COMPSCI 314 S2C Assignment 1

Department of Computer Science
The University of Auckland

Due: 11:59 p.m., Friday, 20 August, 2010
(NO LATE SUBMISSIONS)

Carefully review the tutorial document before starting the assignment. 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****.* You must also carry out experiments using *windump*/*Wireshark* and include your results, e.g., output screen-shots. *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.*

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 may be different and we cannot help if you have problems.

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

[Total: 50 marks]

Q1. Packet capturing **[10 marks]**
[3, 2, 2, 3]

a) Go to **Capture Options** in Wireshark and briefly explain ***Capture Packets in promiscuous mode*** option. Why aren't you able to capture packets which are destined to other computers in the lab even if you enable this option?
Promiscuous mode is a working mode for network device. In this mode, network device captures all packets traveling on the network including packets from/to other computers on the LAN.
All computers in the university are plugged into ethernet switches so unicast traffic between two ports does not appear on other ports.

b) In **Edit** menu, explain functionality of ***Set Time Reference*** item.
It enables users to select a packet as a time reference for following packets. So. The arrival time for that packet is considered as 0 and arrival time of the following packets are calculated relative to that.

c) What is the difference between ***display filter*** and ***capture filter***?
Capture filter, filters out packets when Wireshark is monitoring and capturing the packets. Display filter can be applied to a set of captured packets to show a subset of them.

d) In **Analyze** menu, explain functionality of ***Follow TCP Stream*** item**.**
It installs a display filter to select all the packets in the TCP stream you have selected. All

packets belong to the same flow share the same value for Stream Index in TCP header.

Q2. DNS packet observation [10 marks]

[2, 2, 3, 3]

You need to use the web browser to visit a HTTP web page, e.g., www.altavista.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. You should save the captured packets to files so as to analyze them later.

a) What filter string would you use to filter out ***DNS query*** packets? Note: If you don't see any DNS request packets for www.altavista.com in the trace, try other web sites until you do and then use the address of that web site in sections (b) and (d) instead of www.altavista.com.

The following filter displays only DNS query packets:

dns.flags.response == 0

The following filter displays all packets but DNS queries:

!(dns.flags.response == 0)

Both are acceptable.

b) How many DNS query packets for www.altavista.com have you observed? Explain why, if you have observed more than one.
Two query packets, one for IPv4(A) and one for IPv6(AAAA).

c) What are the IP address and Ethernet address of DNS? Explain how you could find them.
IP address: 130.216.35.35 Ethernet address: Not Known (in the uni labs)
IP can be found by looking at destination/source address in IP header in DNS query/response packets. If DNS client and server are on different subnets, it's not possible to find out the Ethernet address of DNS server. The Ethernet destination/source addresses in DNS request/reply packets are, in fact, the address of default router. Ethernet source/destination addresses in DNS reply/request can be considered as DNS Ethernet address, only if DNS client and server are on the same subnet,.

d) Browse another web site (e.g. www.yahoo.com). Then try to browse www.altavista.com again and capture the packets. How many DNS queries for www.altavista.com have you observed this time? Explain why, if different from last time.
No query packet. Because clients cache the results from DNS servers to reduce traffic and delay.

Q3. ICMP packet observation [15 marks]

[5, 4, 4, 2]

a) tracert is a utility which helps network users to find the routing path between two hosts in the Internet. Run the following command and capture traveling packets. Look into the packets and try to explain how this utility works.

Windows: tracert google.ca Linux: traceroute google.ca

Tracert uses ICMP protocol to explore the path between two hosts. It plays with Time to Live(TTL) field in IP header. When a router receives a packet, it looks at this field. If TTL is zero, it drops the packets and sends an error message back to the sender, otherwise it decrements the TTL by 1 and forwards the packet.

Tracert starts by sending an ICMP request with TTL field set to 1. The second router will drop the packet and send back an error message. The source address of the error message shows the address of the second router in the path. Then it sends another ICMP request with TTL equal to 2. This time third router drops the packet and its address can be extracted from the error message. This process continues until it receives a reply from destination host. It tries three times with each TTL value to calculate the average round trip time for each router.

b) Run the following command and capture the packets. Is there any ICMP echo request for this address among the captured packets? If not, explain why.

Ping 127.0.0.1

No, there is not. This address is called loopback address. The packets which are sent to this address are forwarded to the loopback which is a virtual network device. Each outgoing packet which is received by this device is simply put back to the receiving queue of the host protocol stack. This device is usually used for debugging purposes.

Wireshark for Linux is able to capture loopback packets if "any" device is selected.

c) Ping two different web sites (e.g. mail.yahoo.com and www.google.com) and capture ICMP echo request packets. Why are the destination Ethernet addresses the same in request packets while destination IP addresses are different?

Both website are located outside the university and clients are not able to contact them directly. To contact such addresses, clients will have to use Internet routing system. So, they send their request to the nearest router(default router). The Ethernet address which is appeared in request packets is, in fact, the ethernet address of default router but the IP address is the address of final destination.

d) Next, ping www.auckland.ac.nz and then www.cs.auckland.ac.nz, capturing ICMP echo request packets. What differences do you see in the captured packets? (Note: this particular test should certainly be made in the CS labs.)

System uses IPv4 to ping university web site and IPv6 (ICMPv6) to ping department web site.

Q4. Packet trace file [15 marks]

Download **test.pcap** from the 314 webpage Assignment section and open it by Wireshark and answer the following questions:

[2, 2, 5, 4, 2]

a) Is there any fragmented packet in the trace file? Explain how you investigated this.

No, there is not. A display filter like ip.flags.mf == 1 which displays fragmented packets, shows nothing in this file.

b) What are the minimum and maximum packet sizes?

Minimum = 54 Maximum=1514

c) A file named ***2-important-dates.pdf*** (380 KB) has been download from a web site. Look into the captured packets and calculate the file download speed (payload Byte/s)? Explain

how you calculated that. (hint: filter out HTTP GET packets and look for the file name in **Info** column to find the start of download and http response code 200 shows the end of download).

Start Time (packet# 808) = 38.689360 (display filter: http.request.method == GET)
End time (packet# 1200) = 39.027999 (display filter: http.response.code == 200)
Download time = 39.027999 - 38.689360 = 0.338639 s
Downlad speed = 380 /0.338639 = 1122.13 KByte/s = 1.09 MByte/s= 1149061.12 Byte/s

d) There are some packets which have been detected by Wireshark as SMB packets. SMB is the native network file sharing protocol in Microsoft Windows environments. Choose a response packet to QUERY_PATH_INFO at random. QUERY_PATH_INFO command is used by the client to retrieve attributes of a specified file which is resided on the server. How many protocols do you observe in the packet? List protocol names and header sizes. What percentage of the total packet is useful data? Don't forget to illustrate your answer with a screen shot.

5 protocols:

- Ethernet: 14 bytes
- IP: 20 bytes
- TCP: 20 bytes
- NetBOIS: 4 bytes
- SMB: 32 bytes

QUERY_PATH_INFO Data, at the end of the packet, contains the requested information. So, percentage of useful data can be calculated by dividing size of this section by total frame length.

e) What TCP ports have been used by HTTP server/client and SMB server/client?

HTTP Server Port: 80 HTTP Client Port: depends on the selected packet
SMB Server Port: 445 SMB Client Port: 50533

End of Assignment-1