Lab 3: DNS

CSE5355

The University of Texas Rio Grande Valley

Spring 2018

Dr. Quweider

Juan Bermudez

November 16, 2018

Lab03: DNS

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
nslookup at alibaba.com in China

```
C:\Users\jaber> nslookup alibaba.com
Server:  ns.vtx1.net
Address:  216.183.32.6

Non-authoritative answer:
Name:    alibaba.com
Addresses:  198.11.132.23
          205.204.101.42
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
authoritative nslookup for the University of Barcelona

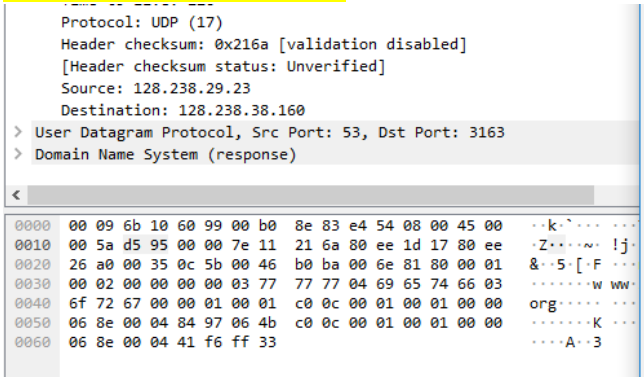
```
Non-authoritative answer:
ub.edu  nameserver = chico.rediris.es
ub.edu  nameserver = sun.rediris.es
ub.edu  nameserver = rnpro07.com.ub.edu
ub.edu  nameserver = rnpro01.com.ub.edu
ub.edu  nameserver = rnpro04.com.ub.edu

rnpro01.com.ub.edu      internet address = 161.116.160.1
sun.rediris.es  internet address = 130.206.1.2
sun.rediris.es  AAAA IPv6 address = 2001:720:418:caf1::2
rnpro07.com.ub.edu      internet address = 161.116.230.1
chico.rediris.es        internet address = 130.206.1.3
chico.rediris.es        AAAA IPv6 address = 2001:720:418:caf1::3
rnpro04.com.ub.edu      internet address = 161.116.110.95
```

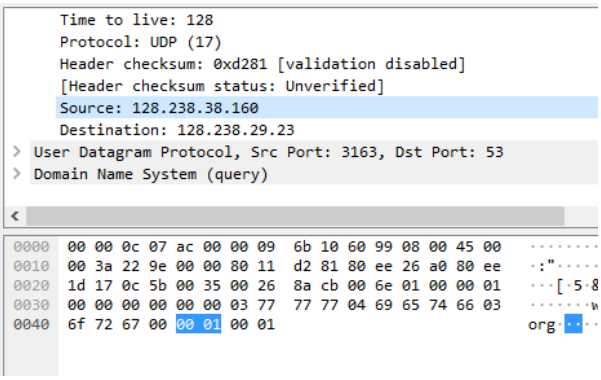
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
C:\Users\jaber> nslookup mail.yahoo.com rnpro04.com.ub.edu
Server:  rnpro04.com.ub.edu
Address:  161.116.110.95
```

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

They are both sent over UDP





5. What is the destination port for the DNS query message? What is the source port of DNS response message?

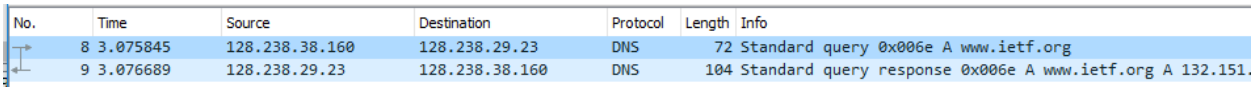
For query, Dst Port: 53

For response, Src Port: 53

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query is sent to: 128.238.29.23

Using ipconfig shows that the IP addresses do not match



No.	Time	Source	Destination	Protocol	Length	Info
8	3.075845	128.238.38.160	128.238.29.23	DNS	72	Standard query 0x006e A www.ietf.org
9	3.076689	128.238.29.23	128.238.38.160	DNS	104	Standard query response 0x006e A www.ietf.org A 132.151.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   Physical Address. . . . . . . . . : 3C-95-09-52-1A-BB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4cf2:6160:979c:156c%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.21.33.208(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : Friday, November 16, 2018 3:52:59 PM
   Lease Expires . . . . . . . . . . : Saturday, November 17, 2018 3:52:59 PM
   Default Gateway . . . . . . . . . : 172.21.32.2
   DHCP Server . . . . . . . . . . . : 192.168.2.36
   DHCPv6 IAID . . . . . . . . . . . : 37524745
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-C0-D7-60-54-E1-AD-2A-34-99
   DNS Servers . . . . . . . . . . . : 216.183.32.6
                                       216.183.32.7
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

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

The DNS query message is Type A, it is standard message.

The message does not contain any answers.

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

The DNS response has 2 answers.

```
▾ Domain Name System (response)
    Transaction ID: 0x006e
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.ietf.org: type A, class IN
  ▾ Answers
    ▸ www.ietf.org: type A, class IN, addr 132.151.6.75
    ▸ www.ietf.org: type A, class IN, addr 65.246.255.51
```

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The SYN packet IP address corresponds to 132.151.6.75

```
10 3.078479    128.238.38.160    132.151.6.75      TCP    62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
11 3.096413    132.151.6.75      128.238.38.160    TCP    62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
12 3.096463    128.238.38.160    132.151.6.75      TCP    54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
```

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries? No queries were issued for images.

11. What is the destination port for the DNS query message? What is the source port of DNS response message? The DNS query message is dest: port 53, the source port for the DNS response is source port: 53

```
    Destination: 128.238.29.22
▾ User Datagram Protocol, Src Port: 3742, Dst Port: 53
    Source Port: 3742
    Destination Port: 53

▾ User Datagram Protocol, Src Port: 53, Dst Port: 3742
    Source Port: 53
    Destination Port: 3742
```

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? The DNS query is sent to destination IP 128.238.29.22 and it does not math the default address of the local DNS server.

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? The Query is standard query type A, and it does not contain any answers.

```
▾ Queries
  ▾ www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 20]
```

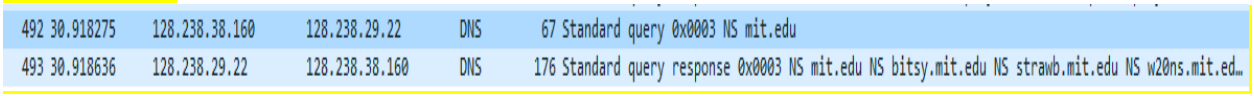
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? The DNS response message contains 1 answer.

15. Provide a screenshot.

```
Queries
  www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
Answers
  www.mit.edu: type A, class IN, addr 18.7.22.83
```

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The IP address the DNS query message is sent to is 128.238.29.22. This is not the IP address of the default server.



17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? The type is NS, and it contains no answers

```
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

It provides bitsy.mit.edu, strab.mit.edu, and w20ns.mit.edu. and it also provides their IP addresses.

19. Provide a screenshot.

```
bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    Name: bitsy.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20736
    Data length: 4
    Address: 18.72.0.3
strawb.mit.edu: type A, class IN, addr 18.71.0.151
    Name: strawb.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20736
    Data length: 4
    Address: 18.71.0.151
w20ns.mit.edu: type A, class IN, addr 18.70.0.160
    Name: w20ns.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20736
    Data length: 4
    Address: 18.70.0.160
```

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
The DNS query sends the message to IP address 18.72.0.3. It does not correspond to the local server, it corresponds to bitsy.mit.edu

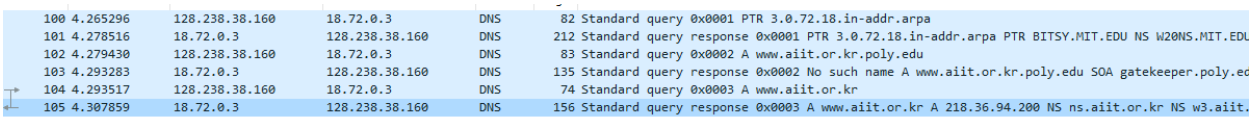
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? The DNS query is of Standard type A, it contains no answers.

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
    www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain? It contains 1 answer, it contains what is shown below:

```
Answers
    www.aiit.or.kr: type A, class IN, addr 218.36.94.200
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3338
        Data length: 4
        Address: 218.36.94.200
```

23. Provide a screenshot.



```
100 4.265296    128.238.38.160  18.72.0.3       DNS      82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101 4.278516    18.72.0.3       128.238.38.160  DNS     212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU
102 4.279430    128.238.38.160  18.72.0.3       DNS      83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
103 4.293283    18.72.0.3       128.238.38.160  DNS     135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.ed
104 4.293517    128.238.38.160  18.72.0.3       DNS      74 Standard query 0x0003 A www.aiit.or.kr
105 4.307859    18.72.0.3       128.238.38.160  DNS     156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.
```

```
Authority RRs: 2
Additional RRs: 2
Queries
    www.aiit.or.kr: type A, class IN
Answers
    www.aiit.or.kr: type A, class IN, addr 218.36.94.200
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3338
        Data length: 4
        Address: 218.36.94.200
Authoritative nameservers
```