**计算机网络DNS实验报告**

**姓名：陈鹤影 学号：PB21061287 日期：2022.10.7**

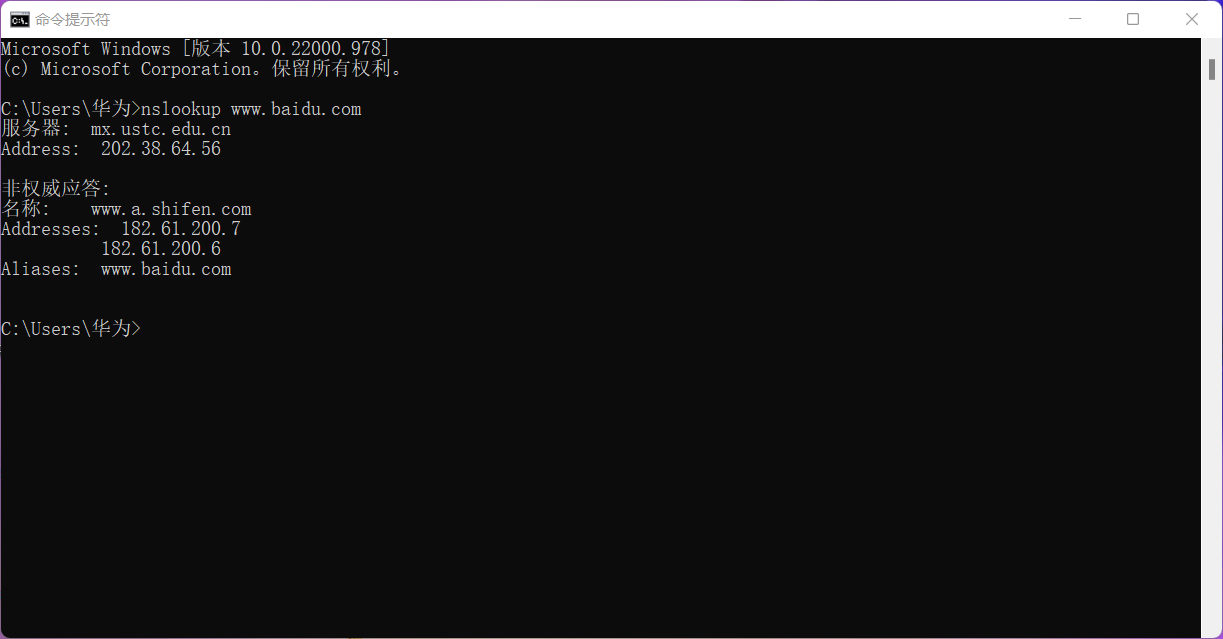
1. **实验目的：**
2. **熟练掌握nslookup和ipconfig的使用方法**
3. **体会不同的命令格式在域名解析过程中产生的区别**
4. **利用Wireshark抓包深入观察域名解析客户端的具体过程**
5. **实验流程及问题回答：**

**Part 1：nslookup**

**Q&A：**

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

**Ans：**实验中选择[www.baidu.com](http://www.baidu.com)作为需要查询的主机。实验结果如下：



**（图1-1 对[www.baidu.com](http://www.baidu.com)查询结果）**

可见[www.baidu.com](http://www.baidu.com)对应的IP地址有两个，分别为182.61.200.7和182.61.200.6。上述查询结果来自本地域名服务器mx.ustc.edu.cn。此外，上述结果是一个非权威应答，即来自某DNS服务器的缓存。查询IP信息可知，182.61.200.7和182.61.200.6对应主机均位于中国-北京-北京市-电信。

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

**Ans：**实验中选择剑桥大学的域cam.ac.uk发起查询。为查询cam.ac.uk域对应的权威DNS服务器，将nslookup置为-type=NS模式，查询结果如下：

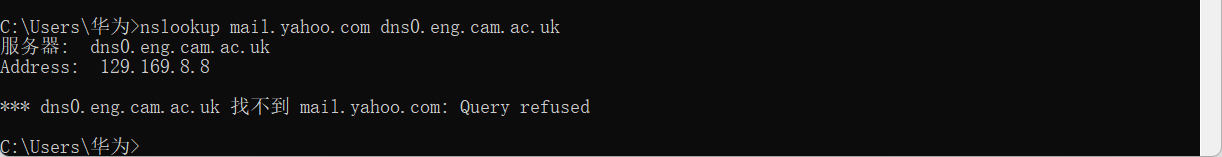


**（图1-2 对cam.ac.uk查询结果）**

对应有六个主机dns0.eng.cam.ac.uk、dns0.cl.cam.ac.uk、ns3.mythic-beasts.com、ns1.mythic-beasts.com、auth0.dns.cam.ac.uk、ns2.ic.ac.uk。

1. **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?**

**Ans：**这里向上述获得的第一个主机名dns0.eng.cam.ac.uk发起查询，查询mail.yahoo.com对应的IP地址，结果如下：



**（图1-3 对mail.yahoo.com查询结果）**

dns0.eng.cam.ac.uk主机上没有相关信息，显示找不到。用本地服务器查询后得知：

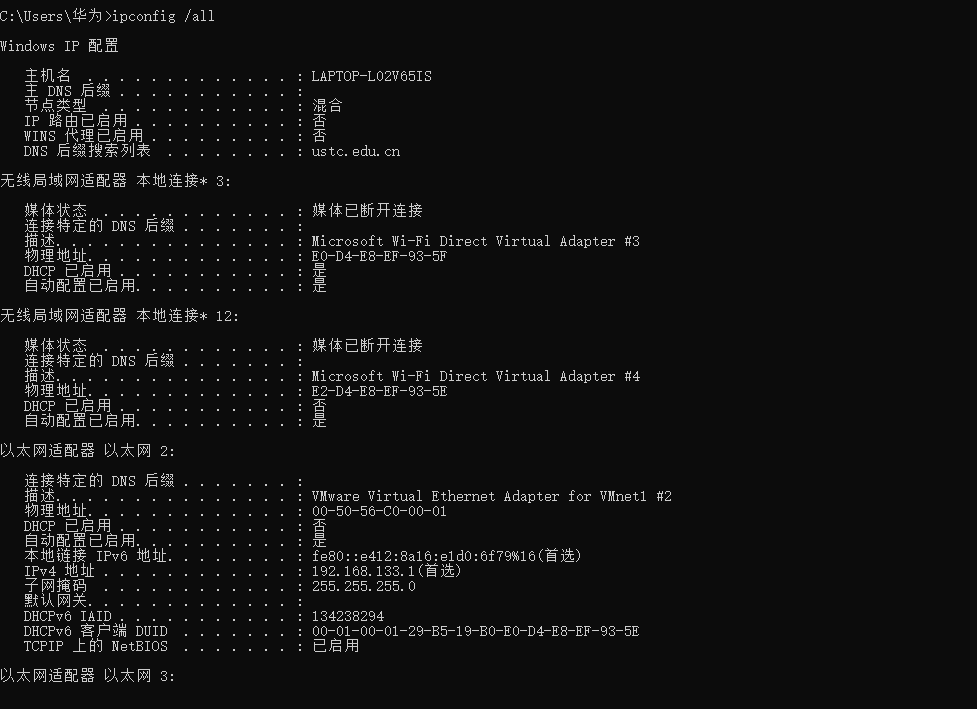


**（图1-4 用本地服务器对mail.yahoo.com查询结果）**

mail.yahoo.com对应多台主机，相应的的IP地址为2001:4998:64:800::6001、2001:4998:64:800::6000、69.147.80.15、69.147.80.12。

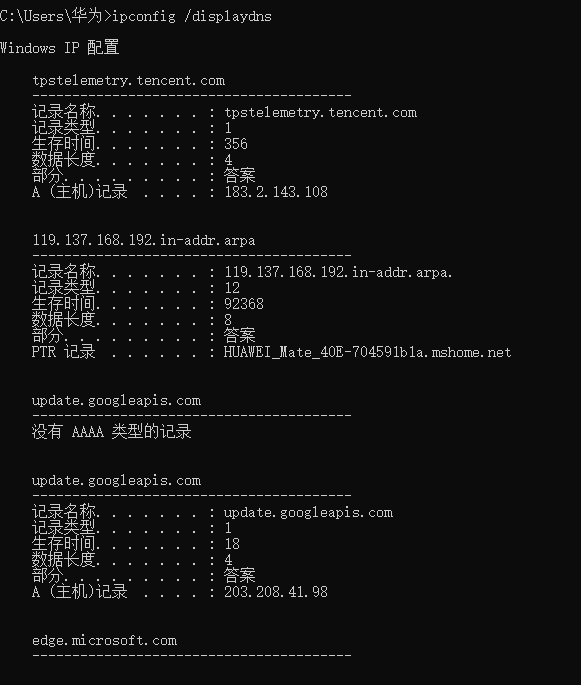
**Part 2：ipconfig**

利用ipconfig查看主机当前TCP/IP全部信息，使用ipconfig /all命令。实验结果如下：



**（图1-5 用ipconfig命令查看当前全部TCP/IP信息）**

利用ipconfig查看主机DNS缓存，使用ipconfig /displaydns命令。实验部分结果如下：



**（图1-6 用ipconfig命令查看主机DNS缓存信息）**

利用ipconfig清除主机DNS缓存，使用ipconfig /flushdns命令。

**Part 3：Tracing DNS with Wireshark**

**Step 1：使用ipconfig命令清除主机DNS缓存** 结果如下：



**（图1-7 用ipconfig命令清除主机DNS缓存信息）**

**Step 2：清除浏览器缓存**

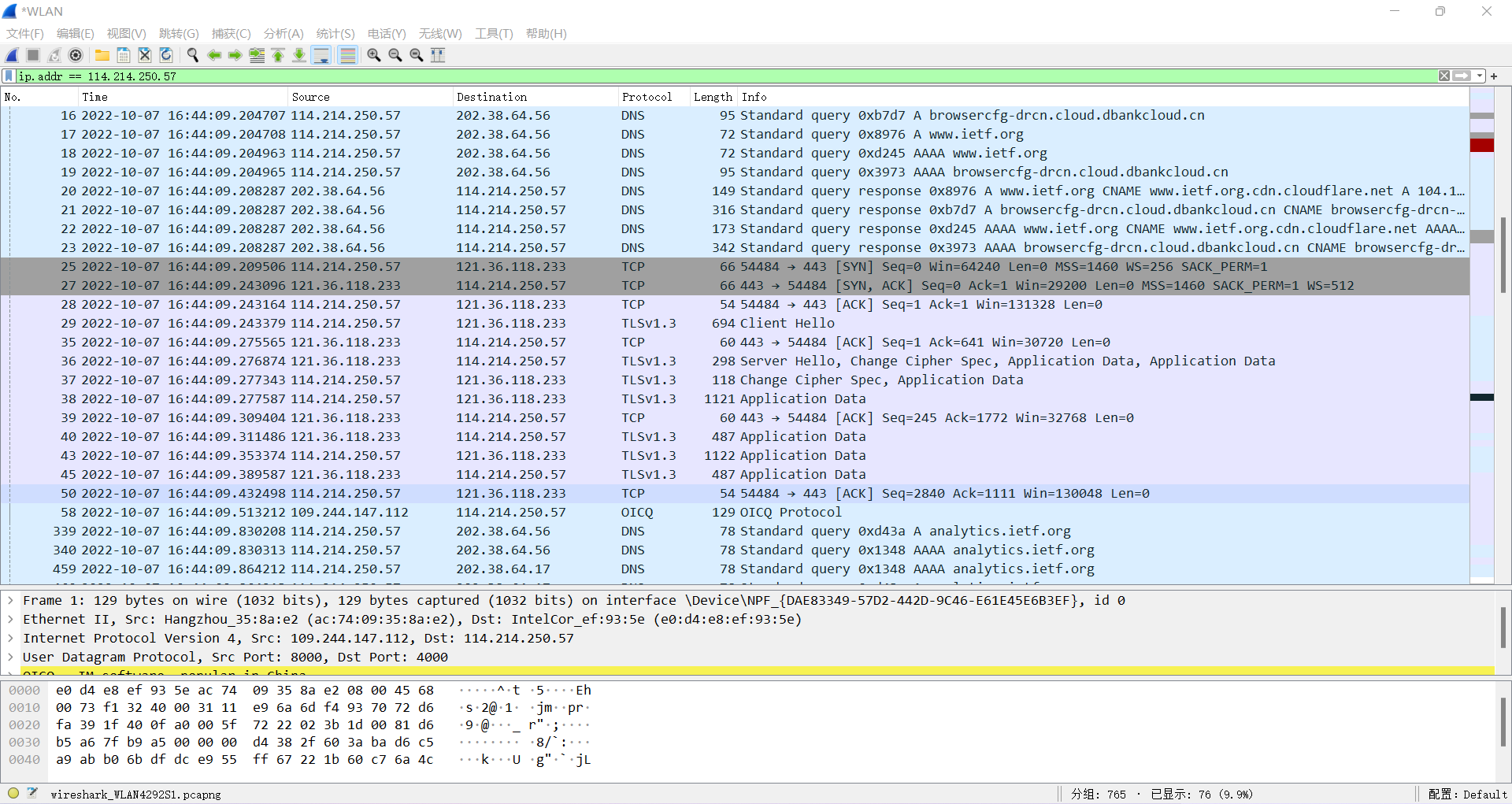
**Step 3：启动Wireshark选择地址过滤**

由ipconfig /all可知，主机iPv4地址为114.214.250.57。

**Step 4：启动Wireshark抓包，在浏览器端访问Web网页：http：//www.ietf.org**

**Step 5：停止抓包**

实验结果如下：

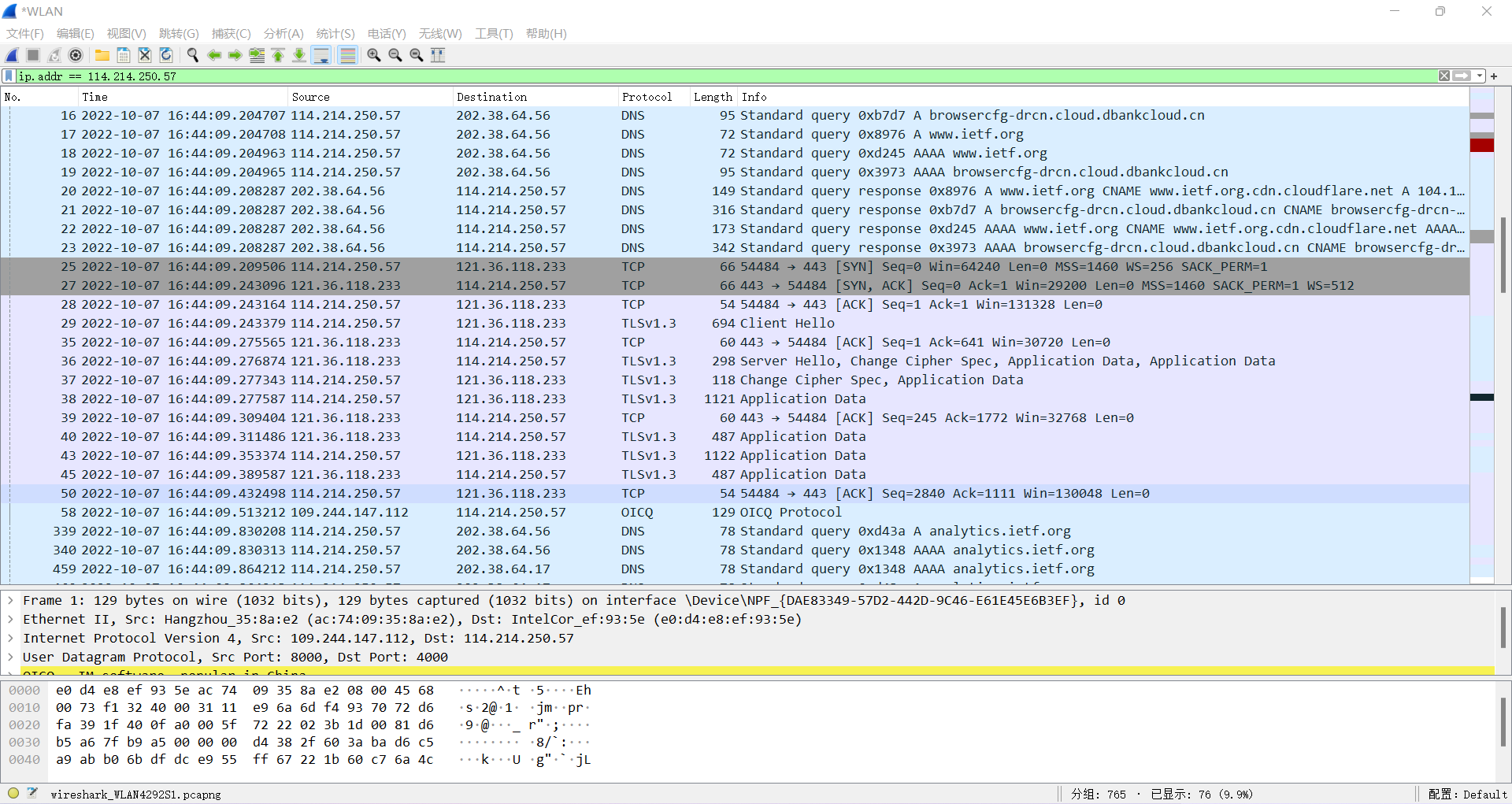


**（图1-8 Wireshark抓包结果）**

**Q&A：**

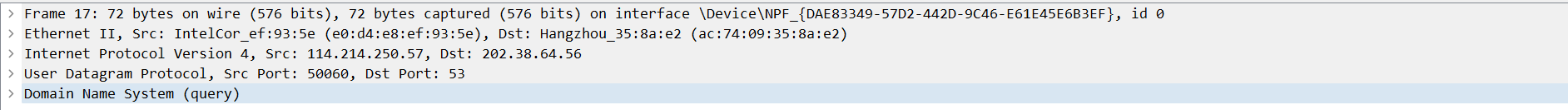
1. **Locate the DNS query and response messages. Are then sent over UDP or TCP?**

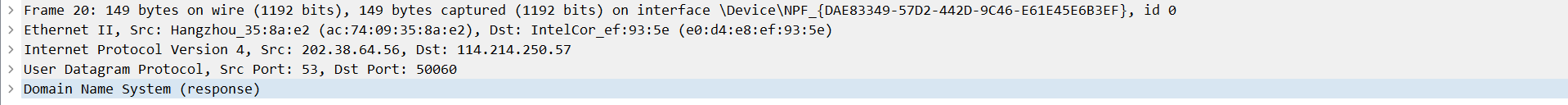
**Ans：**DNS请求和相应报文位置如下：



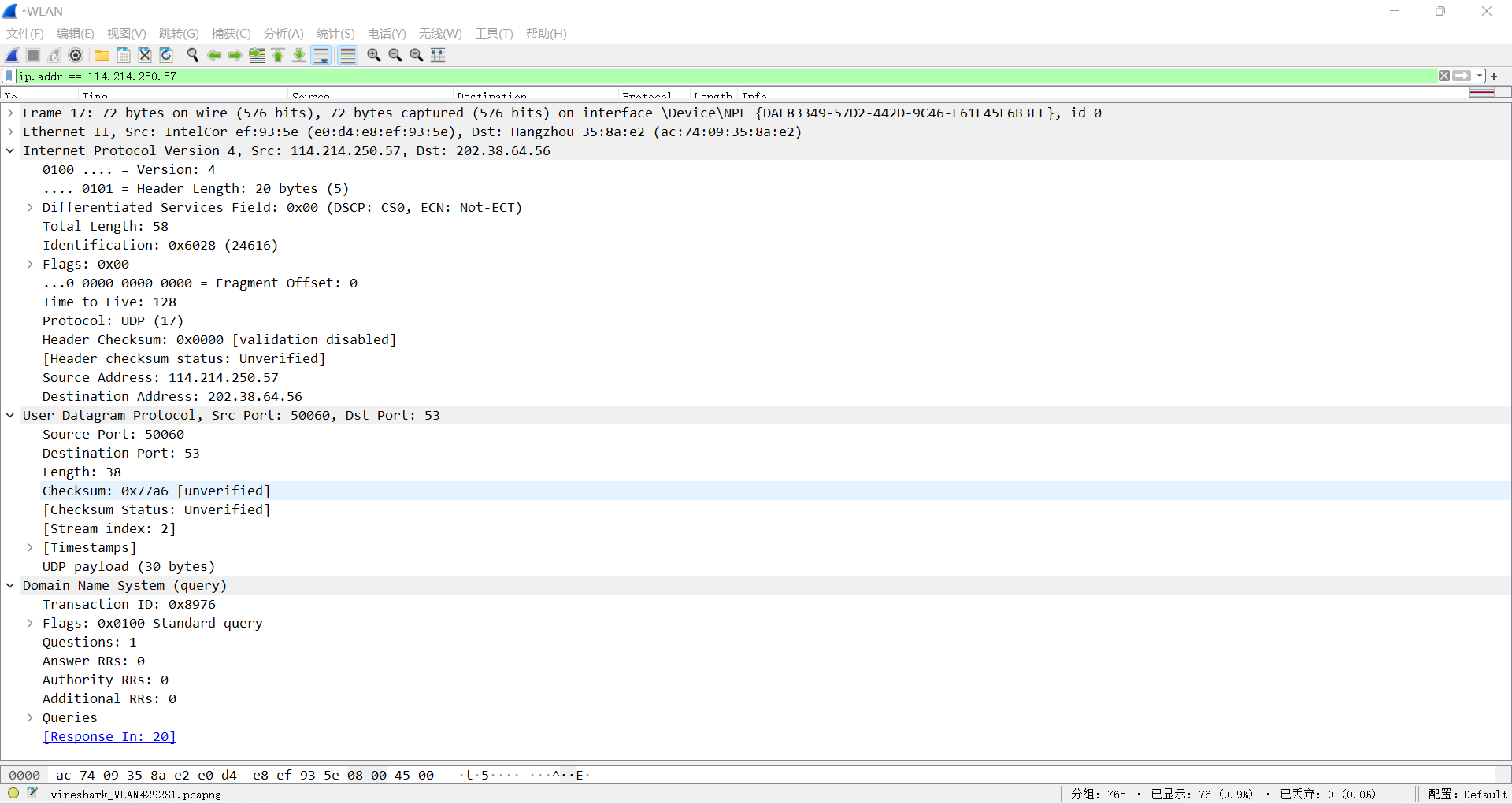
**（图1-9 请求响应报文位置）**

他们均使用UDP协议。

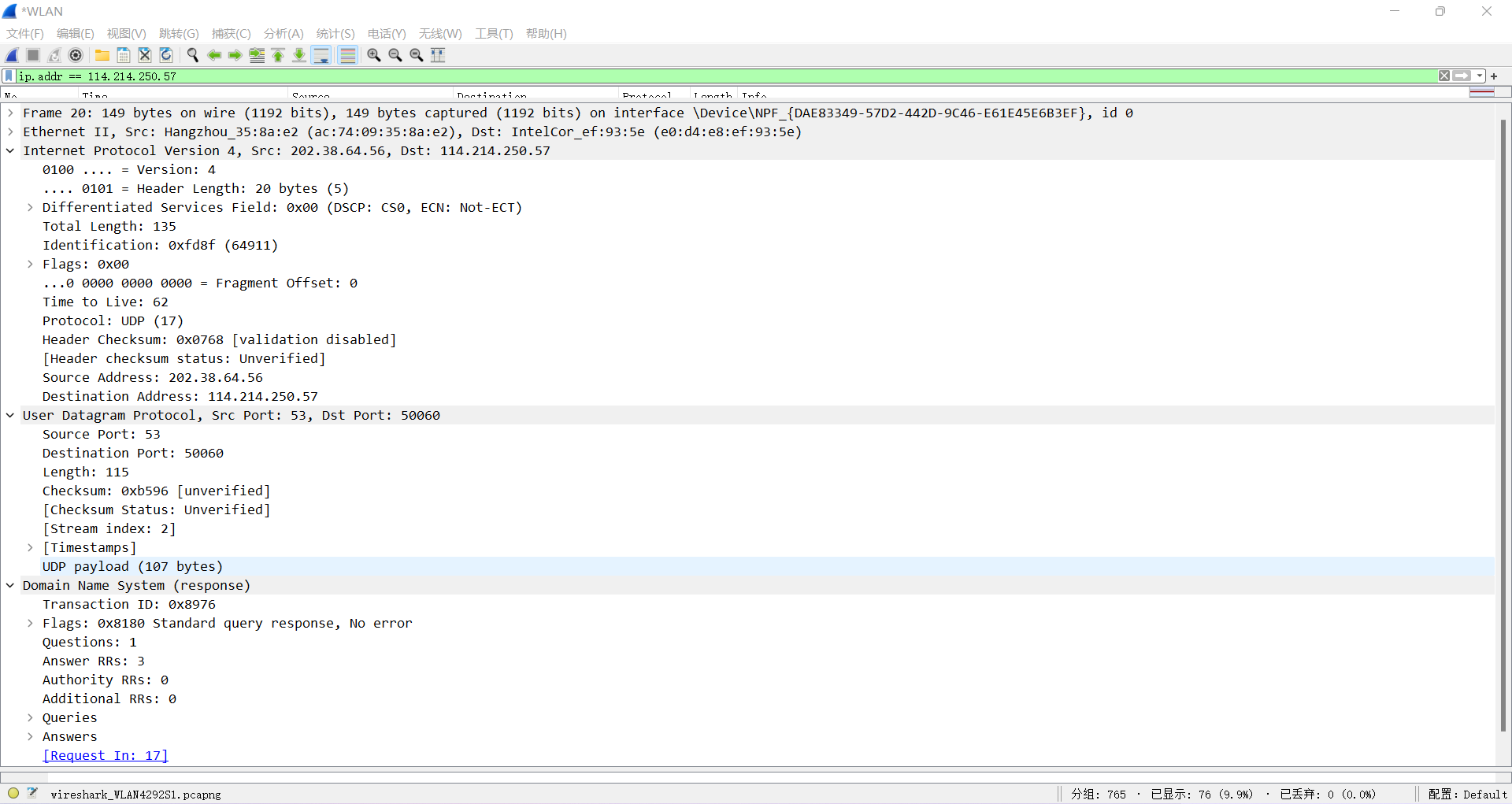




报文具体内容如下：



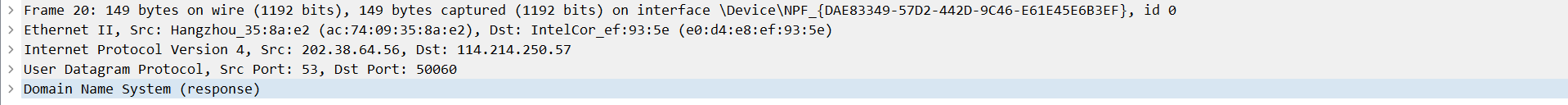
**（图1-10 请求报文内容）**

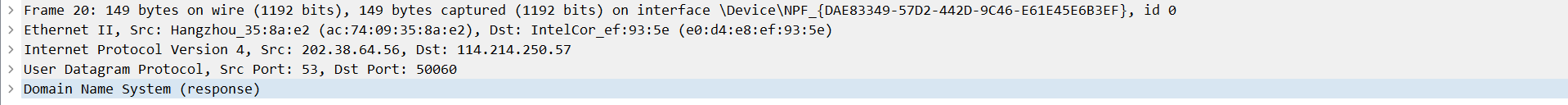


**（图1-11 响应报文内容）**

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

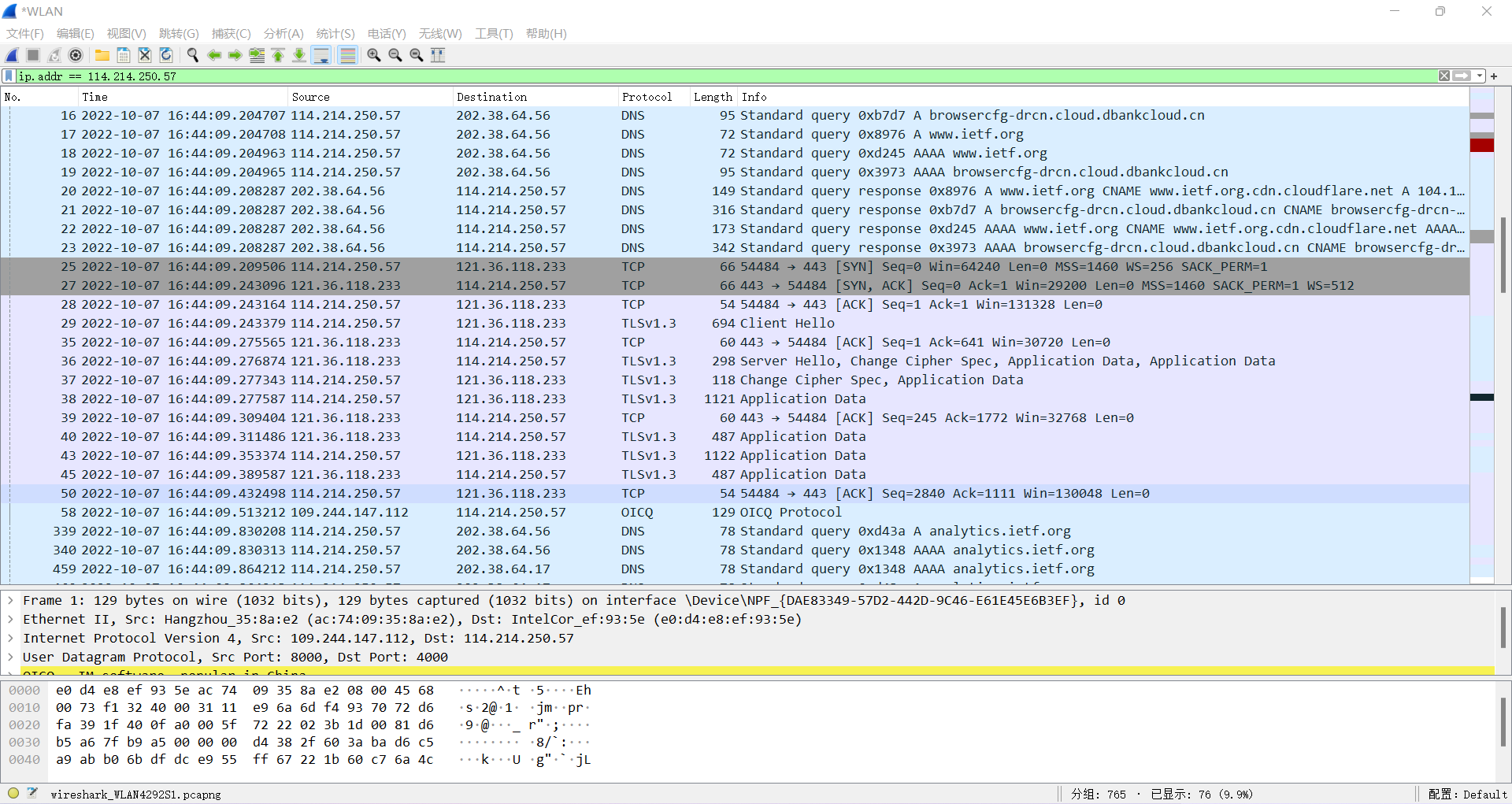
**Ans：**请求报文的目的端口为：53；响应报文的源端口为：53.



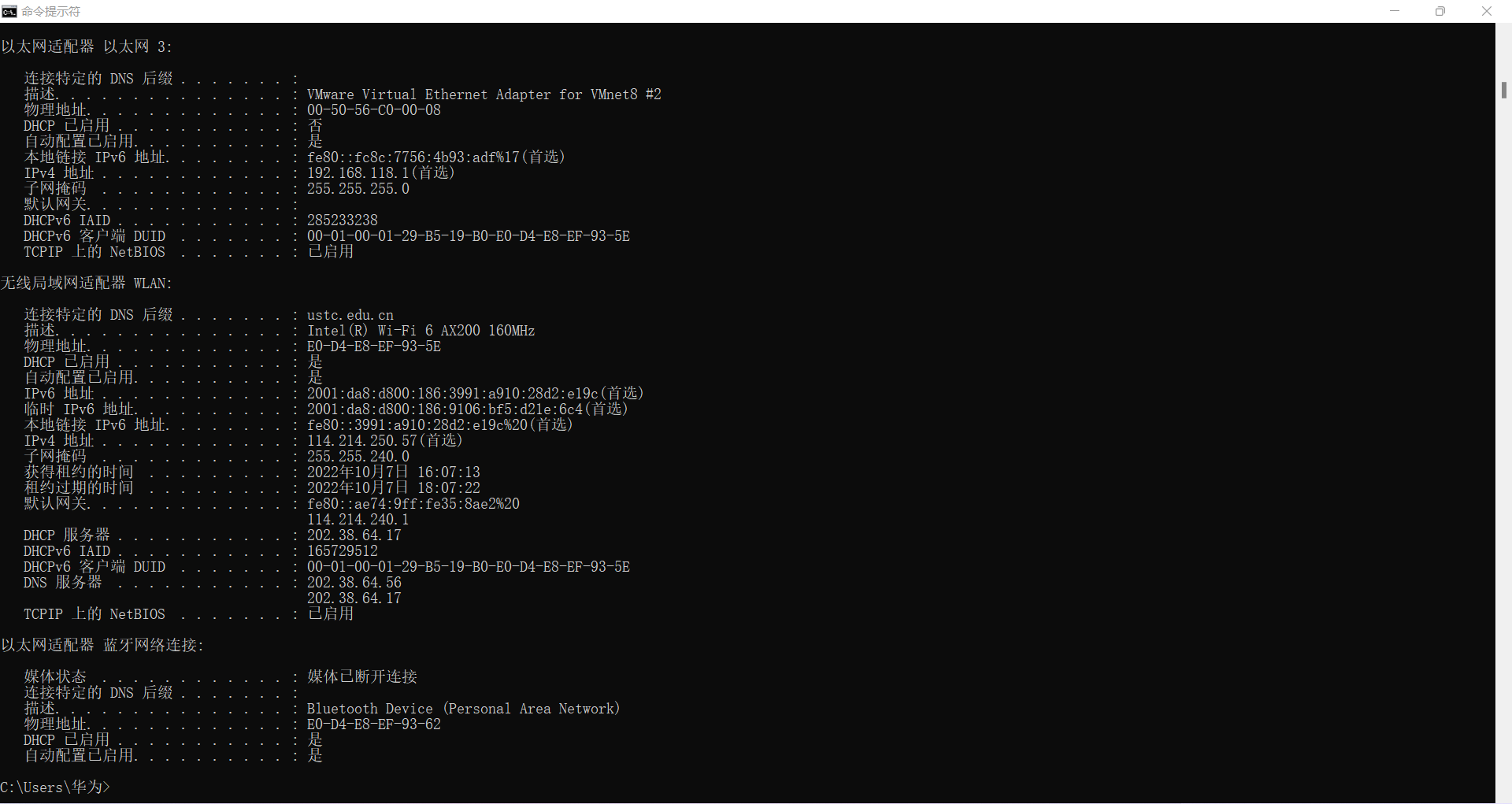


1. **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

**Ans：**请求报文的目的IP地址202.38.64.56。

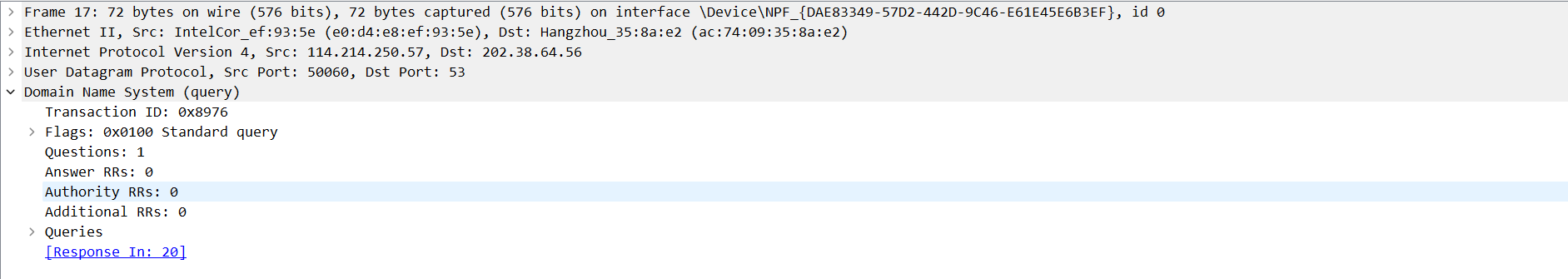


用ipconfig查询到本地DNS服务器的IP地址为202.38.64.56。两者一致。



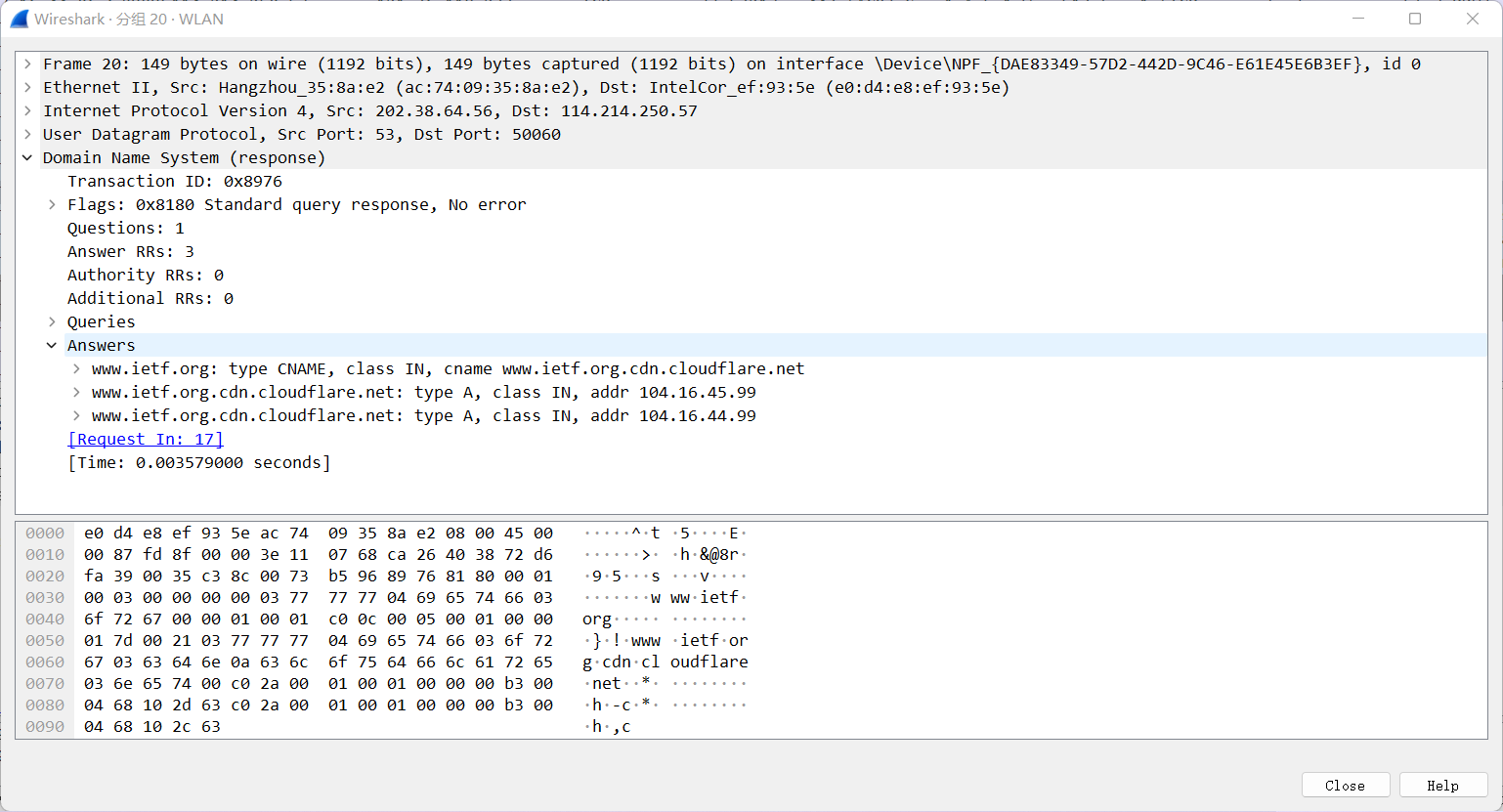
1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

**Ans：**请求报文的类型为A类型，报文中没有包含任何“answers”。



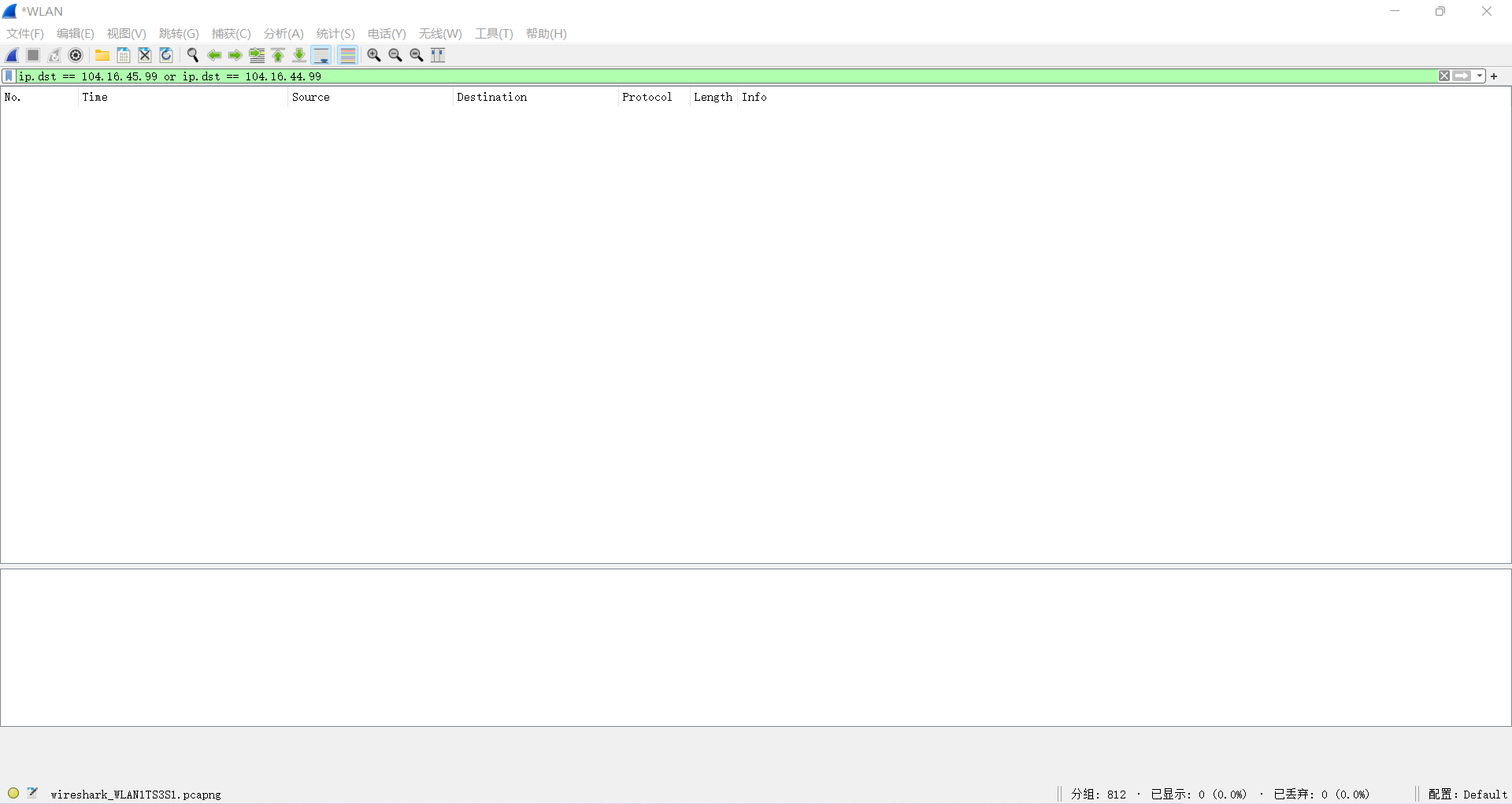
1. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

**Ans：**一共有3条answers；第一条answer包括[www.ietf.org](http://www.ietf.org)对应的标准名（type = CNAME），后两条包含对应主机的iPv4地址(type = A)。

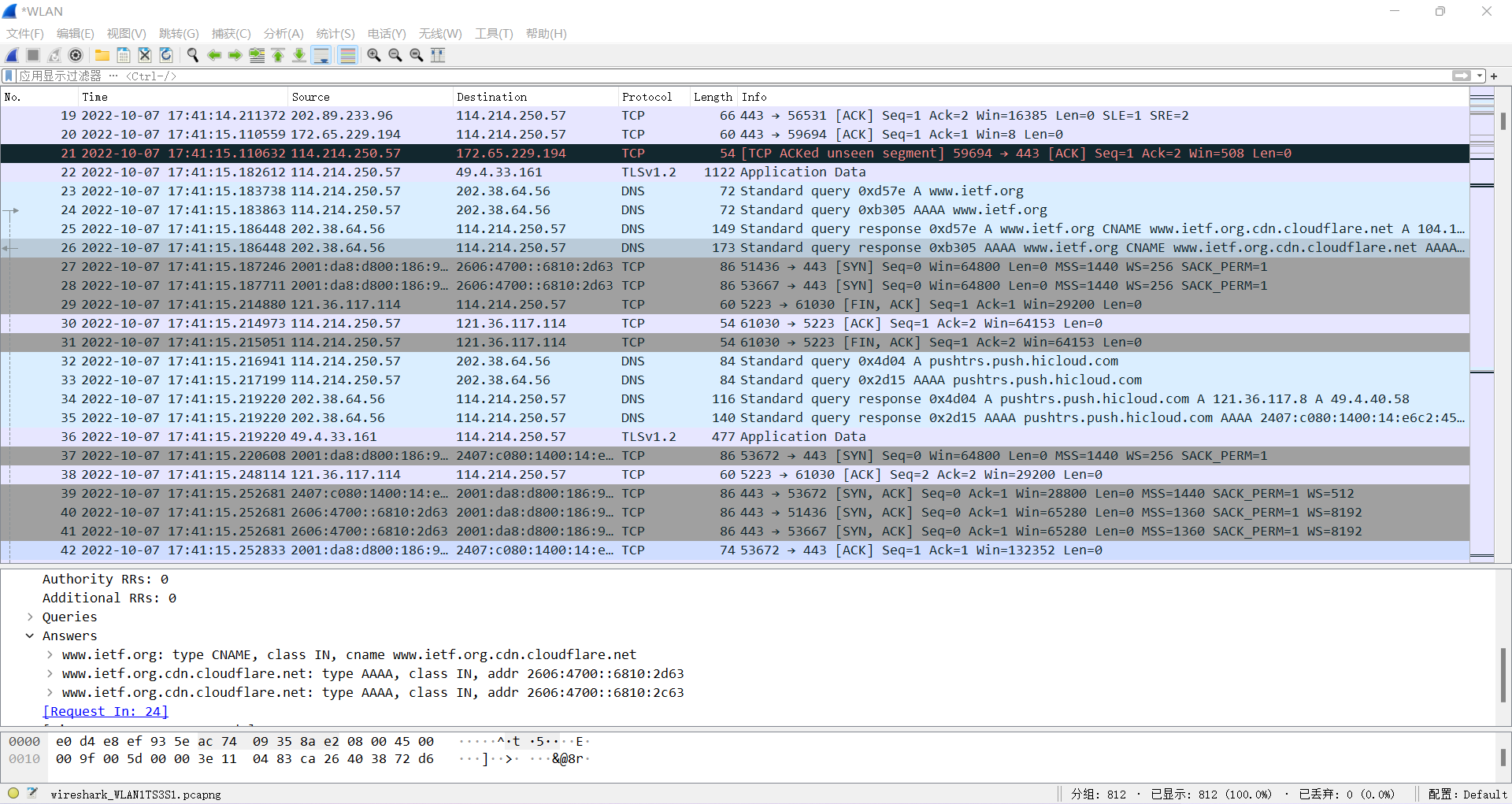


1. **Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

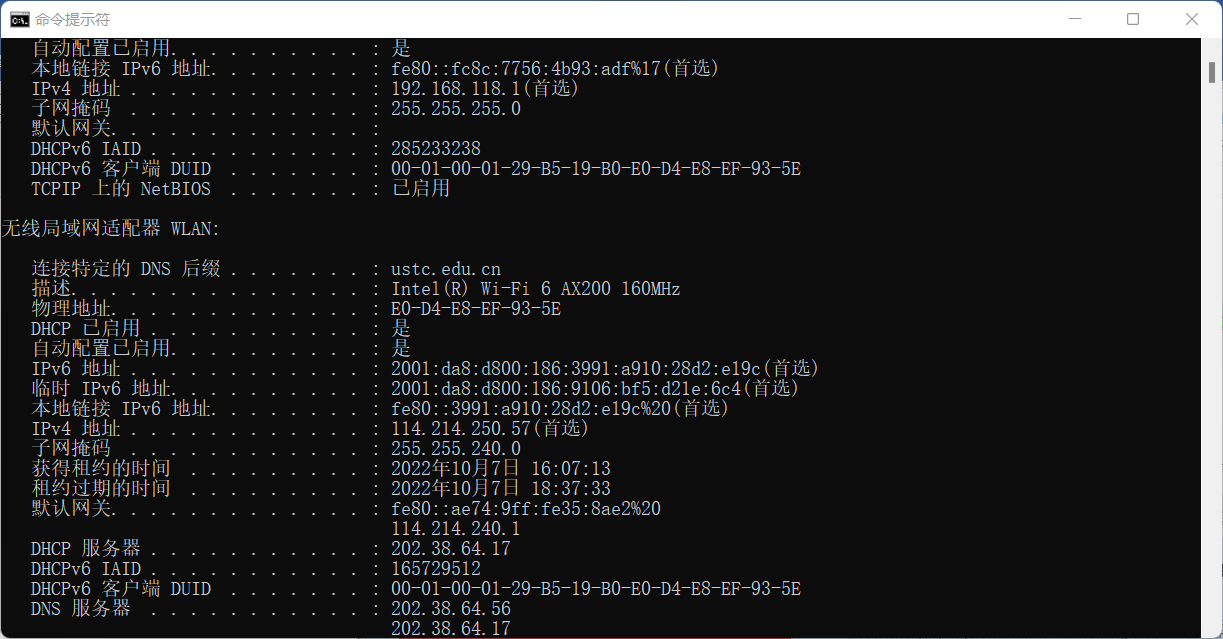
**Ans：**并未找到对应上述iPv4地址的TCP SYN packet。



但观察后发现可以找到对应AAAA响应返回的iPv6地址的TCP SYN packet：

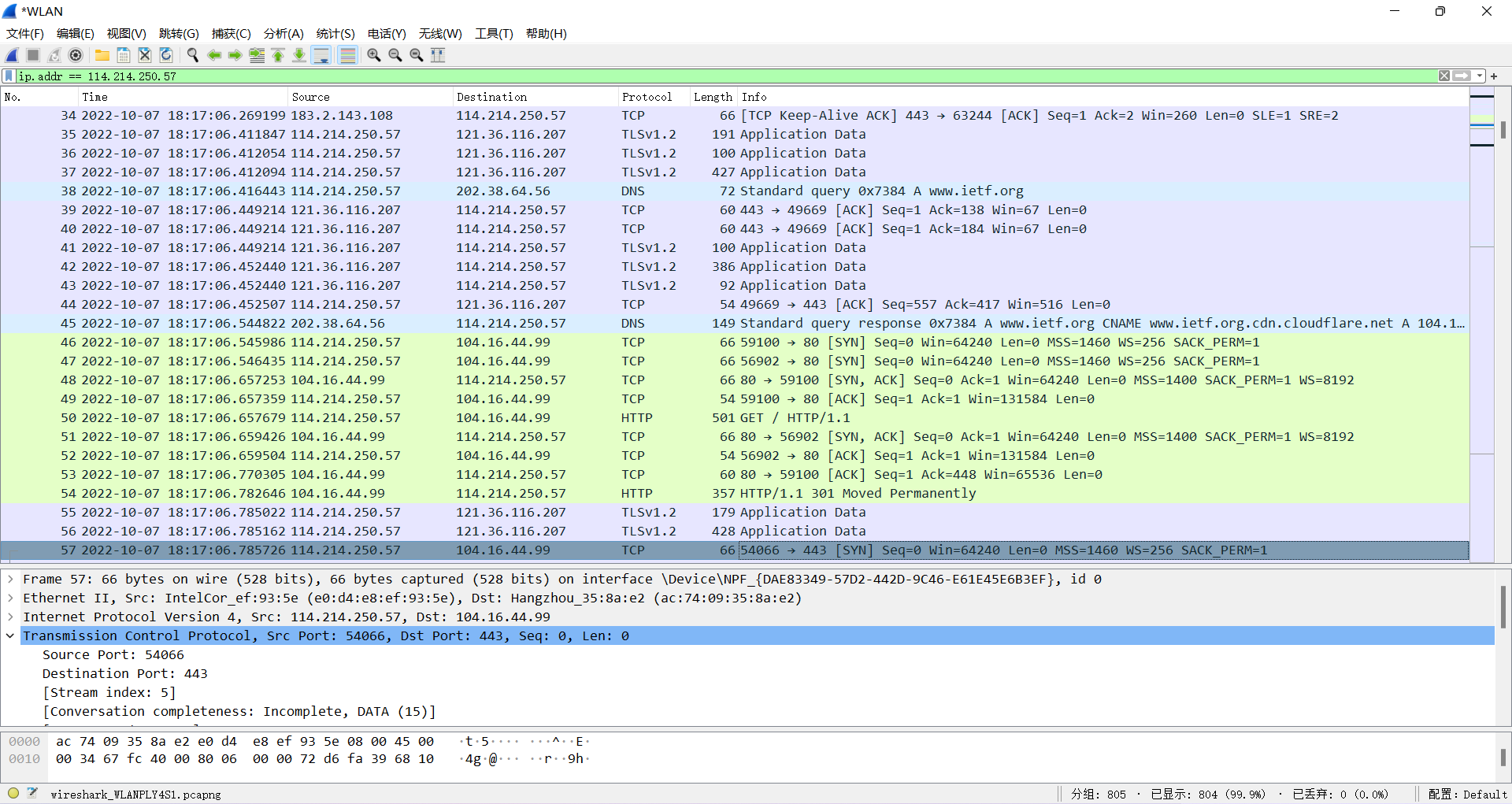


且源地址与主机iPv6地址一致：



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

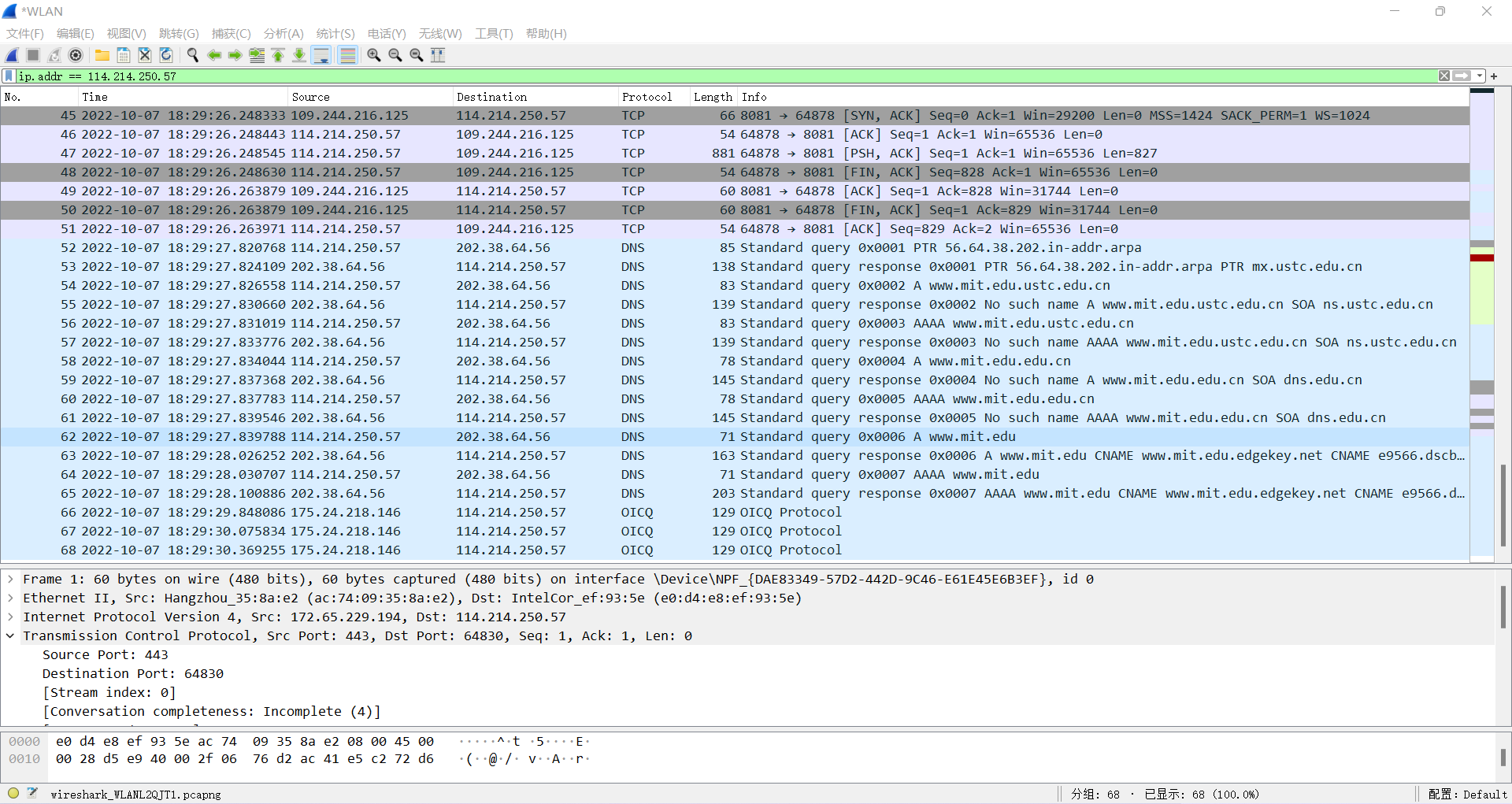
**Ans：**为避免iPv6对实验的影响，后续实验关闭iPv6重新进行。实验结果如下：



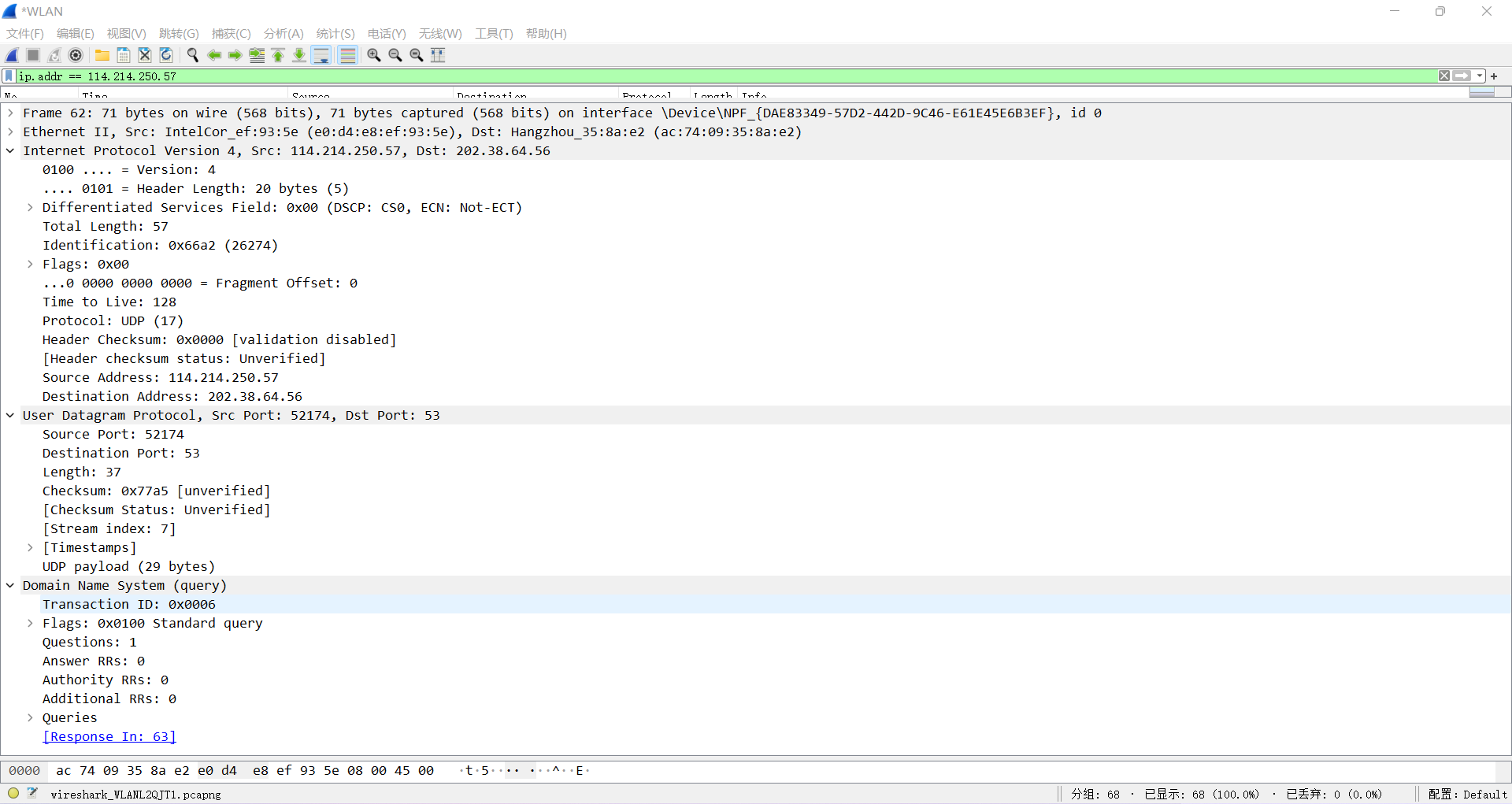
在后续检索过程中并未发送新的DNS请求，原因可能是本地DNS缓存了对应的IP地址。

**Step 6：利用nslookup查询www.mit.edu的IP地址，并抓包**

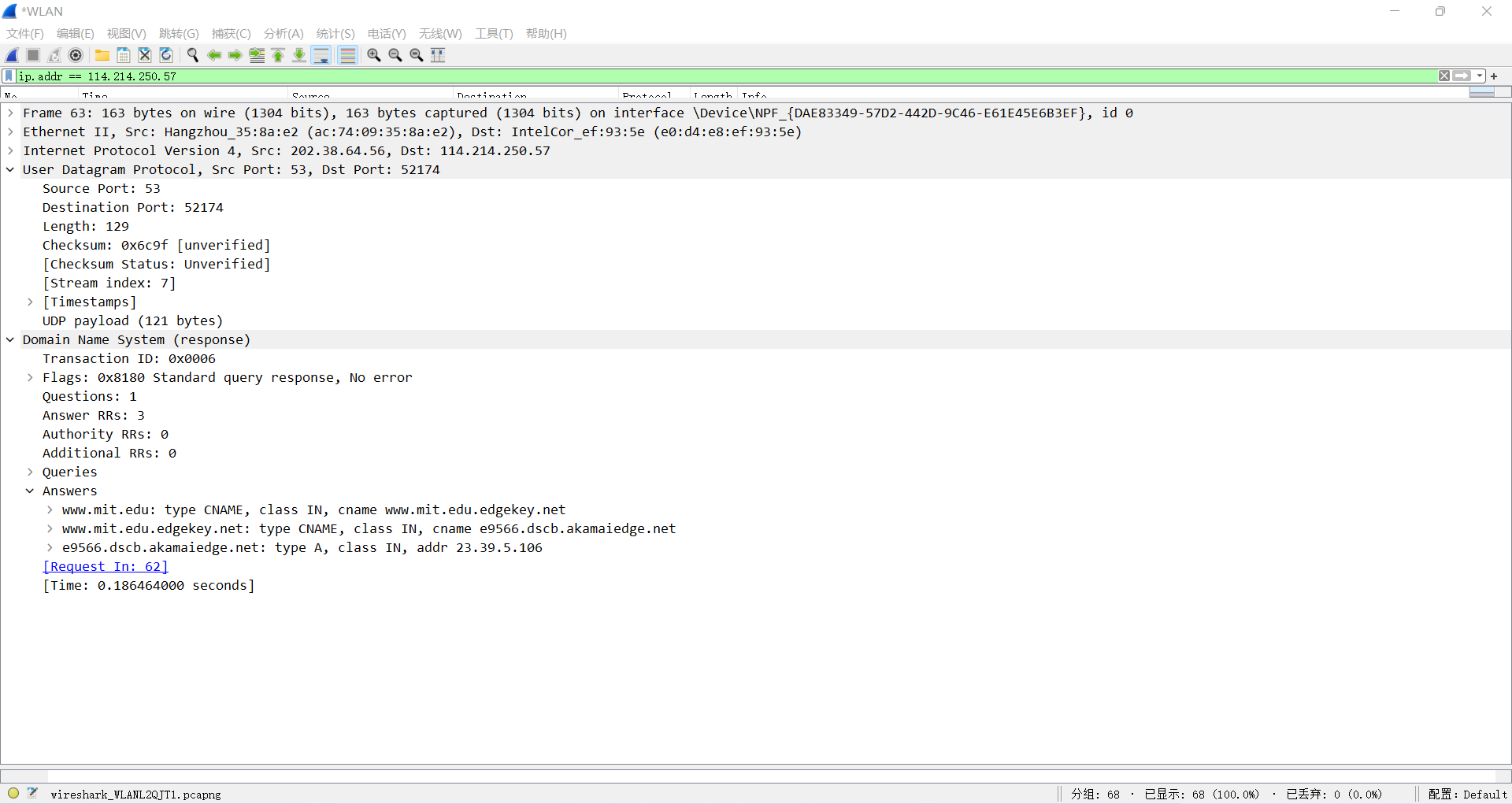
实验结果如下：



**（图1-12 对nslookup抓包结果）**



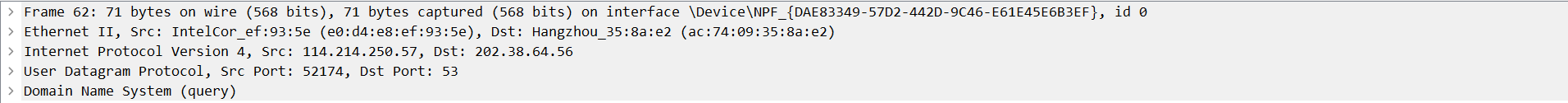
**（图1-13 请求报文内容）**

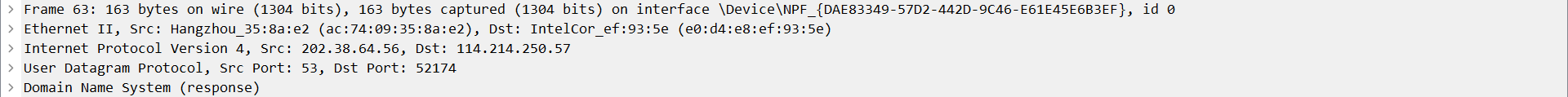


**（图1-14 响应报文内容）**

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

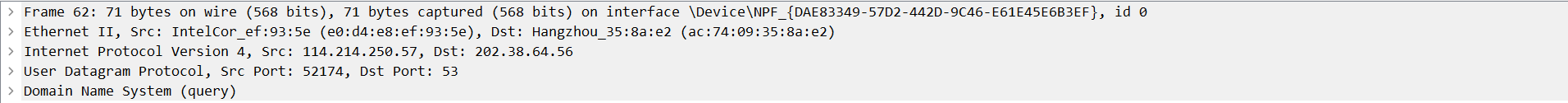
**Ans：**DNS请求报文的目的端口为：53；DNS响应报文的源端口为：53。

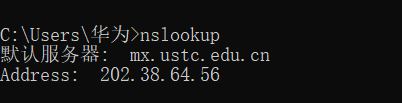




1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

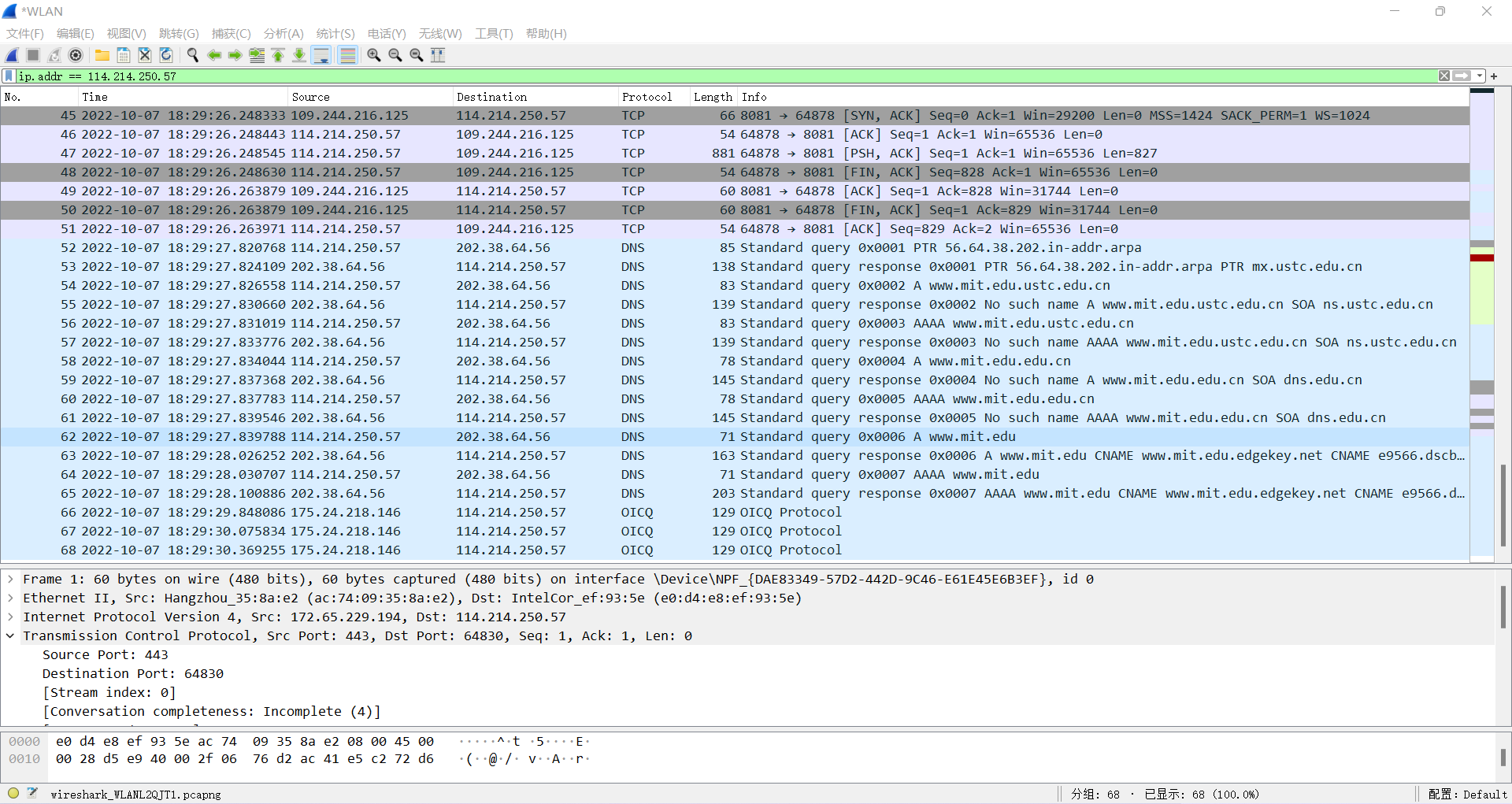
**Ans：**DNS请求报文的目的地址为：202.38.64.56。默认本地DNS服务器的地址为：202.38.64.56。二者一致。

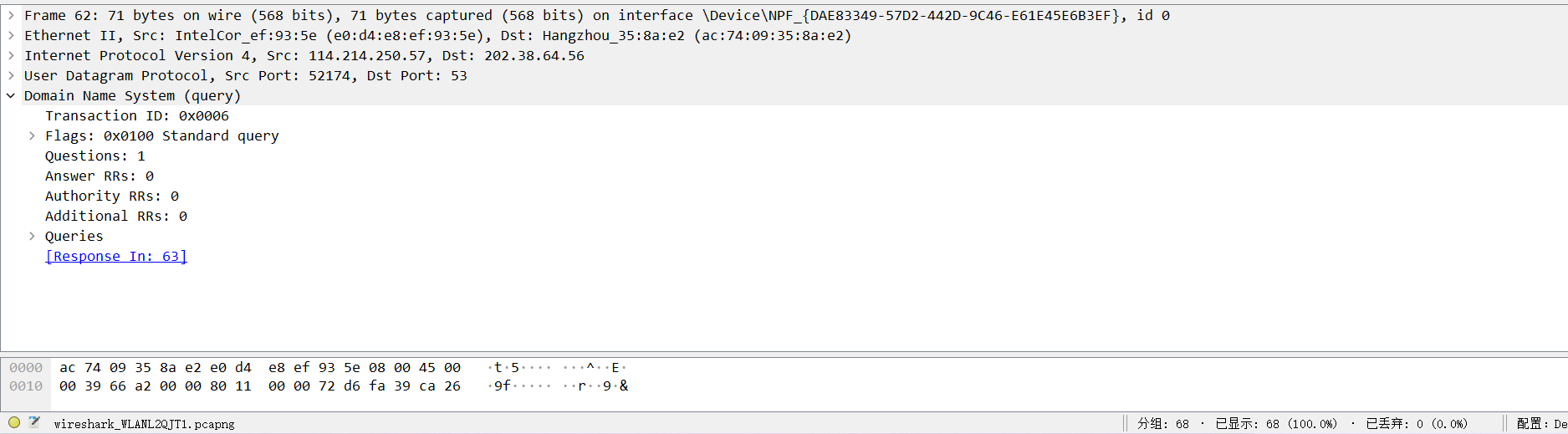




1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

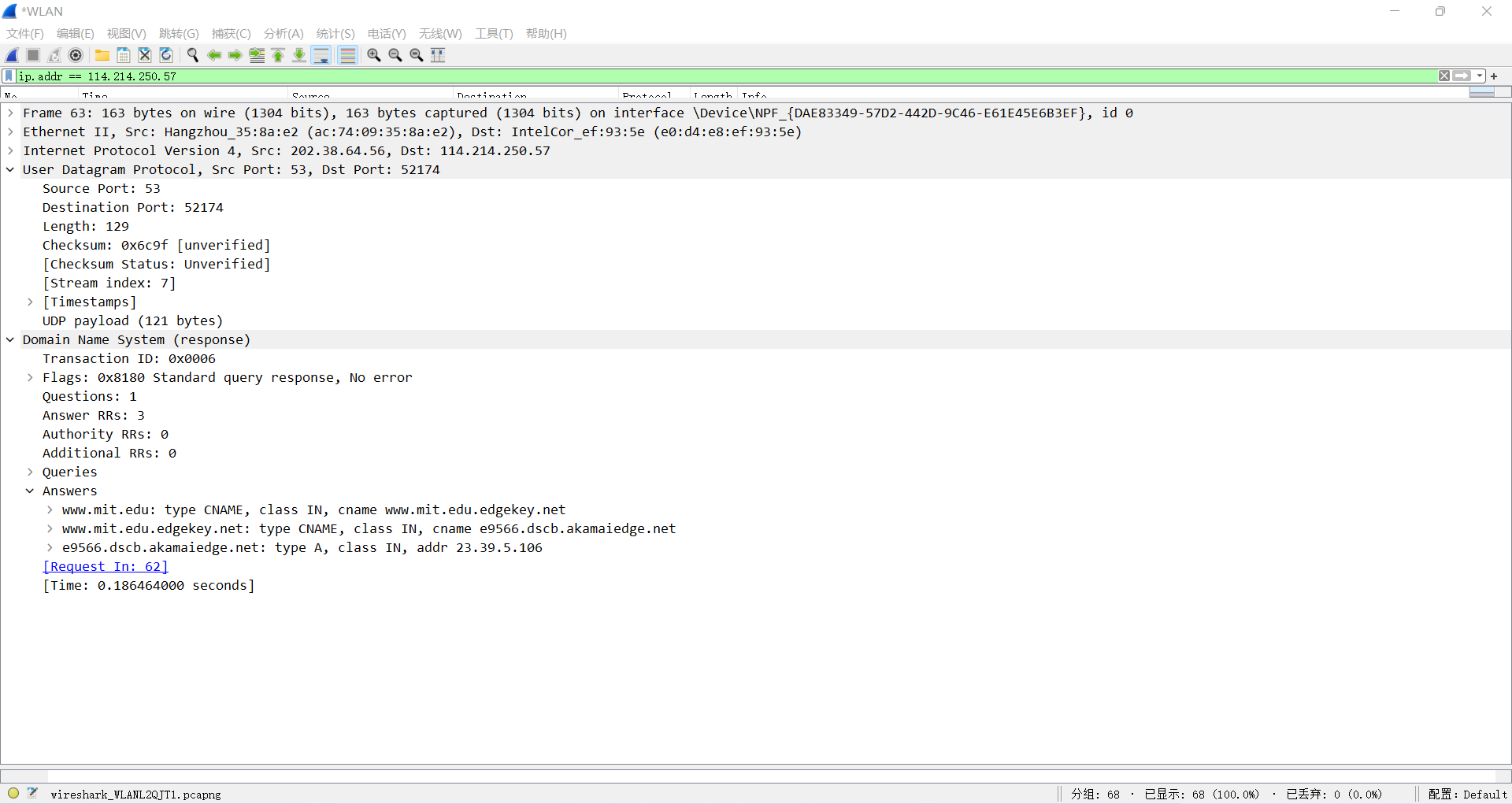
**Ans：**DNS请求报文的类型为A类型。它不含有任何“answers”。





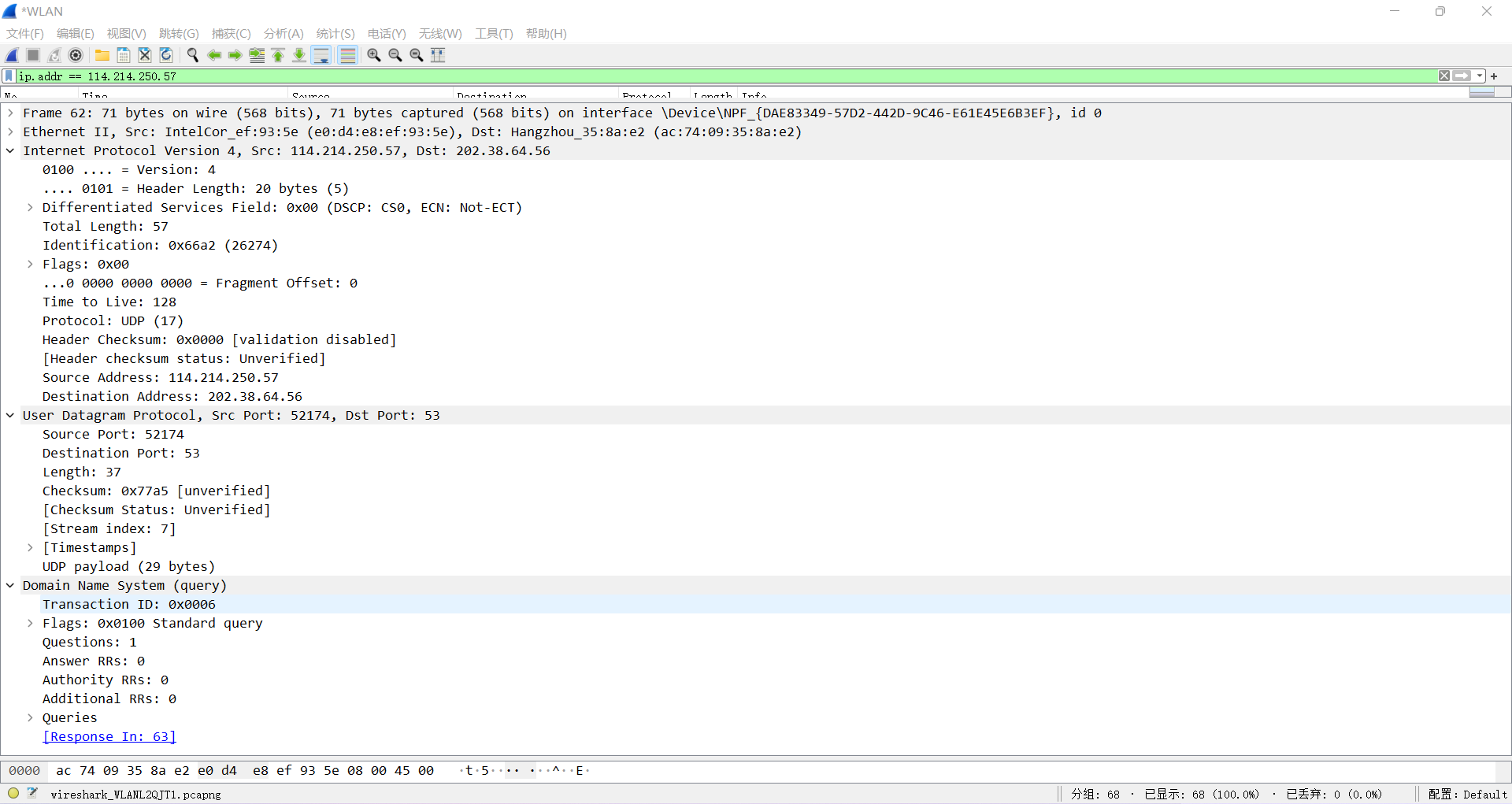
1. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

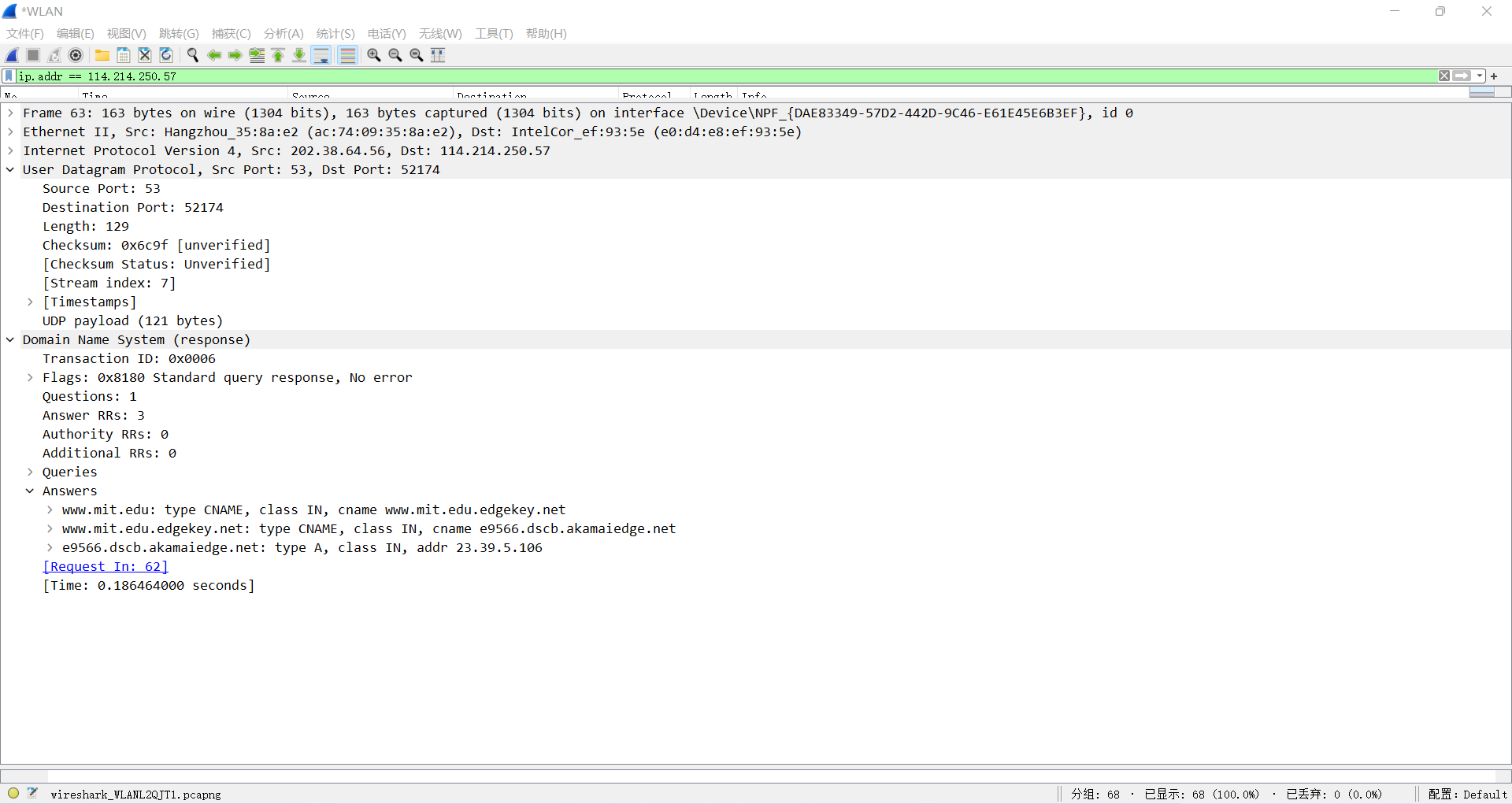
**Ans：**DNS响应报文含有三条“answers”。前两条包含对应域名的标准名（type = CNAME），最后一条包含标准名对应的IP地址（type = A）。



1. **Provide a screenshot.**

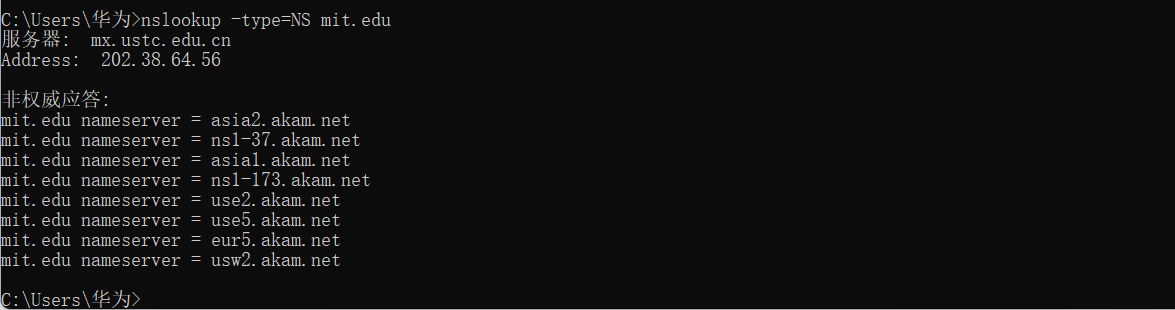
**Ans：**如下：



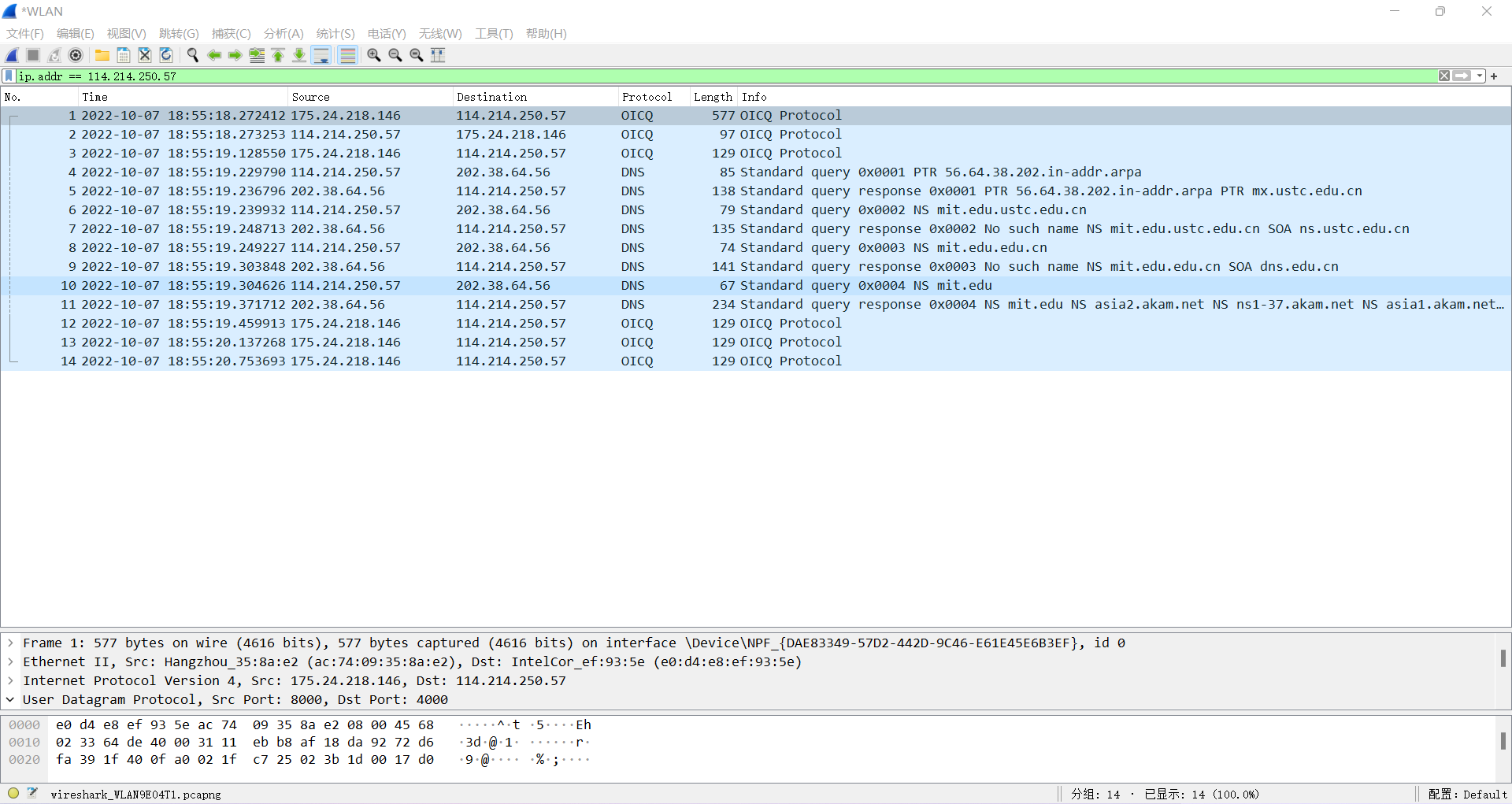


**Step 6：使用nslookup –type=NS mit.edu命令，并抓包**

实验结果如下：



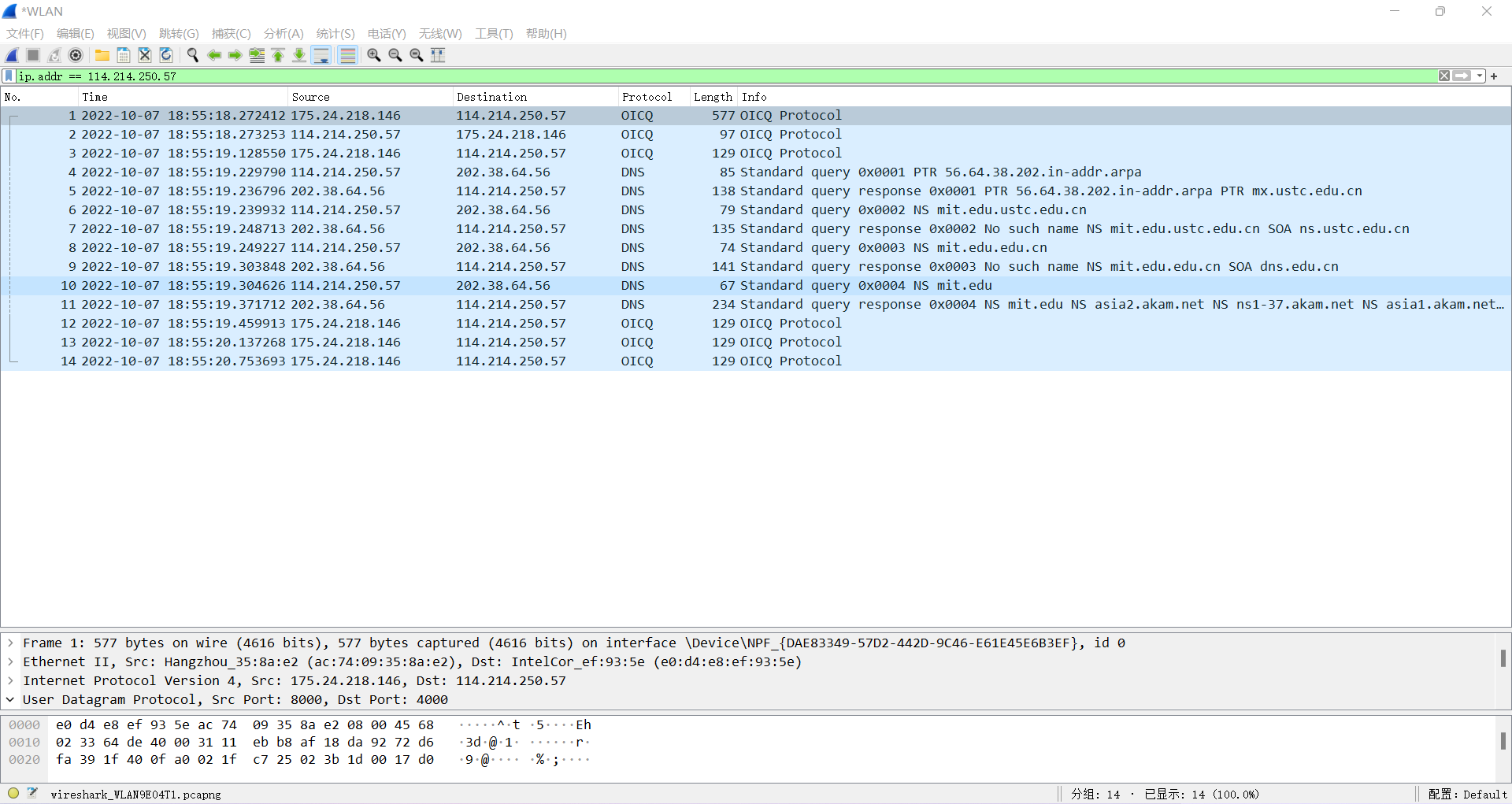
**（图1-15 实验结果）**

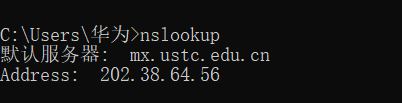


**（图1-16 实验抓包结果）**

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

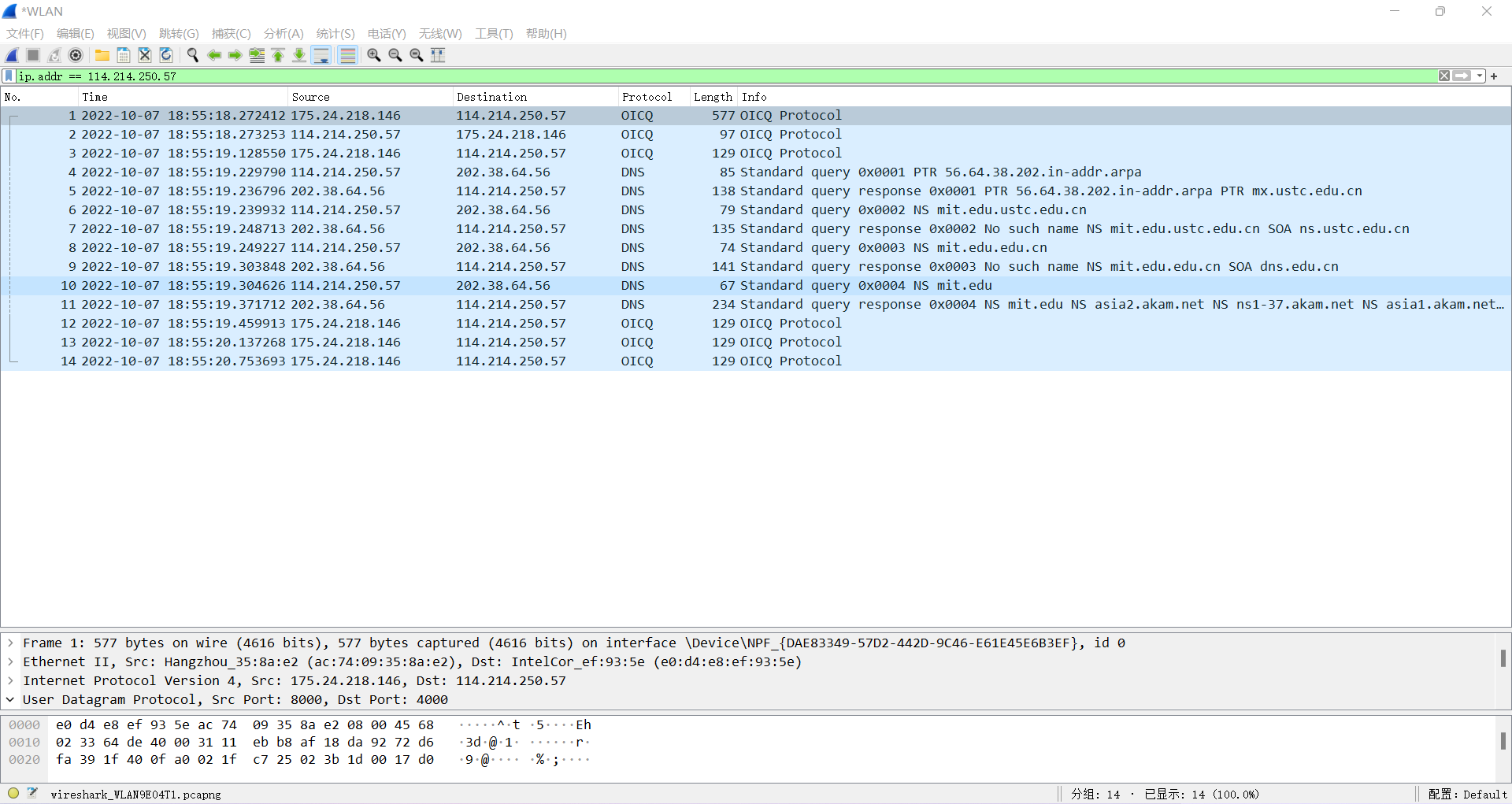
**Ans：**DNS请求报文的目的地址为：202.38.64.56。默认本地DNS服务器的地址为：202.38.64.56。二者一致。

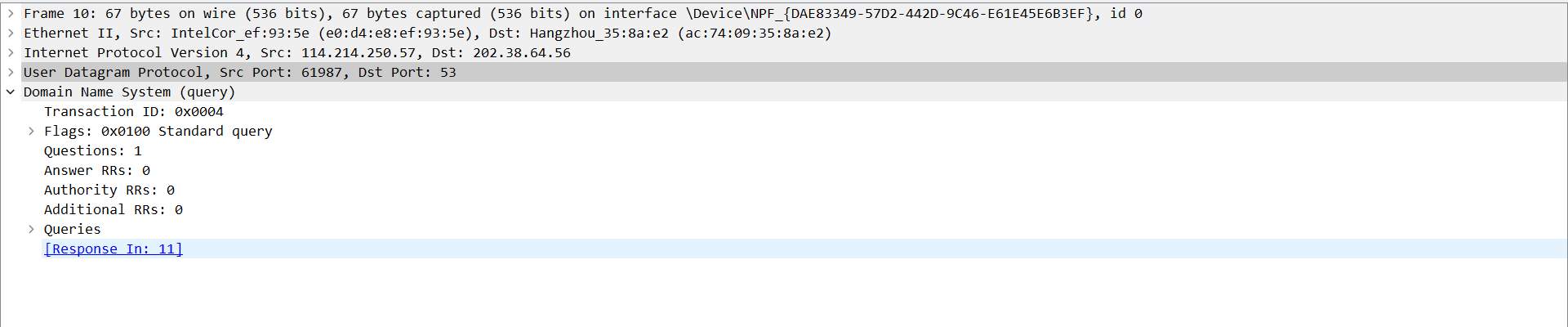




1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

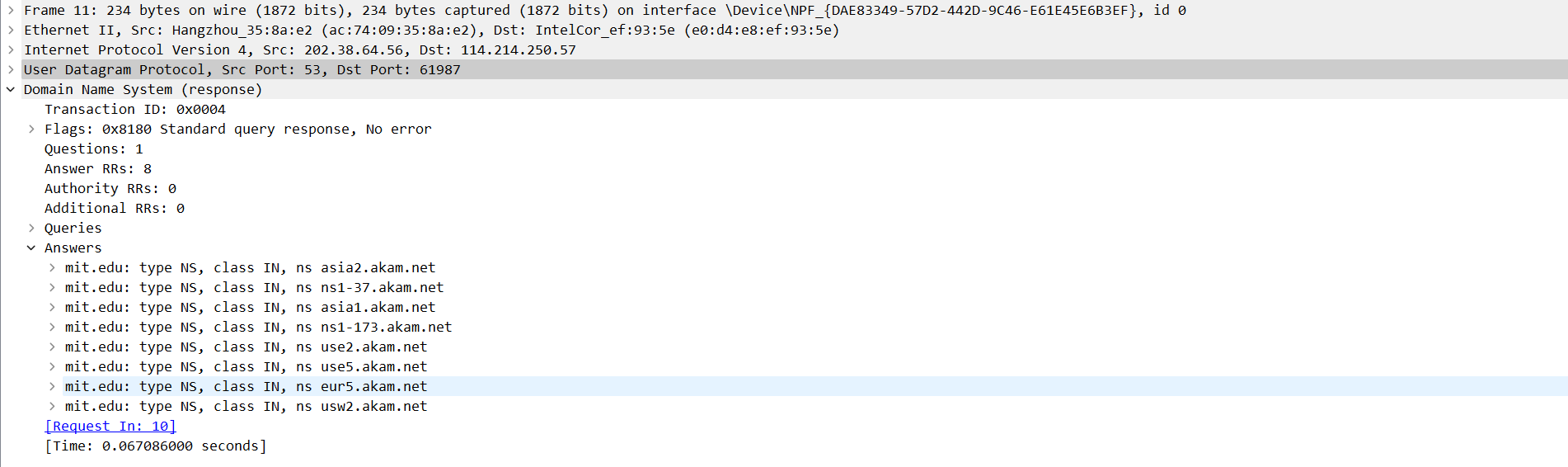
**Ans：**DNS请求报文的类型为NS 类型。它不含有任何“answers”。





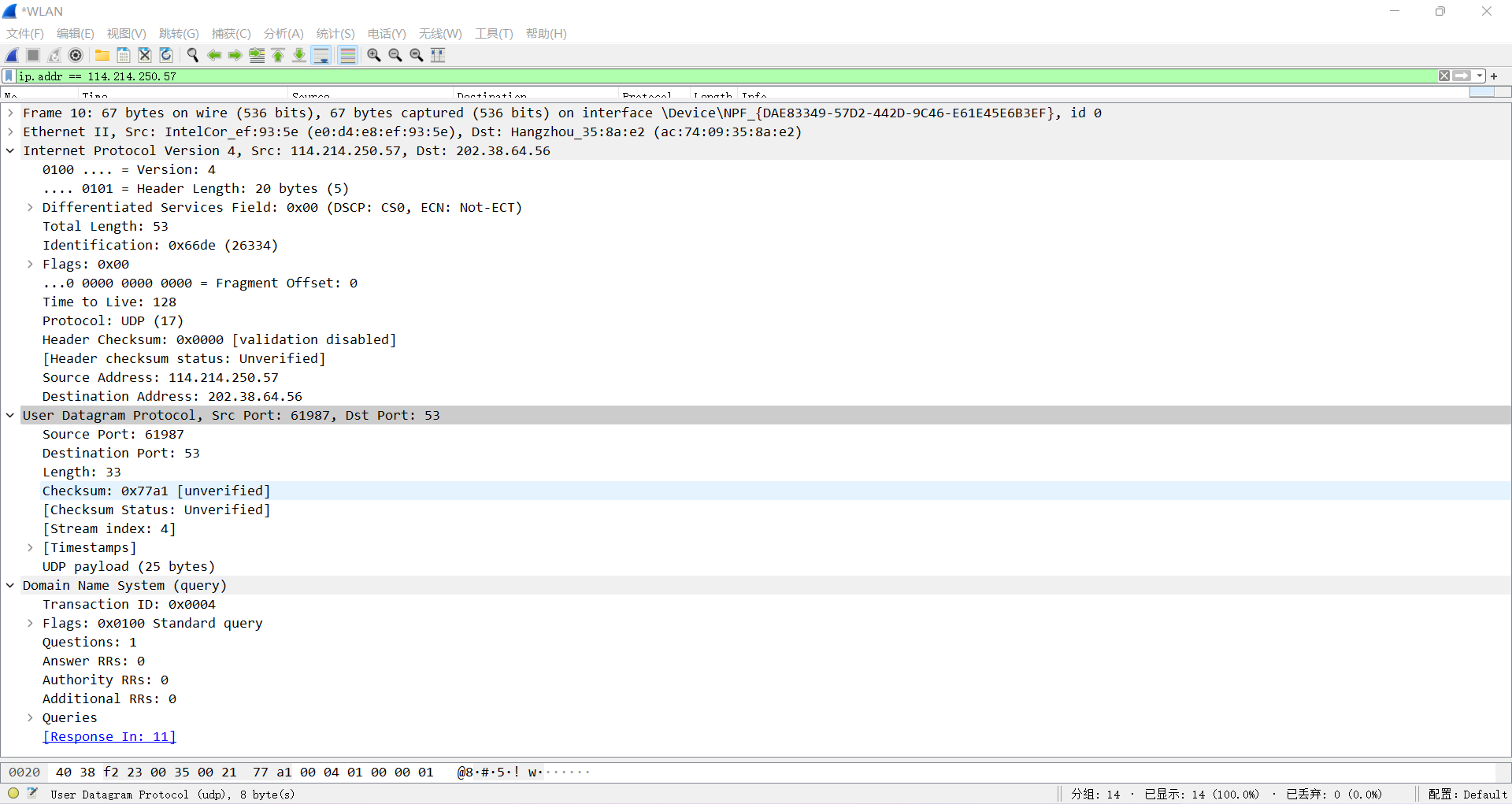
1. **Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?**

**Ans：**DNS响应报文提供了mit.edu对应的权威域名服务器（8个），但并未提供相应的IP地址。

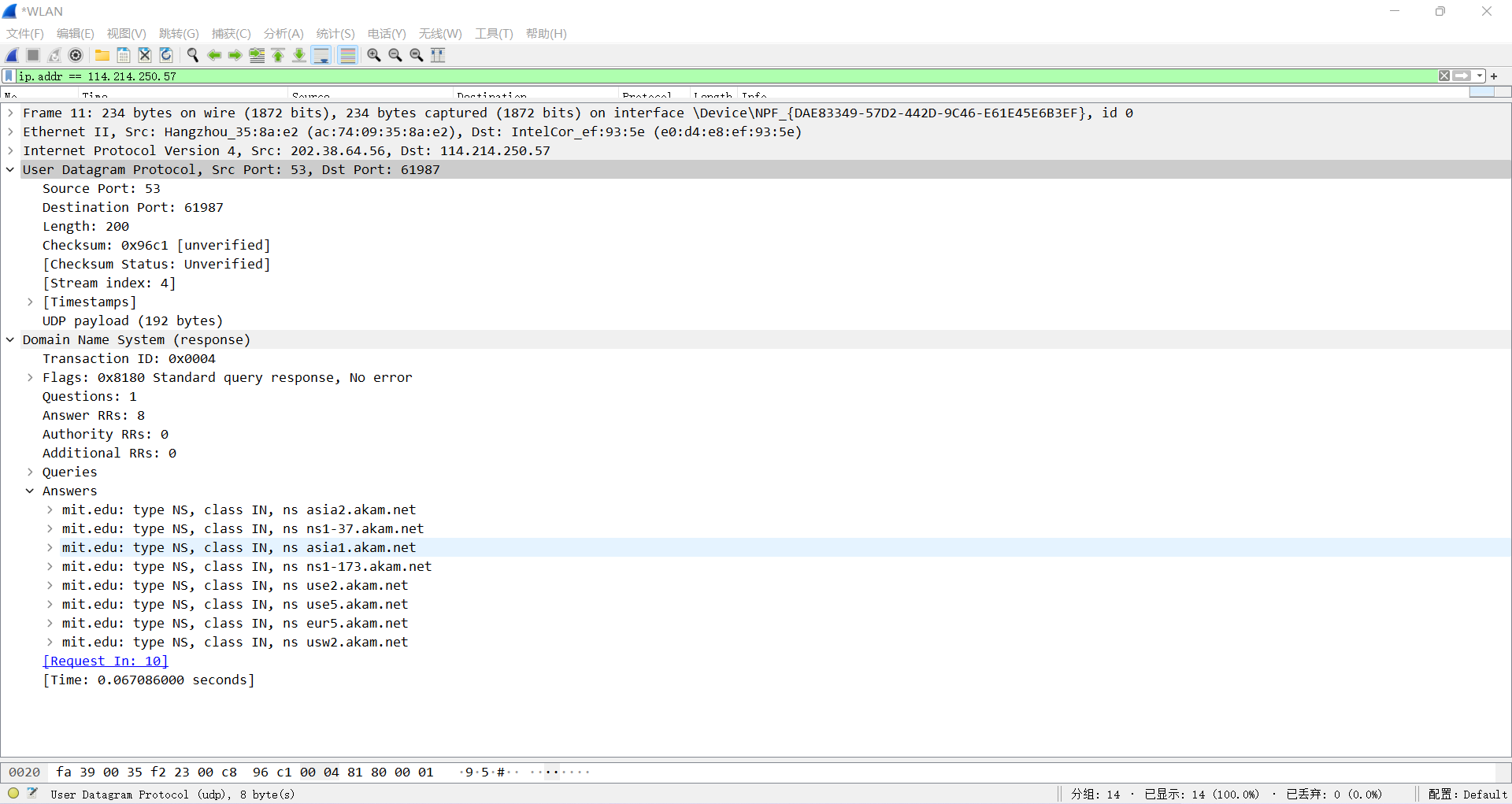


1. **Provide a screenshot.**

**Ans：**如下图：



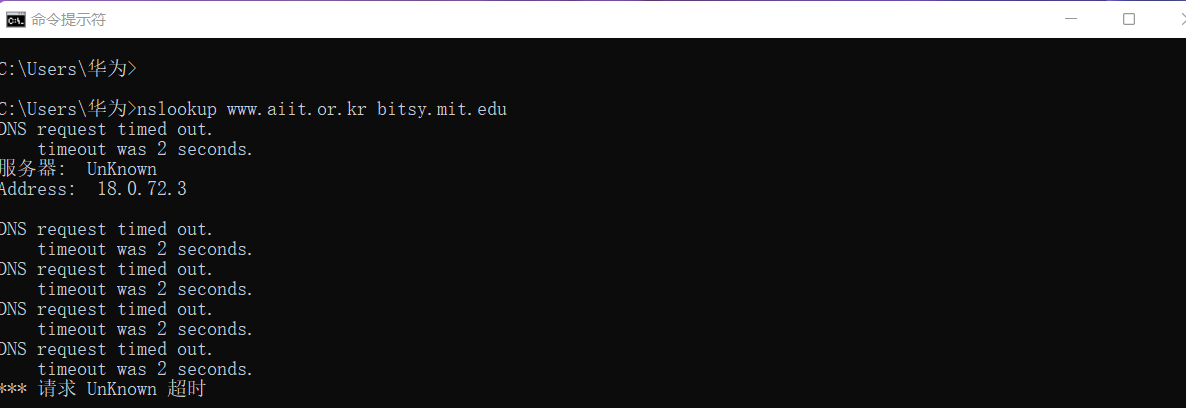
**（图1-17 DNS请求报文内容）**



**（图1-18 DNS响应报文内容）**

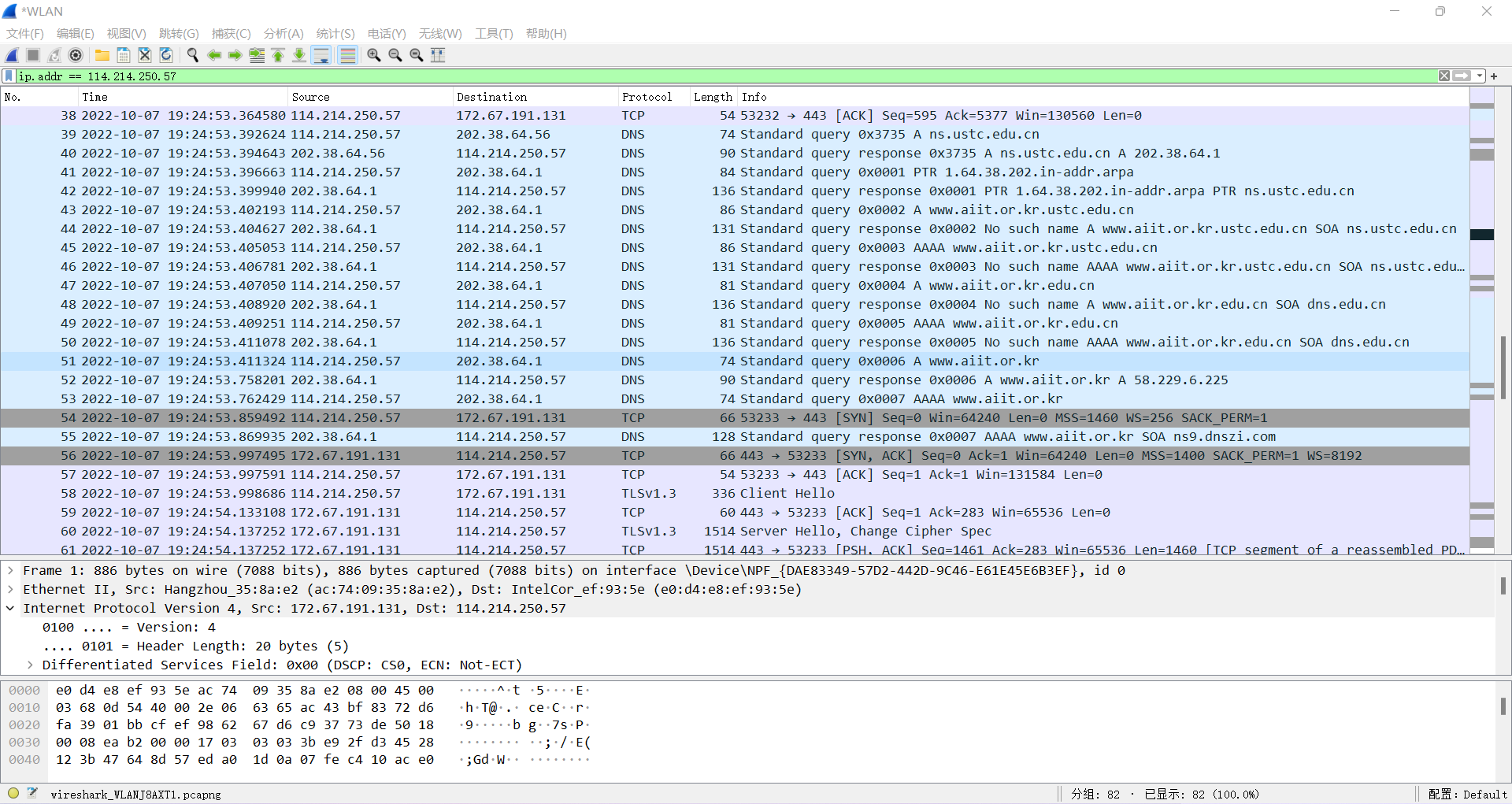
**Step 7：使用nslookup www.aiit.or.kr bitsy.mit.edu命令，并抓包**

实验结果如下：



**（图1-19 实验结果）**

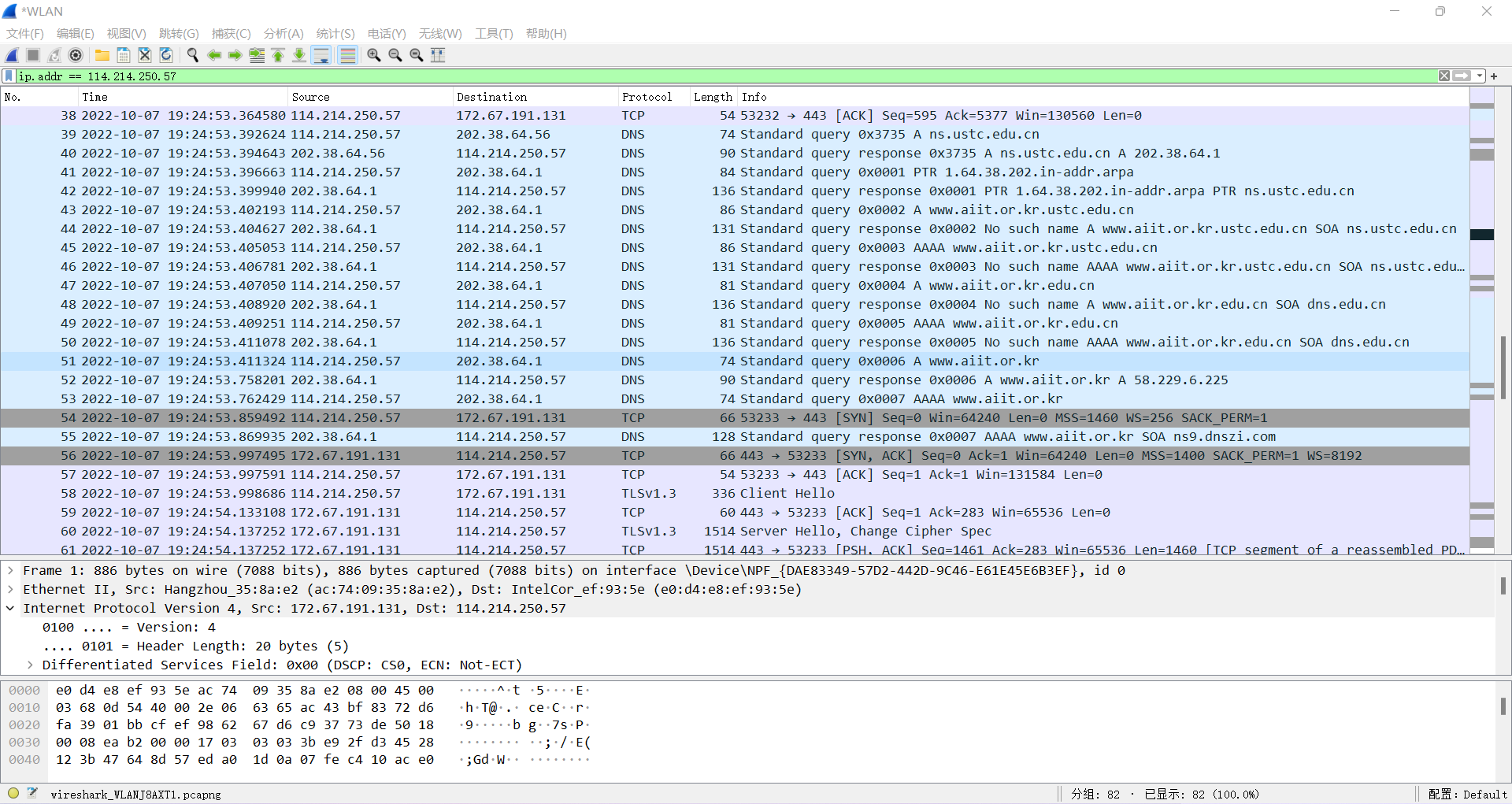
由于请求超时，故将bitsy.mit.edu换成ns.ustc.edu.cn,实验结果如下：

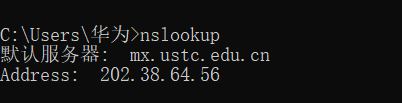


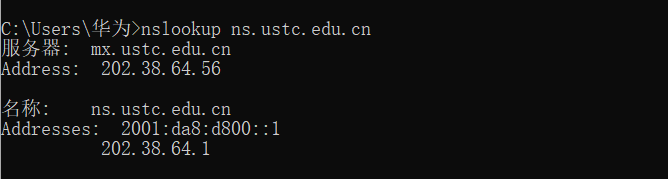
**（图1-20 实验抓包结果）**

1. **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?**

**Ans：**DNS请求报文的目的地址为：202.38.64.1。默认本地DNS服务器的地址为：202.38.64.56。二者不一致。此IP地址与所选用的查询DNS服务器ns.ustc.edu.cn相对应。

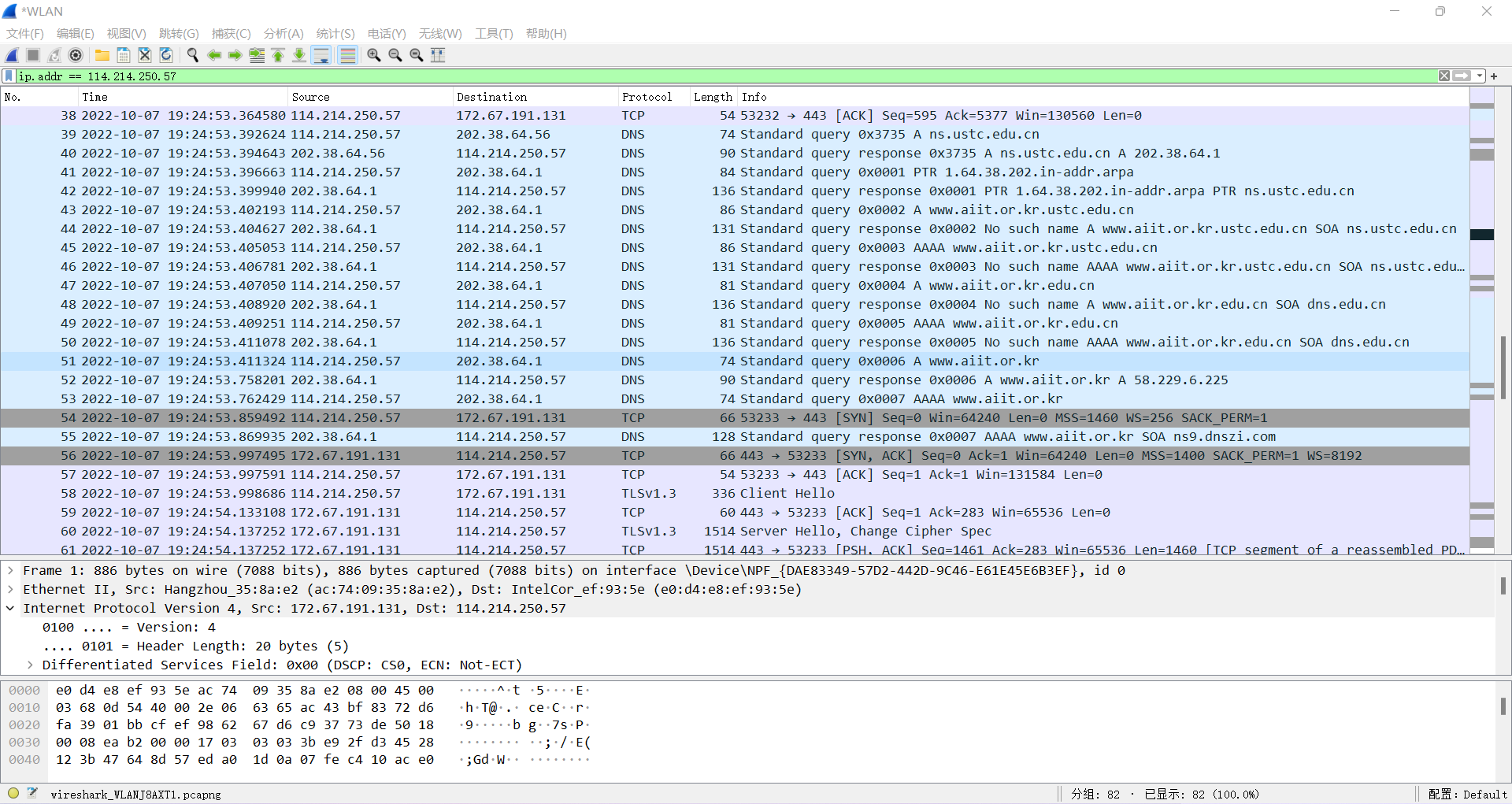


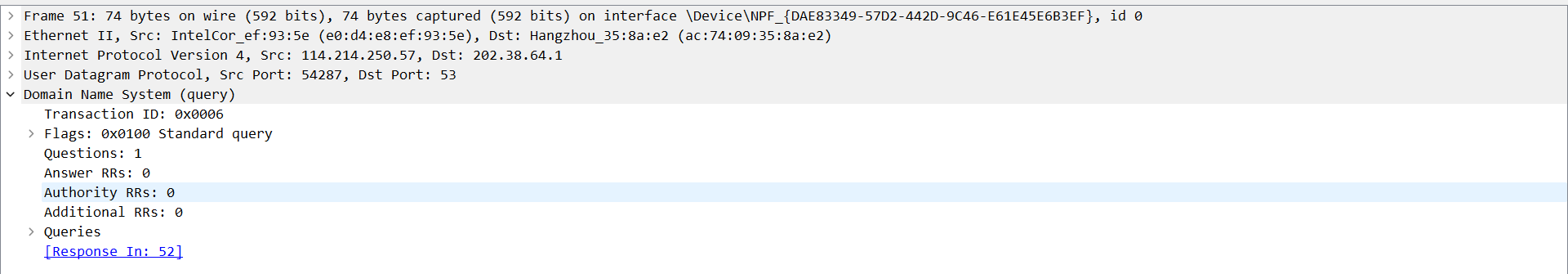




1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

**Ans：**DNS请求报文的类型为A类型。它不含有任何“answers”。

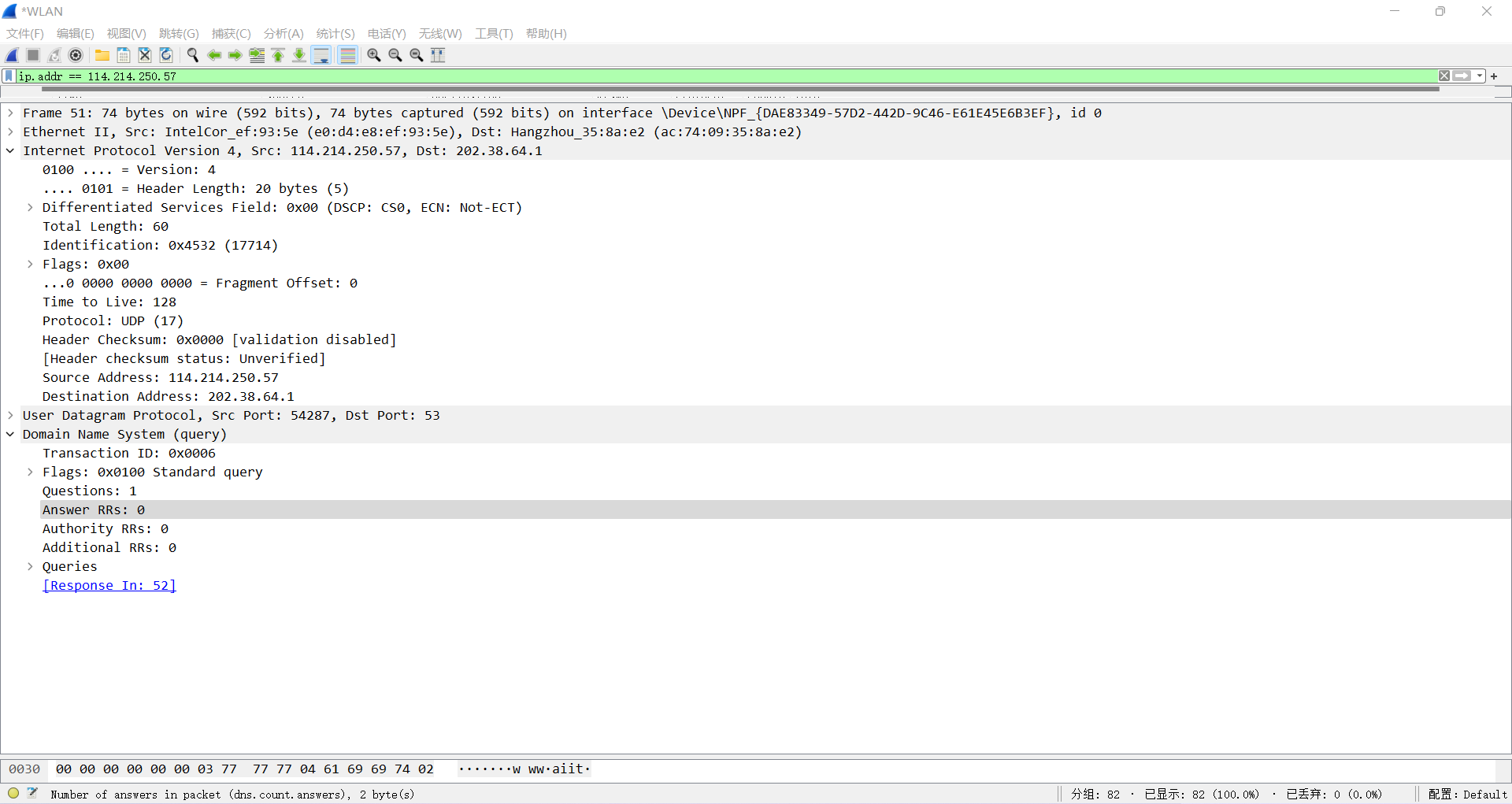


 **22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?**

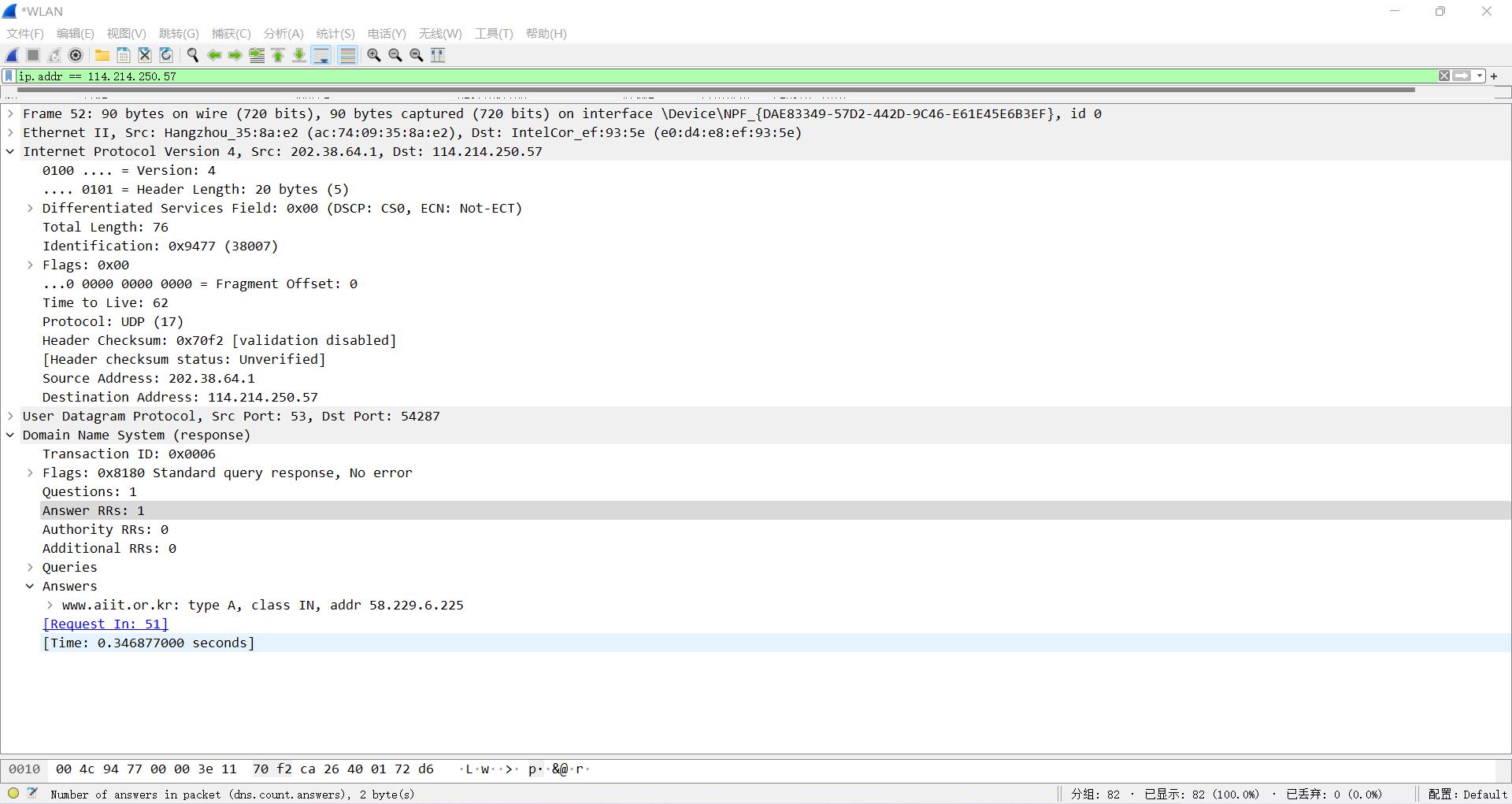
**Ans：**DNS响应报文提供了1个answer，它包含了[www.aiit.or.kr](http://www.aiit.or.kr)对应的IP地址（A类型）。

 **23. Provide a screenshot.**

**Ans：**如下图：



**（图1-21 DNS请求报文内容）**



**（图1-22 DNS响应报文内容）**

1. **补充内容：**

DNS客户端解析超时：

1. 在 NIC 上配置1个 DNS 服务器时



1. 在 NIC 上配置2个 DNS 服务器时



1. 在 NIC 上配置3个 DNS 服务器时



**成功！您的提交显示在此页面上。该提交的确认编号为 80151613-410e-47bd-8c1b-4e0666b1653c。请复制并保存此编号以作为提交证明。**[**在“我的成绩”中查看您的所有提交确认。**](https://www.bb.ustc.edu.cn/webapps/bb-mygrades-BBLEARN/myGrades?course_id=_12565_1&stream_name=mygrades&is_stream=false)