Robert Martinez

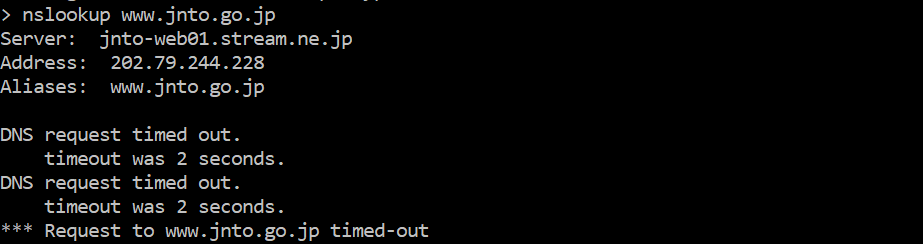
Wireshark Lab

October 21, 2017

Wire Shark Lab

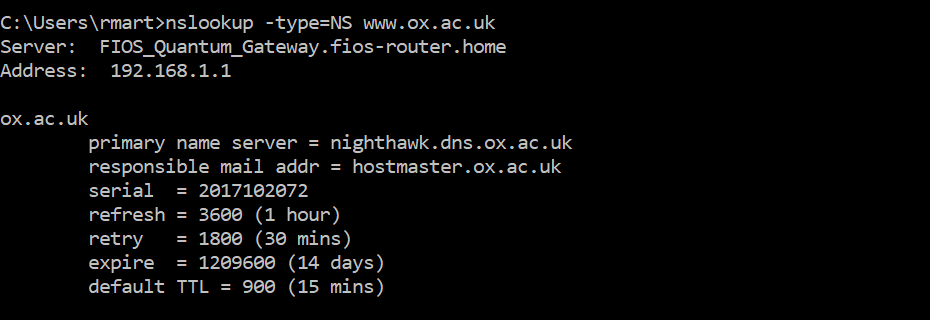
1. **Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

I used a Japanese web server called www.jnto.go.jp. The IP address of this server was ***202.79.244.288***.



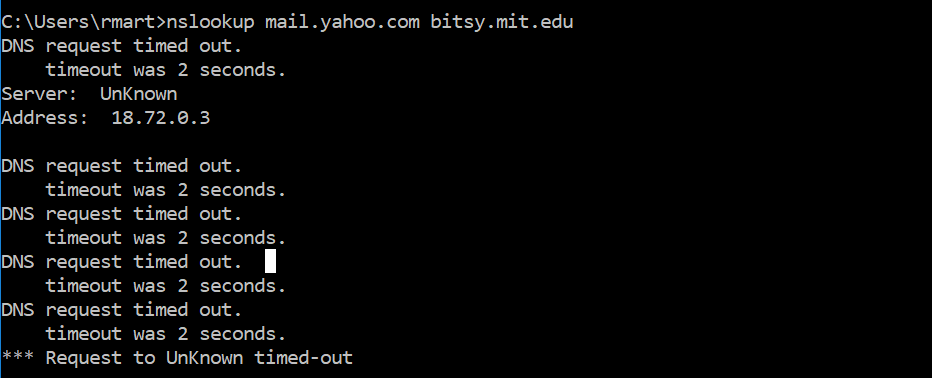
1. **Run nslookup to determine the authoritative DNS servers for a university in Europe.**

I used a Oxford University for my European school. The authoritative DNS server is: ***nighthawk.dns.ox.ac.uk*.**



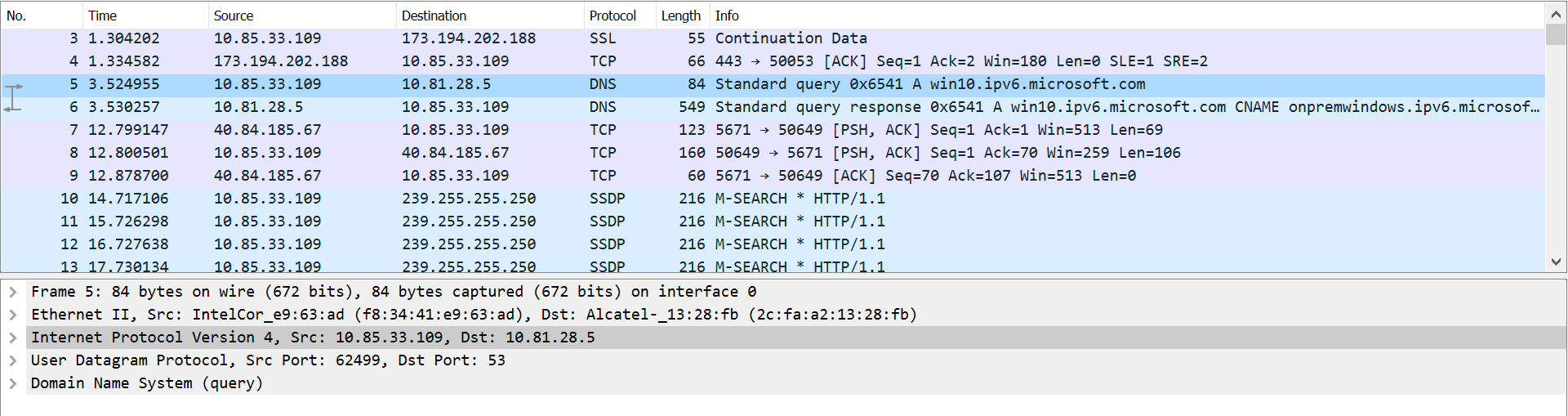
1. **Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

I used the following command to execute the following: nslookup mail.yahoo.com bitsy.mit.ede. This unfortunately showed me the following error messages.



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

I launched Wireshark and located the DNS query and response messages.Both DNS and response messages are sent over ***UDP***.



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

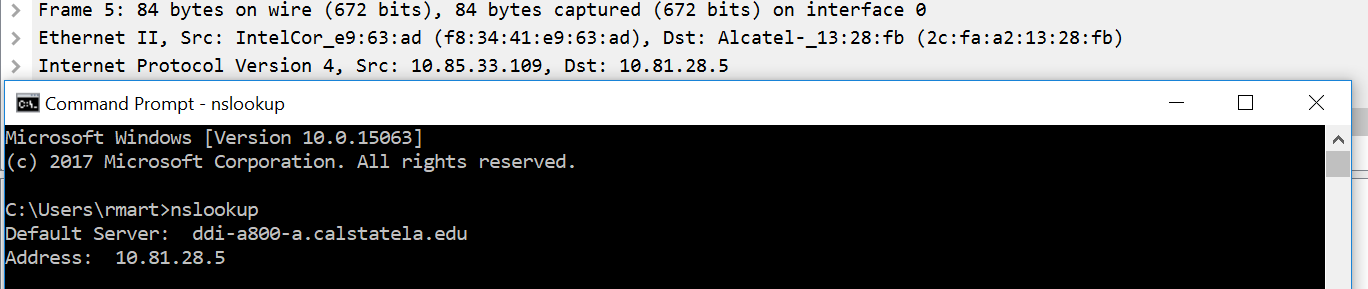
The destination port for the DNS query message is ***53****.*

The source port of the DNS response message is ***62499****.*



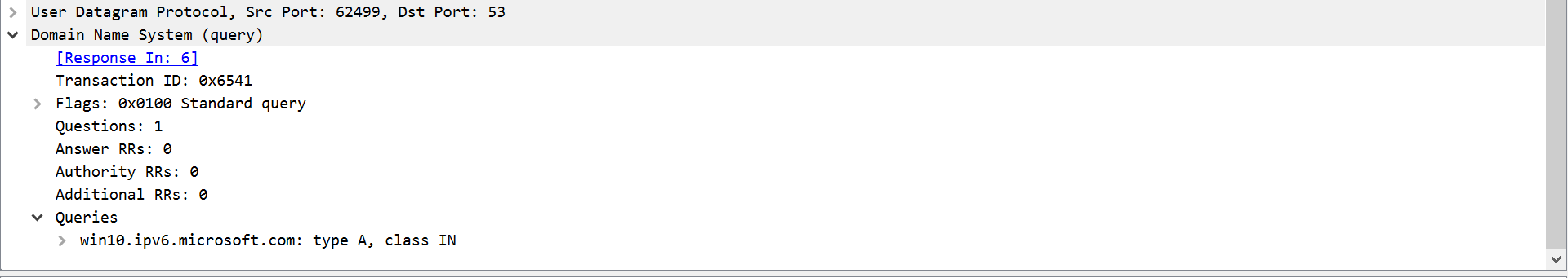
1. **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

The DNS servers of both these two are the same, because after checking the local DNS server with nslookup command on command prompt, you could see **they are the same**.

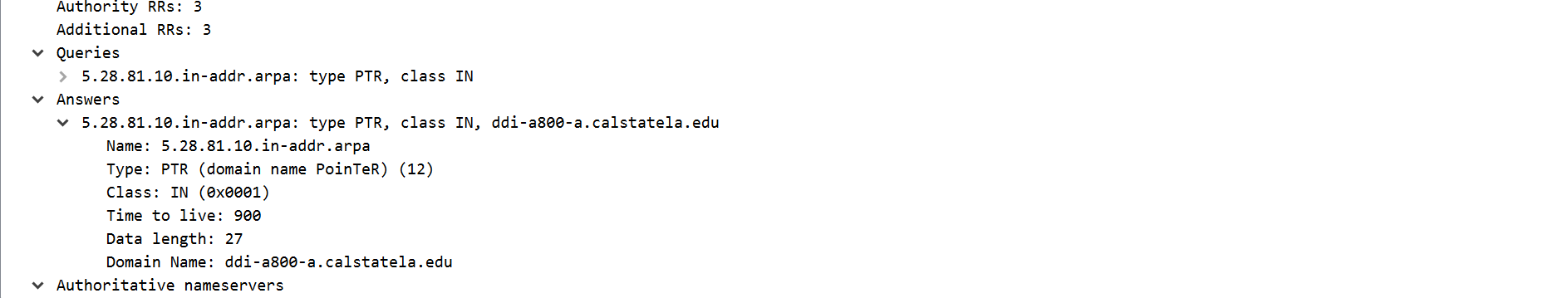


1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

The DNS query “Type” is ***A***. The query does not contain any messages.



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

The DNS response message provides contains only one answer. As shown in the screenshot, only ***one answer*** was provided.

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?**

Yes, ***both SYN packet correspond*** to the IP address provided by the DNS response message.

First screenshot:

C:\Users\rmart\AppData\Local\Microsoft\Windows\INetCache\Content.Word\9.1.png

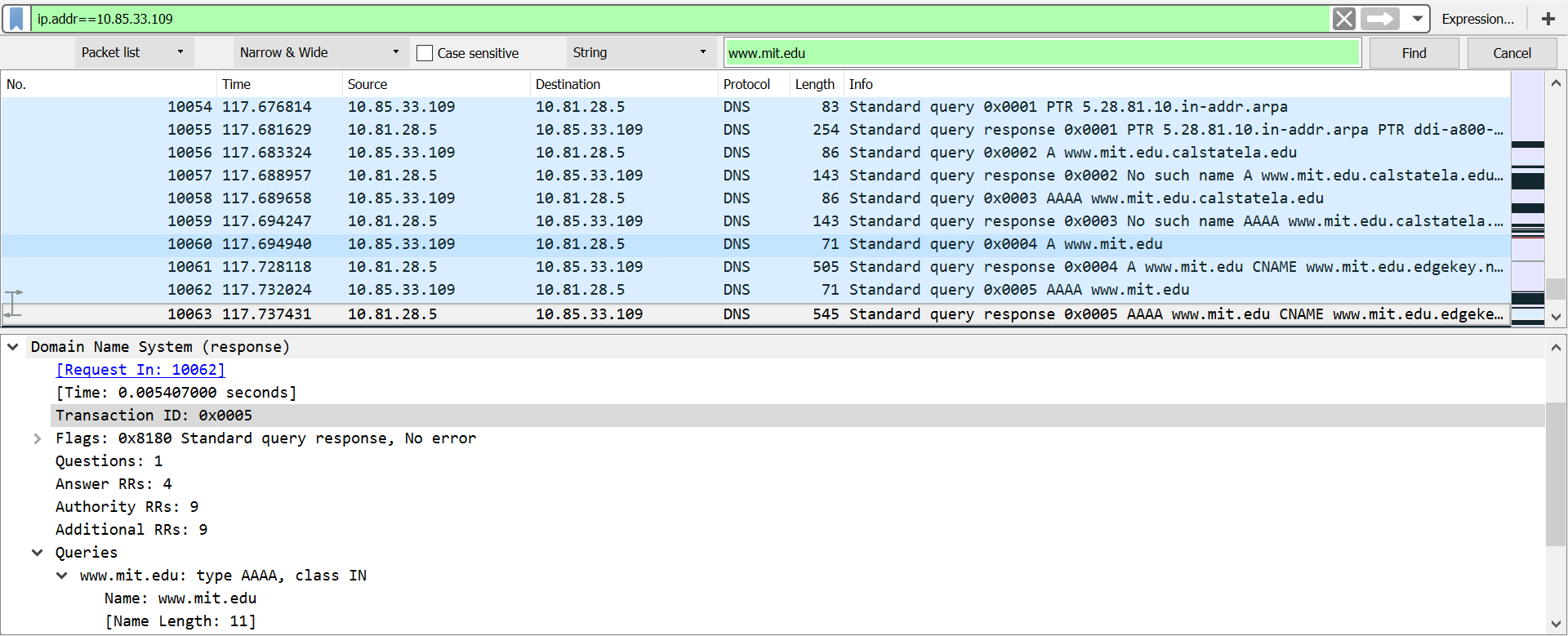
Second screenshot:



From both screenshots we can see that the IP address of the DNS response server is the same.

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

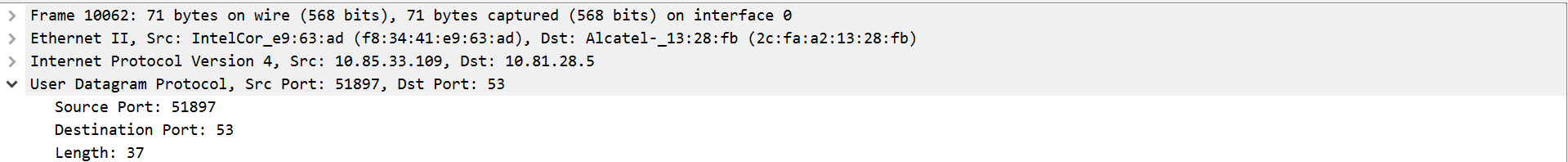
The host issues new DNS queries. As shown in the screenshot below, you can see that there is a change in the number of DNS queries.



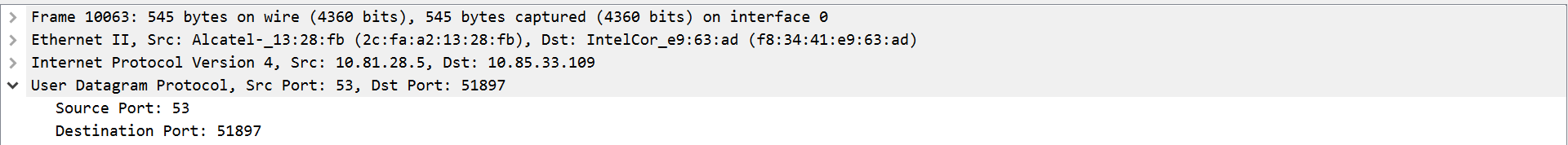
1. **What is the destination port for the DNS query message? What is the source port of DNS response message?**

As show in the screenshot above, the destination port number for the DNS query message is: “***53***”. The source port for the DNS response message is: “***53***”.

Here is a screenshot of the DNS destination port number (DNS query message):



Here is a screenshot of the DNS source port number (DNS response message):



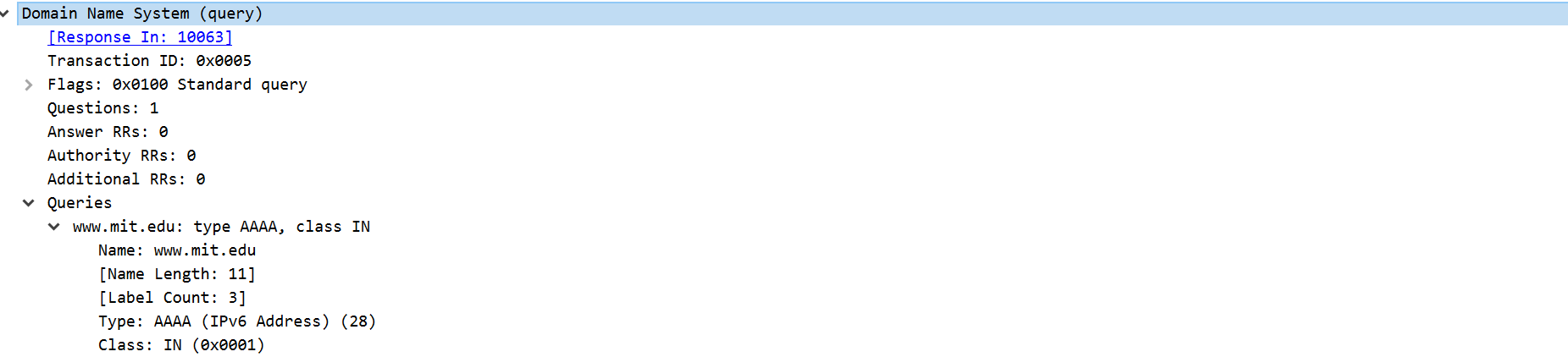
1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

As show in the screenshot above, the destination port number for the DNS query message is: “***10.81.28.5***”. The source port for the DNS response message is: “***10.81.28.5***”.

C:\Users\rmart\AppData\Local\Microsoft\Windows\INetCache\Content.Word\#12.png

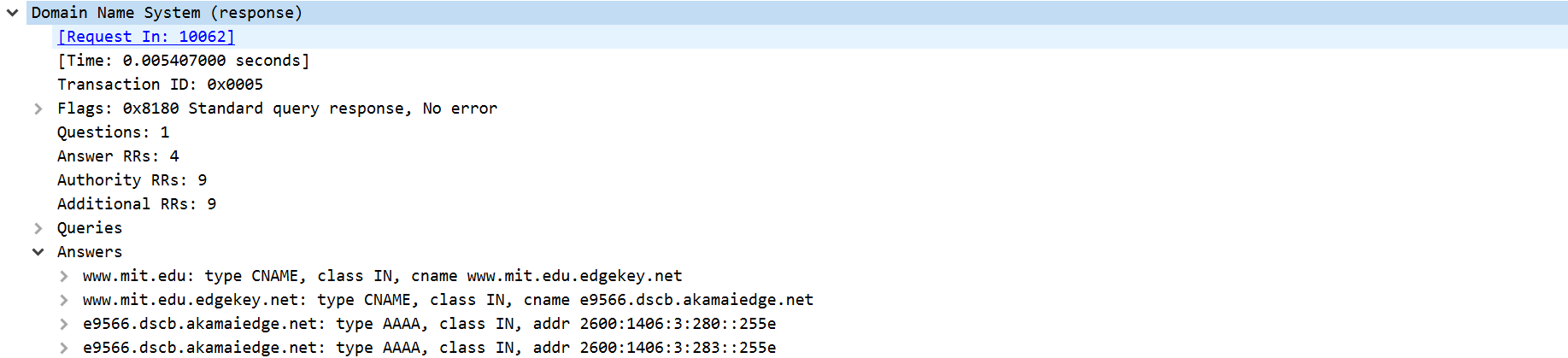
1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

The type of the DNS query is: “***AAAA***”, however it does not contain any answers.

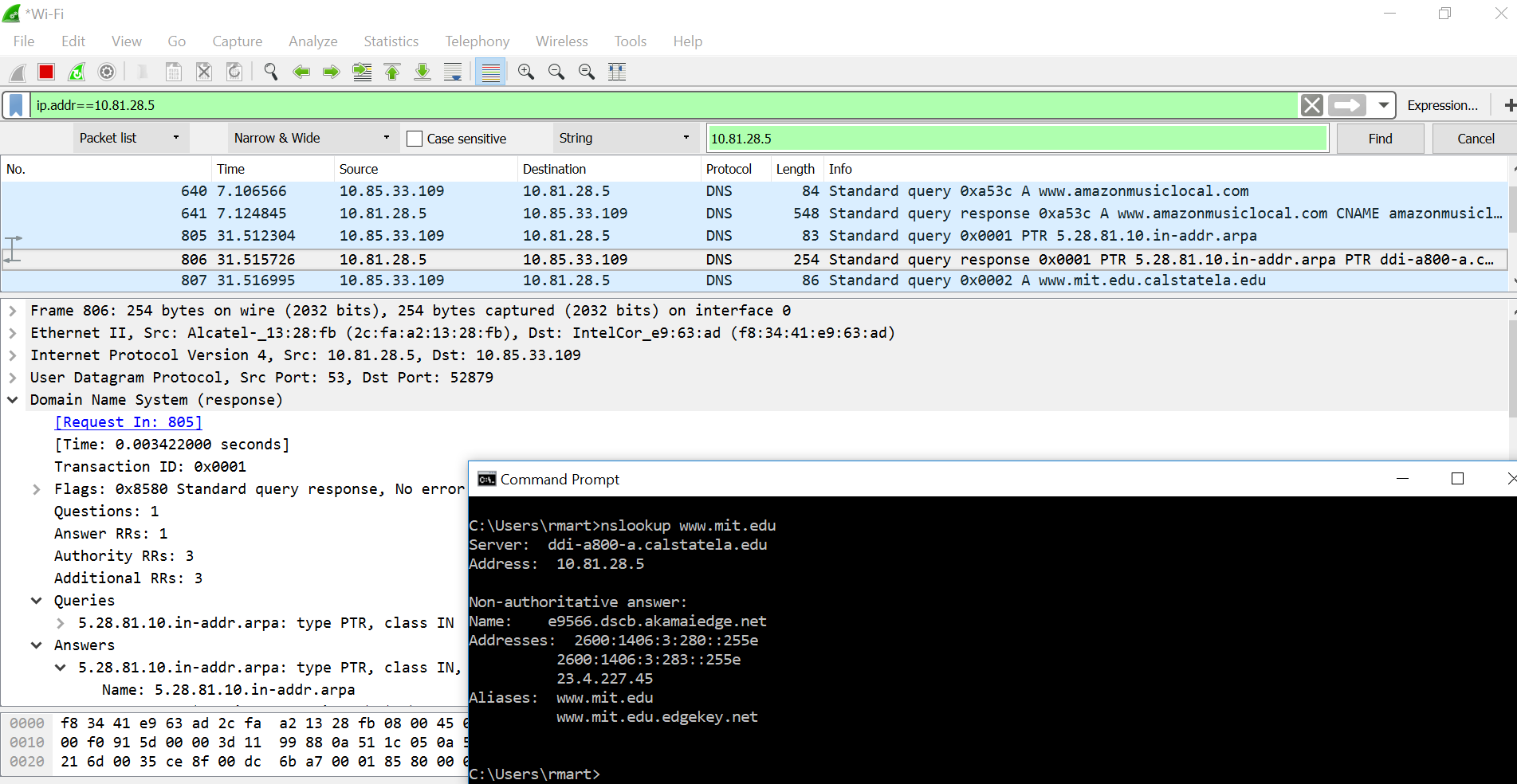


1. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

The DNS response message contains ***4 different answers***.



1. **Provide a screenshot**

****

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

The IP address that was sent was:

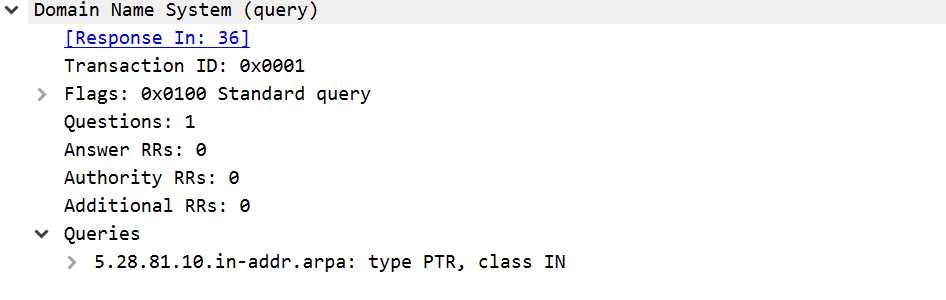
**C:\Users\rmart\AppData\Local\Microsoft\Windows\INetCache\Content.Word\16.png**

This is the default of my local DNS sever:

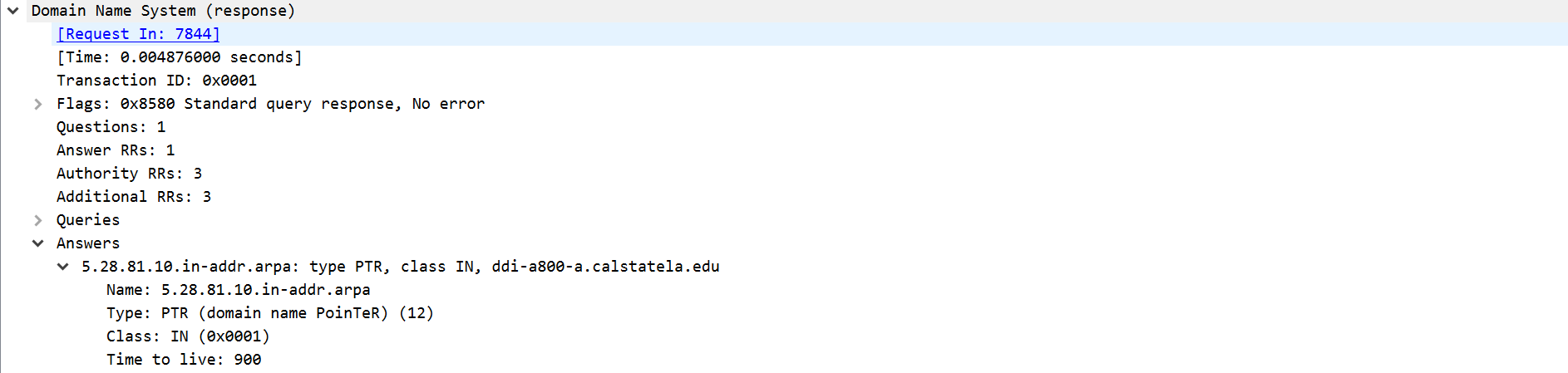
C:\Users\rmart\AppData\Local\Microsoft\Windows\INetCache\Content.Word\17.png

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

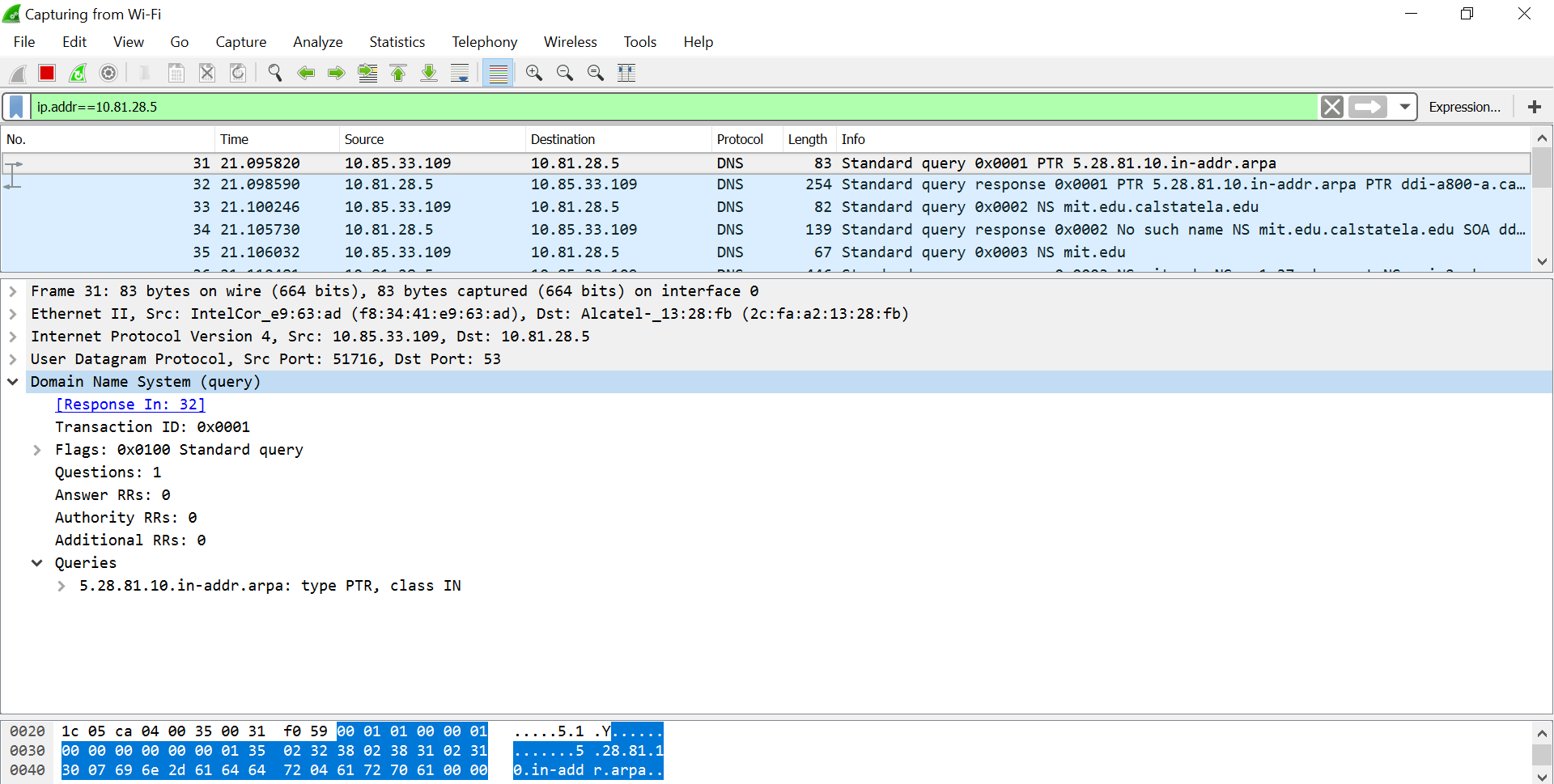
The DNS query message “Type” is ***PTR***.



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?**

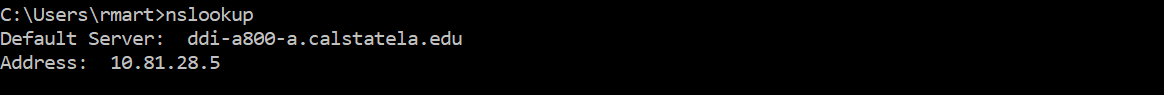
The MIT nameserver response message provides the name of: “***5.28.81.10.in-addr.arpa***”. However, there is ***no IP address***.

1. **Provide a screenshot.**



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?**

The IP address was sent to ***10.81.28.5***. C:\Users\rmart\AppData\Local\Microsoft\Windows\INetCache\Content.Word\#20.png

Yes, this information is the same as my default local DNS server. 

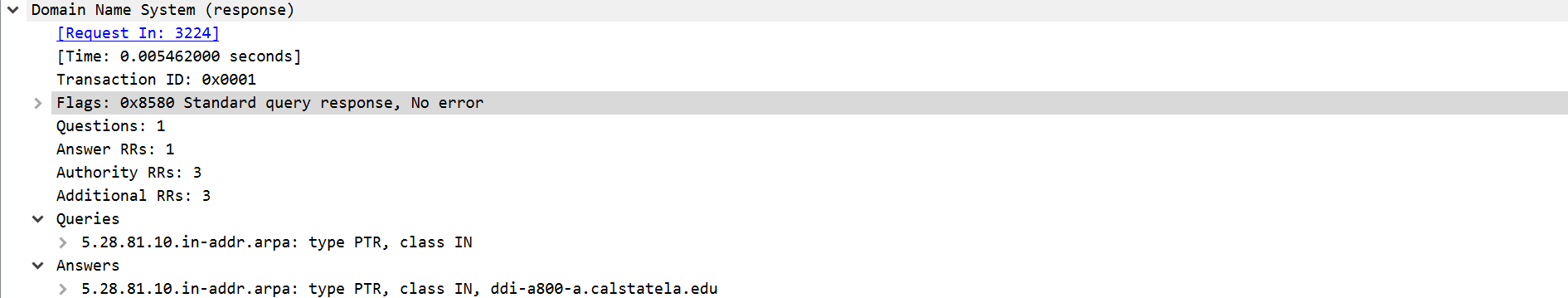
1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

The type of the DNS query is “***PTR***”. The query does not contain any answers.

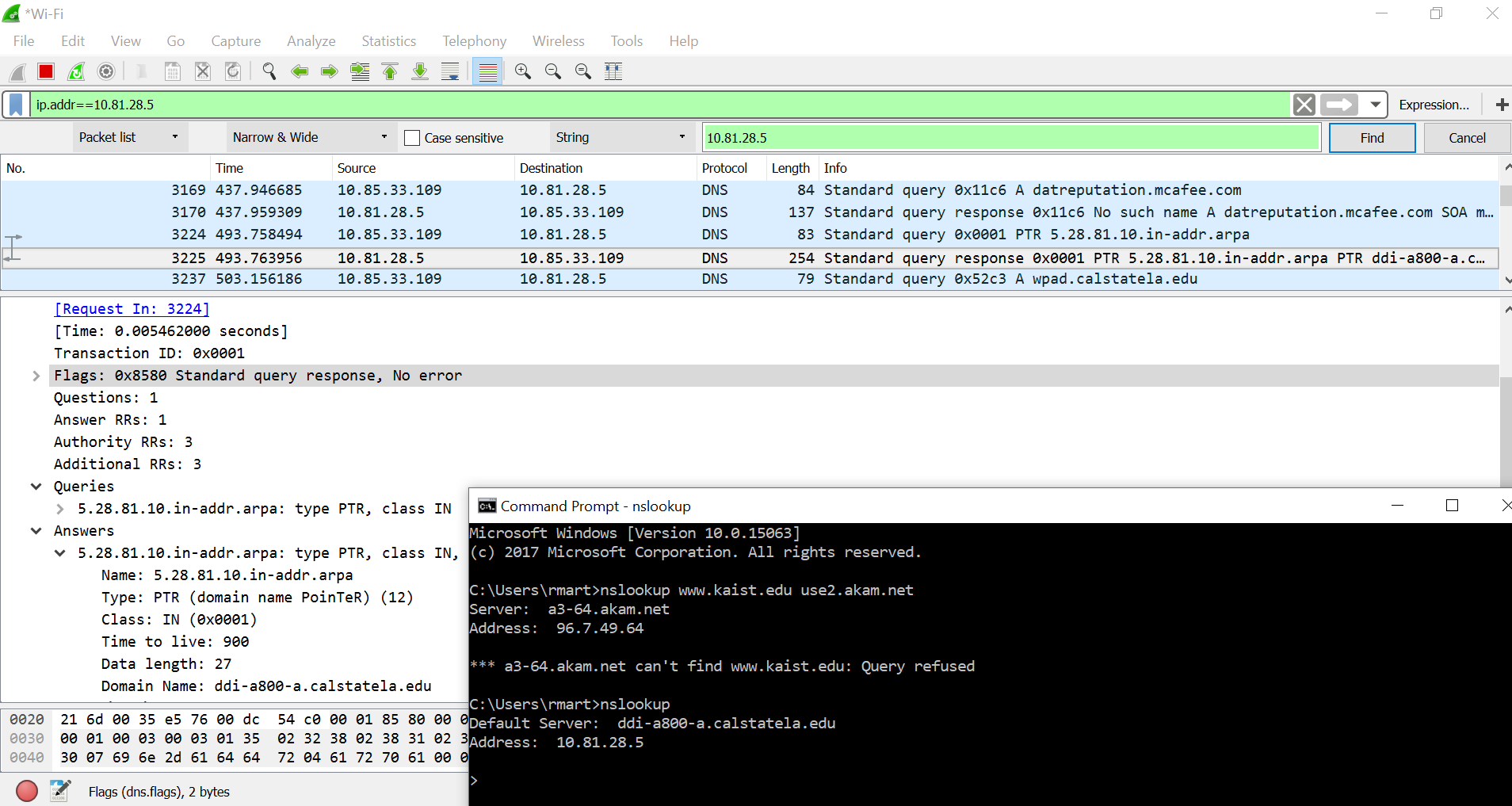
****

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

There is only one answer provided as my DNS response message. My one and only answer contains a type of PTR (Domain Name Pointer).



1. **Provide a screenshot**

****