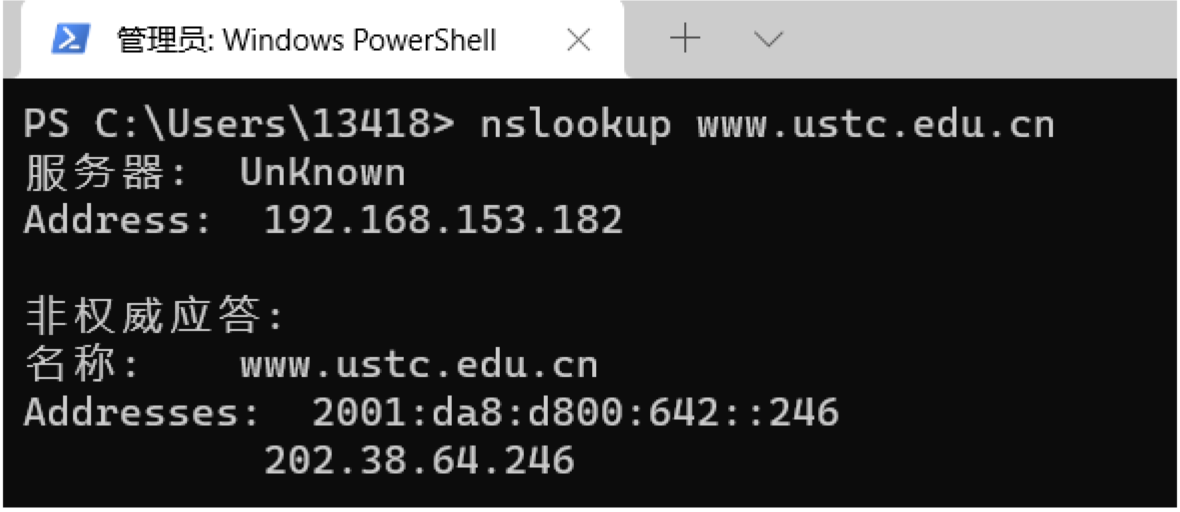
Computer Network Study Lab 3

- Author:PB19000362 钟书锐
- Time:2021.10.6

1. nslookup

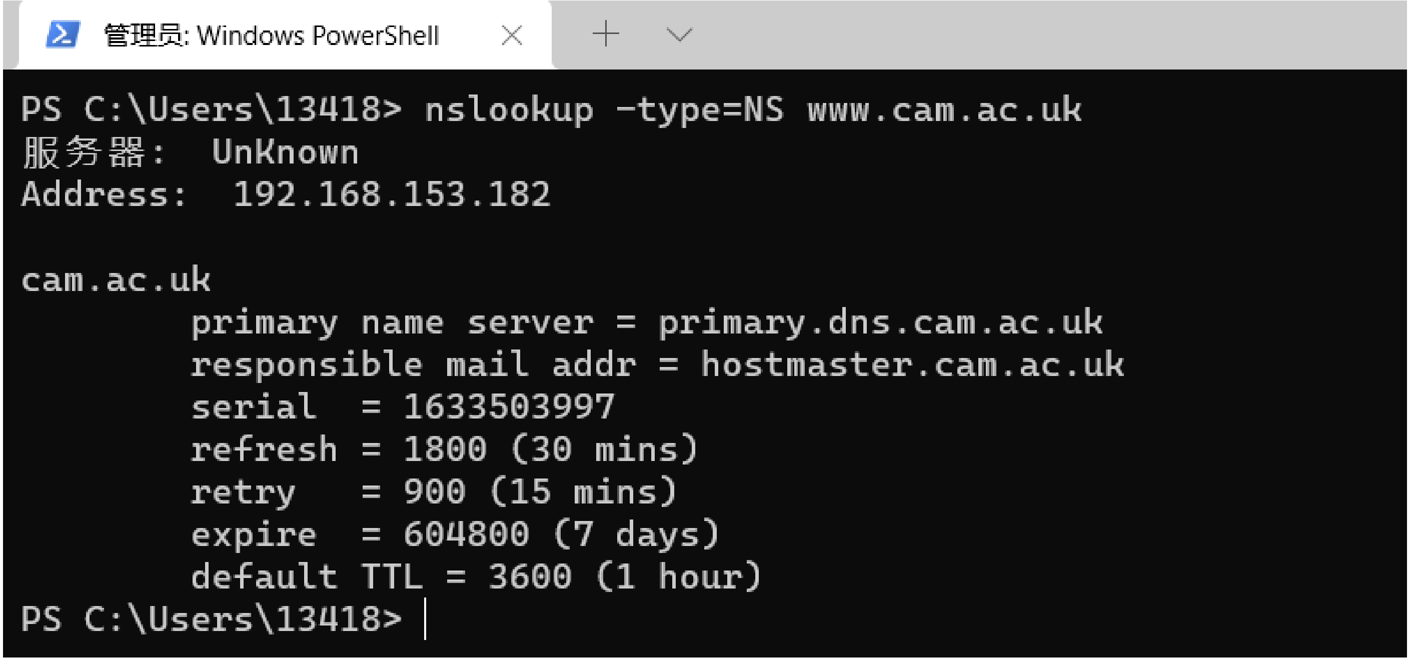
Q1.Run nslookupto obtain the IP address of a Web server in Asia. What is the IP address of that server?



```
PS C:\Users\13418> nslookup www.ustc.edu.cn
服务器:  UnKnown
Address:  192.168.153.182

非权威应答:
名称:    www.ustc.edu.cn
Addresses:  2001:da8:d800:642::246
          202.38.64.246
```

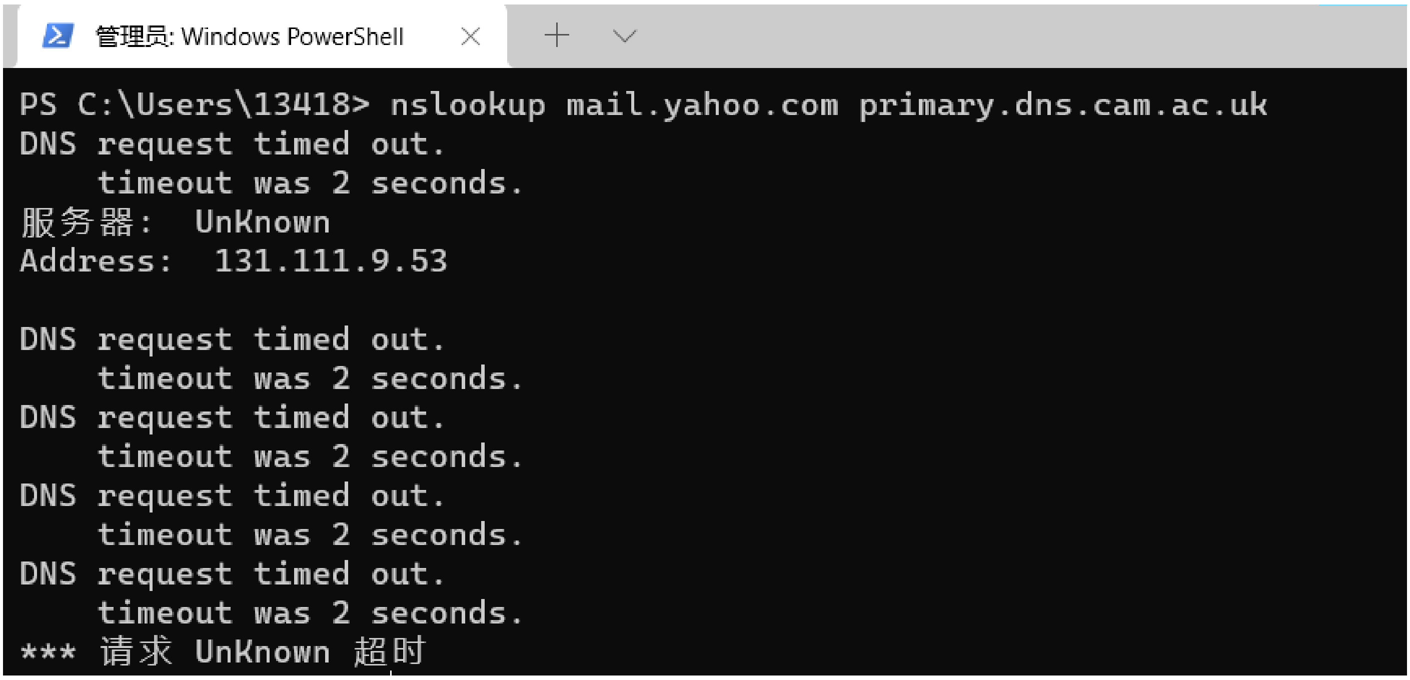
- Addresses: 2001:da8:d800:642::246 202.38.64.246

Q2.Run nslookupto determine the authoritative DNS servers for a university in Europe.



```
PS C:\Users\13418> nslookup -type=NS www.cam.ac.uk
服务器:  UnKnown
Address:  192.168.153.182

cam.ac.uk
        primary name server = primary.dns.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1633503997
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
PS C:\Users\13418>
```

Q3.Run nslookupso that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

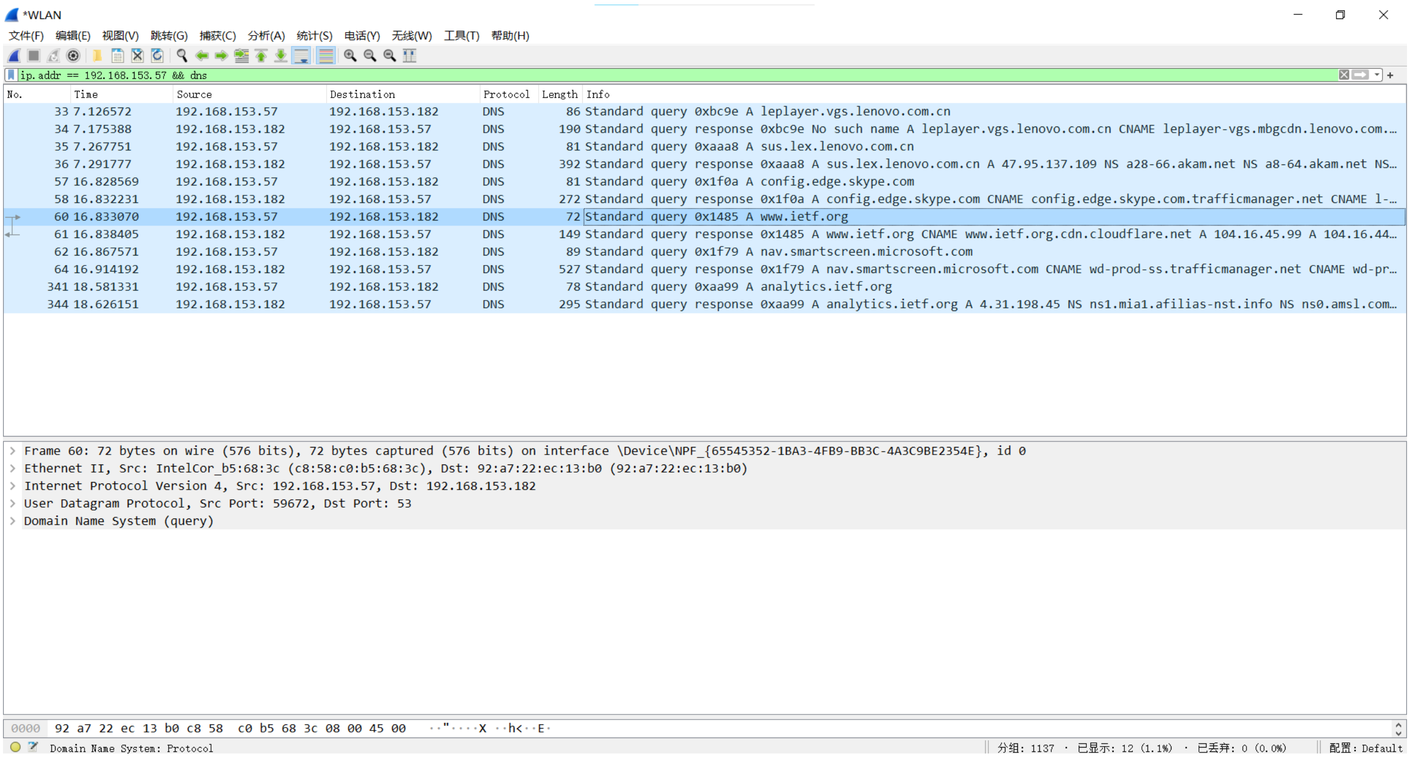


```
PS C:\Users\13418> nslookup mail.yahoo.com primary.dns.cam.ac.uk
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  131.111.9.53

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时
```

查询失败

2.ipconfig

3.Tracing DNS with Wireshark



```
ip.addr == 192.168.153.57 && dns
```

```
No.  Time       Source           Destination      Protocol Length Info
  33 7.126572   192.168.153.57   192.168.153.182  DNS        86 Standard query 0xbc9e A leplayer.vgs.lenovo.com.cn
  34 7.175388   192.168.153.182  192.168.153.57   DNS       190 Standard query response 0xbc9e No such name A leplayer.vgs.lenovo.com.cn CNAME leplayer-vgs.mbgcdn.lenovo.com.…
  35 7.267751   192.168.153.57   192.168.153.182  DNS        81 Standard query 0xaaa8 A sus.lex.lenovo.com.cn
  36 7.291777   192.168.153.182  192.168.153.57   DNS       392 Standard query response 0xaaa8 A sus.lex.lenovo.com.cn A 47.95.137.109 NS a28-66.akam.net NS a8-64.akam.net NS…
  57 16.828569  192.168.153.57   192.168.153.182  DNS        81 Standard query 0x1f0a A config.edge.skype.com
  58 16.832231  192.168.153.182  192.168.153.57   DNS       272 Standard query response 0x1f0a A config.edge.skype.com CNAME config.edge.skype.com.trafficmanager.net CNAME l-…
  60 16.833070  192.168.153.57   192.168.153.182  DNS        72 Standard query 0x1485 A www.ietf.org
  61 16.838405  192.168.153.182  192.168.153.57   DNS       149 Standard query response 0x1485 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44…
  62 16.867571  192.168.153.57   192.168.153.182  DNS        89 Standard query 0x1f79 A nav.smartscreen.microsoft.com
  64 16.914192  192.168.153.182  192.168.153.57   DNS       527 Standard query response 0x1f79 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pr…
 341 18.581331  192.168.153.57   192.168.153.182  DNS        78 Standard query 0xaa99 A analytics.ietf.org
 344 18.626151  192.168.153.182  192.168.153.57   DNS       295 Standard query response 0xaa99 A analytics.ietf.org A 4.31.198.45 NS ns1.mia1.afilias-nst.info NS ns0.amsl.com…
```

```
> Frame 60: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 59672, Dst Port: 53
> Domain Name System (query)
```

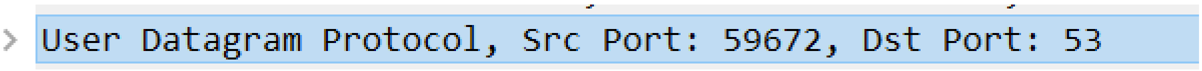
```
0000  92 a7 22 ec 13 b0 c8 58  c0 b5 68 3c 08 00 45 00   ··"····X ··h<··E·
```

```
Domain Name System: Protocol          分组: 1137 · 已显示: 12 (1.1%) · 已丢弃: 0 (0.0%)    配置: Default
```

Q4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

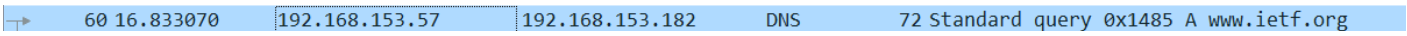
- UDP

Q5. What is the destination port for the DNS query message? What is the source port of DNS response message?

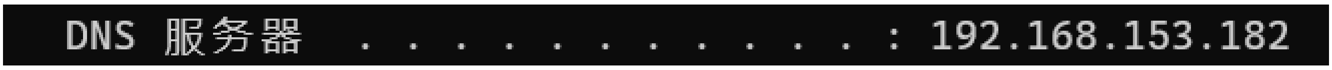
- 53 

```
> User Datagram Protocol, Src Port: 59672, Dst Port: 53
```

Q6. 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?



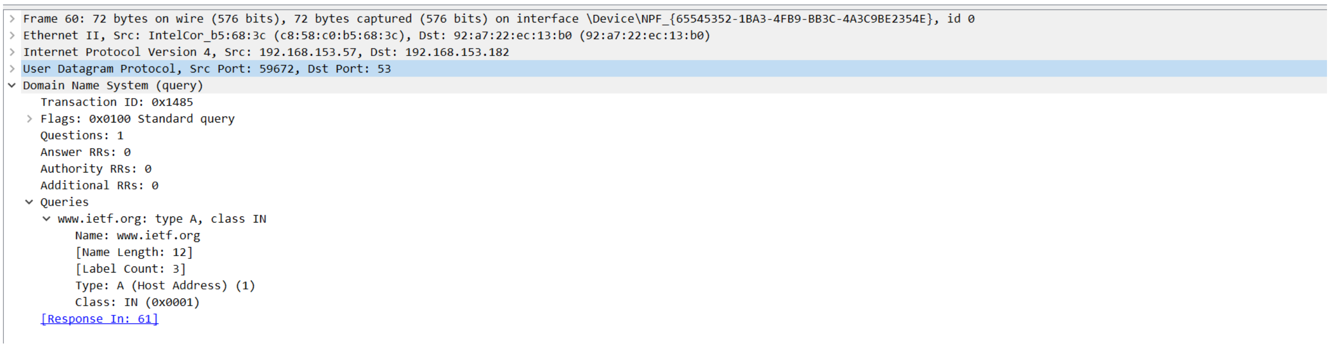
```
60 16.833070   192.168.153.57   192.168.153.182   DNS   72 Standard query 0x1485 A www.ietf.org
```



```
DNS 服务器  . . . . . . . . . . . : 192.168.153.182
```

- 192. 168. 153. 182
- same

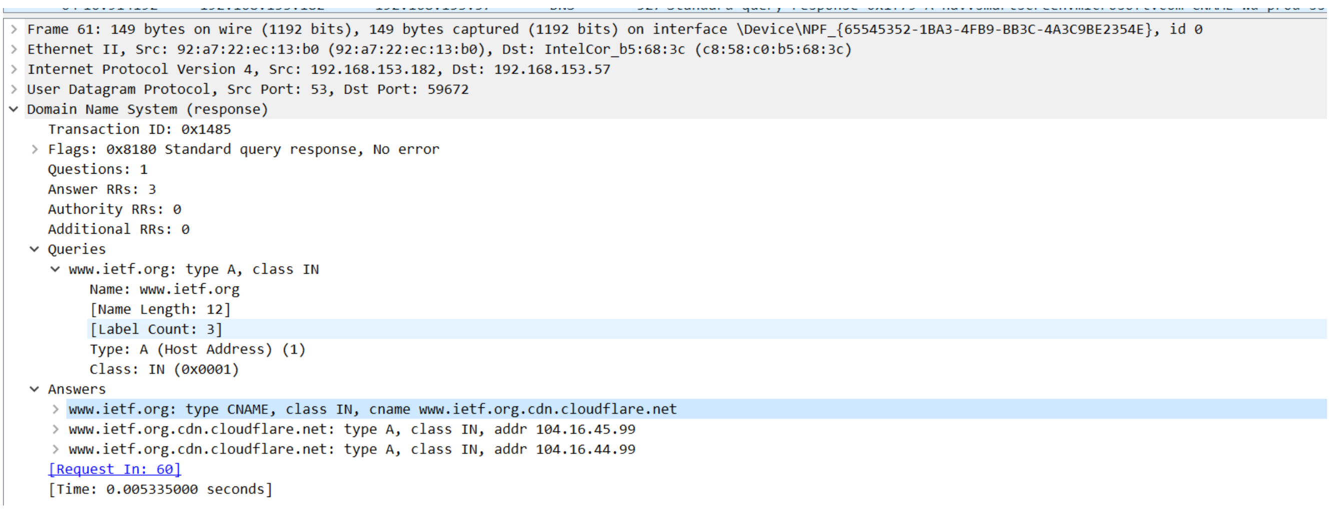
Q7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- 

```
> Frame 60: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 59672, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x1485
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 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)
    [Response In: 61]
```

- type A
- no any “answers”

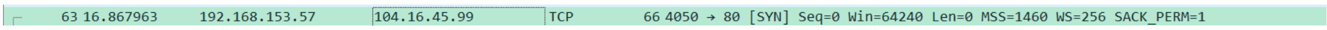
Q8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

- 

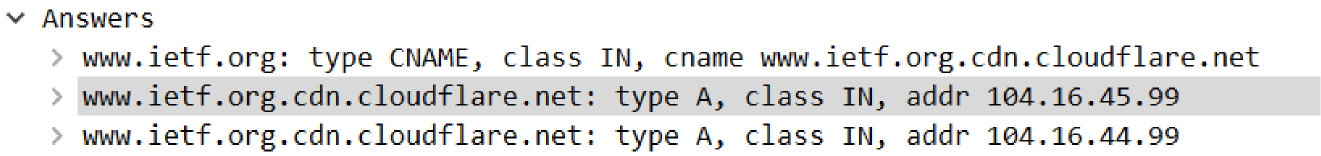
```
> Frame 61: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0), Dst: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c)
> Internet Protocol Version 4, Src: 192.168.153.182, Dst: 192.168.153.57
> User Datagram Protocol, Src Port: 53, Dst Port: 59672
v Domain Name System (response)
    Transaction ID: 0x1485
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 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)
  v 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 104.16.45.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 60]
    [Time: 0.005335000 seconds]
```

- 3

Q9. 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?

- 

```
63 16.867963    192.168.153.57    104.16.45.99    TCP    66 4050 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

- 

```
∨ 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 104.16.45.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

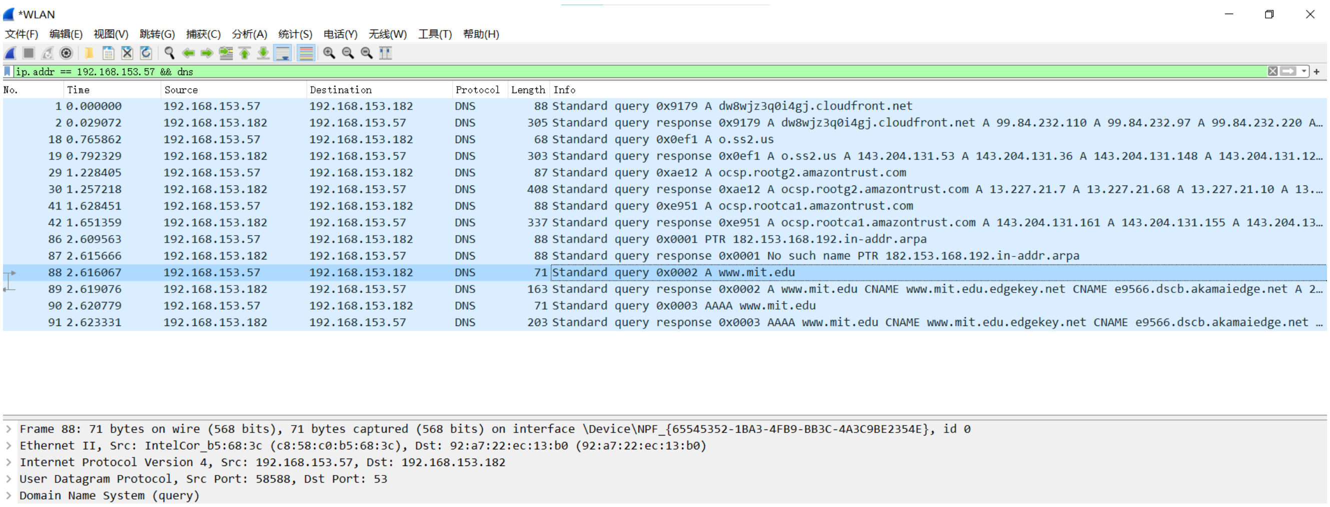
- yes

Q10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

- no

Q11. What is the destination port for the DNS query message? What is the source port of DNS response message?

- 53

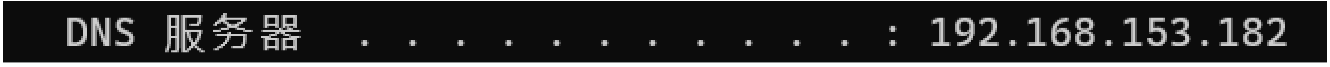


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

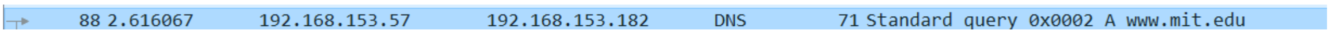
```
ip.addr == 192.168.153.57 && dns
No.  Time        Source            Destination       Protocol Length Info
   1 0.000000    192.168.153.57    192.168.153.182   DNS      88 Standard query 0x9179 A dw8wjz3q0i4gj.cloudfront.net
   2 0.029072    192.168.153.182   192.168.153.57    DNS     305 Standard query response 0x9179 A dw8wjz3q0i4gj.cloudfront.net A 99.84.232.110 A 99.84.232.97 A 99.84.232.220 A…
  18 0.765862    192.168.153.57    192.168.153.182   DNS      68 Standard query 0x0ef1 A o.ss2.us
  19 0.792329    192.168.153.182   192.168.153.57    DNS     303 Standard query response 0x0ef1 A o.ss2.us A 143.204.131.53 A 143.204.131.36 A 143.204.131.148 A 143.204.131.12…
  29 1.228405    192.168.153.57    192.168.153.182   DNS      87 Standard query 0xae12 A ocsp.rootg2.amazontrust.com
  30 1.257218    192.168.153.182   192.168.153.57    DNS     408 Standard query response 0xae12 A ocsp.rootg2.amazontrust.com A 13.227.21.7 A 13.227.21.68 A 13.227.21.10 A 13.…
  41 1.628451    192.168.153.57    192.168.153.182   DNS      88 Standard query 0xe951 A ocsp.rootca1.amazontrust.com
  42 1.651359    192.168.153.182   192.168.153.57    DNS     337 Standard query response 0xe951 A ocsp.rootca1.amazontrust.com A 143.204.131.161 A 143.204.131.155 A 143.204.13…
  86 2.609563    192.168.153.57    192.168.153.182   DNS      88 Standard query 0x0001 PTR 182.153.168.192.in-addr.arpa
  87 2.615666    192.168.153.182   192.168.153.57    DNS      88 Standard query response 0x0001 No such name PTR 182.153.168.192.in-addr.arpa
  88 2.616067    192.168.153.57    192.168.153.182   DNS      71 Standard query 0x0002 A www.mit.edu
  89 2.619076    192.168.153.182   192.168.153.57    DNS     163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 2…
  90 2.620779    192.168.153.57    192.168.153.182   DNS      71 Standard query 0x0003 AAAA www.mit.edu
  91 2.623331    192.168.153.182   192.168.153.57    DNS     203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net …

> Frame 88: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 58588, Dst Port: 53
> Domain Name System (query)
```

-

Q12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

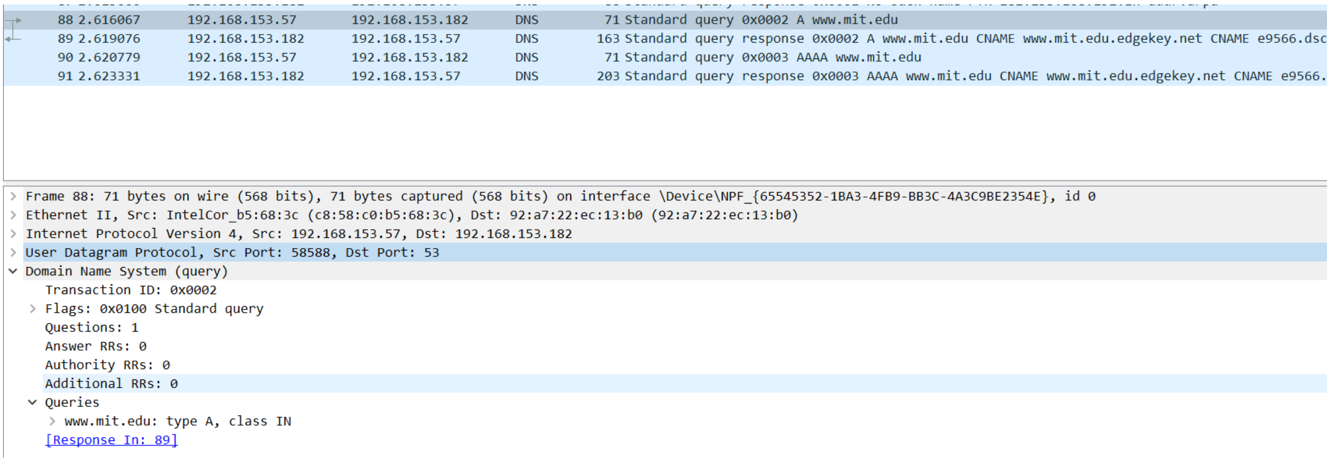
- 192. 168. 153. 182
- yes
- 

```
DNS 服务器 . . . . . . . . . . . : 192.168.153.182
```

- 

```
88 2.616067    192.168.153.57    192.168.153.182    DNS    71 Standard query 0x0002 A www.mit.edu
```

Q13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- 

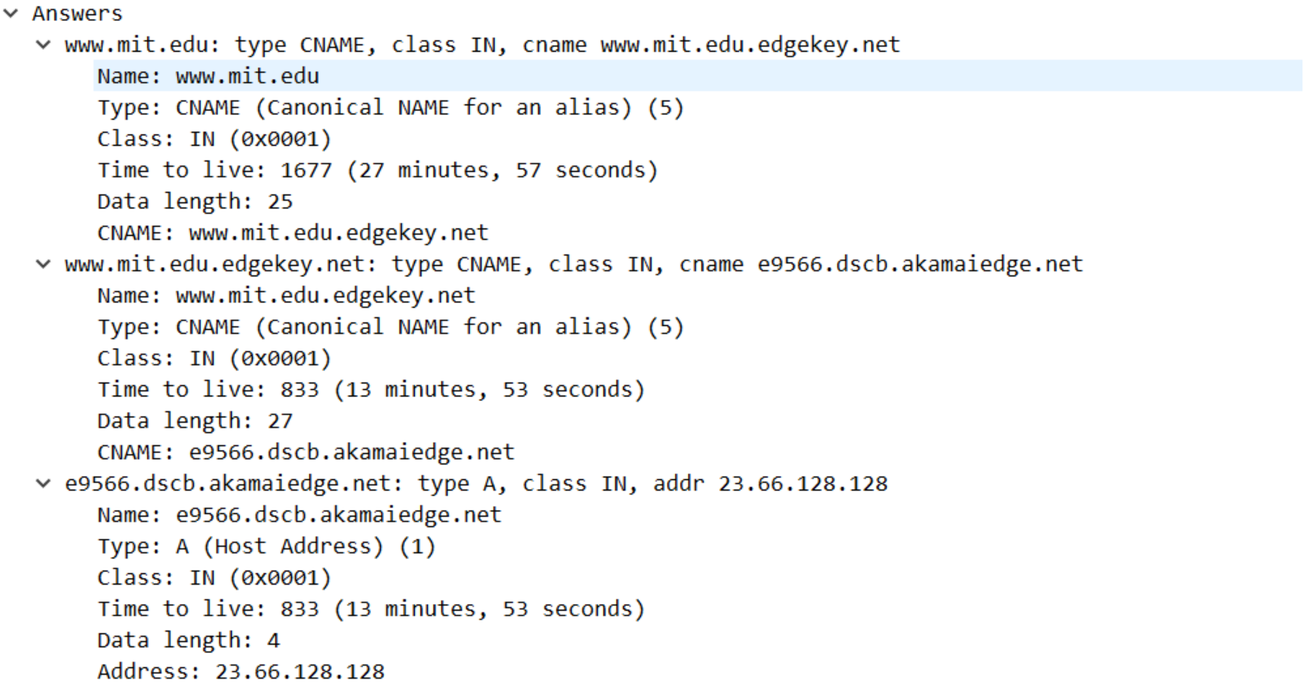
```
 88 2.616067   192.168.153.57    192.168.153.182   DNS    71 Standard query 0x0002 A www.mit.edu
 89 2.619076   192.168.153.182   192.168.153.57    DNS   163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dsc
 90 2.620779   192.168.153.57    192.168.153.182   DNS    71 Standard query 0x0003 AAAA www.mit.edu
 91 2.623331   192.168.153.182   192.168.153.57    DNS   203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.
```

```
> Frame 88: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 58588, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
    [Response In: 89]
```

- type A
- no any “answers”

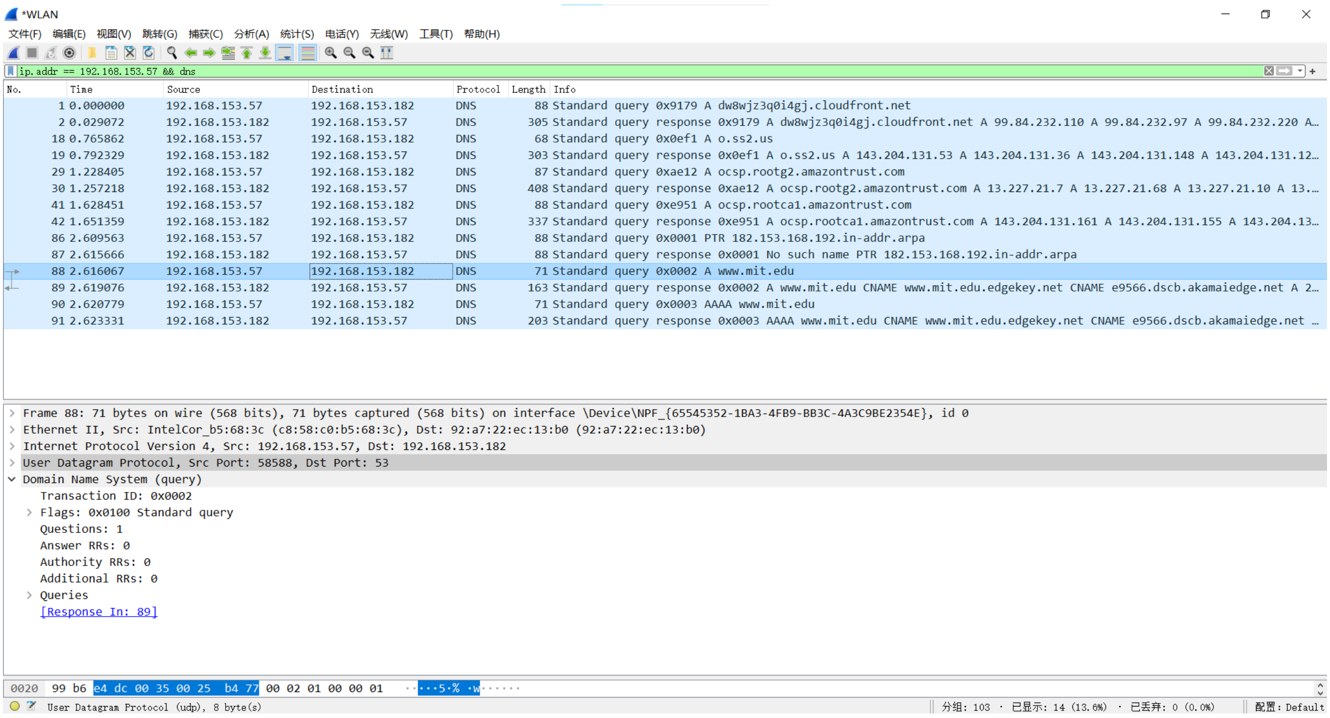
Q14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

- 3



```
v Answers
  v 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: 1677 (27 minutes, 57 seconds)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  v 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: 833 (13 minutes, 53 seconds)
      Data length: 27
      CNAME: e9566.dscb.akamaiedge.net
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.66.128.128
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 833 (13 minutes, 53 seconds)
      Data length: 4
      Address: 23.66.128.128
```

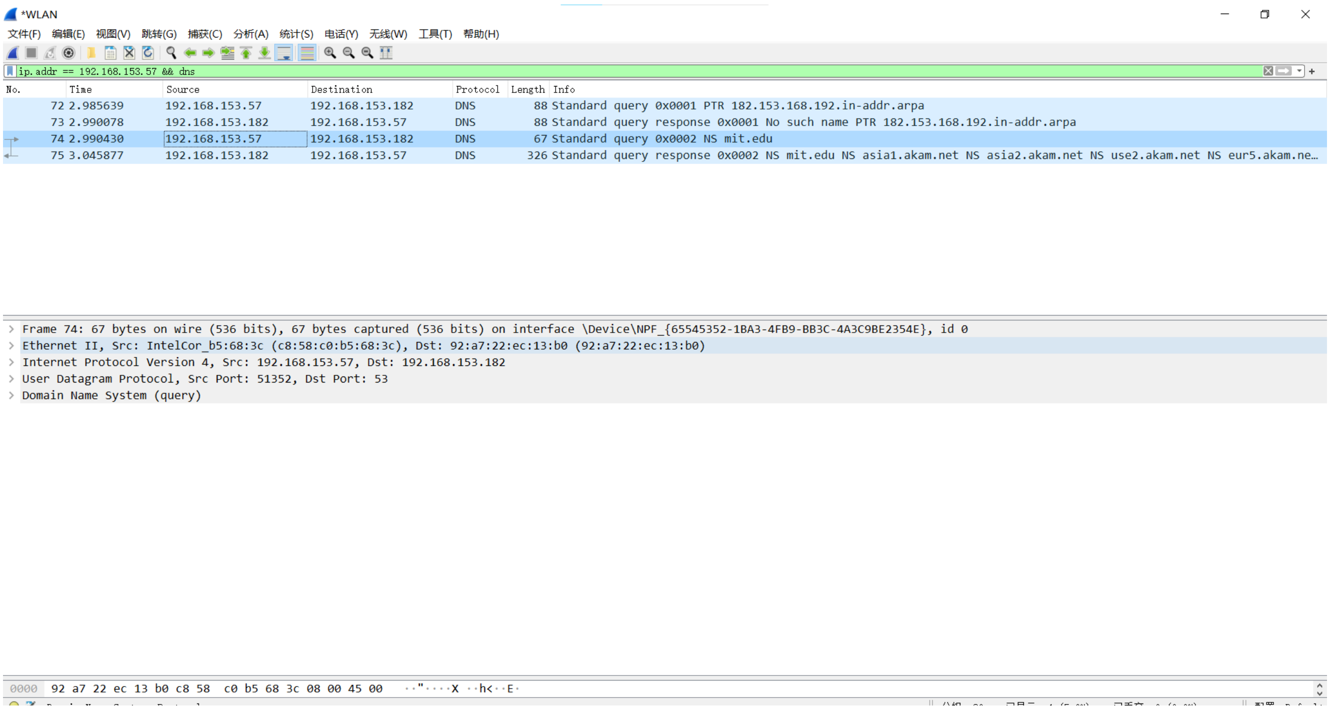
Q15. Provide a screenshot.

- 

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

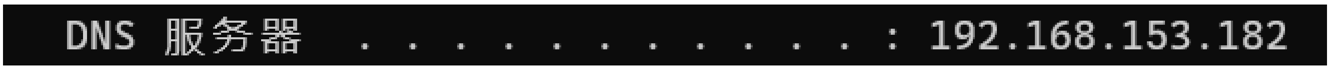
```
ip.addr == 192.168.153.57 && dns

No.   Time      Source           Destination      Protocol Length Info
    1 0.000000  192.168.153.57   192.168.153.182  DNS       88 Standard query 0x9179 A dw8wjz3q0i4gj.cloudfront.net
    2 0.029072  192.168.153.182  192.168.153.57   DNS      305 Standard query response 0x9179 A dw8wjz3q0i4gj.cloudfront.net A 99.84.232.110 A 99.84.232.97 A 99.84.232.220 A…
   18 0.765862  192.168.153.57   192.168.153.182  DNS       68 Standard query 0x0ef1 A o.ss2.us
   19 0.792329  192.168.153.182  192.168.153.57   DNS      303 Standard query response 0x0ef1 A o.ss2.us A 143.204.131.53 A 143.204.131.36 A 143.204.131.148 A 143.204.131.12…
   29 1.228405  192.168.153.57   192.168.153.182  DNS       87 Standard query 0xae12 A ocsp.rootg2.amazontrust.com
   30 1.257218  192.168.153.182  192.168.153.57   DNS      408 Standard query response 0xae12 A ocsp.rootg2.amazontrust.com A 13.227.21.7 A 13.227.21.68 A 13.227.21.10 A 13.…
   41 1.628451  192.168.153.57   192.168.153.182  DNS       88 Standard query 0xe951 A ocsp.rootca1.amazontrust.com
   42 1.651359  192.168.153.182  192.168.153.57   DNS      337 Standard query response 0xe951 A ocsp.rootca1.amazontrust.com A 143.204.131.161 A 143.204.131.155 A 143.204.13…
   86 2.609563  192.168.153.57   192.168.153.182  DNS       88 Standard query 0x0001 PTR 182.153.168.192.in-addr.arpa
   87 2.615666  192.168.153.182  192.168.153.57   DNS       88 Standard query response 0x0001 No such name PTR 182.153.168.192.in-addr.arpa
   88 2.616067  192.168.153.57   192.168.153.182  DNS       71 Standard query 0x0002 A www.mit.edu
   89 2.619076  192.168.153.182  192.168.153.57   DNS      163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 2…
   90 2.620779  192.168.153.57   192.168.153.182  DNS       71 Standard query 0x0003 AAAA www.mit.edu
   91 2.623331  192.168.153.182  192.168.153.57   DNS      203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net …

> Frame 88: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 58588, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 89]

0020  99 b6 e4 dc 00 35 00 25  b4 77 00 02 01 00 00 01   ·····5·%·w······

User Datagram Protocol (udp), 8 byte(s)     分组: 103 · 已显示: 14 (13.6%) · 已丢弃: 0 (0.0%)     配置: Default
```

Q16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

- 

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

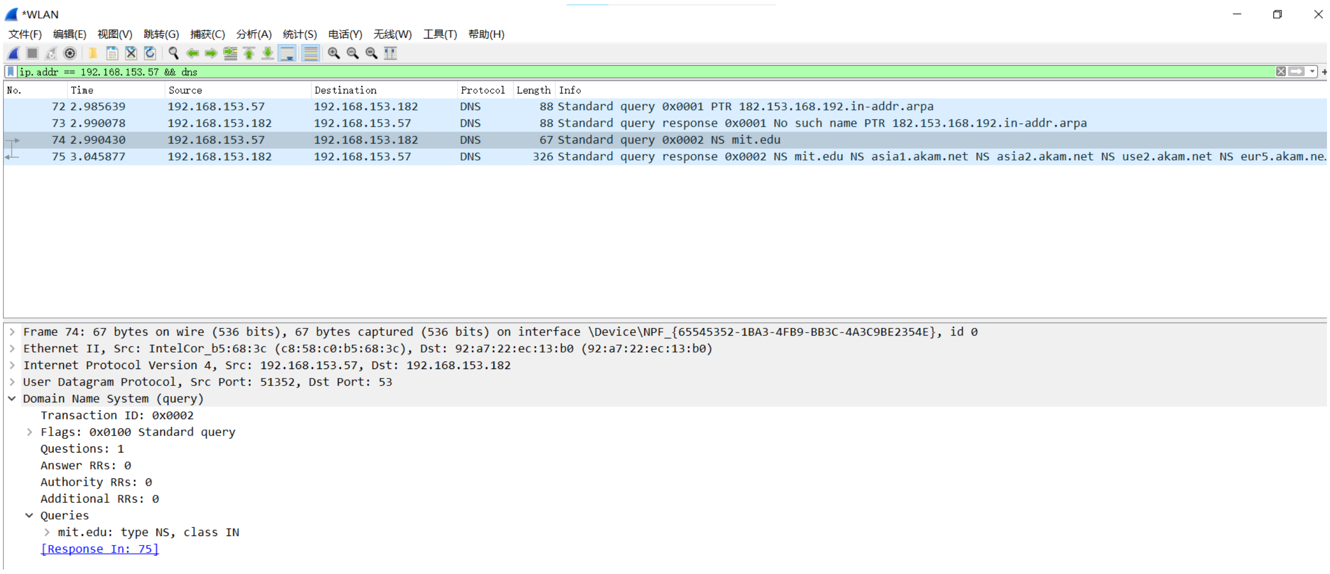
```
ip.addr == 192.168.153.57 && dns

No.   Time      Source           Destination      Protocol Length Info
   72 2.985639  192.168.153.57   192.168.153.182  DNS       88 Standard query 0x0001 PTR 182.153.168.192.in-addr.arpa
   73 2.990078  192.168.153.182  192.168.153.57   DNS       88 Standard query response 0x0001 No such name PTR 182.153.168.192.in-addr.arpa
   74 2.990430  192.168.153.57   192.168.153.182  DNS       67 Standard query 0x0002 NS mit.edu
   75 3.045877  192.168.153.182  192.168.153.57   DNS      326 Standard query response 0x0002 NS mit.edu NS asia1.akam.net NS asia2.akam.net NS use2.akam.net NS eur5.akam.ne…

> Frame 74: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 51352, Dst Port: 53
> Domain Name System (query)

0000  92 a7 22 ec 13 b0 c8 58  c0 b5 68 3c 08 00 45 00   ··"····X ··h<··E·
```

- 

```
DNS 服务器 . . . . . . . . . . . : 192.168.153.182
```

- 192. 168. 153. 182
- yes

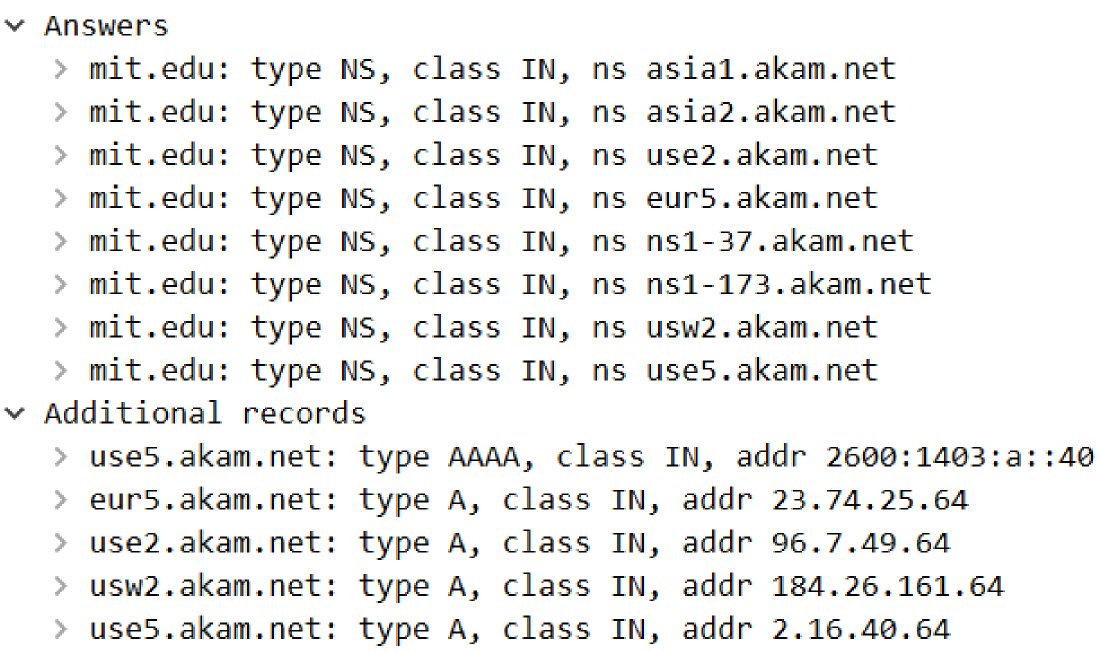
Q17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers” ?


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.addr == 192.168.153.57 && dns

No.   Time        Source            Destination       Protocol Length Info
   72 2.985639    192.168.153.57    192.168.153.182   DNS        88 Standard query 0x0001 PTR 182.153.168.192.in-addr.arpa
   73 2.990078    192.168.153.182   192.168.153.57    DNS        88 Standard query response 0x0001 No such name PTR 182.153.168.192.in-addr.arpa
   74 2.990430    192.168.153.57    192.168.153.182   DNS        67 Standard query 0x0002 NS mit.edu
   75 3.045877    192.168.153.182   192.168.153.57    DNS       326 Standard query response 0x0002 NS mit.edu NS asia1.akam.net NS asia2.akam.net NS use2.akam.net NS eur5.akam.ne

> Frame 74: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 51352, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type NS, class IN
    [Response In: 75]
```

- type NS
- no any “answers”

Q18. 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?

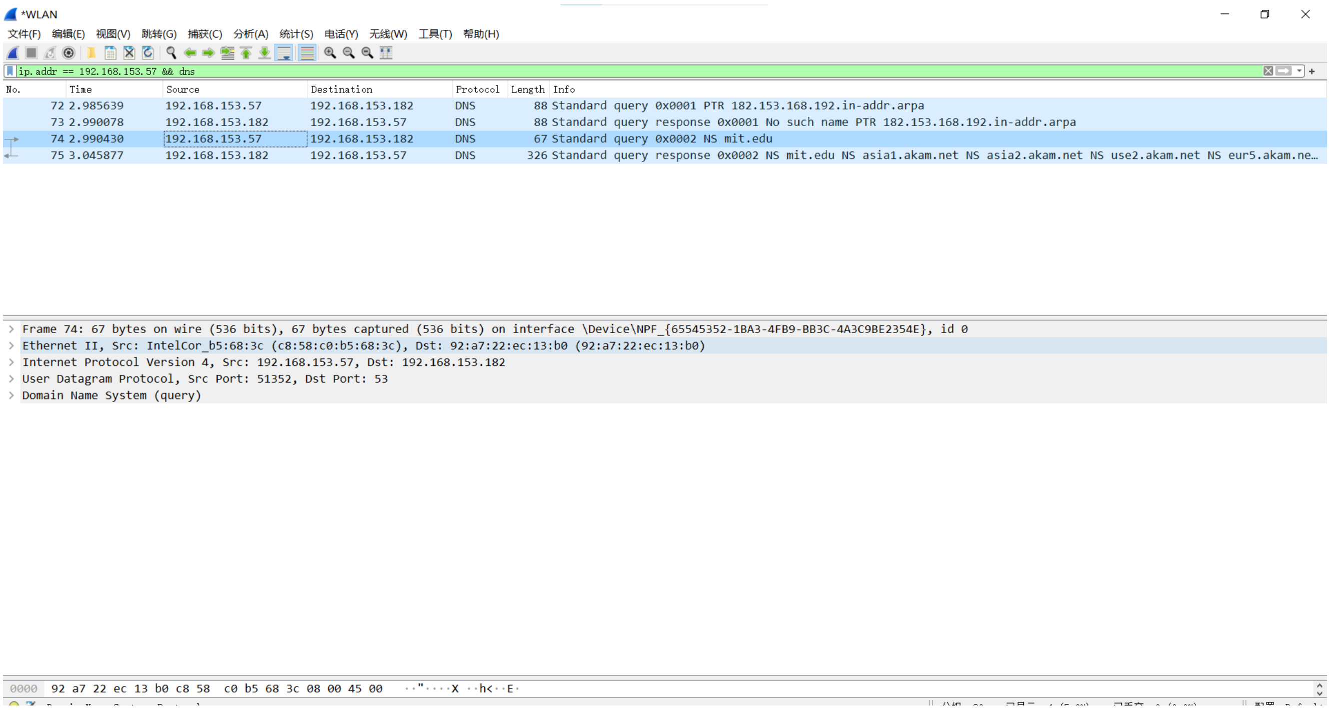


```
v Answers
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
v Additional records
    > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    > eur5.akam.net: type A, class IN, addr 23.74.25.64
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > usw2.akam.net: type A, class IN, addr 184.26.161.64
    > use5.akam.net: type A, class IN, addr 2.16.40.64
```

- mit.edu nameserver = asia1.akam.net
- mit.edu nameserver = asia2.akam.net
- mit.edu nameserver = use2.akam.net
- mit.edu nameserver = eur5.akam.net
- mit.edu nameserver = ns1-37.akam.net
- mit.edu nameserver = ns1-173.akam.net
- mit.edu nameserver = usw2.akam.net

- mit.edu nameserver = use5.akam.net
- yes, in Additional records.
  - use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
  - eur5.akam.net: type A, class IN, addr 23.74.25.64
  - use2.akam.net: type A, class IN, addr 96.7.49.64
  - usw2.akam.net: type A, class IN, addr 184.26.161.64
  - use5.akam.net: type A, class IN, addr 2.16.40.64

Q19. Provide a screenshot

- 

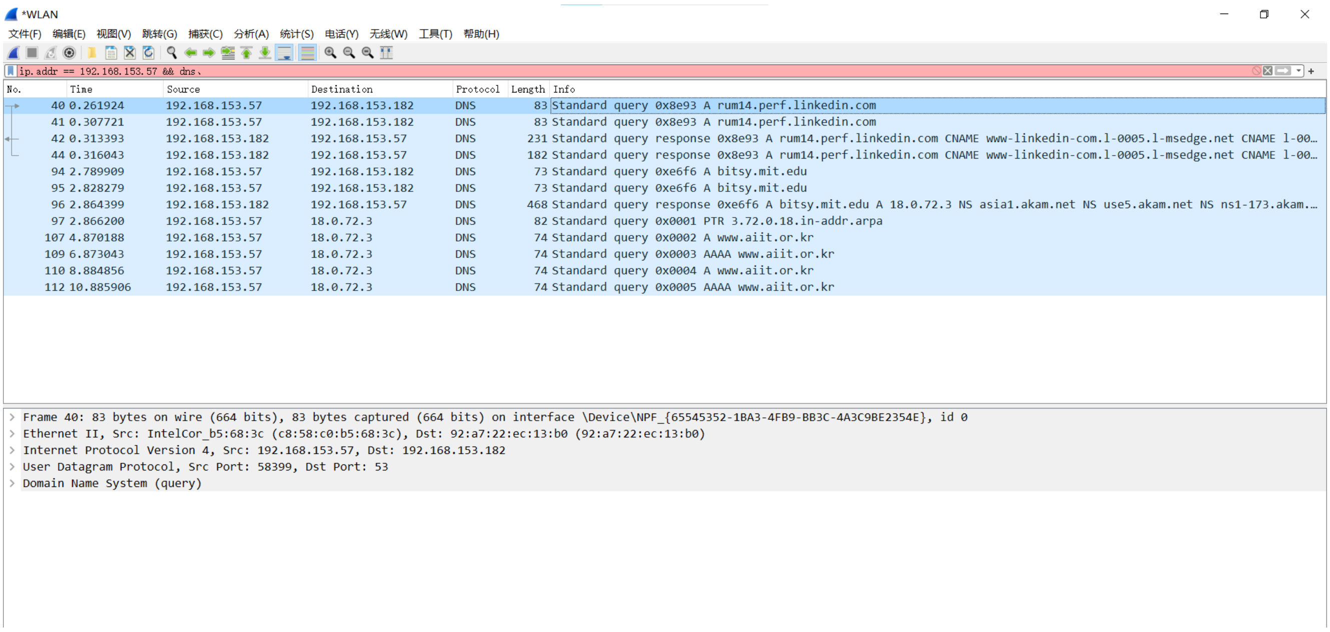
*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.addr == 192.168.153.57 && dns

No.   Time      Source           Destination      Protocol Length Info
   72 2.985639  192.168.153.57   192.168.153.182  DNS        88 Standard query 0x0001 PTR 182.153.168.192.in-addr.arpa
   73 2.990078  192.168.153.182  192.168.153.57   DNS        88 Standard query response 0x0001 No such name PTR 182.153.168.192.in-addr.arpa
   74 2.990430  192.168.153.57   192.168.153.182  DNS        67 Standard query 0x0002 NS mit.edu
   75 3.045877  192.168.153.182  192.168.153.57   DNS       326 Standard query response 0x0002 NS mit.edu NS asia1.akam.net NS asia2.akam.net NS use2.akam.net NS eur5.akam.ne…
```

```
> Frame 74: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 51352, Dst Port: 53
> Domain Name System (query)
```

```
0000  92 a7 22 ec 13 b0 c8 58  c0 b5 68 3c 08 00 45 00   ··"····X ··h<··E·
```

Q20. 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?

- 

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

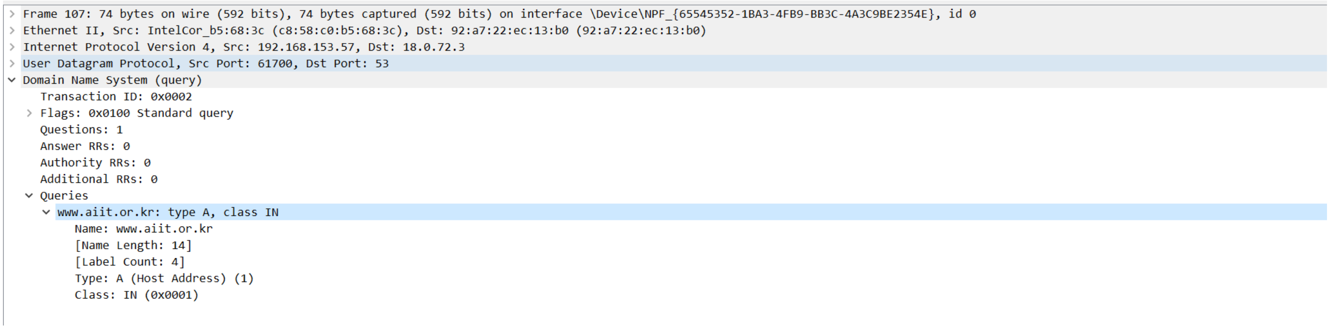
```
ip.addr == 192.168.153.57 && dns、

No.   Time      Source           Destination      Protocol Length Info
   40 0.261924  192.168.153.57   192.168.153.182  DNS        83 Standard query 0x8e93 A rum14.perf.linkedin.com
   41 0.307721  192.168.153.57   192.168.153.182  DNS        83 Standard query 0x8e93 A rum14.perf.linkedin.com
   42 0.313393  192.168.153.182  192.168.153.57   DNS       231 Standard query response 0x8e93 A rum14.perf.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-00…
   44 0.316043  192.168.153.182  192.168.153.57   DNS       182 Standard query response 0x8e93 A rum14.perf.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-00…
   94 2.789909  192.168.153.57   192.168.153.182  DNS        73 Standard query 0xe6f6 A bitsy.mit.edu
   95 2.828279  192.168.153.57   192.168.153.182  DNS        73 Standard query 0xe6f6 A bitsy.mit.edu
   96 2.864399  192.168.153.182  192.168.153.57   DNS       468 Standard query response 0xe6f6 A bitsy.mit.edu A 18.0.72.3 NS asia1.akam.net NS use5.akam.net NS ns1-173.akam.…
   97 2.866200  192.168.153.57   18.0.72.3        DNS        82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  107 4.870188  192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0002 A www.aiit.or.kr
  109 6.873043  192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0003 AAAA www.aiit.or.kr
  110 8.884856  192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0004 A www.aiit.or.kr
  112 10.885906 192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
> Frame 40: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 58399, Dst Port: 53
> Domain Name System (query)
```

- 访问 bitsy.mit.edu

    - yes
    - 192.168.153.182
- 访问 www.aiit.or.kr
    - no
    - 18.0.72.3
    - 不是默认本地 DNS 服务器的 IP 地址，是 bitsy.mit.edu 这个域名服务器的 IP 地址。

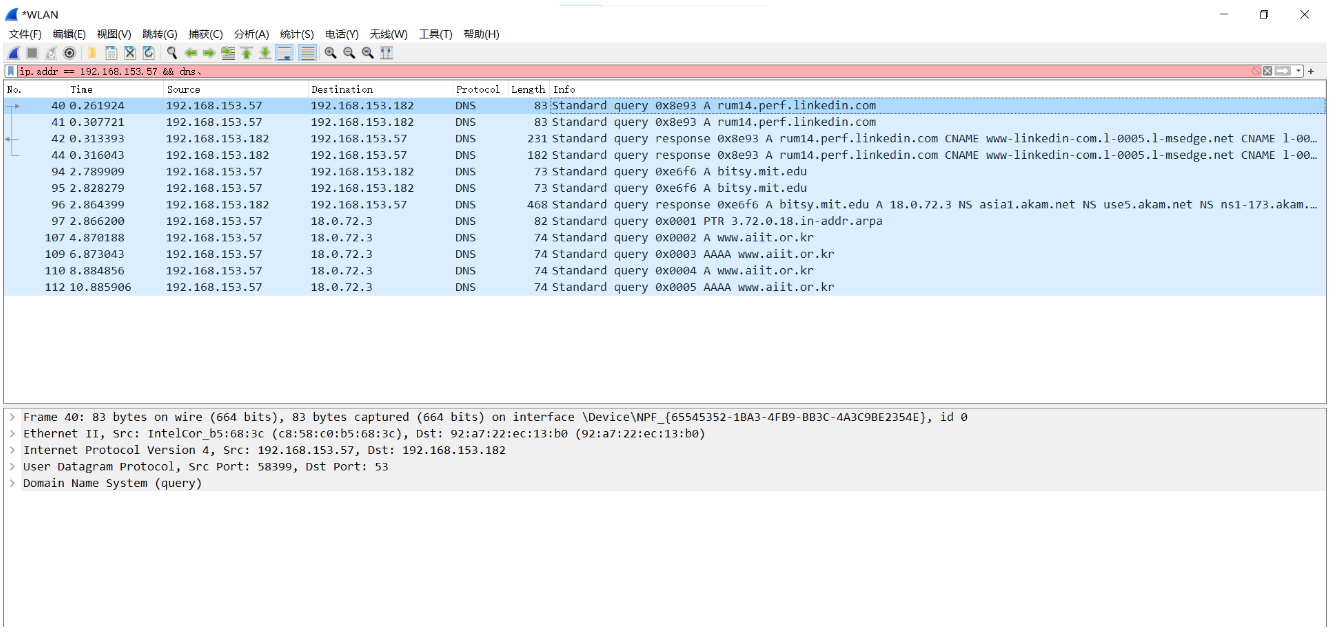
Q21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- 

```
> Frame 107: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 61700, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

- type:A
- no answer

Q22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

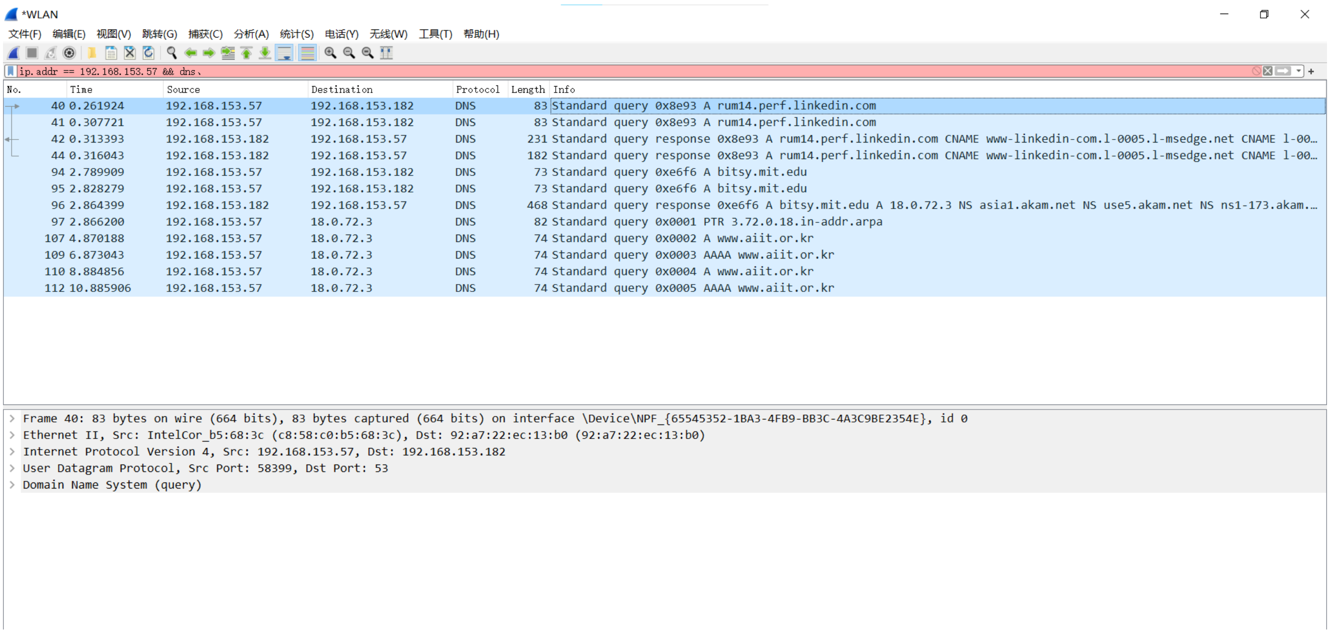
- 

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.addr == 192.168.153.57 && dns、

No.   Time       Source           Destination      Protocol Length Info
   40 0.261924   192.168.153.57   192.168.153.182  DNS        83 Standard query 0x8e93 A rum14.perf.linkedin.com
   41 0.307721   192.168.153.57   192.168.153.182  DNS        83 Standard query 0x8e93 A rum14.perf.linkedin.com
   42 0.313393   192.168.153.182  192.168.153.57   DNS       231 Standard query response 0x8e93 A rum14.perf.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-00…
   44 0.316043   192.168.153.182  192.168.153.57   DNS       182 Standard query response 0x8e93 A rum14.perf.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-00…
   94 2.789909   192.168.153.57   192.168.153.182  DNS        73 Standard query 0xe6f6 A bitsy.mit.edu
   95 2.828279   192.168.153.57   192.168.153.182  DNS        73 Standard query 0xe6f6 A bitsy.mit.edu
   96 2.864399   192.168.153.182  192.168.153.57   DNS       468 Standard query response 0xe6f6 A bitsy.mit.edu A 18.0.72.3 NS asia1.akam.net NS use5.akam.net NS ns1-173.akam.…
   97 2.866200   192.168.153.57   18.0.72.3        DNS        82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  107 4.870188   192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0002 A www.aiit.or.kr
  109 6.873043   192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0003 AAAA www.aiit.or.kr
  110 8.884856   192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0004 A www.aiit.or.kr
  112 10.885906  192.168.153.57   18.0.72.3        DNS        74 Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 40: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 58399, Dst Port: 53
> Domain Name System (query)
```

- no respose.
- 0

Q23. Provide a screenshot

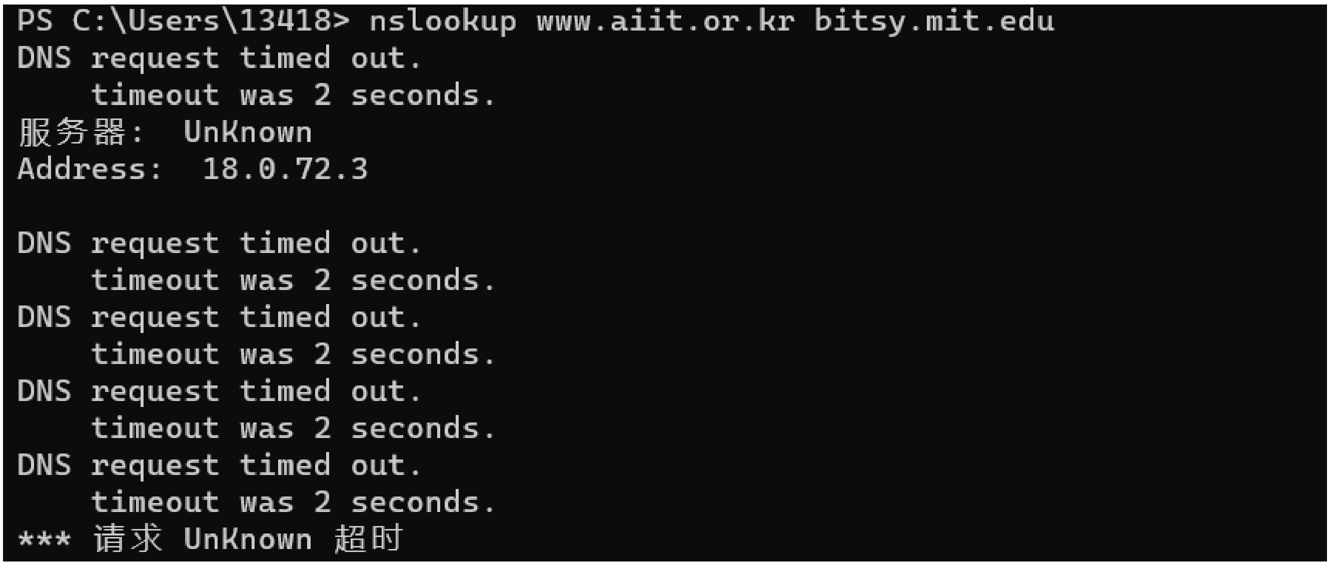
- 

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.addr == 192.168.153.57 && dns、
```

```
No.     Time       Source            Destination       Protocol  Length Info
     40 0.261924   192.168.153.57    192.168.153.182   DNS          83 Standard query 0x8e93 A rum14.perf.linkedin.com
     41 0.307721   192.168.153.57    192.168.153.182   DNS          83 Standard query 0x8e93 A rum14.perf.linkedin.com
     42 0.313393   192.168.153.182   192.168.153.57    DNS         231 Standard query response 0x8e93 A rum14.perf.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-00…
     44 0.316043   192.168.153.182   192.168.153.57    DNS         182 Standard query response 0x8e93 A rum14.perf.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-00…
     94 2.789909   192.168.153.57    192.168.153.182   DNS          73 Standard query 0xe6f6 A bitsy.mit.edu
     95 2.828279   192.168.153.57    192.168.153.182   DNS          73 Standard query 0xe6f6 A bitsy.mit.edu
     96 2.864399   192.168.153.182   192.168.153.57    DNS         468 Standard query response 0xe6f6 A bitsy.mit.edu A 18.0.72.3 NS asia1.akam.net NS use5.akam.net NS ns1-173.akam.…
     97 2.866200   192.168.153.57    18.0.72.3         DNS          82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
    107 4.870188   192.168.153.57    18.0.72.3         DNS          74 Standard query 0x0002 A www.aiit.or.kr
    109 6.873043   192.168.153.57    18.0.72.3         DNS          74 Standard query 0x0003 AAAA www.aiit.or.kr
    110 8.884856   192.168.153.57    18.0.72.3         DNS          74 Standard query 0x0004 A www.aiit.or.kr
    112 10.885906  192.168.153.57    18.0.72.3         DNS          74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
> Frame 40: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.153.57, Dst: 192.168.153.182
> User Datagram Protocol, Src Port: 58399, Dst Port: 53
> Domain Name System (query)
```

- 

```
PS C:\Users\13418> nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时
```