计网Lab3-DNS

学号：PB21111723 姓名：王涵

问题解答

1.运行*nslookup*以获取一个亚洲的Web服务器的IP地址。该服务器的IP地址是什么?

```
PS C:\Users\wangh\Desktop> nslookup qq.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    qq.com
Address:  157.255.219.143
```

2.运行*nslookup*来确定一个欧洲的大学的权威DNS服务器。

```
PS C:\Users\wangh\Desktop> 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 = dns1.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 = auth4.dns.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
```

3.运行nslookup，使用问题2中一个已获得的DNS服务器，来查询Yahoo!邮箱的邮件服务器。它的IP地址是什么?

```
PS C:\Users\wangh\Desktop> nslookup -type=MX yahoo.com dns0.ox.ac.uk
服务器:  auth0.dns.ox.ac.uk
Address:  129.67.1.190

*** auth0.dns.ox.ac.uk 找不到 yahoo.com: Query refused
```

雅虎找不到，难绷，换成助教在群里发的8.8.8.8

```
PS C:\Users\wangh\Desktop> nslookup -type=MX yahoo.com 8.8.8.8
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
yahoo.com       MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
```

4.找到DNS查询和响应报文。它们是否通过UDP或TCP发送?

```
65 8.719751    100.64.145.245    202.38.64.56      DNS    … Standard query 0xe18e AAAA www.ietf.org
66 8.719863    100.64.145.245    202.38.64.56      DNS    … Standard query 0x0255 A www.ietf.org
67 8.719947    100.64.145.245    202.38.64.56      DNS    … Standard query 0x0f6f HTTPS www.ietf.org
68 8.904953    202.38.64.56      100.64.145.245    DNS    … Standard query response 0x0255 A www.ietf.org A 104.16.45.99 A 104.16.44.
```

```
Time to Live: 128
Protocol: UDP (17)
```

通过UDP发送。

5.DNS查询消息的目标端口是什么？ DNS响应消息的源端口是什么?

```
User Datagram Protocol, Src Port: 60528, Dst Port: 53
   Source Port: 60528
   Destination Port: 53
   Length: 38
```

目标端口：53 源端口：60528

6.DNS查询报文发送到哪个IP地址？使用ipconfig来确定本地DNS服务器的IP地址。这两个IP地址是否相同?

发送到202.38.64.56

```
65 8.719751    100.64.145.245    202.38.64.56    DNS    … Standard query 0xe18e AAAA www.ietf.org
66 8.719863    100.64.145.245    202.38.64.56    DNS    … Standard query 0x0255 A www.ietf.org
```

本地DNS服务器的ip地址是20.38.64.56，二者相同。

```
DHCPv6 客户端 DUID  . . . . . : 00-01-00-01-2C-A3-DD-5B-90-2E-16-EB-BC-09
DNS 服务器  . . . . . : 202.38.64.56
                                202.38.64.17
```

7.检查DNS查询消息。DNS查询是什么"Type"的？查询消息是否包含任何"answers"?

```
202.38.64.56    DNS    … Standard query 0x0255 A www.ietf.org
```

Wireshark · 分组 66 · dns.pcapng

```
> Frame 66: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on inter
> Ethernet II, Src: Chongqin_76:2e:23 (b4:b5:b6:76:2e:23), Dst: HuaweiTe_8a:5c
> Internet Protocol Version 4, Src: 100.64.145.245, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 60528, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0255
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

type A；没有answer。

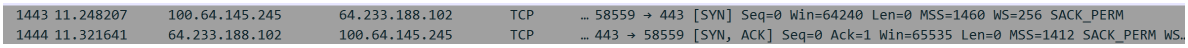
8.检查DNS响应消息。提供了多少个"answers"？这些答案具体包含什么?

2个“answer”。

```
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
> Queries
v Answers
  v www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  v www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
[Request In: 66]
[Time: 0.185090000 seconds]
```

Parameter	Description
Name	域名的名称，即 www.ietf.org
Type	记录类型。
Class	记录类别，IN是Internet即互联网中的记录。
Time to live	记录的生存时间，以秒为单位，这里是300秒（5分钟），表示这个记录在本地DNS缓存中可以保存5分钟。
Data length	数据的长度，这里是4个字节。
Address	给出ip的实际地址

9.考虑从您主机发送的后续TCP SYN数据包。 SYN数据包的目的IP地址是否与DNS响应消息中提供的任何IP地址相对应?



对应。

10.这个网页包含一些图片。在获取每个图片前，您的主机是否都发出了新的DNS查询

没有。

11.DNS查询报文的目标端口是什么? DNS响应报文的源端口是什么?

查询报文：目标端口53

```
User Datagram Protocol, Src Port: 60528, Dst Port: 53
   Source Port: 60528
   Destination Port: 53
   Length: 38
```

响应报文：源端口53

```
User Datagram Protocol, Src Port: 53, Dst Port: 60528
   Source Port: 53
   Destination Port: 60528
```

12.DNS 查询消息的目标 IP 地址是什么？这是你的默认本地 DNS 服务器的 IP 地址吗？

Source	Destination	Protocol	Le	Info
202.38.64.56	100.64.145.245	DNS	…	Standard query response 0x0001 PTR 56
100.64.145.245	202.38.64.56	DNS	…	Standard query 0x0002 A www.mit.edu

目标ip是202.38.64.56

```
DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2C-A3-DD-5B-90-2E-16-EB-BC-09
DNS 服务器  . . . . . . . . . . . : 202.38.64.56
                                    202.38.64.17
```

本地DNS服务器ip也是202.38.64.56，是一样的。

13.检查 DNS 查询消息。DNS 查询是什么 “Type” 的？查询消息是否包含任何 “answers”？

```
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 ⌄ Queries
   ⌄ www.mit.edu: type A, class IN
```

Type:A.没有answer。

14.检查DNS响应报文。提供了多少个"answers"？这些答案包含什么？

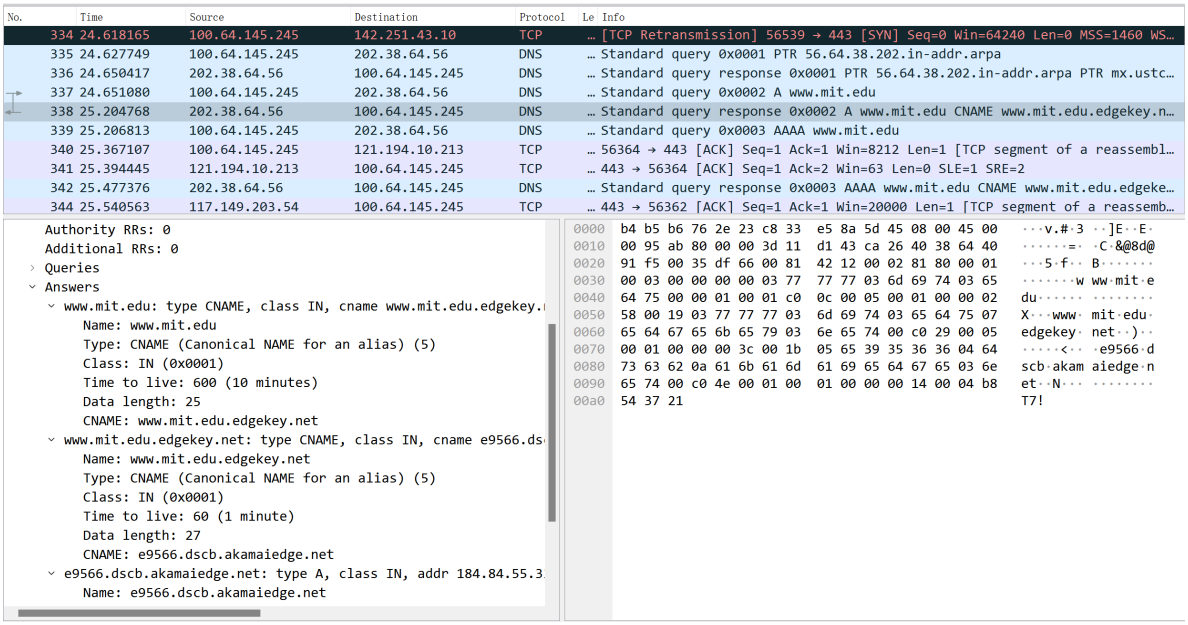
3个。

```
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: 600 (10 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: 27
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 184.84.55.33
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 184.84.55.33
```

包含了如下信息：

Parameter	Description
Name	域名
Type	记录类型。A
Class	记录类别，IN是Internet即互联网中的记录。
Time to live	记录的生存时间，以秒为单位。
Data length	数据的长度。
Address	给出ip地址
CNAME	规范名称的别名

15.提供屏幕截图。



No.	Time	Source	Destination	Protocol	Le	Info
334	24.618165	100.64.145.245	142.251.43.10	TCP	…	[TCP Retransmission] 56539 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
335	24.627749	100.64.145.245	202.38.64.56	DNS	…	Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
336	24.650417	202.38.64.56	100.64.145.245	DNS	…	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PTR mx.ustc…
337	24.651080	100.64.145.245	202.38.64.56	DNS	…	Standard query 0x0002 A www.mit.edu
338	25.204768	202.38.64.56	100.64.145.245	DNS	…	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.n…
339	25.206813	100.64.145.245	202.38.64.56	DNS	…	Standard query 0x0003 AAAA www.mit.edu
340	25.367107	100.64.145.245	121.194.10.213	TCP	…	56364 → 443 [ACK] Seq=1 Ack=1 Win=8212 Len=1 [TCP segment of a reassembl…
341	25.394445	121.194.10.213	100.64.145.245	TCP	…	443 → 56364 [ACK] Seq=1 Ack=2 Win=63 Len=0 SLE=1 SRE=2
342	25.477376	202.38.64.56	100.64.145.245	DNS	…	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgeke…
344	25.540563	117.149.203.54	100.64.145.245	TCP	…	443 → 56362 [ACK] Seq=1 Ack=1 Win=20000 Len=1 [TCP segment of a reassemb…

```
Authority RRs: 0
Additional RRs: 0
› Queries
˅ Answers
  ˅ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 600 (10 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ˅ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.ds
      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: 27
      CNAME: e9566.dscb.akamaiedge.net
  ˅ e9566.dscb.akamaiedge.net: type A, class IN, addr 184.84.55.3
      Name: e9566.dscb.akamaiedge.net
```

```
0000  b4 b5 b6 76 2e 23 c8 33  e5 8a 5d 45 08 00 45 00   ···v.#·3 ··]E··E·
0010  00 95 ab 80 00 00 3d 11  d1 43 ca 26 40 38 64 40   ·····=· ·C·&@8d@
0020  91 f5 00 35 df 66 00 81  42 12 00 02 81 80 00 01   ···5·f·· B·······
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 02   du······ ········
0050  58 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   X···www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 3c 00 1b  05 65 39 35 36 36 04 64   ·····<·· ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 03 6e   scb·akam aiedge·n
0090  65 74 00 c0 4e 00 01 00  01 00 00 00 14 00 04 b8   et··N··· ········
00a0  54 37 21                                          T7!
```

16.NS查询报文发送到的IP地址是什么？这是您的默认本地DNS服务器的IP地址吗？

89	2.574310	100.64.145.245	202.38.64.56	DNS	… Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
90	2.577402	202.38.64.56	100.64.145.245	DNS	… Standard query response 0x0001 PTR 56.64.38.202.in-ad
91	2.577964	100.64.145.245	202.38.64.56	DNS	… Standard query 0x0002 NS mit.edu
92	2.697712	202.38.64.56	100.64.145.245	DNS	… Standard query response 0x0002 NS mit.edu NS eur5.aka

发送到202.338.64.56，是我默认的DNS服务器的ip地址。

17.检查DNS查询报文。DNS查询是什么"Type"的？查询报文是否包含任何"answers"？

```
Domain Name System (query)
    Transaction ID: 0x0002
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    ˅ mit.edu: type NS, class IN
        Name: mit.edu
```

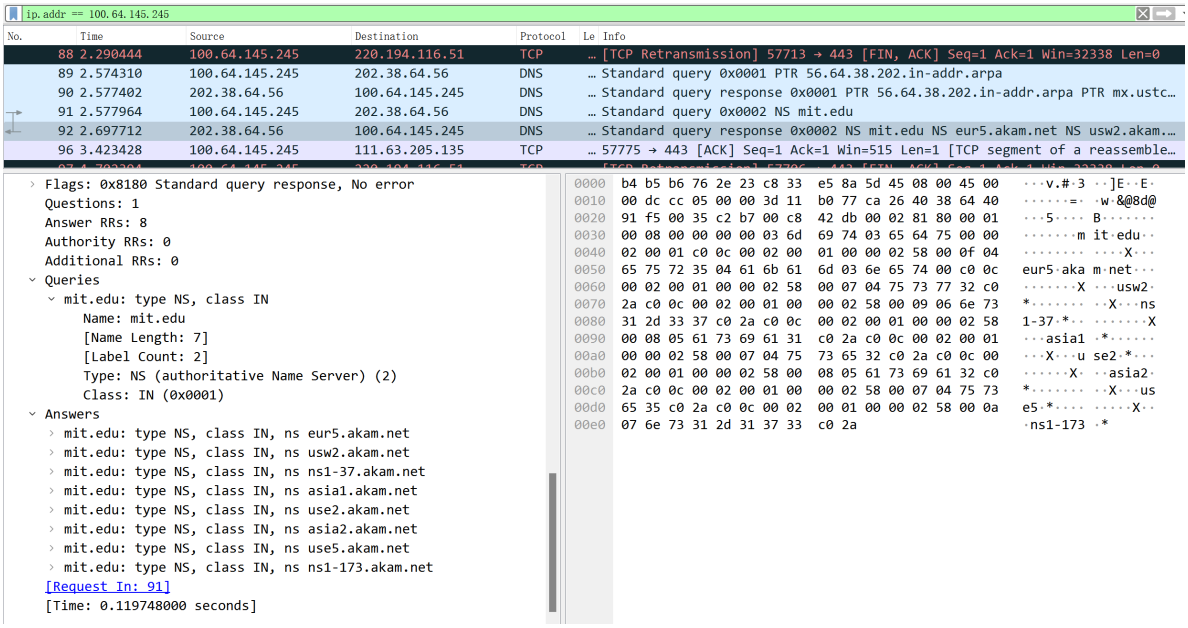
Type: NS，不包含answer。

18.检查DNS响应报文。响应报文提供的MIT域名服务器是什么？此响应报文还提供了MIT域名服务器的IP地址吗？

提供了八个域名服务器，没有ip地址。

```
˅ Answers
  › mit.edu: type NS, class IN, ns eur5.akam.net
  › 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 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 use5.akam.net
  › mit.edu: type NS, class IN, ns ns1-173.akam.net
```

19.提供屏幕截图。



20-23用nslookup www.aiit.or.kr bitsy.mit.edu超时换成了Google的DNS

20.DNS查询报文发送到的IP地址是什么？这是您的默认本地DNS服务器的IP地址吗？如果不是，这个IP地址是什么？

7	2.101381	100.64.145.245	8.8.8.8	DNS	… Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
8	2.163373	8.8.8.8	100.64.145.245	DNS	… Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
9	2.164229	100.64.145.245	8.8.8.8	DNS	… Standard query 0x0002 A www.aiit.or.kr
10	2.227216	8.8.8.8	100.64.145.245	DNS	… Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
11	2.229661	100.64.145.245	8.8.8.8	DNS	… Standard query 0x0003 AAAA www.aiit.or.kr
12	2.292437	8.8.8.8	100.64.145.245	DNS	… Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

发送到了8.8.8.8，不是默认本地DNS服务器的IP地址，它是我设置的GoogleDNS

21.检查DNS查询报文。DNS查询是什么"Type"的？查询消息是否包含任何"answers"？

Type：A和AAAA

A：

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

AAAA：

```
Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

22.检查DNS响应报文。提供了多少个"answers"？这些答案包含什么?

1个。

```
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
  > Queries
  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: 3193 (53 minutes, 13 seconds)
        Data length: 4
        Address: 58.229.6.225
    [Request In: 9]
```

Parameter	Description
Name	域名
Type	记录类型。A
Class	记录类别，IN是Internet即互联网中的记录。
Time to live	记录的生存时间，以秒为单位。
Data length	数据的长度。
Address	给出ip地址

23.提供屏幕截图