1.nslookup

实验步骤

1.**run the first command : nslookup www.mit.edu**

```
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Eiffel>nslookup www.mit.edu
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:9800:39a::255e
          2600:1417:9800:3b9::255e
          104.105.119.179
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

显示了本地服务器的名字及其IP地址和非权威服务器的应答，非权威应答包括了名称、www.mit.edu的IP地址及其别称。

（由于本地DNS服务器能够缓存权威DNS服务器的IP地址，故答案是从缓存中得到的而不是权威DNS服务器）

2.**run the command : nslookup -type=NS mit.edu**

```
C:\Users\Eiffel>nslookup -type=NS mit.edu
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-173.akam.net
```

option : -type = NS　　domain : mit.edu

这条命令让nslookup发送了一条type为NS的报文给默认本地DNS服务器。type为NS意味着RR（存储资源记录）中的name为域，value为该域的权威DNS服务器的主机名。

由于本地DNS服务器能够缓存权威DNS服务器的IP地址，故答案是从缓存中得到的而不是权威DNS服务器。

3.**run the command : nslookup www.aiit.or.kr bitsy.mit.edu**

这条命令是让主机向DNS服务器bitsy.mit.edu发送查询报文而不是默认的本地DNS服务器mx.ustc.edu.cn，要查询的是www.aiit.or.kr的IP地址

```
C:\Users\Eiffel>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
```

由于DNS服务器bitsy.mit.edu停用导致请求超时，故此处用阿里的DNS服务器，查到阿里的DNS服务器的首选IP地址为223.5.5.5，用命令

nslookup 223.5.5.5

进行查询其名称得到其名称为public1.alidns.com

```
C:\Users\Eiffel>nslookup 223.5.5.5
服务器:  UnKnown
Address:  fe80::27:53e9:753:973

名称:    public1.alidns.com
Address:  223.5.5.5
```

```
C:\Users\Eiffel>nslookup www.aiit.or.kr public1.alidns.com
服务器:  UnKnown
Address:  2400:3200::1

非权威应答:
名称:    www.aiit.or.kr
Address:  58.229.6.225
```

题目

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

```
C:\Users\Eiffel>nslookup jw.ustc.edu.cn
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

名称:    revproxy.ustc.edu.cn
Addresses:  2001:da8:d800:642::248
          202.38.64.246
Aliases:  jw.ustc.edu.cn
```

IP address : 2001:da8:d800:642::248
202.38.64.246

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

```
C:\Users\Eiffel>nslookup -type=NS ox.ac.uk
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk
ox.ac.uk        nameserver = ns2.ja.net
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk
```

权威DNS服务器的主机名

ox.ac.uk nameserver = auth5.dns.ox.ac.uk
ox.ac.uk nameserver = dns2.ox.ac.uk
ox.ac.uk nameserver = dns1.ox.ac.uk
ox.ac.uk nameserver = dns0.ox.ac.uk
ox.ac.uk nameserver = ns2.ja.net
ox.ac.uk nameserver = auth6.dns.ox.ac.uk
ox.ac.uk nameserver = auth4.dns.ox.ac.uk

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?**

```
C:\Users\Eiffel>nslookup mail.yahoo.com ox.ac.uk
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  151.101.2.216

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
```

由于请求超时，故直接对mail.yahoo.com进行查询

```
C:\Users\Eiffel>nslookup mail.yahoo.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    edge.gycpi.b.yahoodns.net
Addresses:  2001:4998:18:800::4002
          2001:4998:18:800::4003
          69.147.88.8
          69.147.88.7
Aliases:  mail.yahoo.com
```

IP地址为 2001:4998:18:800::4002
2001:4998:18:800::4003
69.147.88.8
69.147.88.7

2.ipconfig

1.ipconfig /all : 查看当前电脑网卡的IP信息、DNS信息、DHCP服务器信息等

```
C:\Users\Eiffel>ipconfig /all

Windows IP 配置

   主机名 . . . . . . . . . . . . . : LAPTOP-NHD5G5N9
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 以太网:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   物理地址. . . . . . . . . . . . . : 38-F3-AB-B7-A4-C7
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 本地连接* 1:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址. . . . . . . . . . . . . : 76-4C-A1-DA-20-A1
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 本地连接* 2:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   物理地址. . . . . . . . . . . . . : F6-4C-A1-DA-20-A1
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
   物理地址. . . . . . . . . . . . . : 74-4C-A1-DA-20-A1
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2409:8930:451:98f:78f9:f30e:d8ca:b6d7(首选)
   临时 IPv6 地址. . . . . . . . . . : 2409:8930:451:98f:d914:dde1:1e1a:46f4(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::78f9:f30e:d8ca:b6d7%15(首选)
   IPv4 地址 . . . . . . . . . . . . : 172.20.10.5(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.240
   获得租约的时间  . . . . . . . . . : 2021年10月5日 18:48:37
   租约过期的时间  . . . . . . . . . : 2021年10月6日 19:32:19
   默认网关. . . . . . . . . . . . . : fe80::27:53e9:753:973%15
                                       172.20.10.1
   DHCP 服务器 . . . . . . . . . . . : 172.20.10.1
   DHCPv6 IAID . . . . . . . . . . . : 158616737
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-28-5C-C2-7D-38-F3-AB-B7-A4-C7
```


```
                                       172.20.10.1
   DHCP 服务器 . . . . . . . . . . . : 172.20.10.1
   DHCPv6 IAID . . . . . . . . . . . : 158616737
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-28-5C-C2-7D-38-F3-AB-B7-A4-C7
```


```
   DNS 服务器  . . . . . . . . . . . : fe80::1888:2e6c:ea46:778d%15
                                       172.20.10.1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

以太网适配器 蓝牙网络连接:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   物理地址. . . . . . . . . . . . . : 74-4C-A1-DA-20-A2
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
```

2.ipconfig /displaydns : 以秒为单位显示了每个条目的生存时间(TTL)

太长了故只展示部分

```
C:\Users\Eiffel>ipconfig /displaydns

Windows IP 配置

    policy.video.iqiyi.com
    ----------------------------------------
    记录名称. . . . . . . . : policy.video.iqiyi.com
    记录类型. . . . . . . . : 5
    生存时间. . . . . . . . : 403
    数据长度. . . . . . . . : 8
    部分. . . . . . . . . . : 答案
    CNAME 记录 . . . . . . : static.dns.iqiyi.com


    记录名称. . . . . . . . : static.dns.iqiyi.com
    记录类型. . . . . . . . : 1
    生存时间. . . . . . . . : 403
    数据长度. . . . . . . . : 4
    部分. . . . . . . . . . : 答案
    A (主机)记录 . . . . . : 58.205.196.20


    ip.if.iqiyi.com
    ----------------------------------------
    记录名称. . . . . . . . : ip.if.iqiyi.com
    记录类型. . . . . . . . : 5
    生存时间. . . . . . . . : 28
    数据长度. . . . . . . . : 8
    部分. . . . . . . . . . : 答案
    CNAME 记录 . . . . . . : apigateway.iqiyi.com


    记录名称. . . . . . . . : apigateway.iqiyi.com
    记录类型. . . . . . . . : 1
    生存时间. . . . . . . . : 28
    数据长度. . . . . . . . : 4
    部分. . . . . . . . . . : 答案
    A (主机)记录 . . . . . : 49.7.32.101
```

3.ipconfig /flushdns : 刷新缓存并清除所有条目，再从主机文件上重新加载条目

```
C:\Users\Eiffel>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

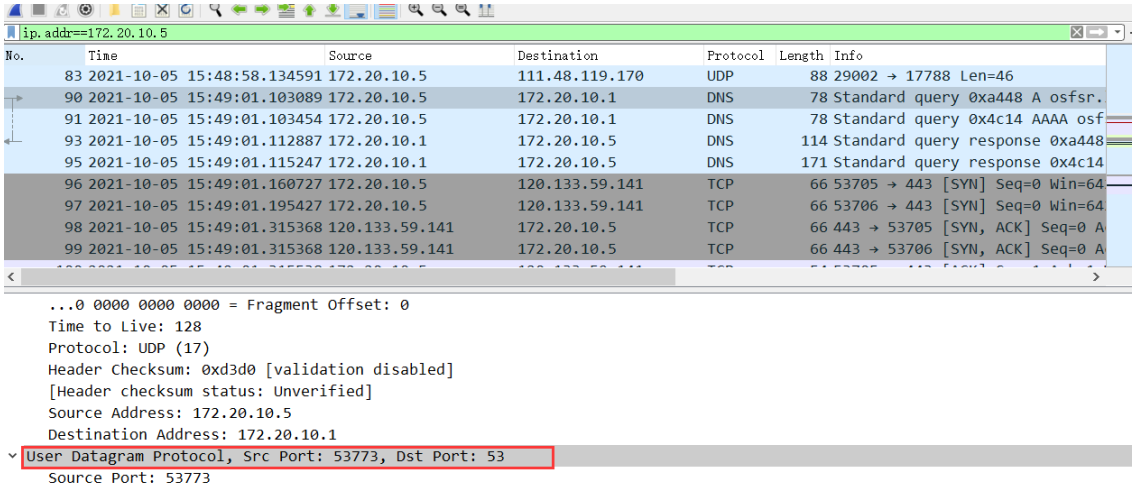
3.Tracing DNS with Wireshark

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

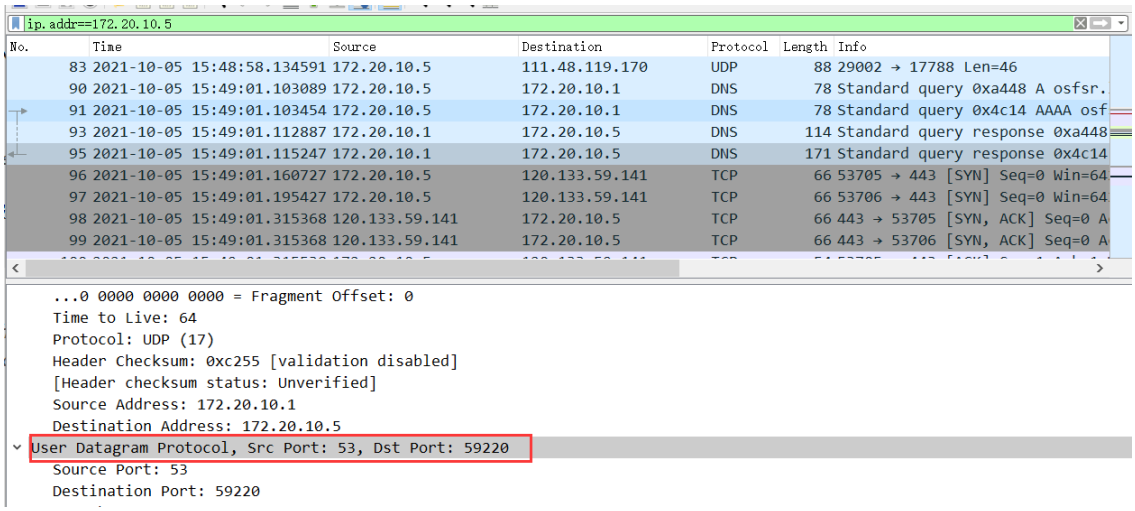
   UDP

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

   destination port for the DNS query message : 53

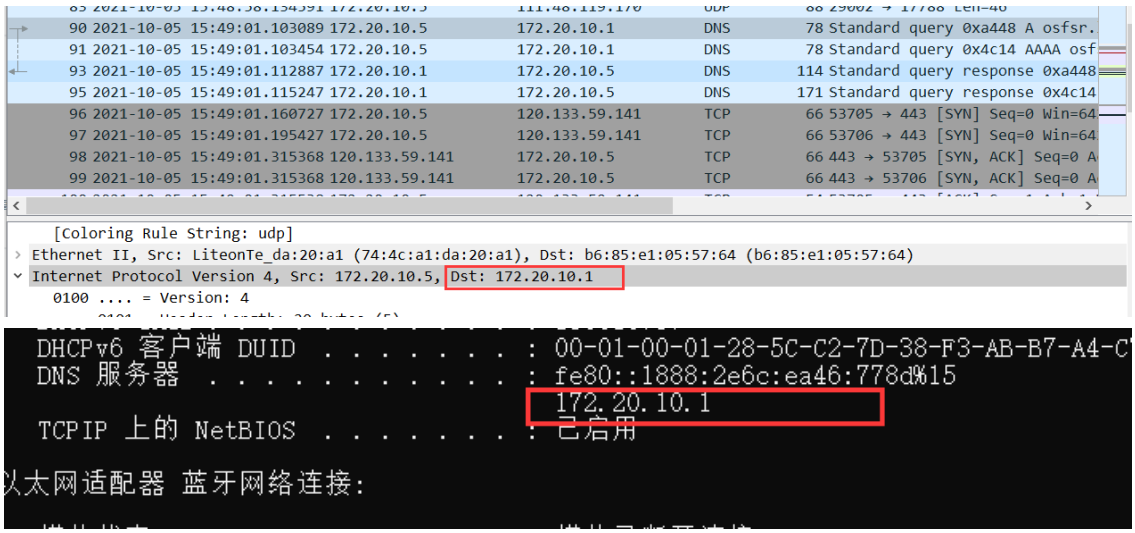


sorce port of DNS response message : 53



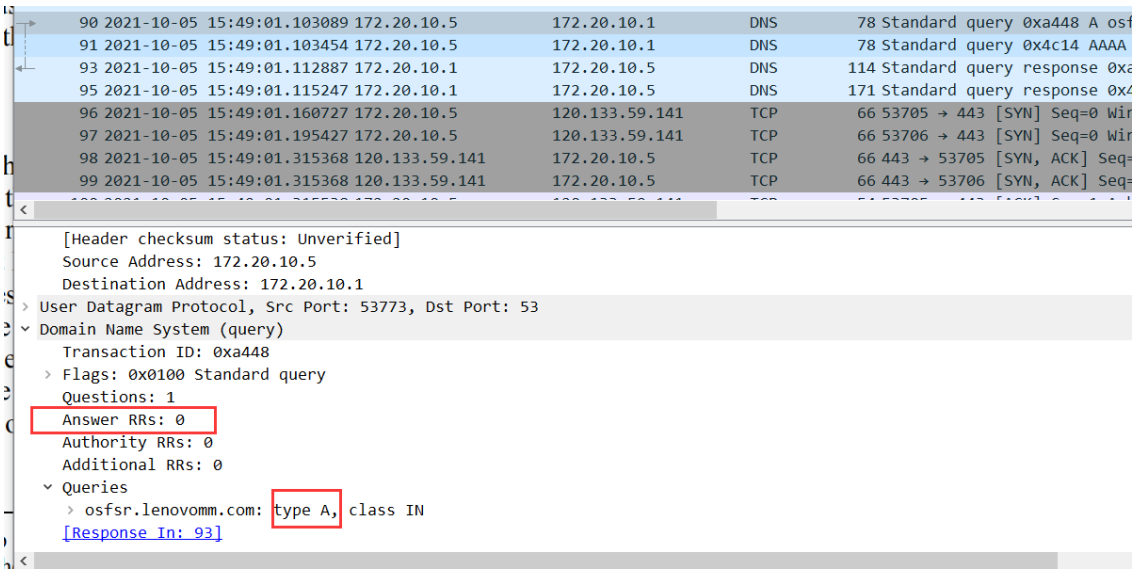
6. **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

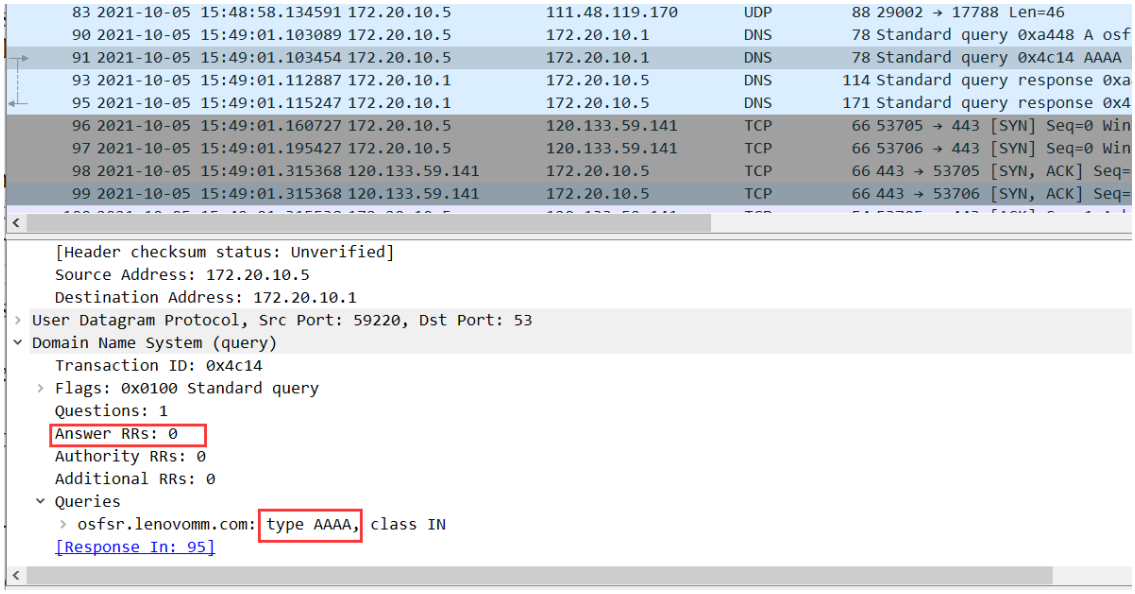
都是172.20.10.1



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

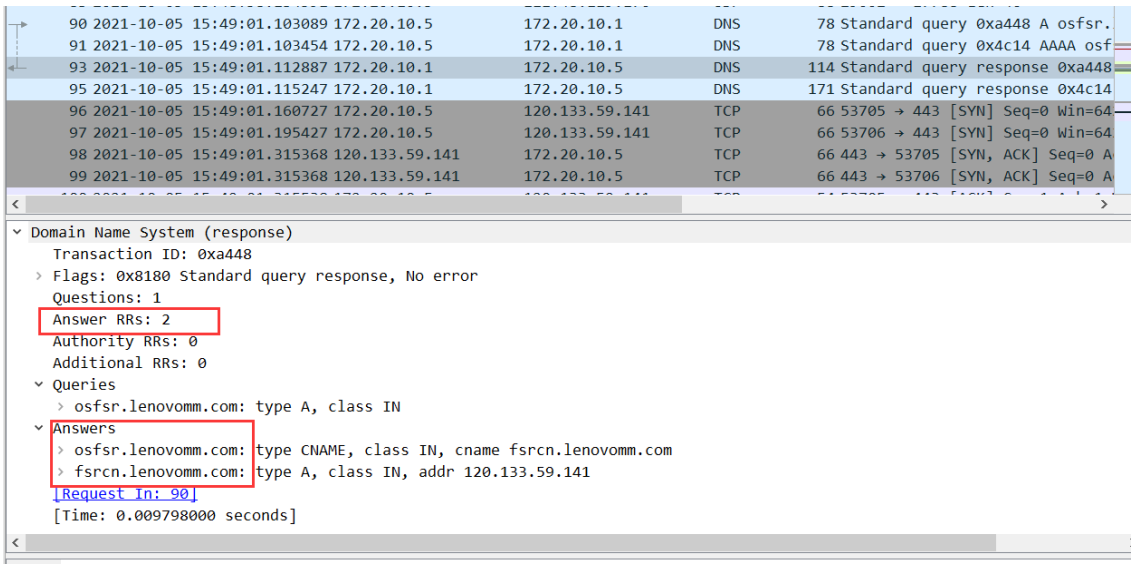
type A和type AAAA，没有answer





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

query的type为A包含2条answers，query的type为AAAA包含1条answers，故总共包含三条answers



91	2021-10-05 15:49:01.103454	172.20.10.5	172.20.10.1	DNS	78	Standard query 0x4c14 AAAA os
93	2021-10-05 15:49:01.112887	172.20.10.1	172.20.10.5	DNS	114	Standard query response 0xa44
95	2021-10-05 15:49:01.115247	172.20.10.1	172.20.10.5	DNS	171	Standard query response 0x4c1
96	2021-10-05 15:49:01.160727	172.20.10.5	120.133.59.141	TCP	66	53705 → 443 [SYN] Seq=0 Win=6
97	2021-10-05 15:49:01.195427	172.20.10.5	120.133.59.141	TCP	66	53706 → 443 [SYN] Seq=0 Win=6
98	2021-10-05 15:49:01.315368	120.133.59.141	172.20.10.5	TCP	66	443 → 53705 [SYN, ACK] Seq=0
99	2021-10-05 15:49:01.315368	120.133.59.141	172.20.10.5	TCP	66	443 → 53706 [SYN, ACK] Seq=0

```
Transaction ID: 0x4c14
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
v Queries
  > osfsr.lenovomm.com: type AAAA, class IN
v Answers
  > osfsr.lenovomm.com: type CNAME, class IN, cname fsrcn.lenovomm.com
v Authoritative nameservers
  > lenovomm.com: type SOA, class IN, mname ns1.dnsv5.com
[Request In: 91]
[Time: 0.011793000 seconds]
```

answers包含的内容如下

```
v Answers
  v osfsr.lenovomm.com: type CNAME, class IN, cname fsrcn.lenovomm.com
      Name: osfsr.lenovomm.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 604 (10 minutes, 4 seconds)
      Data length: 8
      CNAME: fsrcn.lenovomm.com
  v fsrcn.lenovomm.com: type A, class IN, addr 120.133.59.141
      Name: fsrcn.lenovomm.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 129 (2 minutes, 9 seconds)
      Data length: 4
      Address: 120.133.59.141
  [Request In: 90]
  [Time: 0.009798000 seconds]

v Queries
  > osfsr.lenovomm.com: type AAAA, class IN
v Answers
  v osfsr.lenovomm.com: type CNAME, class IN, cname fsrcn.lenovomm.com
      Name: osfsr.lenovomm.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 604 (10 minutes, 4 seconds)
      Data length: 8
      CNAME: fsrcn.lenovomm.com
```

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?**

是一样的，都是120.133.59.141

0.10.5	172.20.10.1	DNS	78	Standard query 0x4c14 AAAA osfsr.lenovomm.com
0.10.1	172.20.10.5	DNS	114	Standard query response 0xa448 A osfsr.lenovomm.com CNAME fsrcn.lenovomm.com A 120.133.59.141
0.10.1	172.20.10.5	DNS	171	Standard query response 0x4c14 AAAA osfsr.lenovomm.com CNAME fsrcn.lenovomm.com SOA ns1.dnsv5.com
0.10.5	120.133.59.141	TCP	66	53705 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
0.10.5	120.133.59.141	TCP	66	53706 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
33.59.141	172.20.10.5	TCP	66	443 → 53705 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=512
33.59.141	172.20.10.5	TCP	66	443 → 53706 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=512
0.10.5	120.133.59.141	TCP	54	53705 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0

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

    没有，因为有缓存

play with *nslookup*4 .

由于没有买校园WiFi，连了校园网再进行以下操作会出现多于6个的DNS，故连热点进行以下实验，此时，默认的本地DNS服务器的IP地址为fe80::44a:4870:35f3:e42d

• Start packet capture.

• Do an *nslookup* on www.mit.edu

```
C:\Users\Eiffel>nslookup www.mit.edu
服务器:  UnKnown
Address:  fe80::1888:2e6c:ea46:778d

非权威应答:
名称:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:a000:7a3::255e
          2600:1417:a000:795::255e
          104.71.147.10
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

• Stop packet capture.

（以下题目只需关注3条query和response中的最后一条query和response）

连了手机热点的本地DNS服务器的IP地址为：fe80::44a:4870:35f3:e42d

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

    两个都是53

```
270 2021-10-05 18:54:38.938678 fe80::44a:4870:35f3… fe80::78f9:f30e:d8c… DNS  180 Standard quer
271 2021-10-05 18:54:38.940817 fe80::78f9:f30e:d8c… fe80::44a:4870:35f3… DNS   91 Standard quer
310 2021-10-05 18:54:39.094399 fe80::44a:4870:35f3… fe80::78f9:f30e:d8c… DNS  220 Standard quer
```

```
> Frame 271: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{9FFF19E
v Ethernet II, Src: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1), Dst: b6:85:e1:05:57:64 (b6:85:e1:05:57:64)
  > Destination: b6:85:e1:05:57:64 (b6:85:e1:05:57:64)
  > Source: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::78f9:f30e:d8ca:b6d7, Dst: fe80::44a:4870:35f3:e42d
v User Datagram Protocol, Src Port: 64157, Dst Port: 53
    Source Port: 64157
    Destination Port: 53
    Length: 37
    Checksum: 0x379b [unverified]
    [Checksum Status: Unverified]
```

```
271 2021-10-05 18:54:38.940817 fe80::78f9:f30e:d8c… fe80::44a:4870:35f3… DNS   91 Standard query 0x0003 AA
310 2021-10-05 18:54:39.094399 fe80::44a:4870:35f3… fe80::78f9:f30e:d8c… DNS  220 Standard query response
```

```
> Frame 310: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{9FFF19E3-A853-
v Ethernet II, Src: b6:85:e1:05:57:64 (b6:85:e1:05:57:64), Dst: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1)
  > Destination: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1)
  > Source: b6:85:e1:05:57:64 (b6:85:e1:05:57:64)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::44a:4870:35f3:e42d, Dst: fe80::78f9:f30e:d8ca:b6d7
v User Datagram Protocol, Src Port: 53, Dst Port: 64157
    Source Port: 53
    Destination Port: 64157
    Length: 166
    Checksum: 0x3089 [unverified]
    [Checksum Status: Unverified]
```

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

    DNS查询报文发送的目的IP地址为fe80::44a:4870:35f3:e42d，这个地址就是本地默认的DNS服务器的地址

```
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::78f9:f30e:d8ca:b6d7, Dst: fe80::44a:4870:35f3:e42d
v User Datagram Protocol, Src Port: 64157, Dst Port: 53
    Source Port: 64157
```

```
C:\Users\Eiffel>nslookup www.mit.edu
服务器:  UnKnown
Address:  fe80::44a:4870:35f3:e42d

非权威应答:
名称:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:a000:795::255e
          2600:1417:a000:7a3::255e
          104.71.147.10
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

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

    type A，不包含任何answers

```
> User Datagram Protocol, Src Port: 64156, Dst Port:
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: 270]
```

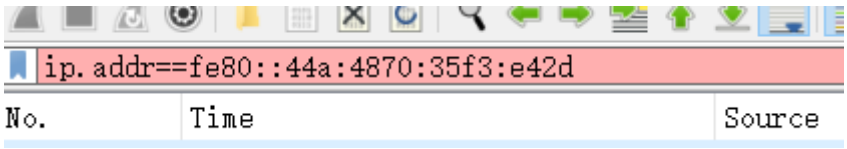
14. **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**

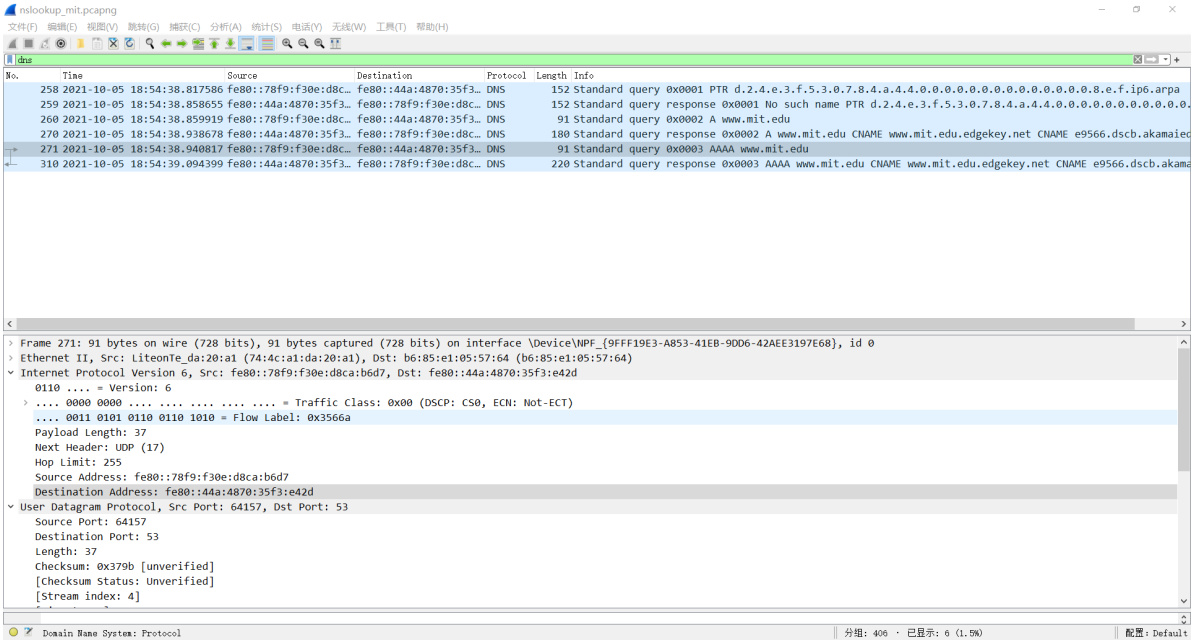
    四条，包含的内容如下所示

```
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    v Answers
      > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:a000:795::255e
      > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:a000:7a3::255e
    [Request In: 271]
    [Time: 0.153582000 seconds]
```

15. **Provide a screenshot.**

    由于无法对ip地址fe80::44a:4870:35f3:e42d进行过滤，故采用过滤dns的形式进行过滤（下同）



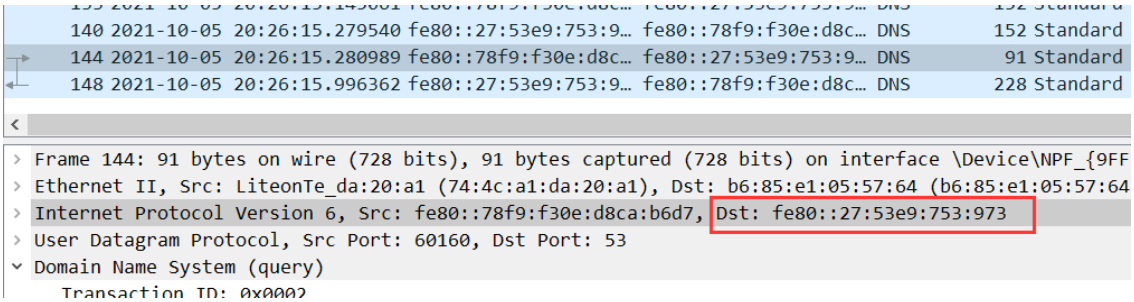


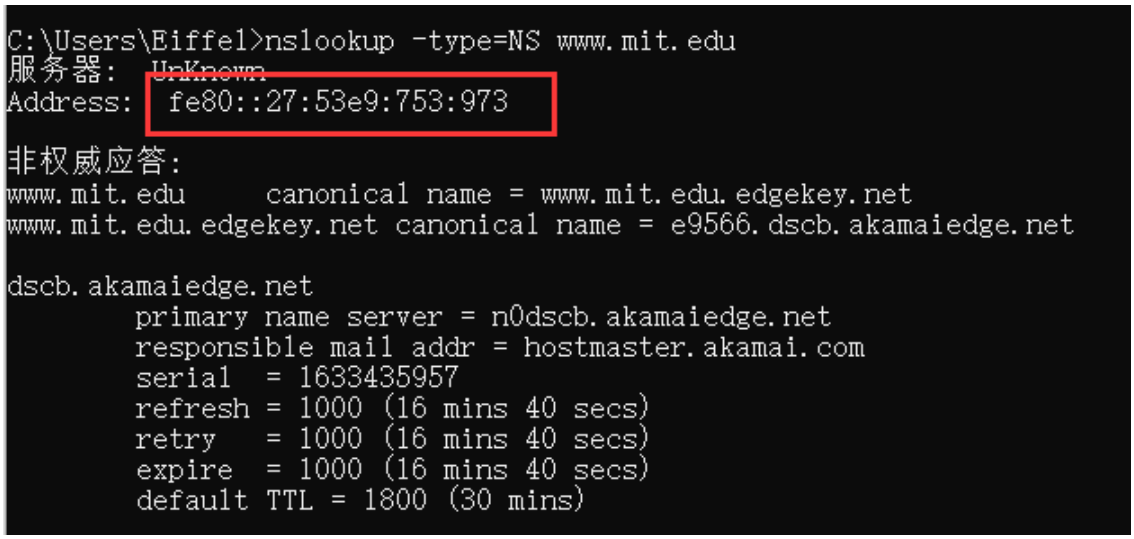
Now repeat the previous experiment, but instead issue the command:

nslookup –type=NS mit.edu

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

    DNS查询报文发送的目的IP地址为fe80::27:53e9:753:973，这个地址就是本地默认的DNS服务器的地址





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

type NS，没有含任何answers

```
144 2021-10-05 20:26:15.280989 fe80::78f9:f30e:d8c… fe80::27:53e9:753:9… DNS 91
148 2021-10-05 20:26:15.996362 fe80::27:53e9:753:9… fe80::78f9:f30e:d8c… DNS 228

> Frame 144: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\
> Ethernet II, Src: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1), Dst: b6:85:e1:05:57:64 (b6:85:e1:
> Internet Protocol Version 6, Src: fe80::78f9:f30e:d8ca:b6d7, Dst: fe80::27:53e9:753:973
> User Datagram Protocol, Src Port: 60160, 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 NS, class IN
    [Response In: 148]
```

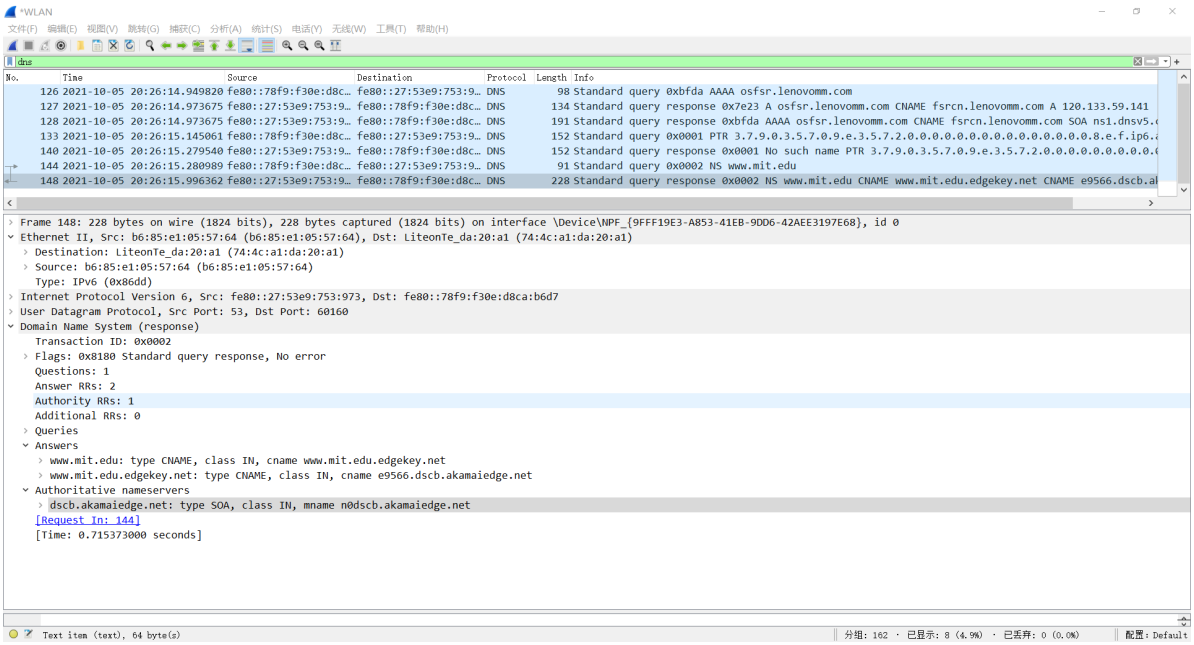
18. **Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

提供的服务器：dscb.akamaiedge.net , 没有提供IP地址

```
144 2021-10-05 20:26:15.280989 fe80::78f9:f30e:d8c… fe80::27:53e9:753:9… DNS 91
148 2021-10-05 20:26:15.996362 fe80::27:53e9:753:9… fe80::78f9:f30e:d8c… DNS 228

  > Destination: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1)
  > Source: b6:85:e1:05:57:64 (b6:85:e1:05:57:64)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::27:53e9:753:973, Dst: fe80::78f9:f30e:d8ca:b6d7
> User Datagram Protocol, Src Port: 53, Dst Port: 60160
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 1
    Additional RRs: 0
  > Queries
  v Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  v Authoritative nameservers
    > dscb.akamaiedge.net: type SOA, class IN, mname n0dscb.akamaiedge.net
    [Request In: 144]
    [Time: 0.715373000 seconds]
```

19. **Provide a screenshot.**



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

nslookup www.aiit.or.kr bitsy.mit.edu

由于DNS服务器bitsy.mit.edu停用导致请求超时，故此处用阿里的DNS服务器

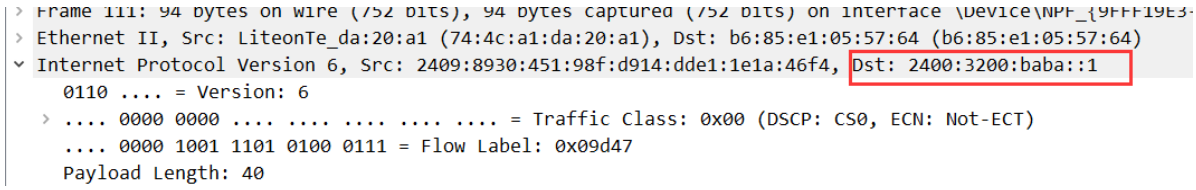
查到阿里的DNS服务器的首选IP地址为223.5.5.5，用命令

nslookup 223.5.5.5

进行查询其名称得到其名称为public1.alidns.com

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?**

目的IP地址：2400:3200:baba::1，和默认DNS服务器地址不一样，这个IP地址与指定服务器IP地址一致，即阿里的DNS服务器



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

type A , 没有answers

```
> User Datagram Protocol, Src Port: 63313, 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.aiit.or.kr: type A, class IN
    [Response In: 112]
```

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

1个answers，answers的内容如图所示

```
> User Datagram Protocol, Src Port: 53, Dst Port: 63313
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.aiit.or.kr: type A, class IN
  v Answers
    v www.aiit.or.kr: type A, class IN, addr 58.229.6.225
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3203 (53 minutes, 23 seconds)
        Data length: 4
        Address: 58.229.6.225
    [Request In: 111]
    [Time: 0.101132000 seconds]
```

23. **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)

dns

No.	Time	Source	Destination	Protocol	Length	Info
17	2021-10-05 21:06:53.857388	fe80::78f9:f30e:d8c…	fe80::27:53e9:753:9…	DNS	98	Standard query 0xeddd A public1.alidns.com
18	2021-10-05 21:06:53.857542	fe80::78f9:f30e:d8c…	fe80::27:53e9:753:9…	DNS	98	Standard query 0x600e AAAA public1.alidns.com
19	2021-10-05 21:06:53.892531	fe80::27:53e9:753:9…	fe80::78f9:f30e:d8c…	DNS	154	Standard query response 0x600e AAAA public1.alidns.com AAAA 2400:3200:baba::1 AAAA 2400:3200::1
108	2021-10-05 21:06:53.994727	fe80::27:53e9:753:9…	fe80::78f9:f30e:d8c…	DNS	130	Standard query response 0xeddd A public1.alidns.com A 223.6.6.6 A 223.5.5.5
109	2021-10-05 21:06:53.996526	2409:8930:451:98f:d…	2400:3200:baba::1	DNS	152	Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.b.a.b.0.0.2.3.0.0.4.2.ip6.arpa
110	2021-10-05 21:06:54.097018	2400:3200:baba::1	2409:8930:451:98f:d…	DNS	223	Standard query response 0x0001 No such name PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.b.a.b.0.0.
111	2021-10-05 21:06:54.098287	2409:8930:451:98f:d…	2400:3200:baba::1	DNS	94	Standard query 0x0002 A www.aiit.or.kr
112	2021-10-05 21:06:54.199419	2400:3200:baba::1	2409:8930:451:98f:d…	DNS	110	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
113	2021-10-05 21:06:54.202137	2409:8930:451:98f:d…	2400:3200:baba::1	DNS	94	Standard query 0x0003 AAAA www.aiit.or.kr
114	2021-10-05 21:06:54.302227	2400:3200:baba::1	2409:8930:451:98f:d…	DNS	148	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

```
> Frame 109: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface \Device\NPF_{9FFF19E3-A853-41EB-9DD6-42AEE3197E68}, id 0
> Ethernet II, Src: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1), Dst: b6:85:e1:05:57:64 (b6:85:e1:05:57:64)
v Internet Protocol Version 6, Src: 2409:8930:451:98f:d914:dde1:1e1a:46f4, Dst: 2400:3200:baba::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 1000 1000 0000 0111 = Flow Label: 0x08807
    Payload Length: 98
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2409:8930:451:98f:d914:dde1:1e1a:46f4
    Destination Address: 2400:3200:baba::1
> User Datagram Protocol, Src Port: 63312, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.b.a.b.0.0.2.3.0.0.4.2.ip6.arpa: type PTR, class IN
    [Response In: 110]
```

Domain Name System: Protocol | 分组: 128 · 已显示: 10 (7.8%) · 已丢弃: 0 (0.0%) | 配置: Default