Lyndon Renaud
104 566 776
Computer Networks Lab 1: DNS
03-60-367

Lab 1: DNS

nslookup

1. **Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?**
   The web server I used for this is www.aiit.or.kr. The IP address of this server is 58.229.6.225

2. **Run *nslookup* to determine the authoritative DNS servers for a university in Europe.**
   The web server I used for this is www.ucl.ac.uk. The authoritative DNS servers for this university are:
   ns0.gtm.ucl.ac.uk
   ns1.gtm.ucl.ac.uk

3. **Run nslookup so that one of the DNS servers obtains in Question 2 queries for the mail servers for Yahoo! Mail. What is its IP address?**
   The IP address for ns1.gtm.ucl.ac.uk is 193.60.224.2. For this question I tried “nslookup ns1.gtm.ucl.ac.uk mail.yahoo.com” which returned “;; connection timed out; no servers could be reached”. I also tried “nslookup www.mail.yahoo.com ns1.gtm.ucl.ac.uk” which returned “** server can’t find www.yahoo.com: REFUSED”. I tried this with www.mail.google.com and with the DNS ns2.google.com which also returned the same result.

Tracing DNS with Wireshark

4. **Locate the DNS query and response messages. Are they sent over UDP or TCP?**
   There were 4 total DNS messages, 2 query and 2 response. All these messages are sent over UDP.

5. **What is the destination port for the DNS query message? What is the source port of the DNS response message?**
   The destination port for the DNS query message is port 53.
   The source port of the DNS response message is port 53.

6. **To what IP address is the DNS query 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 the IP address 137.207.32.2. The IP address of my local DNS server is 137.207.32.2. These addresses are the same.

7. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**
   The DNS query is type A. The query message does not contain any answers.

8. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**
   In the DNS response message, 3 answers are provided. These answers contain attributes of domains. These attributes name, type, class, time to live, data length, cname, and address

9. **Consider the subsequent TCP SYN packet sent by your host. Does this destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**
   The destination IP address of the SYN packet is 104.20.0.85. This IP corresponds to the IP of an answer given in the DNS response message. It is the IP for www.ietf.org.cdn.cloudflare.net.

10. **This web page contains images. Before retrieving each image, does your host issue new DNS queries?**
    No, the only DNS queries my host issues are at the very beginning.

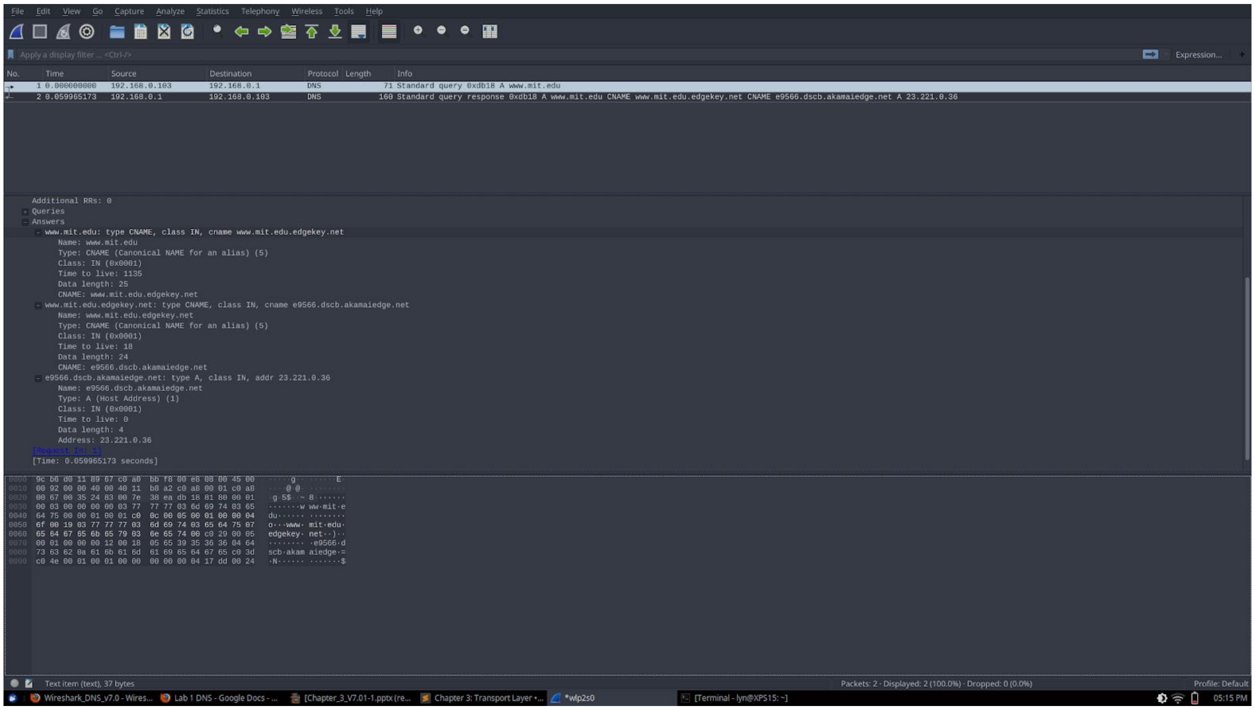
11. **What is the destination port for the DNS query message? What is the source port of the DNS response message?**
    The destination port for the DNS query message is 53. The source port of the DNS response message is 53.

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 message is sent to the IP address 192.168.0.1. This is the IP address of my default local DNS server.

13. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any answers?**
    The DNS query is type A. The query message does not contain any answers.

14. **Examine the DNS response message. How many “answers” are provided. What do each of these answers contain?**
    The DNS response message contains 3 answers. These answers contain attributes of domains. These attributes name, type, class, time to live, data length, cname, and address.

15. **Provide a screenshot.**
    Below is a screenshot of the wireshark state from question 14.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.  Time         Source         Destination    Protocol Length Info
   1 0.000000000  192.168.0.103  192.168.0.1    DNS          71 Standard query 0xdb18 A www.mit.edu
   2 0.059965173  192.168.0.1    192.168.0.103  DNS         160 Standard query response 0xdb18 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.221.0.36
```

```
    Additional RRs: 0
  + Queries
  - Answers
    - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
          Name: www.mit.edu
          Type: CNAME (Canonical NAME for an alias) (5)
          Class: IN (0x0001)
          Time to live: 1135
          Data length: 25
          CNAME: www.mit.edu.edgekey.net
    - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
          Name: www.mit.edu.edgekey.net
          Type: CNAME (Canonical NAME for an alias) (5)
          Class: IN (0x0001)
          Time to live: 18
          Data length: 24
          CNAME: e9566.dscb.akamaiedge.net
    - e9566.dscb.akamaiedge.net: type A, class IN, addr 23.221.0.36
          Name: e9566.dscb.akamaiedge.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 0
          Data length: 4
          Address: 23.221.0.36
    [Request In: 1]
    [Time: 0.059965173 seconds]
```

```
0000  9c b6 d0 11 89 67 c0 a0  bb f8 00 e8 08 00 45 00   ·····g·· ······E·
0010  00 92 00 00 40 00 40 11  b8 a2 c0 a8 00 01 c0 a8   ····@·@· ········
0020  00 67 00 35 24 83 00 7e  38 ea db 18 81 80 00 01   ·g·5$··~ 8·······
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 04   du······ ········
0050  6f 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   o···www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 12 00 18  05 65 39 35 36 36 04 64   ········ ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3d   scb·akam aiedge·=
0090  c0 4e 00 01 00 01 00 00  00 00 00 04 17 dd 00 24   ·N······ ·······$
```

Text item (text), 37 bytes
Packets: 2 · Displayed: 2 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Wireshark_DNS_v7.0 - Wires…
Lab 1 DNS - Google Docs - …
[Chapter_3_V7.01-1.pptx (re…
Chapter 3: Transport Layer • …
*wlp2s0
[Terminal - lyn@XPS15: ~]
05:15 PM

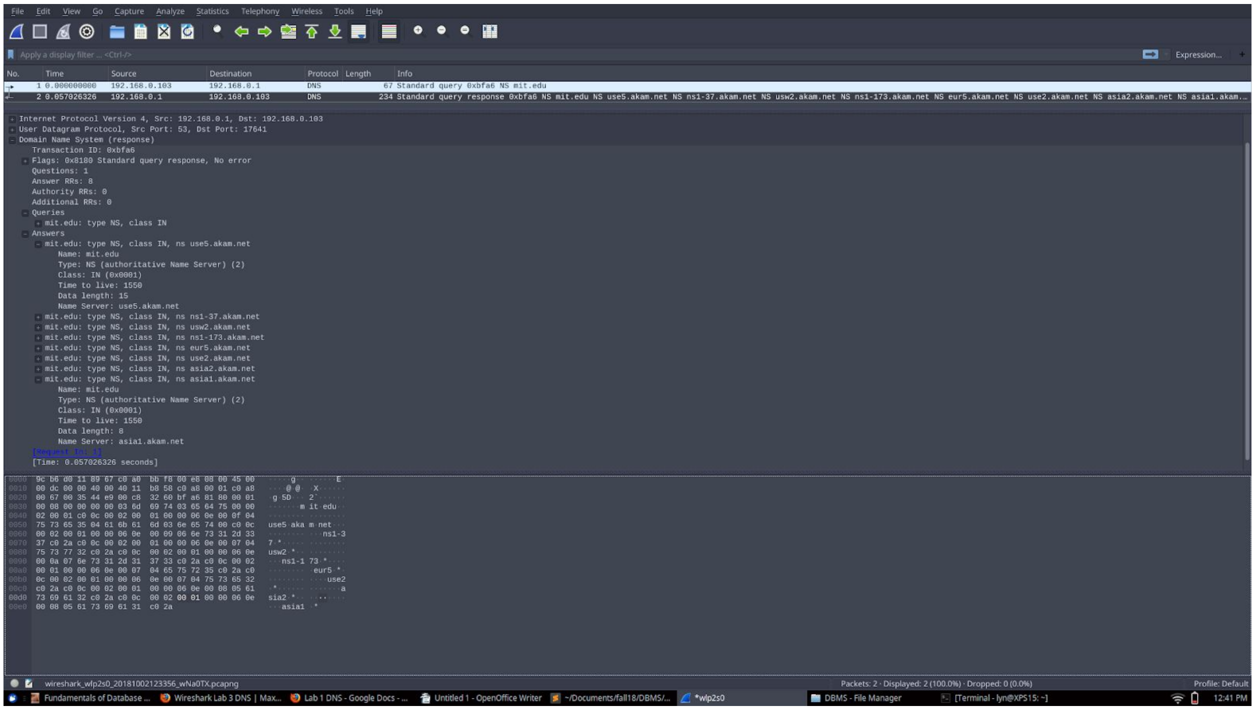
“nslookup -type=NS mit.edu”

16. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**
    The DNS query message is sent to the IP address 192.168.0.1. This is my default local DNS server at home.

17. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**
    The DNS query is of type “NS”. The query does not contain any answers.

18. **Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide IP addresses of the MIT nameservers?**
    The DNS response message provided 8 MIT nameservers. These are: use5.akam.net, ns1-37.akam.net, usw2.akam.net, ns1-173.akam.net, eur5.akam.net, use2.akam.net, asia2.akam.net, asia1.akam.net. The response did not provide IP addresses of the MIT nameservers.

19. **Provide a screenshot**



```
No.  Time          Source         Destination    Protocol Length Info
   1 0.000000000   192.168.0.103  192.168.0.1    DNS          67 Standard query 0xbfa6 NS mit.edu
   2 0.057026326   192.168.0.1    192.168.0.103  DNS         234 Standard query response 0xbfa6 NS mit.edu NS use5.akam.net NS ns1-37.akam.net NS usw2.akam.net NS ns1-173.akam.net NS eur5.akam.net NS use2.akam.net NS asia2.akam.net NS asia1.akam...
```

```
+ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103
+ User Datagram Protocol, Src Port: 53, Dst Port: 17641
- Domain Name System (response)
    Transaction ID: 0xbfa6
  + Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  - Queries
    + mit.edu: type NS, class IN
  - Answers
    - mit.edu: type NS, class IN, ns use5.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1550
        Data length: 15
        Name Server: use5.akam.net
    + mit.edu: type NS, class IN, ns ns1-37.akam.net
    + mit.edu: type NS, class IN, ns usw2.akam.net
    + mit.edu: type NS, class IN, ns ns1-173.akam.net
    + mit.edu: type NS, class IN, ns eur5.akam.net
    + mit.edu: type NS, class IN, ns use2.akam.net
    + mit.edu: type NS, class IN, ns asia2.akam.net
    - mit.edu: type NS, class IN, ns asia1.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1550
        Data length: 8
        Name Server: asia1.akam.net
    [Request In: 1]
    [Time: 0.057026326 seconds]
```

```
0000  9c b6 d0 11 89 67 c0 a0  bb f8 00 e8 08 00 45 00   .....g.. ......E.
0010  00 dc 00 00 40 00 40 11  b8 58 c0 a8 00 01 c0 a8   ....@.@. .X......
0020  00 67 00 35 44 e9 00 c8  32 60 bf a6 81 80 00 01   .g.5D... 2`......
0030  00 08 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   .......m it.edu..
0040  02 00 01 c0 0c 00 02 00  01 00 00 06 0e 00 0f 04   ........ ........
0050  75 73 65 35 04 61 6b 61  6d 03 6e 65 74 00 c0 0c   use5.aka m.net...
0060  00 02 00 01 00 00 06 0e  00 09 06 6e 73 31 2d 33   ........ ...ns1-3
0070  37 c0 2a c0 0c 00 02 00  01 00 00 06 0e 00 07 04   7.*..... ........
0080  75 73 77 32 c0 2a c0 0c  00 02 00 01 00 00 06 0e   usw2.*.. ........
0090  00 0a 07 6e 73 31 2d 31  37 33 c0 2a c0 0c 00 02   ...ns1-1 73.*....
00a0  00 01 00 00 06 0e 00 07  04 65 75 72 35 c0 2a c0   ........ .eur5.*.
00b0  0c 00 02 00 01 00 00 06  0e 00 07 04 75 73 65 32   ........ ....use2
00c0  c0 2a c0 0c 00 02 00 01  00 00 06 0e 00 08 05 61   .*...... .......a
00d0  73 69 61 32 c0 2a c0 0c  00 02 00 01 00 00 06 0e   sia2.*.. ........
00e0  00 08 05 61 73 69 61 31  c0 2a                     ...asia1 .*
```

wireshark_wlp2s0_20181002123356_wNa0TX.pcapng   Packets: 2 · Displayed: 2 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

Fundamentals of Database ...
Wireshark Lab 3 DNS | Max...
Lab 1 DNS - Google Docs - ...
Untitled 1 - OpenOffice Writer
~/Documents/fall18/DBMS/...
*wlp2s0
DBMS - File Manager
[Terminal - lyn@XPS15: ~]
12:41 PM

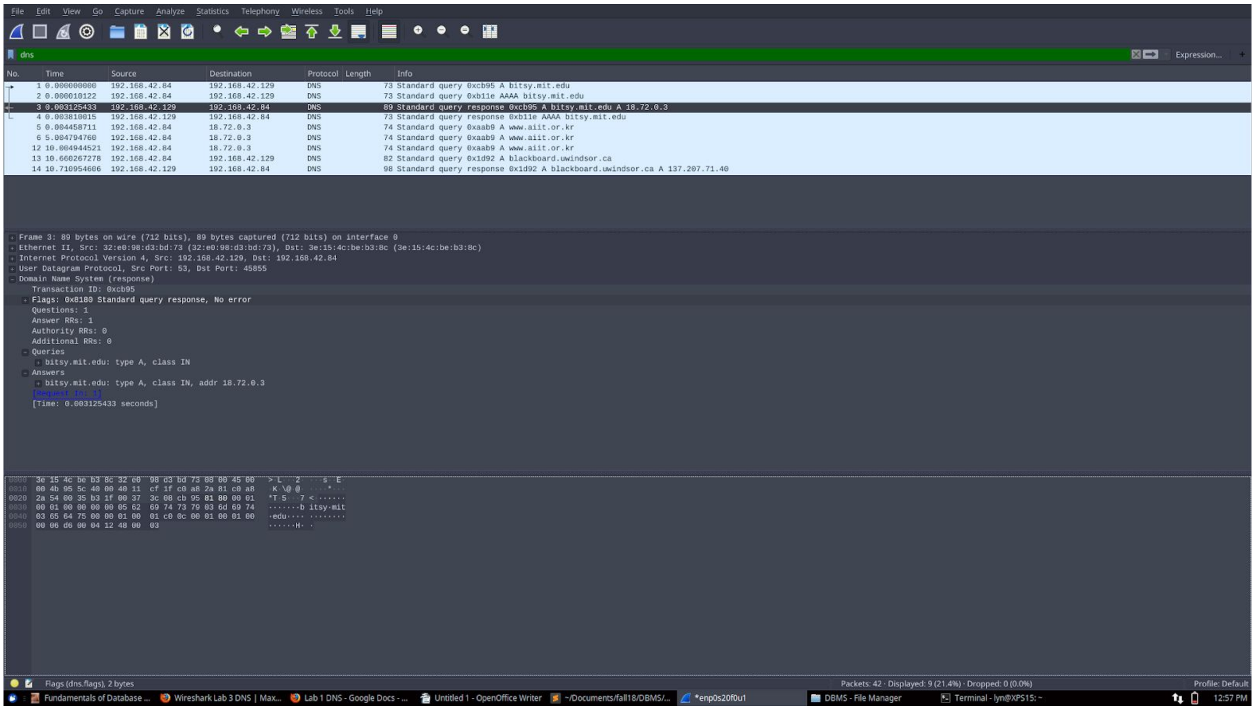
“nslookup www.aiit.or.kr bitsy.mit.edu”

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 message is sent to the IP address 192.168.42.129. This is the default local DNS server on my phone data connection.

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 type “A”. It does not contain any answers.

22. **Examine the DNS response message. How many “answers” are provided?/ What does each of these answers contain?**
    The DNS response message contains 1 answer. This answer contains the bitsy.mit.edu IP address, 18.72.0.3.

23. Provide a screenshot.


File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Expression...
Fundamentals of Database ...
Wireshark Lab 3 DNS | Max...
Lab 1 DNS - Google Docs - ...
Untitled 1 - OpenOffice Writer
~/Documents/fall18/DBMS/...
*enp0s20f0u1
DBMS - File Manager
Terminal - lyn@XPS15: ~
12:57 PM

dns

```
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   192.168.42.84    192.168.42.129   DNS          73 Standard query 0xcb95 A bitsy.mit.edu
    2 0.000010122   192.168.42.84    192.168.42.129   DNS          73 Standard query 0xb11e AAAA bitsy.mit.edu
    3 0.003125433   192.168.42.129   192.168.42.84    DNS          89 Standard query response 0xcb95 A bitsy.mit.edu A 18.72.0.3
    4 0.003810015   192.168.42.129   192.168.42.84    DNS          73 Standard query response 0xb11e AAAA bitsy.mit.edu
    5 0.004458711   192.168.42.84    18.72.0.3        DNS          74 Standard query 0xaab9 A www.aiit.or.kr
    6 5.004794760   192.168.42.84    18.72.0.3        DNS          74 Standard query 0xaab9 A www.aiit.or.kr
   12 10.004944521  192.168.42.84    18.72.0.3        DNS          74 Standard query 0xaab9 A www.aiit.or.kr
   13 10.660267278  192.168.42.84    192.168.42.129   DNS          82 Standard query 0x1d92 A blackboard.uwindsor.ca
   14 10.710954606  192.168.42.129   192.168.42.84    DNS          98 Standard query response 0x1d92 A blackboard.uwindsor.ca A 137.207.71.40
```

```
+ Frame 3: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
+ Ethernet II, Src: 32:e0:98:d3:bd:73 (32:e0:98:d3:bd:73), Dst: 3e:15:4c:be:b3:8c (3e:15:4c:be:b3:8c)
+ Internet Protocol Version 4, Src: 192.168.42.129, Dst: 192.168.42.84
+ User Datagram Protocol, Src Port: 53, Dst Port: 45855
- Domain Name System (response)
      Transaction ID: 0xcb95
    + Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 1
      Authority RRs: 0
      Additional RRs: 0
    - Queries
        + bitsy.mit.edu: type A, class IN
    - Answers
        + bitsy.mit.edu: type A, class IN, addr 18.72.0.3
      [Request In: 1]
      [Time: 0.003125433 seconds]
```

```
0000  3e 15 4c be b3 8c 32 e0  98 d3 bd 73 08 00 45 00   >·L···2· ···s··E·
0010  00 4b 95 5c 40 00 40 11  cf 1f c0 a8 2a 81 c0 a8   ·K·\@·@· ····*···
0020  2a 54 00 35 b3 1f 00 37  3c 08 cb 95 81 80 00 01   *T·5···7 <·······
0030  00 01 00 00 00 00 05 62  69 74 73 79 03 6d 69 74   ·······b itsy·mit
0040  03 65 64 75 00 00 01 00  01 c0 0c 00 01 00 01 00   ·edu···· ········
0050  00 06 d6 00 04 12 48 00  03                        ······H· ·
```

Flags (dns.flags), 2 bytes

Packets: 42 · Displayed: 9 (21.4%) · Dropped: 0 (0.0%)

Profile: Default