

Wireshark Lab: DNS v6.01

Vandré Leal Cândido

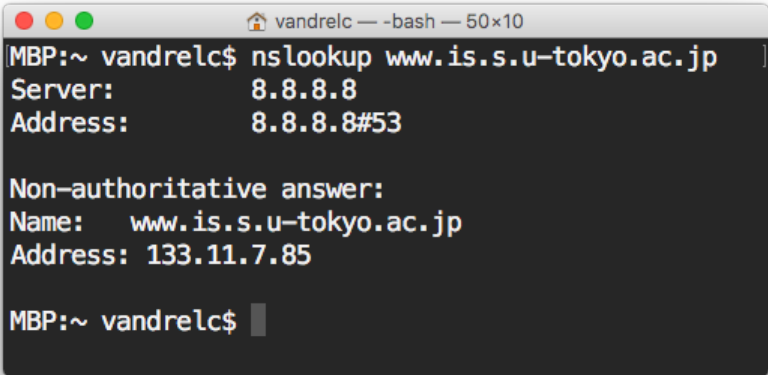
August 27, 2017

1 nslookup

- *Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?*

The IP address is 133.11.7.85

Figure 1: Question 01

A terminal window titled 'vandrele — -bash — 50x10' showing the execution of the 'nslookup www.is.s.u-tokyo.ac.jp' command. The output displays the server address as 8.8.8.8 and the non-authoritative answer for the domain as 133.11.7.85.

```
MBP:~ vandrele$ nslookup www.is.s.u-tokyo.ac.jp
Server:      8.8.8.8
Address:     8.8.8.8#53

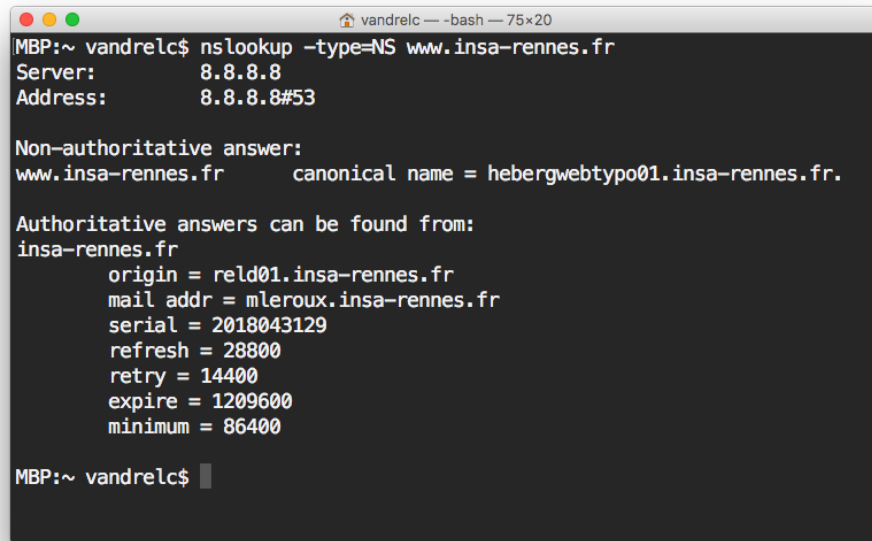
Non-authoritative answer:
Name:   www.is.s.u-tokyo.ac.jp
Address: 133.11.7.85

MBP:~ vandrele$
```

- Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

The authoritative DNS server is reld01.insa-rennes.fr.

Figure 2: Question 02



```
MBP:~ vandrelc$ nslookup -type=NS www.insa-rennes.fr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.insa-rennes.fr      canonical name = hebergwebtypo01.insa-rennes.fr.

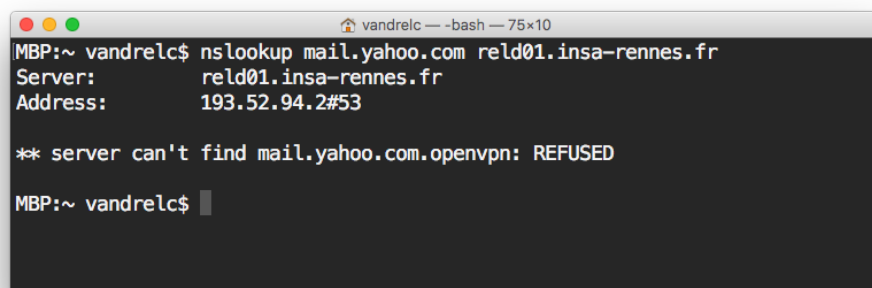
Authoritative answers can be found from:
insa-rennes.fr
  origin = reld01.insa-rennes.fr
  mail addr = mleroux.insa-rennes.fr
  serial = 2018043129
  refresh = 28800
  retry = 14400
  expire = 1209600
  minimum = 86400

MBP:~ vandrelc$
```

- 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?

The IP address is 193.52.94.2.

Figure 3: Question 03



```
MBP:~ vandrelc$ nslookup mail.yahoo.com reld01.insa-rennes.fr
Server:      reld01.insa-rennes.fr
Address:     193.52.94.2#53

** server can't find mail.yahoo.com.openvpn: REFUSED

MBP:~ vandrelc$
```

2 Tracing DNS with Wireshark

Figure 4: DNS Query Message

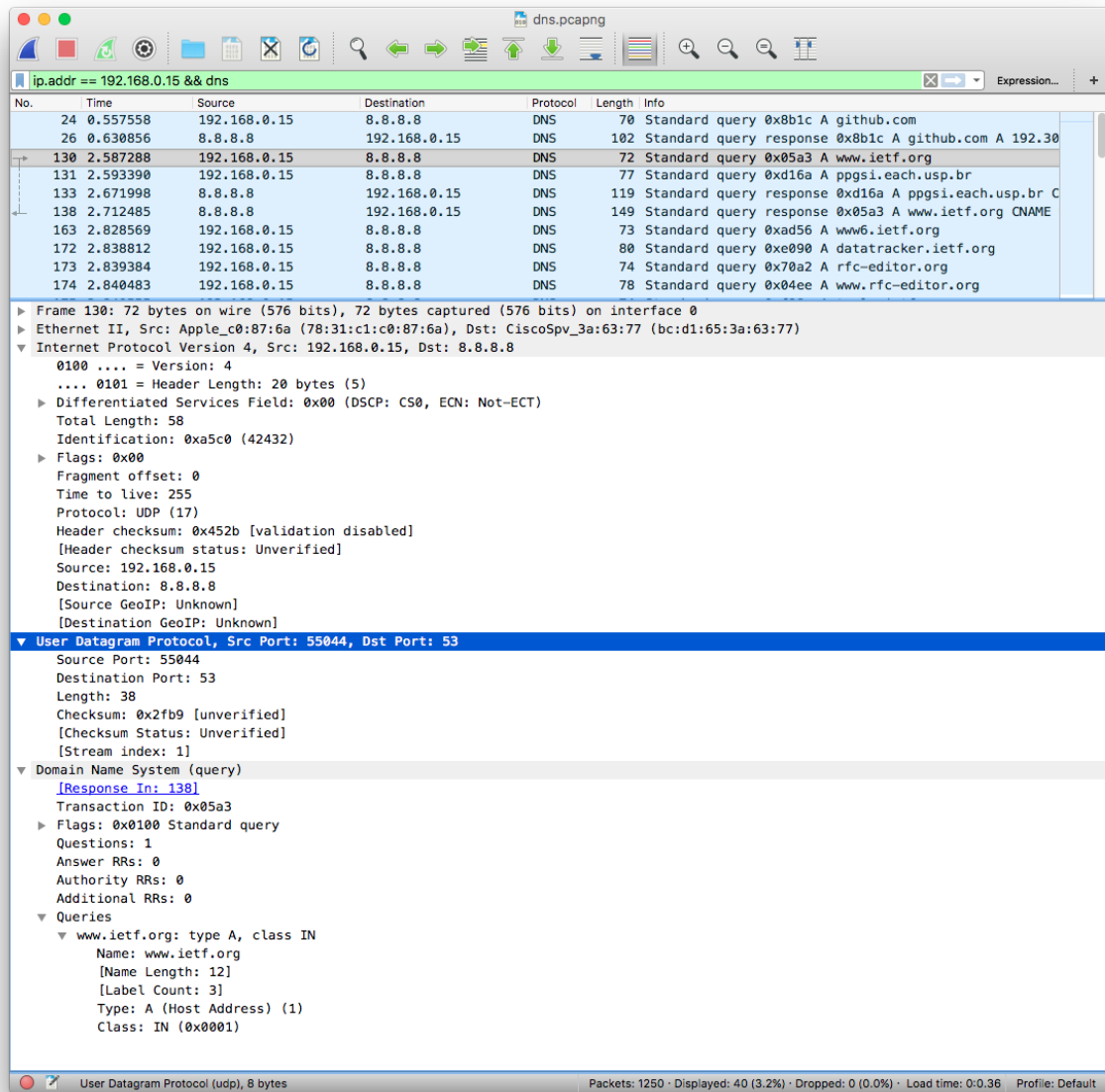


Figure 5: DNS Response Message

Filter: `ip.addr == 192.168.0.15 && dns`

No.	Time	Source	Destination	Protocol	Length	Info
24	0.557558	192.168.0.15	8.8.8.8	DNS	70	Standard query 0x8b1c A github.com
26	0.630856	8.8.8.8	192.168.0.15	DNS	102	Standard query response 0x8b1c A github.com A 192.30
130	2.587288	192.168.0.15	8.8.8.8	DNS	72	Standard query 0x05a3 A www.ietf.org
131	2.593390	192.168.0.15	8.8.8.8	DNS	77	Standard query 0xd16a A ppgsi.each.usp.br
133	2.671998	8.8.8.8	192.168.0.15	DNS	119	Standard query response 0xd16a A ppgsi.each.usp.br C
138	2.712485	8.8.8.8	192.168.0.15	DNS	149	Standard query response 0x05a3 A www.ietf.org CNAME
163	2.828569	192.168.0.15	8.8.8.8	DNS	73	Standard query 0xad56 A www6.ietf.org
172	2.838812	192.168.0.15	8.8.8.8	DNS	80	Standard query 0xe090 A datatracker.ietf.org
173	2.839384	192.168.0.15	8.8.8.8	DNS	74	Standard query 0x70a2 A rfc-editor.org
174	2.840483	192.168.0.15	8.8.8.8	DNS	78	Standard query 0x04ee A www.rfc-editor.org

Frame 138: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0

Ethernet II, Src: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77), Dst: Apple_c0:87:6a (78:31:c1:c0:87:6a)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.15

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 135
 Identification: 0xf910 (63760)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 44
 Protocol: UDP (17)
 Header checksum: 0xc48e [validation disabled]
 [Header checksum status: Unverified]
 Source: 8.8.8.8
 Destination: 192.168.0.15
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

User Datagram Protocol, Src Port: 53, Dst Port: 55044

Source Port: 53
 Destination Port: 55044
 Length: 115
 Checksum: 0xee9a [unverified]
 [Checksum Status: Unverified]
 [Stream index: 1]

Domain Name System (response)

[Request In: 130]
 [Time: 0.125197000 seconds]
 Transaction ID: 0x05a3
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 3
 Authority RRs: 0
 Additional RRs: 0

Queries

www.ietf.org: type A, class IN
 Name: www.ietf.org
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

User Datagram Protocol (udp), 8 bytes

Packets: 1250 · Displayed: 40 (3.2%) · Dropped: 0 (0.0%) · Load time: 0:0.36 · Profile: Default

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

Both the query and response messages are sent over UDP.

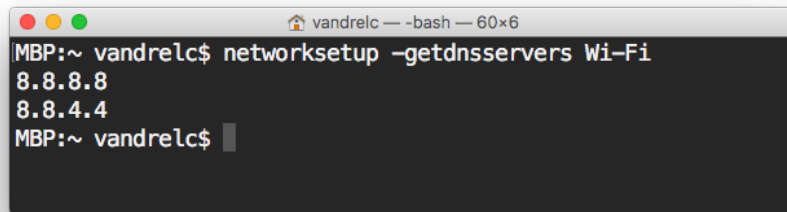
- *What is the destination port for the DNS query message? What is the source port of DNS response message?*

The destination port of the DNS query message is 53. The source port of the response message is also 53.

- *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 message is sent to 8.8.8.8, which is the IP address of one of the local DNS servers (Google DNS).

Figure 6: Local DNS servers



```
MBP:~ vandrelc$ networksetup -getdnsservers Wi-Fi
8.8.8.8
8.8.4.4
MBP:~ vandrelc$
```

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

It’s a standard query (Type A). It doesn’t contain any answers.

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

3 answers were provided. Each answer contains the following information: name of the host, type, class, TTL, data length and IP address.

Figure 7: DNS response answers

No.	Time	Source	Destination	Protocol	Length	Info
24	0.557558	192.168.0.15	8.8.8.8	DNS	70	Standard query 0x8b1c A github.com
26	0.630856	8.8.8.8	192.168.0.15	DNS	102	Standard query response 0x8b1c A github.com A 192.30
130	2.587288	192.168.0.15	8.8.8.8	DNS	72	Standard query 0x05a3 A www.ietf.org
131	2.593390	192.168.0.15	8.8.8.8	DNS	77	Standard query 0xd16a A ppgsi.each.usp.br
133	2.671998	8.8.8.8	192.168.0.15	DNS	119	Standard query response 0xd16a A ppgsi.each.usp.br C
138	2.712485	8.8.8.8	192.168.0.15	DNS	149	Standard query response 0x05a3 A www.ietf.org CNAME
163	2.828569	192.168.0.15	8.8.8.8	DNS	73	Standard query 0xad56 A www6.ietf.org
172	2.838812	192.168.0.15	8.8.8.8	DNS	80	Standard query 0xe090 A datatracker.ietf.org
173	2.839384	192.168.0.15	8.8.8.8	DNS	74	Standard query 0x70a2 A rfc-editor.org
174	2.840483	192.168.0.15	8.8.8.8	DNS	78	Standard query 0x04ee A www.rfc-editor.org

Checksum: 0xee9a [unverified]
[Checksum Status: Unverified]
[Stream index: 1]

▼ Domain Name System (response)

[Request In: 130]
[Time: 0.125197000 seconds]
Transaction ID: 0x05a3
Flags: 0x8180 Standard query response, No error

Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0

▼ Queries

▼ www.ietf.org: type A, class IN
Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

▼ Answers

▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
Name: www.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 979
Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net

▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 299
Data length: 4
Address: 104.20.0.85

▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 299
Data length: 4
Address: 104.20.1.85

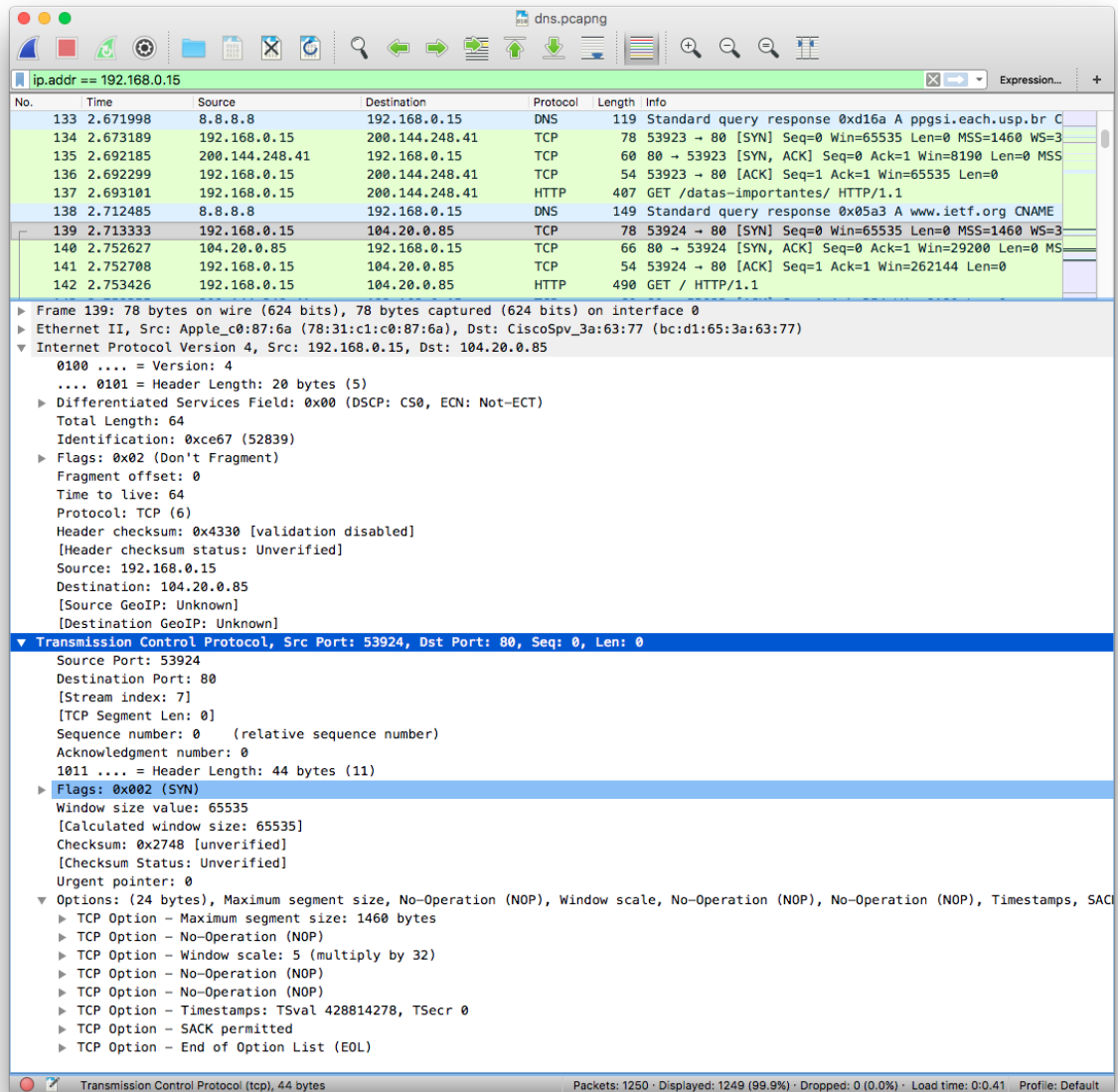
Text item (text), 77 bytes

Packets: 1250 · Displayed: 40 (3.2%) · Dropped: 0 (0.0%) · Load time: 0:0.36 · Profile: Default

- 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?

Yes, the first SYN packet was sent to 104.20.0.85 which is one of the IP addresses provided in the DNS response message.

Figure 8: TCP SYN packet



- This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No.

Now let's play with nslookup.

- Start packet capture.
- Do an nslookup on www.mit.edu
- Stop packet capture.

Figure 9: nslookup www.mit.edu (DNS Request)

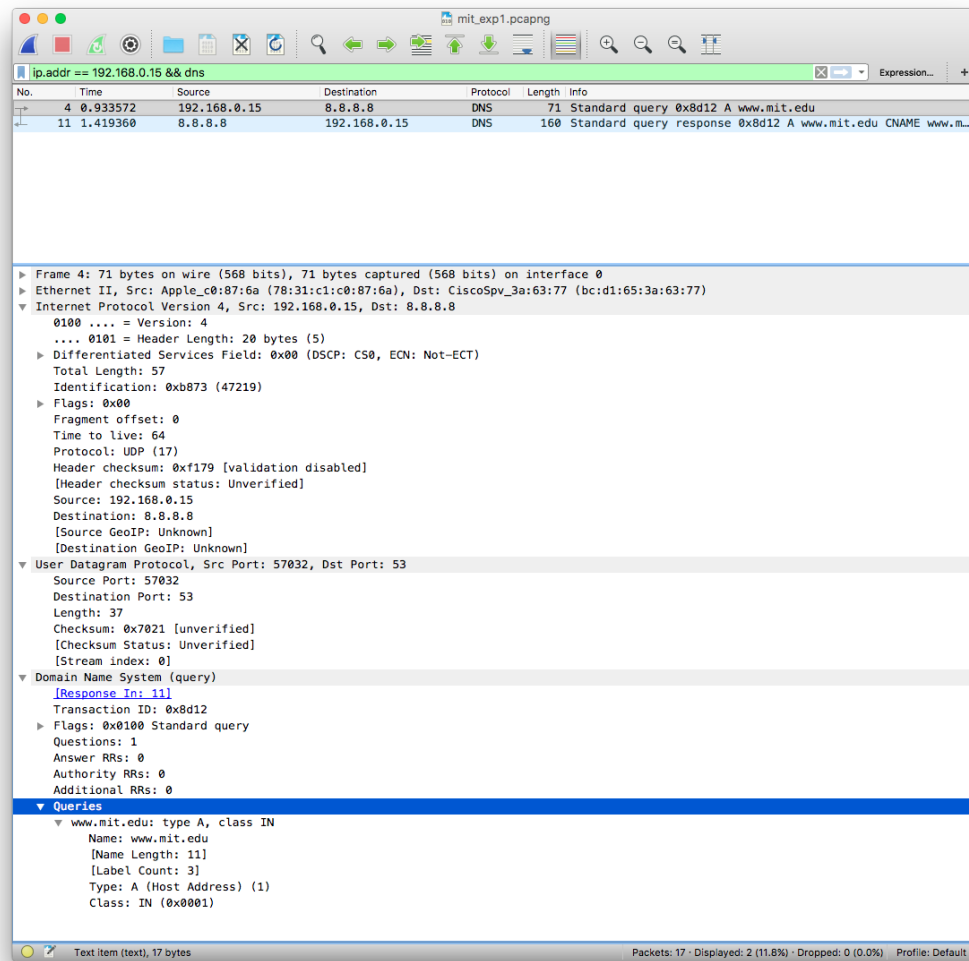
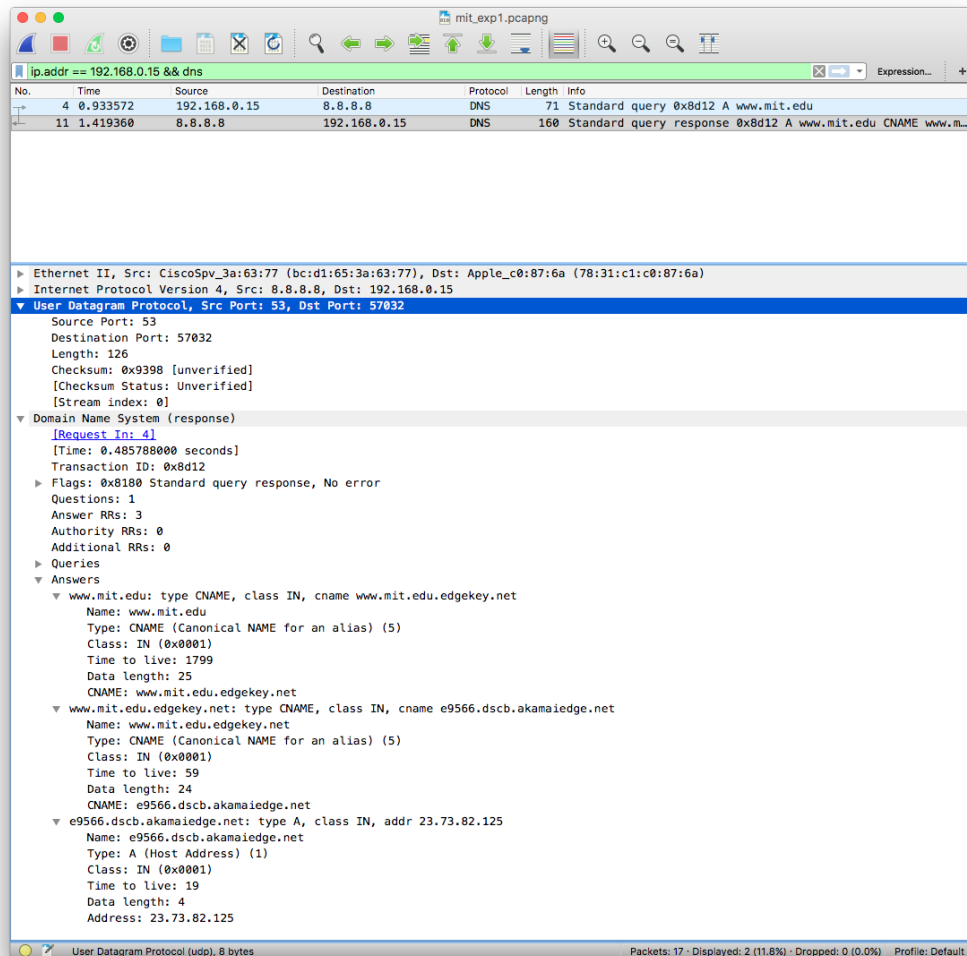


Figure 10: nslookup www.mit.edu (DNS Response)



- *What is the destination port for the DNS query message? What is the source port of DNS response message?*

The destination port of the DNS query message is 53. The source port of the response message is also 53.

- *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 8.8.8.8, which is the IP address of one of the local DNS servers.

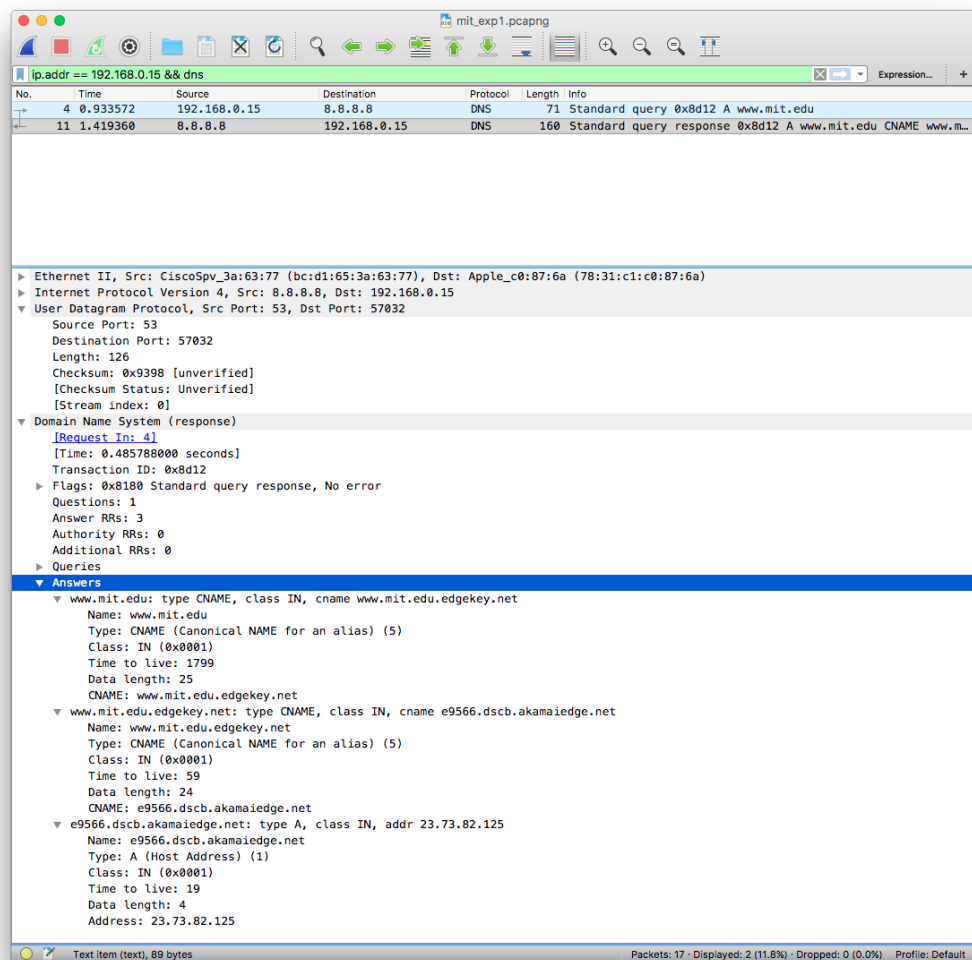
- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A. It doesn’t contain any answers.

- Provide a screenshot.

Figure 11.

Figure 11: nslookup www.mit.edu (DNS Response Answers)



Now repeat the previous experiment, but instead issue the command:

```
nslookup -type=NS mit.edu
```

Figure 12: nslookup -type=NS mit.edu (DNS Request)

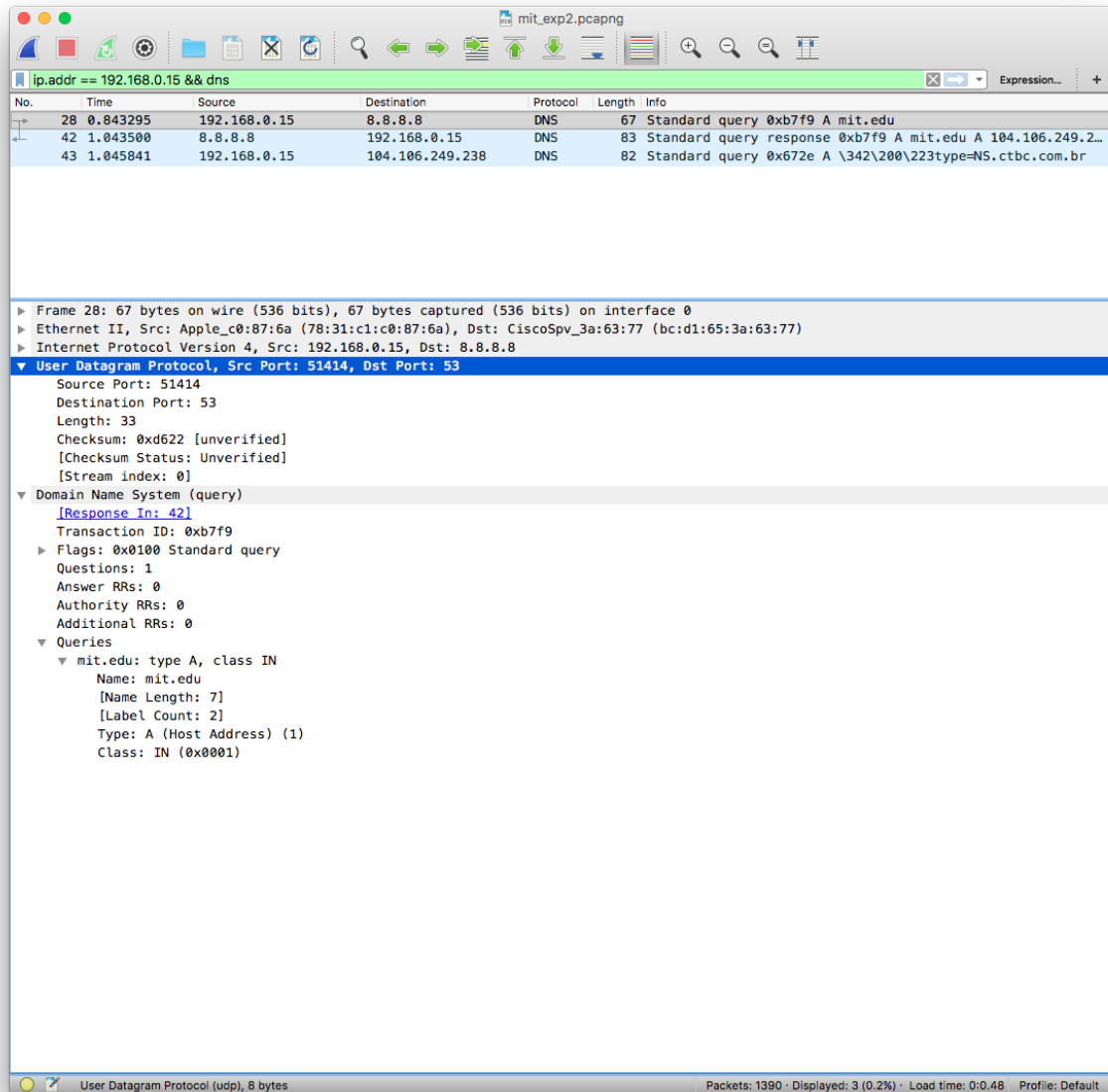


Figure 13: nslookup -type=NS mit.edu (DNS Response)

No.	Time	Source	Destination	Protocol	Length	Info
28	0.843295	192.168.0.15	8.8.8.8	DNS	67	Standard query 0xb7f9 A mit.edu
42	1.043500	8.8.8.8	192.168.0.15	DNS	83	Standard query response 0xb7f9 A mit.edu A 104.106.249.238
43	1.045841	192.168.0.15	104.106.249.238	DNS	82	Standard query 0xb72e A \342\200\223type=NS.ctbc.com.br

Frame 42: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

Ethernet II, Src: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77), Dst: Apple_c0:87:6a (78:31:c1:c0:87:6a)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.15

User Datagram Protocol, Src Port: 53, Dst Port: 51414

Source Port: 53
Destination Port: 51414
Length: 49
Checksum: 0xd65e [unverified]
[Checksum Status: Unverified]
[Stream index: 0]

Domain Name System (response)

[Request In: 28]
[Time: 0.200205000 seconds]
Transaction ID: 0xb7f9

Flags: 0x8180 Standard query response, No error

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries

mit.edu: type A, class IN
Name: mit.edu
Name Length: 7
Label Count: 2
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

mit.edu: type A, class IN, addr 104.106.249.238
Name: mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 19
Data length: 4
Address: 104.106.249.238

Text item (text), 16 bytes

Packets: 1390 - Displayed: 3 (0.2%)

Profile: Default

- *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 8.8.8.8, which is the IP address of one of the local DNS servers.

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

Type A. It doesn't contain any answers.

- *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 nameservers?*

The message provides an unique answer that provides info for the server name 'mit.edu' which address is 104.106.249.238.

- *Provide a screenshot.*

Figures 12 and 13.

Now repeat the previous experiment, but instead issue the command:
nslookup www.aiit.or.kr bitsy.mit.edu

Figure 14: nslookup www.aiit.or.kr bitsy.mit.edu (DNS Request)

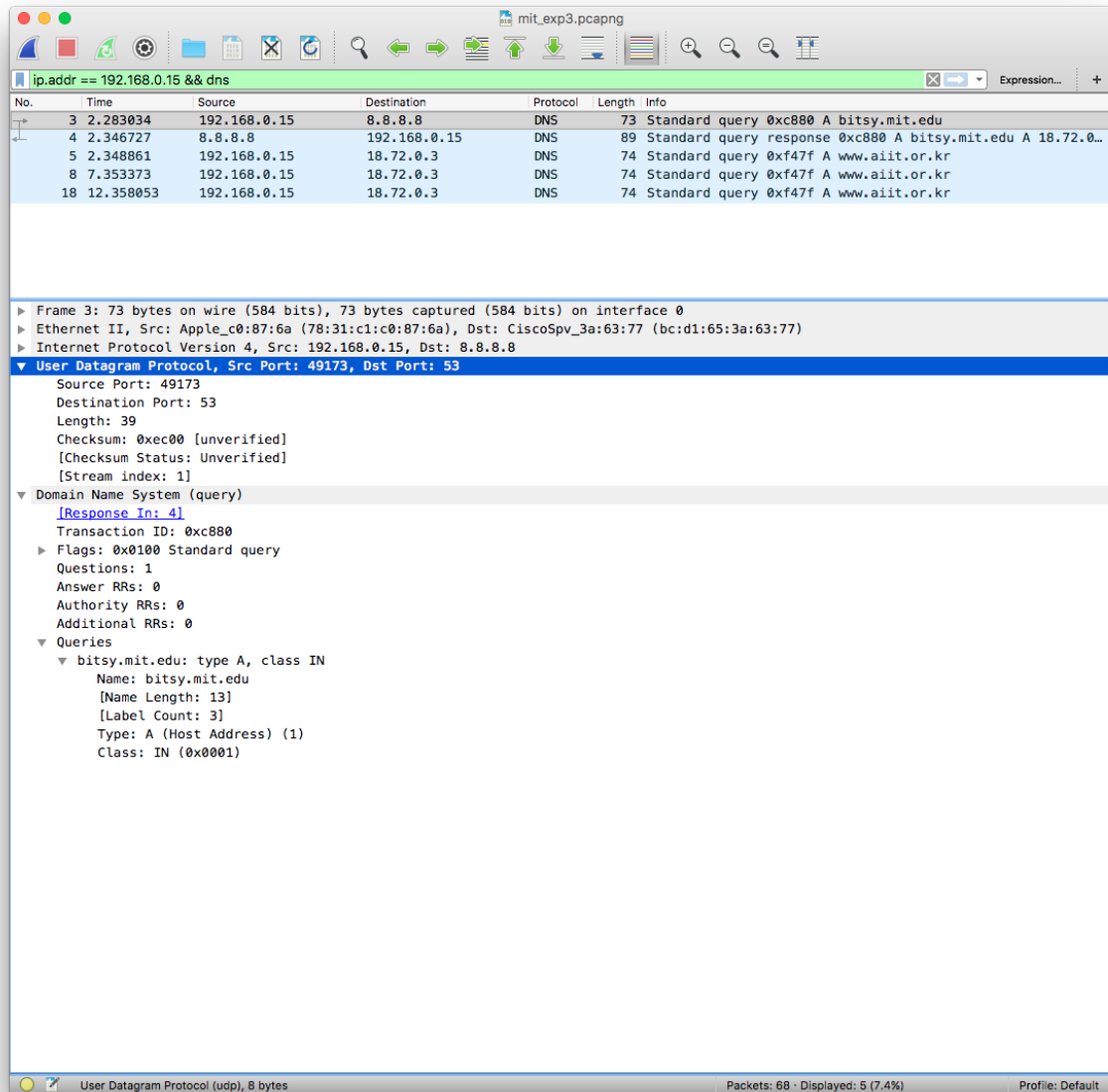
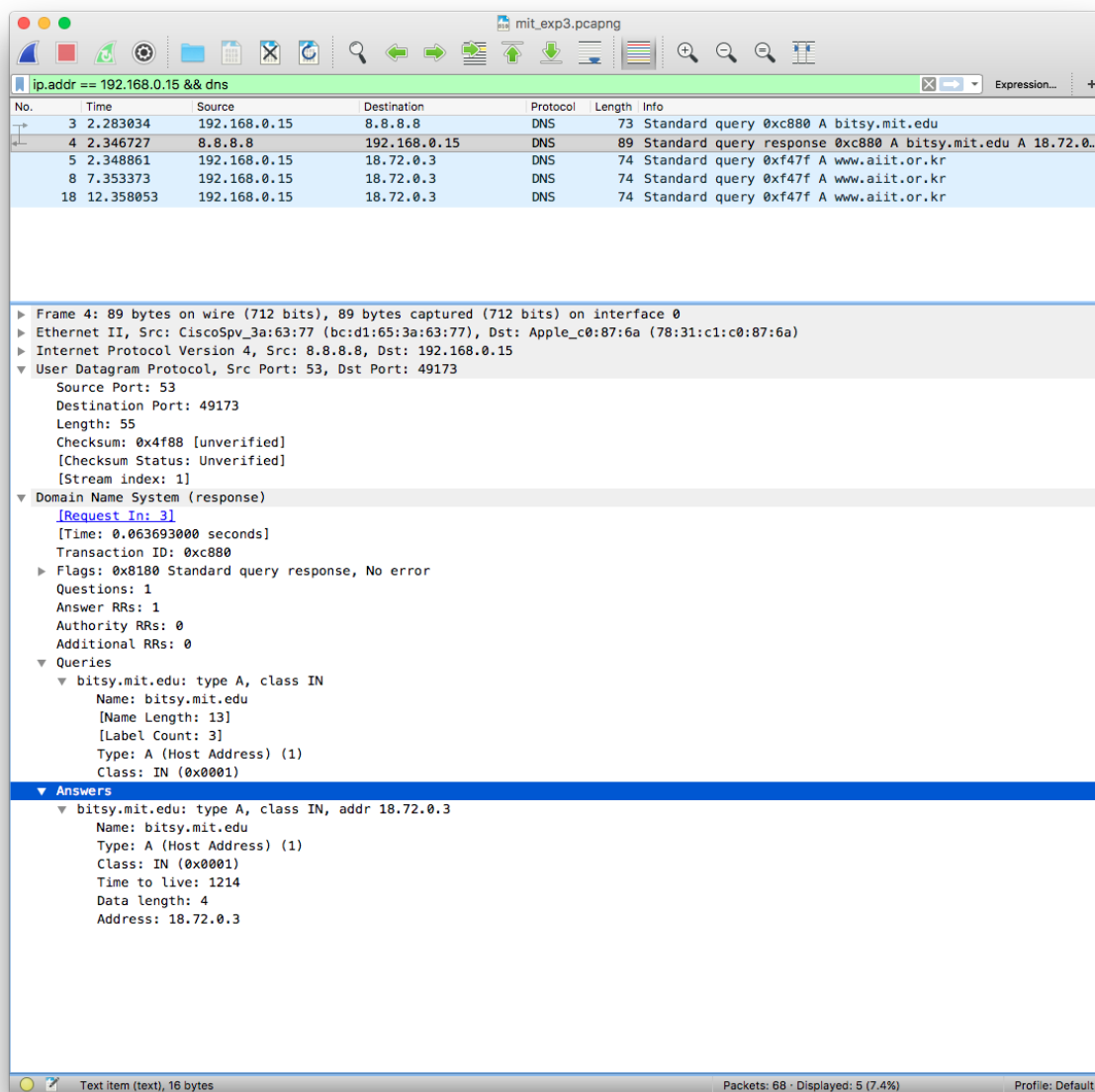


Figure 15: nslookup www.aiit.or.kr bitsy.mit.edu (DNS Response)



No.	Time	Source	Destination	Protocol	Length	Info
3	2.283034	192.168.0.15	8.8.8.8	DNS	73	Standard query 0xc880 A bitsy.mit.edu
4	2.346727	8.8.8.8	192.168.0.15	DNS	89	Standard query response 0xc880 A bitsy.mit.edu A 18.72.0...
5	2.348861	192.168.0.15	18.72.0.3	DNS	74	Standard query 0xf47f A www.aiit.or.kr
8	7.353373	192.168.0.15	18.72.0.3	DNS	74	Standard query 0xf47f A www.aiit.or.kr
18	12.358053	192.168.0.15	18.72.0.3	DNS	74	Standard query 0xf47f A www.aiit.or.kr

Frame 4: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0

Ethernet II, Src: CiscoSpv_3a:63:77 (bc:d1:65:3a:63:77), Dst: Apple_c0:87:6a (78:31:c1:c0:87:6a)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.15

User Datagram Protocol, Src Port: 53, Dst Port: 49173

Source Port: 53
Destination Port: 49173
Length: 55
Checksum: 0x4f88 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]

Domain Name System (response)

[Request In: 3]
[Time: 0.063693000 seconds]
Transaction ID: 0xc880

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
Name: bitsy.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

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: 1214
Data length: 4
Address: 18.72.0.3

- *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 8.8.8.8, which is the IP address of one of the local DNS servers.

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

Type A. It doesn't contain any answers.

- *Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?*

Only one answer is provided. The answer contains the following information: name of the host, type, class, TTL, data length and IP address.

- *Provide a screenshot.*

Figures 14 and 15.