Name: Elsy Fernandes
SID:1001602253

DNS LAB -
PART 1 : nslookup on terminal

1.Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
Command:nslookup www.rediff.com
ANSWER: I performed nslookup for www.rediff.com .Its Ip address is 104.112.67.177.

Screenshot:

```
Elsys-MacBook-Air:~ el$ nslookup www.rediff.com
Server:         209.18.47.61
Address:        209.18.47.61#53

Non-authoritative answer:
www.rediff.com  canonical name = rediff.com.edgekey.net.
rediff.com.edgekey.net  canonical name = e4389.g.akamaiedge.net.
Name:   e4389.g.akamaiedge.net
Address: 104.112.67.177
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
Command: nslookup –type=NS uoi.gr
ANSWER: NS lookup command for European University in Ioannina Greece.

```
Elsys-MacBook-Air:~ el$ nslookup -type=NS uoi.gr
Server:         209.18.47.61
Address:        209.18.47.61#53

Non-authoritative answer:
uoi.gr  nameserver = sns1.grnet.gr.
uoi.gr  nameserver = kouzina.noc.uoi.gr.
uoi.gr  nameserver = sns0.grnet.gr.
uoi.gr  nameserver = marina.noc.uoi.gr.

Authoritative answers can be found from:

Elsys-MacBook-Air:~ el$
```

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?
Command: nslookup mail.yahoo.com marina.noc.uoi.gr
ANSWER : I could not find the server detail for mail.yahoo as shown in the screenshots.
I could find the server Address for marina.noc.uoi.gr and it is :195.130.120.120#53

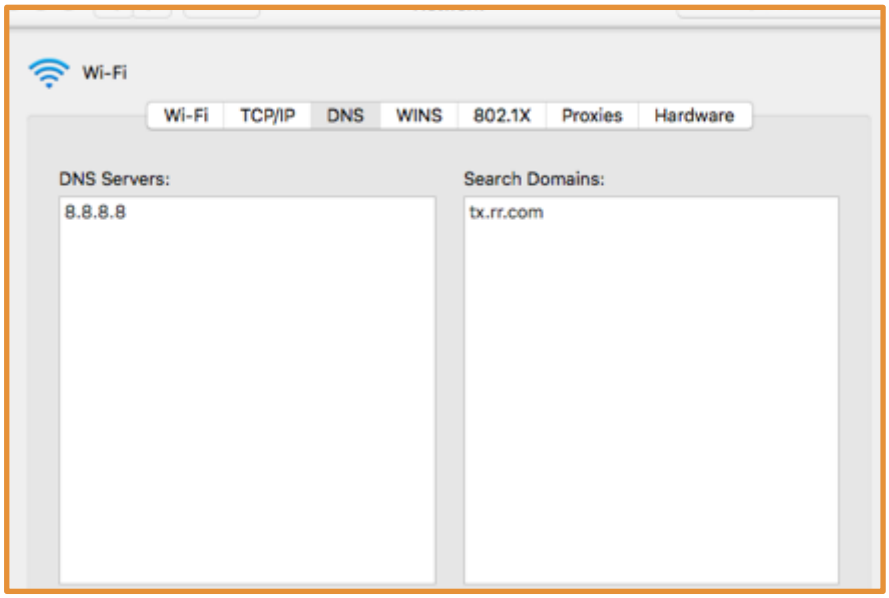
```
Elsys-MacBook-Air:~ el$ nslookup mail.yahoo.com
Server:         129.107.35.89
Address:        129.107.35.89#53

Non-authoritative answer:
mail.yahoo.com  canonical name = fd-geoycpi-uno.gycpi.b.yahoodns.net.
Name:   fd-geoycpi-uno.gycpi.b.yahoodns.net
Address: 69.147.86.12
Name:   fd-geoycpi-uno.gycpi.b.yahoodns.net
Address: 69.147.86.11
```

```
Elsys-MacBook-Air:~ el$ nslookup -type=NS uoi.gr
Server:         129.107.35.89
Address:        129.107.35.89#53

Non-authoritative answer:
uoi.gr  nameserver = marina.noc.uoi.gr.
uoi.gr  nameserver = kouzina.noc.uoi.gr.
uoi.gr  nameserver = sns1.grnet.gr.
uoi.gr  nameserver = sns0.grnet.gr.

Authoritative answers can be found from:

Elsys-MacBook-Air:~ el$ nslookup mail.yahoo marina.noc.uoi.gr
Server:         marina.noc.uoi.gr
Address:        195.130.120.120#53

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

Elsys-MacBook-Air:~ el$
```

Note: I had emailed you regarding this .

PART 2 : Tracing DNS with Wireshark
Steps to be followed before capturing the packets :-

Step 1:-DNS server detail in Macbook

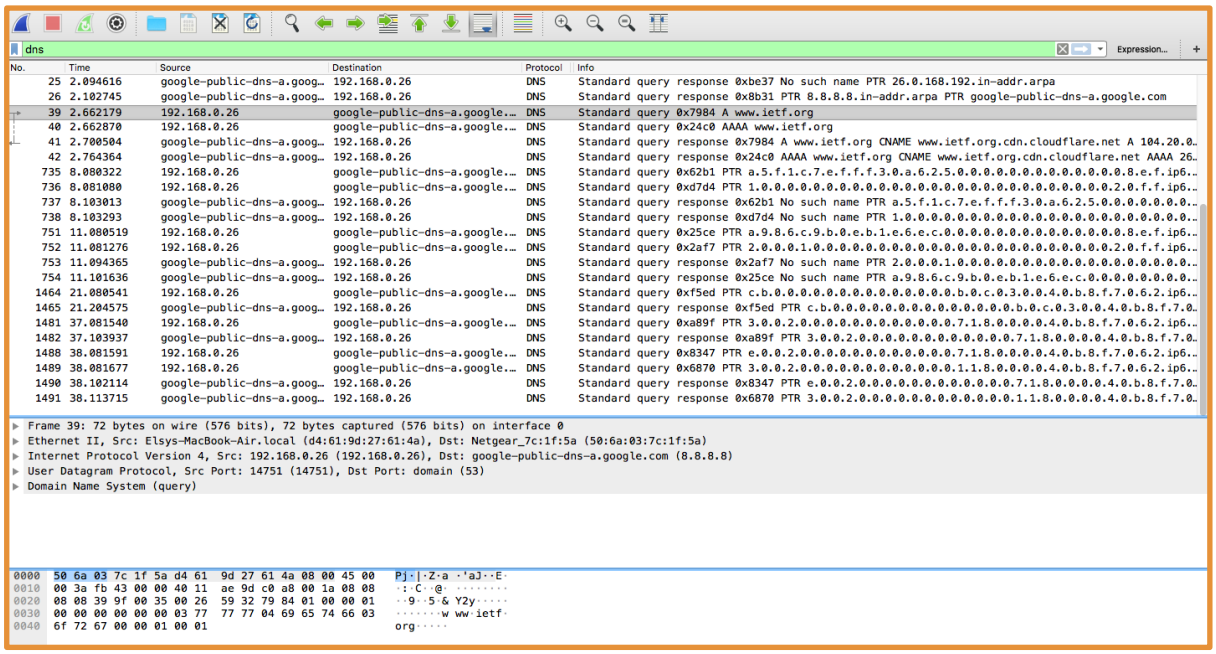


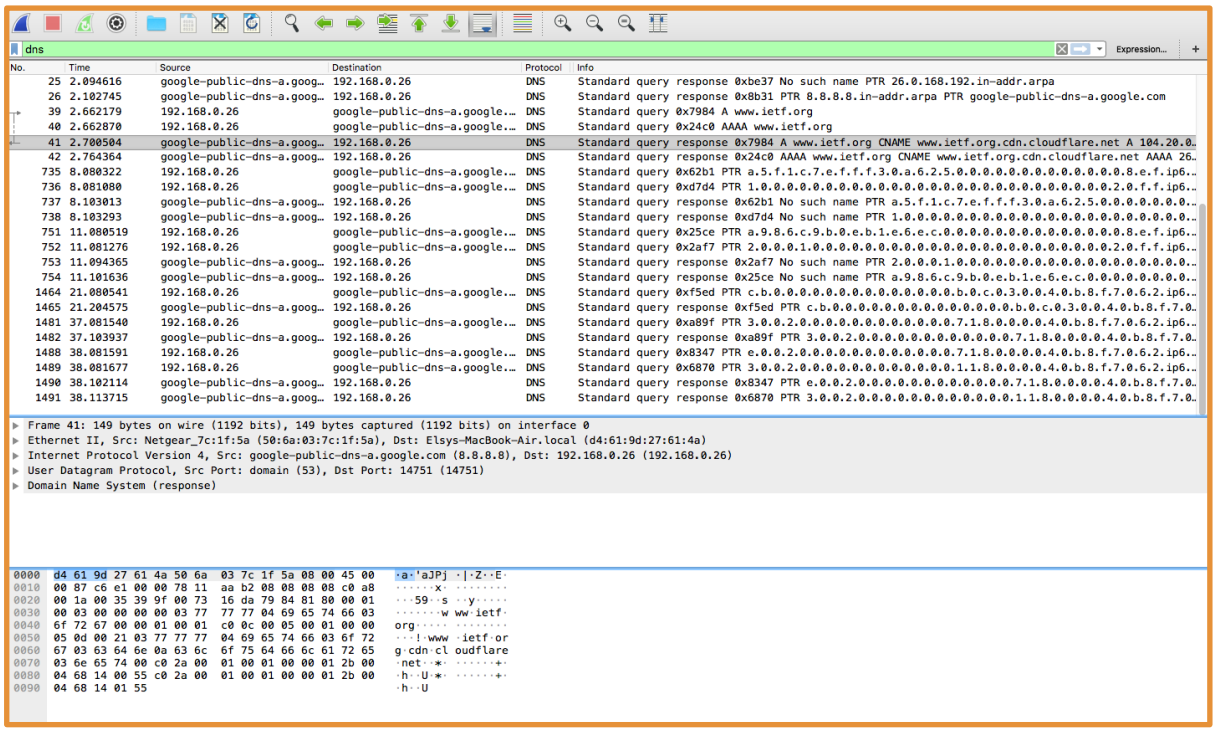
Step 2: Flush DNS in macbook

```
Elsys-MacBook-Air:~ el$ sudo killall -HUP mDNSResponder
Password:
Sorry, try again.
Password:
Elsys-MacBook-Air:~ el$
```

Step 3: Find IP address the machine your sending the request and recording the response :-192.168.0.26

Step 4: Clear the browser cache.
Step 5: Open wireshark.Start the packet capture.
Step 6: Type https://www.ietf.org/ in browser.
Step 7: Stop the packet capture.
Step 8: Standard query and its response captured:





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

ANSWER: This is sent over UDP.

```
▶ Frame 756: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
▶ Ethernet II, Src: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a), Dst: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a)
▶ Internet Protocol Version 4, Src: Elsys-MacBook-Air.local (192.168.0.26), Dst: google-public-dns-a.google.com (8.8.8.8)
▶ User Datagram Protocol, Src Port: 32612 (32612), Dst Port: domain (53)
▶ Domain Name System (query)
```

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

ANSWER : Destination port of DNS query message: 53 and source port of DNS response message : 53

Standard query Destination port:

dns

No.	Time	Source	Destination	Protocol	Info
25	2.094616	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0xbe37 No such name PTR 26.0.168.192.in-addr.arpa
26	2.102745	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0x8b31 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
39	2.662179	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0x7984 A www.ietf.org
40	2.662870	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0x24c0 AAAA www.ietf.org
41	2.700504	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0x7984 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20
42	2.764364	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0x24c0 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA
735	8.080322	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0x62b1 PTR a.5.f.1.c.7.e.f.f.f.3.0.a.6.2.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip
736	8.081080	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0xd7d4 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip

```
▶ Frame 39: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
▶ Ethernet II, Src: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a), Dst: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a)
▶ Internet Protocol Version 4, Src: 192.168.0.26 (192.168.0.26), Dst: google-public-dns-a.google.com (8.8.8.8)
▶ User Datagram Protocol, Src Port: 14751 (14751), Dst Port: domain (53)
▶ Domain Name System (query)
```

Standard Response source Port:

718	103.817082	google-public-dns-a.google.com	Elsys-MacBook-Air.local	DNS	Standard query response 0xcce7 No such name PTR 6.f.1.f.e.d.a.e.5.2.c.e.3.b
755	125.208596	Elsys-MacBook-Air.local	google-public-dns-a.google.com	DNS	Standard query 0xf8c4 A www.ietf.org
756	125.209383	Elsys-MacBook-Air.local	google-public-dns-a.google.com	DNS	Standard query 0x7edf AAAA www.ietf.org
771	125.242885	google-public-dns-a.google.com	Elsys-MacBook-Air.local	DNS	Standard query response 0xf8c4 A www.ietf.org CNAME www.ietf.org.cdn.cloudf
772	125.309700	google-public-dns-a.google.com	Elsys-MacBook-Air.local	DNS	Standard query response 0x7edf AAAA www.ietf.org CNAME www.ietf.org.cdn.clo
829	148.800018	Elsys-MacBook-Air.local	google-public-dns-a.google.com	DNS	Standard query 0xb09f PTR 27.0.168.192.in-addr.arpa
830	148.817286	google-public-dns-a.google.com	Elsys-MacBook-Air.local	DNS	Standard query response 0xb09f No such name PTR 27.0.168.192.in-addr.arpa

```
▶ Frame 771: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
▶ Ethernet II, Src: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a), Dst: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a)
▶ Internet Protocol Version 4, Src: google-public-dns-a.google.com (8.8.8.8), Dst: Elsys-MacBook-Air.local (192.168.0.26)
▶ User Datagram Protocol, Src Port: domain (53), Dst Port: 49856 (49856)
▶ Domain Name System (response)
```

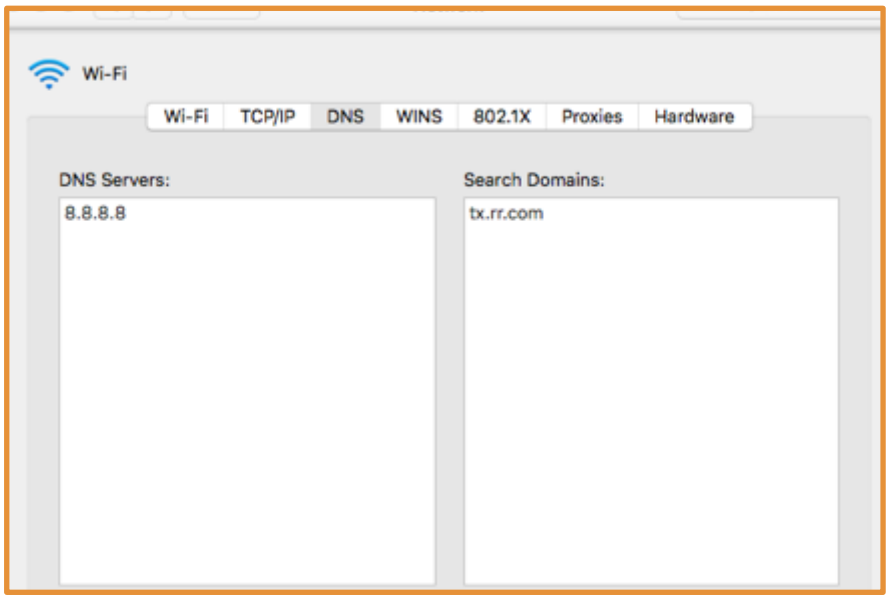
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

ANSWER:DNS query message sent over 8.8.8.8 as shown in the image. Yes it is same as local DNS Server

dns

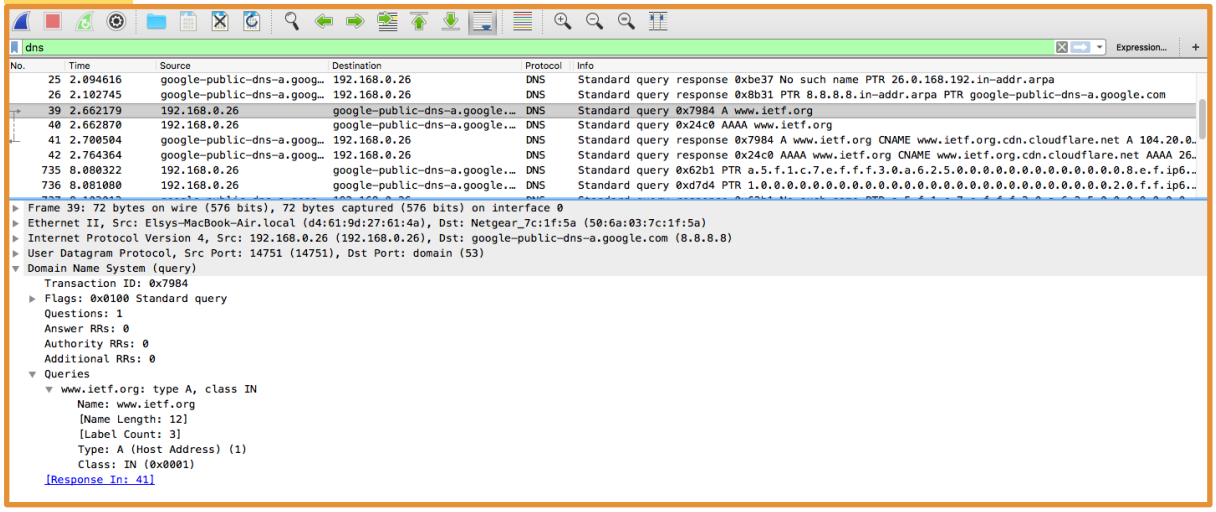
No.	Time	Source	Destination	Protocol	Info
25	2.094616	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0xbe37 No such name PTR 26.0.168.192.in-addr.arpa
26	2.102745	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0x8b31 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
39	2.662179	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0x7984 A www.ietf.org
40	2.662870	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0x24c0 AAAA www.ietf.org
41	2.700504	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0x7984 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20
42	2.764364	google-public-dns-a.goog…	192.168.0.26	DNS	Standard query response 0x24c0 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA
735	8.080322	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0x62b1 PTR a.5.f.1.c.7.e.f.f.f.3.0.a.6.2.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip
736	8.081080	192.168.0.26	google-public-dns-a.google.…	DNS	Standard query 0xd7d4 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip

```
▶ Frame 39: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
▶ Ethernet II, Src: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a), Dst: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a)
▶ Internet Protocol Version 4, Src: 192.168.0.26 (192.168.0.26), Dst: google-public-dns-a.google.com (8.8.8.8)
▶ User Datagram Protocol, Src Port: 14751 (14751), Dst Port: domain (53)
▶ Domain Name System (query)
```



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

ANSWER:Query is of Type A . Doesn’t contain any answers.



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

ANSWER: 3 . It Contains the information about Name, Type,Address and also the canonical name(Cname). It also contains information on Time to live ,Data length,Class.

```
755 125.208596   Elsys-MacBook-Air.local          google-public-dns-a.google.com  DNS   Standard query 0xf8c4 A www.ietf.org
756 125.209383   Elsys-MacBook-Air.local          google-public-dns-a.google.com  DNS   Standard query 0x7edf AAAA www.ietf.org
771 125.242885   google-public-dns-a.google.com   Elsys-MacBook-Air.local         DNS   Standard query response 0xf8c4 A www.ietf.org CNAME www.ietf.org.cdn.cloudf
772 125.309700   google-public-dns-a.google.com   Elsys-MacBook-Air.local         DNS   Standard query response 0x7edf AAAA www.ietf.org CNAME www.ietf.org.cdn.clo
829 148.800018   Elsys-MacBook-Air.local          google-public-dns-a.google.com  DNS   Standard query 0xb09f PTR 27.0.168.192.in-addr.arpa
830 148.817286   google-public-dns-a.google.com   Elsys-MacBook-Air.local         DNS   Standard query response 0xb09f No such name PTR 27.0.168.192.in-addr.arpa

    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  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
    ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  [Request In: 755]
  [Time: 0.034289000 seconds]
```

```
        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: 222
        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
    ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  [Request In: 755]
  [Time: 0.034289000 seconds]
```

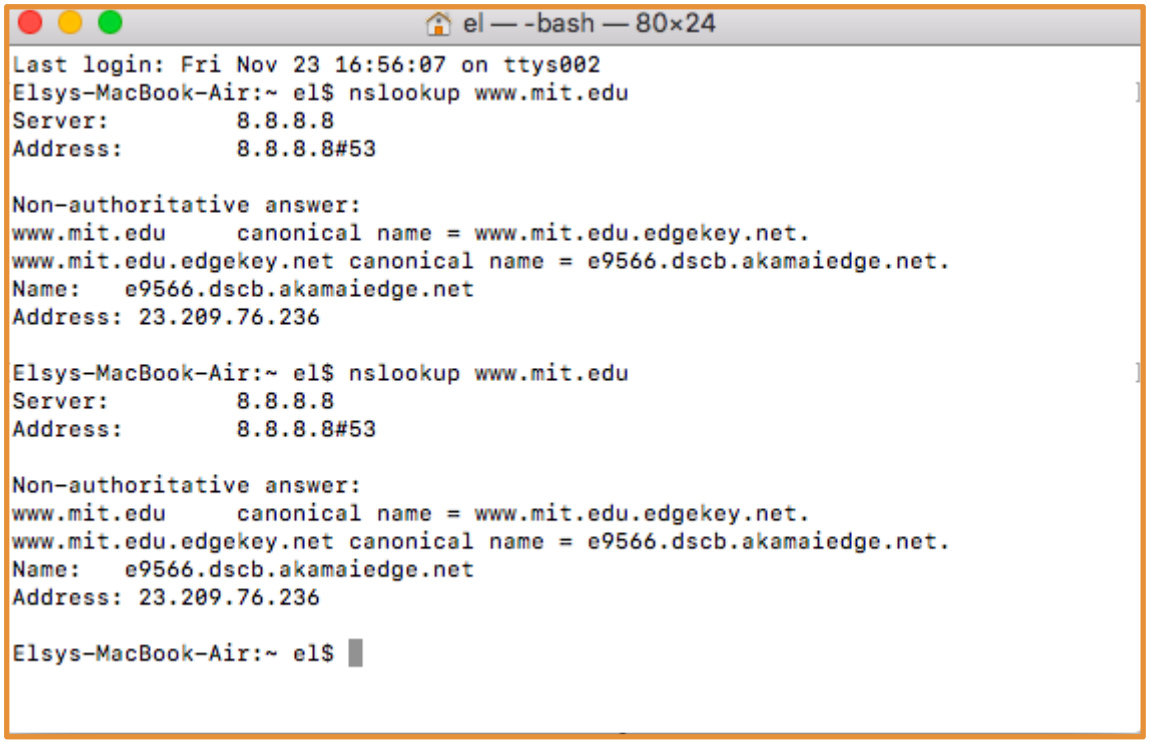
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
ANSWER:The first SYN packet was sent to 104.20.0.85 which corresponds to the first IP address provided in the DNS response message.

```
        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: 222
        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
    ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  [Request In: 755]
  [Time: 0.034289000 seconds]
```

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

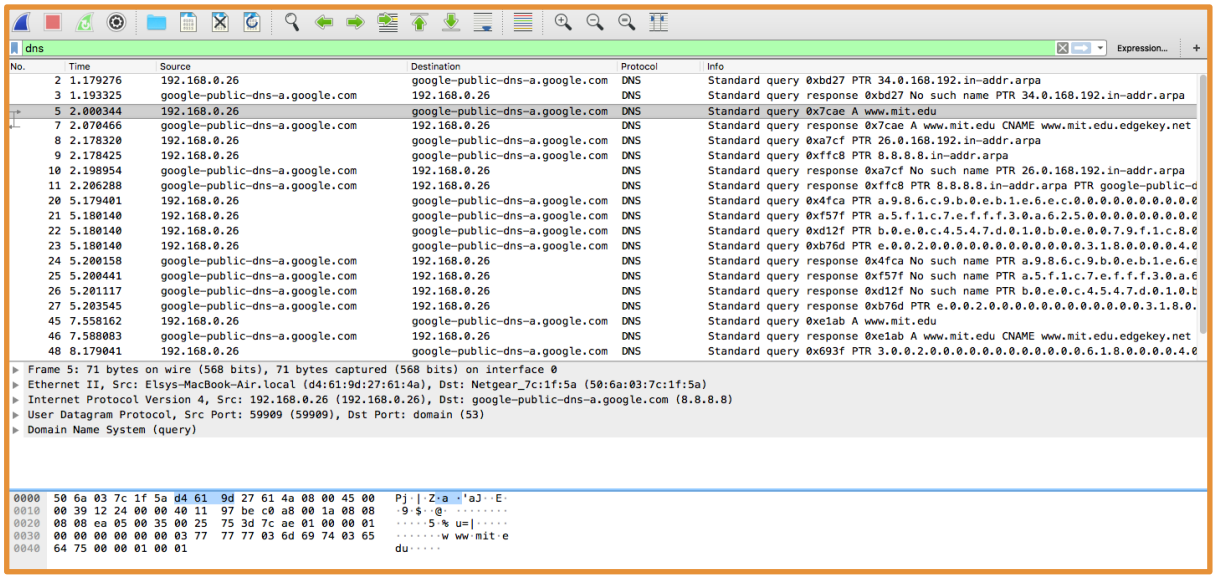
PART 3 : Tracing DNS with Wireshark(With NSLOOKUP)
Steps to be followed before capture the packet.

Step 1: Start packet capture.
Step 2: Do an nslookup on www.mit.edu.



```
el — -bash — 80×24
Last login: Fri Nov 23 16:56:07 on ttys002
Elsys-MacBook-Air:~ el$ nslookup www.mit.edu
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 23.209.76.236

Elsys-MacBook-Air:~ el$ nslookup www.mit.edu
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 23.209.76.236

Elsys-MacBook-Air:~ el$
```

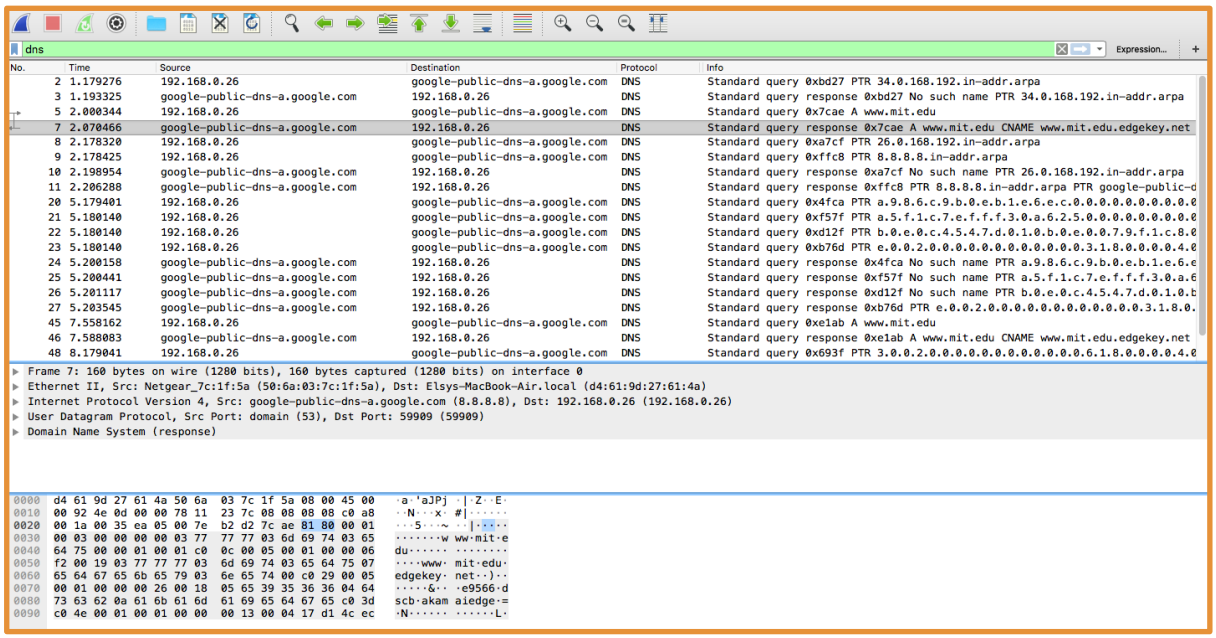
Step 3: Stop the packet capture.
Step 4: Standard query and its response captured:



dns

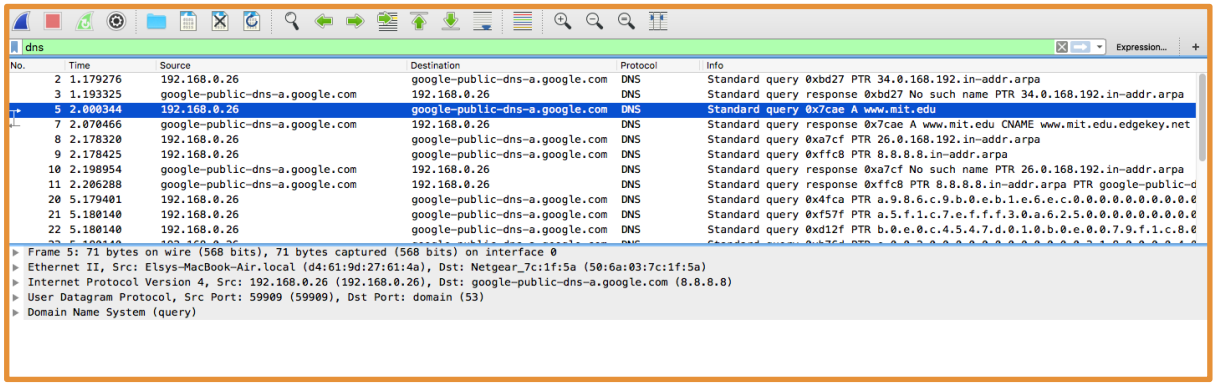
No.	Time	Source	Destination	Protocol	Info
2	1.179276	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xbd27 PTR 34.0.168.192.in-addr.arpa
3	1.193325	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xbd27 No such name PTR 34.0.168.192.in-addr.arpa
5	2.000344	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0x7cae A www.mit.edu
7	2.070466	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0x7cae A www.mit.edu CNAME www.mit.edu.edgekey.net
8	2.178320	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xa7cf PTR 26.0.168.192.in-addr.arpa
9	2.178425	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xffc8 PTR 8.8.8.8.in-addr.arpa
10	2.198954	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xa7cf No such name PTR 26.0.168.192.in-addr.arpa
11	2.206288	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xffc8 PTR 8.8.8.8.in-addr.arpa PTR google-public-d
20	5.179401	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0x4fca PTR a.9.8.6.c.9.b.0.e.b.1.e.6.e.c.0.0.0.0.0.0.0.0.0.0
21	5.180140	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xf57f PTR a.5.f.1.c.7.e.f.f.f.3.0.a.6.2.5.0.0.0.0.0.0.0.0.0
22	5.180140	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xd12f PTR b.0.e.0.c.4.5.4.7.d.0.1.0.b.0.e.0.0.7.9.f.1.c.8.0
23	5.180140	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xb76d PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.8.0.0.0.0.4.0
24	5.200158	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0x4fca No such name PTR a.9.8.6.c.9.b.0.e.b.1.e.6.e
25	5.200441	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xf57f No such name PTR a.5.f.1.c.7.e.f.f.f.3.0.a.6
26	5.201117	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xd12f No such name PTR b.0.e.0.c.4.5.4.7.d.0.1.0.b
27	5.203545	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xb76d PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.8.0.
45	7.558162	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0xe1ab A www.mit.edu
46	7.588083	google-public-dns-a.google.com	192.168.0.26	DNS	Standard query response 0xe1ab A www.mit.edu CNAME www.mit.edu.edgekey.net
48	8.179041	192.168.0.26	google-public-dns-a.google.com	DNS	Standard query 0x693f PTR 3.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.6.1.8.0.0.0.0.4.0

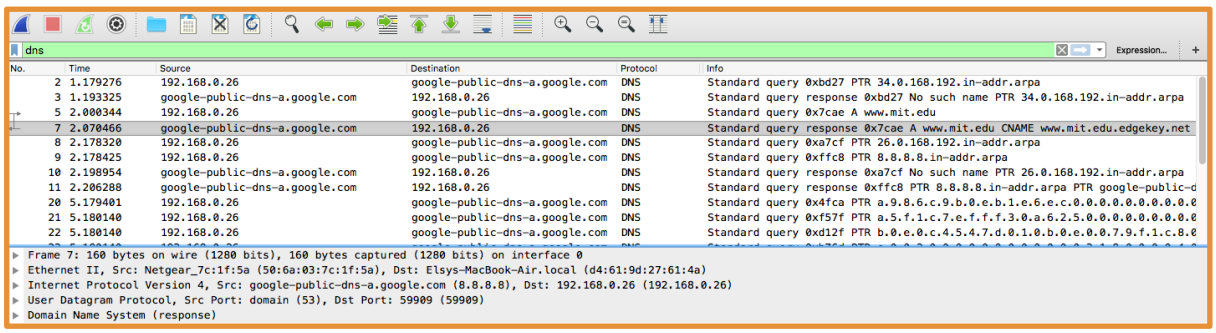
```
▶ Frame 5: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▶ Ethernet II, Src: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a), Dst: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a)
▶ Internet Protocol Version 4, Src: 192.168.0.26 (192.168.0.26), Dst: google-public-dns-a.google.com (8.8.8.8)
▶ User Datagram Protocol, Src Port: 59909 (59909), Dst Port: domain (53)
▶ Domain Name System (query)

0000  50 6a 03 7c 1f 5a d4 61  9d 27 61 4a 08 00 45 00   Pj·|·Z·a ·'aJ··E·
0010  00 39 12 24 00 00 40 11  97 be c0 a8 00 1a 08 08   ·9·$··@· ........
0020  08 08 ea 05 00 35 00 25  75 3d 7c ae 01 00 00 01   ·····5·% u=|·····
0030  00 00 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                               du·····
```



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

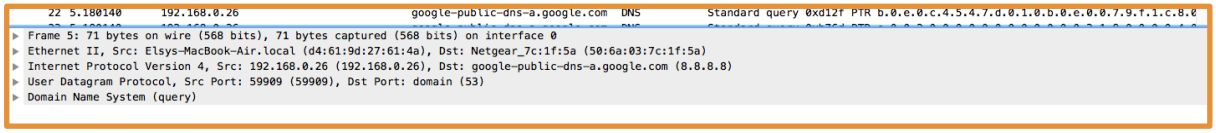
ANSWER:Destination port for the DNS query message -53 .Source port of DNS response message-53

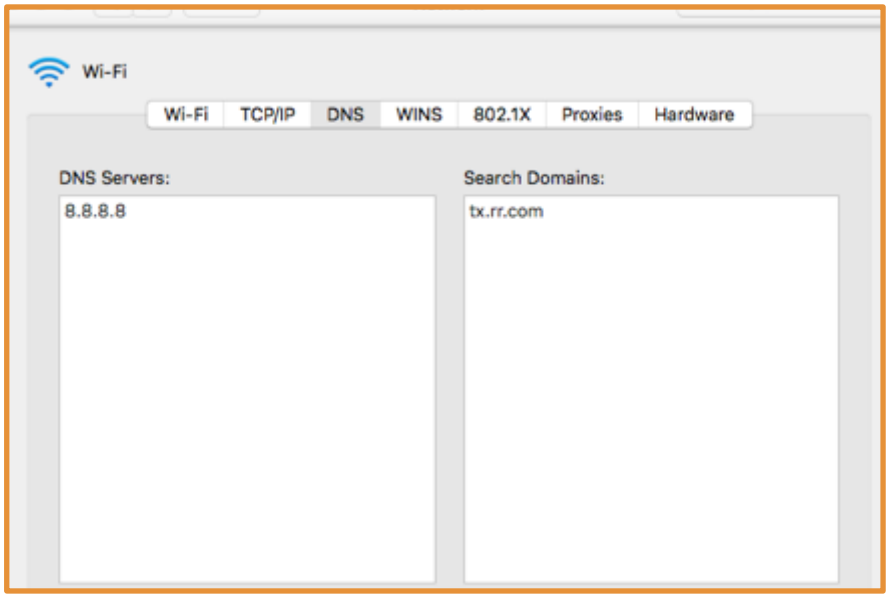


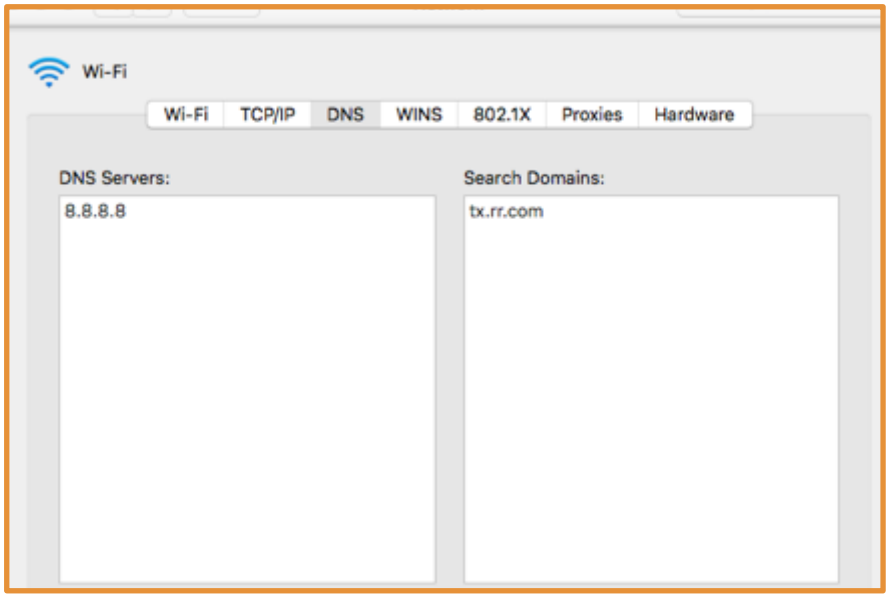


12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

ANSWER:DNS query message sent over 8.8.8.8 as shown in the image. Yes it is same as local DNS Server

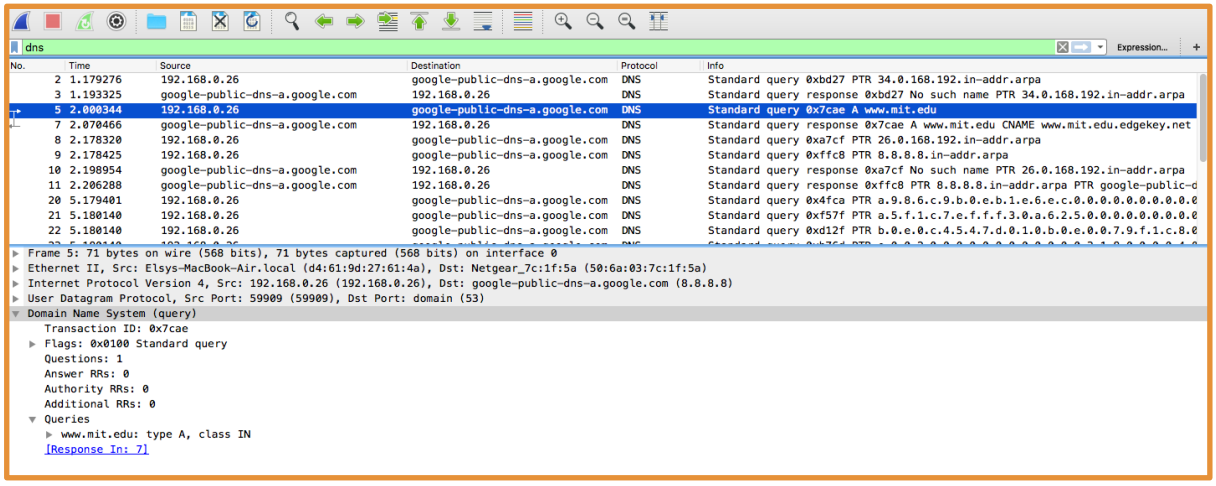






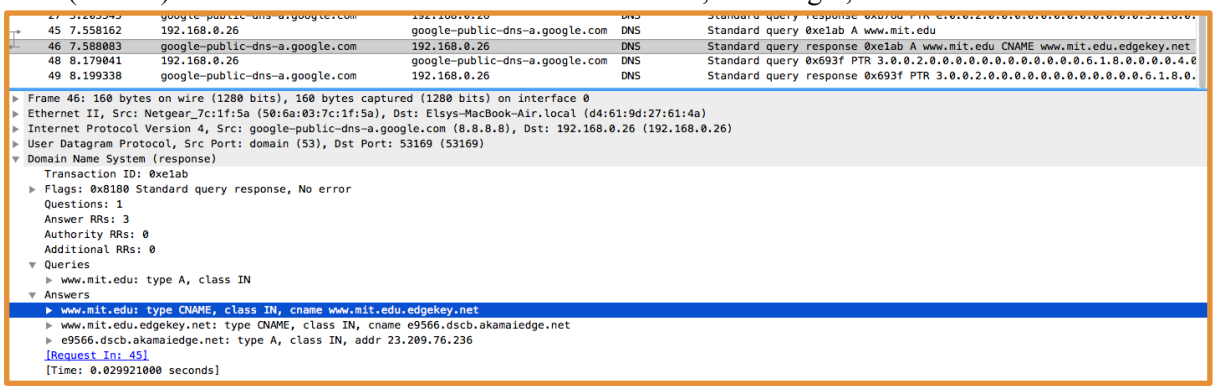
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

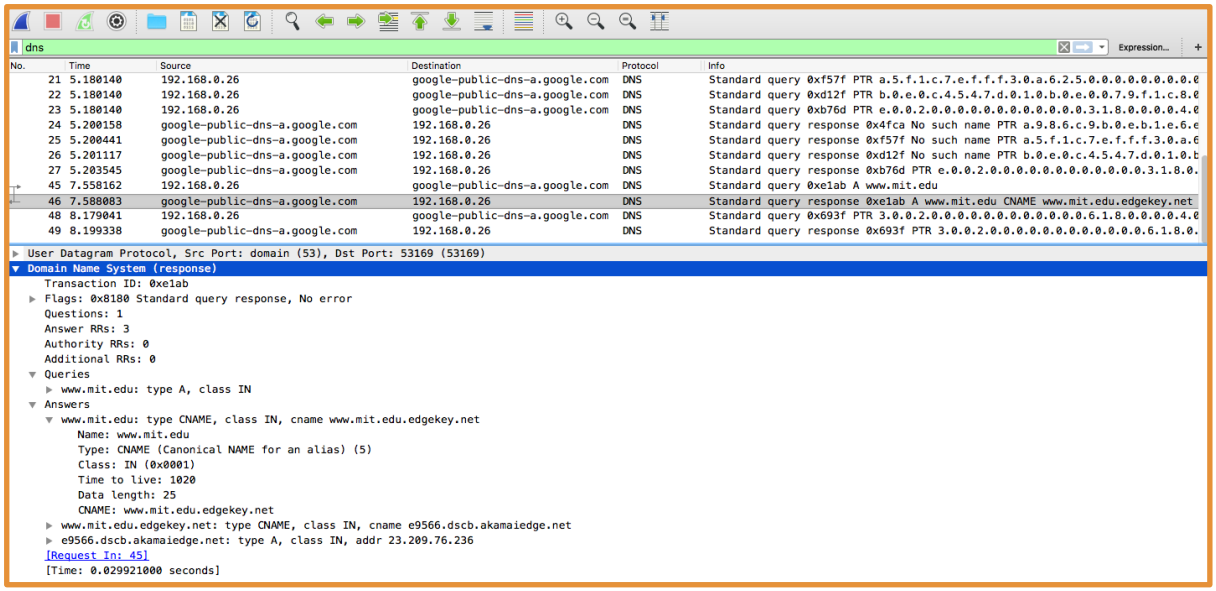
ANSWER:Query is of Type A . Doesn’t contain any answers.



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

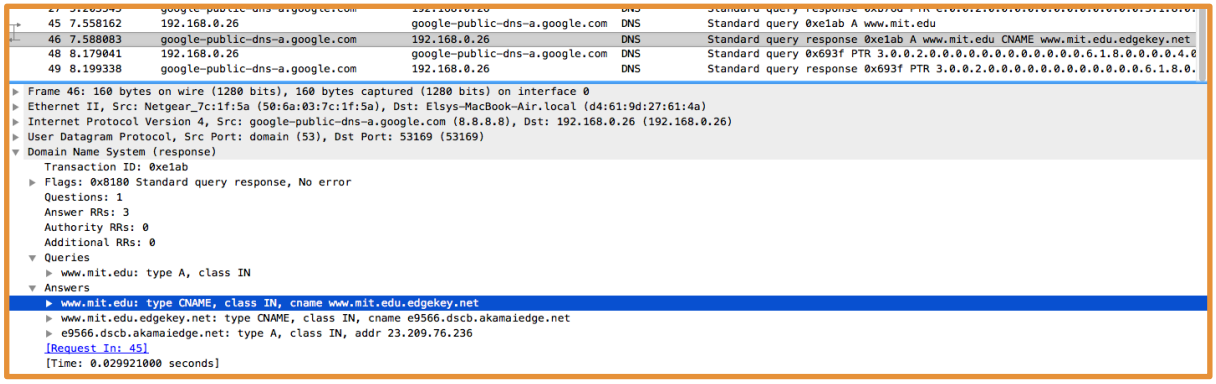
ANSWER:3 . It Contains the information about Name, Type,Address and also the canonical name(Cname). It also contains information on Time to live ,Data length,Class.

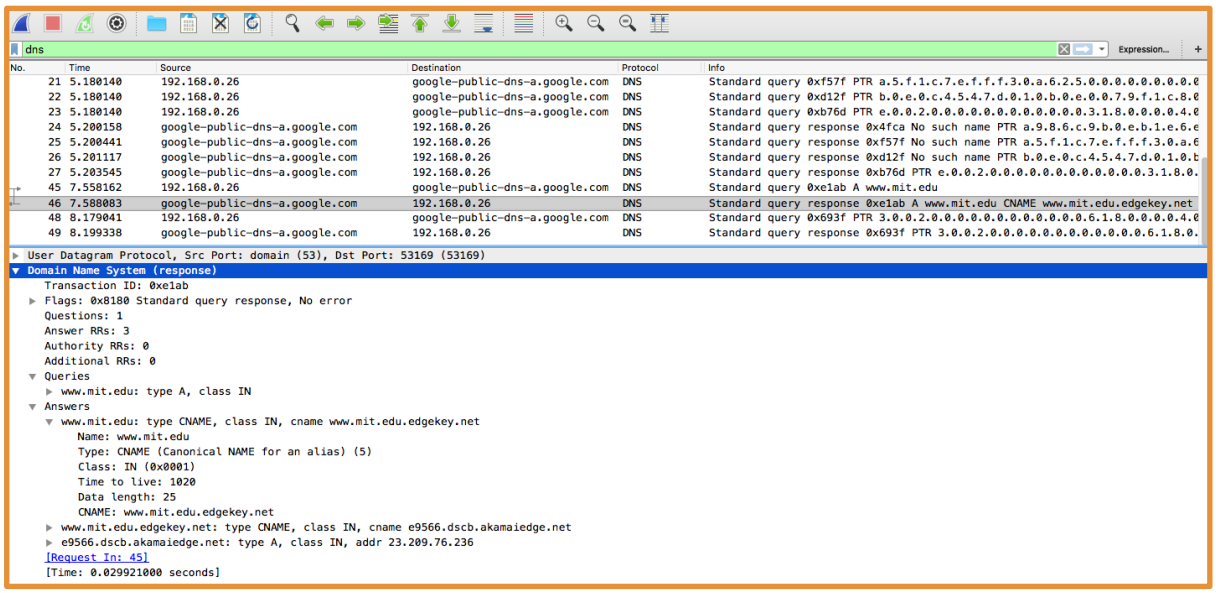




15. Provide a screenshot.

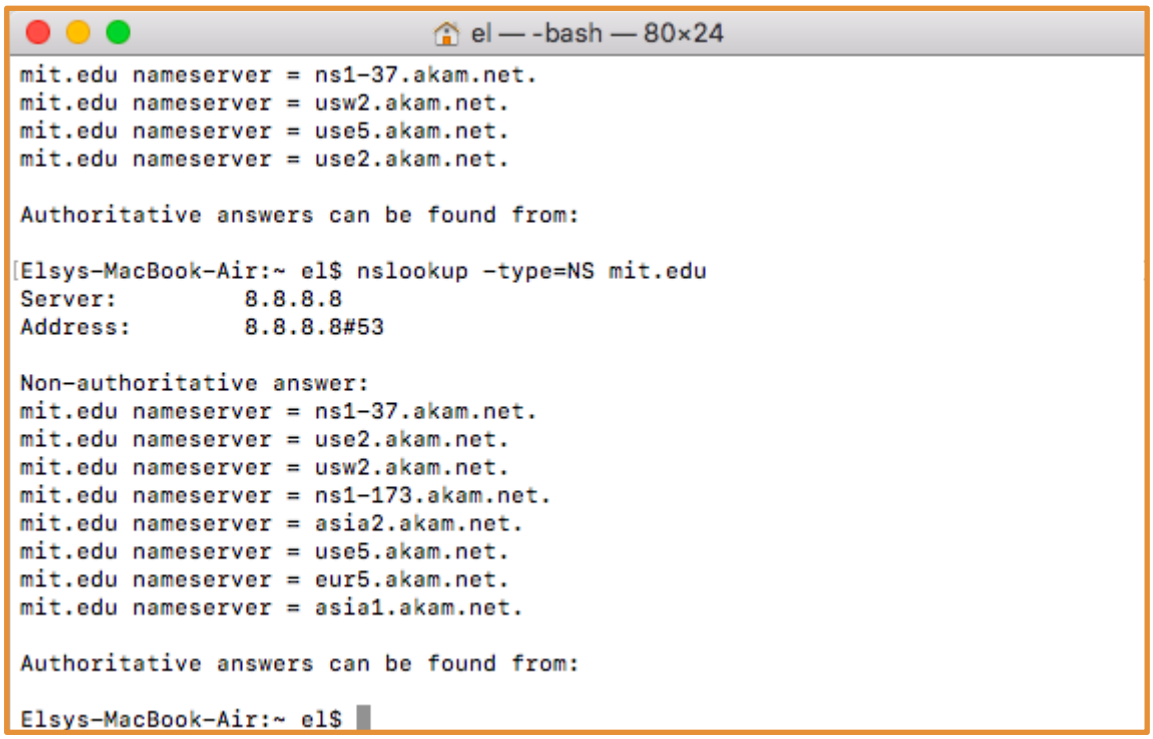
ANSWER:





PART 4 : Tracing DNS with Wireshark(With -TYPE NSLOOKUP)
Steps to be followed before capture the packet.

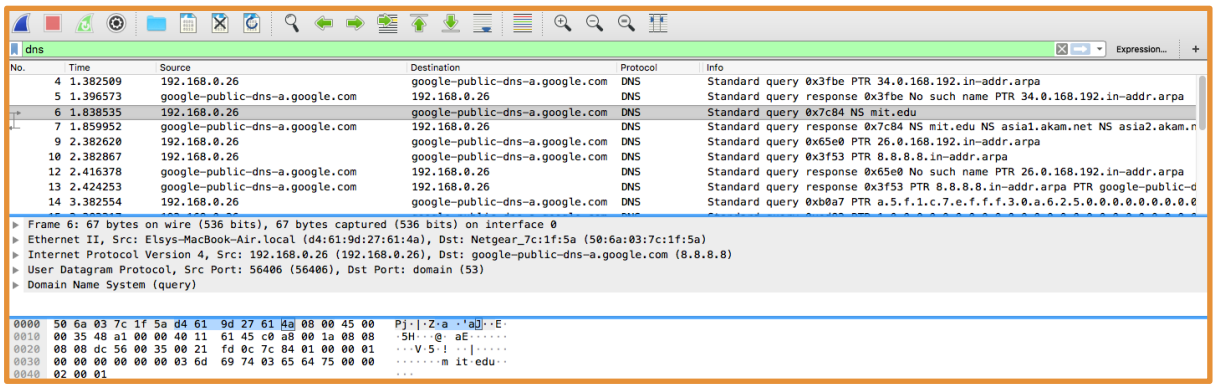
Step 1: Start packet capture.
Step 2: Do an nslookup on: **nslookup –type=NS mit.edu**



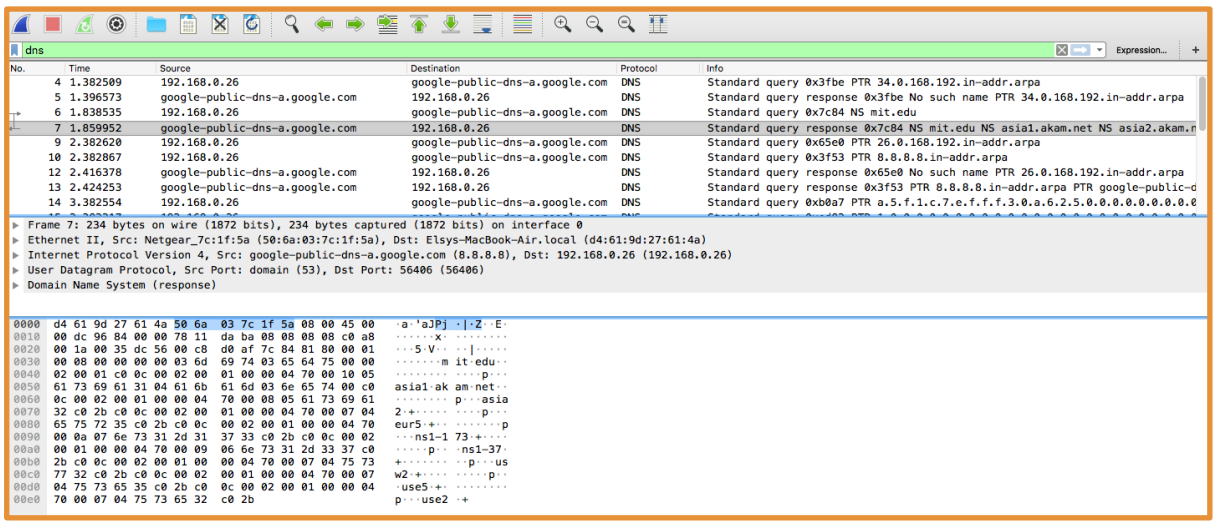
```
el — -bash — 80×24
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = use2.akam.net.

Authoritative answers can be found from:

Elsys-MacBook-Air:~ el$ nslookup -type=NS mit.edu
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = asia1.akam.net.

Authoritative answers can be found from:

Elsys-MacBook-Air:~ el$
```

Step 3: Stop the packet capture.

Step 4: Standard query and its response captured:



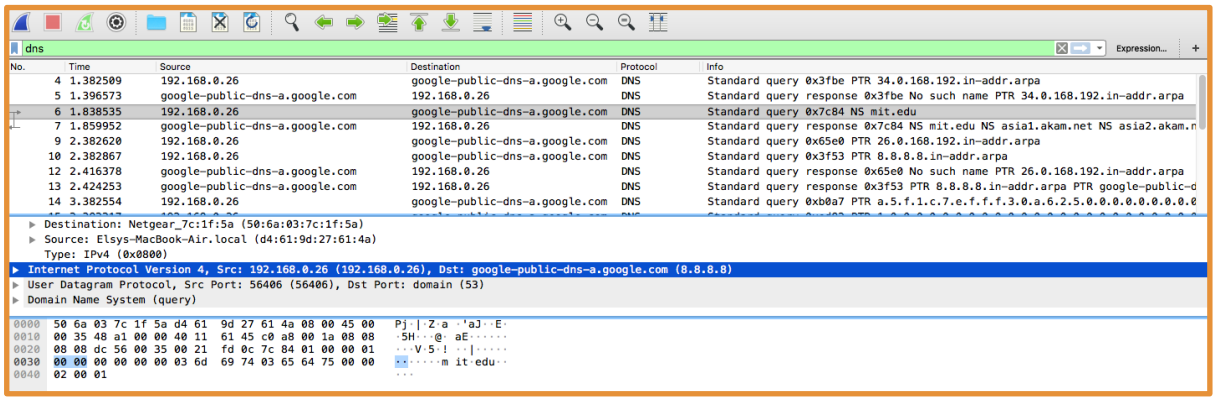
```
No.  Time        Source                    Destination               Protocol  Info
 4   1.382509    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x3fbe PTR 34.0.168.192.in-addr.arpa
 5   1.396573    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x3fbe No such name PTR 34.0.168.192.in-addr.arpa
 6   1.838535    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x7c84 NS mit.edu
 7   1.859952    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x7c84 NS mit.edu NS asia1.akam.net NS asia2.akam.n
 9   2.382620    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x65e0 PTR 26.0.168.192.in-addr.arpa
10   2.382867    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x3f53 PTR 8.8.8.8.in-addr.arpa
12   2.416378    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x65e0 No such name PTR 26.0.168.192.in-addr.arpa
13   2.424253    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x3f53 PTR 8.8.8.8.in-addr.arpa PTR google-public-d
14   3.382554    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0xb0a7 PTR a.5.f.1.c.7.e.f.f.f.3.0.a.6.2.5.0.0.0.0.0.0.0.0.0.0

▸ Frame 6: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a), Dst: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a)
▸ Internet Protocol Version 4, Src: 192.168.0.26 (192.168.0.26), Dst: google-public-dns-a.google.com (8.8.8.8)
▸ User Datagram Protocol, Src Port: 56406 (56406), Dst Port: domain (53)
▸ Domain Name System (query)

0000  50 6a 03 7c 1f 5a d4 61  9d 27 61 4a 08 00 45 00   Pj·|·Z·a ·'aJ··E·
0010  00 35 48 a1 00 00 40 11  61 45 c0 a8 00 1a 08 08   ·5H···@· aE------
0020  08 08 dc 56 00 35 00 21  fd 0c 7c 84 01 00 00 01   ···V·5·! ··|-----
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   -------m it·edu··
0040  02 00 01                                           ···
```

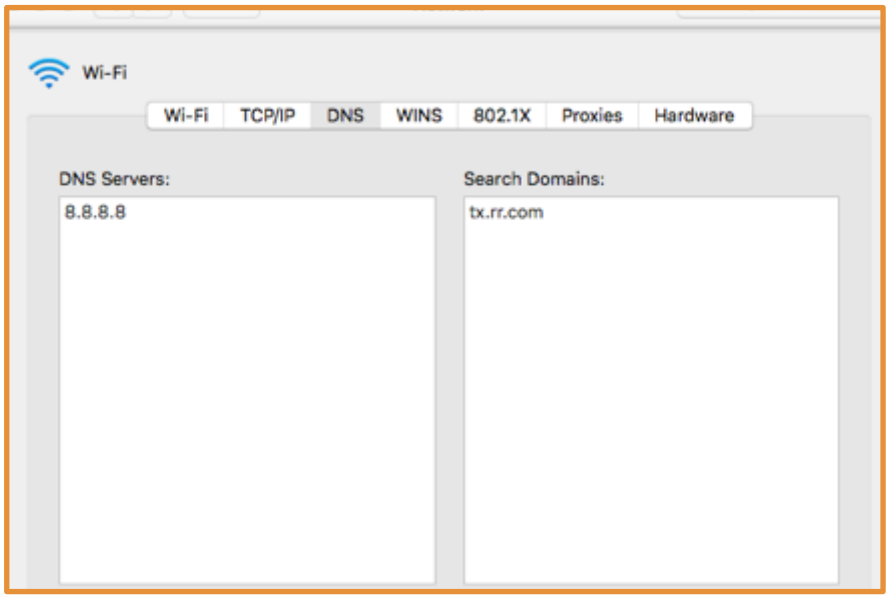


```
No.  Time        Source                    Destination               Protocol  Info
 4   1.382509    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x3fbe PTR 34.0.168.192.in-addr.arpa
 5   1.396573    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x3fbe No such name PTR 34.0.168.192.in-addr.arpa
 6   1.838535    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x7c84 NS mit.edu
 7   1.859952    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x7c84 NS mit.edu NS asia1.akam.net NS asia2.akam.n
 9   2.382620    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x65e0 PTR 26.0.168.192.in-addr.arpa
10   2.382867    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0x3f53 PTR 8.8.8.8.in-addr.arpa
12   2.416378    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x65e0 No such name PTR 26.0.168.192.in-addr.arpa
13   2.424253    google-public-dns-a.google.com  192.168.0.26          DNS  Standard query response 0x3f53 PTR 8.8.8.8.in-addr.arpa PTR google-public-d
14   3.382554    192.168.0.26              google-public-dns-a.google.com  DNS  Standard query 0xb0a7 PTR a.5.f.1.c.7.e.f.f.f.3.0.a.6.2.5.0.0.0.0.0.0.0.0.0.0

▸ Frame 7: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
▸ Ethernet II, Src: Netgear_7c:1f:5a (50:6a:03:7c:1f:5a), Dst: Elsys-MacBook-Air.local (d4:61:9d:27:61:4a)
▸ Internet Protocol Version 4, Src: google-public-dns-a.google.com (8.8.8.8), Dst: 192.168.0.26 (192.168.0.26)
▸ User Datagram Protocol, Src Port: domain (53), Dst Port: 56406 (56406)
▸ Domain Name System (response)

0000  d4 61 9d 27 61 4a 50 6a  03 7c 1f 5a 08 00 45 00   ·a·'aJPj ·|·Z··E·
0010  00 dc 96 84 00 00 78 11  da ba 08 08 08 08 c0 a8   ------x· --------
0020  00 1a 00 35 dc 56 00 c8  d0 af 7c 84 81 80 00 01   ···5·V·· ··|-----
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 04 70 00 10 05   -------- ----p···
0050  61 73 69 61 31 04 61 6b  61 6d 03 6e 65 74 00 c0   asia1·ak am·net···
0060  0c 00 02 00 01 00 00 04  70 00 08 05 61 73 69 61   -------- p···asia
0070  32 c0 2b c0 0c 00 02 00  01 00 00 04 70 00 07 04   2·+----- ----p···
0080  65 75 72 35 c0 2b c0 0c  00 02 00 01 00 00 04 70   eur5·+·· -------p
0090  00 0a 07 6e 73 31 2d 31  37 33 c0 2b c0 0c 00 02   ···ns1-1 73·+----
00a0  00 01 00 00 04 70 00 09  06 6e 73 31 2d 33 37 c0   -----p·· ·ns1-37·
00b0  2b c0 0c 00 02 00 01 00  00 04 70 00 07 04 75 73   +------- --p···us
00c0  77 32 c0 2b c0 0c 00 02  00 01 00 00 04 70 00 07   w2·+---- -----p··
00d0  04 75 73 65 35 c0 2b c0  0c 00 02 00 01 00 00 04   ·use5·+· --------
00e0  70 00 07 04 75 73 65 32  c0 2b                     p···use2 ·+
```

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

ANSWER:DNS query message sent over 8.8.8.8 as shown in the image. Yes it is same as local DNS Server





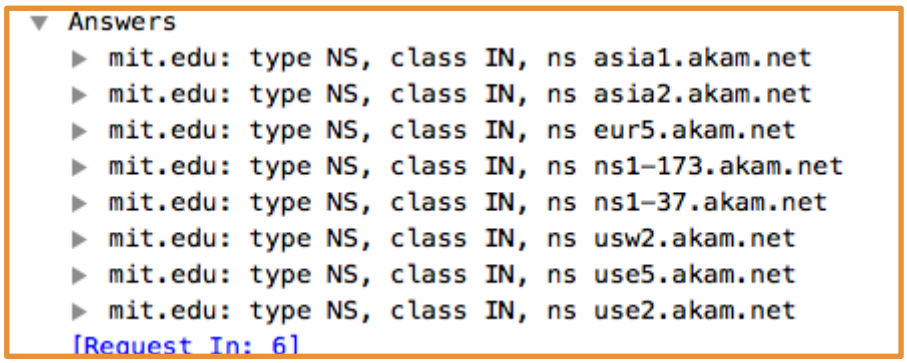
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANSWER:Query is of Type NS . Doesn't contain any answers.

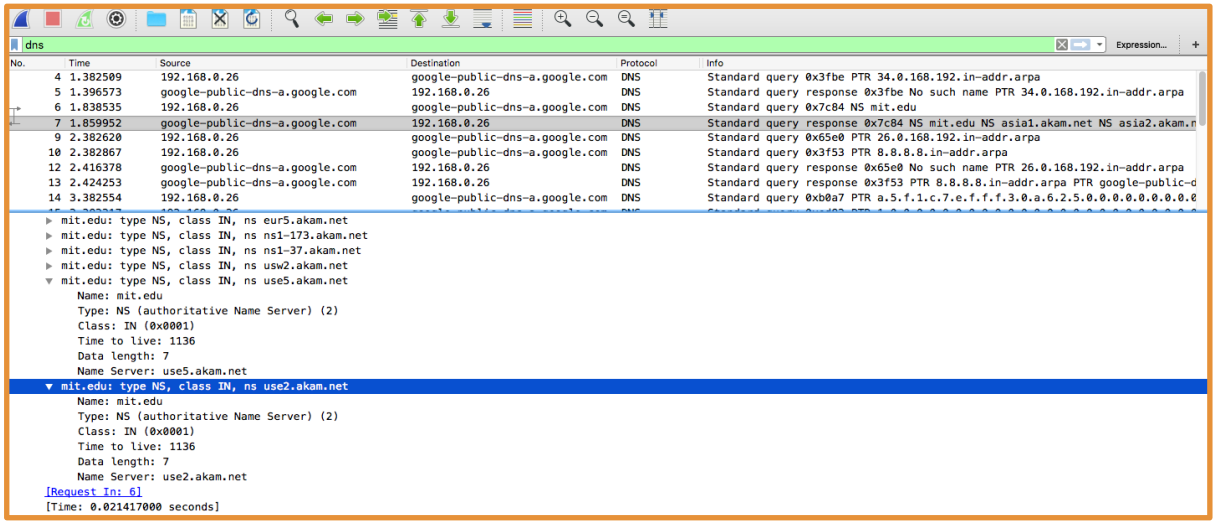
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

ANSWER: It provides 8 answers. Of Type =NS

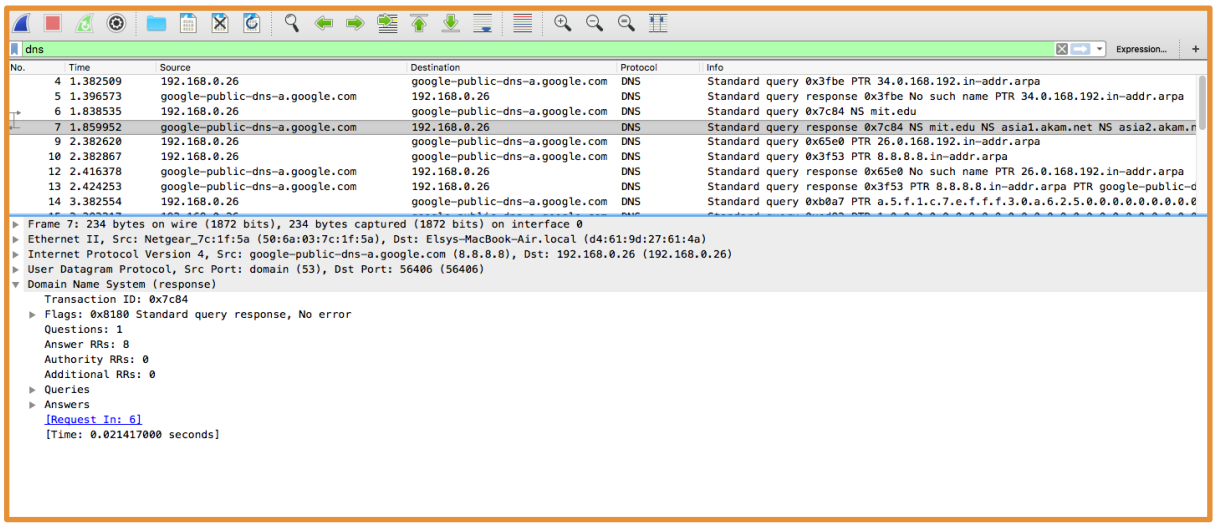
The MIT nameservers are:-

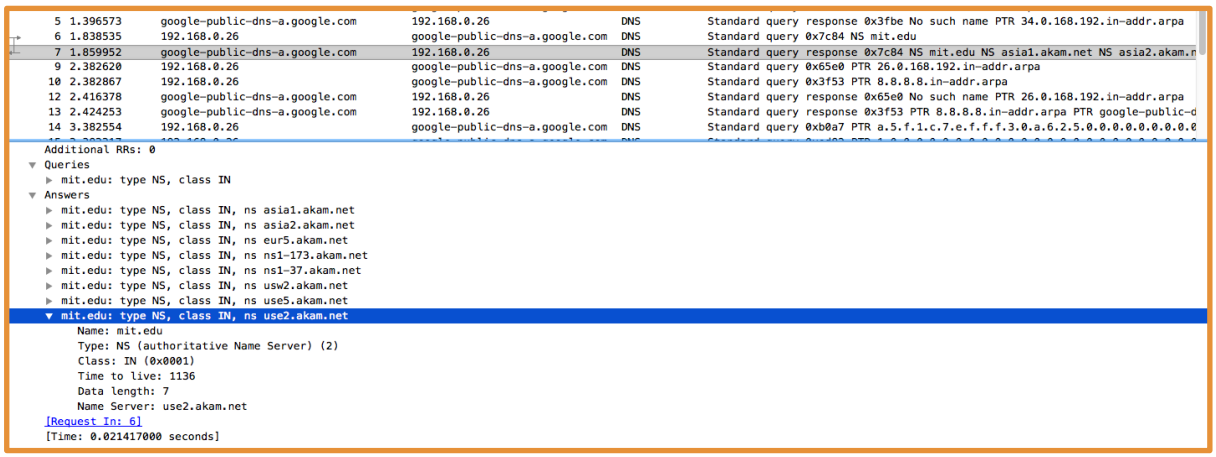


It does not give IP Address of nameservers .But, if you expand the answers you will find the details such as its type , Name, class,time to live,data length,name server but do not give IP Address.



19. Provide a screenshot.





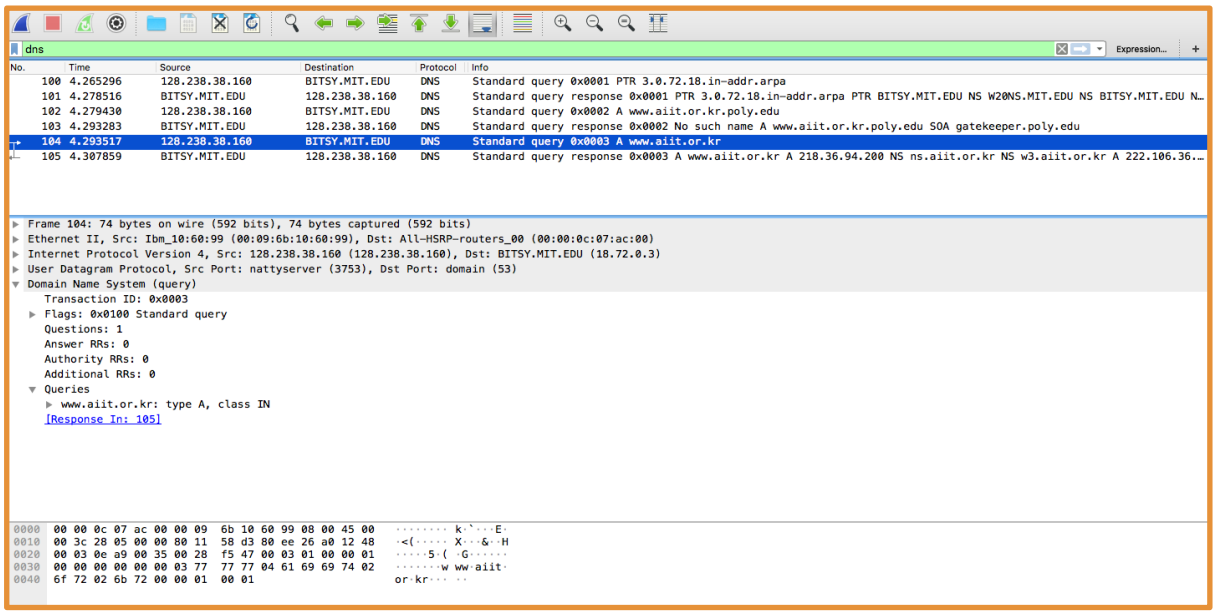
PART 5 : Tracing DNS with Wireshark(With -TYPE NSLOOKUP on two websites)
Steps to be followed before capture the packet.

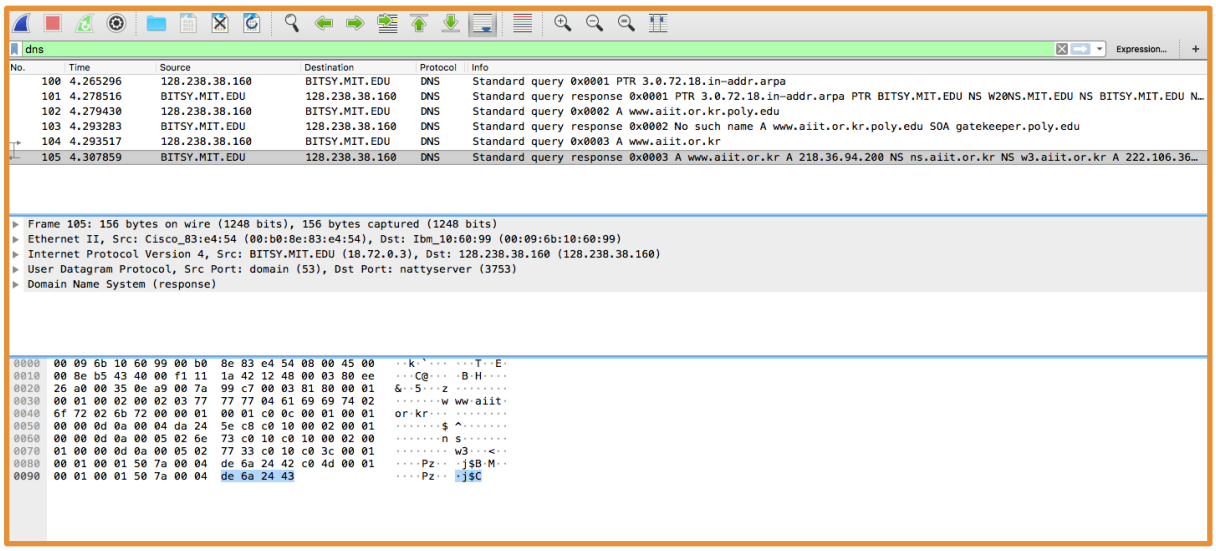
Step 1: Start packet capture.
Step 2: Do an nslookup on: **nslookup www.aiit.or.kr bitsy.mit.edu**

Note: As i had already mentioned in the email when i do nslookup with these two above websites in my system i get connection timed out error.

```
Elsys-MacBook-Air:~ el$ nslookup www.aiit.or bitsy.mit.edu
;; connection timed out; no servers could be reached

Elsys-MacBook-Air:~ el$
```

Hence, picking up the wireshark traces from the document to answer the below questions:-





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?

```
▶ Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
▼ Internet Protocol Version 4, Src: 128.238.38.160 (128.238.38.160), Dst: BITSY.MIT.EDU (18.72.0.3)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x2805 (10245)
  ▼ Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x58d3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.238.38.160 (128.238.38.160)
    Destination: BITSY.MIT.EDU (18.72.0.3)
▶ User Datagram Protocol, Src Port: nattyserver (3753), Dst Port: domain (53)
▶ Domain Name System (query)
```

Note: This is the trace i picked from the document .

ANSWER: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”?

ANSWER:Query is of Type A . Doesn’t contain any answers.

```
104 4.293517   128.238.38.160   BITSY.MIT.EDU   DNS   Standard query 0x0003 A www.aiit.or.kr
105 4.307859   BITSY.MIT.EDU    128.238.38.160   DNS   Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.…

▶ Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
▶ Internet Protocol Version 4, Src: 128.238.38.160 (128.238.38.160), Dst: BITSY.MIT.EDU (18.72.0.3)
▶ User Datagram Protocol, Src Port: nattyserver (3753), 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.aiit.or.kr: type A, class IN
    [Response In: 105]
```

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

```
104 4.293517   128.238.38.160   BITSY.MIT.EDU   DNS   Standard query 0x0003 A www.aiit.or.kr
105 4.307859   BITSY.MIT.EDU    128.238.38.160   DNS   Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36…

▶ Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
▶ Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09:6b:10:60:99)
▶ Internet Protocol Version 4, Src: BITSY.MIT.EDU (18.72.0.3), Dst: 128.238.38.160 (128.238.38.160)
▶ User Datagram Protocol, Src Port: domain (53), Dst Port: nattyserver (3753)
▼ 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 IN
  ▼ Answers
    ▶ www.aiit.or.kr: type A, class IN, addr 218.36.94.200
  ▼ Authoritative nameservers
    ▶ aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
    ▶ aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
  ▼ Additional records
    ▶ ns.aiit.or.kr: type A, class IN, addr 222.106.36.66
    ▶ w3.aiit.or.kr: type A, class IN, addr 222.106.36.67
    [Request In: 104]
    [Time: 0.014342000 seconds]

0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 8e b5 43 40 00 f1 11  1a 42 12 48 00 03 80 ee   ···C@··· ·B·H····
0020  26 a0 00 35 0e a9 00 7a  99 c7 00 03 81 80 00 01   &··5···z ********
0030  00 01 00 02 00 02 03 77  77 77 04 61 69 69 74 02   *******w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01 c0 0c 00 01 00 01   or·kr··· ********
0050  00 00 0d 0a 00 04 da 24  5e c8 c0 10 00 02 00 01   *******$ ^*******
0060  00 00 0d 0a 00 05 02 6e  73 c0 10 c0 10 00 02 00   *******n s*******
0070  01 00 00 0d 0a 00 05 02  77 33 c0 10 c0 3c 00 01   ******** w3···<··
0080  00 01 00 01 50 7a 00 04  de 6a 24 42 c0 4d 00 01   ····Pz·· ·j$B·M··
0090  00 01 00 01 50 7a 00 04  de 6a 24 43               ····Pz·· ·j$C
```

```
Class: IN (0x0001)
▼ 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: www.aiit.or.kr (218.36.94.200)
```

ANSWER:Contain 1 answer. Answer basically contain Name,Type, class,Time to live,Datalength and address information.

23. Provide a screenshot.

ANSWER:-

```
104 4.293517   128.238.38.160   BITSY.MIT.EDU   DNS   Standard query 0x0003 A www.aiit.or.kr
105 4.307859   BITSY.MIT.EDU    128.238.38.160  DNS   Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36…

▶ Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
▶ Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09:6b:10:60:99)
▶ Internet Protocol Version 4, Src: BITSY.MIT.EDU (18.72.0.3), Dst: 128.238.38.160 (128.238.38.160)
▶ User Datagram Protocol, Src Port: domain (53), Dst Port: nattyserver (3753)
▼ 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 IN
  ▼ Answers
    ▶ www.aiit.or.kr: type A, class IN, addr 218.36.94.200
  ▼ Authoritative nameservers
    ▶ aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
    ▶ aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
  ▼ Additional records
    ▶ ns.aiit.or.kr: type A, class IN, addr 222.106.36.66
    ▶ w3.aiit.or.kr: type A, class IN, addr 222.106.36.67
    [Request In: 104]
    [Time: 0.014342000 seconds]

0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 8e b5 43 40 00 f1 11  1a 42 12 48 00 03 80 ee   ···C@··· ·B·H····
0020  26 a0 00 35 0e a9 00 7a  99 c7 00 03 81 80 00 01   &··5···z ********
0030  00 01 00 02 00 02 03 77  77 77 04 61 69 69 74 02   *******w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01 c0 0c 00 01 00 01   or·kr··· ********
0050  00 00 0d 0a 00 04 da 24  5e c8 c0 10 00 02 00 01   *******$ ^*******
0060  00 00 0d 0a 00 05 02 6e  73 c0 10 c0 10 00 02 00   *******n s*******
0070  01 00 00 0d 0a 00 05 02  77 33 c0 10 c0 3c 00 01   ******** w3···<··
0080  00 01 00 01 50 7a 00 04  de 6a 24 42 c0 4d 00 01   ····Pz·· ·j$B·M··
0090  00 01 00 01 50 7a 00 04  de 6a 24 43               ····Pz·· ·j$C
```


```
Class: IN (0x0001)
▼ 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: www.aiit.or.kr (218.36.94.200)
```

dns-ethereal-trace-4

dns

No.	Time	Source	Destination	Protocol	Info
100	4.265296	128.238.38.160	BITSY.MIT.EDU	DNS	Standard query 0x0001 .
101	4.278516	BITSY.MIT.EDU	128.238.38.160	DNS	Standard query respons.
102	4.279430	128.238.38.160	BITSY.MIT.EDU	DNS	Standard query 0x0002 .
103	4.293283	BITSY.MIT.EDU	128.238.38.160	DNS	Standard query respons.
104	4.293517	128.238.38.160	BITSY.MIT.EDU	DNS	Standard query 0x0003 .

```
▼ Authoritative nameservers
  ▼ aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
      Name: aiit.or.kr
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 3338
      Data length: 5
      Name Server: ns.aiit.or.kr
  ▶ aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
▼ Additional records
  ▶ ns.aiit.or.kr: type A, class IN, addr 222.106.36.66
  ▶ w3.aiit.or.kr: type A, class IN, addr 222.106.36.67
  [Request In: 104]
  [Time: 0.014342000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 8e b5 43 40 00 f1 11  1a 42 12 48 00 03 80 ee   ···C@··· ·B·H····
0020  26 a0 00 35 0e a9 00 7a  99 c7 00 03 81 80 00 01   &··5···z ********
0030  00 01 00 02 00 02 03 77  77 77 04 61 69 69 74 02   *******w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01 c0 0c 00 01 00 01   or·kr··· ********
0050  00 00 0d 0a 00 04 da 24  5e c8 c0 10 00 02 00 01   *******$ ^*******
0060  00 00 0d 0a 00 05 02 6e  73 c0 10 c0 10 00 02 00   *******n s*******
0070  01 00 00 0d 0a 00 05 02  77 33 c0 10 c0 3c 00 01   ******** w3···<··
```

Query Class (dns.qry.class), 2 bytes Packets: 155 · Displayed: 6 (3.9%) Profile: Default