

## 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:

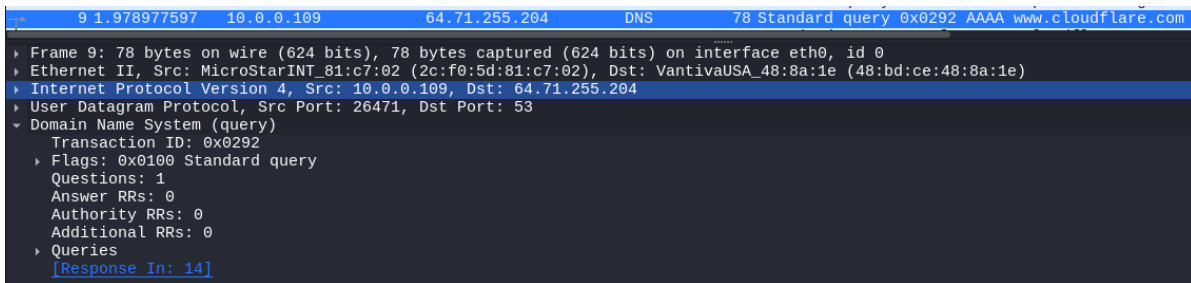
In this lab, we used Wireshark to explore the use of Domain Name System (DNS). Different types of DNS query and response messages are studied in detail.

### 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

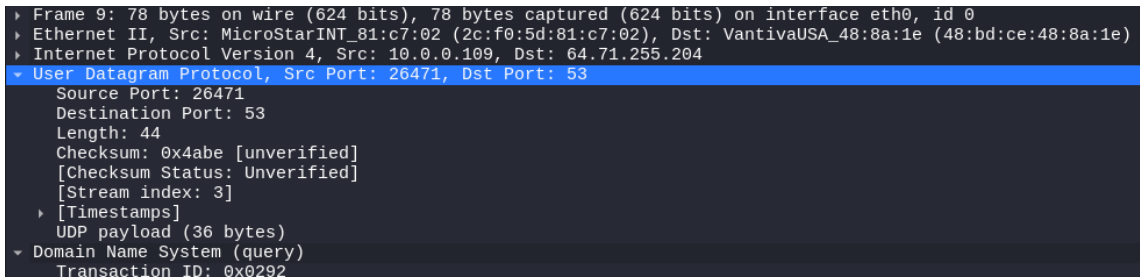


```

9 1.978977597 10.0.0.109 64.71.255.204 DNS 78 Standard query 0x0292 AAAA www.cloudflare.com
  Frame 9: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
  Ethernet II, Src: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02), Dst: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)
  Internet Protocol Version 4, Src: 10.0.0.109, Dst: 64.71.255.204
  User Datagram Protocol, Src Port: 26471, Dst Port: 53
  Domain Name System (query)
    Transaction ID: 0x0292
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      [Response In: 14]
  
```

- 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

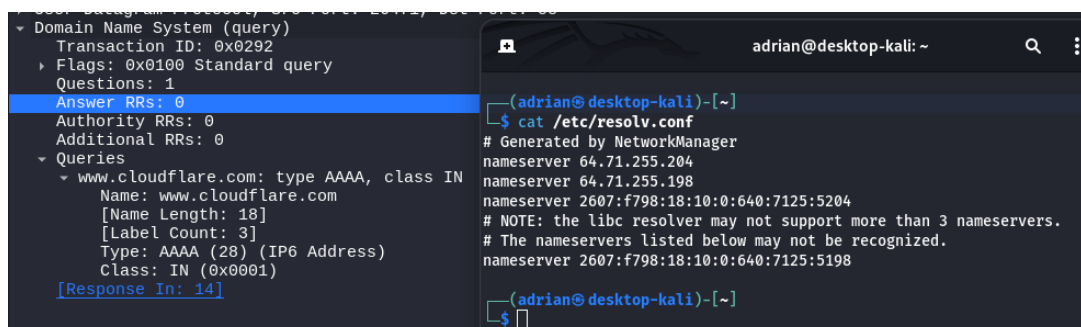


```

  Frame 9: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
  Ethernet II, Src: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02), Dst: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)
  Internet Protocol Version 4, Src: 10.0.0.109, Dst: 64.71.255.204
  User Datagram Protocol, Src Port: 26471, Dst Port: 53
    Source Port: 26471
    Destination Port: 53
    Length: 44
    Checksum: 0x4abe [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Timestamps]
    UDP payload (36 bytes)
  Domain Name System (query)
    Transaction ID: 0x0292
  
```

- 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.



```

Domain Name System (query)
  Transaction ID: 0x0292
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.cloudflare.com: type AAAA, class IN
      Name: www.cloudflare.com
      [Name Length: 18]
      [Label Count: 3]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
    [Response In: 14]

(adrian@desktop-kali)-[~]
$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 64.71.255.204
nameserver 64.71.255.198
nameserver 2607:f798:18:10:0:640:7125:5204
# NOTE: the libc resolver may not support more than 3 nameservers.
# The nameservers listed below may not be recognized.
nameserver 2607:f798:18:10:0:640:7125:5198
  
```

- 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

```

14 2.002542585 64.71.255.204 10.0.0.109 DNS 134 Standard query response 0x0292 AAAA www.cloudflare.com
Frame 14: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface eth0, id 0
Ethernet II, Src: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e), Dst: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)
Internet Protocol Version 4, Src: 64.71.255.204, Dst: 10.0.0.109
User Datagram Protocol, Src Port: 53, Dst Port: 26471
Source Port: 53
Destination Port: 26471
Length: 100
Checksum: 0x3fd1 [unverified]
[Checksum Status: Unverified]
[Stream Index: 3]
[Timestamps]
UDP payload (92 bytes)
Domain Name System (response)
Transaction ID: 0x0292
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
Answers
www.cloudflare.com: type AAAA, class IN, addr 2606:4700::6810:7b60
Name: www.cloudflare.com
Type: AAAA (28) (IPv6 Address)
Class: IN (0x0001)
Time to live: 278 (4 minutes, 38 seconds)
Data length: 16
AAAA Address: 2606:4700::6810:7b60
www.cloudflare.com: type AAAA, class IN, addr 2606:4700::6810:7c60
Name: www.cloudflare.com
Type: AAAA (28) (IPv6 Address)
Class: IN (0x0001)
Time to live: 278 (4 minutes, 38 seconds)
Data length: 16
AAAA Address: 2606:4700::6810:7c60
[Request In: 9]
[Time: 0.023564988 seconds]

```

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.

```

Wireshark - Packet 16 - eth0
[Name Length: 10]
[Label Count: 2]
Type: AAAA (28) (IPv6 Address)
Class: IN (0x0001)
Answers
dns.google: type AAAA, class IN, addr 2001:4860:4860::8844
Name: dns.google
Type: AAAA (28) (IPv6 Address)
Class: IN (0x0001)
Time to live: 43 (43 seconds)
Data length: 16
AAAA Address: 2001:4860:4860::8844
dns.google: type AAAA, class IN, addr 2001:4860:4860::8888
Name: dns.google
Type: AAAA (28) (IPv6 Address)
Class: IN (0x0001)
Time to live: 43 (43 seconds)
Data length: 16
AAAA Address: 2001:4860:4860::8888
[Request In: 14]
[Time: 0.022065773 seconds]

Wireshark - Packet 15 - eth0
[Name Length: 10]
[Label Count: 2]
Type: A (1) (Host Address)
Class: IN (0x0001)
Answers
dns.google: type A, class IN, addr 8.8.8.8
Name: dns.google
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 608 (10 minutes, 8 seconds)
Data length: 4
Address: 8.8.8.8
dns.google: type A, class IN, addr 8.8.4.4
Name: dns.google
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 608 (10 minutes, 8 seconds)
Data length: 4
Address: 8.8.4.4
[Request In: 55]
[Time: 0.015029188 seconds]

```

- 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 2001:4860:4860::8888. (I had to remove the `ip.addr==my_ip` to see this)

17 4.0...	10.0.0.109	64.71.255.204	DNS	70 Standard query 0x4d3c A dns.google
18 4.0...	10.0.0.109	64.71.255.204	DNS	70 Standard query 0xb93a AAAA dns.google
19 4.0...	64.71.255.204	10.0.0.109	DNS	102 Standard query response 0x4d3c A dns.google A 8.8.4.4 A 8.8.8.8
20 4.0...	64.71.255.204	10.0.0.109	DNS	126 Standard query response 0xb93a AAAA dns.google AAAA 2001:4860:4860::8888 AAAA 26
21 4.0...	2607:fea8:e923:2c00...	2001:4860:4860::8888	DNS	98 Standard query 0xe5a2 A id415m01.cs.unb.ca
22 4.1...	2001:4860:4860::8888	2607:fea8:e923:2c00...	DNS	114 Standard query response 0xe5a2 A id415m01.cs.unb.ca A 131.202.240.161
23 4.1...	2607:fea8:e923:2c00...	2001:4860:4860::8888	DNS	98 Standard query 0xea1b AAAA id415m01.cs.unb.ca
24 4.2...	2001:4860:4860::8888	2607:fea8:e923:2c00...	DNS	145 Standard query response 0xea1b AAAA id415m01.cs.unb.ca SOA ns1.cs.unb.ca

- 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)

```

Answers
  id415m01.cs.unb.ca: type A, class IN, addr 131.202.240.161
    Name: id415m01.cs.unb.ca
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 2744 (45 minutes, 44 seconds)
    Data length: 4
    Address: 131.202.240.161

```

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

```

Internet Protocol Version 4, Src: 10.0.0.109, Dst: 64.71.255.204
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentially Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xff44 (65348)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xf0f3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.0.109
Destination Address: 64.71.255.204
User Datagram Protocol, Src Port: 45683, Dst Port: 53
Source Port: 45683
Destination Port: 53
Length: 32
Checksum: 0x4ab2 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
UDP payload (24 bytes)
Domain Name System (query)
Transaction ID: 0xd143
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  ubc.ca: type A, class IN
    Name: ubc.ca
    [Name Length: 6]
    [Label Count: 2]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
[Response In: 25]

adrian@desktop-kali: ~
;; communications error to 52.223.56.149#53: timed out
;; no servers could be reached

(adrian@desktop-kali)-[~]
$ nslookup -type=NS ubc.ca.
;; communications error to 52.223.56.149#53: timed out
;; communications error to 52.223.56.149#53: timed out
;; communications error to 52.223.56.149#53: timed out
;; no servers could be reached

(adrian@desktop-kali)-[~]
$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 64.71.255.204
nameserver 64.71.255.198
nameserver 2607:f798:18:10:0:640:7125:5204
# NOTE: the libc resolver may not support more than 3 nameser
# The nameservers listed below may not be recognized.
nameserver 2607:f798:18:10:0:640:7125:5198

(adrian@desktop-kali)-[~]
$

```

- 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.

```

Domain Name System (response)
Transaction ID: 0xd143
Flags: 0x0180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  ubc.ca: type A, class IN
    Name: ubc.ca
    [Name Length: 6]
    [Label Count: 2]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Answers
  ubc.ca: type A, class IN, addr 52.223.56.149
    Name: ubc.ca
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
No. 25 - Time: 3.961347816 - Source: 64.71.255.204 - Destination: 10.0.0.109 - Protocol: DNS - Length: 82 - Info: Standard query response 0xd143 A ubc.ca A 52.223.56.149
Show packet bytes
Close Help

Domain Name System (response)
Transaction ID: 0x8945
Flags: 0x0180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
  ubc.ca: type AAAA, class IN
    Name: ubc.ca
    [Name Length: 6]
    [Label Count: 2]
    Type: AAAA (28) (IPv6 Address)
    Class: IN (0x0001)
Authoritative nameservers
  ubc.ca: type SOA, class IN, mname hub.ubc.ca
    Name: ubc.ca
    Type: SOA (6) (Start Of a zone of Authority)
    Class: IN (0x0001)
    Time to live: 2036 (33 minutes, 56 seconds)
    Data length: 32
  
```

- 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.

```

25 3.961347816 64.71.255.204 10.0.0.109 DNS 82 Standard query response 0xd143 A ubc.ca A 52.223.56.149
26 3.961399026 64.71.255.204 10.0.0.109 DNS 110 Standard query response 0x8945 AAAA ubc.ca SOA hub.ubc.ca

Transaction ID: 0x8945
Flags: 0x0180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
  ubc.ca: type AAAA, class IN
    Name: ubc.ca
    [Name Length: 6]
    [Label Count: 2]
    Type: AAAA (28) (IPv6 Address)
    Class: IN (0x0001)
Authoritative nameservers
  ubc.ca: type SOA, class IN, mname hub.ubc.ca
    Name: ubc.ca
    Type: SOA (6) (Start Of a zone of Authority)
    Class: IN (0x0001)
    Time to live: 2036 (33 minutes, 56 seconds)
    Data length: 32
    Primary name server: hub.ubc.ca
    Responsible authority's mailbox: nmc.ubc.ca
    Serial Number: 725110858
    Refresh Interval: 1200 (20 minutes)
    Retry Interval: 180 (3 minutes)
    Expire limit: 1209600 (14 days)
    Minimum TTL: 3600 (1 hour)
[Request in: 22]
[Time: 0.048568190 seconds]
  
```