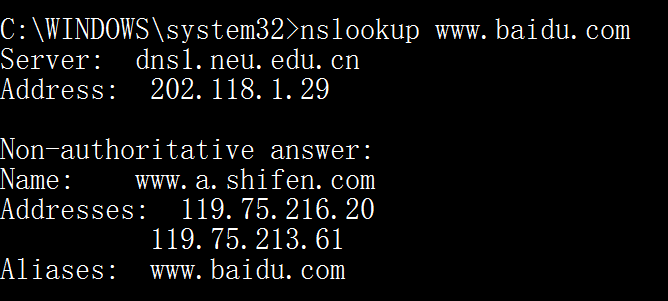
Lab05-Wireshark DNS Lab

Part 1 nslookup

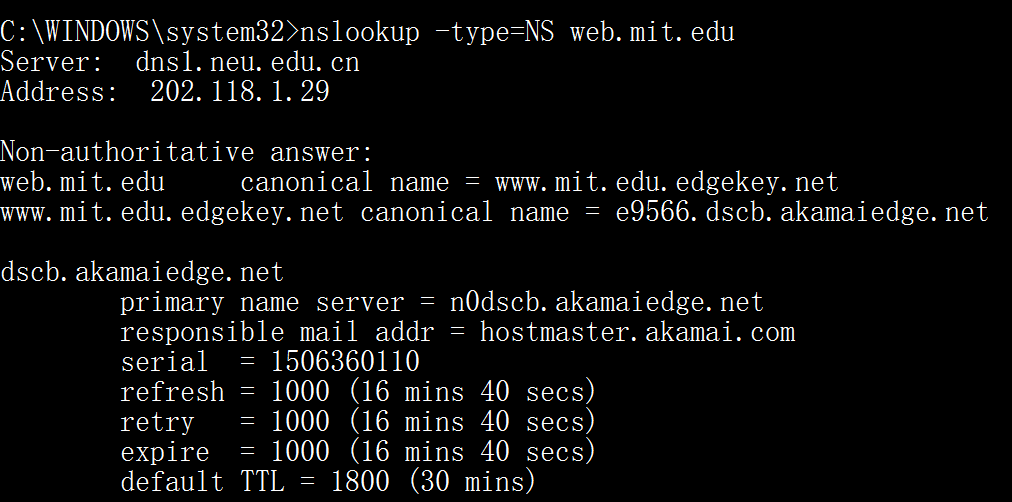
1. *Run nslookup to obtain the IP address of another Web server in China. What is the IP address of that server?*

Okay, I tried to obtain the IP address of Chinese biggest search engine website [www.baidu.com](http://www.baidu.com).

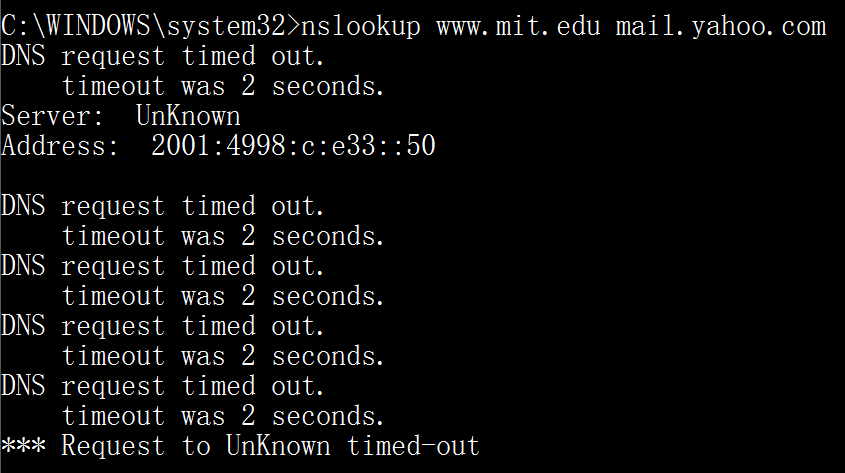


The IP address of that server is “**119.75.216.20**” and “**119.75.213.61**”, it has two public dns server.

2. *Run nslookup to determine the authoritative DNS servers for a* [*www.mit.edu*](http://www.mit.edu)*.*

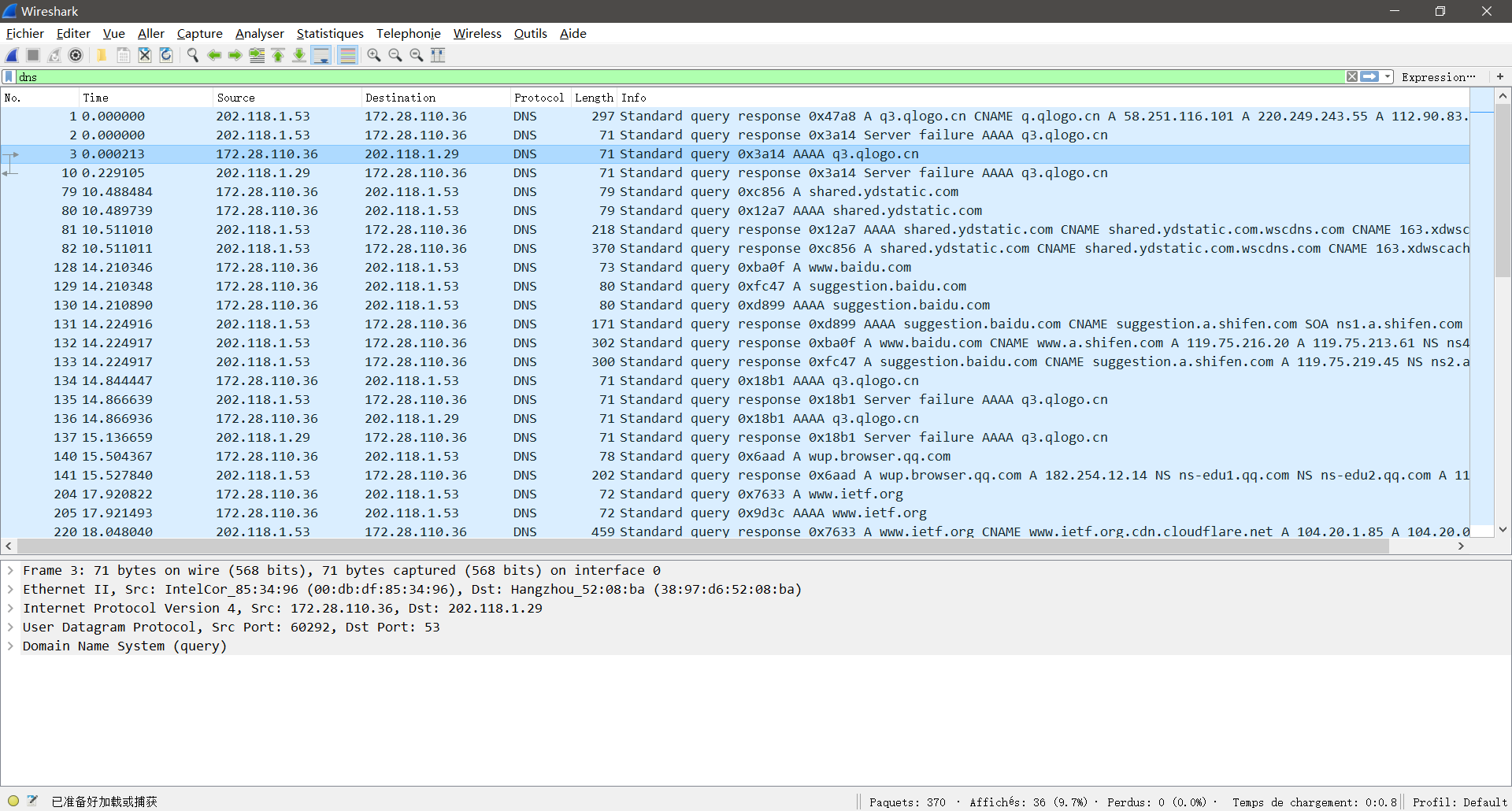


3. *Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo.co.uk. What is its IP address?*



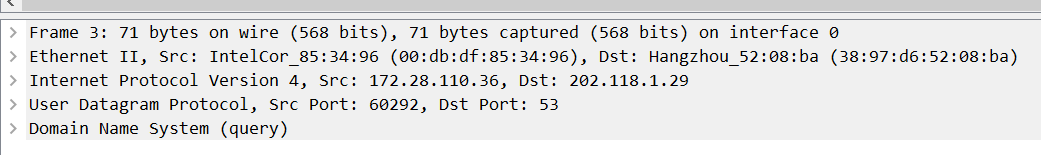
The IP address for the DNS server if queried for the Yahoo mail server is 2001:4998:c:e33::50.

Part 2 ipconfig

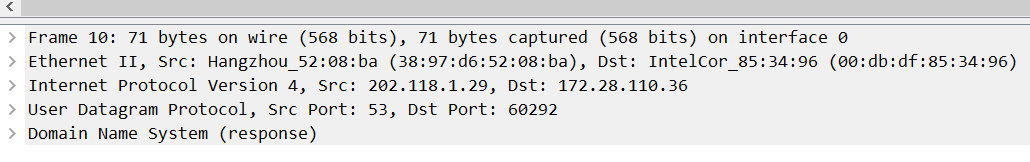
4. *Locate the DNS query and response messages. Are they sent over UDP or TCP?* 

All of them are sent over **UDP**.

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

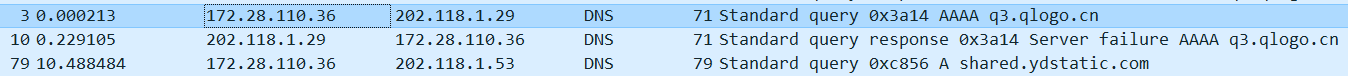


The destination port of the DNS query message is **port** **53**.

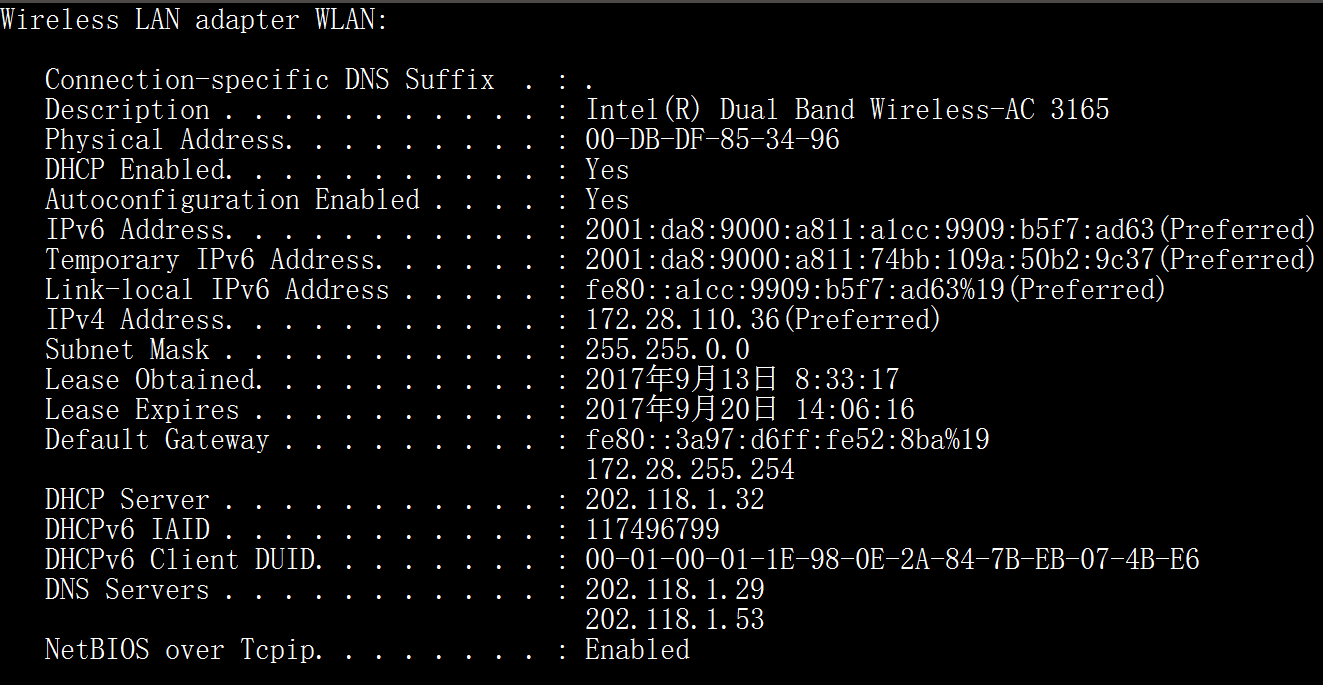


And the source port of DNS response message is also **port 53**.

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?*

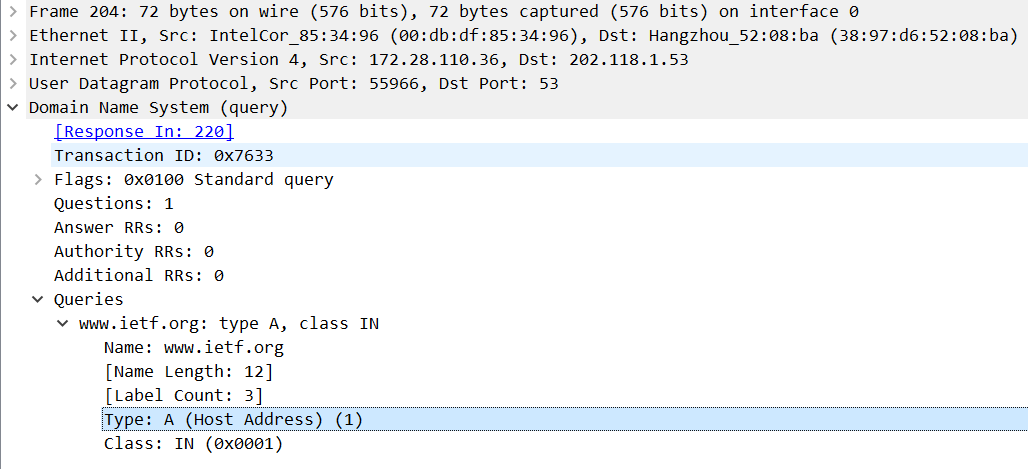
First step, I find my DNS query message sent to **202.118.1.29** and **202.118.1.53**. 

And next, I use ipconfig to get my local DNS server IP address.



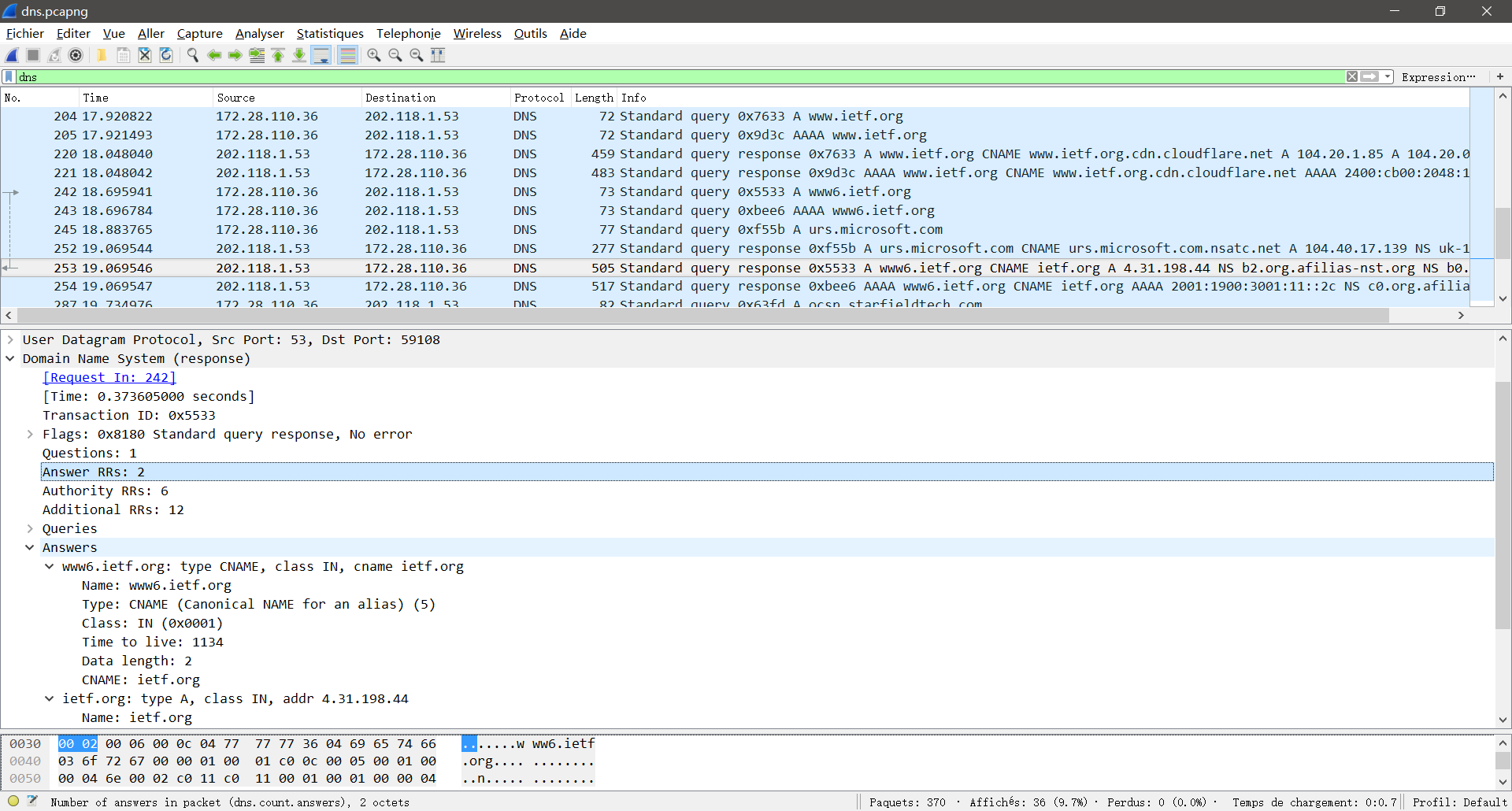
Yep, I find there are 2 local DNS server. 202.118.1.29 and 202.118.1.53. So, I can say they are the **same** IP addresses.

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



It is a “**type A**” query. **No** answers included in it.

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



**2** answers are provided. The first answer contain the **canonical name** for the alias. And the other answer contain the **IPv4 Address** of this website.

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?*

**Yes**.

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

No, the images are also from [www.itef.org](http://www.itef.org), and there have been DNS cache about it. So, it’s unnecessary to send DNS queries again.

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

A: The destination port for the DNS query message is **53**,

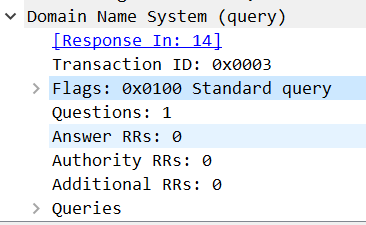
and the source port of DNS response message is **also 53**.

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

The message is sent to **202.118.1.29**.

**Yes,** it’s one of my DNS servers.

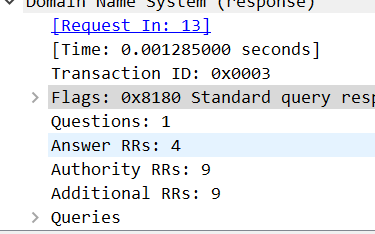
13. *Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?*

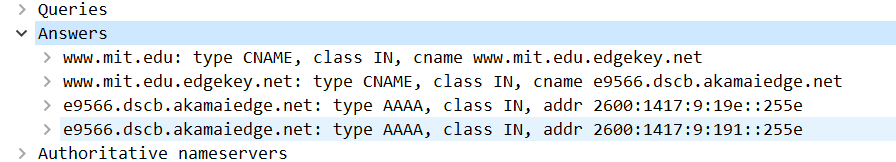


The type of it is “**AAAA**”, a query for IPv6 address.

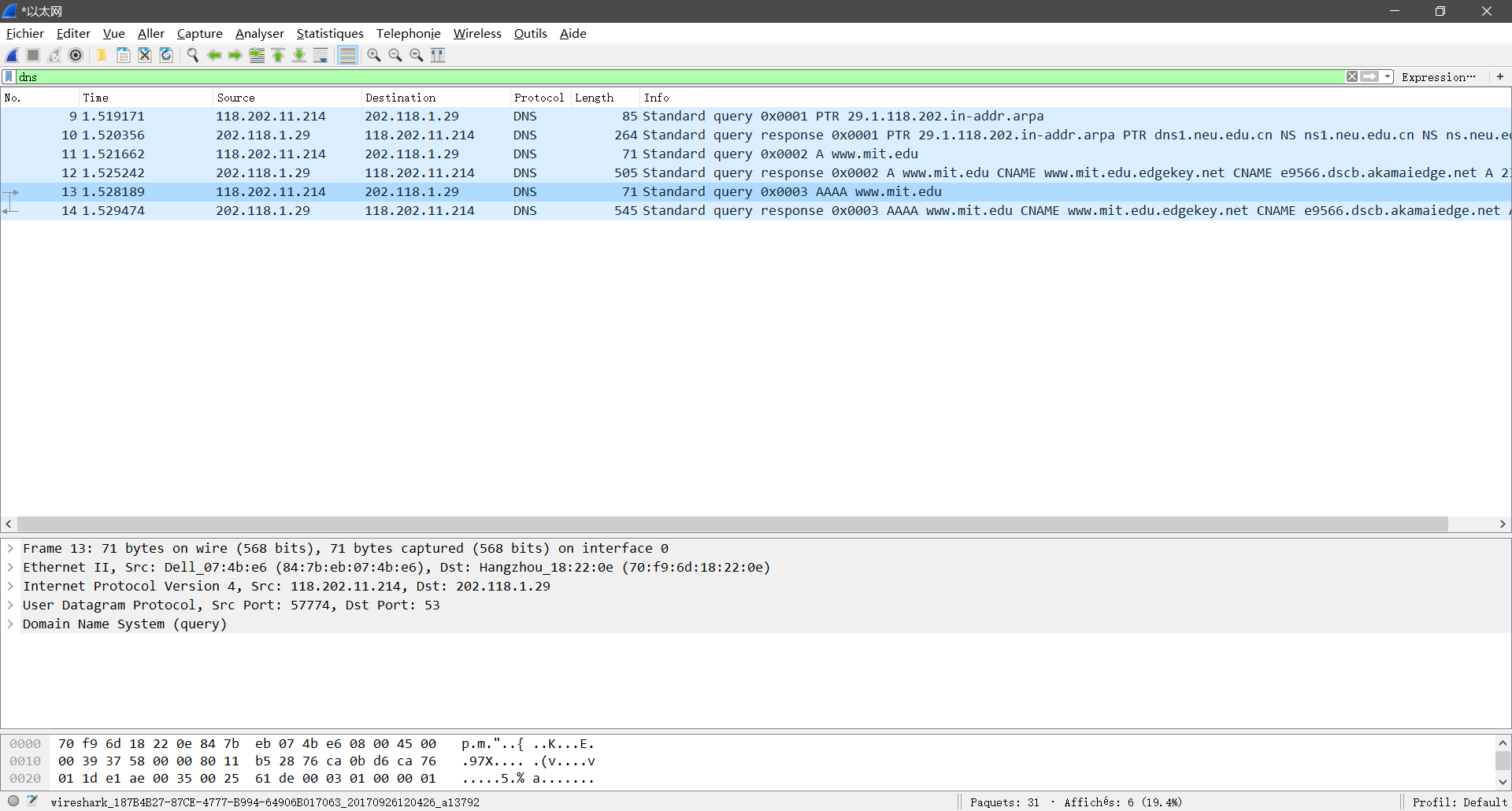
**No**, it contains only one question and doesn’t contain any answers.

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

**4** answers are provided.

  
The response message contains 2 answers to the mentioned query which is the type “AAAA” address of [www.mit.edu](http://www.mit.edu). And it contains another 2 additional records.

15. *Provide a screenshot.*



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

The message is sent to **202.118.1.29**.

**Yes,** it’s one of my DNS servers.

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

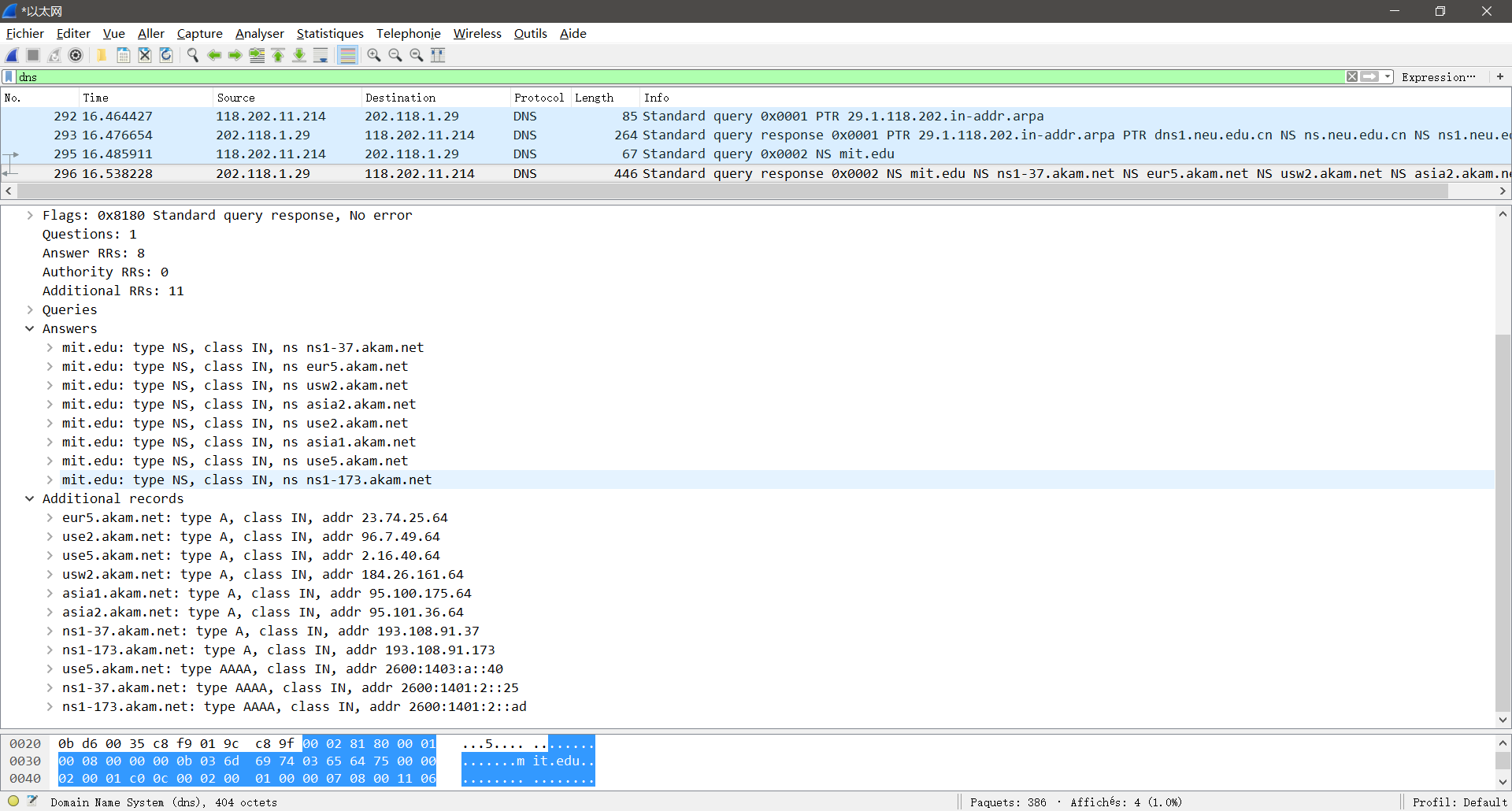
The type of it is “**NS**”, a query for the name servers responsible for a domain.

**No**, it contains only one question and doesn’t contain any answers.

*18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?*

The response message provides 3 MIT nameservers: w20ns.mit.edu[18.70.0.160],strawb.mit.edu[18.71.0.150], and bitsy.mit.edu[18.72.0.3]. The IP addresses for the nameservers was included under the additional records category sent back as part of the response message.

19. *Provide a screenshot.*



*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?*

The message is sent to **8.8.8.8**.

**No,** it isn’t my DNS server. It correspond to Google’s DNS server.

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

The type of it is “**AAAA**”, a query getting request of the IPv6 address.

**No**, it contains only one question and doesn’t contain any answers.

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

**2** answers are provided.

The answer with a CNAME type contain the alias of [www.neu.edu.cn](http://www.neu.edu.cn), and the other answer with an AAAA type contain the IPv6 address of www.neu.edu.cn.

*23. Provide a screenshot.*

