山东大学＿＿＿计算机＿＿＿＿学院

＿＿计算机网络＿＿课程实验报告

学号：202400130039	姓名：张汇智	班级：智能
实验题目： Wireshark_DNS		
实验学时：2h	实验日期： 2025.	
实验目的： 深入研究 DNS 的客户端		
硬件环境： AMD ryzen R9 7900HX ; NVIDIA RTX4070LAPTOP ; RAM SAMSUNG 16GB*2 ; ROM WD770 1T+2T;		
软件环境：Windows11 23H2 （KB5056580）		

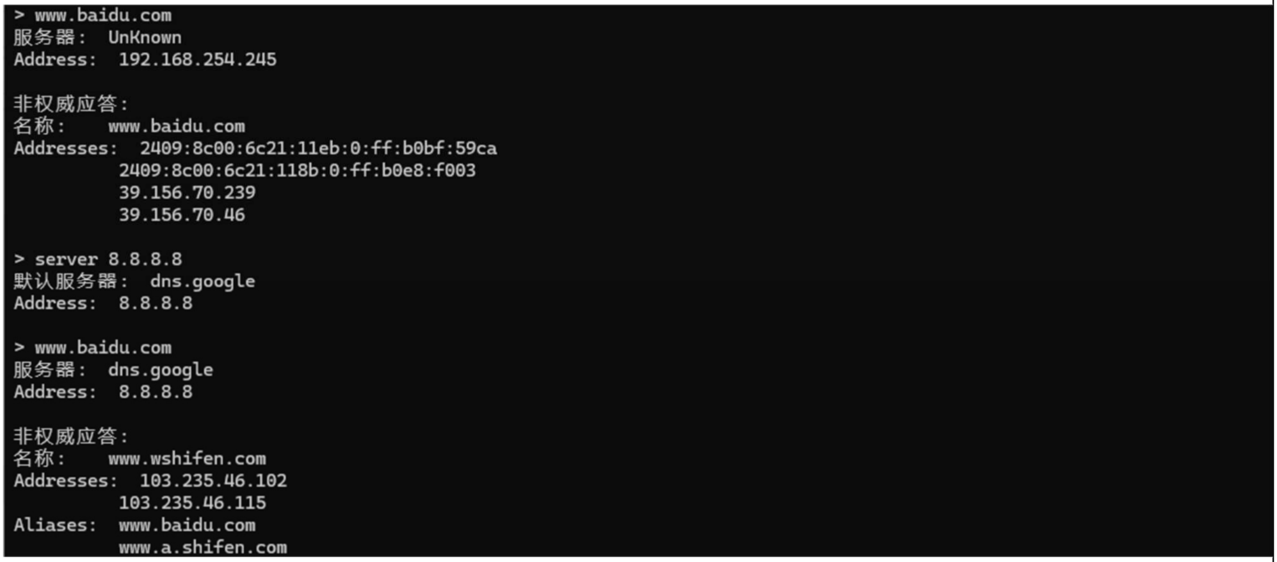
实验步骤与内容：

尝试 PDF 的三个指令

问题：

1.运行 nslookup 获取亚洲某台 Web 服务器的 IP 地址。该服务器的 IP 地址是多少？

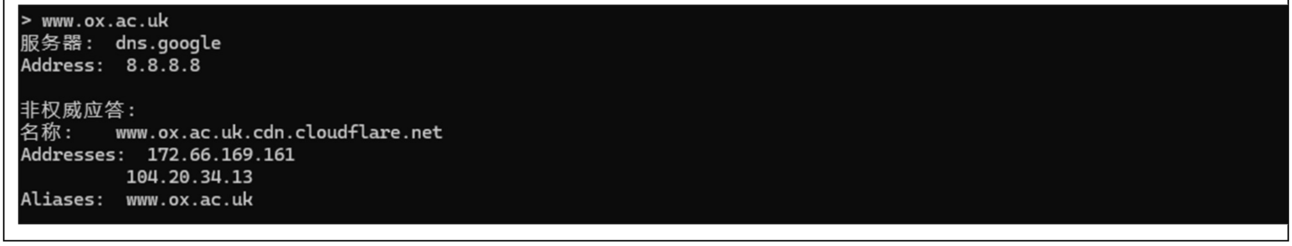
A:



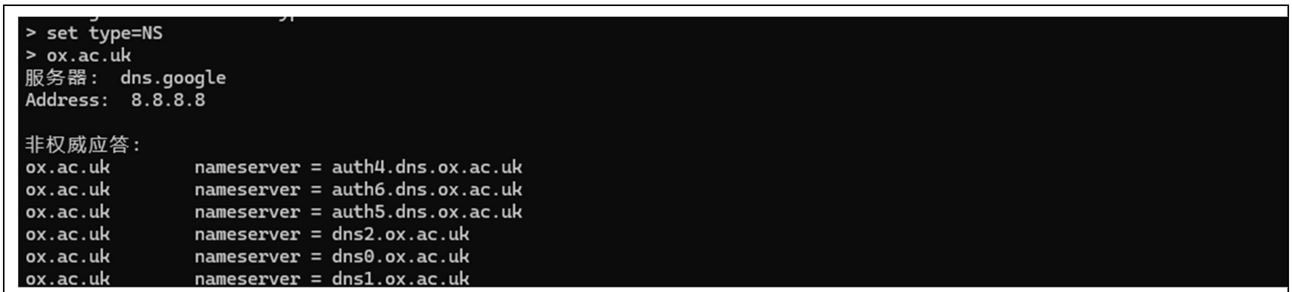
```
> www.baidu.com
服务器:  UnKnown
Address:  192.168.254.245

非权威应答:
名称:    www.baidu.com
Addresses:  2409:8c00:6c21:11eb:0:ff:b0bf:59ca
          2409:8c00:6c21:118b:0:ff:b0e8:f003
          39.156.70.239
          39.156.70.46

> server 8.8.8.8
默认服务器:  dns.google
Address:  8.8.8.8

> www.baidu.com
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
名称:    www.wshifen.com
Addresses:  103.235.46.102
          103.235.46.115
Aliases:  www.baidu.com
          www.a.shifen.com
```

2.运行 nslookup 来确定欧洲某所大学的权威 DNS 服务器。

A:



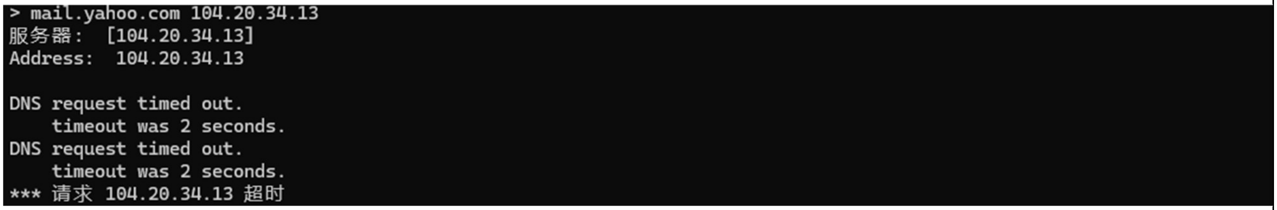
```
> www.ox.ac.uk
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
名称:    www.ox.ac.uk.cdn.cloudflare.net
Addresses:  172.66.169.161
          104.20.34.13
Aliases:  www.ox.ac.uk
```



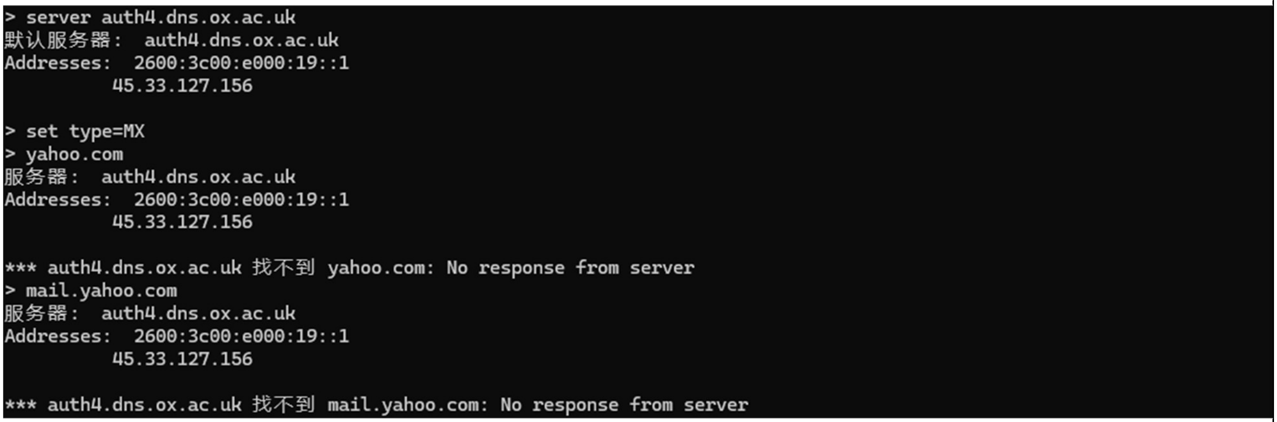
```
> set type=NS
> ox.ac.uk
服务器:  dns.google
Address:  8.8.8.8

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

3.行 nslookup，查询问题 2 中获取的其中一个 DNS 服务器，获取 Yahoo! 邮件的邮件服务器。它的 IP 地址是什么？

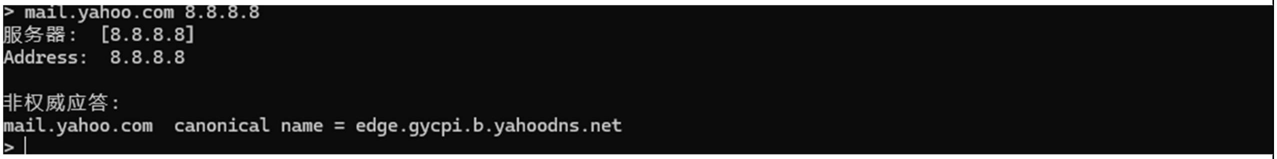
A:



```
> mail.yahoo.com 104.20.34.13
服务器:  [104.20.34.13]
Address:  104.20.34.13

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 104.20.34.13 超时
```



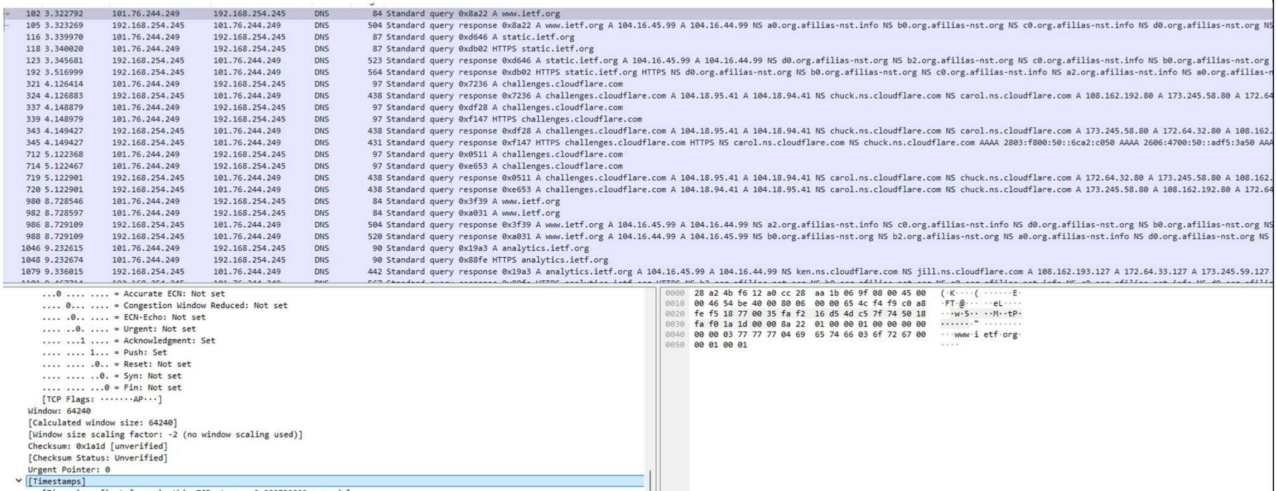
```
> server auth4.dns.ox.ac.uk
默认服务器:  auth4.dns.ox.ac.uk
Addresses:  2600:3c00:e000:19::1
          45.33.127.156

> set type=MX
> yahoo.com
服务器:  auth4.dns.ox.ac.uk
Addresses:  2600:3c00:e000:19::1
          45.33.127.156

*** auth4.dns.ox.ac.uk 找不到 yahoo.com: No response from server
> mail.yahoo.com
服务器:  auth4.dns.ox.ac.uk
Addresses:  2600:3c00:e000:19::1
          45.33.127.156

*** auth4.dns.ox.ac.uk 找不到 mail.yahoo.com: No response from server
```



```
> mail.yahoo.com 8.8.8.8
服务器:  [8.8.8.8]
Address:  8.8.8.8

非权威应答:
mail.yahoo.com  canonical name = edge.gycpi.b.yahoodns.net
>
```

牛津找不到我佛，谷歌找得到。

4.找到 DNS 查询和响应消息。然后通过 UDP 还是 TCP 发送？



```
 102 3.322792    101.76.244.249    192.168.254.245   DNS    84 Standard query 0x8a22 A www.ietf.org
 105 3.323269    192.168.254.245   101.76.244.249    DNS   504 Standard query response 0x8a22 A www.ietf.org A 104.16.45.99 A 104.16.44.99 NS a0.org.afilias-nst.info NS b0.org.afilias-nst.org NS c0.org.afilias-nst.info NS d0.org.afilias-nst.org NS
 116 3.339970    101.76.244.249    192.168.254.245   DNS    87 Standard query 0xd646 A static.ietf.org
 118 3.340020    101.76.244.249    192.168.254.245   DNS    87 Standard query 0xdb02 HTTPS static.ietf.org
 123 3.345681    192.168.254.245   101.76.244.249    DNS   523 Standard query response 0xd646 A static.ietf.org A 104.16.45.99 A 104.16.44.99 NS d0.org.afilias-nst.org NS b2.org.afilias-nst.org NS c0.org.afilias-nst.info NS b0.org.afilias-nst.org
 192 3.516999    192.168.254.245   101.76.244.249    DNS   564 Standard query response 0xdb02 HTTPS static.ietf.org HTTPS NS d0.org.afilias-nst.org NS b0.org.afilias-nst.org NS c0.org.afilias-nst.info NS a2.org.afilias-nst.info NS a0.org.afilias-n
 321 4.126414    101.76.244.249    192.168.254.245   DNS    97 Standard query 0x7236 A challenges.cloudflare.com
 324 4.126883    192.168.254.245   101.76.244.249    DNS   438 Standard query response 0x7236 A challenges.cloudflare.com A 104.18.95.41 A 104.18.94.41 NS chuck.ns.cloudflare.com NS carol.ns.cloudflare.com A 108.162.192.80 A 173.245.58.80 A 172.64
 337 4.148879    101.76.244.249    192.168.254.245   DNS    97 Standard query 0xdf28 A challenges.cloudflare.com
 339 4.148979    101.76.244.249    192.168.254.245   DNS    97 Standard query 0xf147 HTTPS challenges.cloudflare.com
 343 4.149427    192.168.254.245   101.76.244.249    DNS   438 Standard query response 0xdf28 A challenges.cloudflare.com A 104.18.95.41 A 104.18.94.41 NS chuck.ns.cloudflare.com NS carol.ns.cloudflare.com A 173.245.58.80 A 172.64.32.80 A 108.162.
 345 4.149427    192.168.254.245   101.76.244.249    DNS   431 Standard query response 0xf147 HTTPS challenges.cloudflare.com HTTPS NS carol.ns.cloudflare.com NS chuck.ns.cloudflare.com AAAA 2803:f800:50::6ca2:c050 AAAA 2606:4700:50::adf5:3a50 AAA
 712 5.122368    101.76.244.249    192.168.254.245   DNS    97 Standard query 0x0511 A challenges.cloudflare.com
 714 5.122467    101.76.244.249    192.168.254.245   DNS    97 Standard query 0xe653 A challenges.cloudflare.com
 719 5.122901    192.168.254.245   101.76.244.249    DNS   438 Standard query response 0x0511 A challenges.cloudflare.com A 104.18.95.41 A 104.18.94.41 NS carol.ns.cloudflare.com NS chuck.ns.cloudflare.com A 172.64.32.80 A 173.245.58.80 A 108.162.
 720 5.122901    192.168.254.245   101.76.244.249    DNS   438 Standard query response 0xe653 A challenges.cloudflare.com A 104.18.94.41 A 104.18.95.41 NS carol.ns.cloudflare.com NS chuck.ns.cloudflare.com A 173.245.58.80 A 108.162.192.80 A 172.64
 980 8.728546    101.76.244.249    192.168.254.245   DNS    84 Standard query 0x3f39 A www.ietf.org
 982 8.728597    101.76.244.249    192.168.254.245   DNS    84 Standard query 0xa031 A www.ietf.org
 986 8.729109    192.168.254.245   101.76.244.249    DNS   504 Standard query response 0x3f39 A www.ietf.org A 104.16.45.99 A 104.16.44.99 NS a2.org.afilias-nst.info NS c0.org.afilias-nst.info NS d0.org.afilias-nst.org NS b0.org.afilias-nst.org NS
 988 8.729109    192.168.254.245   101.76.244.249    DNS   520 Standard query response 0xa031 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS b0.org.afilias-nst.org NS b2.org.afilias-nst.org NS a0.org.afilias-nst.info NS d0.org.afilias-nst.org NS
1046 9.232615    101.76.244.249    192.168.254.245   DNS    90 Standard query 0x19a3 A analytics.ietf.org
1048 9.232674    101.76.244.249    192.168.254.245   DNS    90 Standard query 0x88fe HTTPS analytics.ietf.org
1079 9.336015    192.168.254.245   101.76.244.249    DNS   442 Standard query response 0x19a3 A analytics.ietf.org A 104.16.45.99 A 104.16.44.99 NS ken.ns.cloudflare.com NS jill.ns.cloudflare.com A 108.162.193.127 A 172.64.33.127 A 173.245.59.127
```

```
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1a1d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ˅ [Timestamps]
        [Time since first frame in this TCP stream: 0.000730000 seconds]
        [Time since previous frame in this TCP stream: 0.000019000 seconds]
```

```
0000  28 a2 4b f6 12 a0 cc 28  aa 1b 06 9f 08 00 45 00   (·K····( ······E·
0010  00 46 54 be 40 00 80 06  00 00 65 4c f4 f9 c0 a8   ·FT·@··· ··eL····
0020  fe f5 18 77 00 35 fa f2  16 d5 4d c5 7f 74 50 18   ···w·5·· ··M··tP·
0030  fa f0 1a 1d 00 00 8a 22  01 00 00 01 00 00 00 00   ·······" ········
0040  00 00 03 77 77 77 04 69  65 74 66 03 6f 72 67 00   ···www·i etf·org·
0050  00 01 00 01                                        ····
```

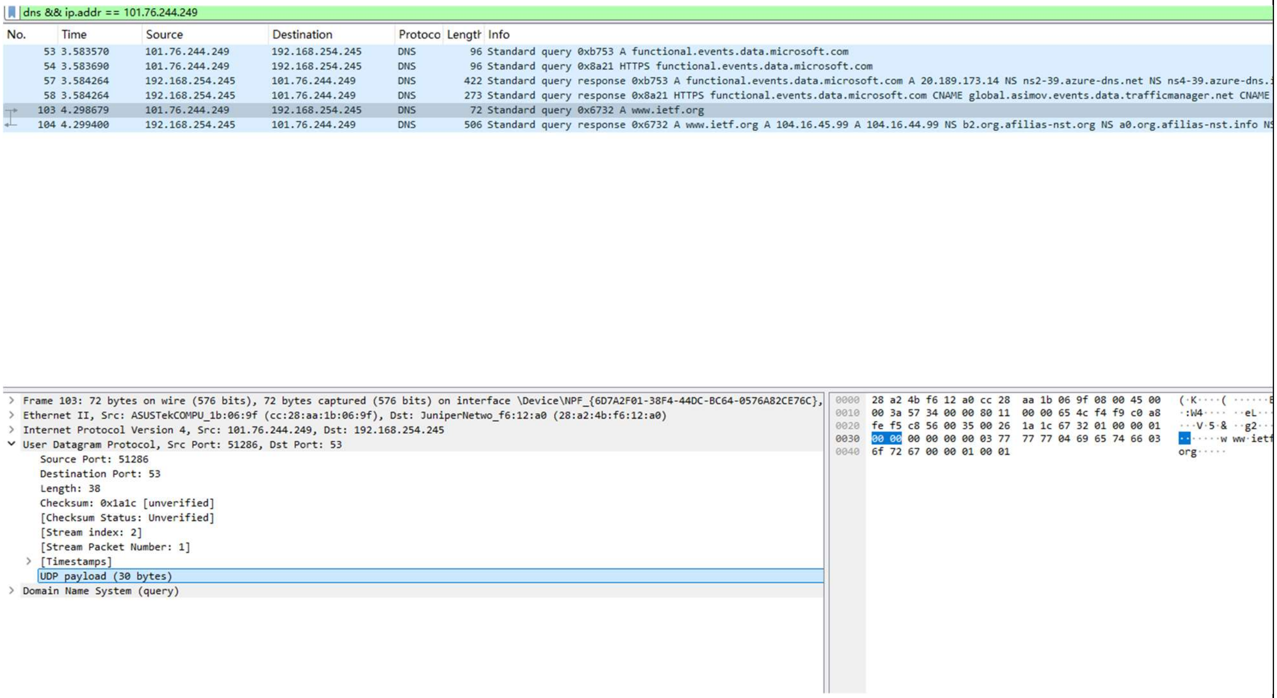
用 TCP 发送

很迷？怎么这么大？？

重启电脑试试。

再抠一次，这次干净了。

UDP 发送



```
dns && ip.addr == 101.76.244.249

No.   Time       Source           Destination      Protoco Length Info
   53 3.583570   101.76.244.249   192.168.254.245  DNS       96 Standard query 0xb753 A functional.events.data.microsoft.com
   54 3.583690   101.76.244.249   192.168.254.245  DNS       96 Standard query 0x8a21 HTTPS functional.events.data.microsoft.com
   57 3.584264   192.168.254.245  101.76.244.249   DNS      422 Standard query response 0xb753 A functional.events.data.microsoft.com A 20.189.173.14 NS ns2-39.azure-dns.net NS ns4-39.azure-dns.i
   58 3.584264   192.168.254.245  101.76.244.249   DNS      273 Standard query response 0x8a21 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME
  103 4.298679   101.76.244.249   192.168.254.245  DNS       72 Standard query 0x6732 A www.ietf.org
  104 4.299400   192.168.254.245  101.76.244.249   DNS      506 Standard query response 0x6732 A www.ietf.org A 104.16.45.99 A 104.16.44.99 NS b2.org.afilias-nst.org NS a0.org.afilias-nst.info NS
```

```
> Frame 103: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{6D7A2F01-38F4-44DC-BC64-0576A82CE76C},
> Ethernet II, Src: ASUSTekCOMPU_1b:06:9f (cc:28:aa:1b:06:9f), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
> Internet Protocol Version 4, Src: 101.76.244.249, Dst: 192.168.254.245
v User Datagram Protocol, Src Port: 51286, Dst Port: 53
    Source Port: 51286
    Destination Port: 53
    Length: 38
    Checksum: 0x1a1c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

```
0000  28 a2 4b f6 12 a0 cc 28  aa 1b 06 9f 08 00 45 00   (·K····( ······E
0010  00 3a 57 34 00 00 80 11  00 00 65 4c f4 f9 c0 a8   ·:W4···· ··eL···
0020  fe f5 c8 56 00 35 00 26  1a 1c 67 32 01 00 00 01   ···V·5·& ··g2···
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf
0040  6f 72 67 00 00 01 00 01                            org·····
```

5.DNS 查询报文的目的端口是什么？DNS 响应报文的源端口是什么？

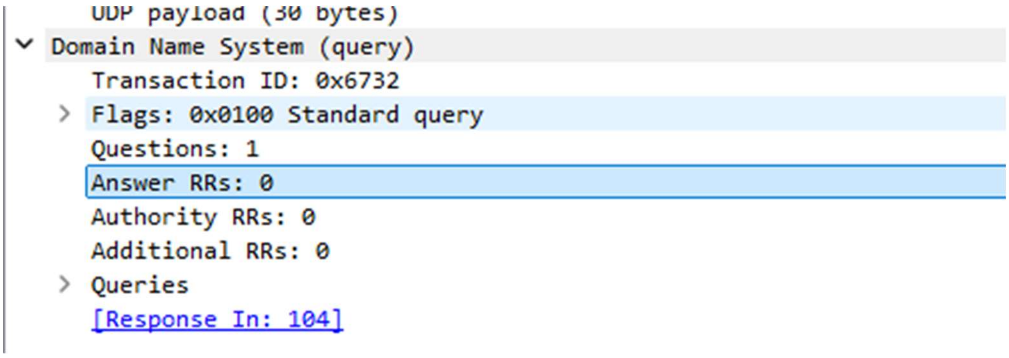
53；53

6.DNS 查询消息发送到哪个 IP 地址？使用 ipconfig 确定本地 DNS 服务器的 IP 地址。这两个 IP 地址相同吗？

192.168.254.245；相同。

7.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？

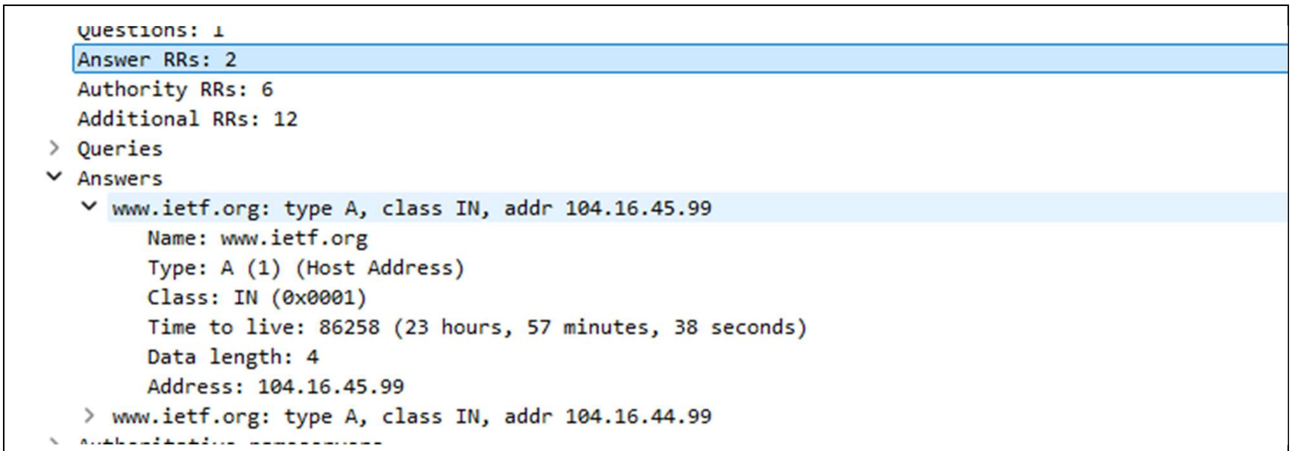
A 类型查询。Answerrrs 是空的



```
    UDP payload (30 bytes)
v Domain Name System (query)
    Transaction ID: 0x6732
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 104]
```

8.检查 DNS 响应消息。它提供了多少个“答案”？每个答案包含什么？

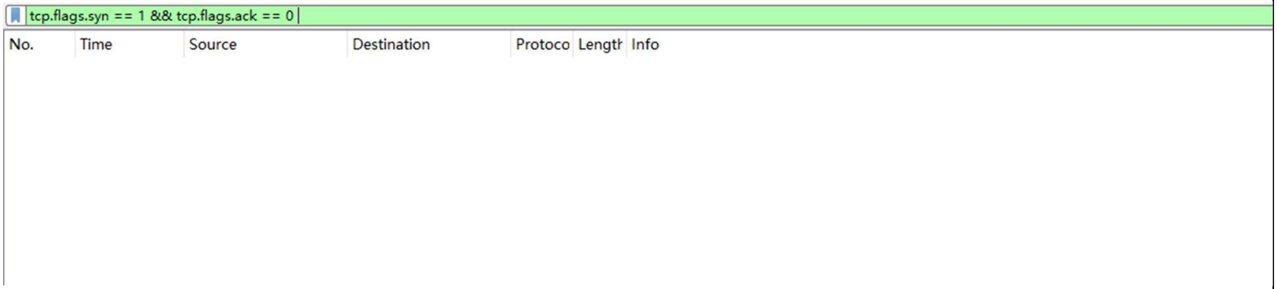
2。NAME;TYPE;CLASS;TIME TO LIVE;DATA LENGTH;ADRESS



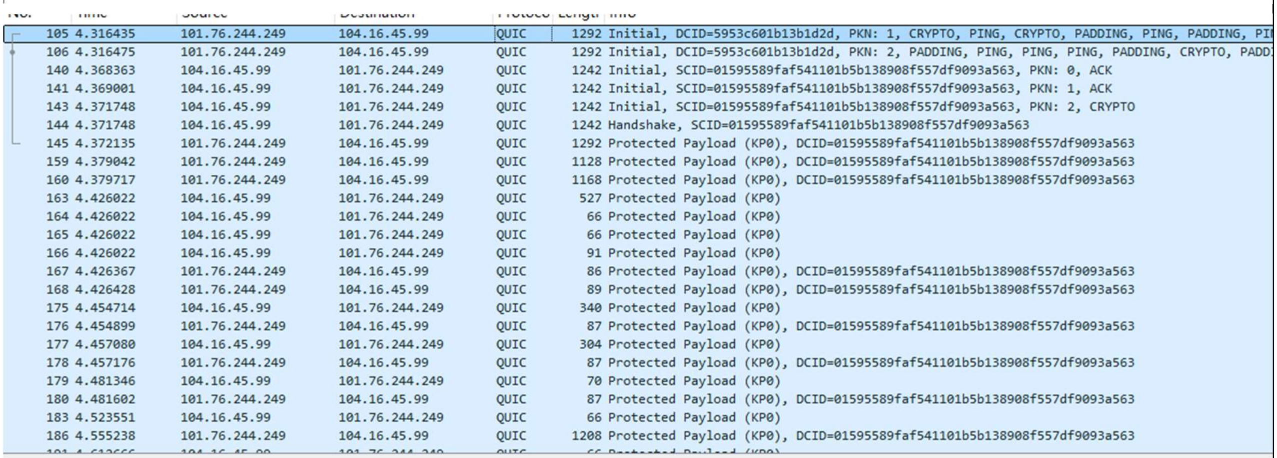
```
    Questions: 1
    Answer RRs: 2
    Authority RRs: 6
    Additional RRs: 12
  > Queries
  v Answers
     v www.ietf.org: type A, class IN, addr 104.16.45.99
          Name: www.ietf.org
          Type: A (1) (Host Address)
          Class: IN (0x0001)
          Time to live: 86258 (23 hours, 57 minutes, 38 seconds)
          Data length: 4
          Address: 104.16.45.99
     > www.ietf.org: type A, class IN, addr 104.16.44.99
```

9.考虑主机随后发送的 TCP SYN 数据包。SYN 数据包的目标 IP 地址是否与 DNS 响应消息中提供的任何 IP 地址相对应？

这次抓包只有 UDP 和 TSL1.3 何意味？？？



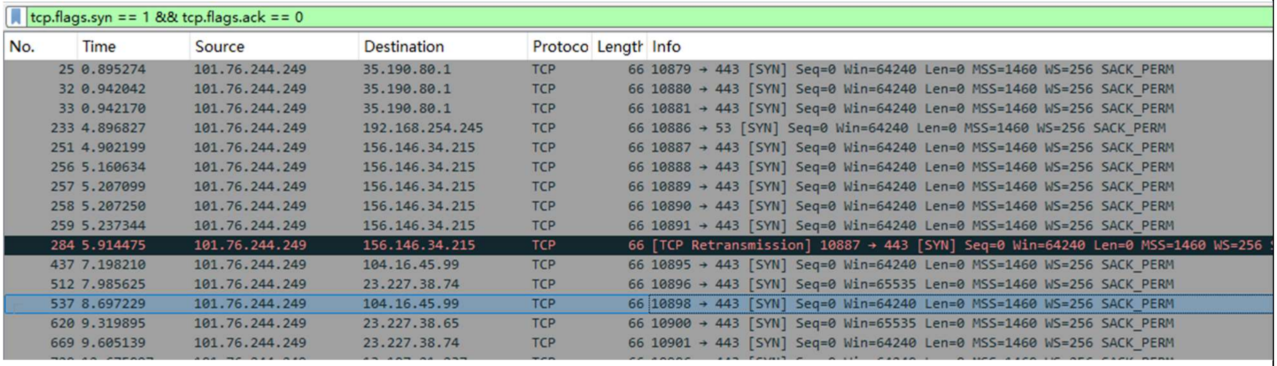
```
tcp.flags.syn == 1 && tcp.flags.ack == 0
No.   Time   Source   Destination   Protoco Lengtl Info
```



```
105 4.316435  101.76.244.249  104.16.45.99    QUIC  1292 Initial, DCID=5953c601b13b1d2d, PKN: 1, CRYPTO, PING, CRYPTO, PADDING, PING, PADDING, PI
106 4.316475  101.76.244.249  104.16.45.99    QUIC  1292 Initial, DCID=5953c601b13b1d2d, PKN: 2, PADDING, PING, PING, PING, PADDING, CRYPTO, PADDI
140 4.368363  104.16.45.99    101.76.244.249  QUIC  1242 Initial, SCID=01595589faf541101b5b138908f557df9093a563, PKN: 0, ACK
141 4.369001  104.16.45.99    101.76.244.249  QUIC  1242 Initial, SCID=01595589faf541101b5b138908f557df9093a563, PKN: 1, ACK
143 4.371748  104.16.45.99    101.76.244.249  QUIC  1242 Initial, SCID=01595589faf541101b5b138908f557df9093a563, PKN: 2, CRYPTO
144 4.371748  104.16.45.99    101.76.244.249  QUIC  1242 Handshake, SCID=01595589faf541101b5b138908f557df9093a563
145 4.372135  101.76.244.249  104.16.45.99    QUIC  1292 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
159 4.379042  101.76.244.249  104.16.45.99    QUIC  1128 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
160 4.379717  101.76.244.249  104.16.45.99    QUIC  1168 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
163 4.426022  104.16.45.99    101.76.244.249  QUIC   527 Protected Payload (KP0)
164 4.426022  104.16.45.99    101.76.244.249  QUIC    66 Protected Payload (KP0)
165 4.426022  104.16.45.99    101.76.244.249  QUIC    66 Protected Payload (KP0)
166 4.426022  104.16.45.99    101.76.244.249  QUIC    91 Protected Payload (KP0)
167 4.426367  101.76.244.249  104.16.45.99    QUIC    86 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
168 4.426428  101.76.244.249  104.16.45.99    QUIC    89 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
175 4.454714  104.16.45.99    101.76.244.249  QUIC   340 Protected Payload (KP0)
176 4.454899  101.76.244.249  104.16.45.99    QUIC    87 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
177 4.457080  104.16.45.99    101.76.244.249  QUIC   304 Protected Payload (KP0)
178 4.457176  101.76.244.249  104.16.45.99    QUIC    87 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
179 4.481346  104.16.45.99    101.76.244.249  QUIC    70 Protected Payload (KP0)
180 4.481602  101.76.244.249  104.16.45.99    QUIC    87 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
183 4.523551  104.16.45.99    101.76.244.249  QUIC    66 Protected Payload (KP0)
186 4.555238  101.76.244.249  104.16.45.99    QUIC  1208 Protected Payload (KP0), DCID=01595589faf541101b5b138908f557df9093a563
```

//为什么不走 TCP SYN 啊啊啊啊啊我是集美我要互搏了

又抓了一次，这次成功了。

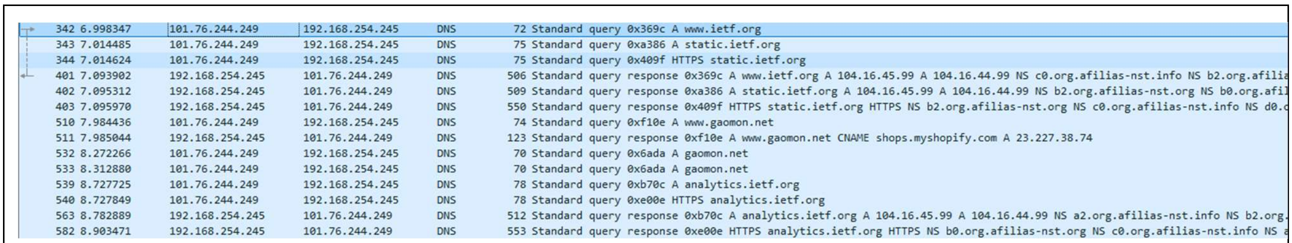


```
tcp.flags.syn == 1 && tcp.flags.ack == 0
No.  Time      Source          Destination      Protoco Lengtl Info
 25 0.895274  101.76.244.249  35.190.80.1      TCP   66 10879 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 32 0.942042  101.76.244.249  35.190.80.1      TCP   66 10880 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 33 0.942170  101.76.244.249  35.190.80.1      TCP   66 10881 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
233 4.896827  101.76.244.249  192.168.254.245  TCP   66 10886 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
251 4.902199  101.76.244.249  156.146.34.215   TCP   66 10887 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
256 5.160634  101.76.244.249  156.146.34.215   TCP   66 10888 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
257 5.207099  101.76.244.249  156.146.34.215   TCP   66 10889 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
258 5.207250  101.76.244.249  156.146.34.215   TCP   66 10890 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
259 5.237344  101.76.244.249  156.146.34.215   TCP   66 10891 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
284 5.914475  101.76.244.249  156.146.34.215   TCP   66 [TCP Retransmission] 10887 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
437 7.198210  101.76.244.249  104.16.45.99     TCP   66 10895 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
512 7.985625  101.76.244.249  23.227.38.74     TCP   66 10896 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
537 8.697229  101.76.244.249  104.16.45.99     TCP   66 10898 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
620 9.319895  101.76.244.249  23.227.38.65     TCP   66 10900 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
669 9.605139  101.76.244.249  23.227.38.74     TCP   66 10901 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

ANSWER:**是的。**

10. 此网页包含图片。在检索每张图片之前，您的主机是否会发出新的 DNS 查询?

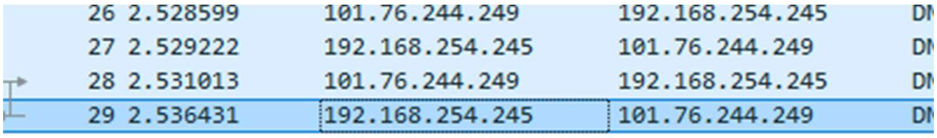
域名不同的 会发出新的查询。



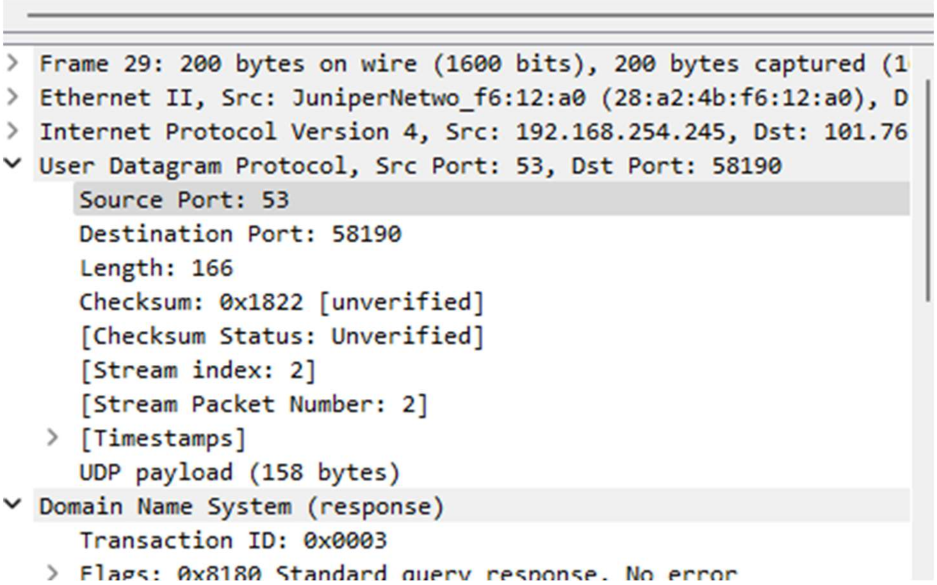
```
342 6.998347   101.76.244.249   192.168.254.245   DNS    72 Standard query 0x369c A www.ietf.org
343 7.014485   101.76.244.249   192.168.254.245   DNS    75 Standard query 0xa386 A static.ietf.org
344 7.014624   101.76.244.249   192.168.254.245   DNS    75 Standard query 0x409f HTTPS static.ietf.org
401 7.093902   192.168.254.245  101.76.244.249    DNS   506 Standard query response 0x369c A www.ietf.org A 104.16.45.99 A 104.16.44.99 NS c0.org.afilias-nst.info NS b2.org.afilia
402 7.095312   192.168.254.245  101.76.244.249    DNS   509 Standard query response 0xa386 A static.ietf.org A 104.16.45.99 A 104.16.44.99 NS b2.org.afilias-nst.org NS b0.org.afil
403 7.095970   192.168.254.245  101.76.244.249    DNS   550 Standard query response 0x409f HTTPS static.ietf.org HTTPS NS b2.org.afilias-nst.org NS c0.org.afilias-nst.info NS d0.c
510 7.984436   101.76.244.249   192.168.254.245   DNS    74 Standard query 0xf10e A www.gaomon.net
511 7.985044   192.168.254.245  101.76.244.249    DNS   123 Standard query response 0xf10e A www.gaomon.net CNAME shops.myshopify.com A 23.227.38.74
532 8.272266   101.76.244.249   192.168.254.245   DNS    70 Standard query 0x6ada A gaomon.net
533 8.312880   101.76.244.249   192.168.254.245   DNS    70 Standard query 0x6ada A gaomon.net
539 8.727725   101.76.244.249   192.168.254.245   DNS    78 Standard query 0xb70c A analytics.ietf.org
540 8.727849   101.76.244.249   192.168.254.245   DNS    78 Standard query 0xe00e HTTPS analytics.ietf.org
563 8.782889   192.168.254.245  101.76.244.249    DNS   512 Standard query response 0xb70c A analytics.ietf.org A 104.16.45.99 A 104.16.44.99 NS a2.org.afilias-nst.info NS b2.org.
582 8.903471   192.168.254.245  101.76.244.249    DNS   553 Standard query response 0xe00e HTTPS analytics.ietf.org HTTPS NS b0.org.afilias-nst.org NS c0.org.afilias-nst.info NS a
```

这里有 analytic 应该是登录的 JS Script 请求

11. DNS 查询报文的目的端口是什么？ DNS 响应报文的源端口是什么？



```
26 2.528599   101.76.244.249    192.168.254.245   DN
27 2.529222   192.168.254.245   101.76.244.249    DN
28 2.531013   101.76.244.249    192.168.254.245   DN
29 2.536431   192.168.254.245   101.76.244.249    DN
```



```
> Frame 29: 200 bytes on wire (1600 bits), 200 bytes captured (1
> Ethernet II, Src: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0), D
> Internet Protocol Version 4, Src: 192.168.254.245, Dst: 101.76
v User Datagram Protocol, Src Port: 53, Dst Port: 58190
    Source Port: 53
    Destination Port: 58190
    Length: 166
    Checksum: 0x1822 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 2]
  > [Timestamps]
    UDP payload (158 bytes)
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
```

53;53.

12.DNS 查询消息发送到哪个 IP 地址？这是您的默认本地 DNS 服务器的 IP 地址吗？

192.168.254.245　是的。

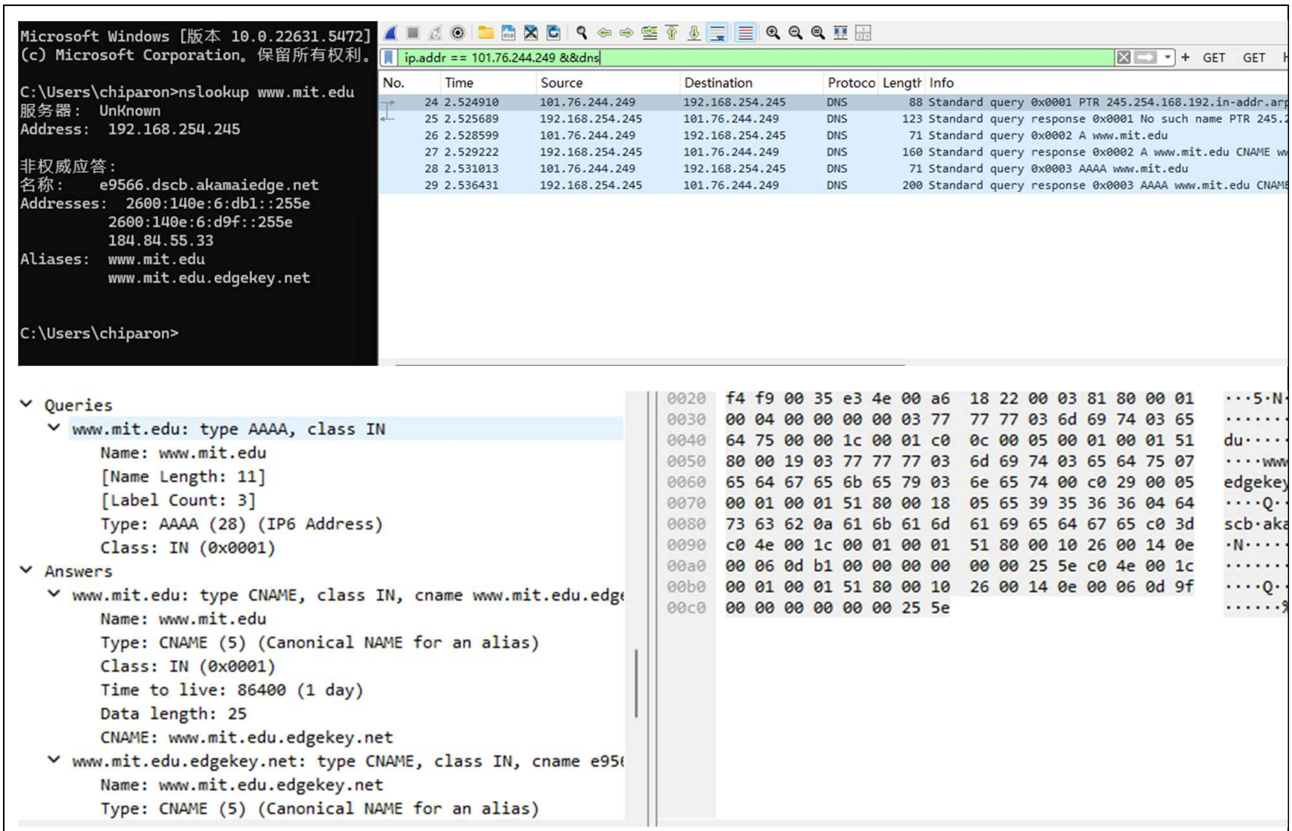
13.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？

AAAA 类型。无答案。

14.检查 DNS 响应消息。它提供了多少个“答案”？每个答案包含什么？

4 答案。2CNAME2AAAA 地址。每个答案包含 name type class timetolive datalength

15.提供截图。



```
Microsoft Windows [版本 10.0.22631.5472]
(c) Microsoft Corporation。保留所有权利。

C:\Users\chiparon>nslookup www.mit.edu
服务器:  UnKnown
Address:  192.168.254.245

非权威应答:
名称:    e9566.dscb.akamaiedge.net
Addresses:  2600:140e:6:db1::255e
          2600:140e:6:d9f::255e
          184.84.55.33
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net


C:\Users\chiparon>
```

```
ip.addr == 101.76.244.249 &&dns

No.  Time      Source           Destination      Protoco Length Info
  24 2.524910  101.76.244.249   192.168.254.245  DNS      88 Standard query 0x0001 PTR 245.254.168.192.in-addr.arp
  25 2.525689  192.168.254.245  101.76.244.249   DNS     123 Standard query response 0x0001 No such name PTR 245.2
  26 2.528599  101.76.244.249   192.168.254.245  DNS      71 Standard query 0x0002 A www.mit.edu
  27 2.529222  192.168.254.245  101.76.244.249   DNS     160 Standard query response 0x0002 A www.mit.edu CNAME ww
  28 2.531013  101.76.244.249   192.168.254.245  DNS      71 Standard query 0x0003 AAAA www.mit.edu
  29 2.536431  192.168.254.245  101.76.244.249   DNS     200 Standard query response 0x0003 AAAA www.mit.edu CNAME
```

```
∨ Queries
  ∨ www.mit.edu: type AAAA, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
∨ Answers
  ∨ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edge
      Name: www.mit.edu
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ∨ www.mit.edu.edgekey.net: type CNAME, class IN, cname e956
      Name: www.mit.edu.edgekey.net
      Type: CNAME (5) (Canonical NAME for an alias)
```

```
0020  f4 f9 00 35 e3 4e 00 a6  18 22 00 03 81 80 00 01   ···5·N·
0030  00 04 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······
0040  64 75 00 00 1c 00 01 c0  0c 00 05 00 01 00 01 51   du·····
0050  80 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····www
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey
0070  00 01 00 01 51 80 00 18  05 65 39 35 36 36 04 64   ····Q··
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3d   scb·aka
0090  c0 4e 00 1c 00 01 00 01  51 80 00 10 26 00 14 0e   ·N·····
00a0  00 06 0d b1 00 00 00 00  00 00 25 5e c0 4e 00 1c   ·······
00b0  00 01 00 01 51 80 00 10  26 00 14 0e 00 06 0d 9f   ····Q··
00c0  00 00 00 00 00 00 25 5e                            ······%
```

16. DNS 查询消息发送到哪个 IP 地址？这是您的默认本地 DNS 服务器的 IP 地址吗？

192.168.254.245 貌似无法访问。切谷歌吧。

8.8.8.8　是的。

17. 检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？

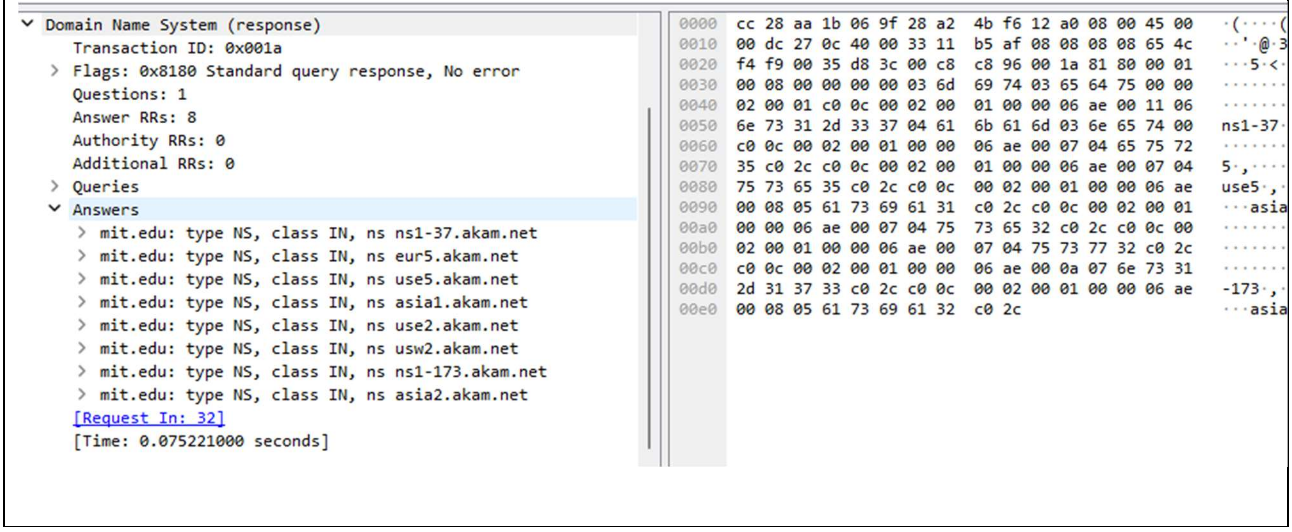
NS. 无答案。（用自己的 DNS 服务器是 A 类型查询，发生什么了？）

18. 检查 DNS 响应消息。响应消息提供了哪些 MIT 域名服务器？该响应消息是否也提供了 MIT 域名服务器的 IP 地址？

给出了上一级域的权威服务器，无 mit 服务器。提供了 IP 地址。此为自己 DNSserver

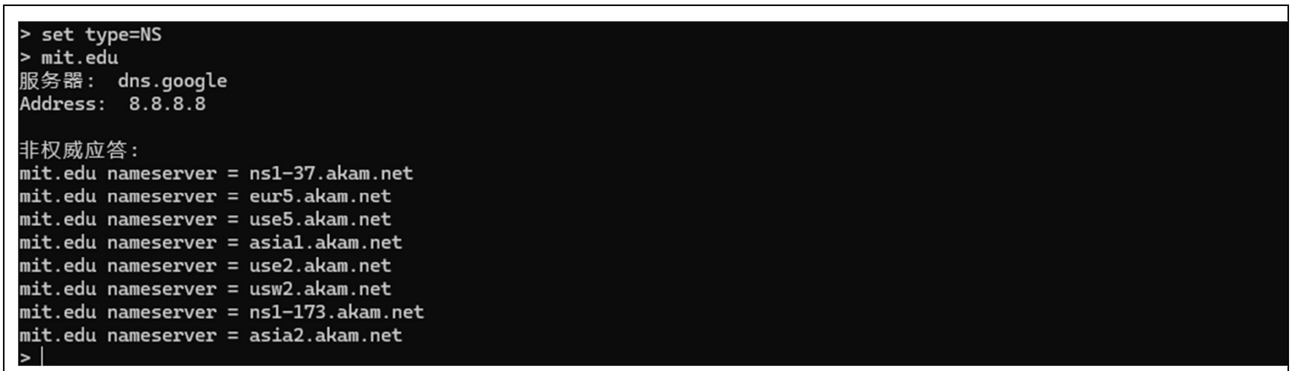
提供了 8 个 MIT 域名的权威名称服务器，没有 IP 地址。

19. 提供截图。



```
∨ Domain Name System (response)
    Transaction ID: 0x001a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  ∨ Answers
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns eur5.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 usw2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    [Request In: 32]
    [Time: 0.075221000 seconds]
```

```
0000  cc 28 aa 1b 06 9f 28 a2  4b f6 12 a0 08 00 45 00   ·(····(
0010  00 dc 27 0c 40 00 33 11  b5 af 08 08 08 08 65 4c   ··'·@·3
0020  f4 f9 00 35 d8 3c 00 c8  c8 96 00 1a 81 80 00 01   ···5·<·
0030  00 08 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······
0040  02 00 01 c0 0c 00 02 00  01 00 00 06 ae 00 11 06   ·······
0050  6e 73 31 2d 33 37 04 61  6b 61 6d 03 6e 65 74 00   ns1-37·
0060  c0 0c 00 02 00 01 00 00  06 ae 00 07 04 65 75 72   ·······
0070  35 c0 2c c0 0c 00 02 00  01 00 00 06 ae 00 07 04   5·,····
0080  75 73 65 35 c0 2c c0 0c  00 02 00 01 00 00 06 ae   use5·,·
0090  00 08 05 61 73 69 61 31  c0 2c c0 0c 00 02 00 01   ···asia
00a0  00 00 06 ae 00 07 04 75  73 65 32 c0 2c c0 0c 00   ·······
00b0  02 00 01 00 00 06 ae 00  07 04 75 73 77 32 c0 2c   ·······
00c0  c0 0c 00 02 00 01 00 00  06 ae 00 0a 07 6e 73 31   ·······
00d0  2d 31 37 33 c0 2c c0 0c  00 02 00 01 00 00 06 ae   -173·,·
00e0  00 08 05 61 73 69 61 32  c0 2c                     ···asia
```



```
> set type=NS
> mit.edu
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.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
> |
```

20.DNS 查询消息发送到哪个 IP 地址？这是你的默认本地 DNS 服务器的 IP 地址吗？如果不是，那么这个 IP 地址对应的是什么？

BITSY.MIT.EDU SEEMS NOT AVAILABLE AT PRESENT.

SO I CHOSE 180.76.76.76.

NO IT CORRESPONDS TO BAIDU’S DNS SERVER.

21.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？

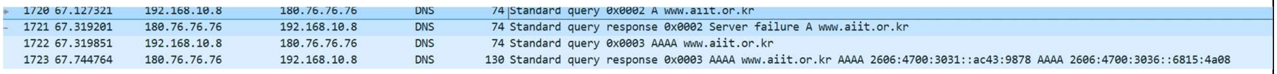
//THERE ARE 2 QUERY AND THE IPV4 ONE RESPONDING WITH FAILURE.LATER THE IPV6 ONE WOULD BE DISPLAYED.

AAAA TYPE WITH NO ANSWER.

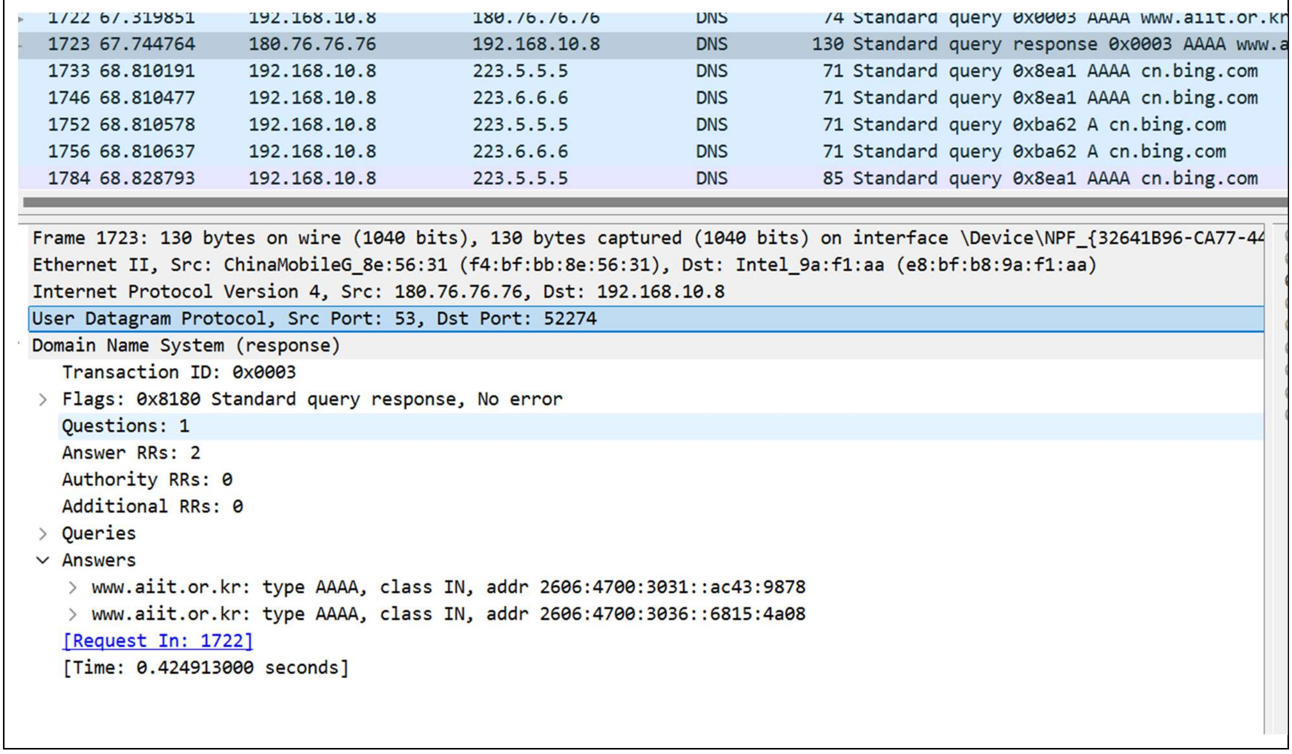
22.检查 DNS 响应消息。它提供了多少个“答案”？每个答案包含什么？

2.NAME TYPE CLASS ADDRESS(HERE IST IPV6 ADDR.)

23.提供截图。



```
1720 67.127321  192.168.10.8   180.76.76.76   DNS   74 Standard query 0x0002 A www.aiit.or.kr
1721 67.319201  180.76.76.76   192.168.10.8   DNS   74 Standard query response 0x0002 Server failure A www.aiit.or.kr
1722 67.319851  192.168.10.8   180.76.76.76   DNS   74 Standard query 0x0003 AAAA www.aiit.or.kr
1723 67.744764  180.76.76.76   192.168.10.8   DNS  130 Standard query response 0x0003 AAAA www.aiit.or.kr AAAA 2606:4700:3031::ac43:9878 AAAA 2606:4700:3036::6815:4a08
```



```
1722 67.319851  192.168.10.8   180.76.76.76   DNS   74 Standard query 0x0003 AAAA www.aiit.or.kr
1723 67.744764  180.76.76.76   192.168.10.8   DNS  130 Standard query response 0x0003 AAAA www.a
1733 68.810191  192.168.10.8   223.5.5.5      DNS   71 Standard query 0x8ea1 AAAA cn.bing.com
1746 68.810477  192.168.10.8   223.6.6.6      DNS   71 Standard query 0x8ea1 AAAA cn.bing.com
1752 68.810578  192.168.10.8   223.5.5.5      DNS   71 Standard query 0xba62 A cn.bing.com
1756 68.810637  192.168.10.8   223.6.6.6      DNS   71 Standard query 0xba62 A cn.bing.com
1784 68.828793  192.168.10.8   223.5.5.5      DNS   85 Standard query 0x8ea1 AAAA cn.bing.com

Frame 1723: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Device\NPF_{32641B96-CA77-44
Ethernet II, Src: ChinaMobileG_8e:56:31 (f4:bf:bb:8e:56:31), Dst: Intel_9a:f1:aa (e8:bf:b8:9a:f1:aa)
Internet Protocol Version 4, Src: 180.76.76.76, Dst: 192.168.10.8
User Datagram Protocol, Src Port: 53, Dst Port: 52274
Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
      > www.aiit.or.kr: type AAAA, class IN, addr 2606:4700:3031::ac43:9878
      > www.aiit.or.kr: type AAAA, class IN, addr 2606:4700:3036::6815:4a08
    [Request In: 1722]
    [Time: 0.424913000 seconds]
```

结论分析与体会：

（1）如果想要访问一个网站，那么计算机要知道 DNS 服务器的 IP 地址

（2）本机只向自己的 DNS 服务器查询；

（3）DNS 服务器查询到每个域名的 IP 地址是通过分级查询的方式；域名的层级结构如下：主机名.次级域名.顶级域名.根域名