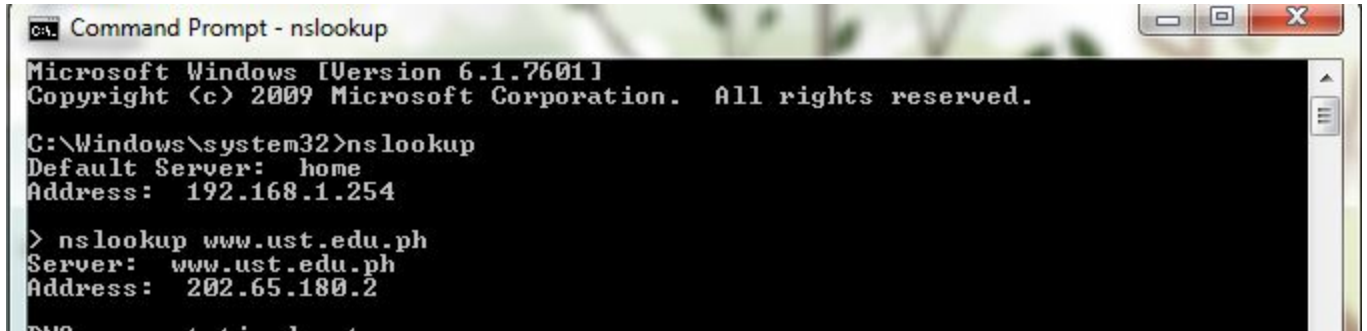


Wireshark Lab # 3 DNS

1. Run *nslookup* to obtain the IP address of a Web server in Asia.

Answer: I chose www.ust.edu.ph - a university in the Philippines.



```
C:\> Command Prompt - nslookup

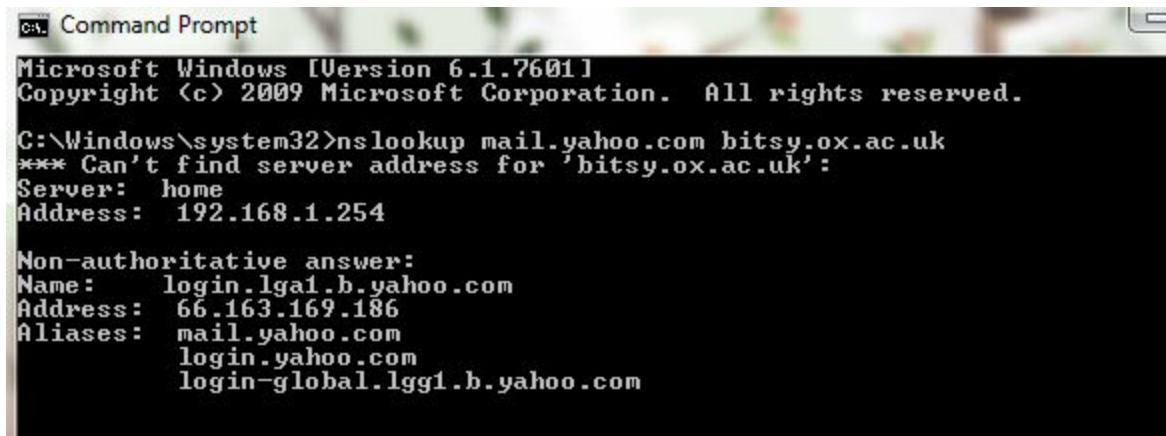
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server: home
Address: 192.168.1.254

> nslookup www.ust.edu.ph
Server: www.ust.edu.ph
Address: 202.65.180.2
```

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

Answer: I performed nslookup for University of Oxford.



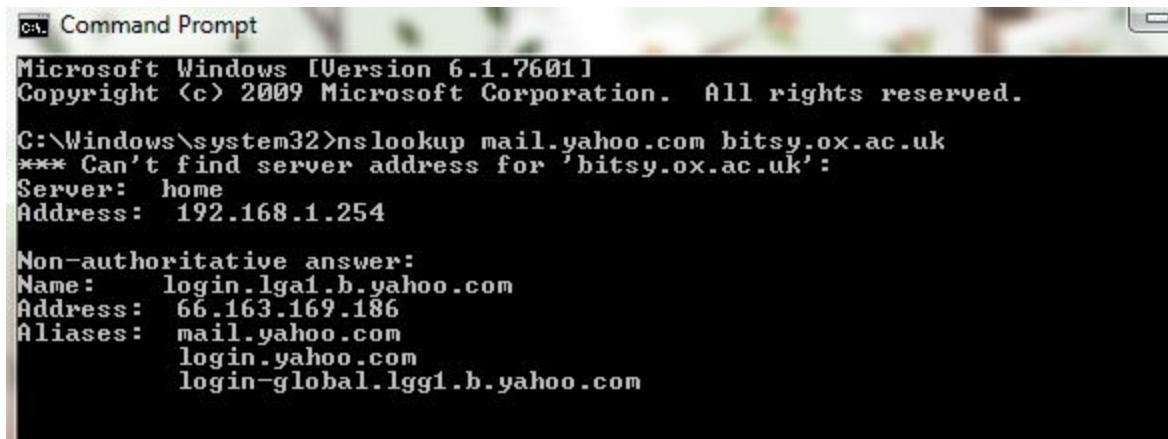
```
C:\> Command Prompt

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup mail.yahoo.com bitsy.ox.ac.uk
*** Can't find server address for 'bitsy.ox.ac.uk':
Server: home
Address: 192.168.1.254

Non-authoritative answer:
Name: login.lga1.b.yahoo.com
Address: 66.163.169.186
Aliases: mail.yahoo.com
login.yahoo.com
login-global.lgg1.b.yahoo.com
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is required for the mail servers for Yahoo! mail.



```
C:\> Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup mail.yahoo.com bitsy.ox.ac.uk
*** Can't find server address for 'bitsy.ox.ac.uk':
Server: home
Address: 192.168.1.254

Non-authoritative answer:
Name: login.lga1.b.yahoo.com
Address: 66.163.169.186
Aliases: mail.yahoo.com
          login.yahoo.com
          login-global.lgg1.b.yahoo.com
```

Microsoft [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==192.168.1.254` Expression... Clear Apply

Source	Destination	Protocol	Length	Info
192.168.1.254	192.168.1.66	DNS	92	Standard query response, refused
2.168.1.66	192.168.1.254	DNS	554	Standard query response, refused
2.168.1.254	192.168.1.66	DNS	74	Standard query A mail.yahoo.com
2.168.1.66	192.168.1.254	DNS	169	Standard query response CNAME login.yahoo.com CNAME login-global.1
2.168.1.254	192.168.1.66	DNS	74	Standard query AAAA mail.yahoo.com
2.168.1.66	192.168.1.254	DNS	214	Standard query response CNAME login.yahoo.com CNAME login-global.1

Frame 164: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: IntelCor_44:46:1c (40:25:c2:44:46:1c), Dst: 2wire_7f:0c:21 (00:18:3f:7f:0c:21)

Internet Protocol Version 4, Src: 192.168.1.66 (192.168.1.66), Dst: 192.168.1.254 (192.168.1.254)

User Datagram Protocol, Src Port: 51340 (51340), Dst Port: domain (53)

Domain Name System (query)

[\[Response In: 169\]](#)

Transaction ID: 0x0004

Flags: 0x0100 (Standard query)

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- mail.yahoo.com: type A, class IN
 - Name: mail.yahoo.com
 - Type: A (Host address)
 - Class: IN (0x0001)

Microsoft [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==192.168.1.254` Expression... Clear Apply

Source	Destination	Protocol	Length	Info
192.168.1.66	192.168.1.254	DNS	92	Standard query response, Refused
192.168.1.254	192.168.1.66	DNS	554	Standard query response, Refused
192.168.1.66	192.168.1.254	DNS	74	Standard query A mail.yahoo.com
192.168.1.254	192.168.1.66	DNS	169	Standard query response CNAME login.yahoo.com CNAME login-global.
192.168.1.66	192.168.1.254	DNS	74	Standard query AAAA mail.yahoo.com
192.168.1.254	192.168.1.66	DNS	214	Standard query response CNAME login.yahoo.com CNAME login-global.

Frame 169: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits)

Ethernet II, Src: 2wire_7f:0c:21 (00:18:3f:7f:0c:21), Dst: IntelCor_44:46:1c (40:25:c2:44:46:1c)

Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.66 (192.168.1.66)

User Datagram Protocol, Src Port: domain (53), Dst Port: 51340 (51340)

Domain Name System (response)

[Request In: 164]

[Time: 0.112236000 seconds]

Transaction ID: 0x0004

Flags: 0x8180 (standard query response, No error)

Questions: 1

Answer RRs: 4

Authority RRs: 0

Additional RRs: 0

Queries

mail.yahoo.com: type A, class IN

Name: mail.yahoo.com

Type: A (Host address)

class: IN (0x0001)

0000 40 25 c2 44 46 1c 00 18 3f 7f 0c 21 08 00 45 00 @%.DF... ?..!...E.

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

Answer: They were sent over using UDP.

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

Answer: The destination port for query message is 53 and the source port of DNS response message is 53.

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

Answer: The DNS query message was sent to 192.168.1.254. Using *ipconfig*, I got my local DNS server and it appears to me that it is the same as the DNS query message was sent.

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answer"?

Answer: Domain Name System (query)

Transaction ID: 0x914f

Flags: 0x0100 (Standard query)

Questions: 1

Answer RRS: 0

It is Standard Query Type and it doesn't have any "answer" in the query message.

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

Answer: There are 2 answers in the DNS response message. Both of them contains the name of the host, type, class, time to live, data length and address.

```
www.ie: type A, class IN, addr 81.17.252.188
  Name: www.ie
  Type: A (Host address)
  Class: IN (0x0001)
  Time to live: 1 hour
  Data length: 4
  Addr: 81.17.252.188
www.ie: type A, class IN, addr 78.153.21.173
  Name: www.ie
  Type: A (Host address)
  Class: IN (0x0001)
  Time to live: 1 hour
  Data length: 4
  Addr: 78.153.21.173
```

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?

Answer: The first SYN packet sent by my host is 81.17.252.188. which corresponds to the first IP address provided in the DNS response message.

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

Answer: No.

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

Answer: The DNS query message destination port is 53 and the source port of 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?

Answer: The DNS query message was sent to 192.168.254. Based on *ipconfig*, yes it is 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”?

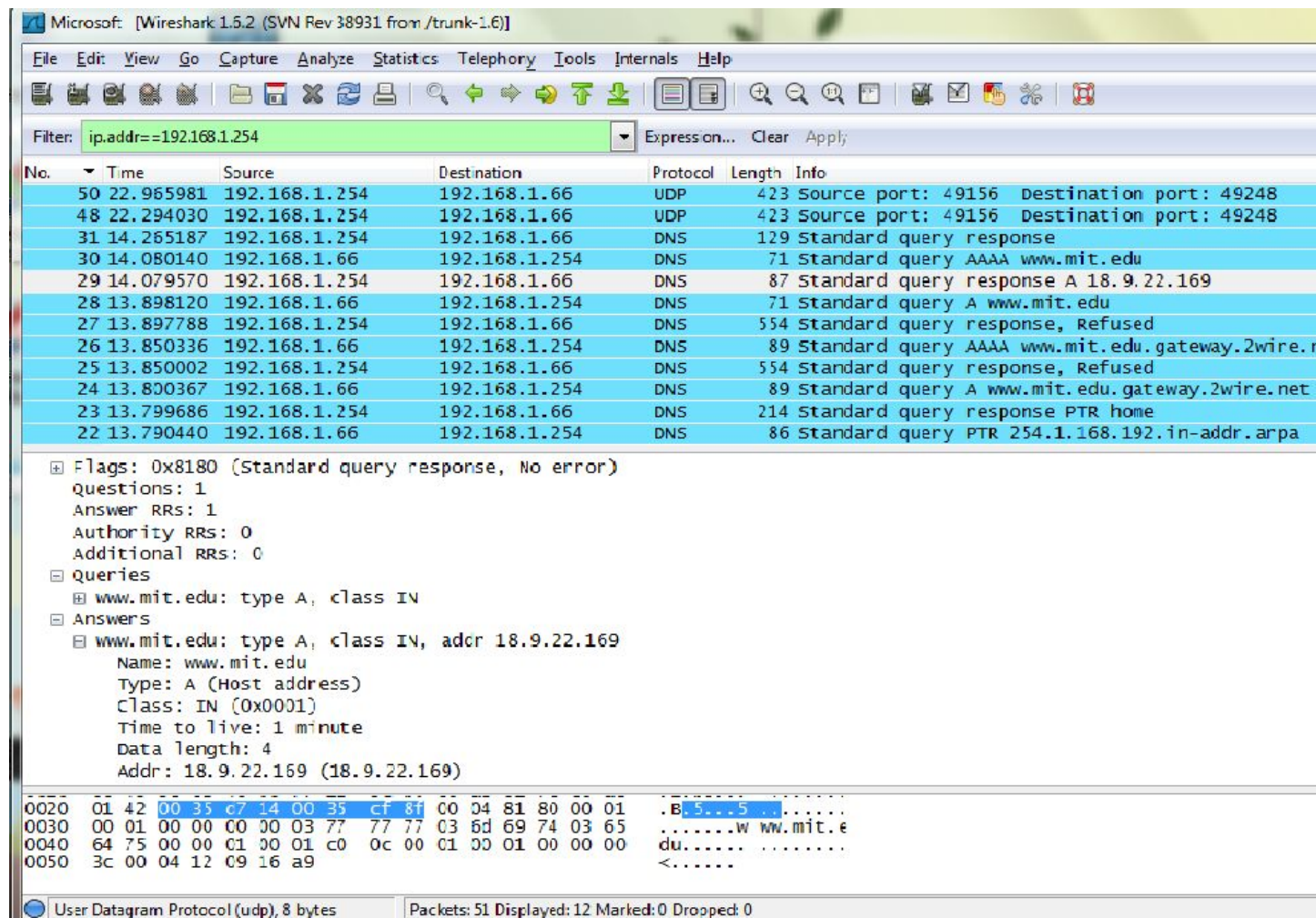
Answer: The “Type” of DNS query message is Type: A. No it does not contain any answer.

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

Answer: There is only one “answer” shown. It contains... It contains the name of the host, type, class, time to live, data length and addr.

```
www.mit.edu: type A, class IN, addr 18.9.22.169
Name: www.mit.edu
Type: A (host address)
Class: IN (0x0001)
Time to live: 1 minute
Data length: 4
Addr. 18.9.22.169
```


15. Provide a screen



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

Answer: The DNS query message was sent to 192.168.1.254 which is my default local DNS server.

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

Answer: The “Type” of DNS query message is NS and it does not contain any “answer”
Type: NS (Authoritative name server)

18. Examine the DNS response message. What MIT name servers does the response message provided? Does this response message also provide the IP addresses of the MIT name servers?

Answers: The MIT name servers are ns STRAWB, ns BITSY, and ns W2ONS.

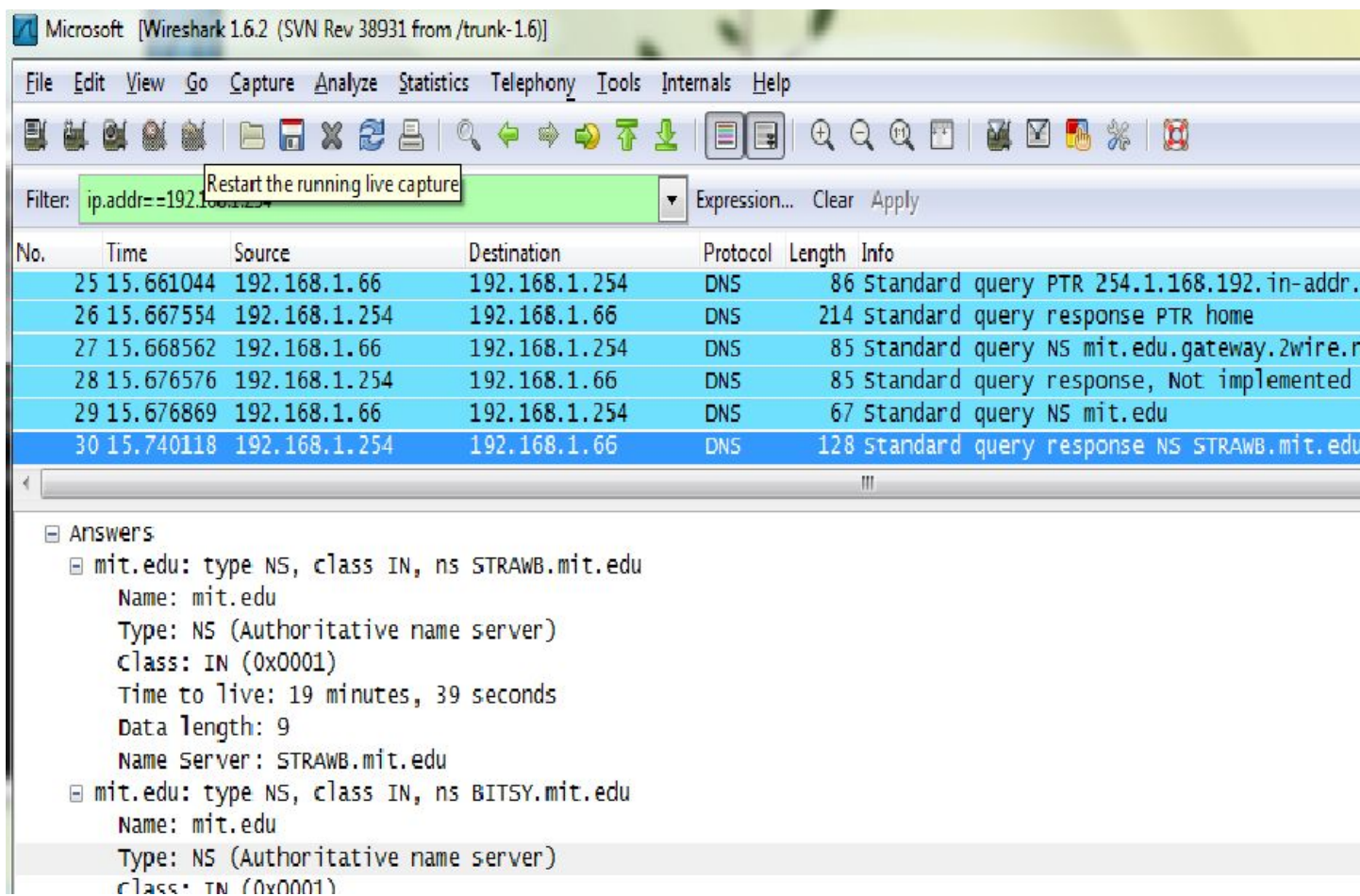
mit.edu:type NS, Class IN, ns STRAWB.mit.edu

mit.edu:type NS, Class IN, ns BISTY.mit.edu

mit.edu:type NS, Class IN, ns W2ONS.mit.edu

By clicking the plus sign in the Additional button, it's gonna show more information about it including the IP addresses.

19. Provide screenshot.



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?

Answers: The IP address was sent to 18.72.0.3 which corresponds to the
Server: BITSY.MIT.EDU.

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

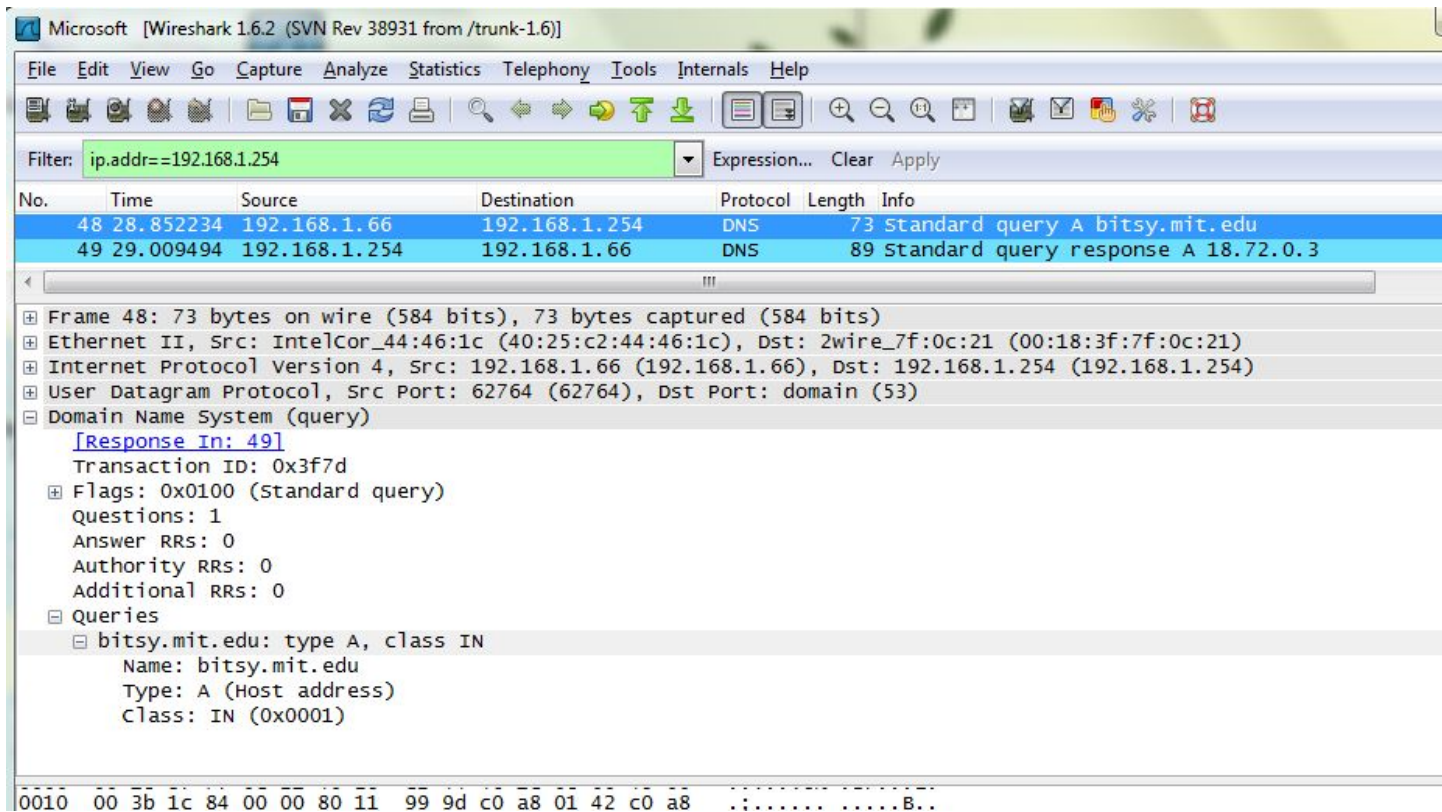
Answers: The Type of DNS is Standard DNS query and it does not contain any “answer”.

22. Examine the DNS response message. How many answers are provided? What does each of these answers contain?

Answers: There is only one “answer” shown. It contains the name of the host, type, and class.

Name: bitsy.mit.edu
Type: A (Host address)
Class: IN (0x0001)

23. Provide screenshot.



Microsoft [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==192.168.1.254` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
48	28.852234	192.168.1.66	192.168.1.254	DNS	73	Standard query A bitsy.mit.edu
49	29.009494	192.168.1.254	192.168.1.66	DNS	89	Standard query response A 18.72.0.3

Frame 49: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)

- Ethernet II, Src: 2wire_7f:0c:21 (00:18:3f:7f:0c:21), Dst: IntelCor_44:46:1c (40:25:c2:44:46:1c)
- Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.66 (192.168.1.66)
- User Datagram Protocol, Src Port: domain (53), Dst Port: 62764 (62764)
- Domain Name System (response)
 - [\[Request In: 48\]](#)
 - [Time: 0.157260000 seconds]
 - Transaction ID: 0x3f7d
 - 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
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Answers

```

0000  40 25 c2 44 46 1c 00 18  3f 7f 0c 21 08 00 45 00  @%.DF... ?...!..E.
0010  00 4b 89 cf 40 00 ff 11  6d 41 c0 a8 01 fe c0 a8  .K..@... mA.....
0020  01 42 00 35 f5 2c 00 37  fb ab 3f 7d 81 80 00 01  .B.5.,.7 ..?}....

```