**电子科技大学**

**实**

**验**

**报**

**告**

学生姓名：李昊霖

学号：2019270102007

课程名称：计算机网络基础

指导教师：杨宁

日期： 2021 年 3 月 12 日

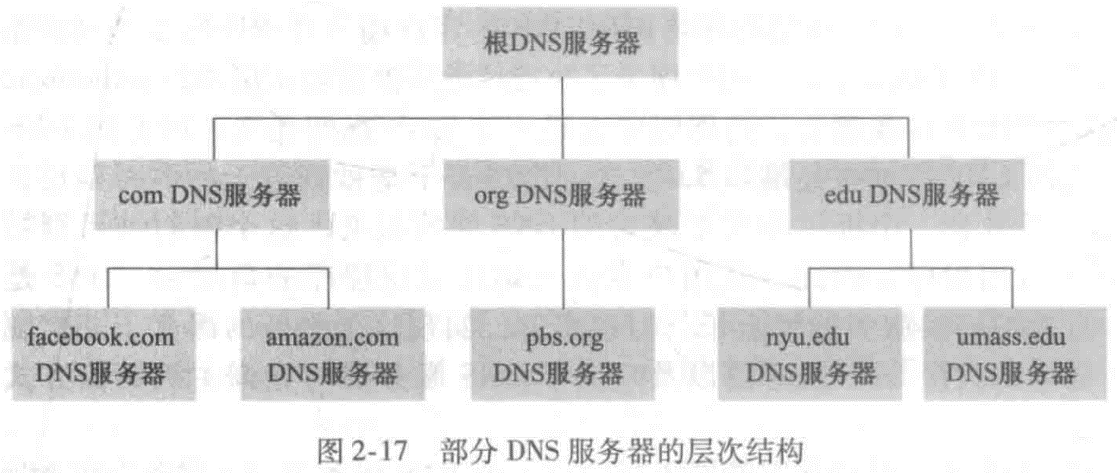
实验项目名称： 2-2 wireshark-dns实验

报告评分： 教师签字：

**一、实验概要**

**实验目的:**

DNS把主机名转化为IP地址，从根服务器，顶级服务器到权威服务器形成树形的层次结构。



通过实验2-2，利用命令行参数访问不同的DNS服务器，理解DNS系统的结构及其作用。

**实验内容**：

使用nslookup工具将DNS查询发送到指定的DNS服务器，分析返回结果。使用ipconfig工具查询网络信息并进行删除缓存等操作。依照指导书进行实验，分析请求，响应报文，学习相关知识。

**二、实验步骤、数据及分析结果**

**实验步骤:**

1**.nslookup**

Run nslookup to obtain the IP address of a Web server in Asia.

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

Europe.

Run nslookup so that one of the DNS servers obtained in Question 2 is queried for

the mail servers for Yahoo! mail.

**2. Tracing DNS with Wireshark**

Use *ipconfig* to empty the DNS cache in your host.

Open your browser and empty your browser cache. (With Internet Explorer,

go to Tools menu and select Internet Options; then in the General tab select

Delete Files.)

Open Wireshark and enter “ip.addr == your\_IP\_address” into the filter, where

you obtain your\_IP\_address with ipconfig. This filter removes all packets that

neither originate nor are destined to your host.

Start packet capture in Wireshark.

With your browser, visit the Web page: http://www.ietf.org

Stop packet capture.

Start packet capture.

Do an *nslookup* on www.mit.edu

Stop packet capture.

repeat the previous experiment, but instead issue the command:

nslookup –type=NS mit.edu

repeat the previous experiment, but instead issue the command:

nslookup www.aiit.or.kr bitsy.mit.edu

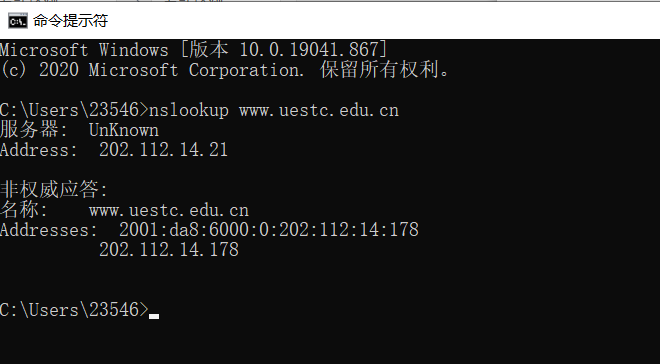
**实验数据及分析:**

问题1-3：

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

address of that server?

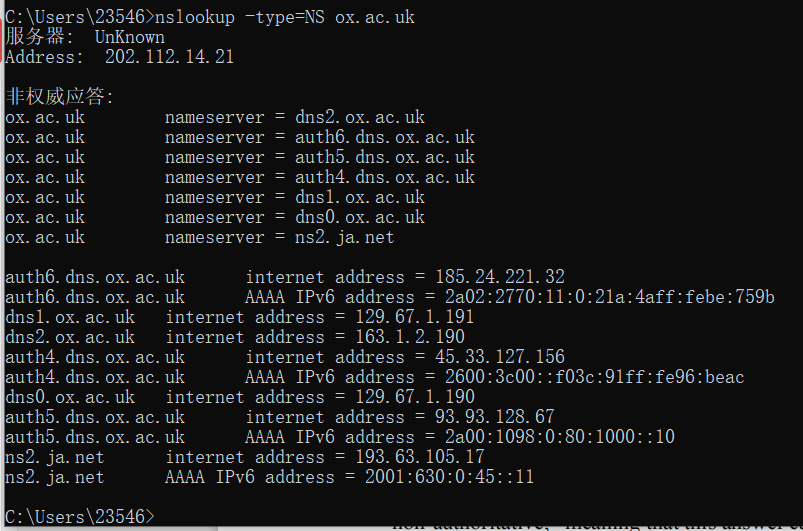
答：Web服务器为电子科技大学，IP地址包括IPV4：202.112.14.78，IPV6：2001：da8:6000:0:202:112:14:178。由于电脑存在缓存，所以为非权威应答，截图如下。



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

Europe.

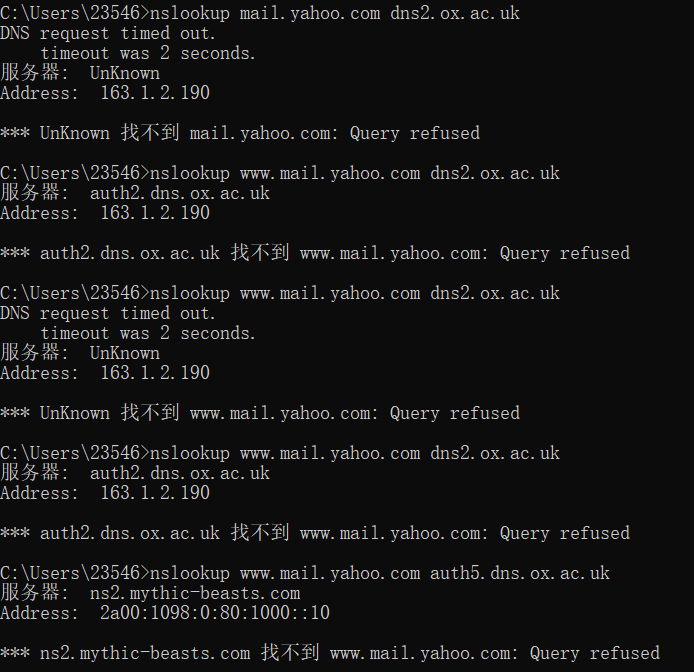
答：经查询后访问牛津大学的权威服务器，结果如下。共七个权威服务器，其中三个为IPV6地址，四个为IPV4地址。

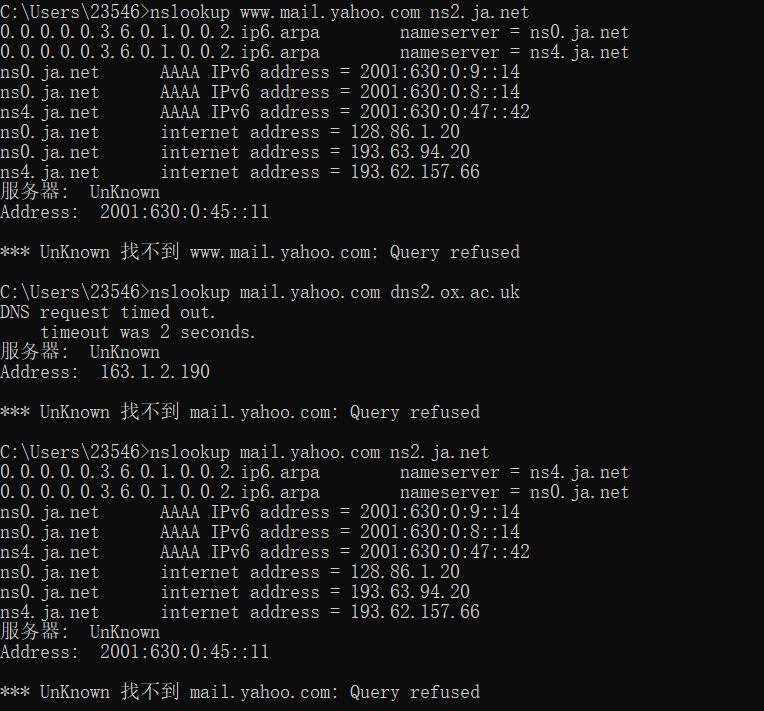


3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for

the mail servers for Yahoo! mail. What is its IP address?

答：使用牛津大学的所有服务器均无法找到yahoo邮箱的IP地址，服务器拒绝应答。但使用默认dns服务器查询到了yahoo邮箱地址，可能是其dns服务器禁止了递归查询以防止大量数据流影响正常服务。雅虎邮箱的IP地址包括两个IPV4地址与两个IPV6地址，截图如下。



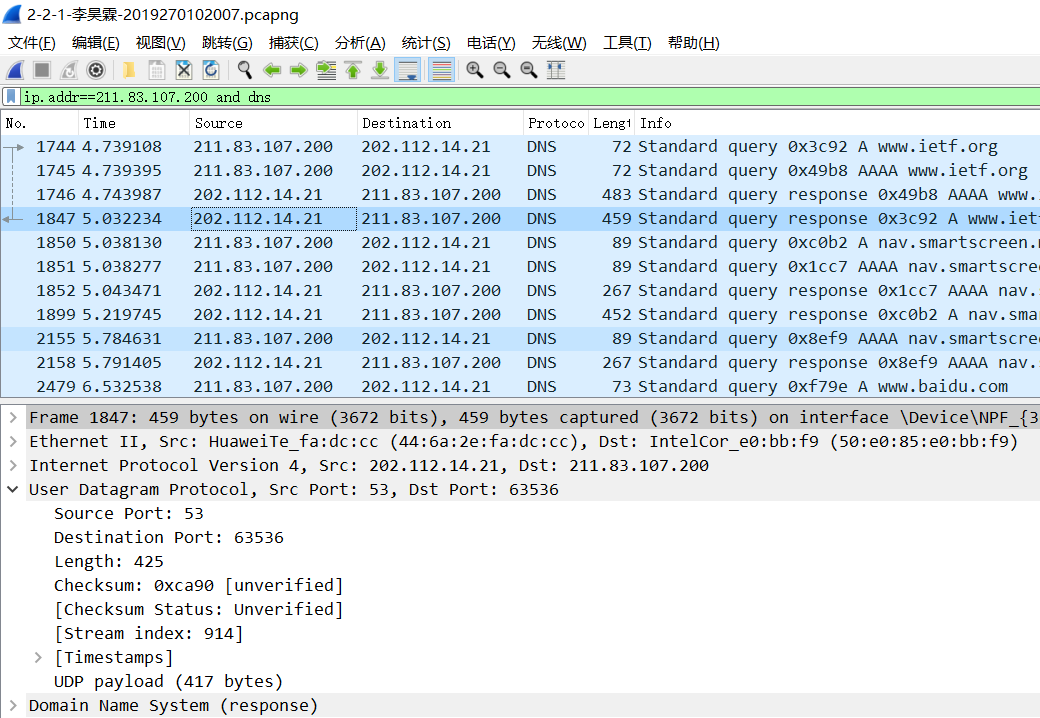




问题4-10：

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

答：如图，使用UDP协议，端口号为53.



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

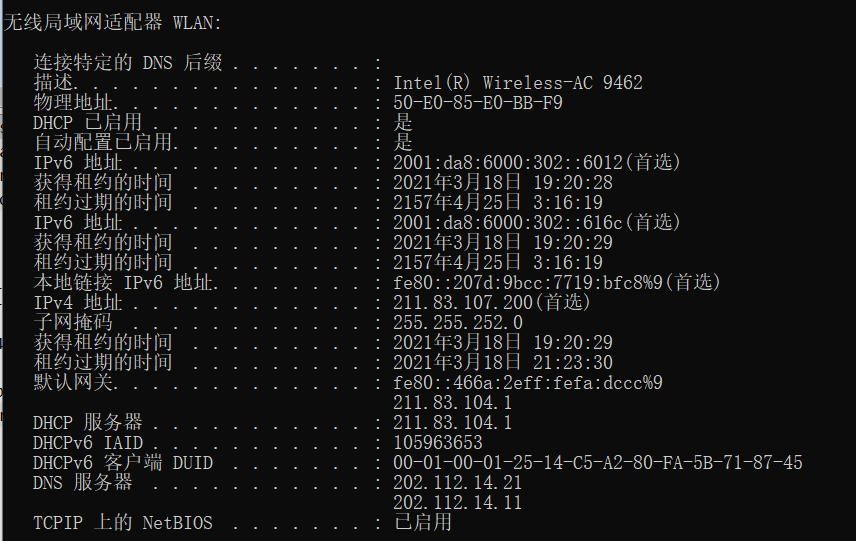
of DNS response message?

答：请求报文的目的端口与响应报文的源端口均为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?

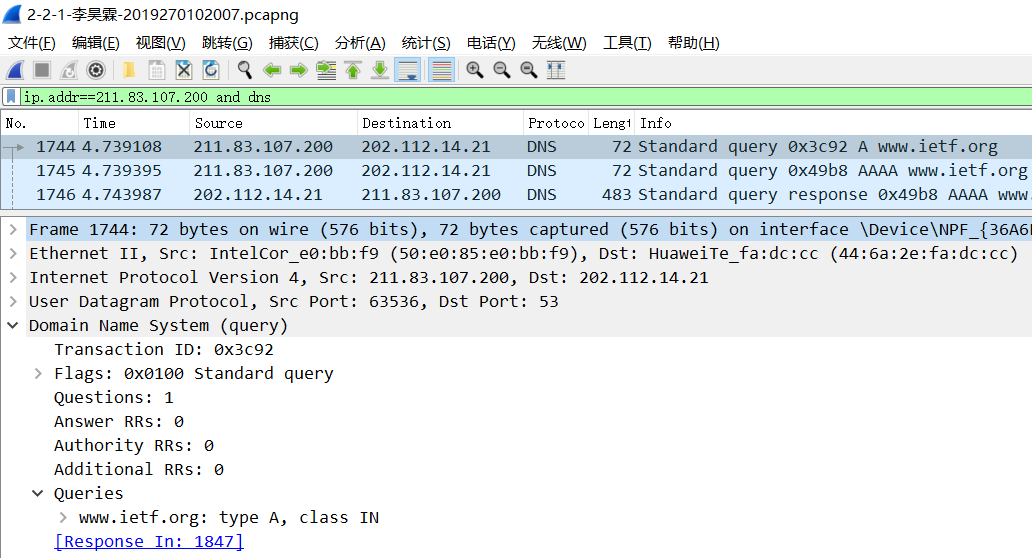
答：发送到IP地址：202.112.14.21即为本地DNS服务器。



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

query message contain any “answers”?

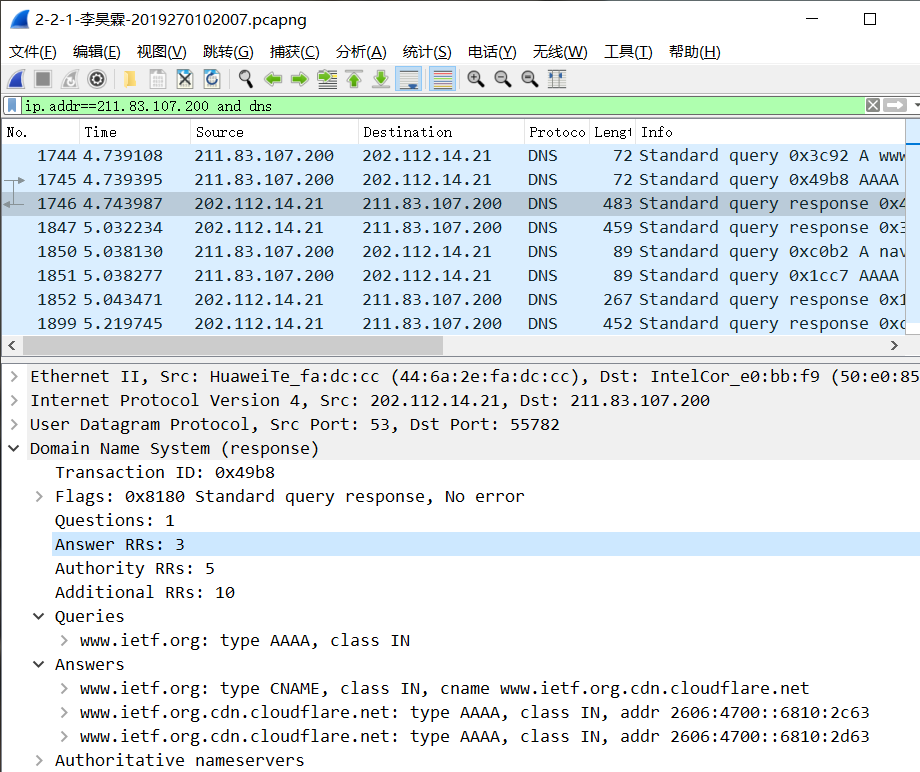
答：如图，请求类型type:A，answer数量0。



8. Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?

答：answer数量为3，分别为：一个cname别名记录，两个IPV6地址，服务提供商为Cloudflare。

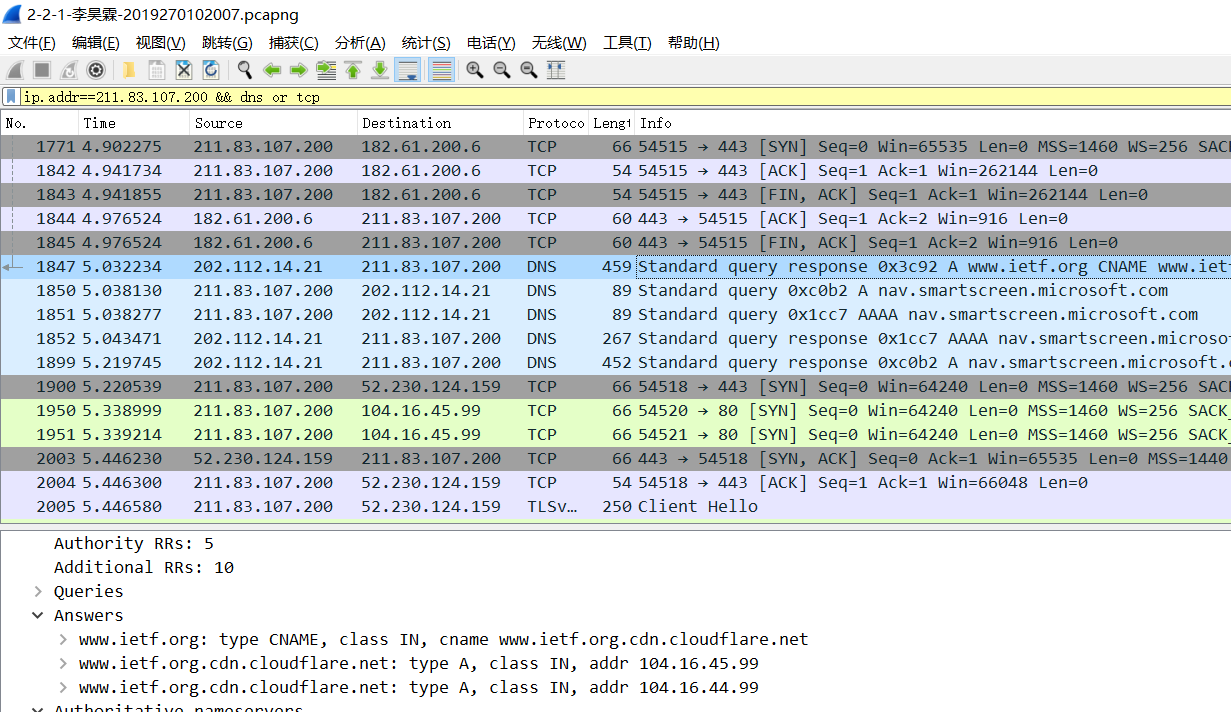


9. Consider the subsequent TCP SYN packet sent by your host. Does the destination

IP address of the SYN packet correspond to any of the IP addresses provided in

the DNS response message?

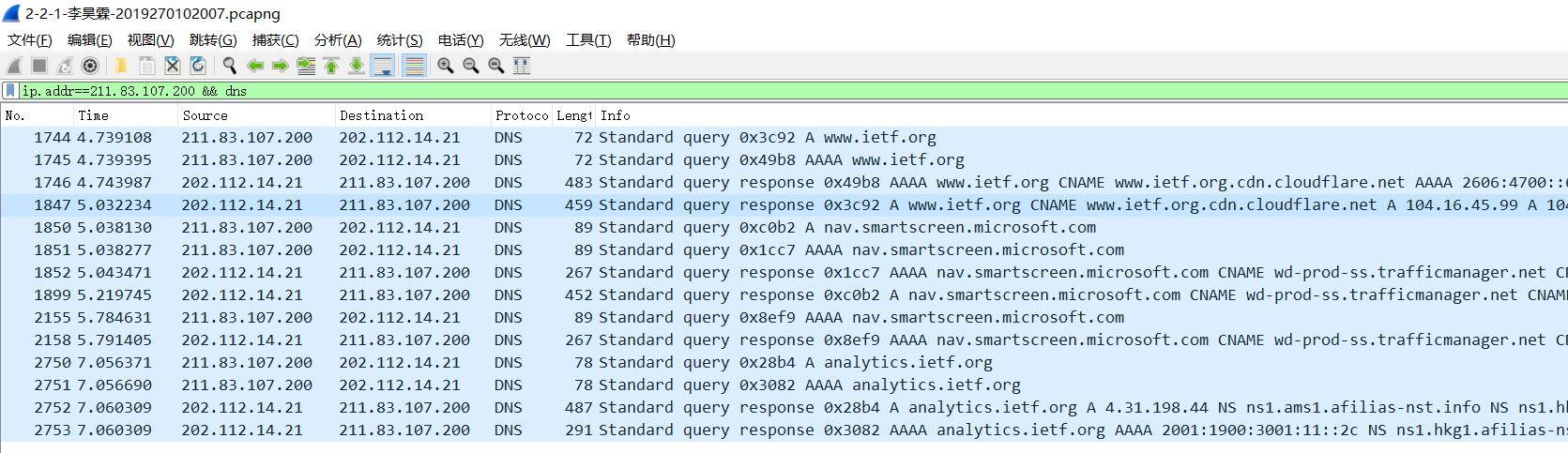
答：是对应的，如下图中DNS响应报文中返回的answer中的IP地址为104.16.45.99；可看到后续的TCP SYN数据包（绿色）的目的地址为该地址。



10. This web page contains images. Before retrieving each image, does your host

issue new DNS queries?

答：不是全部，部分重新发出请求。



问题11-15：

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

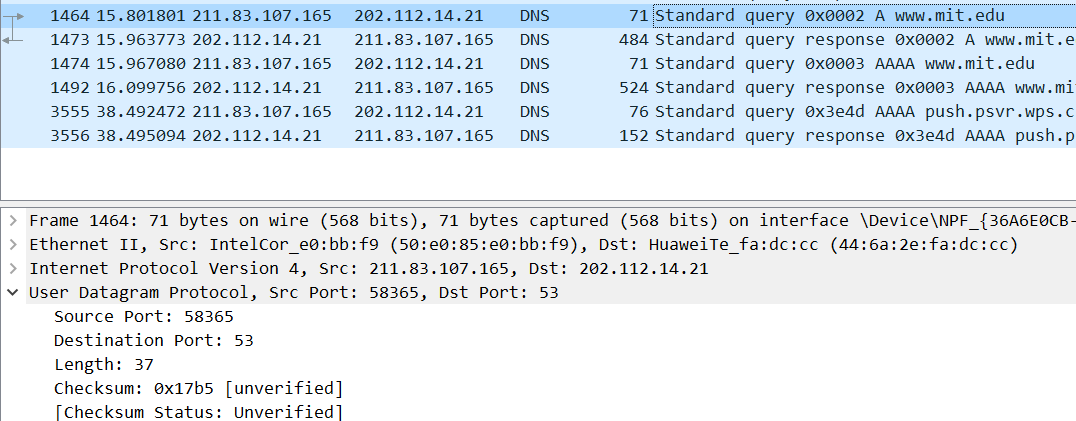
of DNS response message?

答：均为53。

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

default local DNS server?

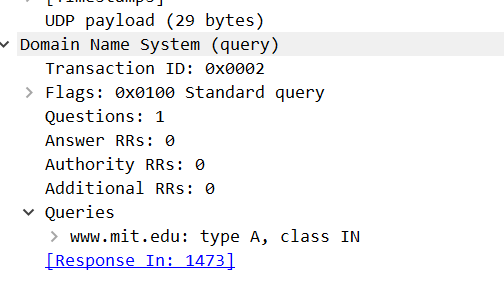
答：地址202.112.14.21，是本地服务器。



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

query message contain any “answers”?

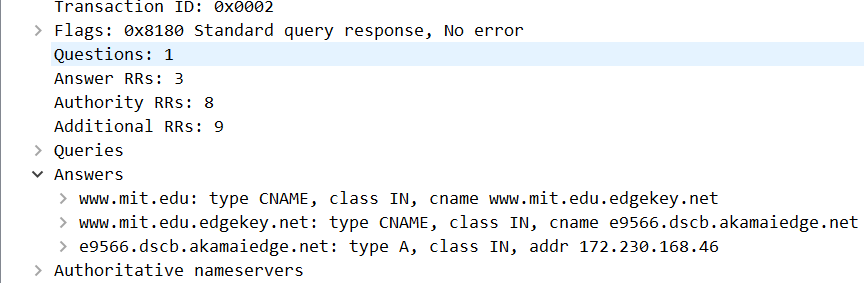
答：type:A，不包括answer。



14. Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?

答：3个answer，分别为：两个cname别名记录，一个IPV4地址。



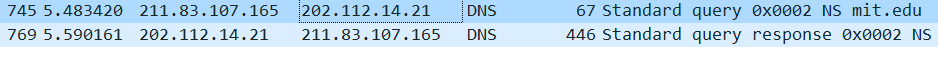
15. Provide a screenshot.

问题16-19：

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

default local DNS server?

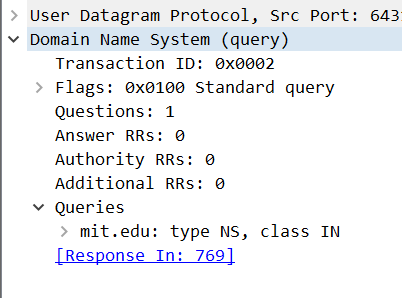
答：发送到202.112.14.21，即本地DNS服务器。



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

query message contain any “answers”?

答：类型为NS，不包含answer。

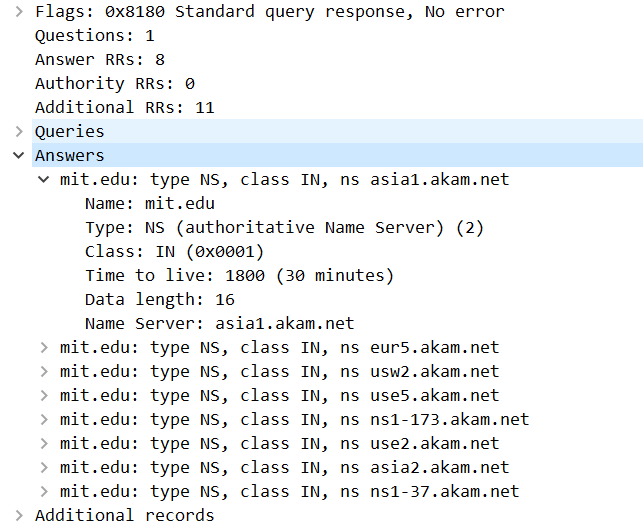


18. Examine the DNS response message. What MIT nameservers does the response

message provide? Does this response message also provide the IP addresses of the

MIT namesers?

答：提供了共8个MIT的权威服务器域名，没有提供相应的IP地址。



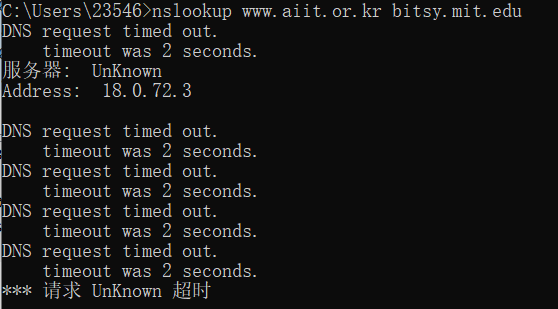
19. Provide a screenshot.

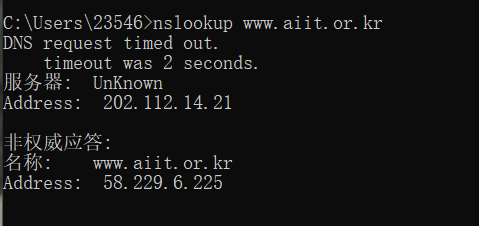
问题20-23：

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?

答：18.0.72.3，不是本地服务器地址，是MIT的权威服务器地址。这里使用该服务器无法得到应答，使用本地服务器得到了应答，如下图





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

query message contain any “answers”?

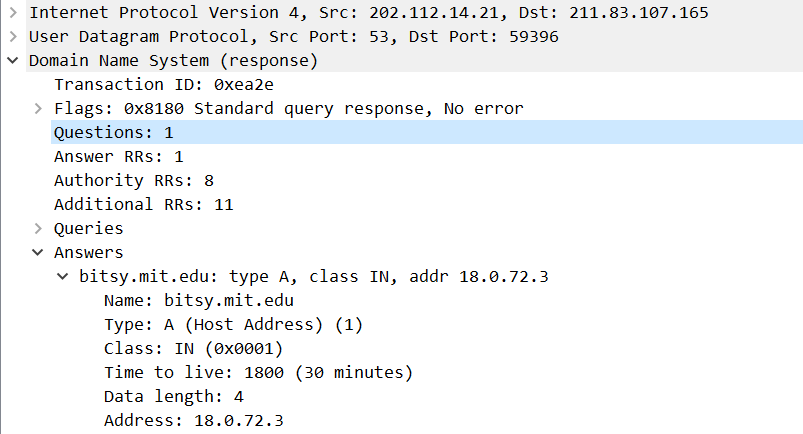
答：DNS请求包括向本地服务器请求的两条type=A类型，向MIT的DNS服务器请求的一条type=PTR类型（将IP反向解析为域名）以及两条type=A类型。均不包含answer。（每条A类型请求报文均跟随一条AAAA类型请求）



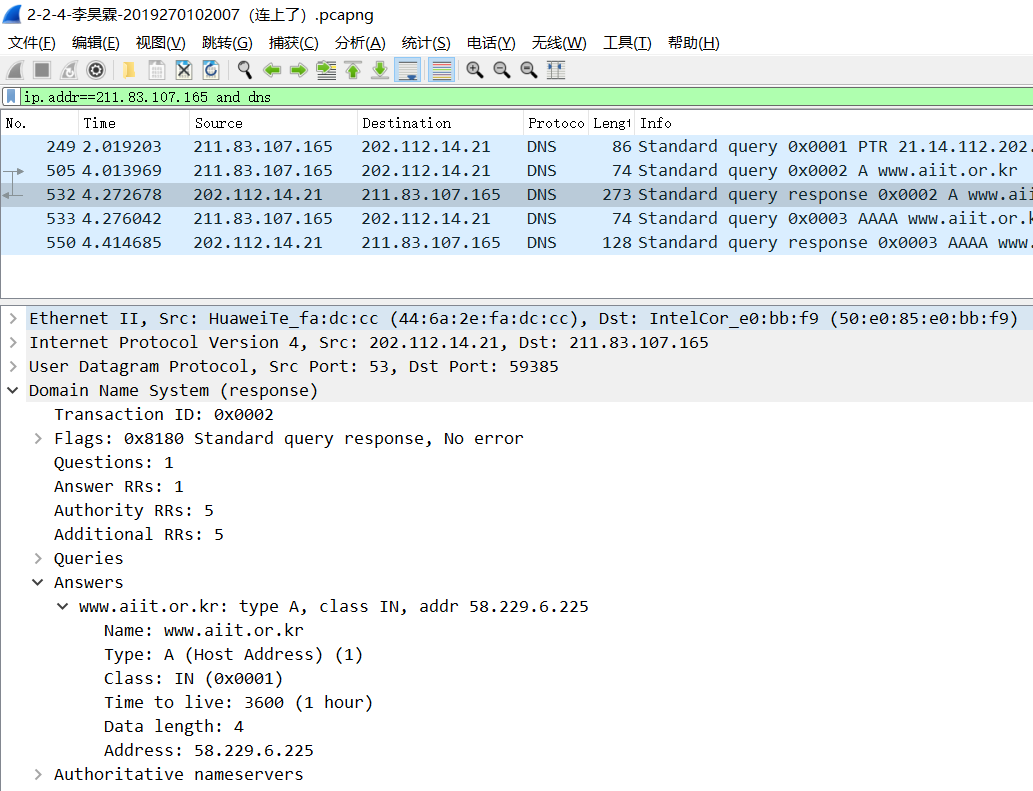
22. Examine the DNS response message. How many “answers” are provided? What

does each of these answers contain?

答：①无结果的MIT服务器：接收到本地服务器的响应报文，answer为要求的服务器的地址（18.0.72.3）；而MIT服务器响应超时，无响应报文。



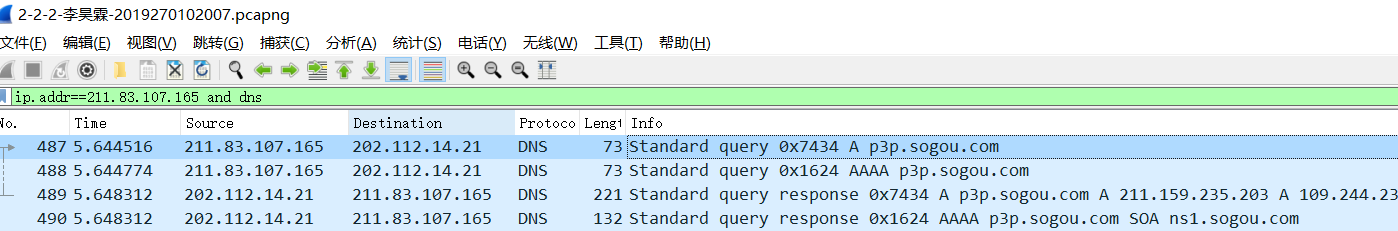
②有结果本地服务器：响应报文的answer为目标域名信息，IP地址为58.229.6.225。

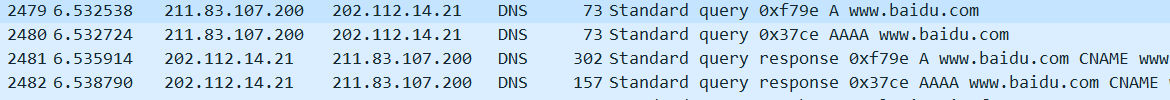


23. Provide a screenshot.

**三、总结及心得体会**

本次让我掌握了分析DNS请求，响应报文的基本方法，并学到了通过命令行参数连接不同的DNS服务器进行查询的方法；同时，在实验过程中，我还发现了在进行DNS查询的抓包时，其它正在使用的软件会产生影响如：搜狗输入法，见下图。还有不清空缓存带来多余报文的问题，如下图所示的百度的相关报文。





**四、对本实验过程及方法、手段的改进建议**

可以在问题设计上减少重复性的问题，对部分问题深入讨论，如不同报文类型的意义等。