs going the other way.]