华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程	**年级：**2021 级	**上机实践成绩：**
指导教师：张召	**姓名：**彭一珅	**学号：**10215501412
上机实践名称：DNS 报文分析		**上机实践日期：**2023.5.12
上机实践编号：10	**组号：**	**上机实践时间：**9:50

一、 **实验目的**

了解系统命令 nslookup 的用法

学习 DNS 协议并掌握 DNS 的工作原理

二、 **实验任务**

nslookup 命令的简单使用

使用 Wireshark 分析 DNS 协议

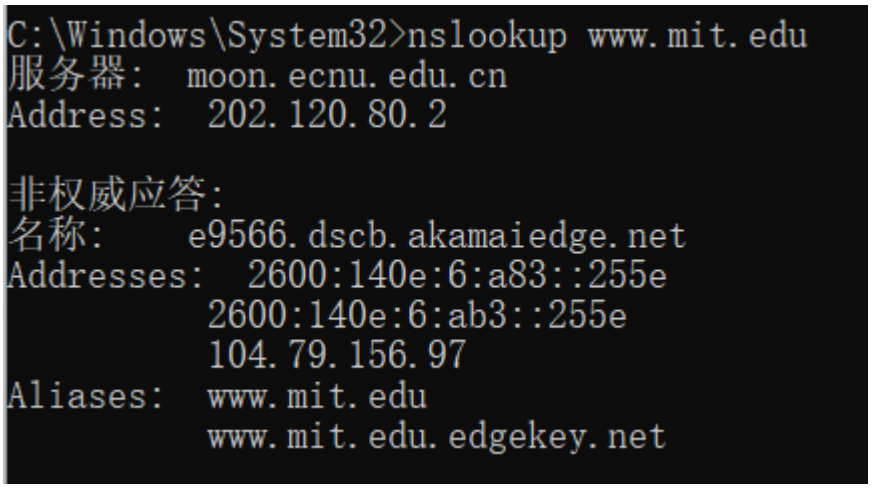
三、 **使用环境**

Wireshark 抓包程序

Windows11

四、 **实验过程**

Task1 运行 nslookup 来确定一个国外大学 (www.mit.edu) 的 IP 地址以及其权威 DNS 服务器，请在实验报告中附上操作截图并详细分析返回信息内容。



这个命令是说，请告诉我 www.mit.edu 的 IP 地址。此命令的响应包含两条信息。1. 提供响应的 DNS 服务器是 moon.ecnu.edu.cn，也就是校园网的服务器，IP 地址是 202.120.80.2。2. 响应本身，即 www.mit.edu 服务器的主机名和 IP 地址，以及别名。因此查询到的 IP 地址是 104.79.156.97。

```
C:\Windows\System32>nslookup -type=NS www.mit.edu
服务器:  moon.ecnu.edu.cn
Address:  202.120.80.2

非权威应答:
www.mit.edu     canonical name = www.mit.edu.edgekey.net
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net

dscb.akamaiedge.net
        primary name server = n0dscb.akamaiedge.net
        responsible mail addr = hostmaster.akamai.com
        serial  = 1683857986
        refresh = 1000 (16 mins 40 secs)
        retry   = 1000 (16 mins 40 secs)
        expire  = 1000 (16 mins 40 secs)
        default TTL = 1800 (30 mins)
```

在查询时加上 NS 选项，可以得到主机 www.mit.edu 的规范名是 www.mit.edu.edgekey.net，而这个主机的规范名是 e9566.dscb.akamaiedge.net，该规范名的 DNS 服务器是 dscb.akamaiedge.net。该服务器还返回了面向服务的一系列数据：权威主机名为 n0dscb.akamaiedge.net，邮箱地址，序列号（机器码），刷新时间，重试时间，该记录的失效时间，默认生存时间值。对该主机名再次查询：

```
C:\Windows\System32>nslookup -type=NS dscb.akamaiedge.net
服务器:  moon.ecnu.edu.cn
Address:  202.120.80.2

非权威应答:
dscb.akamaiedge.net     nameserver = n3dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n6dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n2dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n4dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n0dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n7dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n1dscb.akamaiedge.net
dscb.akamaiedge.net     nameserver = n5dscb.akamaiedge.net
```

可以得到权威服务器的 nameserver 是 n0dscb.akamaiedge.net。非权威应答表示从这些服务器的缓存里得到了应答。

Task2 运行 nslookup ，使用 task1 中一个已获得的 DNS 服务器，来查询 google 服务器 (www.google.com)的 IP 地址(可直接查询)，请在实验报告中附上操作截图并详细分析返回信息内容。

```
C:\Windows\System32>nslookup www.google.com n0dscb.akamaiedge.net
服务器:  UnKnown
Address:  88.221.81.192

非权威应答:
名称:    www.google.com
Addresses:  2a03:2880:f10c:83:face:b00c:0:25de
          174.36.196.242
```

向 task1 中获得的权威主机名查询 www.google.com，得到 IP 地址为 174.36.196.242

Task3 根据 Wireshark 抓取的报文信息（例，下图所示示例），分别分析 DNS 查询报文和响应报文的组成结构，参考上面的报文格式指出报文的每个部分（如，头部区域等），请将实验结果附在实验报告中。

发送 nslookup www.baidu.com 查询，得到以下 dns 数据包：

dns

No.	Time	Source	Destination	Protocol	Length	Info
126	16.099516	172.30.144.220	202.120.80.2	DNS	85	Standard query 0x0001 PTR 2.80.120.202.in-addr.arpa
127	16.102796	202.120.80.2	172.30.144.220	DNS	115	Standard query response 0x0001 PTR 2.80.120.202.in-addr.arpa PTR moon.ecnu.edu.cn
128	16.104964	172.30.144.220	202.120.80.2	DNS	73	Standard query 0x0002 A www.baidu.com
129	16.107385	202.120.80.2	172.30.144.220	DNS	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 182.61.200.7 A 182.61.200.6
130	16.111177	172.30.144.220	202.120.80.2	DNS	73	Standard query 0x0003 AAAA www.baidu.com
131	16.115342	202.120.80.2	172.30.144.220	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com

查看第二条查询报文：

```
> Frame 128: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: IntelCor_2d:c7:9c (44:e5:17:2d:c7:9c), Dst: NewH3C
> Internet Protocol Version 4, Src: 172.30.144.220, Dst: 202.120.80.2
> User Datagram Protocol, Src Port: 57680, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.baidu.com: type A, class IN
    [Response In: 129]
```

首先，报文首部包含了 Transaction ID，对于请求报文和对应的应答报文，该字段相同，通过这个字段可以区分 DNS 应答报文是对哪个请求进行响应的。

Flags 字段包含 16 个位，每组位有自己的含义。第一位标志信息为 0 表示这是查询请求

（响应请求为 1）。

随后四位的操作码为 0 表示标准查询。

TC（Truncated）为 0 表示未被截断，未超过 512 字节。

RD（Recursion Desired）为 1 告诉服务器必须处理这个查询，这种方式被称为递归查询，如果该位为 0，且被请求的名称服务器没有一个授权回答，它将返回一个能解答该查询的其他名称服务器列表。这种方式被称为迭代查询。

Z 是保留字段，在所有的请求和应答报文中，它的值必须为 0。

然后是一行 Queries 查询部分。

Non-authenticated data 也是保留字段，值为 0。

问题计数 Questions 表示查询了一个问题。而由于这是一个查询报文，回答资源记录数为 0，权威名称服务器数目为 0，附加资源数目也为 0。

查看对应的响应请求包：

```
> Internet Protocol Version 4, Src: 202.120.80.2, Dst: 172.30.144.220
> User Datagram Protocol, Src Port: 53, Dst Port: 57680
v Domain Name System (response)
    Transaction ID: 0x0002
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.baidu.com: type A, class IN
  > Answers
    [Request In: 128]
    [Time: 0.002421000 seconds]
```

Transaction ID 与请求包相同，Flags 标志字段中包含以下含义：

第一位标志信息为 1 表示这是响应包。

随后四位操作码表示这是标准查询。

Authoritative 为 0 表示这不是权威服务器。

Truncated 为 0 表示未被截断。

Recursion desired 字段为 1 表示递归查询.

Recursion available 只出现在响应报文中，当值为 1 时，表示服务器支持递归查询。

AA（Authoritative）表示授权应答，该字段只在响应报文中有效。值为 1 时，表示名称服务器是权威服务器；值为 0 时，表示不是权威服务器。

Reply code 也只出现在响应报文中，表示响应的差错状态。当值为 0 时，表示没有错误；当值为 1 时，表示报文格式错误（Format error），服务器不能理解请求的报文；当值为 2 时，表示域名服务器失败（Server failure），因为服务器的原因导致没办法处理这个请求；当值为 3 时，表示名字错误（Name Error），只有对授权域名

解析服务器有意义，指出解析的域名不存在；当值为 4 时，表示查询类型不支持（Not Implemented），即域名服务器不支持查询类型；当值为 5 时，表示拒绝（Refused），一般是服务器由于设置的策略拒绝给出应答，如服务器不希望对某些请求者给出应答。

Questions 表示查询一个问题。Answer RRs 表示获取了 3 条回答。

Task4 基于 task3 中得到的查询和响应报文进行分析，试问这里的查询是什么“Type”的，查询消息是否包含任何“answers”？试问这里的响应消息提供了多少个“answers”，这些“answers”具体包含什么？请将实验结果附在实验报告中。

```
Answers
    www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
        Name: www.baidu.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1895 (31 minutes, 35 seconds)
        Data length: 15
        CNAME: www.a.shifen.com
    www.a.shifen.com: type A, class IN, addr 182.61.200.7
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1895 (31 minutes, 35 seconds)
        Data length: 4
        Address: 182.61.200.7
    www.a.shifen.com: type A, class IN, addr 182.61.200.6
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1895 (31 minutes, 35 seconds)
        Data length: 4
        Address: 182.61.200.6
```

响应消息提供了 3 个 answer，有两个 A 类型，一个规范主机名 CNAME 类型，包含了 IP 地址，主机名，生存时间，数据长度等内容。

```
▾ Queries
  ▾ www.baidu.com: type A, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 203]
```

查询是 A 类型的，查询消息不包含 answer。

五、总结

本次实验的目的是学习 nslookup 命令的用法和 DNS 协议的工作原理。在实验中，我学习了如何使用 nslookup 命令来确定一个国外大学的 IP 地址以及其权威 DNS 服务器，并使用已获得的 DNS 服务器来查询 google 服务器的 IP 地址。同时，我使用 Wireshark 抓包程序分析了 DNS 协议的组成结构，包括 DNS 查询报文和响应报文的头部区域、问题区域、回答区域、授权区域和附加区域等部分。

通过本次实验，我深入了解了 nslookup 命令和 DNS 协议的工作原理，掌握了基本的使用方法和分析技巧。这对我今后的计算机网络课程的学习具有重要的收获。