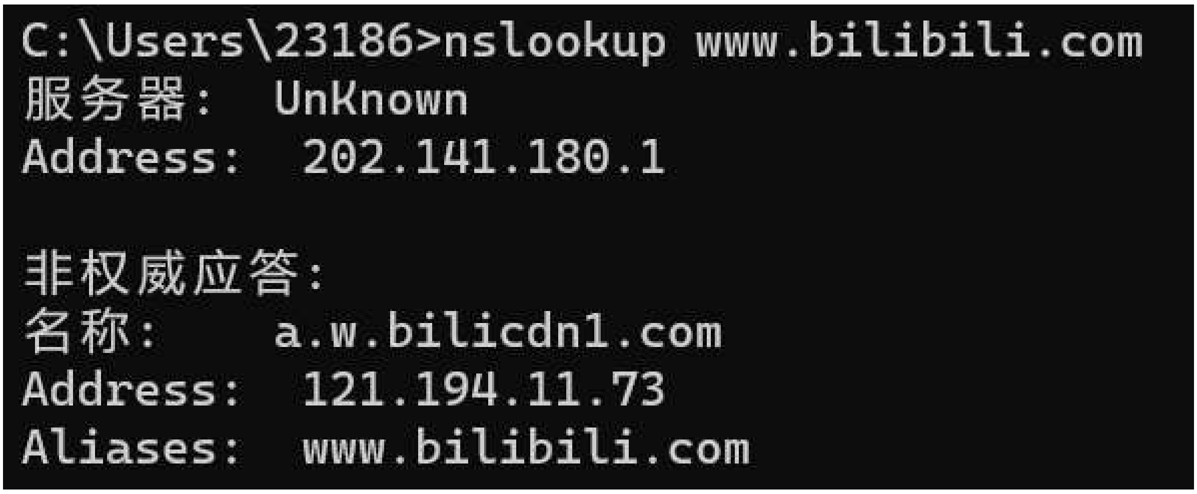
LAB3

牛庆源 PB21111733

- **1.**

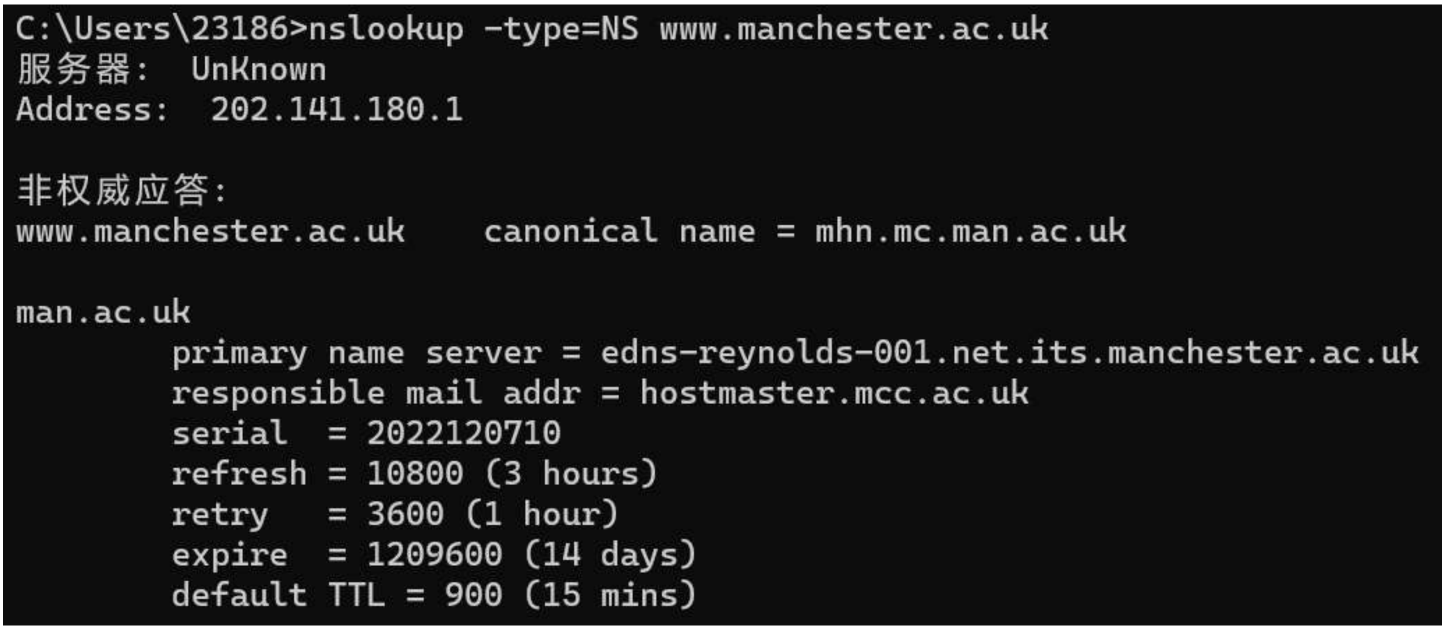
查询bilibili的ip，为121.194.11.73



```
C:\Users\23186>nslookup www.bilibili.com
服务器:  UnKnown
Address:  202.141.180.1

非权威应答:
名称:    a.w.bilicdn1.com
Address:  121.194.11.73
Aliases:  www.bilibili.com
```

- **2.**

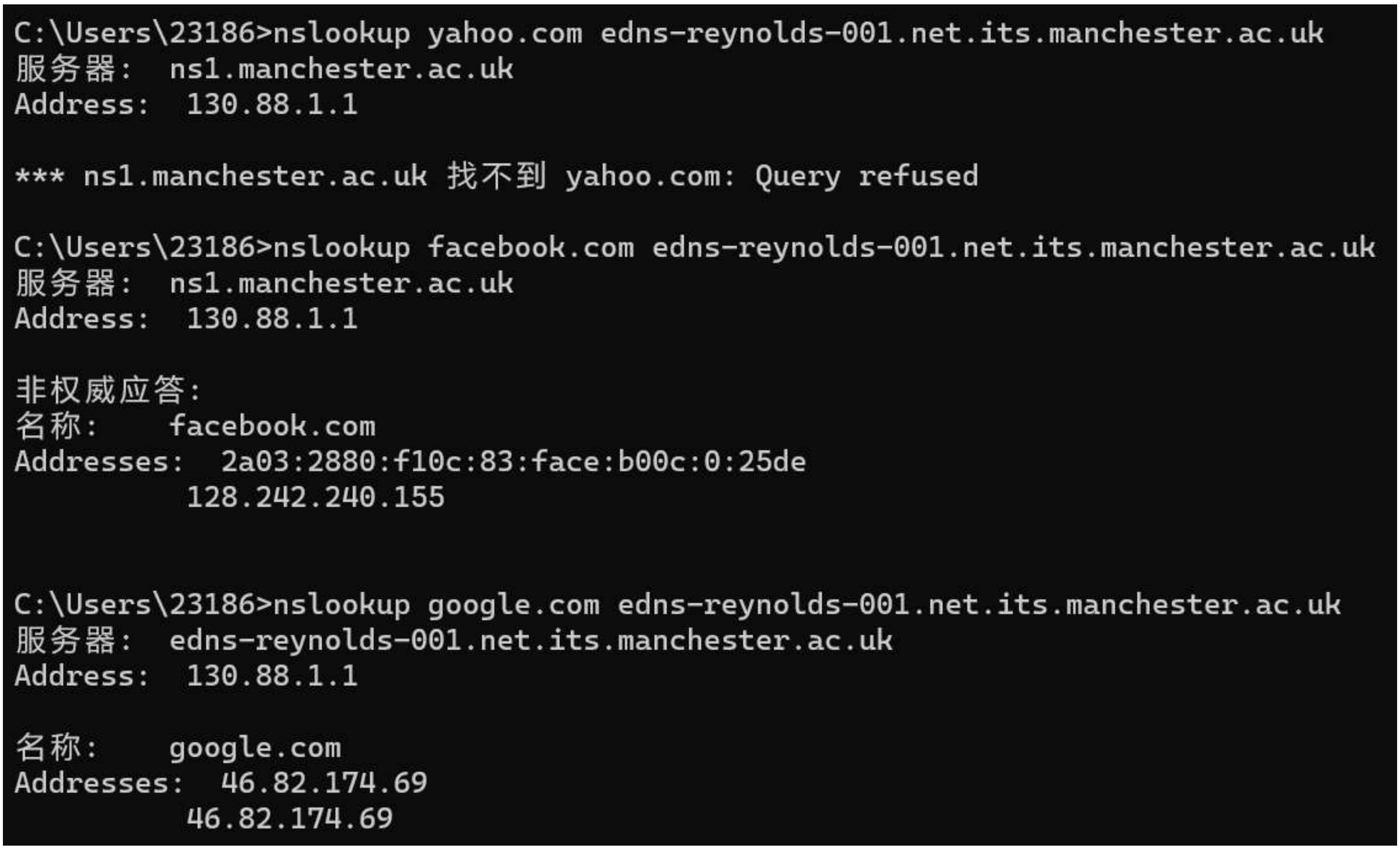
查询英国曼彻斯特大学的权威DNS服务器



```
C:\Users\23186>nslookup -type=NS www.manchester.ac.uk
服务器:  UnKnown
Address:  202.141.180.1

非权威应答:
www.manchester.ac.uk    canonical name = mhn.mc.man.ac.uk

man.ac.uk
        primary name server = edns-reynolds-001.net.its.manchester.ac.uk
        responsible mail addr = hostmaster.mcc.ac.uk
        serial  = 2022120710
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 900 (15 mins)
```

- **3.**

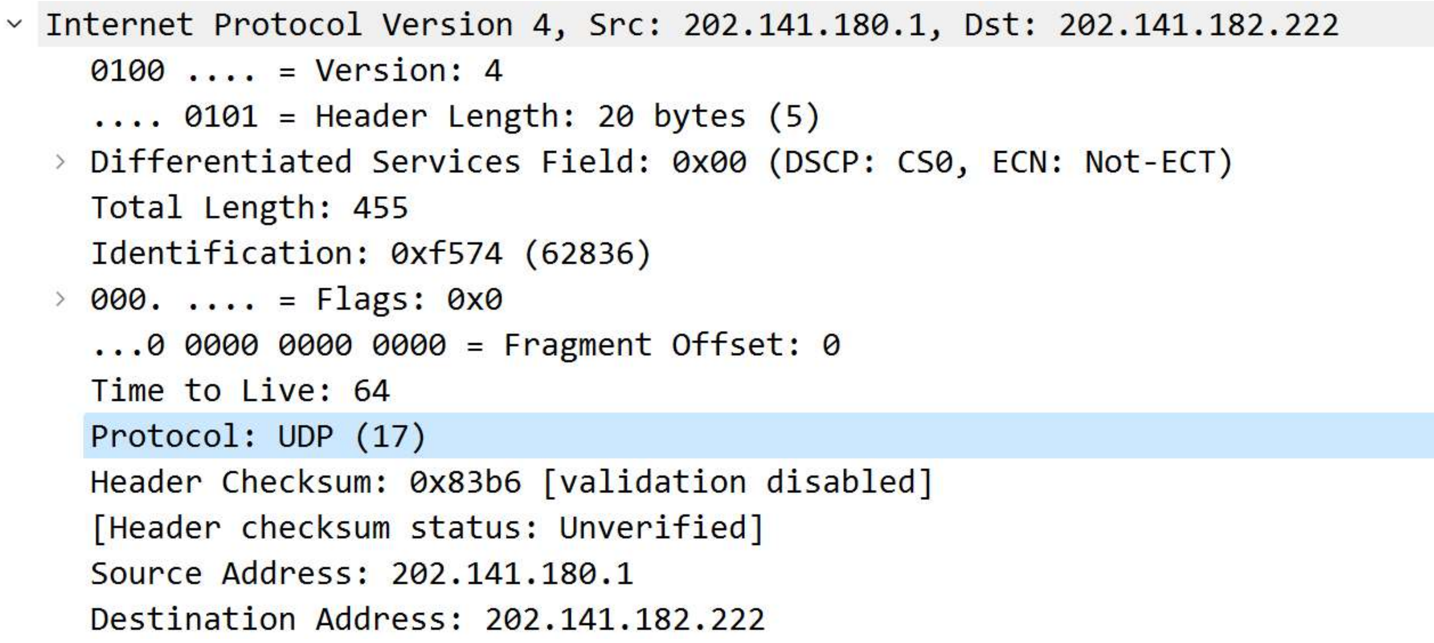
用曼彻斯特大学权威DNS查询yahoo失败，但列出了一些其他查询结果



```
C:\Users\23186>nslookup yahoo.com edns-reynolds-001.net.its.manchester.ac.uk
服务器:  ns1.manchester.ac.uk
Address:  130.88.1.1

*** ns1.manchester.ac.uk 找不到 yahoo.com: Query refused

C:\Users\23186>nslookup facebook.com edns-reynolds-001.net.its.manchester.ac.uk
服务器:  ns1.manchester.ac.uk
Address:  130.88.1.1

非权威应答:
名称:    facebook.com
Addresses:  2a03:2880:f10c:83:face:b00c:0:25de
          128.242.240.155


C:\Users\23186>nslookup google.com edns-reynolds-001.net.its.manchester.ac.uk
服务器:  edns-reynolds-001.net.its.manchester.ac.uk
Address:  130.88.1.1

名称:    google.com
Addresses:  46.82.174.69
          46.82.174.69
```

- **4.**

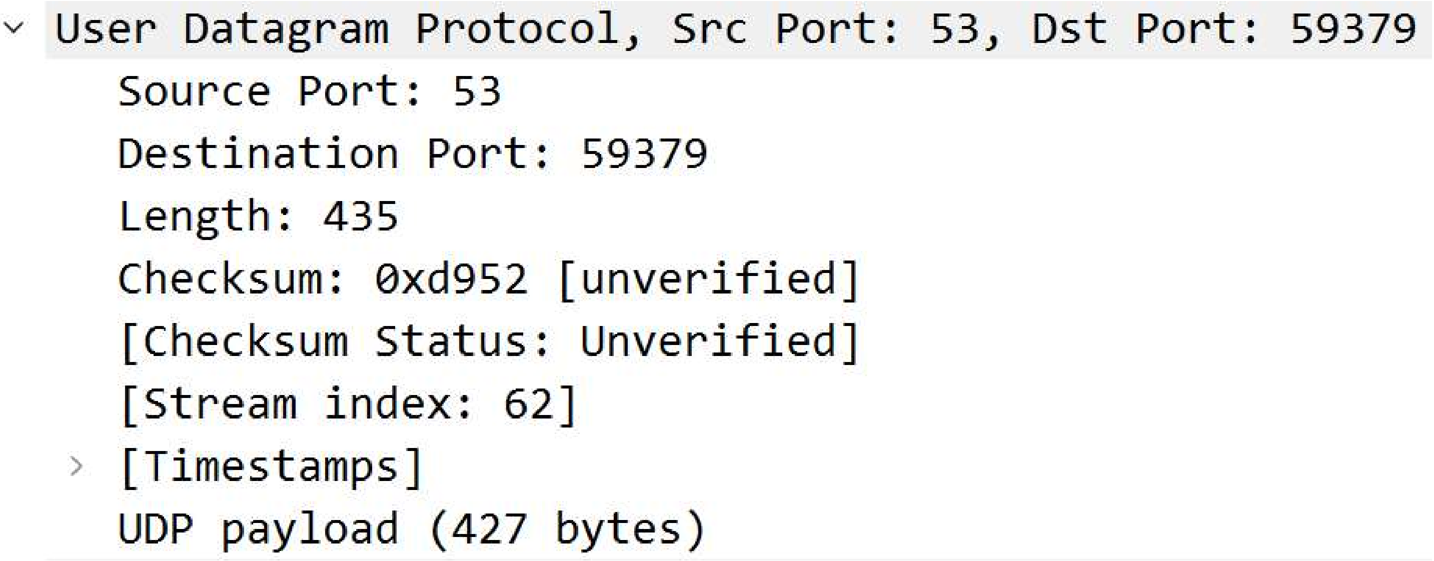
如图，为UDP协议



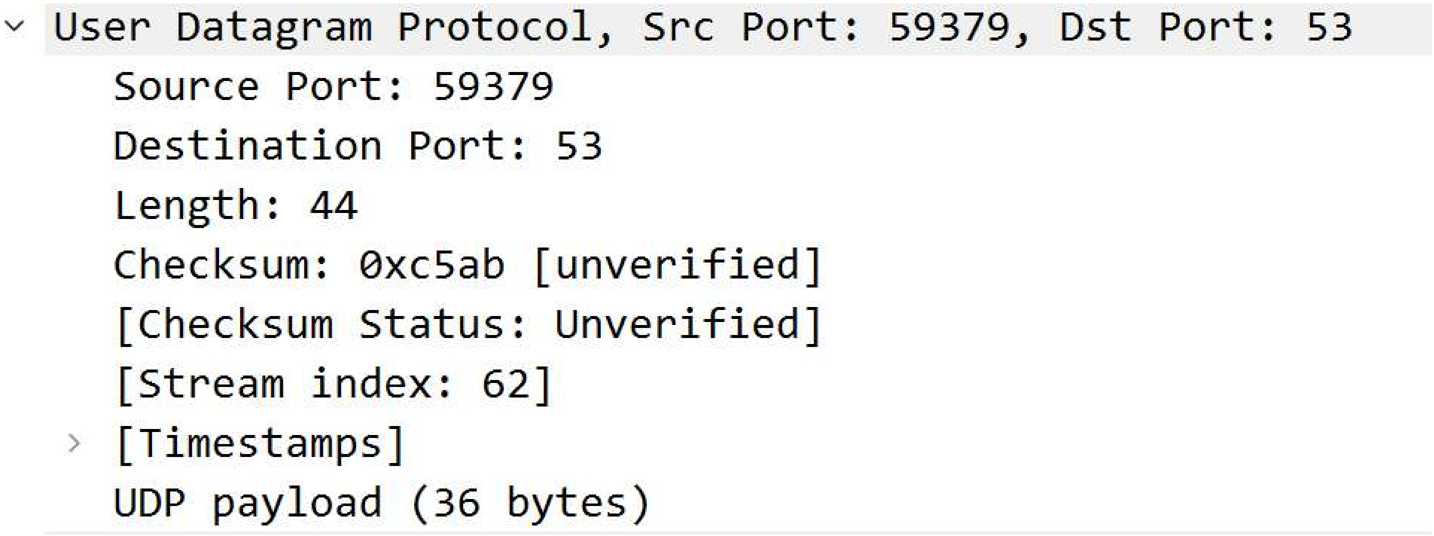
```
⌄ Internet Protocol Version 4, Src: 202.141.180.1, Dst: 202.141.182.222
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 455
    Identification: 0xf574 (62836)
  › 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x83b6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 202.141.180.1
    Destination Address: 202.141.182.222
```

- **5.**

如下两图，都为端口号53



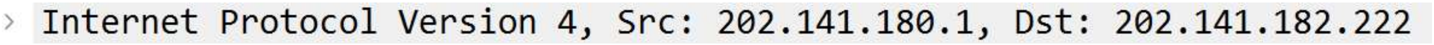
```
∨ User Datagram Protocol, Src Port: 53, Dst Port: 59379
      Source Port: 53
      Destination Port: 59379
      Length: 435
      Checksum: 0xd952 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 62]
    > [Timestamps]
      UDP payload (427 bytes)
```



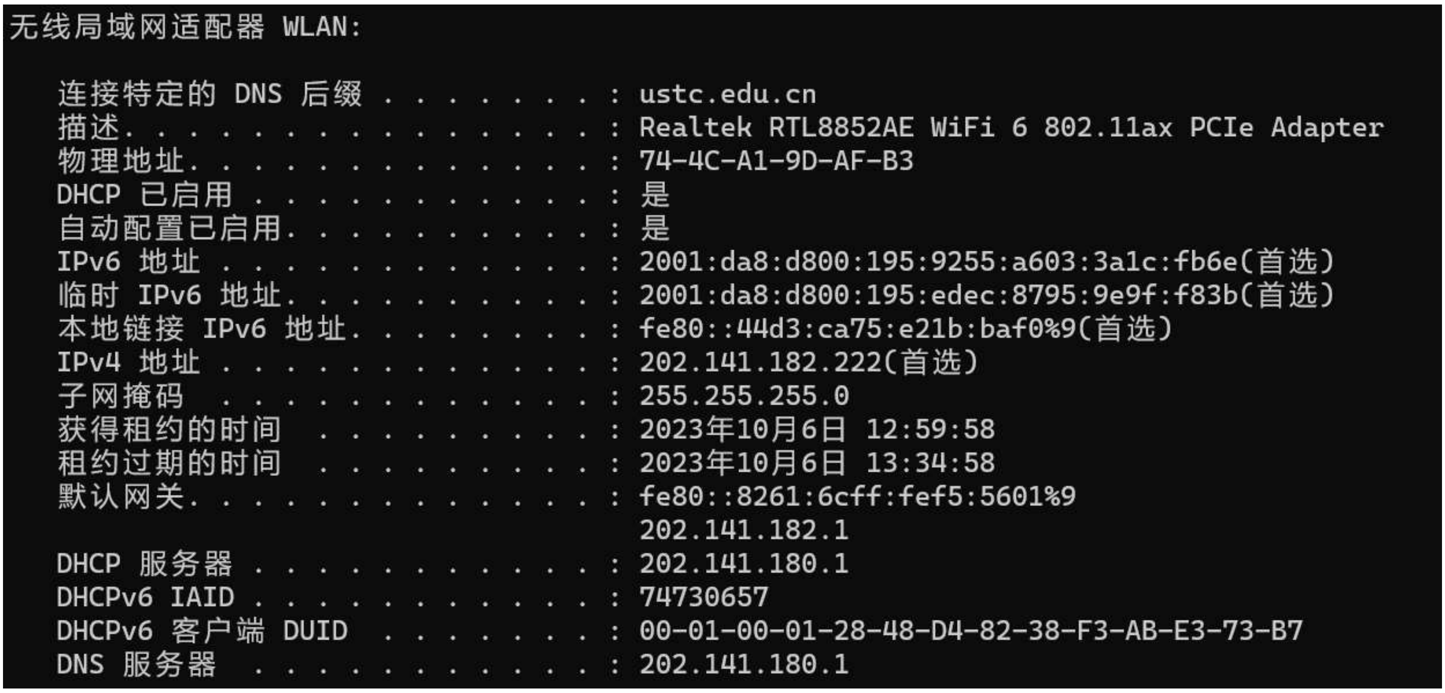
```
∨ User Datagram Protocol, Src Port: 59379, Dst Port: 53
      Source Port: 59379
      Destination Port: 53
      Length: 44
      Checksum: 0xc5ab [unverified]
      [Checksum Status: Unverified]
      [Stream index: 62]
    > [Timestamps]
      UDP payload (36 bytes)
```

- **6.**

二者ip地址相同，均为202.141.180.1



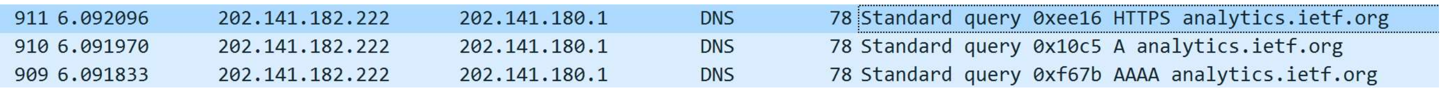
```
> Internet Protocol Version 4, Src: 202.141.180.1, Dst: 202.141.182.222
```



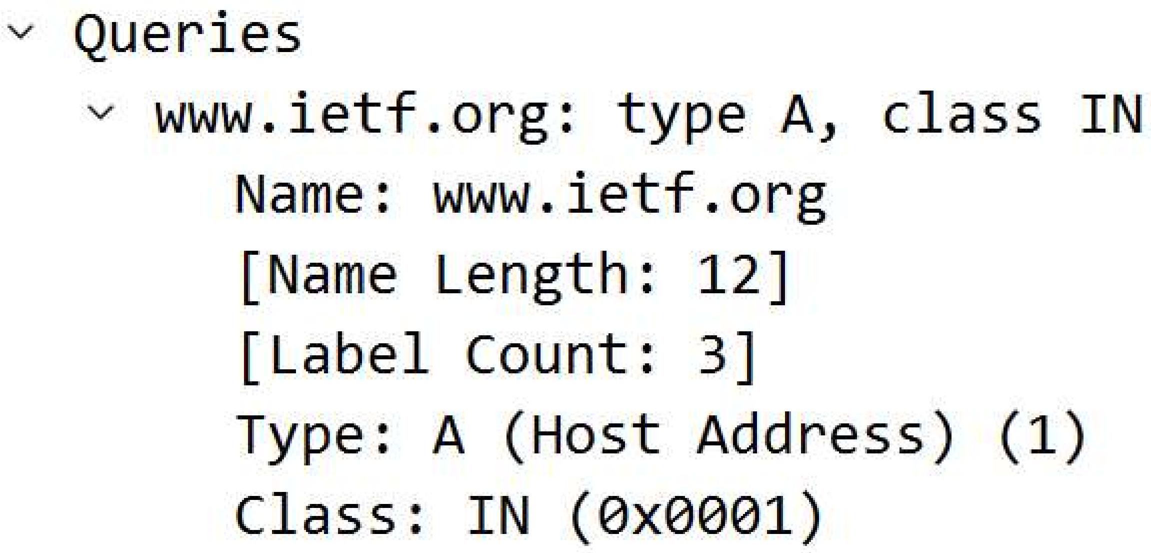
```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . : ustc.edu.cn
   描述. . . . . . . . . . . . . . . : Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
   物理地址. . . . . . . . . . . . . : 74-4C-A1-9D-AF-B3
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2001:da8:d800:195:9255:a603:3a1c:fb6e(首选)
   临时 IPv6 地址. . . . . . . . . . : 2001:da8:d800:195:edec:8795:9e9f:f83b(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::44d3:ca75:e21b:baf0%9(首选)
   IPv4 地址 . . . . . . . . . . . . : 202.141.182.222(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2023年10月6日 12:59:58
   租约过期的时间  . . . . . . . . . : 2023年10月6日 13:34:58
   默认网关. . . . . . . . . . . . . : fe80::8261:6cff:fef5:5601%9
                                       202.141.182.1
   DHCP 服务器 . . . . . . . . . . . : 202.141.180.1
   DHCPv6 IAID . . . . . . . . . . . : 74730657
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-28-48-D4-82-38-F3-AB-E3-73-B7
   DNS 服务器  . . . . . . . . . . . : 202.141.180.1
```

- **7.**

类型为type A，没有answers



```
911 6.092096    202.141.182.222    202.141.180.1    DNS    78 Standard query 0xee16 HTTPS analytics.ietf.org
910 6.091970    202.141.182.222    202.141.180.1    DNS    78 Standard query 0x10c5 A analytics.ietf.org
909 6.091833    202.141.182.222    202.141.180.1    DNS    78 Standard query 0xf67b AAAA analytics.ietf.org
```

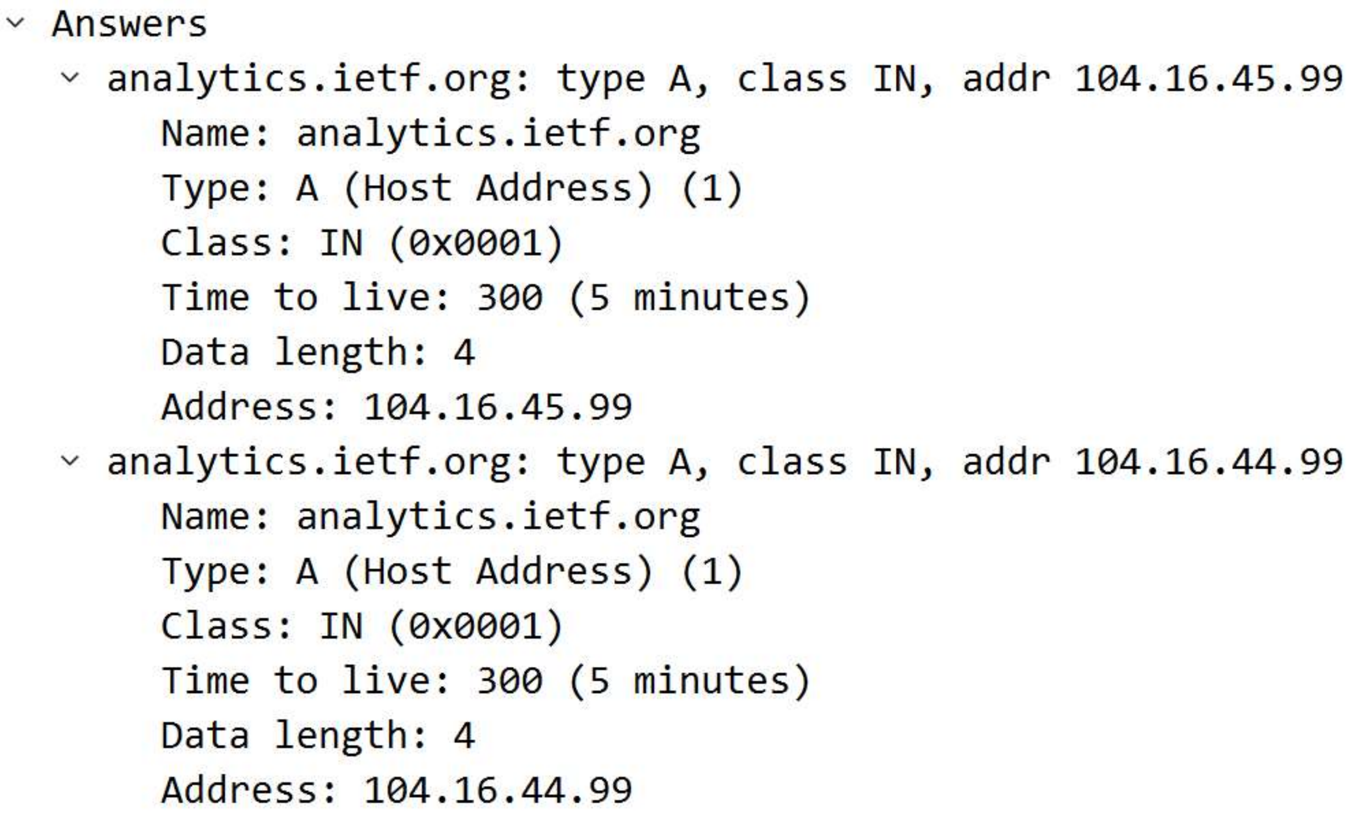


```
⌄ Queries
  ⌄ www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

- **8.**

response中answers中有两条内容，如下

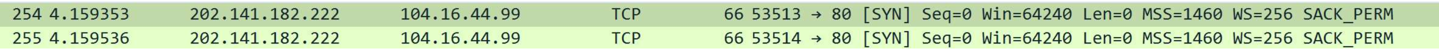
包含域名，类型，分类等信息



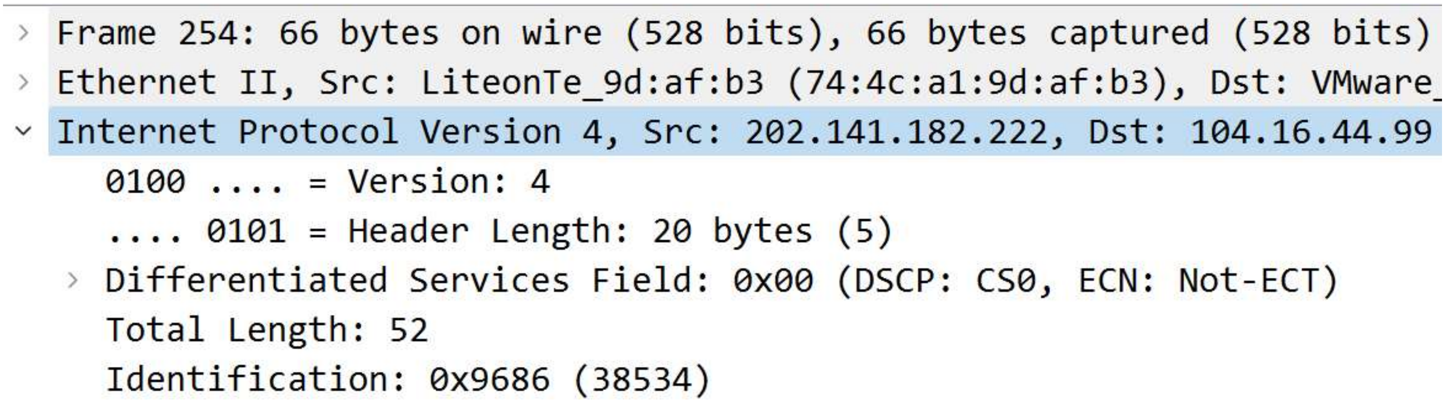
```
⌄ Answers
  ⌄ analytics.ietf.org: type A, class IN, addr 104.16.45.99
      Name: analytics.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  ⌄ analytics.ietf.org: type A, class IN, addr 104.16.44.99
      Name: analytics.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
```

- **9.**

Q8图与下图比较，104.16.44.99是DNS response的answers中的



```
254 4.159353    202.141.182.222    104.16.44.99    TCP    66 53513 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
255 4.159536    202.141.182.222    104.16.44.99    TCP    66 53514 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```



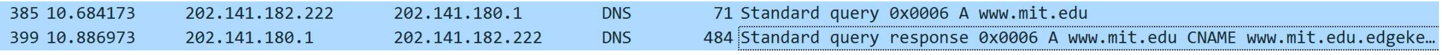
```
> Frame 254: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3), Dst: VMware_
v Internet Protocol Version 4, Src: 202.141.182.222, Dst: 104.16.44.99
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x9686 (38534)
```

- **10.**

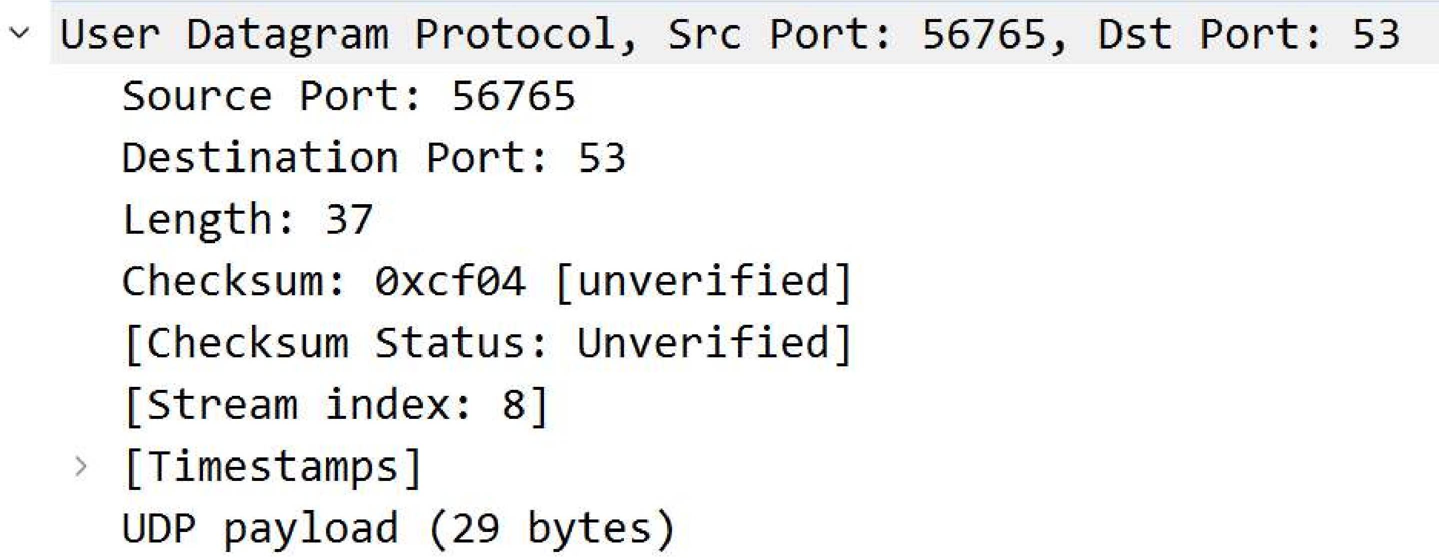
经检查，图片没有新的query

- **11.**

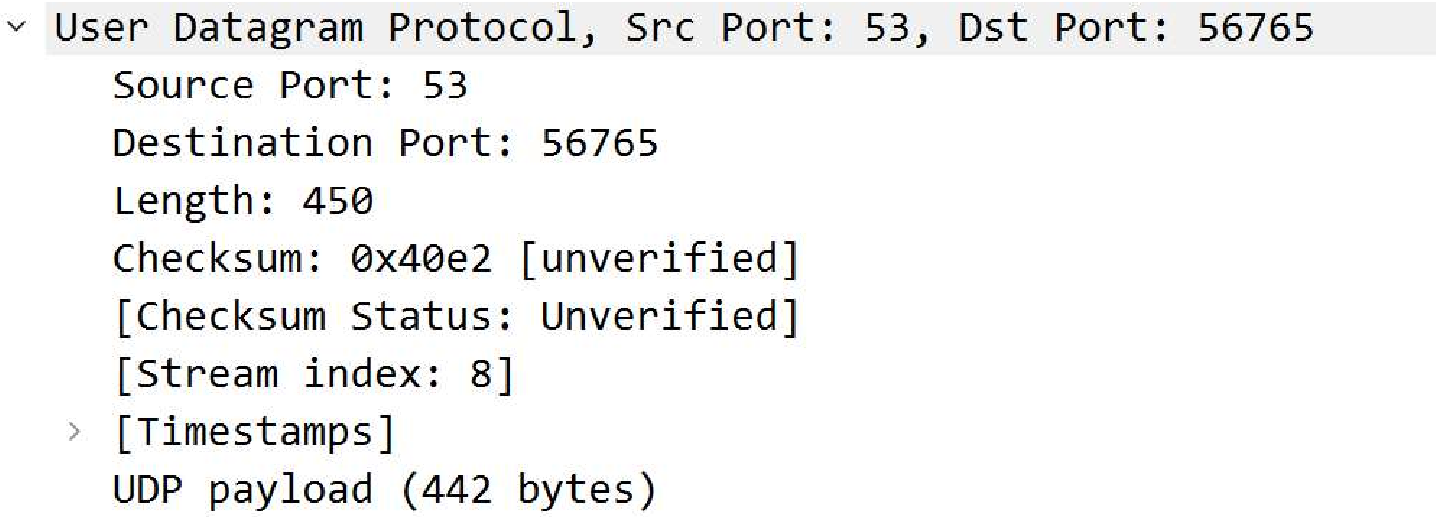
端口号均为53



```
385 10.684173    202.141.182.222    202.141.180.1      DNS     71 Standard query 0x0006 A www.mit.edu
399 10.886973    202.141.180.1      202.141.182.222    DNS    484 Standard query response 0x0006 A www.mit.edu CNAME www.mit.edu.edgeke…
```



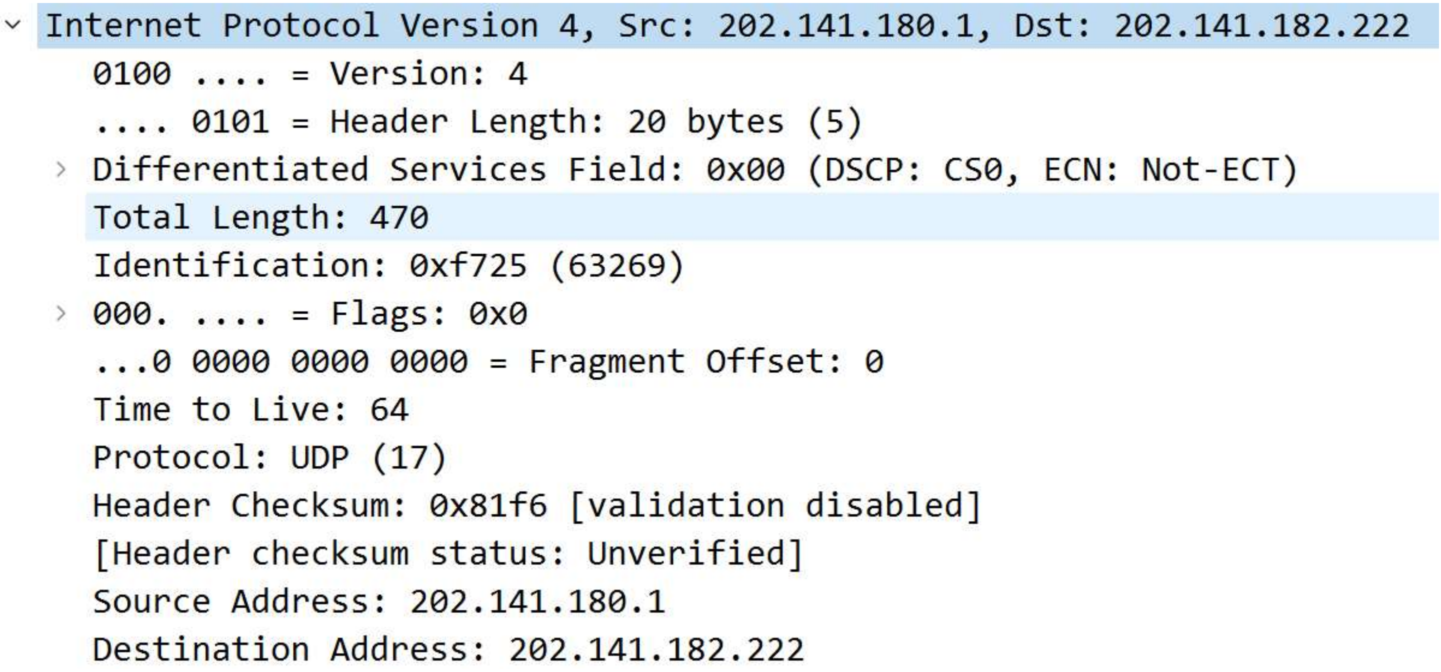
```
v User Datagram Protocol, Src Port: 56765, Dst Port: 53
    Source Port: 56765
    Destination Port: 53
    Length: 37
    Checksum: 0xcf04 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
  > [Timestamps]
    UDP payload (29 bytes)
```



```
User Datagram Protocol, Src Port: 53, Dst Port: 56765
    Source Port: 53
    Destination Port: 56765
    Length: 450
    Checksum: 0x40e2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
  > [Timestamps]
    UDP payload (442 bytes)
```

- **12.**

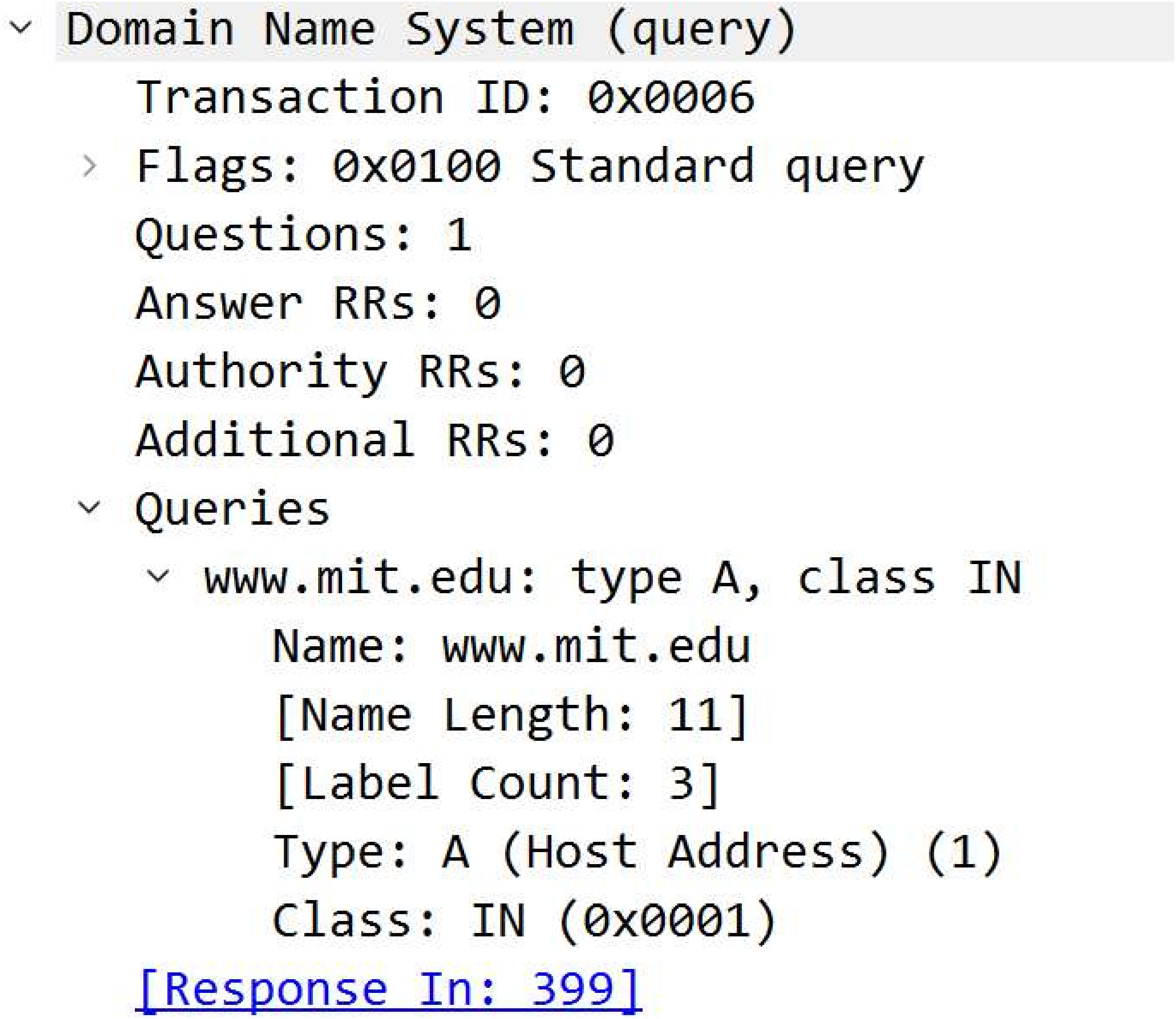
sent到202.141.180.1，与Q6图中本地DNS一致



```
Internet Protocol Version 4, Src: 202.141.180.1, Dst: 202.141.182.222
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 470
    Identification: 0xf725 (63269)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x81f6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 202.141.180.1
    Destination Address: 202.141.182.222
```

- **13.**

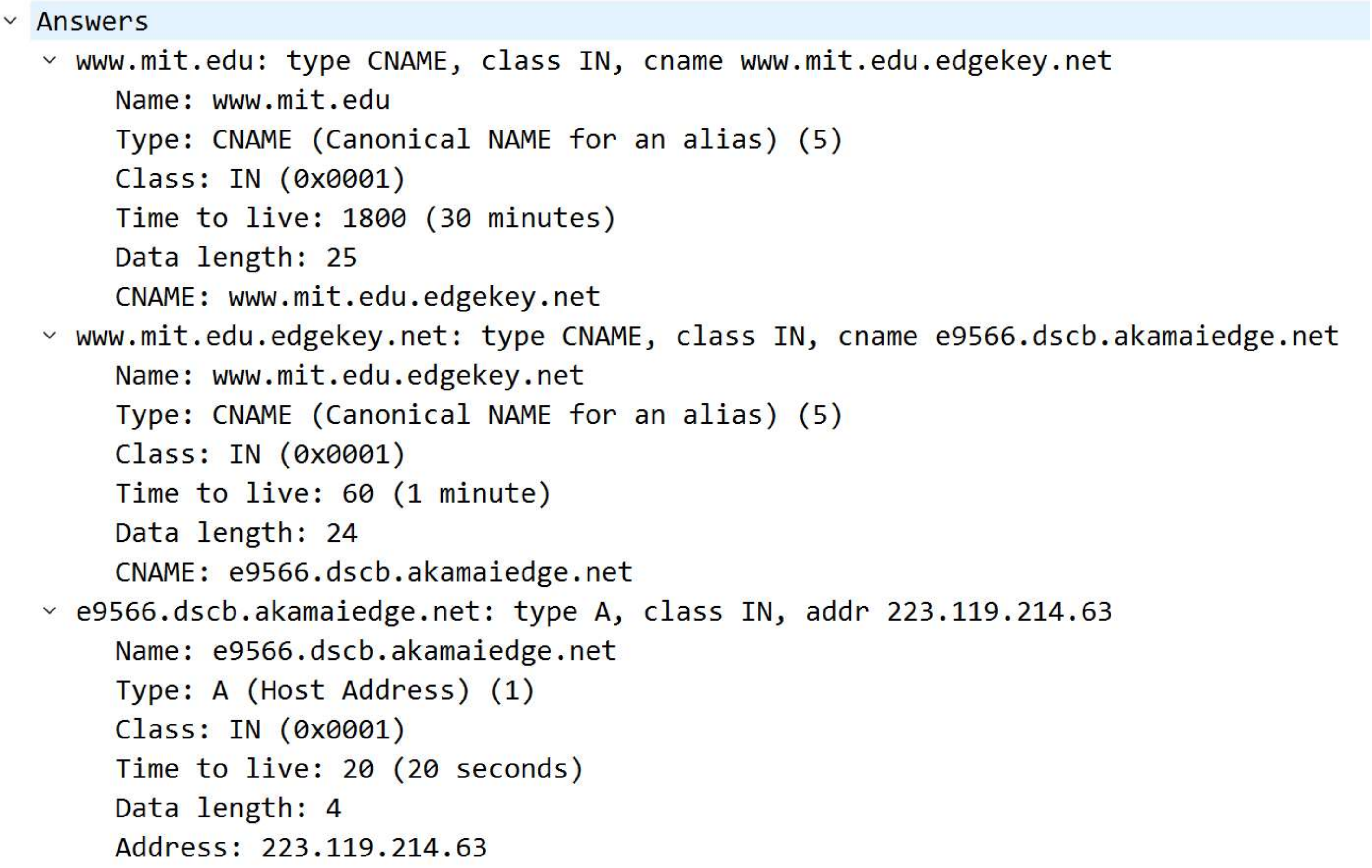
类型为type A，不含answers



```
v Domain Name System (query)
    Transaction ID: 0x0006
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 399]
```

- **14.**

answers中有三个内容，如下，比之前的实验结果多出cname，以及其条目



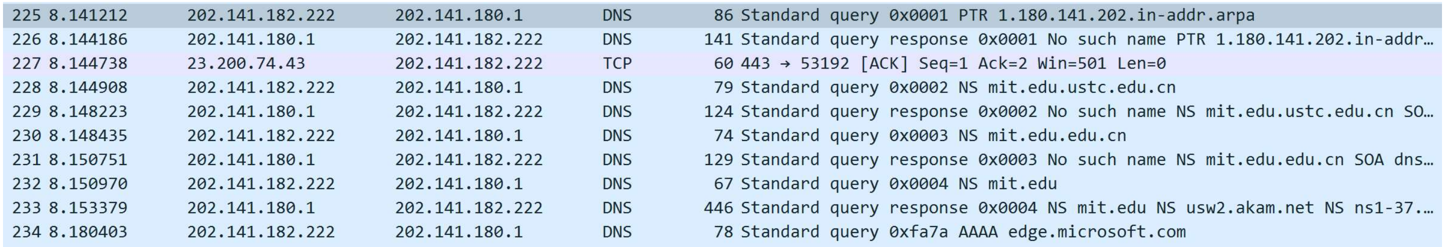
```
⌄ Answers
  ⌄ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ⌄ www.mit.edu.edgekey.net: 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: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ⌄ e9566.dscb.akamaiedge.net: type A, class IN, addr 223.119.214.63
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 223.119.214.63
```

- **15.**

如解答中的截图

- **16.**

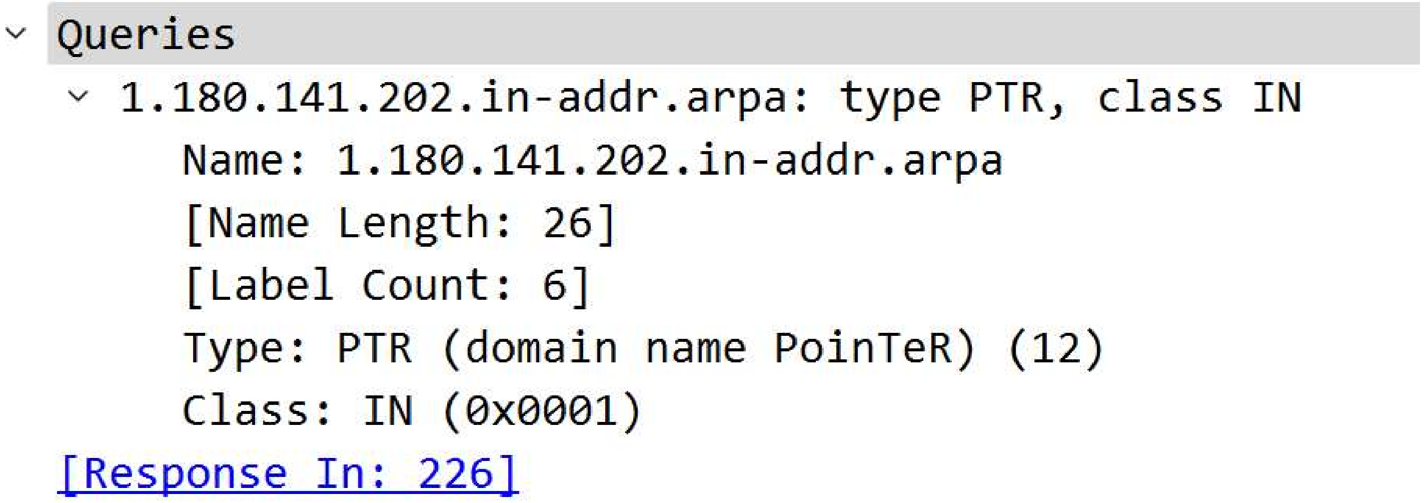
202.141.180.1，为本地DNS



```
225 8.141212   202.141.182.222   202.141.180.1     DNS    86 Standard query 0x0001 PTR 1.180.141.202.in-addr.arpa
226 8.144186   202.141.180.1     202.141.182.222   DNS   141 Standard query response 0x0001 No such name PTR 1.180.141.202.in-addr…
227 8.144738   23.200.74.43      202.141.182.222   TCP    60 443 → 53192 [ACK] Seq=1 Ack=2 Win=501 Len=0
228 8.144908   202.141.182.222   202.141.180.1     DNS    79 Standard query 0x0002 NS mit.edu.ustc.edu.cn
229 8.148223   202.141.180.1     202.141.182.222   DNS   124 Standard query response 0x0002 No such name NS mit.edu.ustc.edu.cn SO…
230 8.148435   202.141.182.222   202.141.180.1     DNS    74 Standard query 0x0003 NS mit.edu.edu.cn
231 8.150751   202.141.180.1     202.141.182.222   DNS   129 Standard query response 0x0003 No such name NS mit.edu.edu.cn SOA dns…
232 8.150970   202.141.182.222   202.141.180.1     DNS    67 Standard query 0x0004 NS mit.edu
233 8.153379   202.141.180.1     202.141.182.222   DNS   446 Standard query response 0x0004 NS mit.edu NS usw2.akam.net NS ns1-37.…
234 8.180403   202.141.182.222   202.141.180.1     DNS    78 Standard query 0xfa7a AAAA edge.microsoft.com
```

- **17.**

是type PTR，不含answers

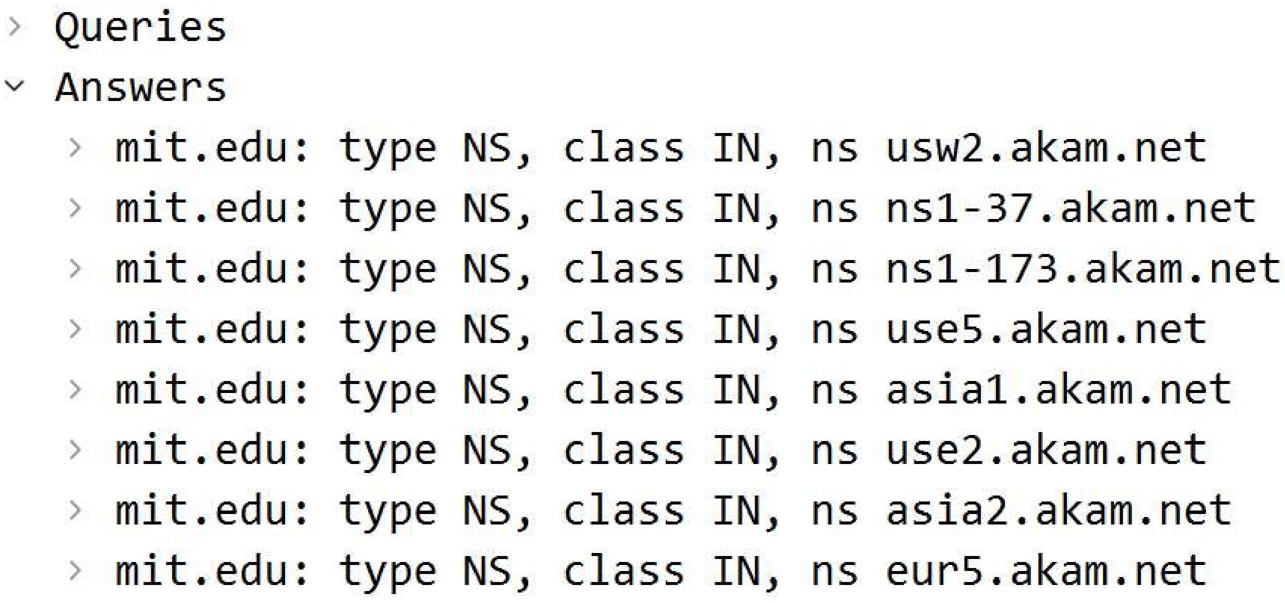


```
⌄ Queries
  ⌄ 1.180.141.202.in-addr.arpa: type PTR, class IN
      Name: 1.180.141.202.in-addr.arpa
      [Name Length: 26]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
  [Response In: 226]
```

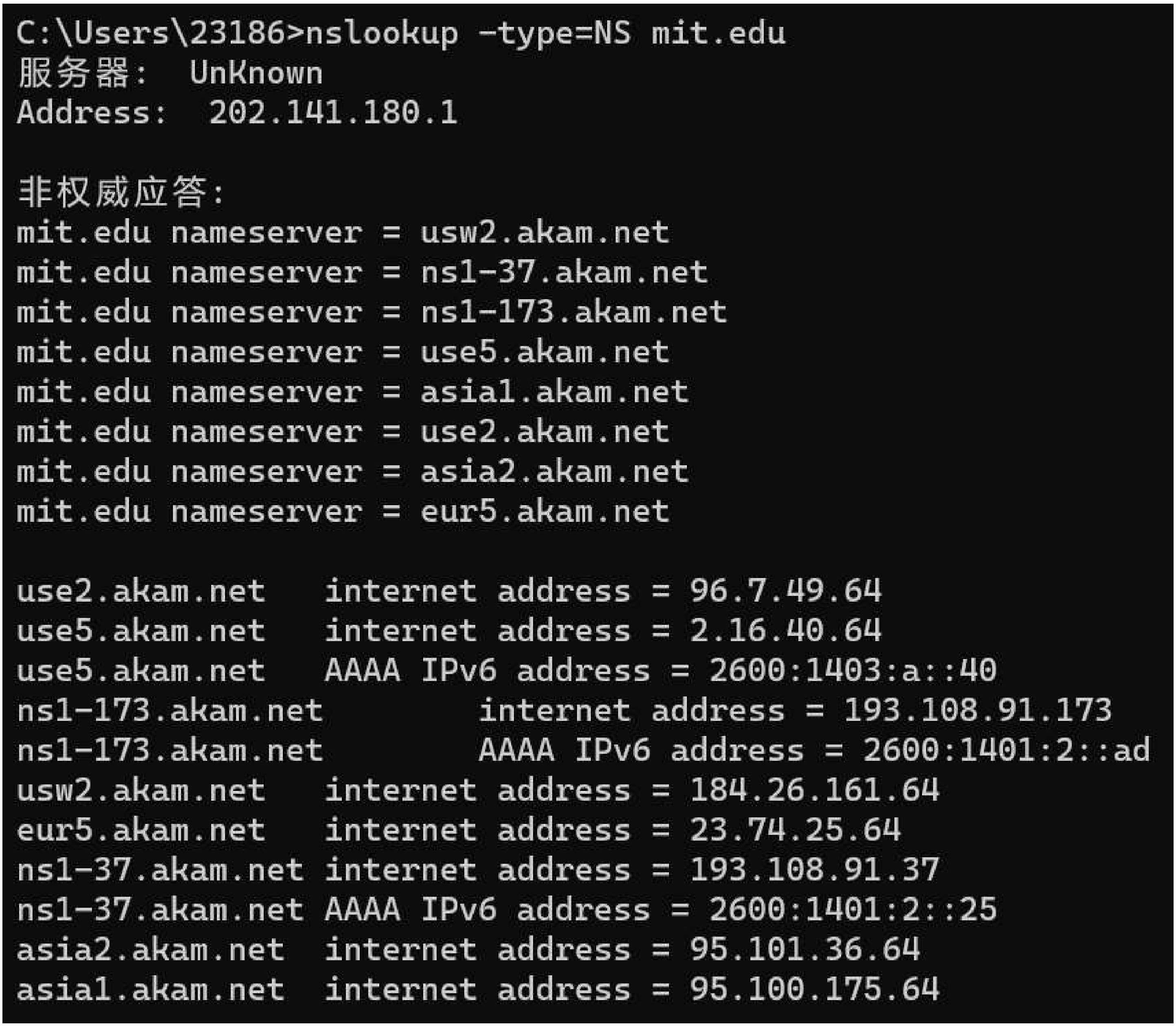
- **18.**

answers中的内容与nslookup得到的nameserver一致

没有给出ip地址但可以通过nslookup再次查询得到（?



```
› Queries
⌄ Answers
  › mit.edu: type NS, class IN, ns usw2.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 use5.akam.net
  › mit.edu: type NS, class IN, ns asia1.akam.net
  › mit.edu: type NS, class IN, ns use2.akam.net
  › mit.edu: type NS, class IN, ns asia2.akam.net
  › mit.edu: type NS, class IN, ns eur5.akam.net
```

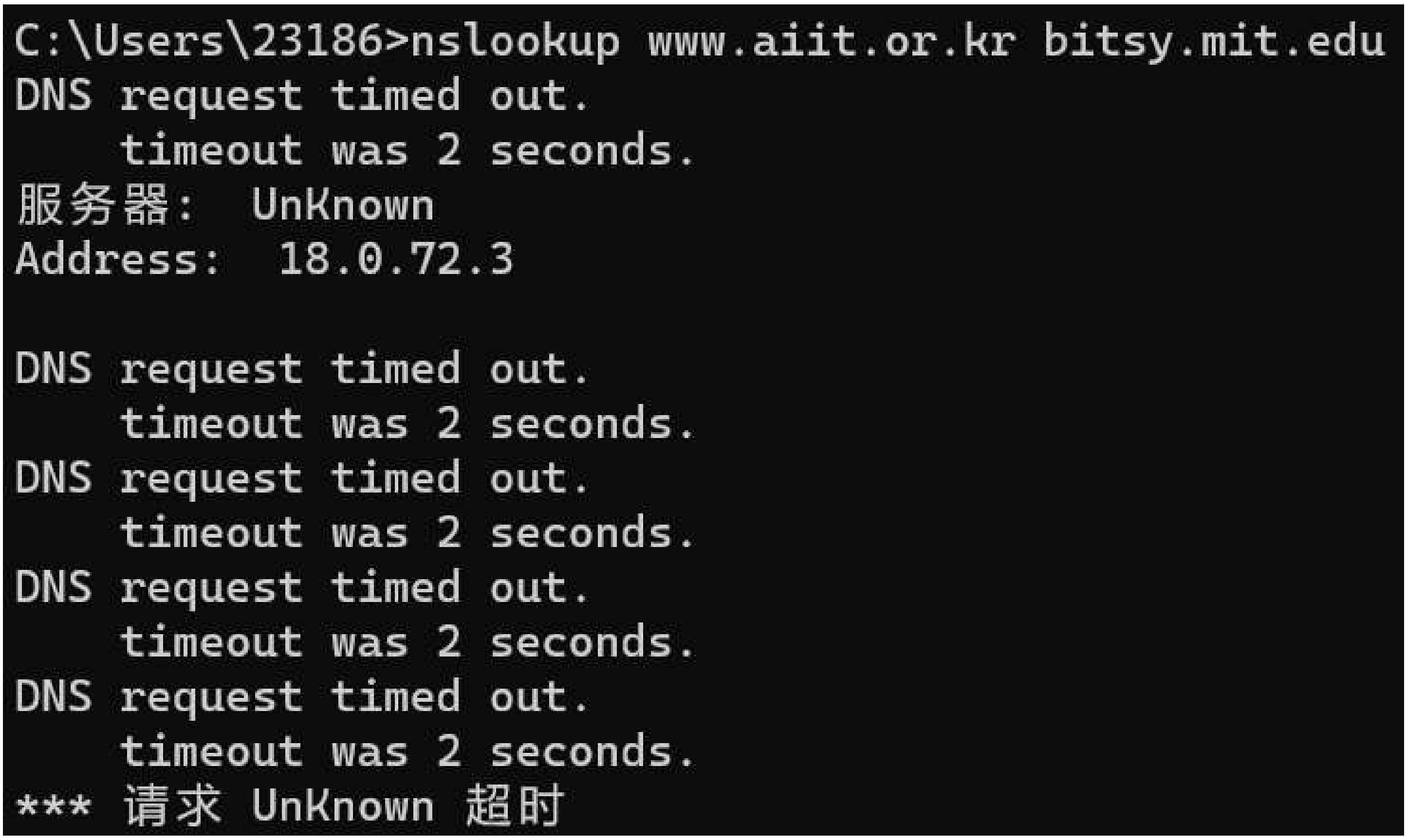


```
C:\Users\23186>nslookup -type=NS mit.edu
服务器:  UnKnown
Address:  202.141.180.1

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

use2.akam.net   internet address = 96.7.49.64
use5.akam.net   internet address = 2.16.40.64
use5.akam.net   AAAA IPv6 address = 2600:1403:a::40
ns1-173.akam.net        internet address = 193.108.91.173
ns1-173.akam.net        AAAA IPv6 address = 2600:1401:2::ad
usw2.akam.net   internet address = 184.26.161.64
eur5.akam.net   internet address = 23.74.25.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-37.akam.net AAAA IPv6 address = 2600:1401:2::25
asia2.akam.net  internet address = 95.101.36.64
asia1.akam.net  internet address = 95.100.175.64
```

- **19.**

如解答中的截图

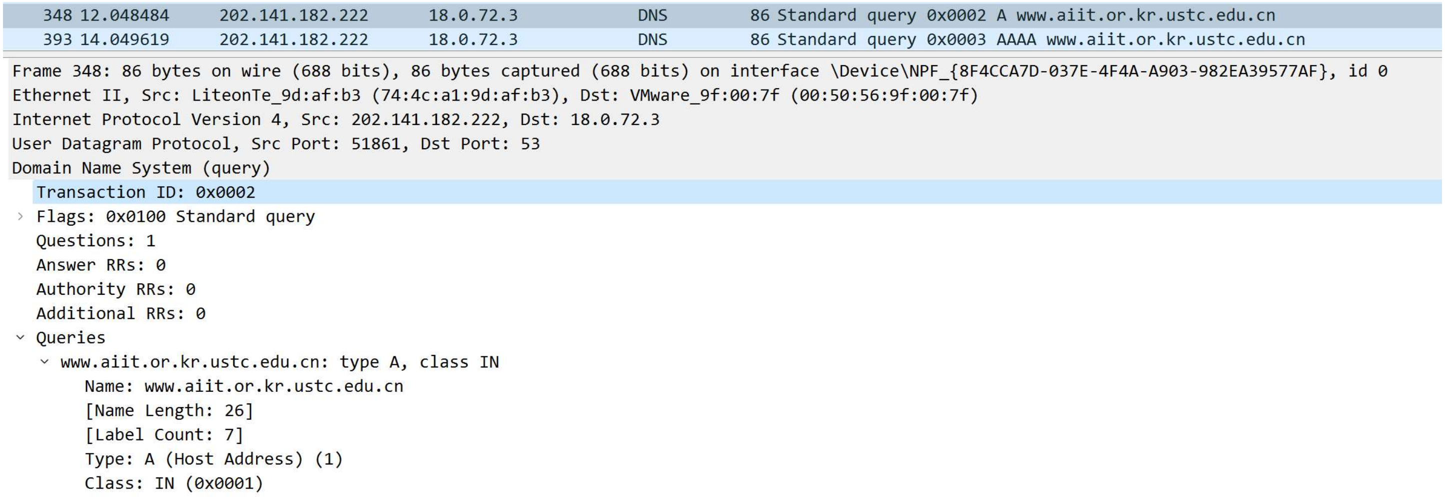
- ***一直超时，如下，所以在解答20与21问时用超时得到的结果，但22问采用了给出zip中文件的结果***



```
C:\Users\23186>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
```

- **20 and 21.**

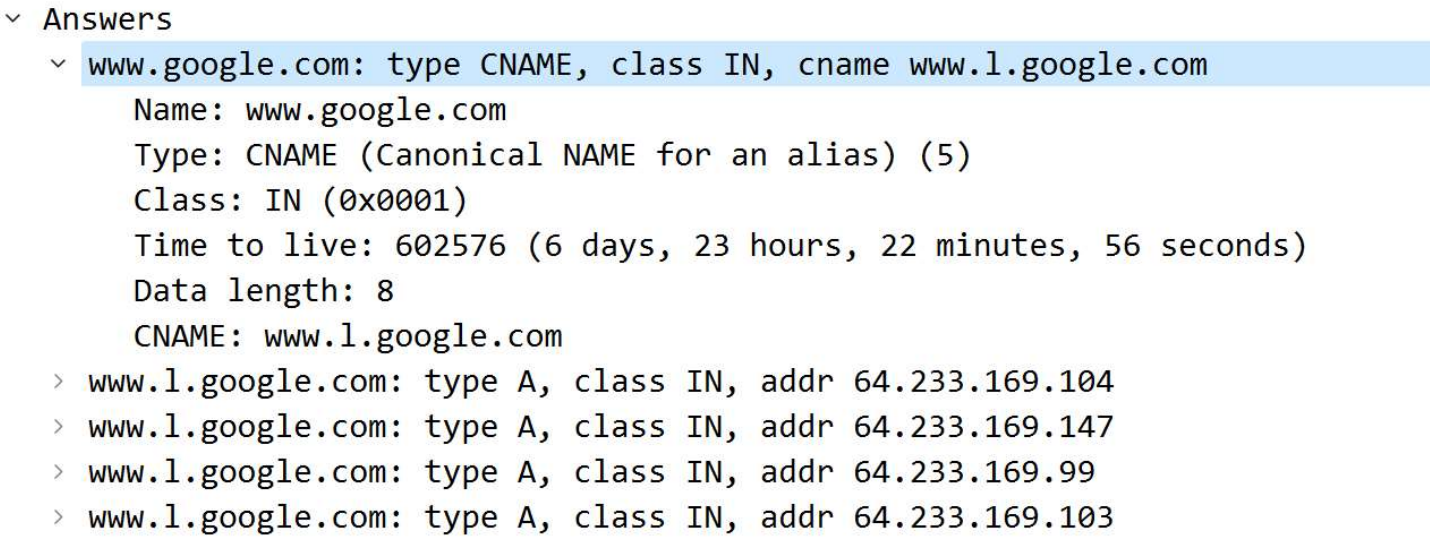
query请求被发送到18.0.72.3，是bitsy.mit.edu的地址，不是本地DNS的地址，类型为type A，没有answers



```
 348 12.048484    202.141.182.222    18.0.72.3     DNS     86 Standard query 0x0002 A www.aiit.or.kr.ustc.edu.cn
 393 14.049619    202.141.182.222    18.0.72.3     DNS     86 Standard query 0x0003 AAAA www.aiit.or.kr.ustc.edu.cn

Frame 348: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}, id 0
Ethernet II, Src: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3), Dst: VMware_9f:00:7f (00:50:56:9f:00:7f)
Internet Protocol Version 4, Src: 202.141.182.222, Dst: 18.0.72.3
User Datagram Protocol, Src Port: 51861, Dst Port: 53
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.ustc.edu.cn: type A, class IN
        Name: www.aiit.or.kr.ustc.edu.cn
        [Name Length: 26]
        [Label Count: 7]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

- **22.**

zip中的文件，其查询并非aiit.or.kr，为google.com，其使用的也并非是bitsy.mit.edu，所以answers个数可能不同，在此例中，个数为5个，包含有域名，类型等



```
v Answers
  v www.google.com: type CNAME, class IN, cname www.l.google.com
      Name: www.google.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 602576 (6 days, 23 hours, 22 minutes, 56 seconds)
      Data length: 8
      CNAME: www.l.google.com
  > www.l.google.com: type A, class IN, addr 64.233.169.104
  > www.l.google.com: type A, class IN, addr 64.233.169.147
  > www.l.google.com: type A, class IN, addr 64.233.169.99
  > www.l.google.com: type A, class IN, addr 64.233.169.103
```