计网实验3

nslookup

T1

> 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？

```
C:\Users\Nutrition>nslookup www.bilibili.com
服务器:  UnKnown
Address:  192.168.147.197

非权威应答:
名称:    a.w.bilicdn1.com
Addresses:  240e:f7:e01f:f1::28
          240e:cf:9000:2::9a
          240e:f7:e01f:f1::30
          240e:cf:9000:2::99
          240e:cf:9000:2::9d
          240e:f7:e01f:f1::31
          240e:f7:e01f:f1::27
          240e:f7:e01f:f1::29
          175.4.62.128
          117.21.179.19
          175.4.62.127
          114.230.222.140
          117.21.179.18
          114.230.222.141
          117.21.179.20
          114.230.222.138
          114.230.222.139
          183.131.147.28
          183.131.147.30
          183.131.147.48
          175.4.62.129
          183.131.147.29
          183.131.147.27
          114.230.222.142
Aliases:  www.bilibili.com
```

183.131.147.29

114.230.222.142

.....

T2

> 运行nslookup来确定一个欧洲的大学的权威DNS服务器

```
C:\Users\Nutrition>nslookup -type=NS cam.ac.uk
服务器:  UnKnown
Address:  192.168.147.197

非权威应答:
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
cam.ac.uk       nameserver = ns1.mythic-beasts.com
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = ns3.mythic-beasts.com
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
```

T3

> 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？

```
C:\Users\Nutrition>nslookup mail.yahoo.com dns0.eng.cam.ac.uk
服务器:  dns0.eng.cam.ac.uk
Address:  129.169.8.8

*** dns0.eng.cam.ac.uk 找不到 mail.yahoo.com: Query refused
```

似乎查不到，换了几个也查不到

但是查到谷歌了

```
C:\Users\Nutrition>nslookup google.com dns0.eng.cam.ac.uk
服务器:  dns0.eng.cam.ac.uk
Address:  129.169.8.8

名称:    google.com
Addresses:  46.82.174.69
          59.24.3.174
```

ipconfig

Tracing DNS with Wireshark

T4

> 找到DNS查询和响应报文，它们是通过UDP还是TCP发送？

`User Datagram Protocol`

UDP

T5

> 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？

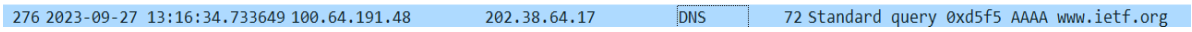
`Destination Port: 53`

`Source Port: 53`

53，53

T6

> 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202.38.64.17

使用ipconfig查询本地DNS服务器ip地址：

是一个ip地址

T7

> 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: 0x2620
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    > www.ietf.org: type A, class IN
```

Type A；不包含

T8

> 检查DNS响应报文。提供了多少个"**answers**"？这些答案具体包含什么？

```
Domain Name System (response)
    Transaction ID: 0x863d
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    > www.ietf.org: type A, class IN, addr 104.16.45.99
    > www.ietf.org: type A, class IN, addr 104.16.44.99
    [Request In: 274]
    [Time: 0.004330000 seconds]
```

两个answer

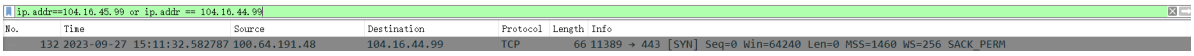
具体内容如图：

```
▾ 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: 225 (3 minutes, 45 seconds)
    Data length: 4
    Address: 104.16.45.99
▾ 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: 225 (3 minutes, 45 seconds)
    Data length: 4
    Address: 104.16.44.99
```

有域名、类型、类别、时长、数据长度、别名

T9

> 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，都是104.16.44.99

T10

> 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

play with nsloopup

T11

> 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？

```
Destination Port: 53
```

```
Source Port: 53
```

53，53

T12

> DNS查询报文的目标IP地址是什么？这是你的默认本地DNS服务器的IP地址吗？

```
206 2023-09-27 13:43:42.934719 100.64.191.48    202.38.64.56    DNS    71 Standard query 0x0002 A www.mit.edu
```

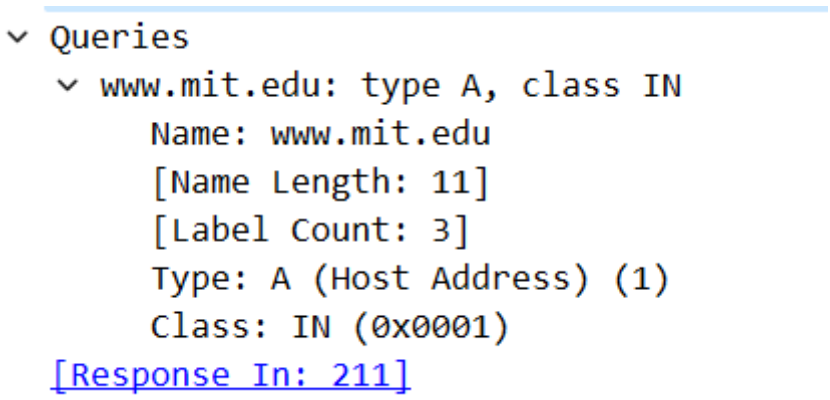
目标ip地址是202.38.64.56

```
DNS 服务器  . . . . . . . . . . . . : 202.38.64.56
                                      202.38.64.17
```

是默认本地DNS服务器的ip地址

T13

> 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

不包含answer

T14

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

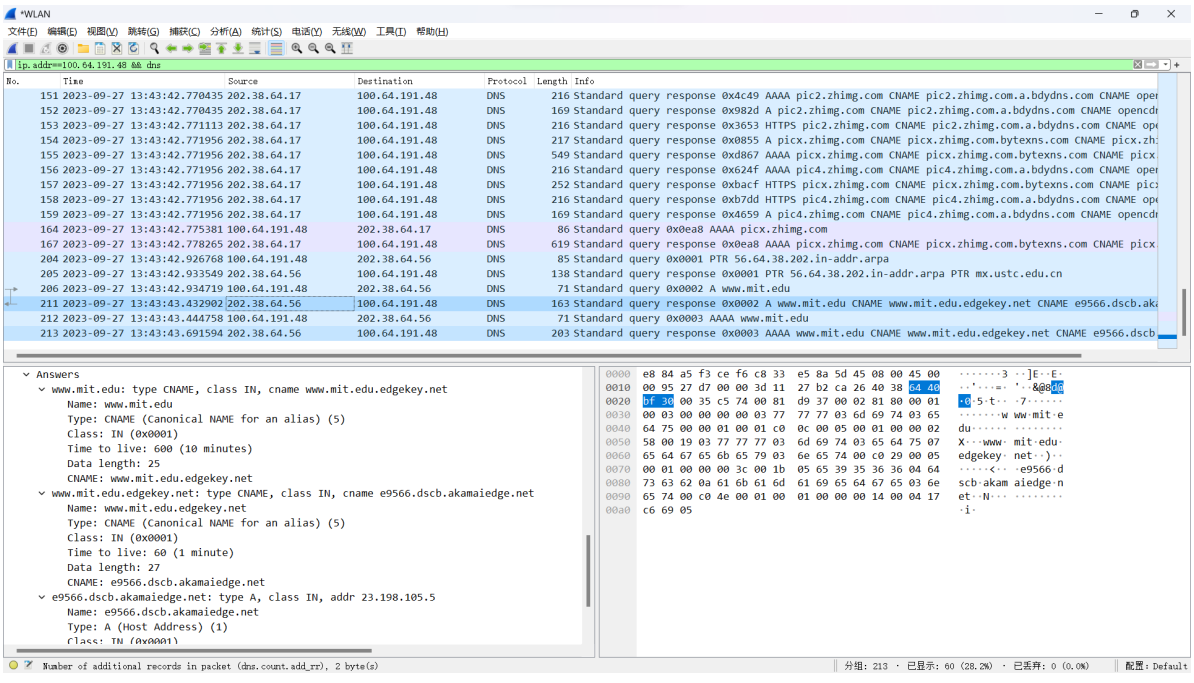
```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 600 (10 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: 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 23.198.105.5
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

三个answer

包含的内容如上图所示，有域名、类型、类别、时长、数据长度、别名

T15

> 提供屏幕截图



Repeat

```
nslookup –type=NS mit.edu
```

T16

> 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？

```
6 2023-09-27 13:55:55.041442 100.64.191.48      202.38.64.56        DNS        67 Standard query 0x0002 NS mit.edu
```

202.38.64.56

```
DNS 服务器  . . . . . . . . . . . . : 202.38.64.56
                                      202.38.64.17
```

是

T17

> 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**"？

```
▾ Queries
  ▾ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

type NS

不包含answer

T18

> 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？

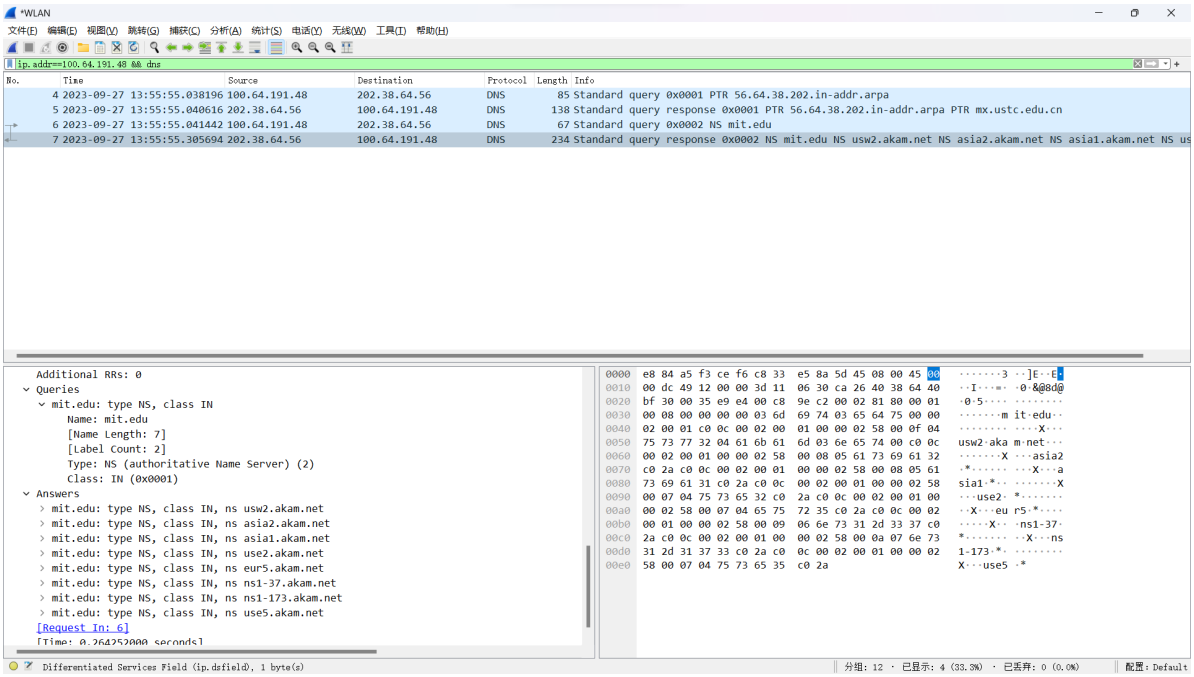
提供如下域名服务器：

```
▾ Answers
  › mit.edu: type NS, class IN, ns usw2.akam.net
  › mit.edu: type NS, class IN, ns asia2.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 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 use5.akam.net
  [Request In: 6]
```

不提供ip地址

T19

> 提供屏幕截图



Repeat

```
1 nslookup mit.edu use2.akam.net
```

T20

> 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？

```
11 2023-09-27 14:02:19.365745 100.64.191.48 96.7.49.64 DNS 67 Standard query 0x0002 A mit.edu
```

96.7.49.64

不是，这是use2.akam.net这个域名服务器的IP地址

T21

> 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**"？

```
Queries
  mit.edu: type A, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

type A

不包含answer

T22

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

```
Answers
  mit.edu: type A, class IN, addr 104.91.11.174
      Name: mit.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 104.91.11.174
  [Request In: 11]
```

提供了一个answer

包含域名、类型、类别、时长、数据长度、ip

T23

提供屏幕截图