中国科学技术大学计算机学院
《计算机网络》实验报告

实验题目：lab3 DNS

学生姓名：张舒恒

学生学号：PB19030888

专业：计算机科学与技术

授课老师：华蓓

完成日期：2021 年 10 月 1 日

一、实验目的

1. 了解 DNS

2. 了解系统命令 NSLOOKUP 和 IPCONFIG 的用法

二、实验环境

1、 硬件： pc 一台

2、 软件： Win10 Professional 1703

Wireshark2.4.0

三、实验过程

1. nslookup

第一个命令：nslookup www.mit.edu

```
C:\Users\ASUS>nslookup www.mit.edu
Server:  mx.ustc.edu.cn
Address:  202.38.64.56

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:1000:7b3::255e
          2600:1417:1000:7b9::255e
          23.7.172.76
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

第二个命令：nslookup -type=NS mit.edu

```
C:\Users\ASUS>nslookup -type=NS mit.edu
Server:  mx.ustc.edu.cn
Address:  202.38.64.56

Non-authoritative answer:
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
```

第三个命令：nslookup www.aiit.or.kr bitsy.mit.edu，由于此 DNS 服务器停用所以改用 8.8.8.8 查询

```
C:\Users\ASUS>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

```
C:\Users\ASUS>nslookup www.aiit.or.kr 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  58.229.6.225
```

2. ipconfig

ipconfig /all：所有关于我的主机信息都类似如下面的屏幕截图所显示。

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-01Q6SOV
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 以太网:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 04-92-26-1B-89-1E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter 本地连接* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : D8-F2-CA-CA-EA-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

ipconfig /displaydns：主机缓存的最近获得的 DNS 记录

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

Windows IP Configuration

    user-images.githubusercontent.com
    ----------------------------------------
    Record Name . . . . . : user-images.githubusercontent.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 1122
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2606:50c0:8001::154


    Record Name . . . . . : user-images.githubusercontent.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 1122
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2606:50c0:8002::154


    Record Name . . . . . : user-images.githubusercontent.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 1122
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2606:50c0:8000::154
```

ipconfig /flushdns：清除了所有条目并从 hosts 文件重新加载条目

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

3. 使用 Wireshark 追踪 DNS

在熟悉 nslookup 和 ipconfig 之后，我们捕获一些由常规上网活动生成的 DNS 数据包。

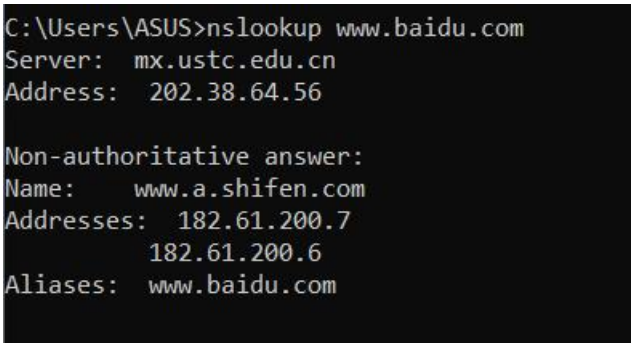
- 使用 ipconfig 清空主机中的 DNS 缓存。
- 打开浏览器并清空浏览器缓存。

- 打开 Wireshark，然后在过滤器中输入“ip.addr==your_IP_address”（可以先使用 ipconfig 获取你的 IP 地址）。此过滤器将删除既从主机不发出也不发往主机的所有数据包。
- 在 Wireshark 中启动数据包捕获。
- 使用浏览器访问网页： http://www.ietf.org
- 停止数据包捕获。

在 cmd 中分别输入命令 nslookup www.mit.edu，nslookup -type=NS mit.edu，nslookup www.aiit.or.kr bitsy.mit.edu，重复上述操作。

四、问题回答

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



查询 www.baidu.com，IP 地址是 182.61.200.7 和 182.61.200.6

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

```
C:\Users\ASUS>nslookup -type=NS berklee.edu
Server:  mx.ustc.edu.cn
Address:  202.38.64.56

Non-authoritative answer:
berklee.edu     nameserver = ns4.p21.dynect.net
berklee.edu     nameserver = ns2.berklee.edu
berklee.edu     nameserver = ns3.p21.dynect.net
berklee.edu     nameserver = ns1.p21.dynect.net
berklee.edu     nameserver = ns2.p21.dynect.net
```

查询 berklee 大学的权威服务器

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?

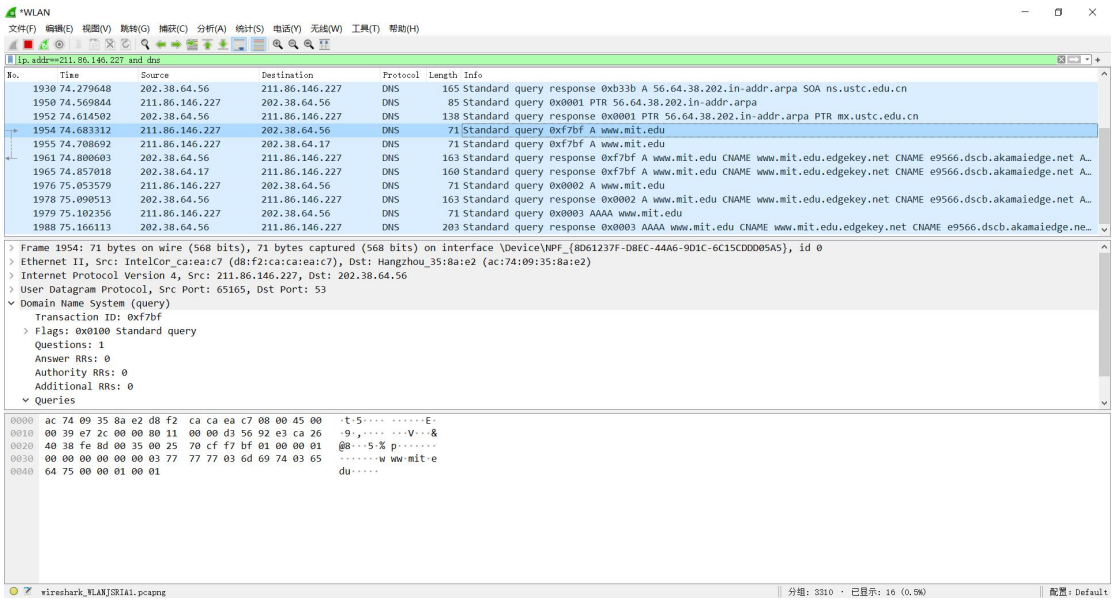
由于服务器一直没响应，所以改用 mx.ustc.edu.cn 查询 lug.ustc.edu.cn，IP 地址是 202.38.95.102

```
C:\Users\ASUS>nslookup lug.ustc.edu.cn mx.ustc.edu.cn
Server:  UnKnown
Address:  2001:da8:d800::56

Non-authoritative answer:
Name:    lug.ustc.edu.cn
Addresses:  2001:da8:d800:95::102
          202.38.95.102
```

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

由图可以观察 DNS 协议是 UDP 协议之上的。

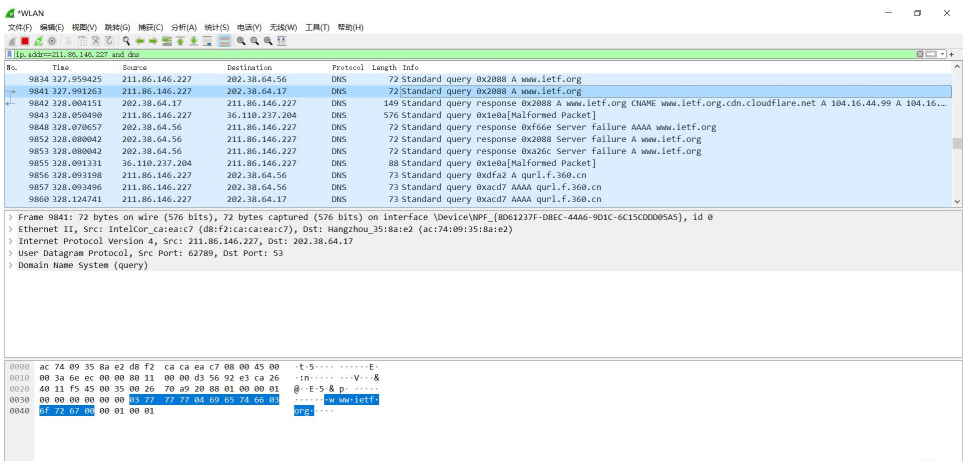


5.What is the destination port for the DNS query message? What is the source port of DNS response message?

查询的目标端口和响应端口都是 53。

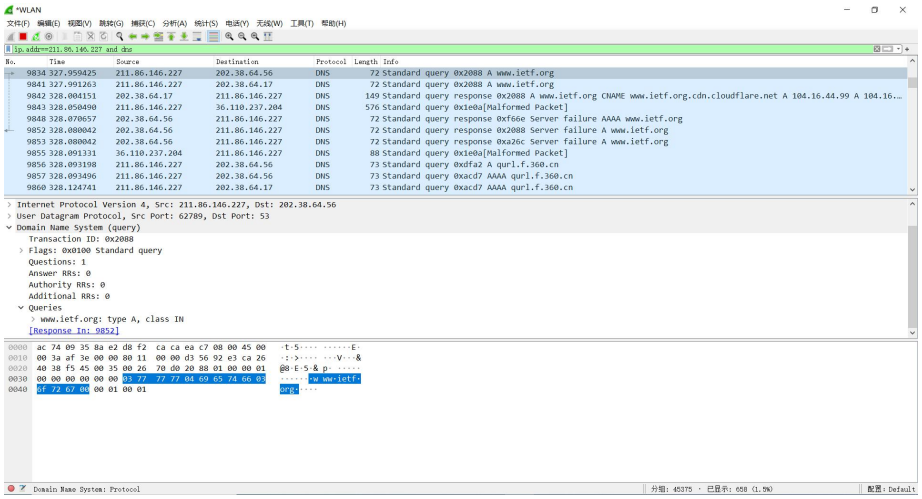
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

发送到 IP 地址 202.38.64.56 和 202.38.64.17，并不是我本地地址



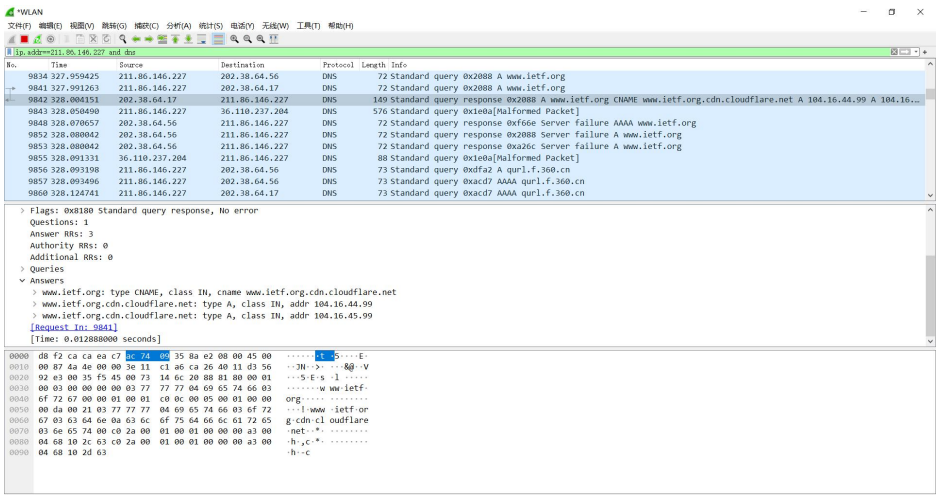
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

TYPE=A，意思查询请求的 IP 地址，查询消息不包括任何的结果



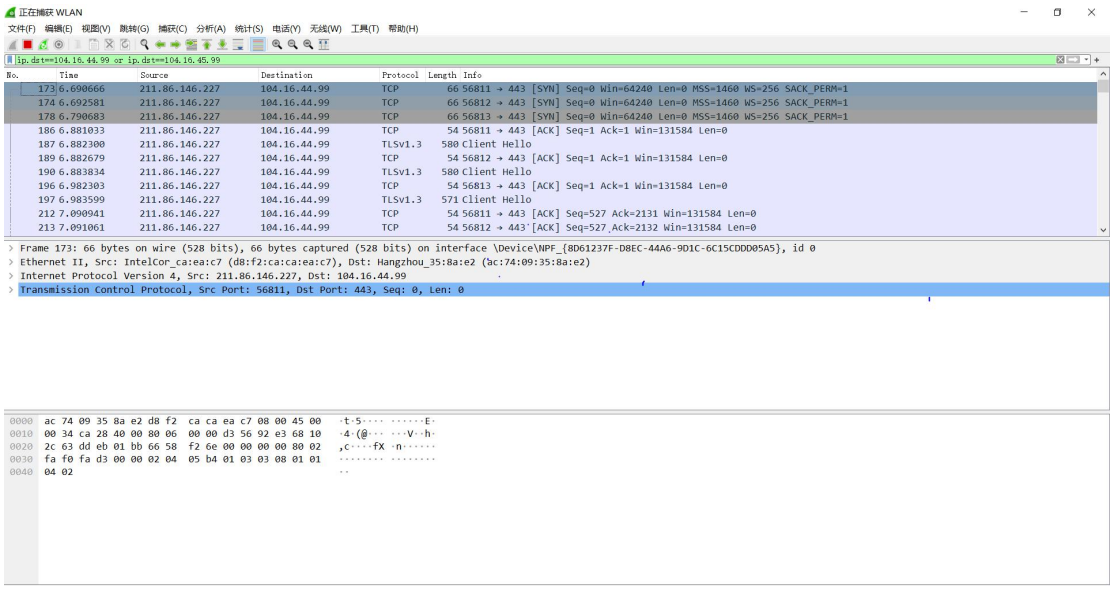
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

提供了 3 个答案,分别是由国外 CDN 厂商 Cloudflare 提供的规范 CNAME 的 CDN 加速(type=cname)地址，以及规范后 CNAME 的两个 IPV4 地址(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?

是的，下图 SYN 数据包的目的 IP 地址 104.16.44.99 和 DNS 响应消息中提供的 IP 地址相同



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

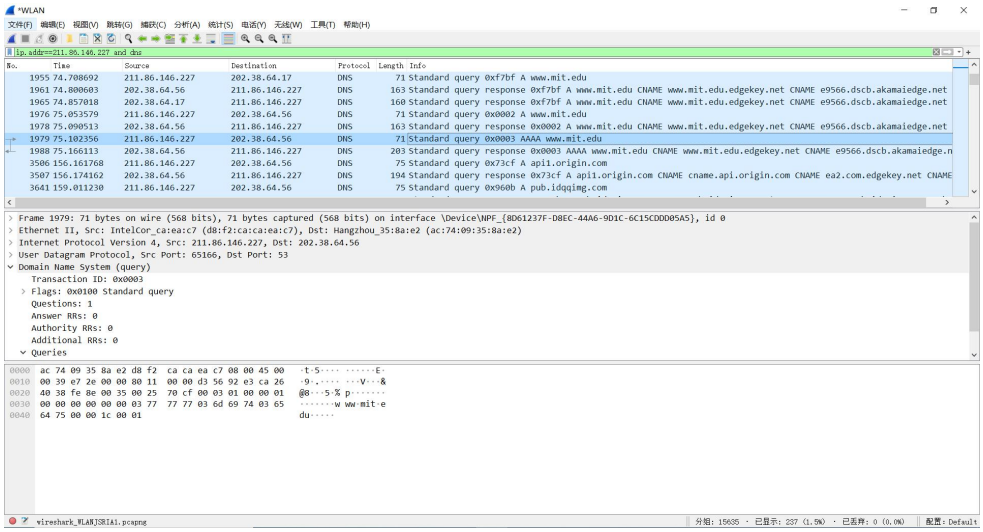
没有，因为本地有 DNS 缓存，部分图片的获取使用缓存

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

查询目标端口和响应源端口还是 53

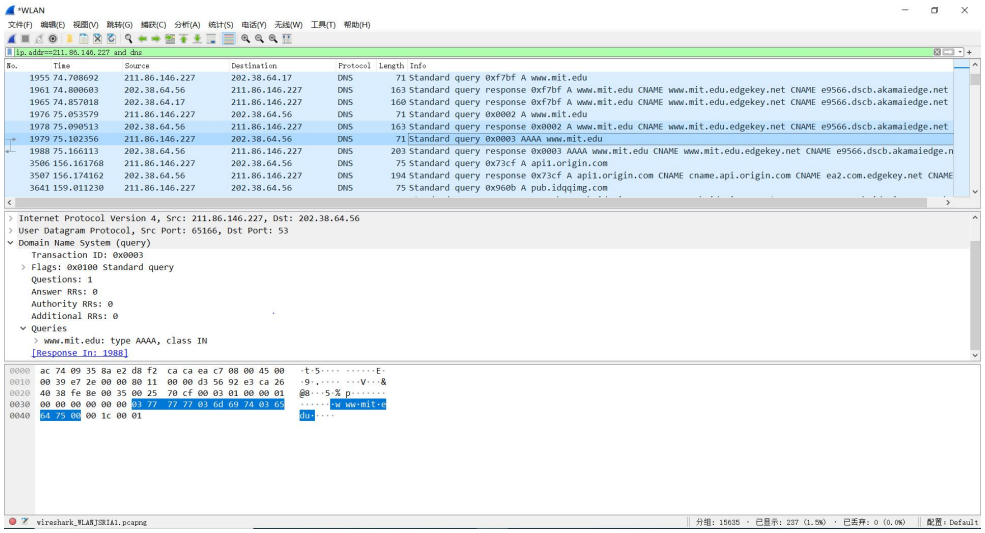
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

发送到 IP 地址 202.38.64.56 和 202.38.64.17，并不是我本地地址



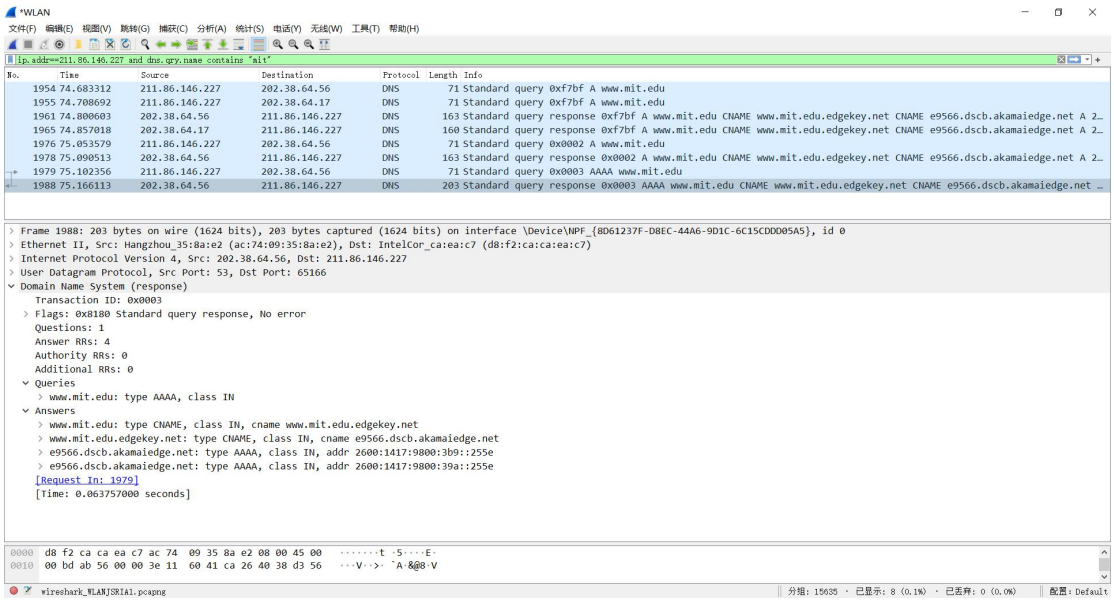
13.Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

TYPE=A（请求 IPV4 地址查询），TYPE=AAAA(请求 IPV6 地址查询)，查询消息不包括任何答案



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

提供了 4 个答案，分别是两个规范主机地址(type=cname)，以及两个 IPV6 地址（type=AAAA）

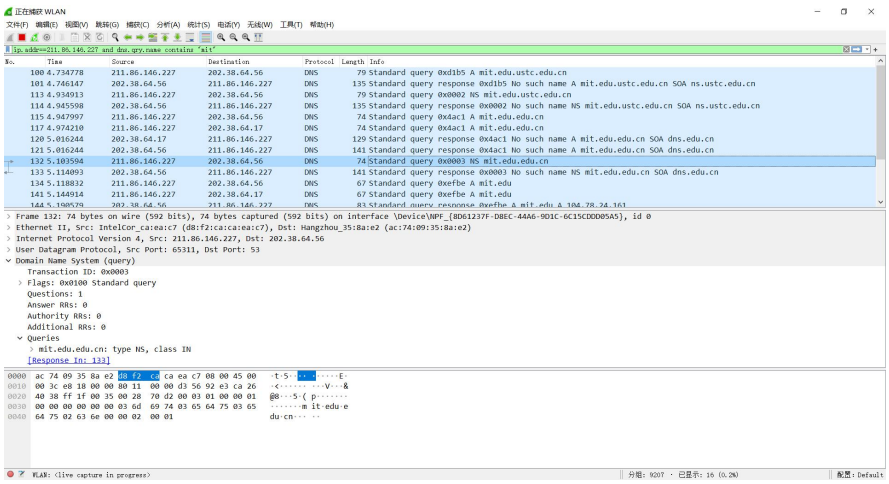


15. Provide a screenshot.

上面已经给出

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

发送到 IP 地址 202.38.64.56 和 202.38.64.17，并不是我本地地址

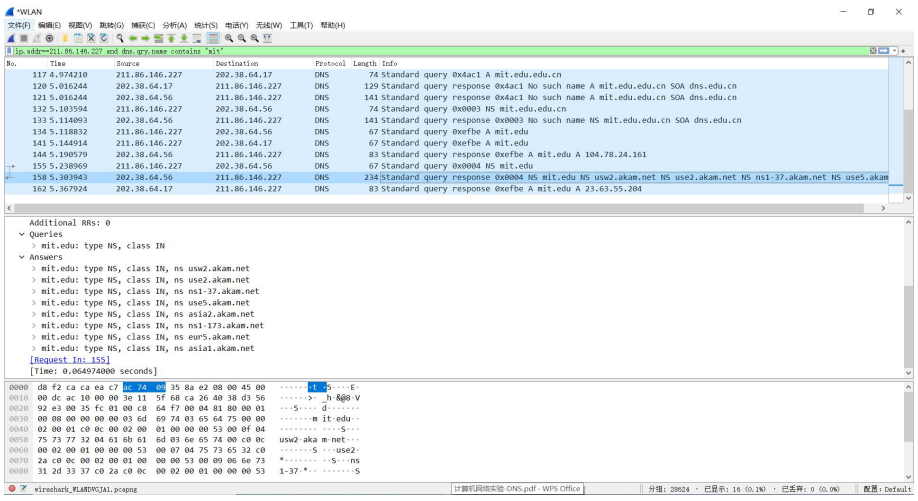


17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

如 16 题图，有两个 TYPE=A（请求 IPV4 地址查询）和一个 TYPE=NS（查询权威 DNS）请求，查询消息均不包含任何结果

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?

提供了 MIT 的权威 DNS 的域名，不提供 MIT 的域名的 IP 地址

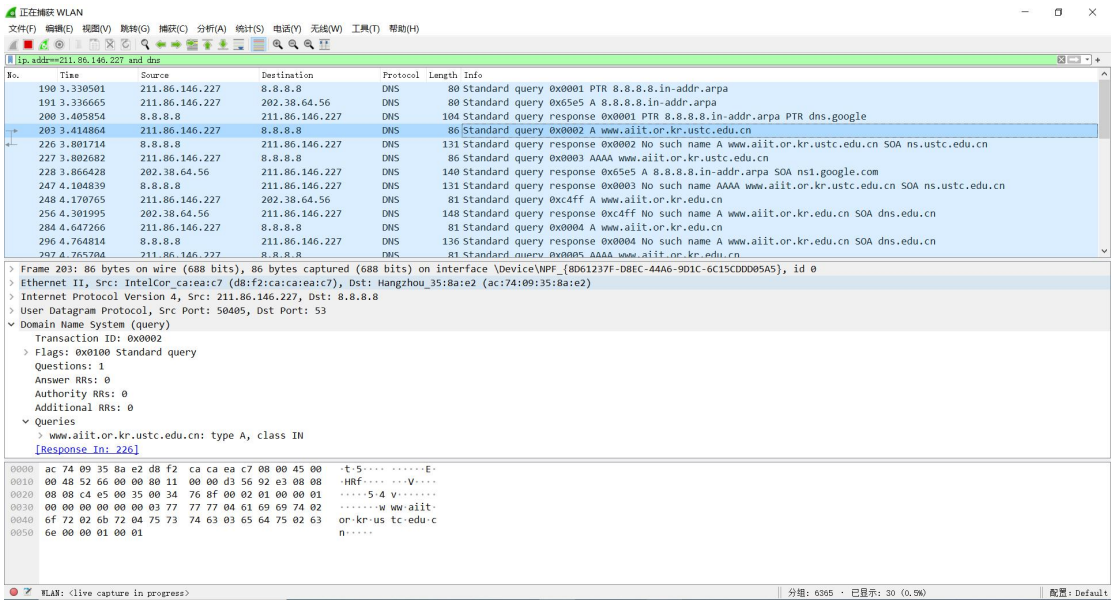


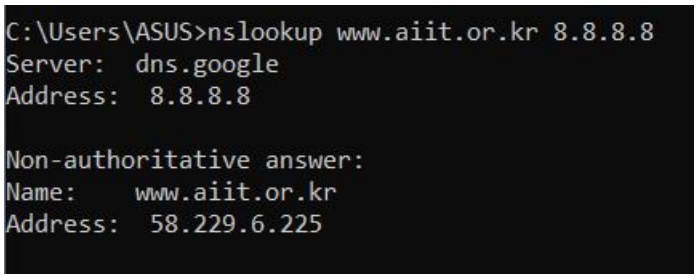
19.Provide a screenshot

上面已经给出

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?

由于 bitsy.mit.edu(18.72.0.3)这个 DNS 已经停用，所以改用 8.8.8.8 查询。查询消息发送到的 IP 地址是 8.8.8.8，不是我的本地地址，而是我指定的 DNS 服务器地址。



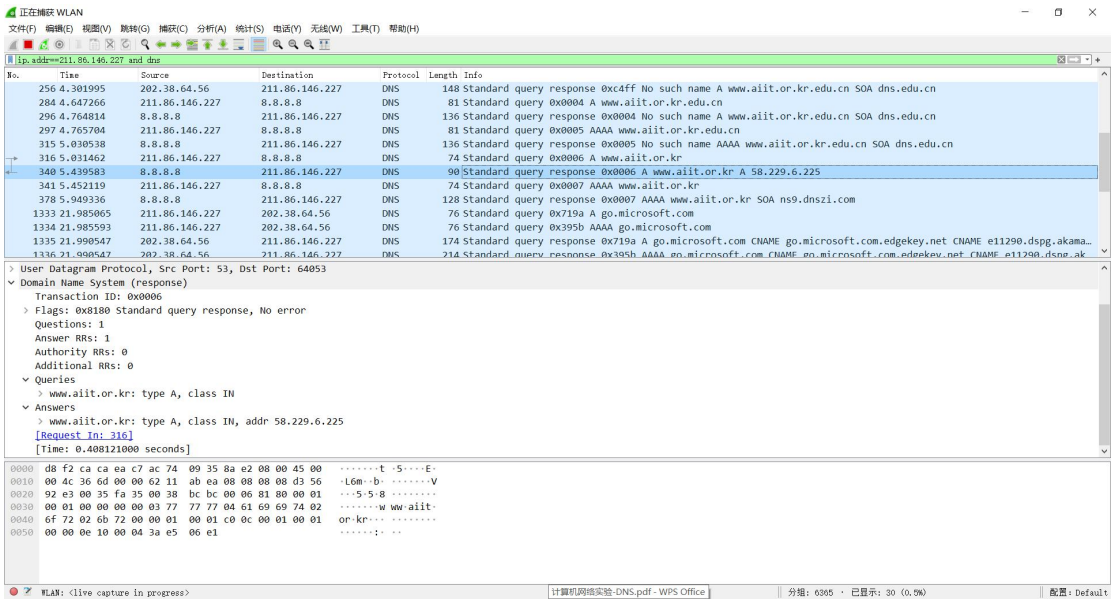


21.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

如 20 题图，有一个 TYPE=PTR(通过 IP 反向查域名)，一个 TYPE=A（请求 IPV4 地址查询），TYPE=AAAA(请求 IPV6 地址查询)，查询消息均不包含任何结果

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

1 个，是 TYPE=A 的查询结果



23. Provide a screenshot.

上面已经给出