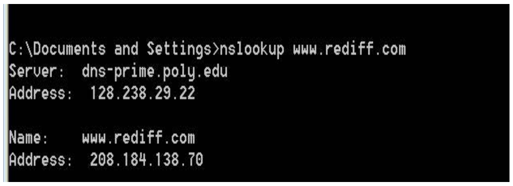
Ethereal Lab: DNS

PART 1

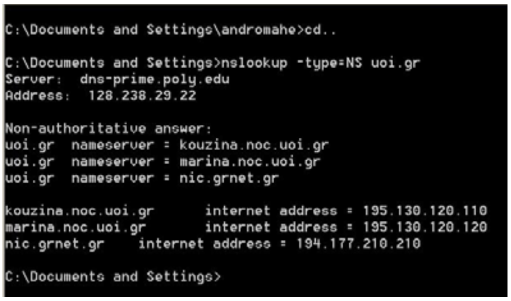
1.Run *nslookup* to obtain the IP address of a Web server in Asia.
I performed nslookup for www.rediff.com



```
C:\Documents and Settings>nslookup www.rediff.com
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.rediff.com
Address:  208.184.138.70
```

Screenshot taken after question 1

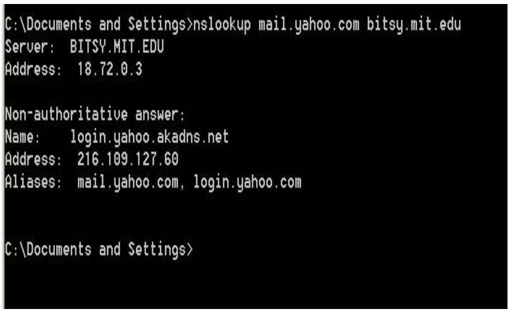
2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.
I performed nslookup for a European University in Ioannina Greece



```
C:\Documents and Settings\andromahe>cd..

C:\Documents and Settings>nslookup -type=NS uoi.gr
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
uoi.gr  nameserver = kouzina.noc.uoi.gr
uoi.gr  nameserver = marina.noc.uoi.gr
uoi.gr  nameserver = nic.grnet.gr

kouzina.noc.uoi.gr      internet address = 195.130.120.110
marina.noc.uoi.gr       internet address = 195.130.120.120
nic.grnet.gr    internet address = 194.177.210.210

C:\Documents and Settings>
```

Screenshot taken after question 2

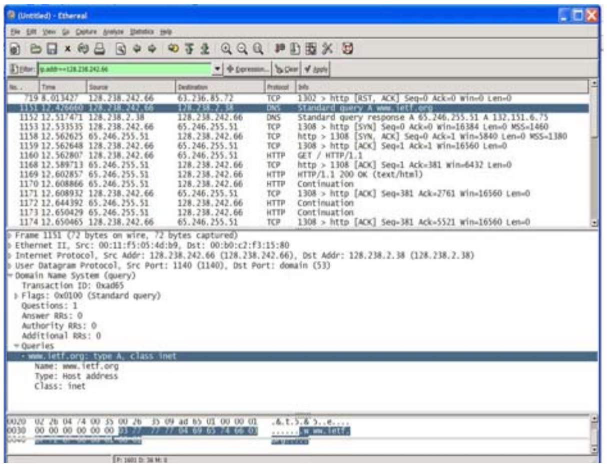
3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.



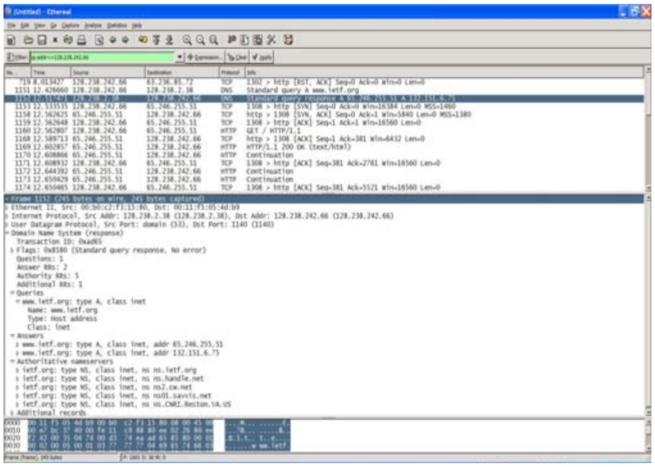
```
C:\Documents and Settings>nslookup mail.yahoo.com bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    login.yahoo.akadns.net
Address:  216.109.127.60
Aliases:  mail.yahoo.com, login.yahoo.com


C:\Documents and Settings>
```

Screenshot taken after question 3

PART 2


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr==128.238.242.66
Expression... Clear Apply

```
No. . Time      Source          Destination     Protocol Info
  719 8.013427  128.238.242.66  63.236.85.72    TCP      1302 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
 1151 12.426660 128.238.242.66  128.238.2.38    DNS      Standard query A www.ietf.org
 1152 12.517471 128.238.2.38    128.238.242.66  DNS      Standard query response A 65.246.255.51 A 132.151.6.75
 1153 12.533535 128.238.242.66  65.246.255.51   TCP      1308 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
 1158 12.562625 65.246.255.51   128.238.242.66  TCP      http > 1308 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
 1159 12.562648 128.238.242.66  65.246.255.51   TCP      1308 > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
 1160 12.562807 128.238.242.66  65.246.255.51   HTTP     GET / HTTP/1.1
 1168 12.589713 65.246.255.51   128.238.242.66  TCP      http > 1308 [ACK] Seq=1 Ack=381 Win=6432 Len=0
 1169 12.602857 65.246.255.51   128.238.242.66  HTTP     HTTP/1.1 200 OK (text/html)
 1170 12.608866 65.246.255.51   128.238.242.66  HTTP     Continuation
 1171 12.608932 128.238.242.66  65.246.255.51   TCP      1308 > http [ACK] Seq=381 Ack=2761 Win=16560 Len=0
 1172 12.644392 65.246.255.51   128.238.242.66  HTTP     Continuation
 1173 12.650429 65.246.255.51   128.238.242.66  HTTP     Continuation
 1174 12.650465 128.238.242.66  65.246.255.51   TCP      1308 > http [ACK] Seq=381 Ack=5521 Win=16560 Len=0

▷ Frame 1151 (72 bytes on wire, 72 bytes captured)
▷ Ethernet II, Src: 00:11:f5:05:4d:b9, Dst: 00:b0:c2:f3:15:80
▷ Internet Protocol, Src Addr: 128.238.242.66 (128.238.242.66), Dst Addr: 128.238.2.38 (128.238.2.38)
▷ User Datagram Protocol, Src Port: 1140 (1140), Dst Port: domain (53)
▽ Domain Name System (query)
    Transaction ID: 0xad65
  ▷ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ www.ietf.org: type A, class inet
        Name: www.ietf.org
        Type: Host address
        Class: inet

0020  02 26 04 74 00 35 00 26  35 09 ad 65 01 00 00 01   .&.t.5.&5..e....
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ......w ww.ietf.
```

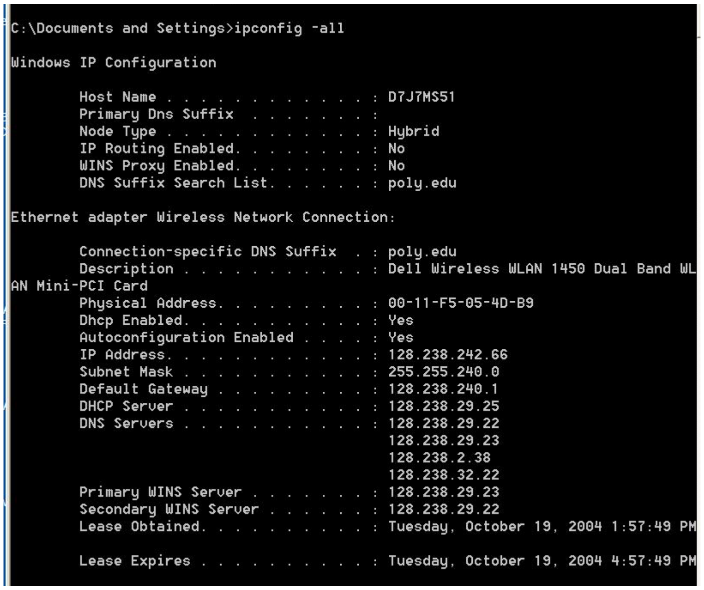

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr==128.238.242.66
Expression... Clear Apply

```
No. . Time      Source          Destination     Protocol Info
  719 8.013427  128.238.242.66  63.236.85.72    TCP      1302 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
 1151 12.426660 128.238.242.66  128.238.2.38    DNS      Standard query A www.ietf.org
 1152 12.517471 128.238.2.38    128.238.242.66  DNS      Standard query response A 65.246.255.51 A 132.151.6.75
 1153 12.533535 128.238.242.66  65.246.255.51   TCP      1308 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
 1158 12.562625 65.246.255.51   128.238.242.66  TCP      http > 1308 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
 1159 12.562648 128.238.242.66  65.246.255.51   TCP      1308 > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
 1160 12.562807 128.238.242.66  65.246.255.51   HTTP     GET / HTTP/1.1
 1168 12.589713 65.246.255.51   128.238.242.66  TCP      http > 1308 [ACK] Seq=1 Ack=381 Win=6432 Len=0
 1169 12.602857 65.246.255.51   128.238.242.66  HTTP     HTTP/1.1 200 OK (text/html)
 1170 12.608866 65.246.255.51   128.238.242.66  HTTP     Continuation
 1171 12.608932 128.238.242.66  65.246.255.51   TCP      1308 > http [ACK] Seq=381 Ack=2761 Win=16560 Len=0
 1172 12.644392 65.246.255.51   128.238.242.66  HTTP     Continuation
 1173 12.650429 65.246.255.51   128.238.242.66  HTTP     Continuation
 1174 12.650465 128.238.242.66  65.246.255.51   TCP      1308 > http [ACK] Seq=381 Ack=5521 Win=16560 Len=0

▷ Frame 1152 (245 bytes on wire, 245 bytes captured)
▷ Ethernet II, Src: 00:b0:c2:f3:15:80, Dst: 00:11:f5:05:4d:b9
▷ Internet Protocol, Src Addr: 128.238.2.38 (128.238.2.38), Dst Addr: 128.238.242.66 (128.238.242.66)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 1140 (1140)
▽ Domain Name System (response)
    Transaction ID: 0xad65
  ▷ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 5
    Additional RRs: 1
  ▽ Queries
    ▽ www.ietf.org: type A, class inet
        Name: www.ietf.org
        Type: Host address
        Class: inet
  ▽ Answers
    ▷ www.ietf.org: type A, class inet, addr 65.246.255.51
    ▷ www.ietf.org: type A, class inet, addr 132.151.6.75
  ▽ Authoritative nameservers
    ▷ ietf.org: type NS, class inet, ns ns.ietf.org
    ▷ ietf.org: type NS, class inet, ns ns.handle.net
    ▷ ietf.org: type NS, class inet, ns ns2.cw.net
    ▷ ietf.org: type NS, class inet, ns ns01.savvis.net
    ▷ ietf.org: type NS, class inet, ns ns.CNRI.Reston.VA.US
  ▷ Additional records
```

Screenshot for DNS query *Screenshot for DNS response*

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

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



```
C:\Documents and Settings>ipconfig -all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : D7J7MS51
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : poly.edu

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . : poly.edu
        Description . . . . . . . . . . . : Dell Wireless WLAN 1450 Dual Band WL
AN Mini-PCI Card
        Physical Address. . . . . . . . . : 00-11-F5-05-4D-B9
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 128.238.242.66
        Subnet Mask . . . . . . . . . . . : 255.255.240.0
        Default Gateway . . . . . . . . . : 128.238.240.1
        DHCP Server . . . . . . . . . . . : 128.238.29.25
        DNS Servers . . . . . . . . . . . : 128.238.29.22
                                            128.238.29.23
                                            128.238.2.38
                                            128.238.32.22
        Primary WINS Server . . . . . . . : 128.238.29.23
        Secondary WINS Server . . . . . . : 128.238.29.22
        Lease Obtained. . . . . . . . . . : Tuesday, October 19, 2004 1:57:49 PM

        Lease Expires . . . . . . . . . . : Tuesday, October 19, 2004 4:57:49 PM
```

Screenshot for ipconfig –all

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?
It's sent to 128.238.2.38 which is the IP address of one of my local DNS servers.

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
It's a type A Standard Query and it doesn't contain any answers.

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

There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

```
        www.ietf.org: type A, class inet, addr 65.246.255.51
            Name: www.ietf.org
            Type: Host address
            Class: inet
            Time to live: 1 hour
            Data length: 4
            Addr: 65.246.255.51
        www.ietf.org: type A, class inet, addr 132.151.6.75
            Name: www.ietf.org
            Type: Host address
            Class: inet
            Time to live: 1 hour
            Data length: 4
            Addr: 132.151.6.75
```

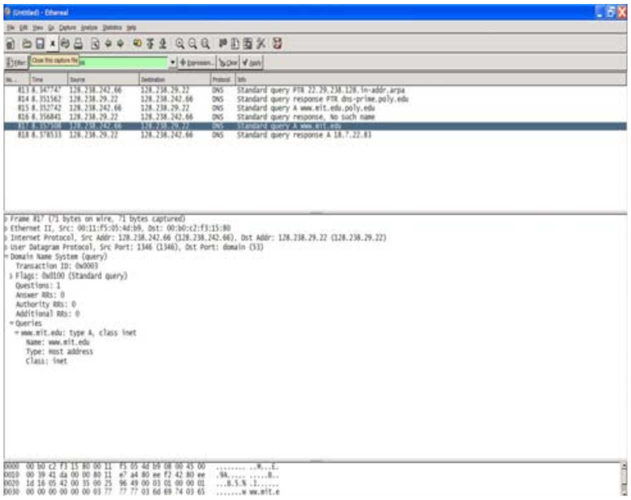
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The first SYN packet was sent to 65.246.255.51 which corresponds to the first IP address provided in the DNS response message.

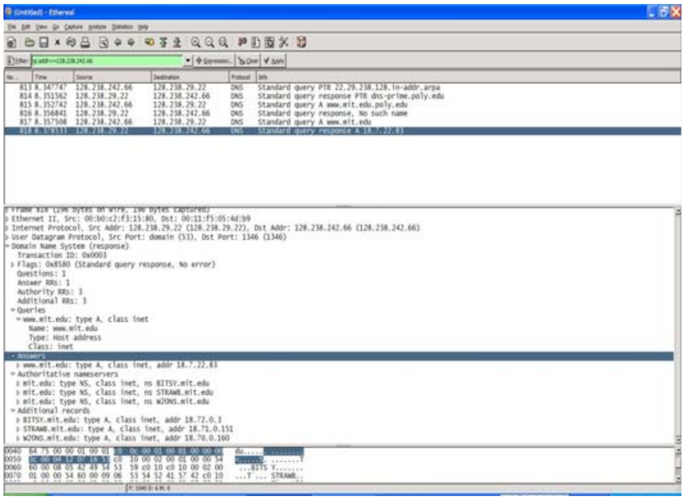
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No

PART 3


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Close this capture file
Expression... Clear Apply

```
No. Time       Source          Destination     Protocol Info
813 8.347747   128.238.242.66  128.238.29.22   DNS      Standard query PTR 22.29.238.128.in-addr.arpa
814 8.351562   128.238.29.22   128.238.242.66  DNS      Standard query response PTR dns-prime.poly.edu
815 8.352742   128.238.242.66  128.238.29.22   DNS      Standard query A www.mit.edu.poly.edu
816 8.356841   128.238.29.22   128.238.242.66  DNS      Standard query response, No such name
817 8.357508   128.238.242.66  128.238.29.22   DNS      Standard query A www.mit.edu
818 8.378533   128.238.29.22   128.238.242.66  DNS      Standard query response A 18.7.22.83

▷ Frame 817 (71 bytes on wire, 71 bytes captured)
▷ Ethernet II, Src: 00:11:f5:05:4d:b9, Dst: 00:b0:c2:f3:15:80
▷ Internet Protocol, Src Addr: 128.238.242.66 (128.238.242.66), Dst Addr: 128.238.29.22 (128.238.29.22)
▷ User Datagram Protocol, Src Port: 1346 (1346), Dst Port: domain (53)
▽ Domain Name System (query)
    Transaction ID: 0x0003
  ▷ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ www.mit.edu: type A, class inet
        Name: www.mit.edu
        Type: Host address
        Class: inet

0000  00 b0 c2 f3 15 80 00 11  f5 05 4d b9 08 00 45 00   ........ ..M...E.
0010  00 39 41 da 00 00 80 11  e7 a4 80 ee f2 42 80 ee   .9A..... .....B..
0020  1d 16 05 42 00 35 00 25  96 49 00 03 01 00 00 01   ...B.5.% .I......
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
```


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr==128.238.242.66
Expression... Clear Apply

```
No. Time       Source          Destination     Protocol Info
813 8.347747   128.238.242.66  128.238.29.22   DNS      Standard query PTR 22.29.238.128.in-addr.arpa
814 8.351562   128.238.29.22   128.238.242.66  DNS      Standard query response PTR dns-prime.poly.edu
815 8.352742   128.238.242.66  128.238.29.22   DNS      Standard query A www.mit.edu.poly.edu
816 8.356841   128.238.29.22   128.238.242.66  DNS      Standard query response, No such name
817 8.357508   128.238.242.66  128.238.29.22   DNS      Standard query A www.mit.edu
818 8.378533   128.238.29.22   128.238.242.66  DNS      Standard query response A 18.7.22.83

▷ Frame 818 (196 bytes on wire, 196 bytes captured)
▷ Ethernet II, Src: 00:b0:c2:f3:15:80, Dst: 00:11:f5:05:4d:b9
▷ Internet Protocol, Src Addr: 128.238.29.22 (128.238.29.22), Dst Addr: 128.238.242.66 (128.238.242.66)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 1346 (1346)
▽ Domain Name System (response)
    Transaction ID: 0x0003
  ▷ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  ▽ Queries
    ▽ www.mit.edu: type A, class inet
        Name: www.mit.edu
        Type: Host address
        Class: inet
  ▽ Answers
    ▷ www.mit.edu: type A, class inet, addr 18.7.22.83
  ▽ Authoritative nameservers
    ▷ mit.edu: type NS, class inet, ns BITSY.mit.edu
    ▷ mit.edu: type NS, class inet, ns STRAWB.mit.edu
    ▷ mit.edu: type NS, class inet, ns W20NS.mit.edu
  ▽ Additional records
    ▷ BITSY.mit.edu: type A, class inet, addr 18.72.0.3
    ▷ STRAWB.mit.edu: type A, class inet, addr 18.71.0.151
    ▷ W20NS.mit.edu: type A, class inet, addr 18.70.0.160

0040  64 75 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   du...... ........
0050  0c 00 04 12 07 16 53 c0  10 00 02 00 01 00 00 54   ......S. .......T
0060  60 00 08 05 42 49 54 53  59 c0 10 c0 10 00 02 00   `...BITS Y.......
0070  01 00 00 54 60 00 09 06  53 54 52 41 57 42 c0 10   ...T`... STRAWB..
```

Screenshot for DNS query

Screenshot for DNS response

11. 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 is 53 and the source port of the DNS response is 53.

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

It’s sent to 128.238.29.22 which as we can see from the ipconfig –all screenshot, is the default local DNS server.

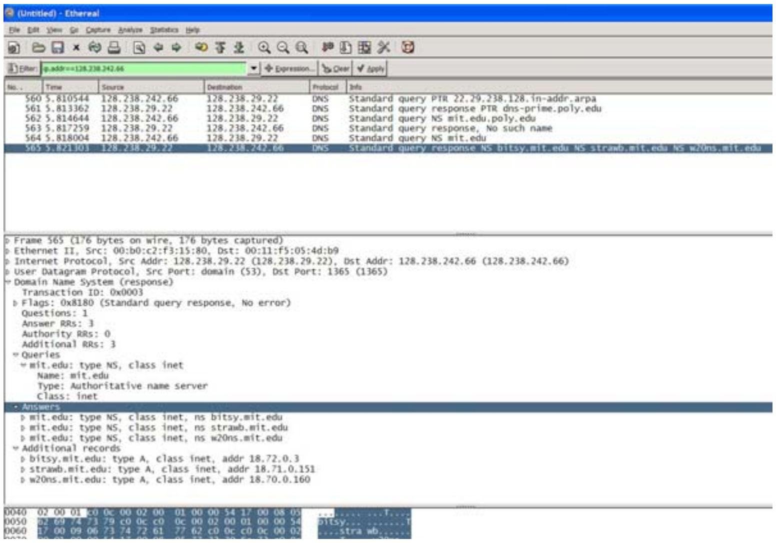
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
The query is of type A and it doesn't contain any answers.

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
The response DNS message contains only one answer containing the name of the host, the type of address, the class, the IP address

```
www.mit.edu: type A, class inet, addr 18.7.22.83
  Name: www.mit.edu
  Type: Host address
     Class: inet
  Time to live: 1 minute
  Data length: 4
  Addr: 18.7.22.83
```

15. Provide a screenshot.

PART 4



```
No. .  Time      Source           Destination      Protocol  Info
  560 5.810544  128.238.242.66   128.238.29.22    DNS   Standard query PTR 22.29.238.128.in-addr.arpa
  561 5.813362  128.238.29.22    128.238.242.66   DNS   Standard query response PTR dns-prime.poly.edu
  562 5.814644  128.238.242.66   128.238.29.22    DNS   Standard query NS mit.edu.poly.edu
  563 5.817259  128.238.29.22    128.238.242.66   DNS   Standard query response, No such name
  564 5.818004  128.238.242.66   128.238.29.22    DNS   Standard query NS mit.edu
  565 5.821303  128.238.29.22    128.238.242.66   DNS   Standard query response NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu

▷ Frame 565 (176 bytes on wire, 176 bytes captured)
▷ Ethernet II, Src: 00:b0:c2:f3:15:80, Dst: 00:11:f5:05:4d:b9
▷ Internet Protocol, Src Addr: 128.238.29.22 (128.238.29.22), Dst Addr: 128.238.242.66 (128.238.242.66)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 1365 (1365)
▽ Domain Name System (response)
    Transaction ID: 0x0003
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
  ▽ Queries
    ▽ mit.edu: type NS, class inet
        Name: mit.edu
        Type: Authoritative name server
        Class: inet
  ▽ Answers
    ▷ mit.edu: type NS, class inet, ns bitsy.mit.edu
    ▷ mit.edu: type NS, class inet, ns strawb.mit.edu
    ▷ mit.edu: type NS, class inet, ns w20ns.mit.edu
  ▽ Additional records
    ▷ bitsy.mit.edu: type A, class inet, addr 18.72.0.3
    ▷ strawb.mit.edu: type A, class inet, addr 18.71.0.151
    ▷ w20ns.mit.edu: type A, class inet, addr 18.70.0.160

0040  02 00 01 c0 0c 00 02 00  01 00 00 54 17 00 08 05   ........ ...T....
0050  62 69 74 73 79 c0 0c c0  0c 00 02 00 01 00 00 54   bitsy... .......T
0060  17 00 09 06 73 74 72 61  77 62 c0 0c c0 0c 00 02   ....stra wb......
```

Screenshot for DNS response

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
It was sent to 128.238.29.22 which again is my default DNS server.

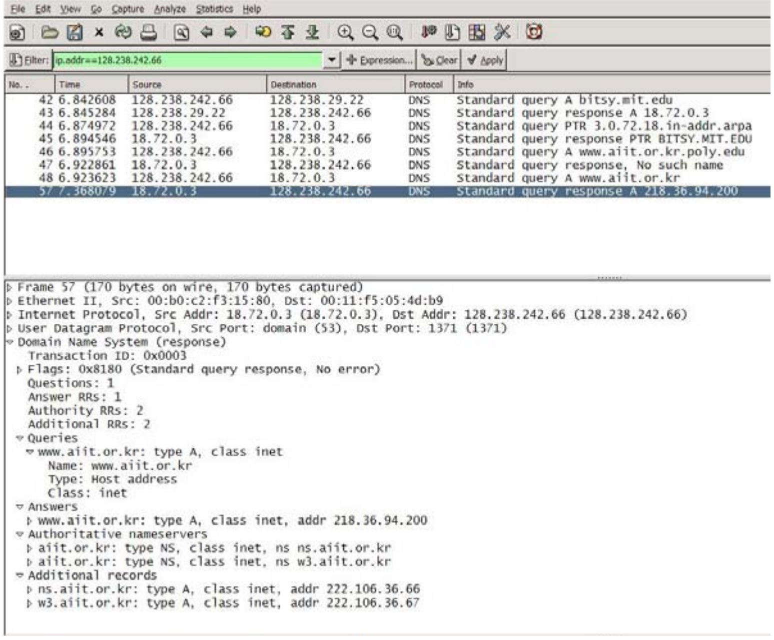
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
It's a type NS DNS query that doesn't contain any answers.

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 nameservers?
The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Ethereal as seen below.

```
Answers
        mit.edu: type NS, class inet, ns bitsy.mit.edu
        mit.edu: type NS, class inet, ns strawb.mit.edu
        mit.edu: type NS, class inet, ns w20ns.mit.edu
    Additional records
        bitsy.mit.edu: type A, class inet, addr 18.72.0.3
        strawb.mit.edu: type A, class inet, addr 18.71.0.151
        w20ns.mit.edu: type A, class inet, addr 18.70.0.160
```

19. Provide a screenshot.

PART 5



Filter: ip.addr==128.238.242.66

No. .	Time	Source	Destination	Protocol	Info
42	6.842608	128.238.242.66	128.238.29.22	DNS	Standard query A bitsy.mit.edu
43	6.845284	128.238.29.22	128.238.242.66	DNS	Standard query response A 18.72.0.3
44	6.874972	128.238.242.66	18.72.0.3	DNS	Standard query PTR 3.0.72.18.in-addr.arpa
45	6.894546	18.72.0.3	128.238.242.66	DNS	Standard query response PTR BITSY.MIT.EDU
46	6.895753	128.238.242.66	18.72.0.3	DNS	Standard query A www.aiit.or.kr.poly.edu
47	6.922861	18.72.0.3	128.238.242.66	DNS	Standard query response, No such name
48	6.923623	128.238.242.66	18.72.0.3	DNS	Standard query A www.aiit.or.kr
57	7.368079	18.72.0.3	128.238.242.66	DNS	Standard query response A 218.36.94.200

```
▷ Frame 57 (170 bytes on wire, 170 bytes captured)
▷ Ethernet II, Src: 00:b0:c2:f3:15:80, Dst: 00:11:f5:05:4d:b9
▷ Internet Protocol, Src Addr: 18.72.0.3 (18.72.0.3), Dst Addr: 128.238.242.66 (128.238.242.66)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 1371 (1371)
▽ Domain Name System (response)
    Transaction ID: 0x0003
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ▽ Queries
    ▽ www.aiit.or.kr: type A, class inet
        Name: www.aiit.or.kr
        Type: Host address
        Class: inet
  ▽ Answers
    ▷ www.aiit.or.kr: type A, class inet, addr 218.36.94.200
  ▽ Authoritative nameservers
    ▷ aiit.or.kr: type NS, class inet, ns ns.aiit.or.kr
    ▷ aiit.or.kr: type NS, class inet, ns w3.aiit.or.kr
  ▽ Additional records
    ▷ ns.aiit.or.kr: type A, class inet, addr 222.106.36.66
    ▷ w3.aiit.or.kr: type A, class inet, addr 222.106.36.67
```

Screenshot for DNS response

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 query is sent to 18.72.0.3 which 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"?
It's a standard type A query that doesn't contain any answers.

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
One answer s provided in the DNS response message. It contains the following:

```
Answers
        www.aiit.or.kr: type A, class inet, addr 218.36.94.200
            Name: www.aiit.or.kr
            Type: Host address
            Class: inet
            Time to live: 1 hour
            Data length: 4
            Addr: 218.36.94.200
```

23. Provide a screenshot.