National University of Singapore
School of Computing

CS2105 **Assignment 3** Semester 2 13/14

Deadline: 18 April, 6:00pm

This assignment can be done on your local computer. We assume that you are familiar with basic user interfaces of Wireshark and have installed it on your computer. Otherwise, please take a look at past DIY exercises for guidance.

The goal of this assignment, like the DIY exercises, is to relate what you have learnt from CS2105 to networking practice in the real world. This exercise also introduces a few new concepts that are not in the book/lecture. You will need to be resourceful (e.g., using Google, Wikipedia) to answer these questions.

Answer all questions in the answer sheet provided, and hand in a hardcopy of the answer sheet to Wei Tsang's office (AS6 05-14) before 6pm, 18 April 2014 (Friday).

Submission of answers in any other form (softcopy, foolscap paper etc.) will result in an automatic deduction of 1 point.

WRITE YOUR MATRICULATION NUMBER OF THE TOP LEFT HAND CORNER OF EVERY PAGE IN THE ANSWER SHEET. Failure to do so could result in 0 marks for the assignment (since we do not know who you are).

Your Task

In this assignment, you are given a file, named a3.packets, that contains a set of packets captured using Wireshark on a host with IP address 172.26.191.153. We call this computer the capturing host in the questions. The host was originally not connected to the Internet and has its Ethernet cable unplugged. Trace collection starts (at Time 0) as soon as the Ethernet cable is plugged into the host.

You can download this file from `http://www.comp.nus.edu.sg/~ooiwt/cs2105/1314s2/a3.packets`. Open this file using Wireshark. Examined the packets carefully, and try to reconstruct the sequence of events when a host is plugged into the network.

1. (10 points) **ARP**
   (a) (1 point) What is the purpose of Packet 9?
   (b) (1 point) Who sends Packet 9?
   (c) (2 points) Does the response to Packet 9 exist in the trace? Why?
   (d) (1 point) What is the purpose of Packet 126?
   (e) (1 point) Which packet is the response to Packet 126? Write down the most important information brought to the capturing host by the response of Packet 126.
   (f) (3 points) What is the purpose of Packet 18?
   (g) (1 point) What is the MAC address of capturing host?
2. (8 points) **DHCP**
   (a) (1 point) Find the IP addresses of two DHCP servers that are accessible from the subnet of capturing host.
   (b) (3 points) Are the DHCP servers in the same subnet as the capturing host? Justify your answer.

(c) (2 points) How many distinct clients (including the capturing host) request for the DHCP IP address in the subnet of capturing host during the trace time?

(d) (2 points) Why is the first DHCP packet a DHCP Request packet, rather than a DHCP Discover packet?

3. (5 points) **DNS**

   (a) (2 points) What are the IP addresses of the three DNS servers which are contacted by capturing host?

   (b) (2 points) What could be the reason for contacting three DNS servers instead of one?

   (c) (1 point) What is the longest TTL among the DNS records corresponding to the IP address of daisy.ubuntu.com (starts from packet 128)? Which DNS server does it come from? (You can use ctrl+F to look for daisy.ubuntu.com)

4. (7 points) **SSL**

   We now turn our focus to Packet 145, which starts a TCP connection to a remote server. Right click on Packet 145 and choose "Conversation Filter", "TCP". You can observe the establishment of a TCP connection, followed by a SSL connection. Click on Packet 211, where the certificate of the server is handed over to 172.26.191.153. Look into the content of the packet, paying attention of the certificates.

   (a) (3 points) Why are there four certificates? What is their relation?

   (b) (2 points) Is it trustable that the forth certificate is self-signed? Explain your answer.

   (c) (2 points) What is the purpose of Packet 211? What is it encrypting, and what is the message encrypted with? (Note: the answer comes from the textbook/lecture, not from the payload of the packet).

THE END