

个人信息

姓名：付文轩

学号：1911410

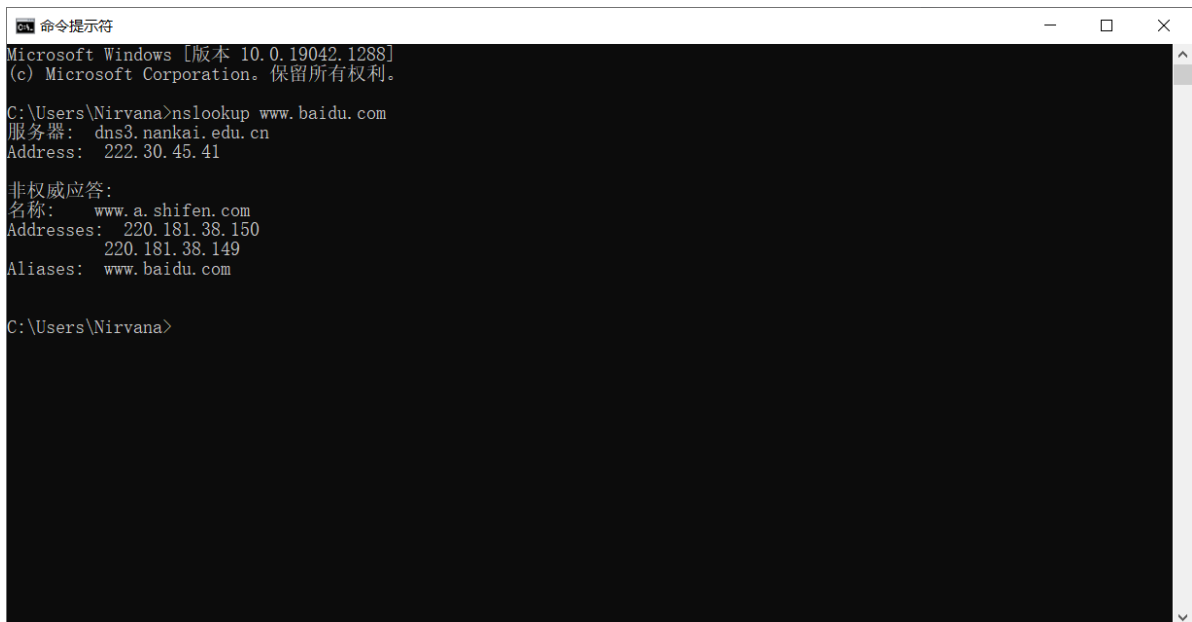
专业：信息安全

学院：网络空间安全学院

作业1.1

nslookup

nslookup运行结果如下



```
命令提示符
Microsoft Windows [版本 10.0.19042.1288]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Nirvana>nslookup www.baidu.com
服务器:  dns3.nankai.edu.cn
Address:  222.30.45.41

非权威应答:
名称:     www.a.shifen.com
Addresses: 220.181.38.150
          220.181.38.149
Aliases:  www.baidu.com

C:\Users\Nirvana>
```

输出结果解释：

- 服务器：dns3.nankai.edu.cn

Address: 220.30.45.41

该内容表示本次查询的DNS服务器和对应的地址，这个地方是可以自己指定的，也可以默认，并且在默认情况下，DNS服务器的端口是53

- 非权威应答

这句话表示反馈的结果不是来自于Baidu的DNS服务器，而是来自于其他服务器的缓存

- name: www.a.shifen.com

根据网上查询到的信息来看，这个URL是百度原本的域名，百度在以前就叫十分网，那么在这里其实可以相当于是baidu的本名

- Addresses: 220.181.38.150

220.181.38.149

此内容就是解析出来的对应www.baidu.com的IP地址

- Aliases: www.baidu.com

这一项就是表示别名

WireShark

在wireshark中捕捉到的数据包经过过滤以后大致如下：

No.	Time	Source	Destination	Protocol	Length	Info
99	9.924118	10.130.88.135	222.30.45.41	DNS	77	Standard query 0x5548 A s-ring.msedge.net
100	9.924346	10.130.88.135	222.30.45.41	DNS	77	Standard query 0xca9f AAAA s-ring.msedge.net
101	9.941169	222.30.45.41	10.130.88.135	DNS	144	Standard query response 0x5548 A s-ring.msedge.net CNAME s-ring.s-9999.s-msedge.net CNAME s-9999.s-msedge.net
102	9.941169	222.30.45.41	10.130.88.135	DNS	188	Standard query response 0xca9f AAAA s-ring.msedge.net CNAME s-ring.s-9999.s-msedge.net CNAME s-9999.s-msedge.net
165	14.954746	10.130.88.135	222.30.45.41	DNS	85	Standard query 0x0001 PTR 41.45.30.222.in-addr.arpa
166	14.957253	222.30.45.41	10.130.88.135	DNS	117	Standard query response 0x0001 PTR 41.45.30.222.in-addr.arpa PTR dns3.nankai.edu.cn
167	14.960734	10.130.88.135	222.30.45.41	DNS	73	Standard query 0x0002 A www.baidu.com
168	14.963812	222.30.45.41	10.130.88.135	DNS	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 220.181.38.149 A 220.181.38.150
169	14.966914	10.130.88.135	222.30.45.41	DNS	73	Standard query 0x0003 AAAA www.baidu.com
170	14.969313	222.30.45.41	10.130.88.135	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com

图中的IP：220.30.45.41是学校的本地DNS服务器；10.130.88.135是我自己的电脑的IP

序号为99和100的包，发起的是DNS请求，发起方为本机，目标IP是学校的DNS服务器，内容如下：

```
▼ Ethernet II, Src: IntelCor_a4:27:16 (90:78:41:a4:27:16), Dst: IETF-VRRP-VRID_0d (00:00:5e:00:01:0d)
  ▼ Destination: IETF-VRRP-VRID_0d (00:00:5e:00:01:0d)
    Address: IETF-VRRP-VRID_0d (00:00:5e:00:01:0d)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: IntelCor_a4:27:16 (90:78:41:a4:27:16)
    Address: IntelCor_a4:27:16 (90:78:41:a4:27:16)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

首先在链路层可以看到最下面有个Type，也就是表示这次的请求是使用的IPv4

```
▼ Internet Protocol Version 4, Src: 10.130.88.135, Dst: 222.30.45.41
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0x71b2 (29106)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.130.88.135
    Destination Address: 222.30.45.41
```

之后在网络层可以看到Source和Destination

```
▼ Domain Name System (query)
  Transaction ID: 0x5548
  ▼ 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
  ▼ Queries
    ▼ s-ring.msedge.net: type A, class IN
      Name: s-ring.msedge.net
      [Name Length: 17]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

而在DNS这一层中，我们可以看到Flags设置为了标准请求，其中有一位置1表示本次的解析使用递归解析的方式；并且在下面可以注意到有Type A，这里稍后和第二个包进行对比

序号为100的包其他基本和99是一样的，只有一个地方不同

```
▼ Queries
  ▼ s-ring.msedge.net: type AAAA, class IN
    Name: s-ring.msedge.net
    [Name Length: 17]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
```

可以看见这里的Type是AAAA，和之前经过对比以后可以发现这里的Type应该就是表示我们是使用IPv4还是IPv6进行解析。

之后的101和102就是DNS对本机的回应（从IPv4和IPv6两种方式）

序号165-170就是具体的查询内容

165	14.954746	10.130.88.135	222.30.45.41	DNS	85	Standard query 0x0001 PTR 41.45.30.222.in-addr.arpa
166	14.957253	222.30.45.41	10.130.88.135	DNS	117	Standard query response 0x0001 PTR 41.45.30.222.in-addr.arpa PTR dns3.nankai.edu.cn
167	14.960734	10.130.88.135	222.30.45.41	DNS	73	Standard query 0x0002 A www.baidu.com
168	14.963812	222.30.45.41	10.130.88.135	DNS	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 220.181.38.149 A 220.181.38.150
169	14.966914	10.130.88.135	222.30.45.41	DNS	73	Standard query 0x0003 AAAA www.baidu.com
170	14.969313	222.30.45.41	10.130.88.135	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com

在DNS之前的基本和前面差不多，这里主要说明一下查询部分的内容（165号报文）

```
▼ Queries
  ▼ 41.45.30.222.in-addr.arpa: type PTR, class IN
    Name: 41.45.30.222.in-addr.arpa
    [Name Length: 25]
    [Label Count: 6]
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
```

其中in-addr.arpa表示这里需要逆向解析IP，那么他前面的41.45.30.222其实就是222.30.45.41

之后的166号报文则是对165号的回复

```
▼ Answers
  ▼ 41.45.30.222.in-addr.arpa: type PTR, class IN, dns3.nankai.edu.cn
    Name: 41.45.30.222.in-addr.arpa
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
    Time to live: 3051 (50 minutes, 51 seconds)
    Data length: 20
    Domain Name: dns3.nankai.edu.cn
```

发现在回复中出现了Time to live，也就是生存期，并且给出了本地DNS服务器的主机名称

167号报文则是本机向DNS服务器发出了baidu.com的相关请求

```

    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)

```

168号报文则是DNS服务器给本机反馈，告诉主机请求的地址

```

    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: 203 (3 minutes, 23 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
    www.a.shifen.com: type A, class IN, addr 220.181.38.149
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 211 (3 minutes, 31 seconds)
      Data length: 4
      Address: 220.181.38.149
    www.a.shifen.com: type A, class IN, addr 220.181.38.150
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 211 (3 minutes, 31 seconds)
      Data length: 4
      Address: 220.181.38.150

```

从返回的内容里来看，告诉了主机百度是有别名的，并且返回了别名的两个IP地址（其实也就是baidu的地址）

最后两条内容（169和170）则是IPv6版本的请求和回复

169	14.966914	10.130.88.135	222.30.45.41	DNS	73 Standard query 0x0003 AAAA www.baidu.com
170	14.969313	222.30.45.41	10.130.88.135	DNS	157 Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com

```

    Queries
    www.baidu.com: type AAAA, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)

```

▼ 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: 203 (3 minutes, 23 seconds)
 - Data length: 15
 - CNAME: www.a.shifen.com
- ▼ Authoritative nameservers
 - ▼ a.shifen.com: type SOA, class IN, mname ns1.a.shifen.com
 - Name: a.shifen.com
 - Type: SOA (Start Of a zone of Authority) (6)
 - Class: IN (0x0001)
 - Time to live: 284 (4 minutes, 44 seconds)
 - Data length: 45
 - Primary name server: ns1.a.shifen.com
 - Responsible authority's mailbox: baidu_dns_master.baidu.com
 - Serial Number: 2111030016
 - Refresh Interval: 5 (5 seconds)
 - Retry Interval: 5 (5 seconds)
 - Expire limit: 2592000 (30 days)
 - Minimum TTL: 3600 (1 hour)

作业1.2

反复解析过程

假如本机处在local.edu.cn，本机想要访问remote.example.edu.cn

1. 首先本地进行解析，查看本地是否有remote.example.edu.cn这个域名的缓存，如果有则直接使用本地缓存打开
2. 如果没有，以本地服务器为发送请求的中心，向根域名服务器发送寻找的请求，然后由根返回顶级域名，也就是告诉本地服务器需要去cn这个顶级域名里找
3. 之后本地服务器去向cn发出请求，cn返回edu，也就是告诉本地服务器去edu.cn里找
4. 本地服务器向edu.cn发送查询请求，返回example
5. 本地服务器向example.edu.cn发送查询，返回remote
6. 本地服务器向remote.example.edu.cn发送请求，得到对应的IP地址
7. 本地服务器得到返回的IP地址，将其交给主机（也就是DNS客户端）进行相应的访问

CDN中DNS重定向的基本方法

基本方法就是设置一个CNAME，在权威DNS服务器上设置一个CNAME，指向另外一个域名，也就是指向CDN的权威DNS服务器，比如example.com会指向example.cdn.com。然后在这个服务器上，还会再设置一个CNAME，这个CNAME指向的是CDN网络的全局负载均衡器。

接下来，本地DNS服务器会去请求CDN的全局负载均衡器解析域名，全局负载均衡器会根据以下条件给用户选择一台合适的缓存服务器提供服务：

1. 根据用户的IP地址，判断哪个服务器离用户最近
2. 用户所在区域的运营商
3. 根据用户请求中的URL携带的内容名称，判断哪个服务器上有用户需要的内容
4. 查询各个服务器当前的负载情况，判断哪个服务器有服务能力

选出了合适的缓存服务器之后，全局负载均衡器会将这个IP地址返回；本地DNS服务器缓存这个IP地址，将这个IP地址返回给客户端。客户端访问这个边缘节点并下载资源。假如说这个缓存服务器上没有用户需要的内容，那么这个服务器就会向他的上一级缓存服务器请求内容，直到将所需要的资源拉到本地。

作业1.3

DNS协议应如何保证可靠机制

1. 给数据包添加序号，保证单词通信的过程中多个数据包之间是有序的
2. 在应用层增加校验机制（DNS就是应用层上的协议），如接收方计算数据包的校验码和数据包中提供的校验码不一致，那么就丢弃该数据包并请求重发
3. 增加确认机制，如果发送方没有在规定时间内接收到接收方的应答包，则会进行重发。发送三次后还未收到应答直接判定本次发送失败。