计算机网络实验报告_3_DNS

学号:PB20000219 姓名:李蔚林

实验目的

1. 巩固并掌握DNS相关知识
2. 了解nslookup和ipconfig等命令的使用

实验过程及问答题

1).nslookup

1.Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

我选取的服务器是www.bilibili.com的服务器(四个),IP地址有如下四个:120.92.168.13, 119.3.33.86, 119.3.44.211, 120.82.162.180

2.Run nslookup to determine the authoritative DNS servers for a university in Europe.

选取的是牛津大学(ox.ac.uk),其DNS服务器如下图所示

```
C:\Users\61794>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 = dns2.ox.ac.uk
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk
ox.ac.uk        nameserver = ns2.ja.net
```

3.Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

通过上述服务器无法查询

```
C:\Users\61794>nslookup mail.yahoo.com dns2.ox.ac.uk
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  163.1.2.190

*** UnKnown 找不到 mail.yahoo.com: Query refused

C:\Users\61794>
```

2)ipconfig

ipconfig \all命令截图如下:

```
C:\Users\61794>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : LAPTOP-P45LULAV
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : ustc.edu.cn

以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   物理地址. . . . . . . . . . . . . : 54-05-DB-87-7C-E8
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 本地连接* 1:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址. . . . . . . . . . . . . : 34-C9-3D-91-74-55
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   物理地址. . . . . . . . . . . . . : 00-50-56-C0-00-01
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::7c00:cda4:9dfd:7f3b%7(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.220.1(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2021年10月6日 22:12:17
   租约过期的时间  . . . . . . . . . : 2021年10月6日 23:57:00
   默认网关. . . . . . . . . . . . . :
   DHCP 服务器 . . . . . . . . . . . : 192.168.220.254
   DHCPv6 IAID . . . . . . . . . . . : 687886422
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-27-23-55-75-54-05-DB-87-7C-E8
```

ipconfig /displaydns 命令截图如下:

```
C:\Users\61794>ipconfig /displaydns

Windows IP 配置

    safebrowsing.googleapis.com
    ----------------------------------------
    记录名称. . . . . : safebrowsing.googleapis.com
    记录类型. . . . . : 1
    生存时间. . . . . : 148
    数据长度. . . . . : 4
    部分. . . . . : 答案
    A (主机)记录 . . . . : 180.163.150.161


    edge.microsoft.com
    ----------------------------------------
    记录名称. . . . . : edge.microsoft.com
    记录类型. . . . . : 5
    生存时间. . . . . : 100
    数据长度. . . . . : 8
    部分. . . . . : 答案
    CNAME 记录 . . . . . : edge-microsoft-com.a-0016.a-msedge.net


    记录名称. . . . . : edge-microsoft-com.a-0016.a-msedge.net
    记录类型. . . . . : 5
    生存时间. . . . . : 100
    数据长度. . . . . : 8
    部分. . . . . : 答案
    CNAME 记录 . . . . . : a-0016.a-msedge.net


    记录名称. . . . . : a-0016.a-msedge.net
    记录类型. . . . . : 1
    生存时间. . . . . : 100
    数据长度. . . . . : 4
    部分. . . . . : 答案
    A (主机)记录 . . . . : 204.79.197.219


    steamcommunity.com
    ----------------------------------------
    记录名称. . . . . : steamcommunity.com
    记录类型. . . . . : 1
    生存时间. . . . . : 599287
    数据长度. . . . . : 4
    部分. . . . . : 答案
    A (主机)记录 . . . . : 23.198.114.132
```

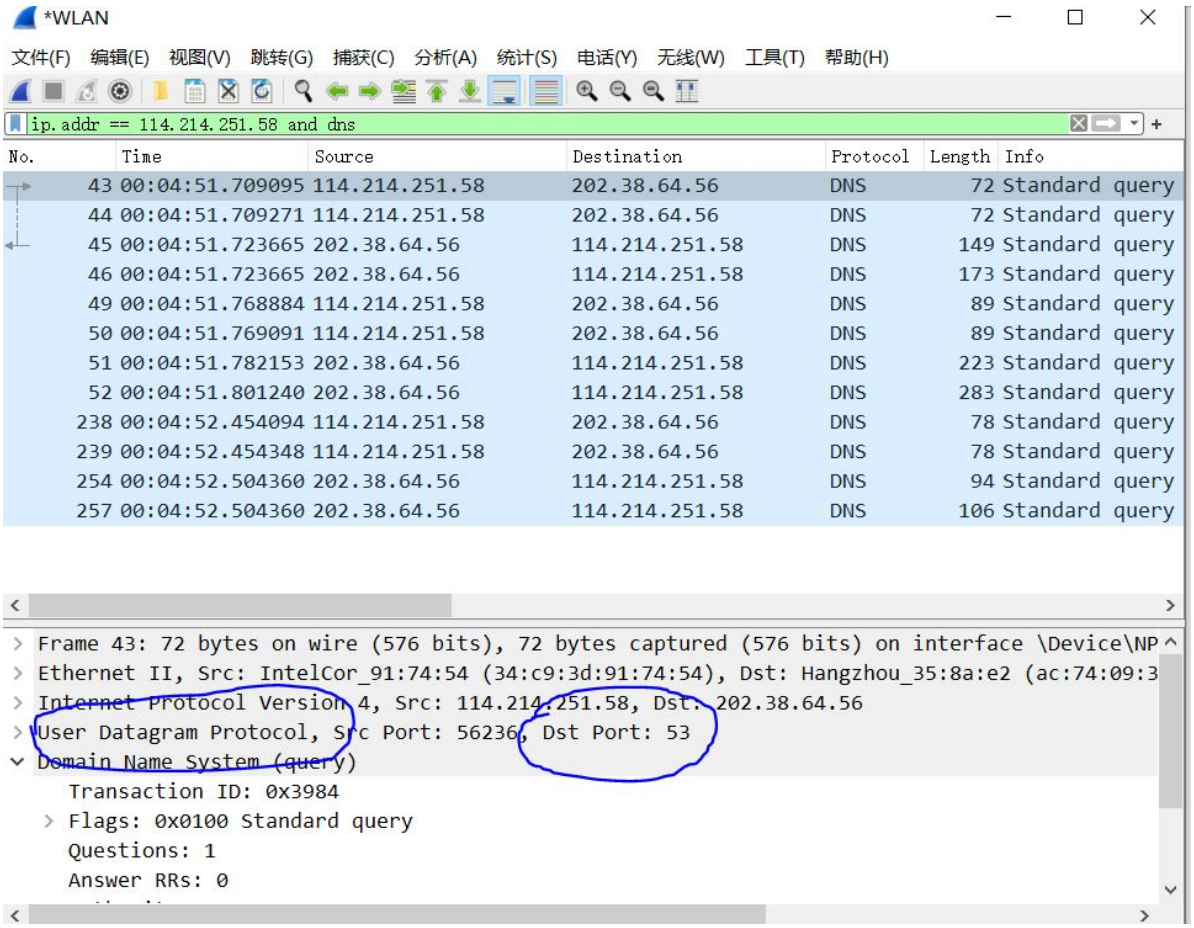
ipconfig /flushdns 命令截图如下:

```
C:\Users\61794>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

3)Tracing DNS with Wireshark

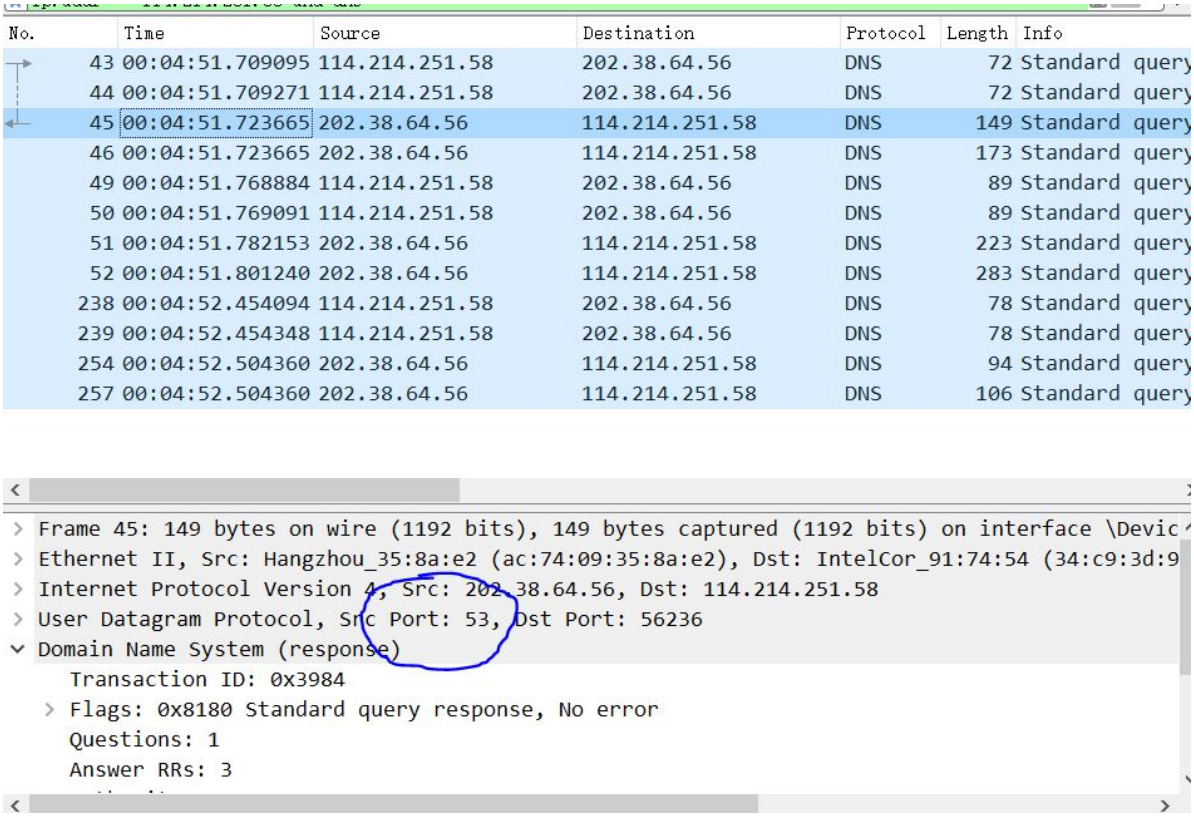
4.Locate the DNS query and response messages. Are then sent over UDP or TCP?

是通过UDP协议发送的



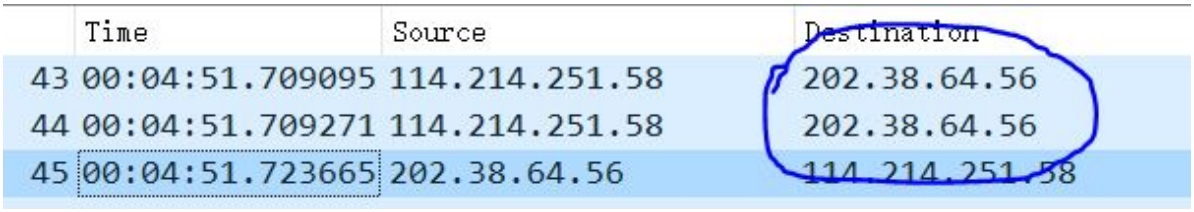
5.What is the destination port for the DNS query message? What is the source port of DNS response message?

DNS查询目标端口(见上题截图)和响应消息的源端口都是53

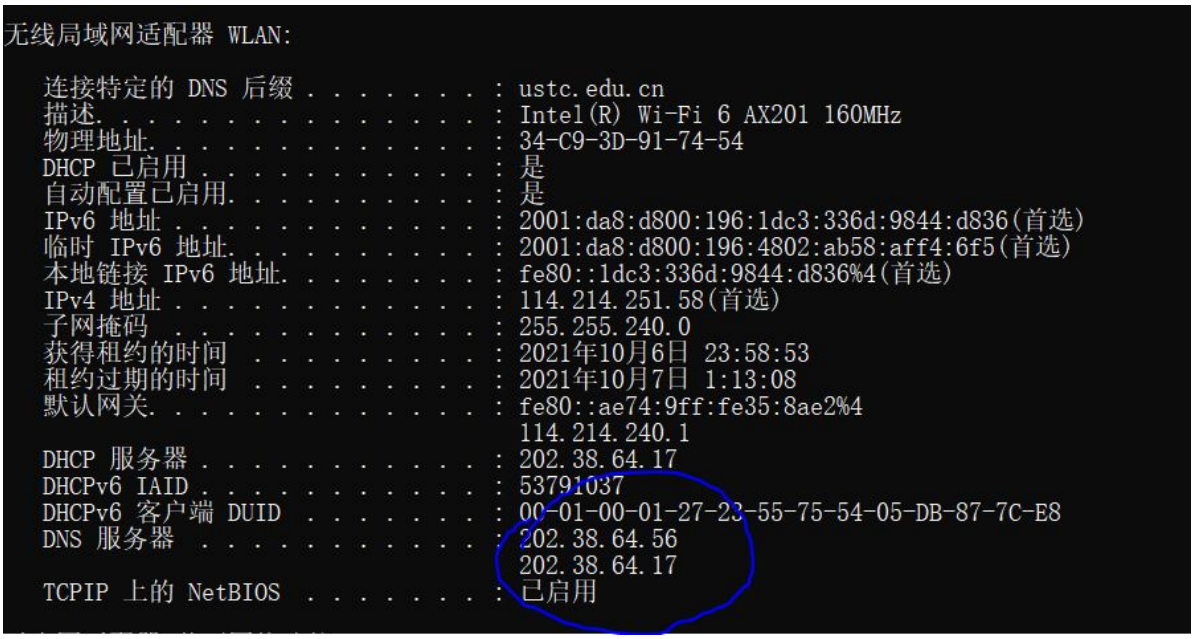


6.To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

发送到202.38.64.56,和本地DNS服务器IP地址相同



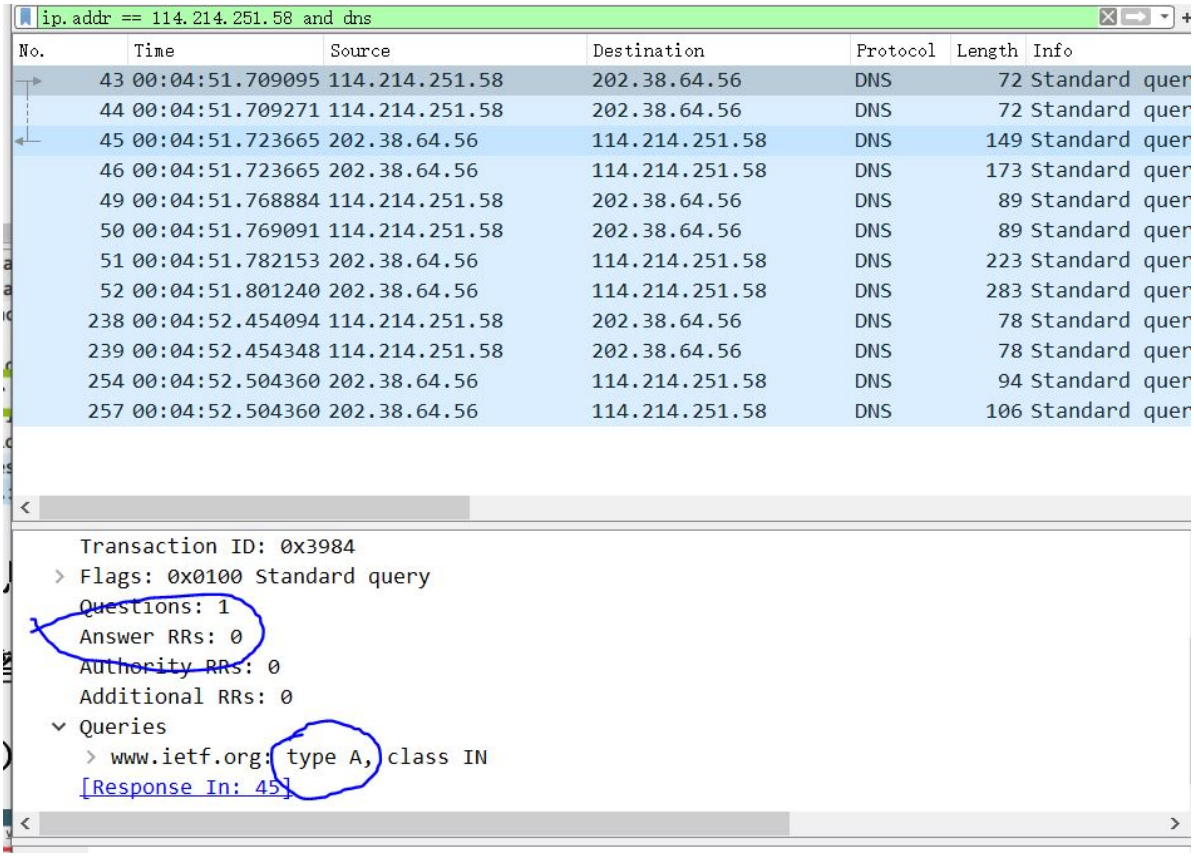
	Time	Source	Destination
43	00:04:51.709095	114.214.251.58	202.38.64.56
44	00:04:51.709271	114.214.251.58	202.38.64.56
45	00:04:51.723665	202.38.64.56	114.214.251.58



```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . : ustc.edu.cn
   描述. . . . . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   物理地址. . . . . . . . . . . . . : 34-C9-3D-91-74-54
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2001:da8:d800:196:1dc3:336d:9844:d836(首选)
   临时 IPv6 地址. . . . . . . . . . : 2001:da8:d800:196:4802:ab58:aff4:6f5(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::1dc3:336d:9844:d836%4(首选)
   IPv4 地址 . . . . . . . . . . . . : 114.214.251.58(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.240.0
   获得租约的时间  . . . . . . . . . : 2021年10月6日 23:58:53
   租约过期的时间  . . . . . . . . . : 2021年10月7日 1:13:08
   默认网关. . . . . . . . . . . . . : fe80::ae74:9ff:fe35:8ae2%4
                                       114.214.240.1
   DHCP 服务器 . . . . . . . . . . . : 202.38.64.17
   DHCPv6 IAID . . . . . . . . . . . : 53791037
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-27-23-55-75-54-05-DB-87-7C-E8
   DNS 服务器  . . . . . . . . . . . : 202.38.64.56
                                       202.38.64.17
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

7.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

TYPE=A(即查询该IP地址),查询消息不包括answers



ip.addr == 114.214.251.58 and dns

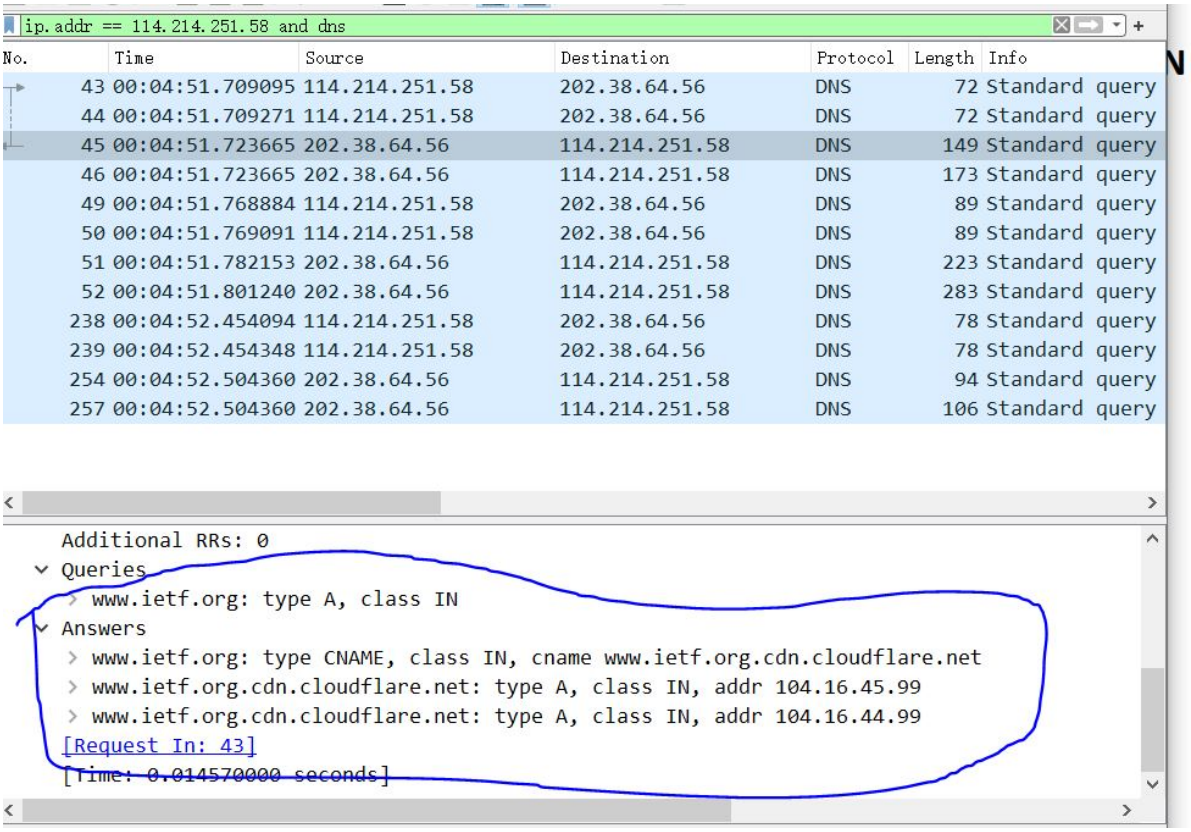
No.	Time	Source	Destination	Protocol	Length	Info
43	00:04:51.709095	114.214.251.58	202.38.64.56	DNS	72	Standard quer
44	00:04:51.709271	114.214.251.58	202.38.64.56	DNS	72	Standard quer
45	00:04:51.723665	202.38.64.56	114.214.251.58	DNS	149	Standard quer
46	00:04:51.723665	202.38.64.56	114.214.251.58	DNS	173	Standard quer
49	00:04:51.768884	114.214.251.58	202.38.64.56	DNS	89	Standard quer
50	00:04:51.769091	114.214.251.58	202.38.64.56	DNS	89	Standard quer
51	00:04:51.782153	202.38.64.56	114.214.251.58	DNS	223	Standard quer
52	00:04:51.801240	202.38.64.56	114.214.251.58	DNS	283	Standard quer
238	00:04:52.454094	114.214.251.58	202.38.64.56	DNS	78	Standard quer
239	00:04:52.454348	114.214.251.58	202.38.64.56	DNS	78	Standard quer
254	00:04:52.504360	202.38.64.56	114.214.251.58	DNS	94	Standard quer
257	00:04:52.504360	202.38.64.56	114.214.251.58	DNS	106	Standard quer

```
Transaction ID: 0x3984
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
  > www.ietf.org: type A, class IN
[Response In: 45]
```

8.Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

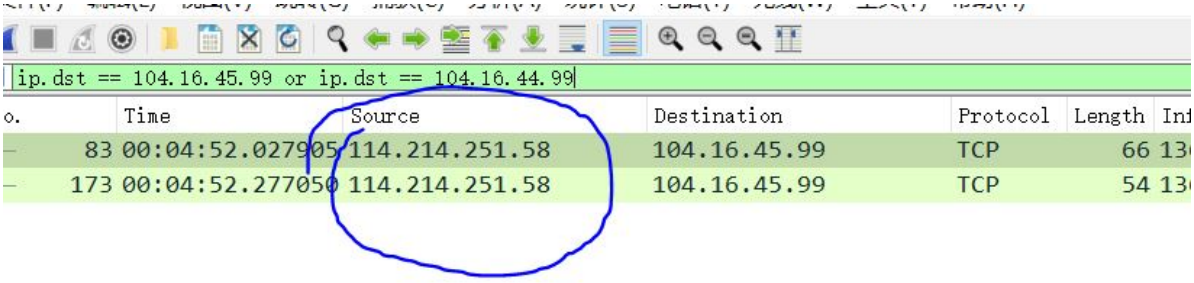
包含了三个:

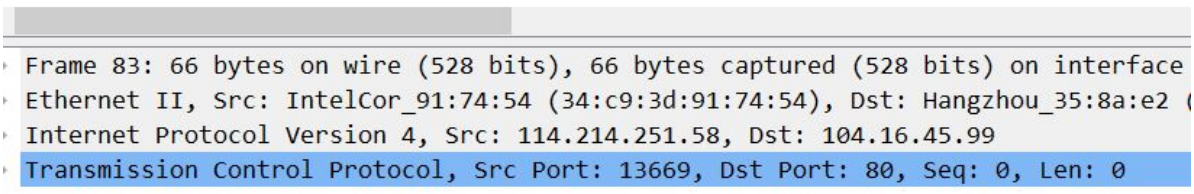
1. 规范CNAME的地址 type = CNAME
2. 规范后的IPV4地址1 type = A
3. 规范后的IPV4地址2 type = A

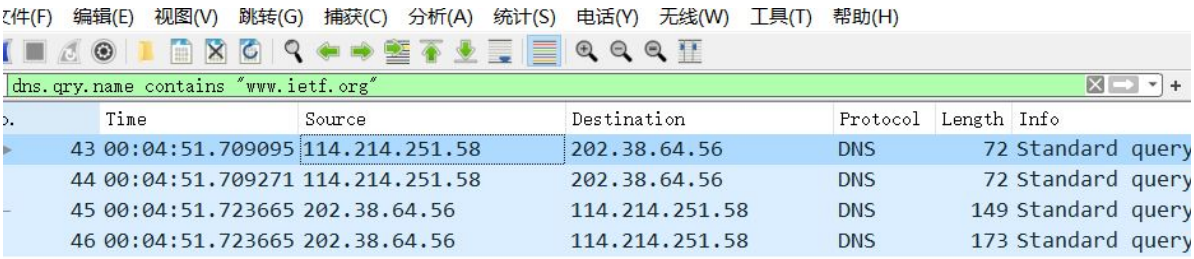


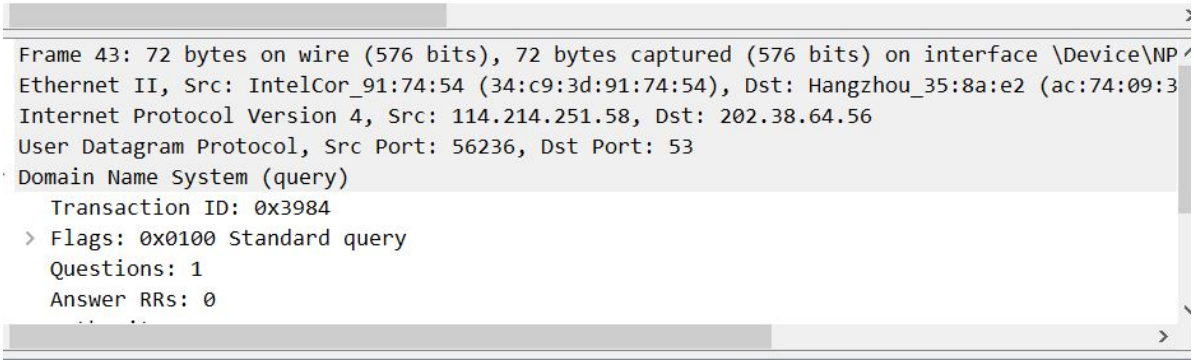
9.Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

该目的地址与DNS响应消息中的IP地址相对应







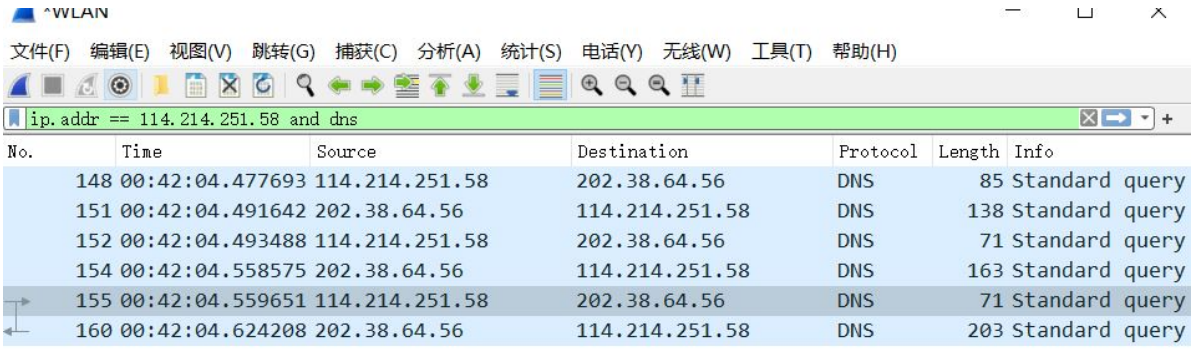


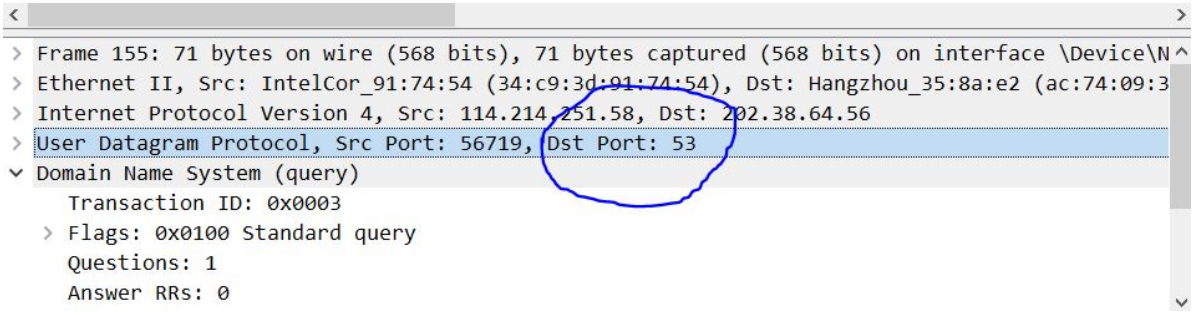
10.This web page contains images. Before retrieving each image, does your host issue new DNS queries?

并没有,由前面的截图知,本地应该有DNS缓存,在获取图片时直接使用了缓存

11.What is the destination port for the DNS query message? What is the source port of DNS response message?

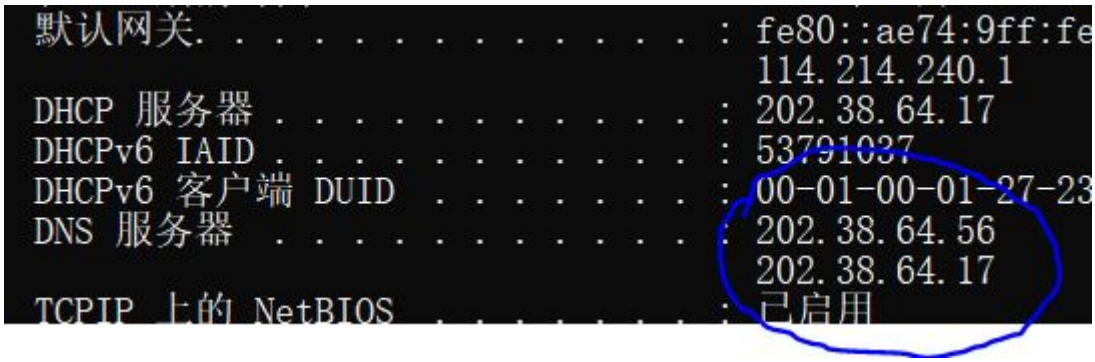
查询目标端口和相应源端口都是53

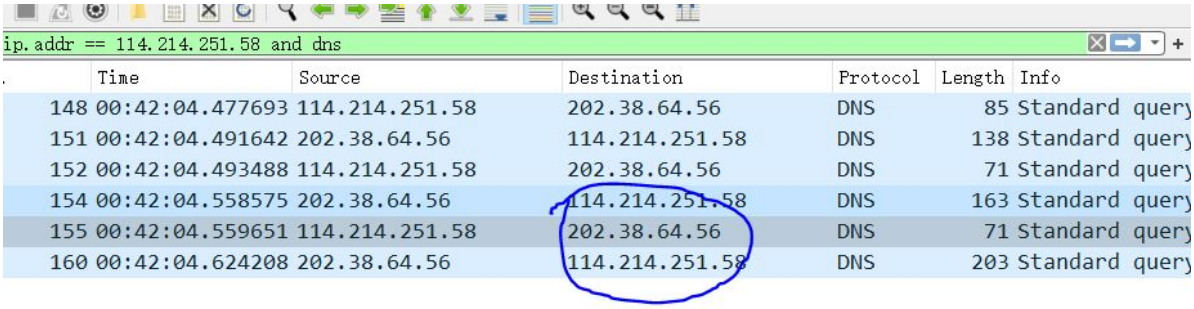


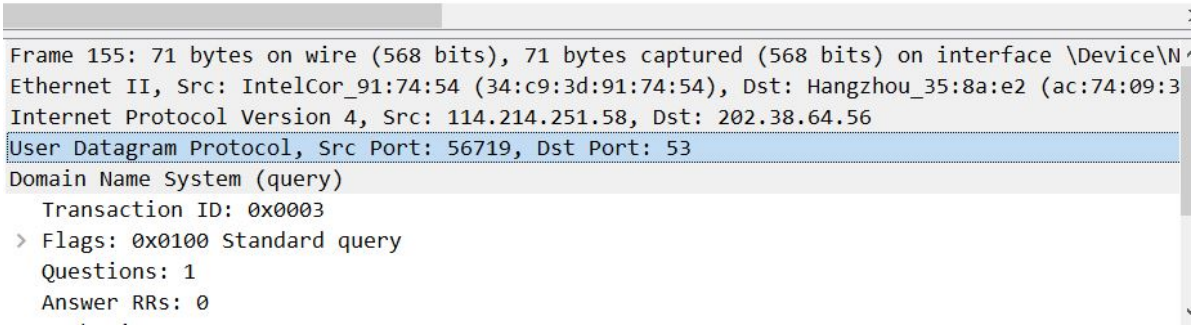


12.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

查询消息的目标IP地址是202.38.64.56,是我的本地DNS服务器IP地址

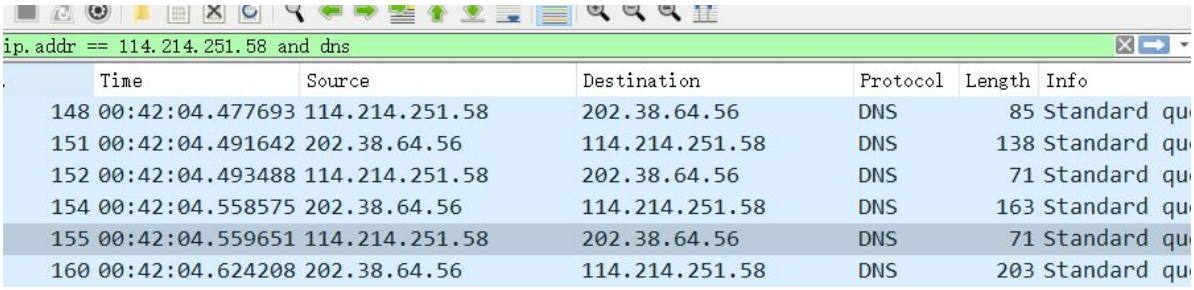


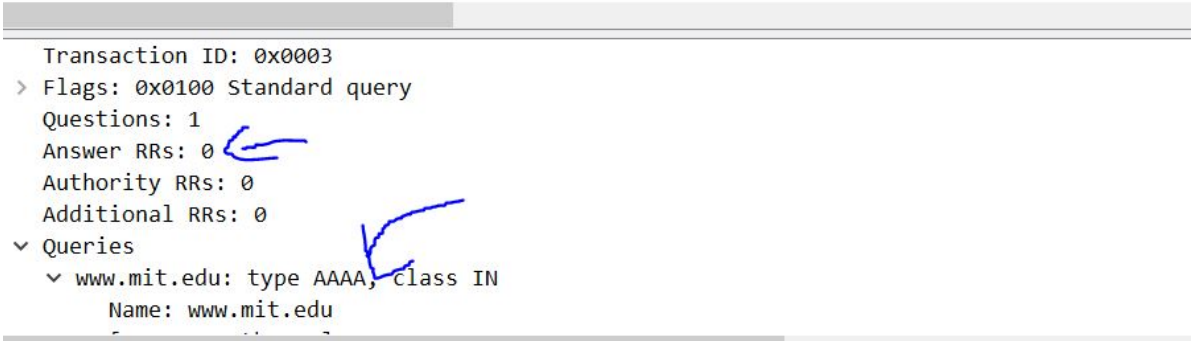




13.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

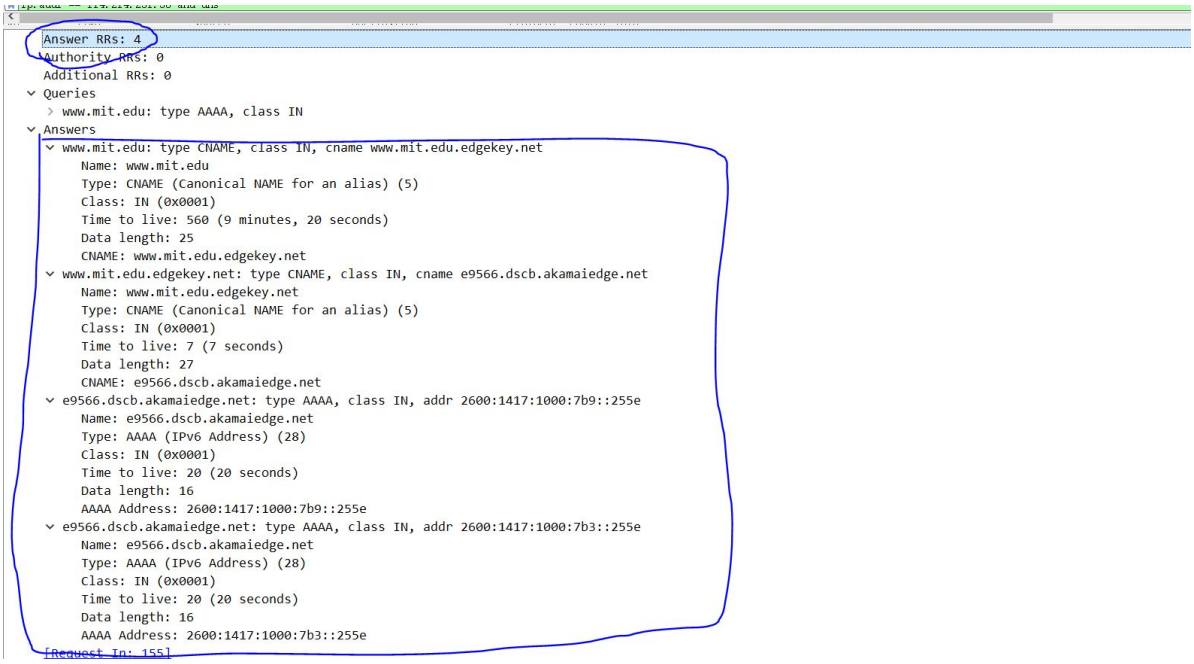
查询是Type = AAAA类型的,不包含Answers.





14.Examine the DNS response message.How many “answers” are provided? What do each of these answers contain?

响应消息提供了4个Answers,这些答案包含两个规范CNAME地址(Type = CNAME)和两个指向的IPv6地址(Type = AAAA)

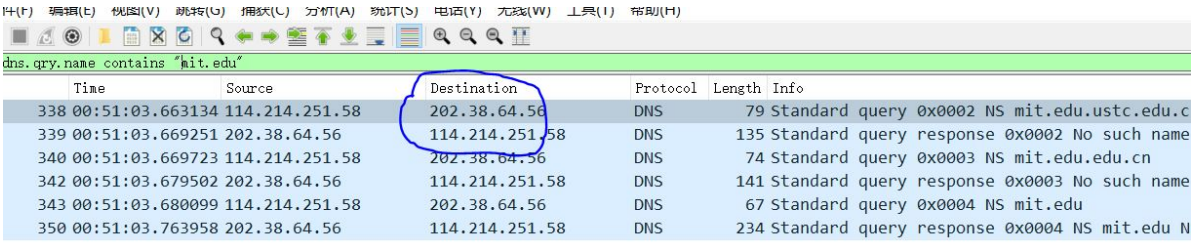


15.Provide a screenshot.

如上图

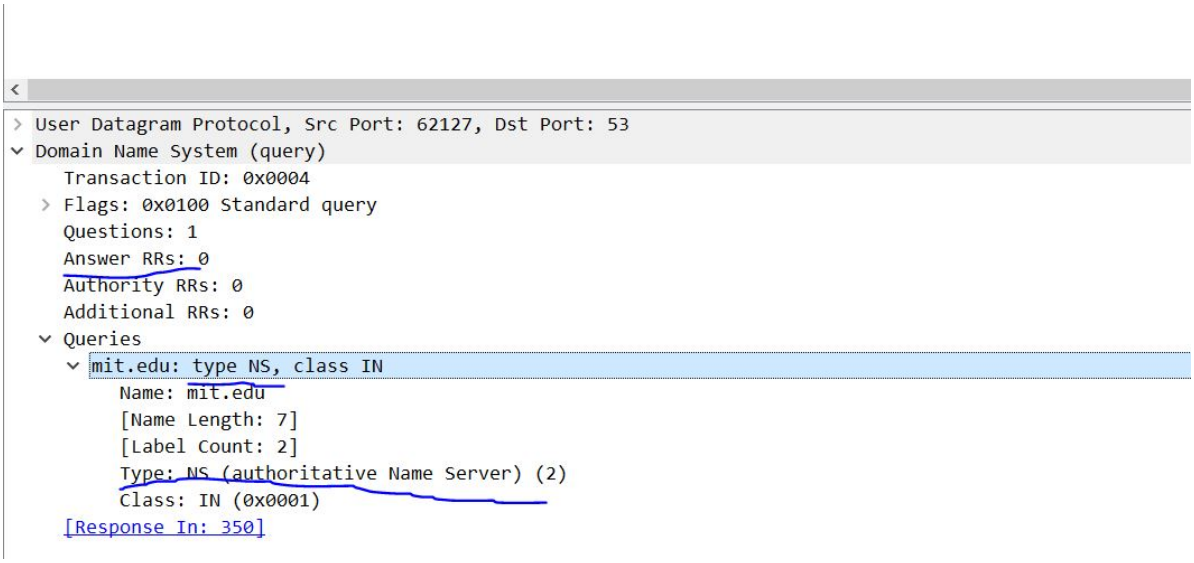
16.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

发往202.38.64.56,是我的本地默认DNS地址



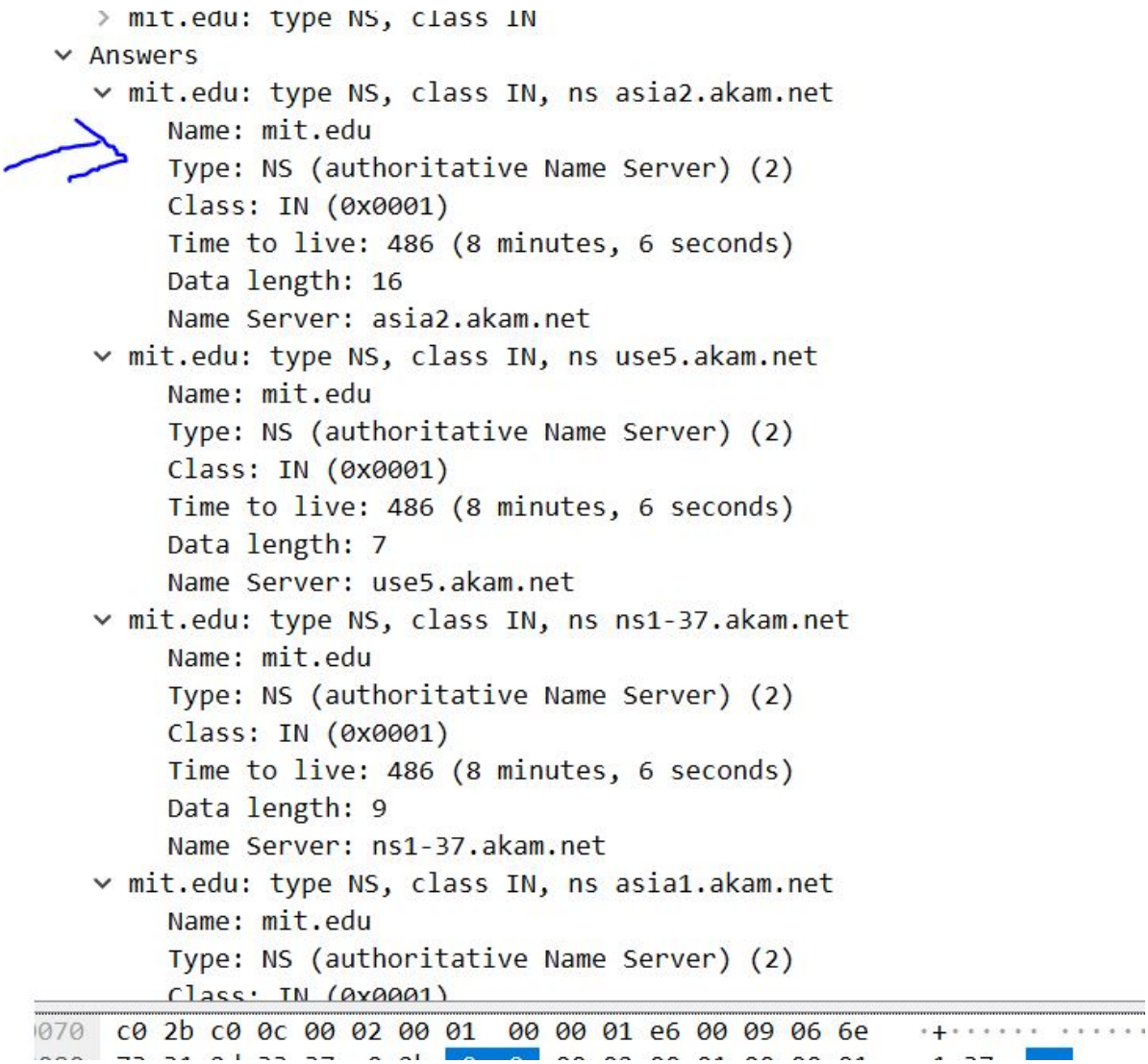
17.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type = NS即查询权威DNS,不包含Answers



18.Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

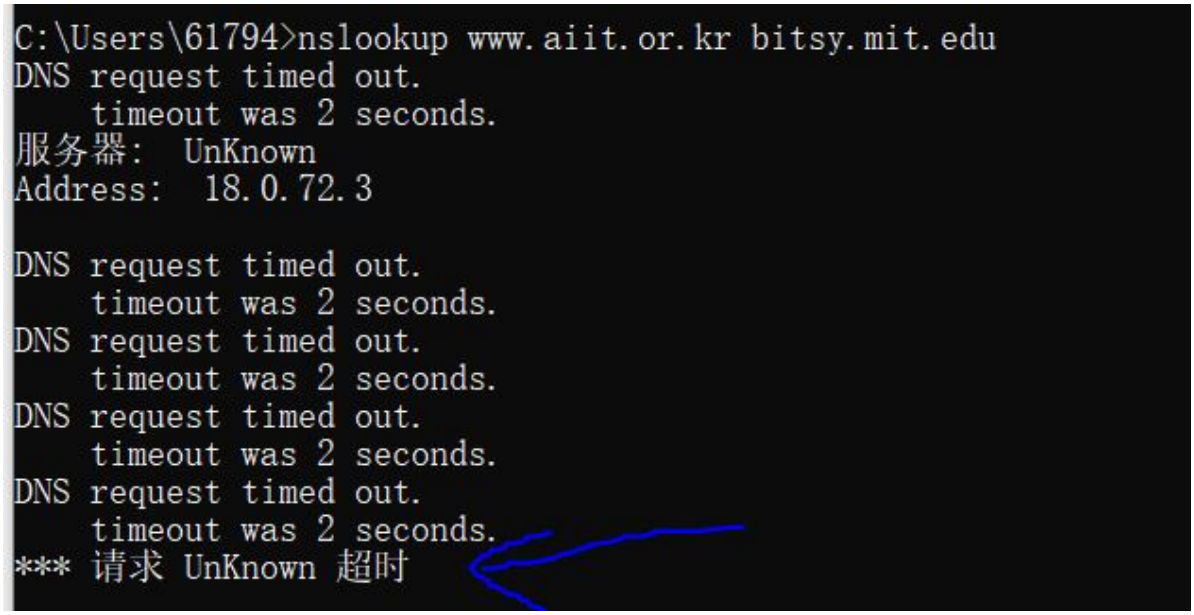
如图,提供的是MIT的权威DNS域名,不提供MIT域名的IP地址



19.Provide a screenshot.

如上图

接下来的20-23题无法回答,由于指令运行TIME OUT,经过助教解答得知这是正常结果,截图如下



20.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

21.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

22.Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

23.Provide a screenshot.

实验思考

本实验通过对ipconfig和nslookup的灵活使用,巩固加深了对DNS相关知识的总结和应用,同时在助教的帮助下排除了实验的意外情况,值得借鉴.