Computer Networks
Wireshar Lab
Due: 27 Khordad 1399

Prepare a report and include a part of the packets you captured in the Wireshark as an image in the report.

Take the following steps before answering the questions:

- Close all tunneling connections in your system if you are using any (VPN, proxies, …)
- Close all the programs in your computer using the Internet.

Part 1: DNS

- Open an Internet browser.
- Start the Wireshark.
- Clear your DNS history by using command "**ipconfig /flushdns**" in Window's command prompt.
- Choose a random website. It can be any university webpage (a http one not a https).
- Open the website in your browser while the Wireshark is capturing the line.
- After the page is loaded, you can stop the capture.

Questions

1. Filter UDP connections with port number 53 which belongs to DNS (udp.dstport==53 || udp.srcport==53). There might be some sequences of DNS. Describe the DNS sequences for the website you opened.

2. Select the DNS query packet. Explain the content of the request.

3. Find the response of the DNS packet in question 1. Describe flags and the answer.

4. What is Time to Live in DNS protocol and in which packet can it be found?

5. You probably see some DNS packets that are the query for another website except one you opened. Can you explain what these DNS queries are?

6. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

7. 8. Open command window and type "nslookup -type=NS + address of a website you opened". For example: "nslookup -type=NS google.com". Please explain what the results are.

Part 2: HTTP

- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
  Your browser should display a short HTML file with two images.
  Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.
- Filter http traffic.

Questions:

1. How many HTTP GET request messages did your browser send?
2. Explain the purposes of all GET messages.
3. Explain the GET responses. What is the content of these messages?