Principles of Internetworking Protocols

Assignment Two (20 marks)
(Due on March 8, 2023)

Rocky K. C. Chang

February 22, 2023

Instructions:

1. Submit a pdf file for your answers to i-Learning before noon on March 8. Put down your name, student ID and program/year in your submission.
2. Late submission will not be accepted.
3. Observe also the penalty for plagiarism as stated in the Course Overview slides.

Question 1: DNS configuration and caching [20 marks]

In this question we are going to explore the typical DNS query-response exchanges and DNS caching. Use the Brave browser for this question. You must include relevant Wireshark screenshots to support your answer. The targeted domain name is `www.mit.edu`.

(a) [2 MARKS] Use `ipconfig` (or `ifconfig`) to find out the DNS servers configured on your machine. Besides their IP addresses, please find out which companies host the DNS servers. Where are the servers physically located (using latency measurement and your best knowledge).

(b) [2 MARKS] Clear your system's DNS cache using `ipconfig /flushdns`. After that, check that the DNS cache is indeed empty using `ipconfig /displaydns` (there may still be some entries there.). Visit `www.mit.edu` and capture the DNS traffic with Wireshark. Save the DNS packets in `part-b.pcapng` using `File/Export Specific Packets`. Submit this file with answers to other questions.

(c) [2 MARKS] How many types of DNS queries captured and what are they for?

(d) [2 MARKS] What are the DNS responses to the queries for `www.mit.edu`?

(e) [2 MARKS] Check whether the answers for `www.mit.edu` are cached in your system's DNS cache using `ipconfig /displaydns | grep mit`. Explain your answer.

(f) [2 MARKS] Reload the page several times. Do you see new DNS queries and replies for `www.mit.edu` and new data packets from the server?

(g) [2 MARKS] Follow the steps in `https://www.cyberciti.biz/faq/google-chrome-clear-or-flush-the-dns-cache/` to clear the browser's DNS cache. Reload the page. Do you find new DNS queries and replies in Wireshark? Do you find the answers in your system's cache?

(h) [2 MARKS] Traceroute to `www.mit.edu` and capture the traffic. Do you see DNS queries and responses in the Wireshark capture? Do you see DNS entries for `www.mit.edu` in the system's DNS cache?

(i) [4 MARKS] Now, if you clear the browser's DNS cache while your system's DNS cache still has the entries for `www.mit.edu`, design an experiment to show whether the browser will use the system's DNS cache.