DNS 实验

陈鸿绪　PB21000224　10.3

1. 运行 nslookup 获取任意一个亚洲 Web 服务器的 IP 地址。该服务器的 IP 地址是什么？

```
C:\Users\86181>nslookup baidu.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    baidu.com
Addresses:  39.156.66.10
          110.242.68.66
```

2. 运行 nslookup 以确定欧洲一所大学的权威 DNS 服务器。

```
C:\Users\86181>nslookup -type=NS ethz.ch
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
ethz.ch nameserver = ns2.ethz.ch
ethz.ch nameserver = ns1.ethz.ch
```

这里我们选取的欧洲大学是苏黎世联邦理工。

3. 运行 nslookup，以便查询在问题 2 中获得的其中一个 DNS 服务器，以获取 Yahoo！邮件的邮件服务器。它的 IP 地址是什么？

由于在 2 中我们获得的权威 DNS 服务器无法解析 Yahoo，这里选取 google.com:

```
C:\Users\86181>nslookup google.com ns1.ethz.ch
服务器:  ns1.ethz.ch
Address:  2001:67c:10ec::a

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

4. 找到 DNS 查询和响应消息。它们是通过 UDP 还是 TCP 发送的？

Source	Destination	Protocol	Length	Info
100.64.130.89	202.38.64.17	DNS	72	Standard query 0x8a3e AAAA www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0xad0b A www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0xcc9f HTTPS www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0xd4d7 AAAA www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0x29c0 A www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0x5325 AAAA www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0x3972 A www.ietf.org
100.64.130.89	202.38.64.17	DNS	72	Standard query 0xecfd HTTPS www.ietf.org
100.64.130.89	202.38.64.17	DNS	75	Standard query 0x87f4 AAAA static.ietf.org
100.64.130.89	202.38.64.17	DNS	75	Standard query 0xea6b A static.ietf.org

Protocol: UDP (17)

均经过 UDP 发送的。

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: 59465, Dst Port: 53
    Source Port: 59465
    Destination Port: 53
```

```
User Datagram Protocol, Src Port: 59964, Dst Port: 53
    Source Port: 59964
    Destination Port: 53
```

```
User Datagram Protocol, Src Port: 49848, Dst Port: 53
    Source Port: 49848
    Destination Port: 53
```

以上是一部分 DNS 的查询消息的端口展示，目标端口均为 53。

```
User Datagram Protocol, Src Port: 53, Dst Port: 62618
    Source Port: 53
    Destination Port: 62618
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 60740
    Source Port: 53
    Destination Port: 60740
```

以上是一部分 DNS 的相应消息的端口展示，相应端口均为 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？

使用 ipconfig -all 指令：

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

在题四中可以发现 DNS 查询消息发送到了 202.38.64.17，所以与上图中下方的 IP 地址相同。

7. 检查 DNS 查询消息。它是什么“类型”的 DNS 查询？查询消息是否包含任何“answers”？

```
▾ Queries
  ▾ www.ietf.org: type AAAA, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
  [Response In: 25]
```

Type=AAAA 查询消息不包含任何形式的“answers”。

8. 检查 DNS 响应消息。提供了多少个“answers”？每个 answers 包含什么内容？

提供了两个答案：

```
▾ Answers
  › www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2d63
  › www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2c63
```

其中一个答案包含了如下内容：

```
▾ www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2d63
    Name: www.ietf.org
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 16
    AAAA Address: 2606:4700::6810:2d63
```

9. 考虑您的主机发送的后续 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？

后续 SYN 数据包的目标 IP 地址一定在 DNS 响应消息中提供的 IP 中。只不过由于 IPv4 与 IPv6 的原因不能直观显示出来。

10. 此网页包含图像。在检索每个图像之前，您的主机会发出新的 DNS 查询吗？

不会，浏览器会缓存之前解析过域名的 IP 地址，IP 地址一般不会变动。

以下是使用 nslookup www.mit.edu 命令的实验：

11. 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？

下面是 DNS 查询，目标端口为 53

```
Source Port: 55829
Destination Port: 53
```

下面是 DNS 响应，源端口为 53

```
Source Port: 53
Destination Port: 55829
```

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

```
100.64.130.89    202.38.64.56                    DNS          71 Standard query 0x0003 AAAA www.mit.edu
202.38.64.56     100.64.130.89                   DNS         203 Standard query response 0x0003 AAAA www.m
```

发送到了 202.38.64.56 地址。是本地 DNS 服务器 IP 地址。

13. 检查 DNS 查询消息。它是什么“类型”的 DNS 查询？查询消息是否包含任何“Answers”？

```
▾ Queries
  ▾ www.mit.edu: type AAAA, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
```

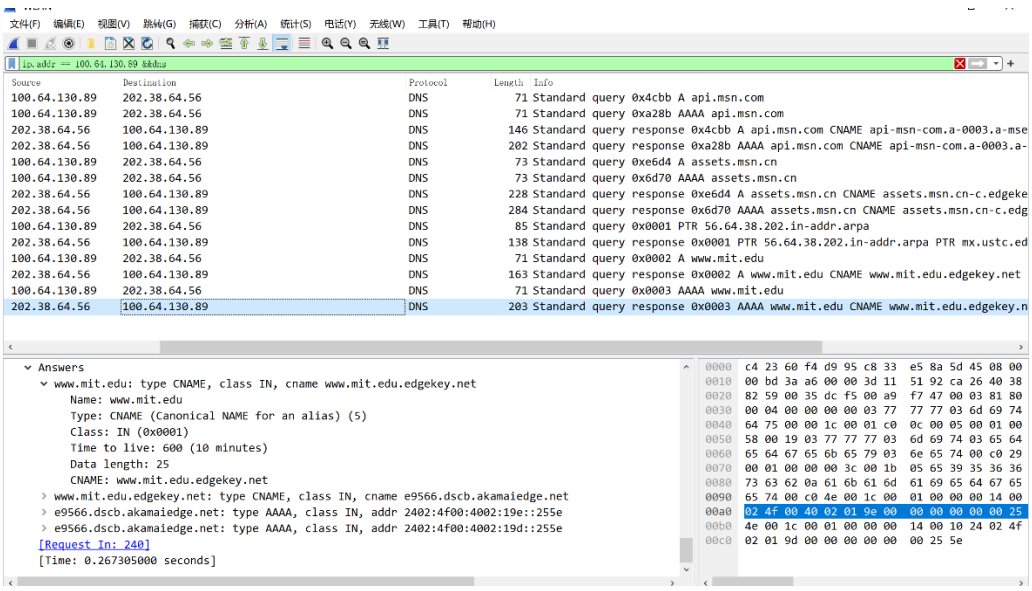
Type: AAAA　不包含任何 Answers 。

14. 检查 DNS 响应消息。提供了多少个“Answers”？Answer 包含什么内容？

提供了四个，其中一个 Answer 中的具体内容如下展示。

```
▾ 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
  › e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2402:4f00:4002:19e::255e
  › e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2402:4f00:4002:19d::255e
```

15. 提供一张屏幕截图



以下是使用 nslookup -type=NS mit.edu 命令的实验：

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

发送到了 202.38.64.56 地址。是本地 DNS 服务器 IP 地址。

17. 检查 DNS 查询消息。它是什么“类型”的 DNS 查询？查询消息是否包含任何“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)
    [Response In: 19]
```

Type:NS 不包含任何 Answers

18. 检查 DNS 响应消息。响应消息提供了哪些 MIT 名称服务器？该响应消息是否还提供了 MIT 名称服务器的 IP 地址？

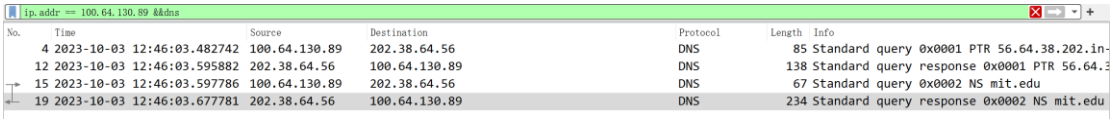
以下是提供的一些 MIT 服务器：

```
▾ Answers
  › mit.edu: type NS, class IN, ns asia1.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 asia2.akam.net
  › mit.edu: type NS, class IN, ns use5.akam.net
  › mit.edu: type NS, class IN, ns ns1-173.akam.net
  › mit.edu: type NS, class IN, ns usw2.akam.net
  › mit.edu: type NS, class IN, ns use2.akam.net
  [Request In: 15]
  [Time: 0.079995000 seconds]
```

展开其中一个发现并没有提供 IP 地址：

```
▾ mit.edu: type NS, class IN, ns asia1.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 17 (17 seconds)
    Data length: 16
    Name Server: asia1.akam.net
```

19. 提供一张屏幕截图。

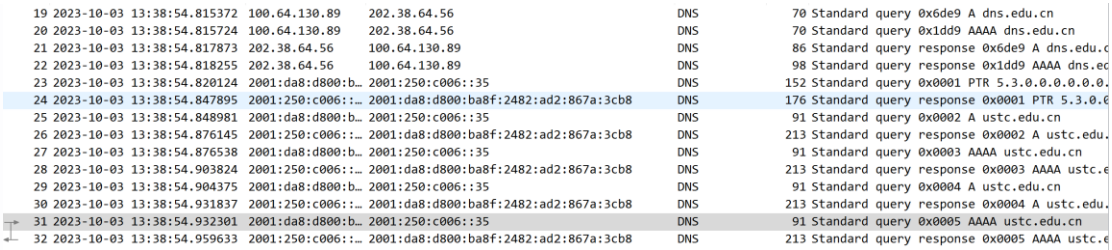


以下是使用 nslookup ustc.edu.cn dns.edu.cn 的命令实验

20. DNS 查询消息发送到哪个 IP 地址？这是您默认本地 DNS 服务器的 IP 地址吗？如果不是，该 IP 地址对应的是什么？

其中有一些发送到了 202.38.64.56 地址。是本地 DNS 服务器 IP 地址。

但是有些并不是上述 IP 地址，该 IPv6 地址对应的应该为 dns.edu.cn。



21. 检查 DNS 查询消息。它是什么“类型”的 DNS 查询？查询消息是否包含任何“Answers”？

这是选取的三个代表性 DNS 查询，一个 type 为 A，一个 type 为 AAAA，还有一个为 PTR，均不包含任何 Answers。

```
Queries
  dns.edu.cn: type A, class IN
      Name: dns.edu.cn
      [Name Length: 10]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 7]
```

```
Queries
  dns.edu.cn: type AAAA, class IN
      Name: dns.edu.cn
      [Name Length: 10]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
  [Response In: 8]
```

```
Queries
  5.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.c.0.5.2.0.
      Name: 5.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.c.
      [Name Length: 72]
      [Label Count: 34]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
```

22. 检查 DNS 响应消息。提供了多少个“Answers”？每个 Answer 包含什么内容？

有的 DNS 响应有 1 个 answer。

```
Answers
  > dns.edu.cn: type A, class IN, addr 202.38.109.35
[Request In: 5]
[Time: 0.002708000 seconds]
```

```
Answers
  > dns.edu.cn: type AAAA, class IN, addr 2001:250:c006::35
[Request In: 6]
```

```
Answers
  > 5.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.c.0.5.2.0.1.0.0.2.ip6.arpa: type PTR, class IN,
[Request In: 23]
[Time: 0.027771000 seconds]
```

三个均每个提供一个答案，答案包含类似以下内容：

```
dns.edu.cn: type A, class IN, addr 202.38.109.35
    Name: dns.edu.cn
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 443 (7 minutes, 23 seconds)
    Data length: 4
    Address: 202.38.109.35
```

但是有的 DNS 响应报文中就并没有 Answers，如下图所示：

```
Domain Name System (response)
    Transaction ID: 0x0005
  > Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 2
    Additional RRs: 4
  > Queries
  > Authoritative nameservers
  > Additional records
    [Request In: 31]
    [Time: 0.027332000 seconds]
```

并没有发现 Answers 的存在。

23. 提供一张屏幕截图。