CS 3873: Net-Centric Computing
Lab 3: Exploring DNS with Wireshark

Student Name: ___Adrian Freeman____ Student Number: _3661616__

[Mandatory] Declaration: “I warrant that this is my own work.”

Signed by _Adrian Freeman__

[Optional] “I hereby give my permission for this work to be used (with my name and identifying information removed) for UNB Faculty of Computer Science program accreditation purposes.”

Signed by _Adrian Freeman__

Report for Lab Exercise 3:
Exploring DNS with Wireshark

LAB ACTIVITIES:

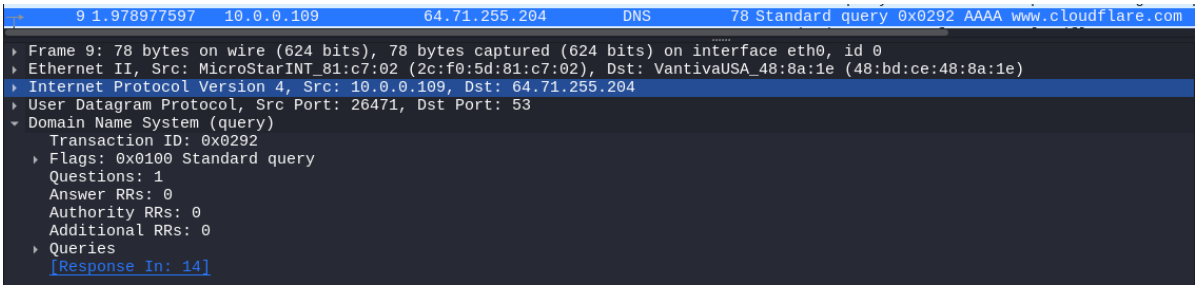
In this lab, we used Wireshark to explore the use of Domain Name System (DNS). Different types of DNS query and response messages are studied in detail.

ANSWERS TO LAB QUESTIONS:

3. Based on your above capture, answer the following questions:

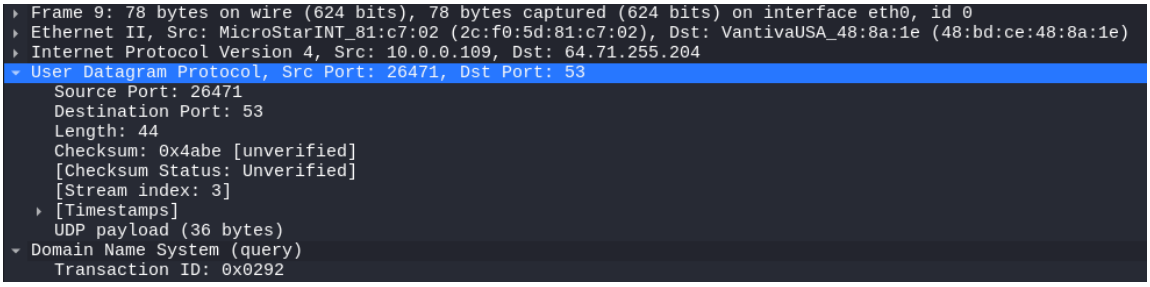
   a. Locate the DNS query and response messages specifically for the hostname "`www.cloudflare.com`". What is their Transaction ID?

   The Transaction ID is 0x0292



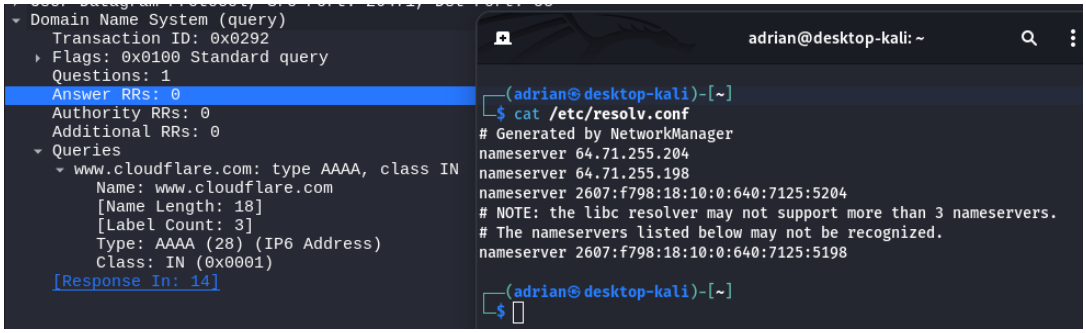
   b. Are these two DNS query and response messages sent over UDP or TCP? What is the destination port for the DNS query message? What is the source port of the DNS response message?

   They are sent over UDP, the destination port is 53, the source port is 26471



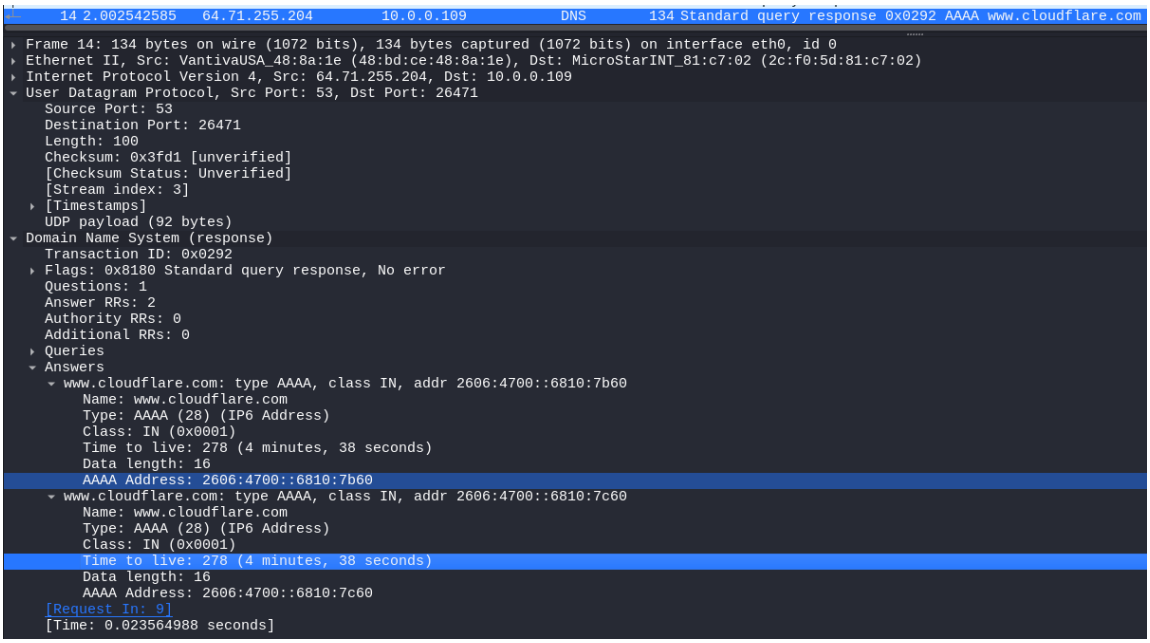
   c. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your default DNS server. Are these two IP addresses the same?

   The "Type" of DNS query is AAAA, There are 0 answers. The destination is the same as my default DNS server.



d. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There are 2 answers provided, each containing 16 bits (2 bytes) of data. I believe what the AAAA response is returning is the IPv6 address associated with www.cloudflare.com

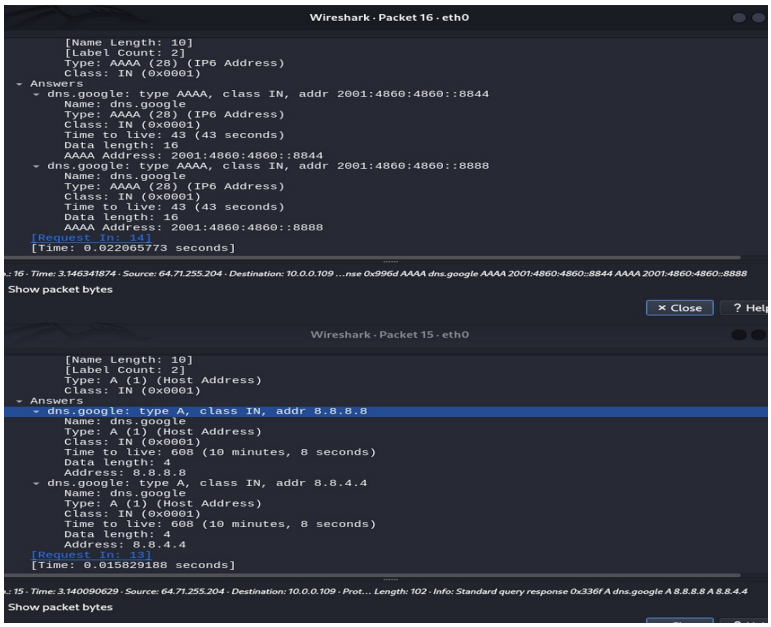


4. Now run the following command and repeat the above experiment and answer the following questions: nslookup id415m01.cs.unb.ca. dns.google

Note that this command uses Google Public DNS2 , which provides free DNS resolution.

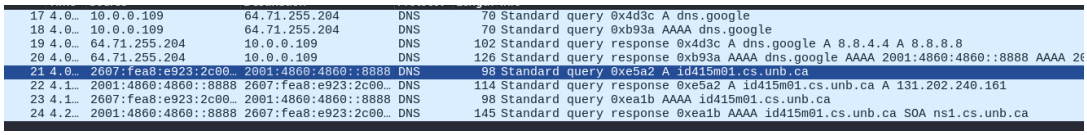
a. Locate the DNS query and response messages specifically to resolve the DNS server with hostname "dns.google"? What IP address(es) does the response show?

There are two DNS queries and responses resolving hostname dns.google. One is of type A and one is of type AAAA. The type A response shows the IPv4 address linked to the domain name. The type AAAA response shows the IPv6 address linked to the domain name.



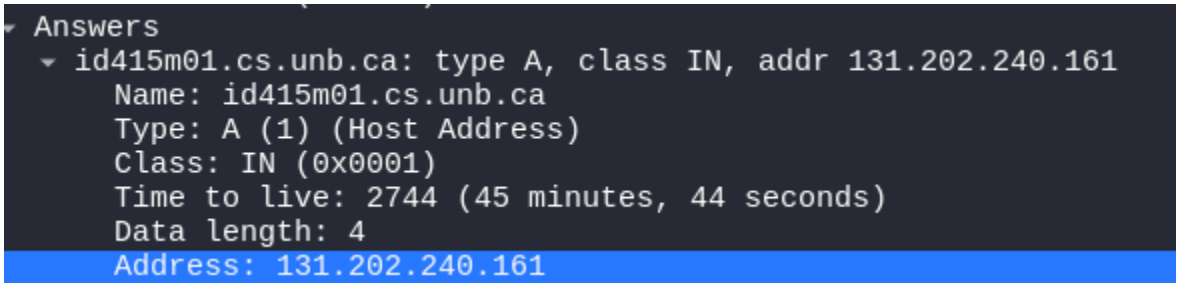
b. Locate the DNS query and response messages specifically to resolve the hostname "id415m01.cs.unb.ca.". To what destination IP address is the DNS query message sent? Is this the IP address of one of your default DNS servers that were obtained above from ipconfig /all?

The query is sent to the IPv6 assigned to the hostname for google, from the previous AAAA response. In this case, it was sent to 2001:48604860::8888. (I had to remove the ip.addr==my_ip to see this)



c. Examine the DNS response message to resolve the hostname "id415m01.cs.unb.ca.", what is the IP address of the hostname being resolved? How long is the valid period of the resource record?

The IP address of the hostname is 131.202.240.161, which has a TTL of 2744 seconds (45 minutes and 44 seconds)



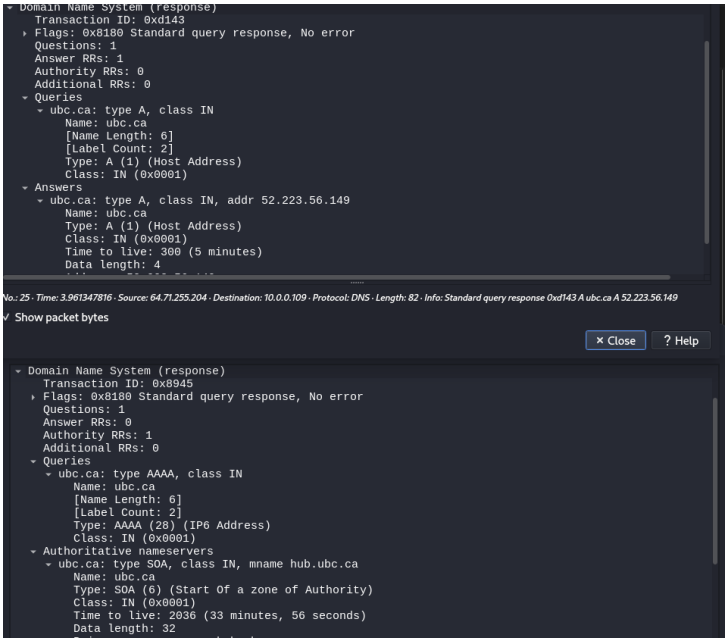
5. Now run the following command and repeat the above experiment and answer the following questions: nslookup –type=NS ubc.ca.

a. Locate the DNS query and response messages specifically to resolve the domain name "ubc.ca". To what IP address is the DNS query message sent? Is this the IP address of one of your default DNS servers?

The query was sent to 64.71.255.204, which is one of my DNS servers

b. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Again, there are two queries, an A type, and an AAAA type. The A type provides the IPv4 in the response, and the AAAA type provides no answers, but does provide one authoritative record.



c. Examine the DNS response message. What DNS name servers does the response message provide? Does this response message also provide the IP addresses of these name servers?

The response provides the name server nmc.ubc.ca, it does not provide the IP of the name servers.