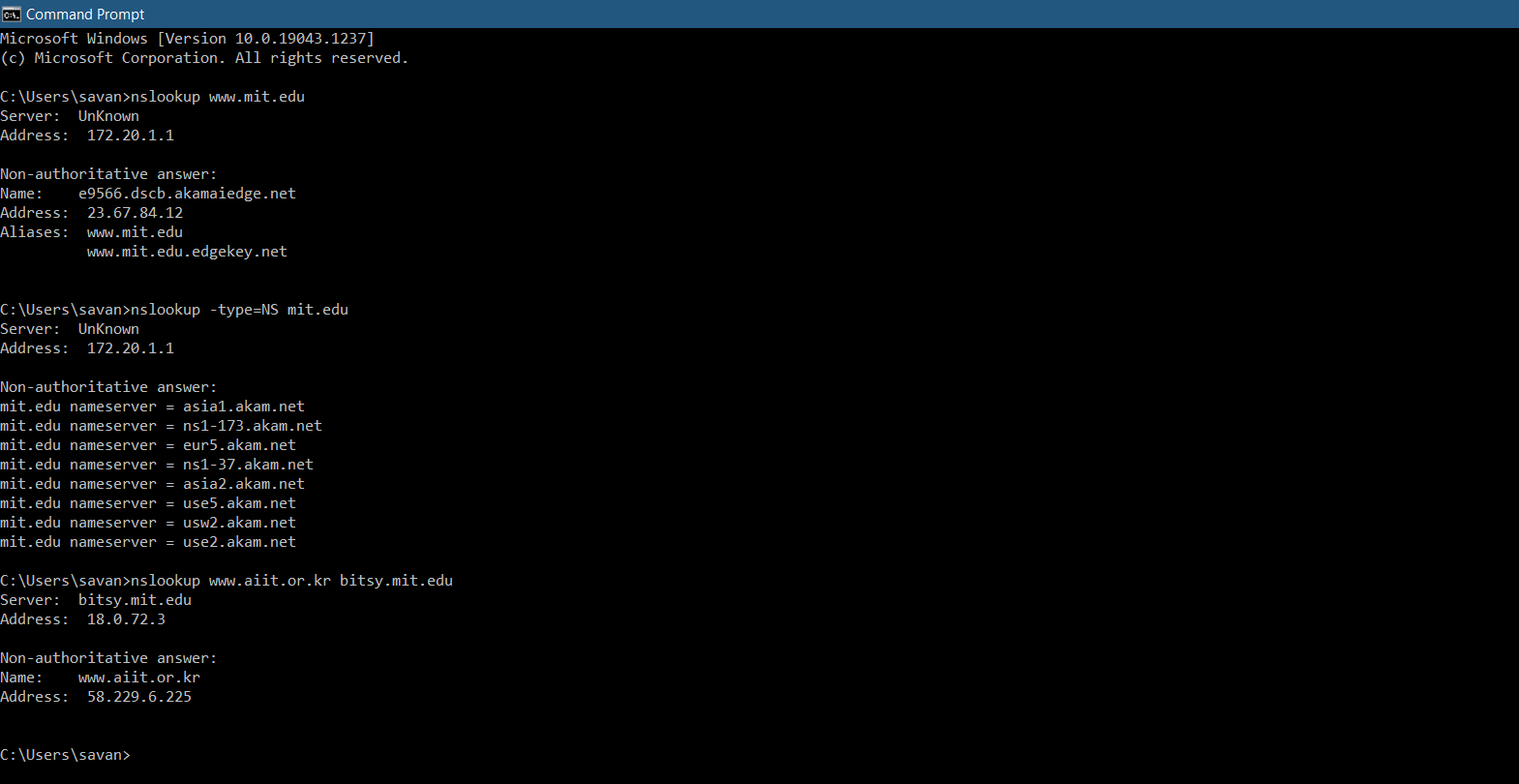
**NAME:** Savan Yeshwanth Rao

**CSUID:** 2784780

**LAB-2 DNS REPORT**

* **Command prompt screenshot:**

****

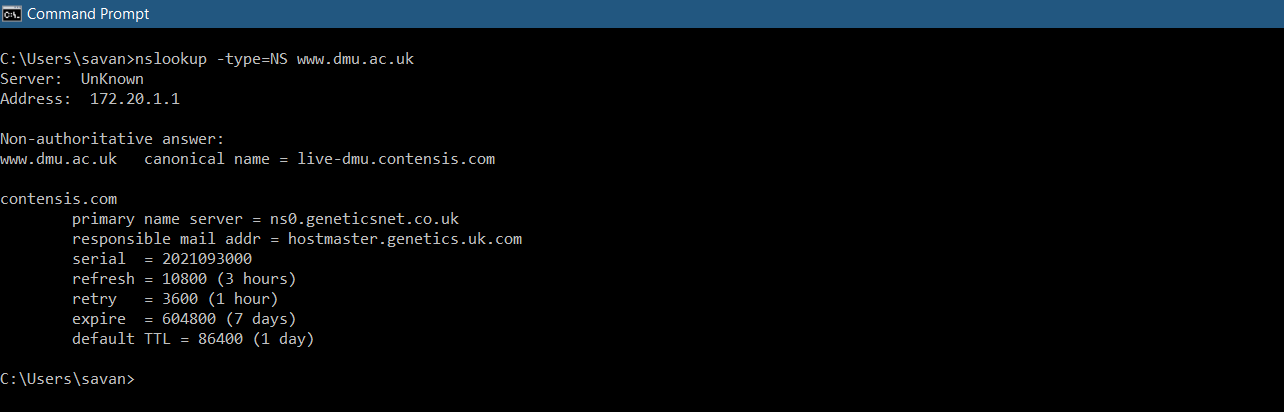
**PART-1**

1. Ran nslookup to obtain IP address of Acharya Institute of technology in India i.e., www.acharya.ac.in.

IP address of that server was – 103.120.179.52



1. De Montfort University in, UK i.e. [www.dmu.ac.uk](http://www.dmu.ac.uk) dns server= ns0.geneticsnet.co.uk

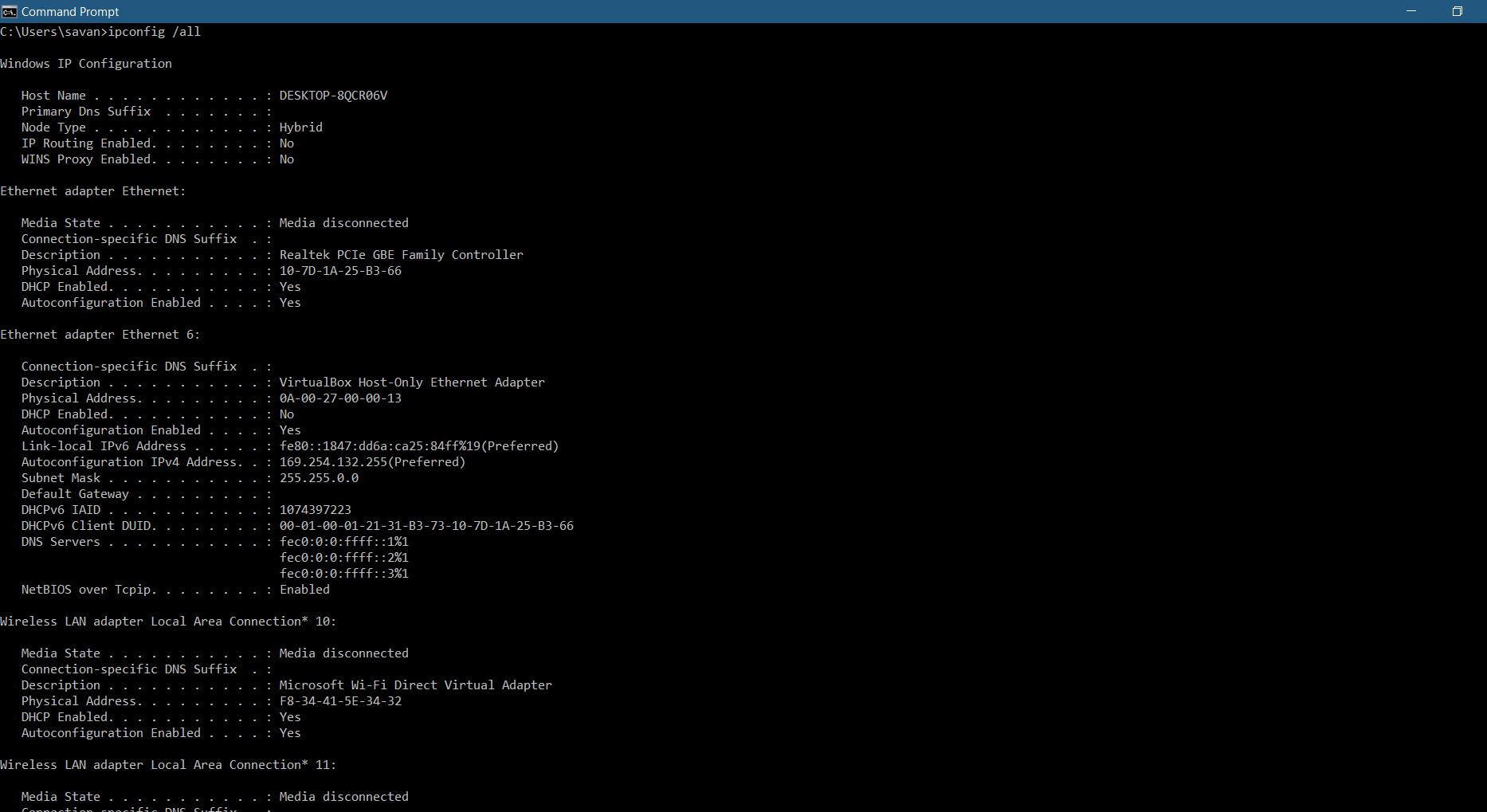


1. For mail service for Yahoo! Mail server and its IP address is- 209.73.179.253

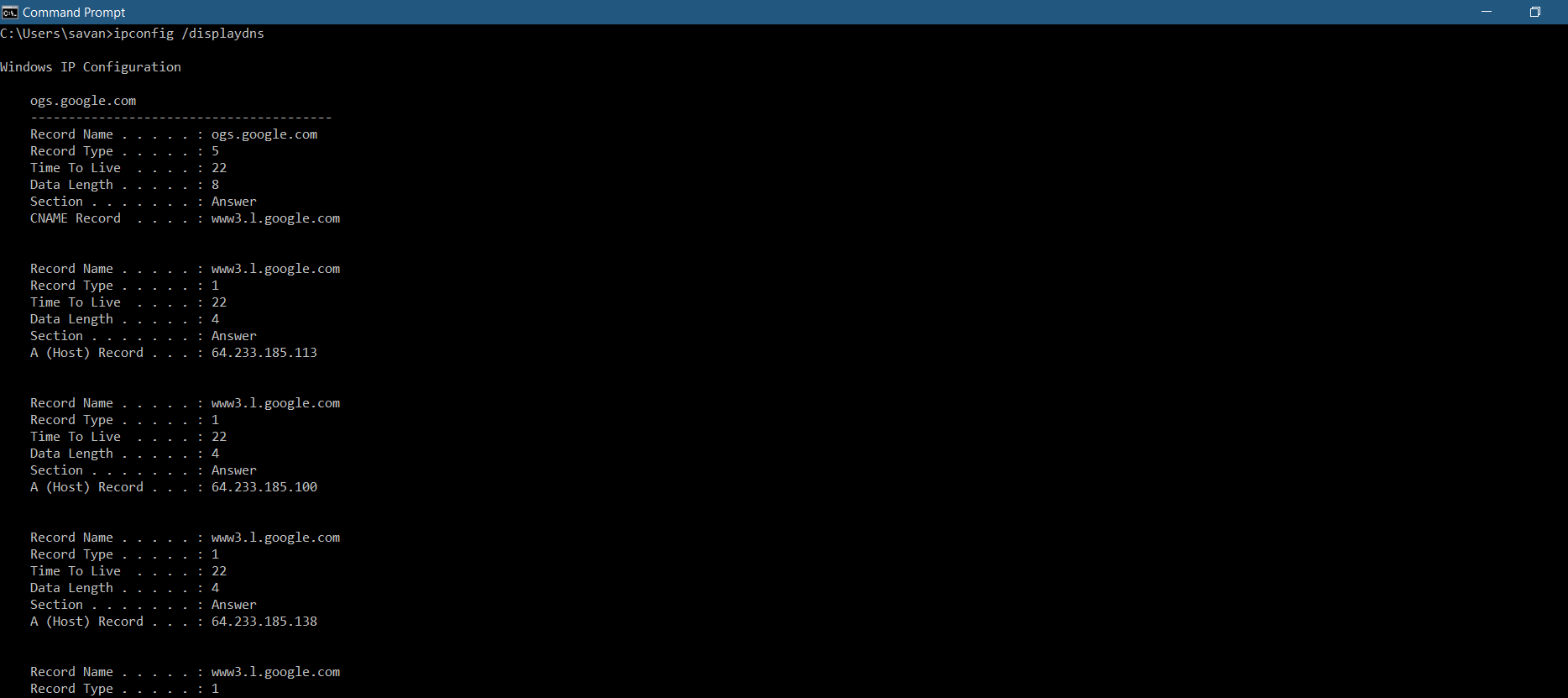


**PART-2**

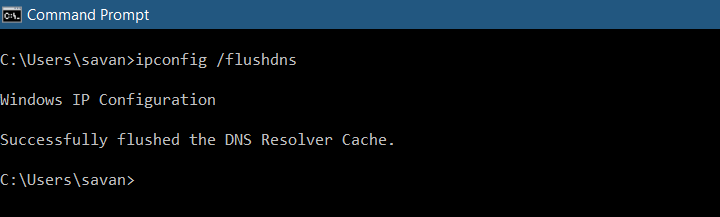
* Ipconfig /all:



* Ipconfig /displaydns:

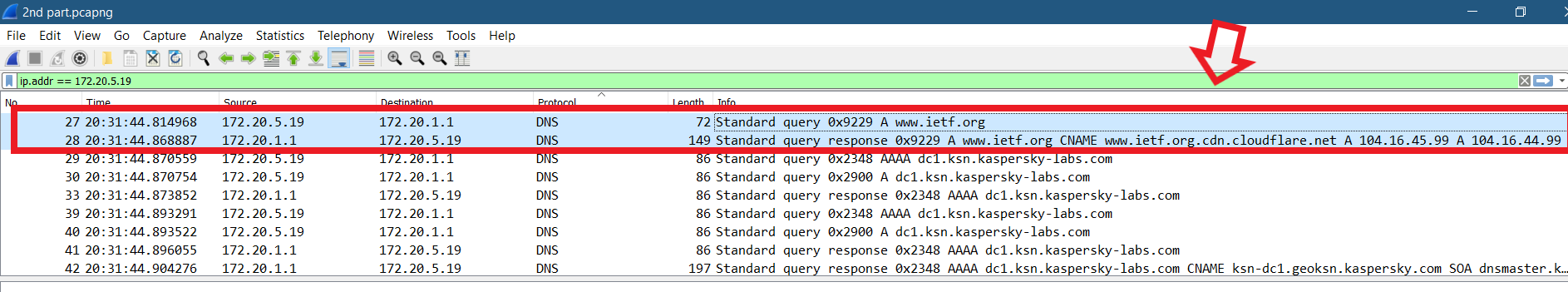


* Ipconfig /flushdns:

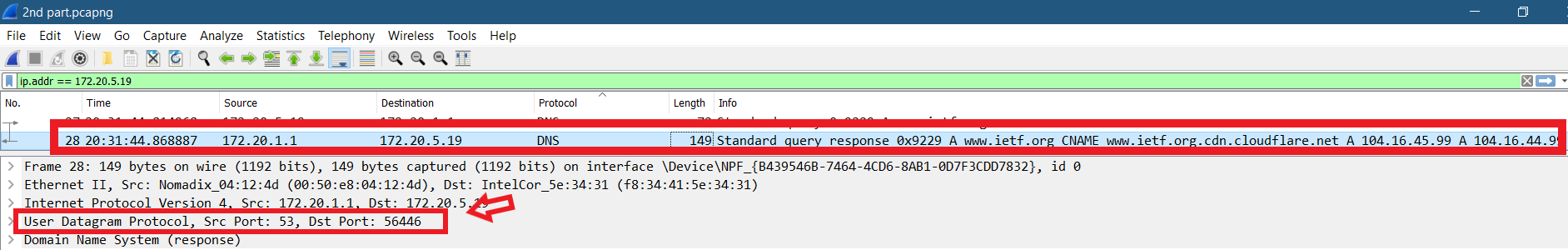
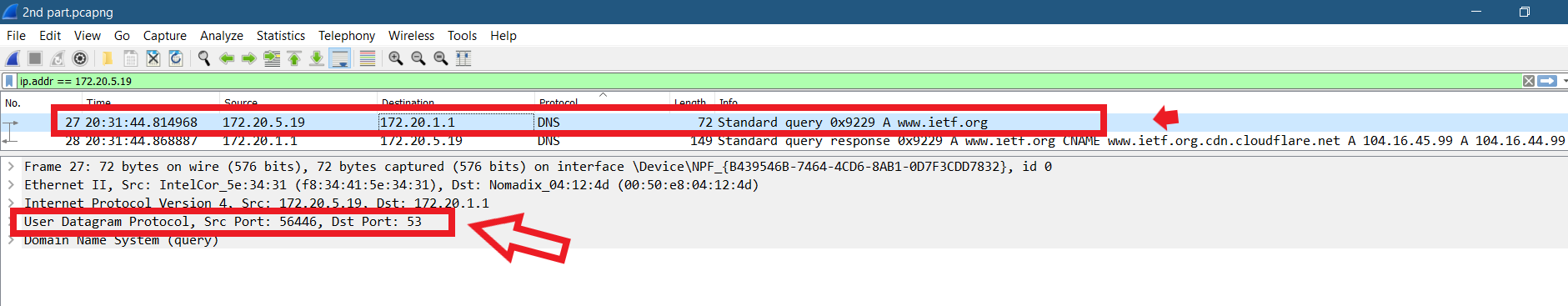


**PART-3: Tracing DNS with Wireshark:**

1. Locating the DNS query and response message:

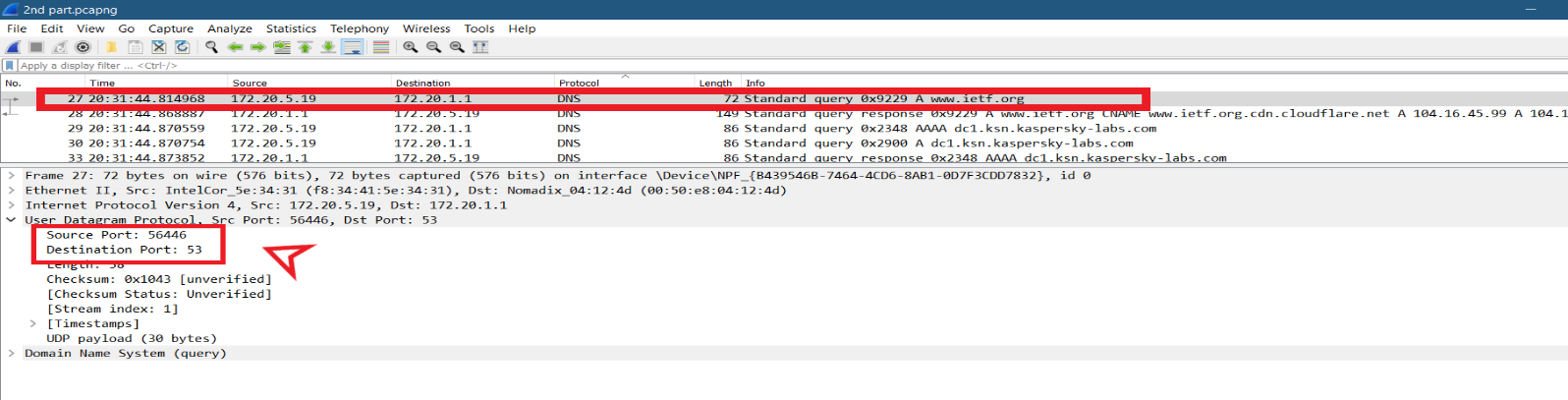


And both the query and the query response use **UDP (User Datagram Protocol)**



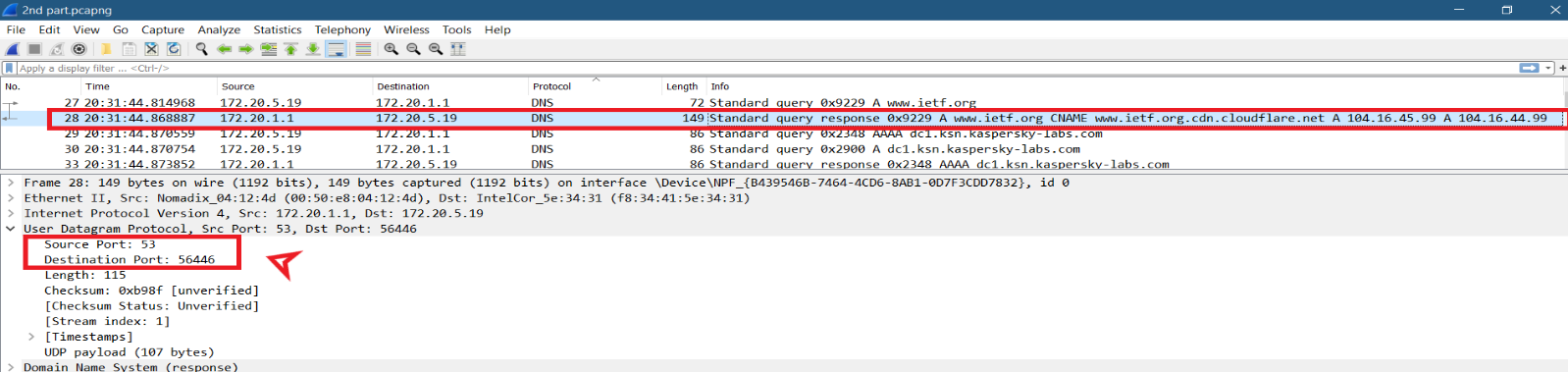
1. The ports of DNS query message:

* Source port: 56446 and Destination port: 53



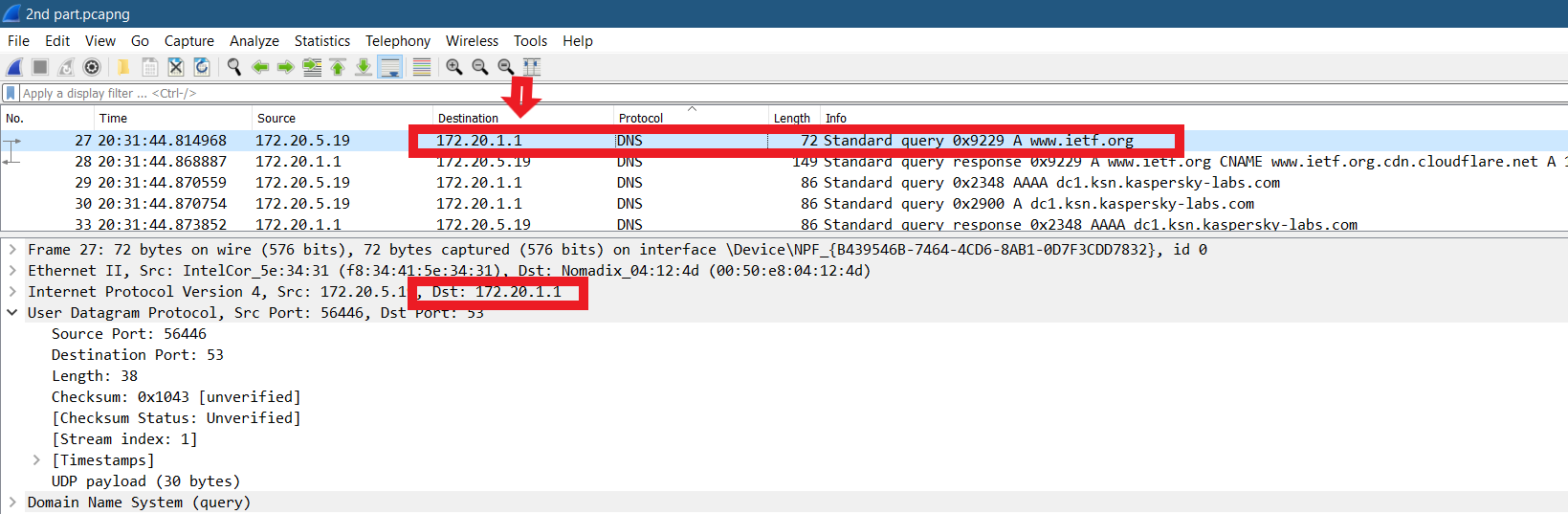
The Ports of DNS response message:

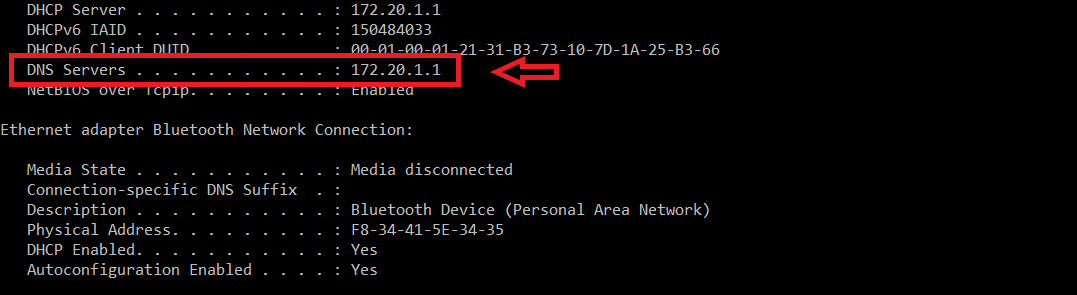
* Source port: 53 and the Destination port: 56446



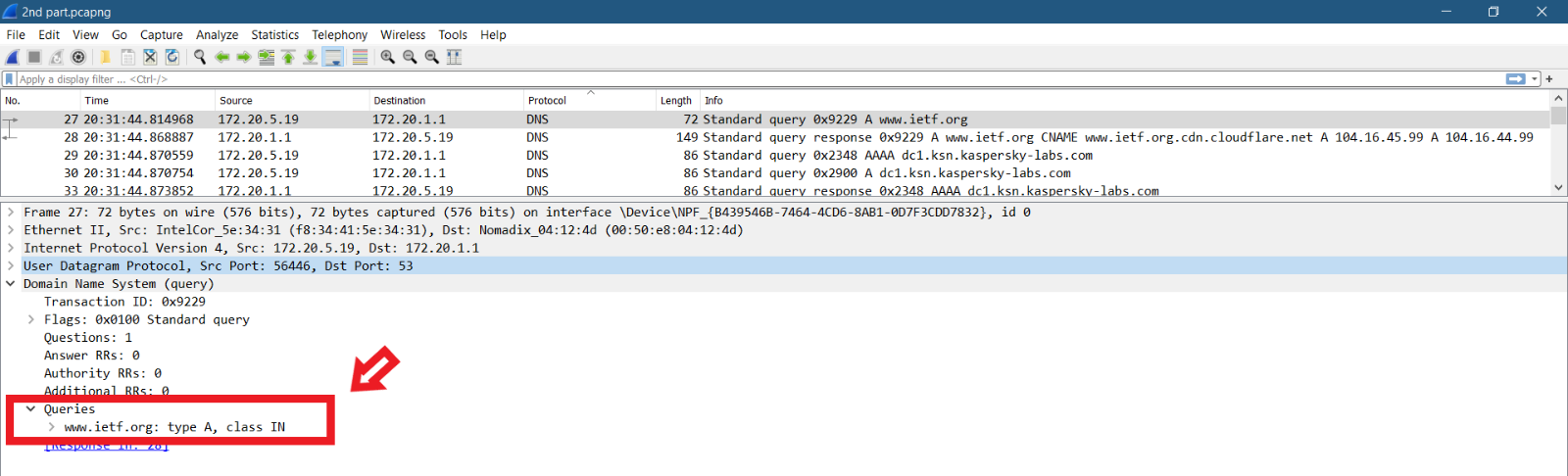
1. The IP address to which the DNS query message was sent was: **172.20.1.1**

Yes, both the DNS query message sent and the ipconfig ip address of my local DNS server were the same.

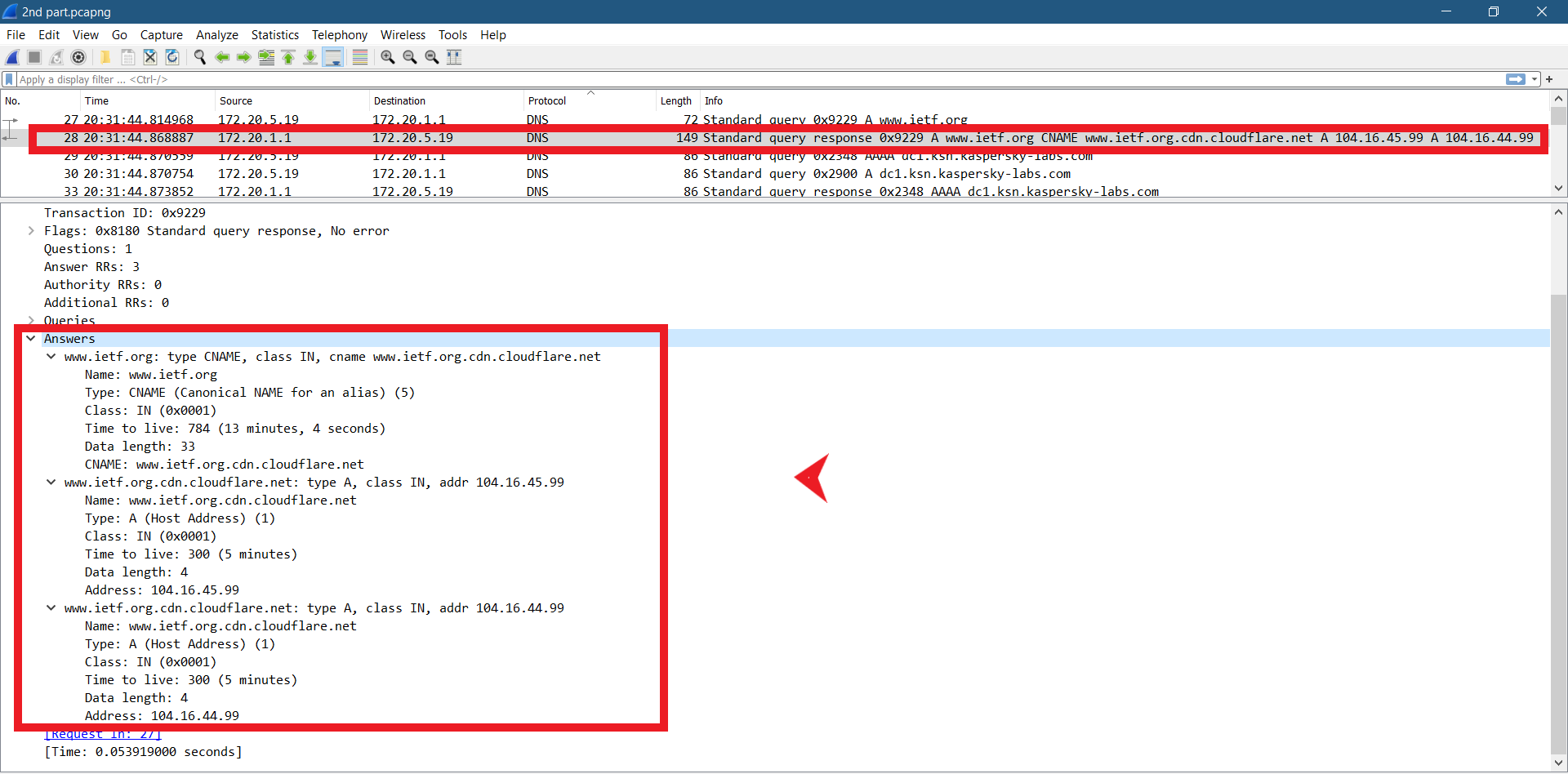




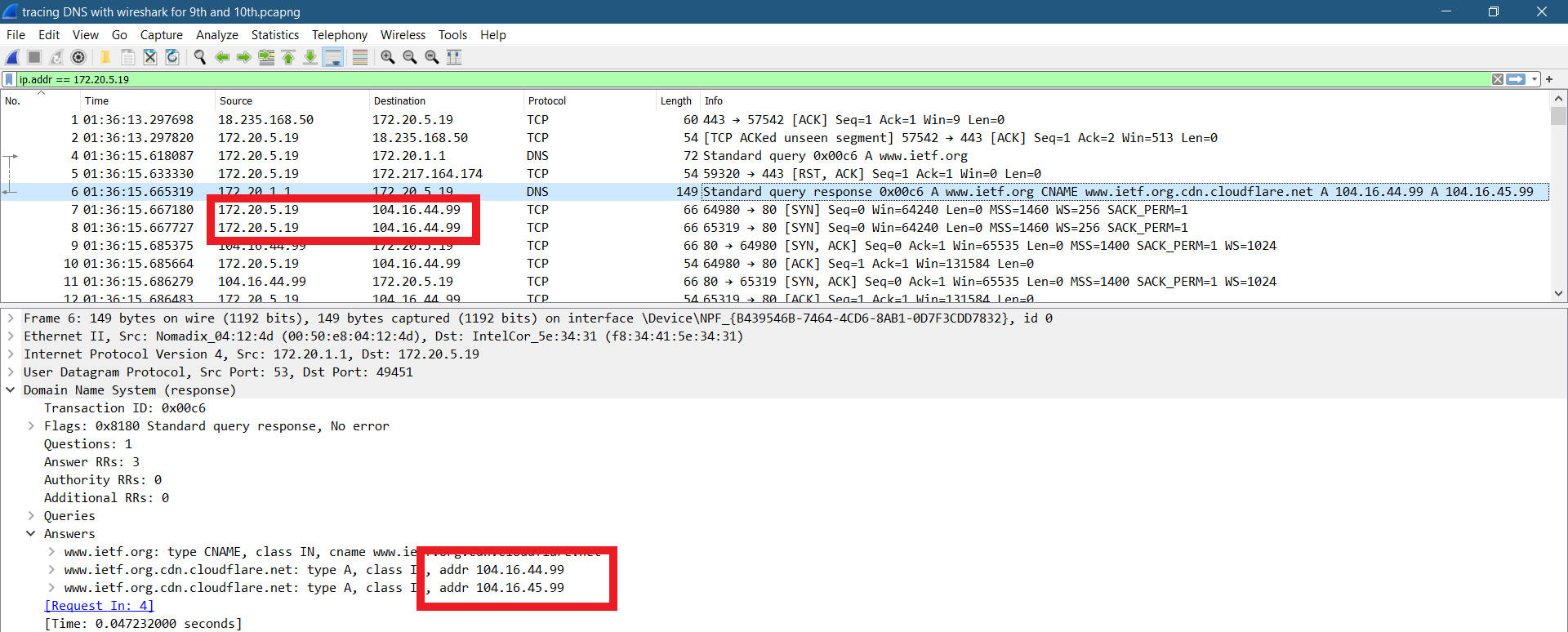
1. The DNS query message was a **Type “A”** query and as can see from the screenshot bellow there are **no answers.**



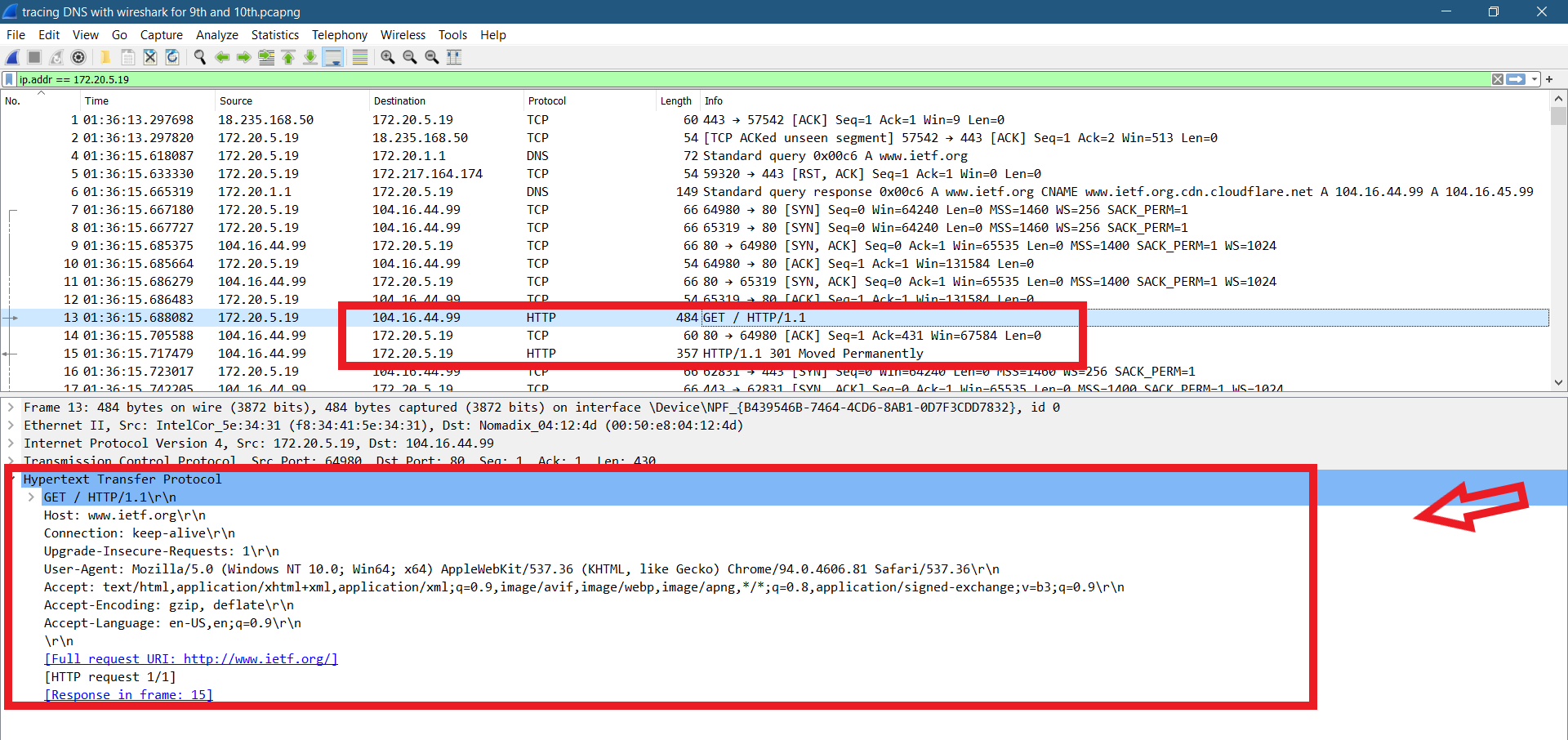
1. There are **3 answers** provided in DNS response message. Each answer contains **Name, Type, Class, Time to live, Data Length, CNAME.**



1. The destination IP of the SYN packet is **104.16.44.99.** It is the same address that was provide in DNS response message as the type A.



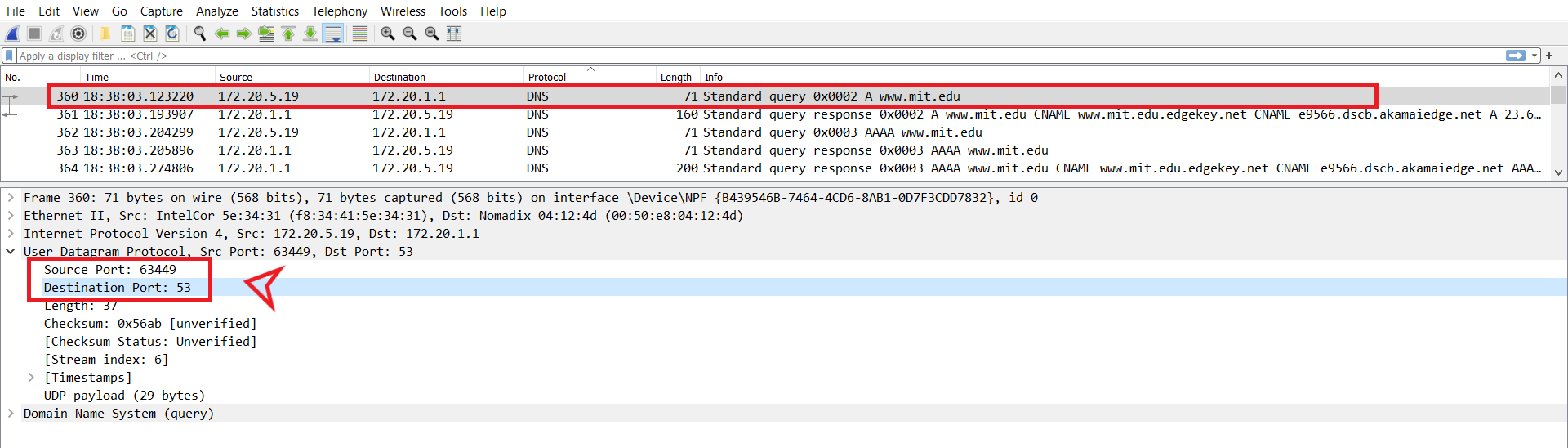
1. **Yes,** my host did issue a new DNS quire before retrieving images.



* **Nslookup** [**www.mit.edu**](http://www.mit.edu)**:**

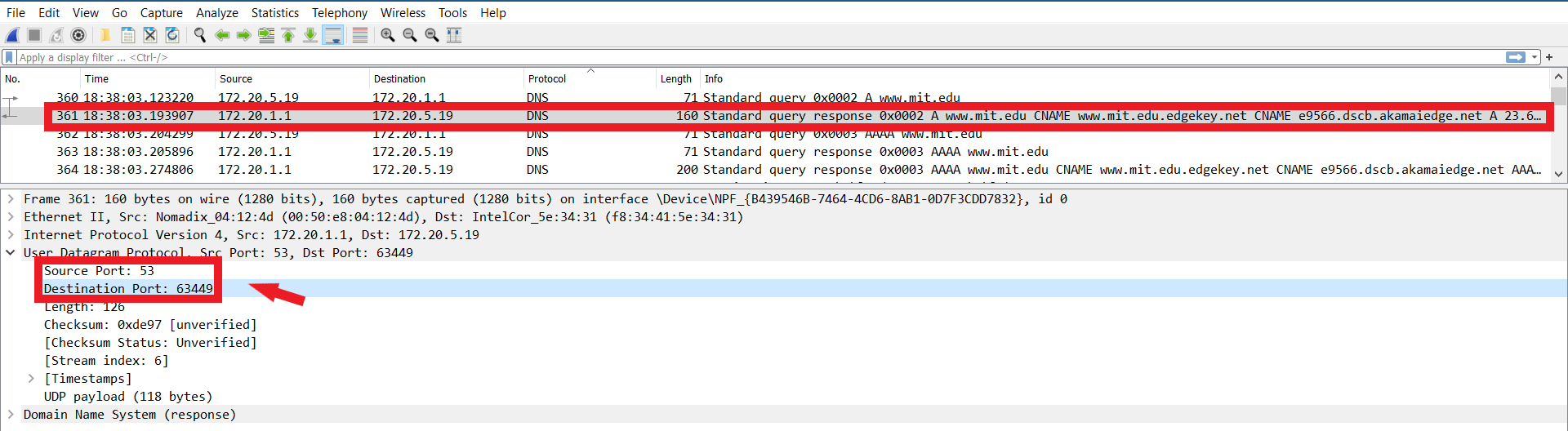
1. The ports of DNS query message:

* Source port: 63449 and Destination port: 53



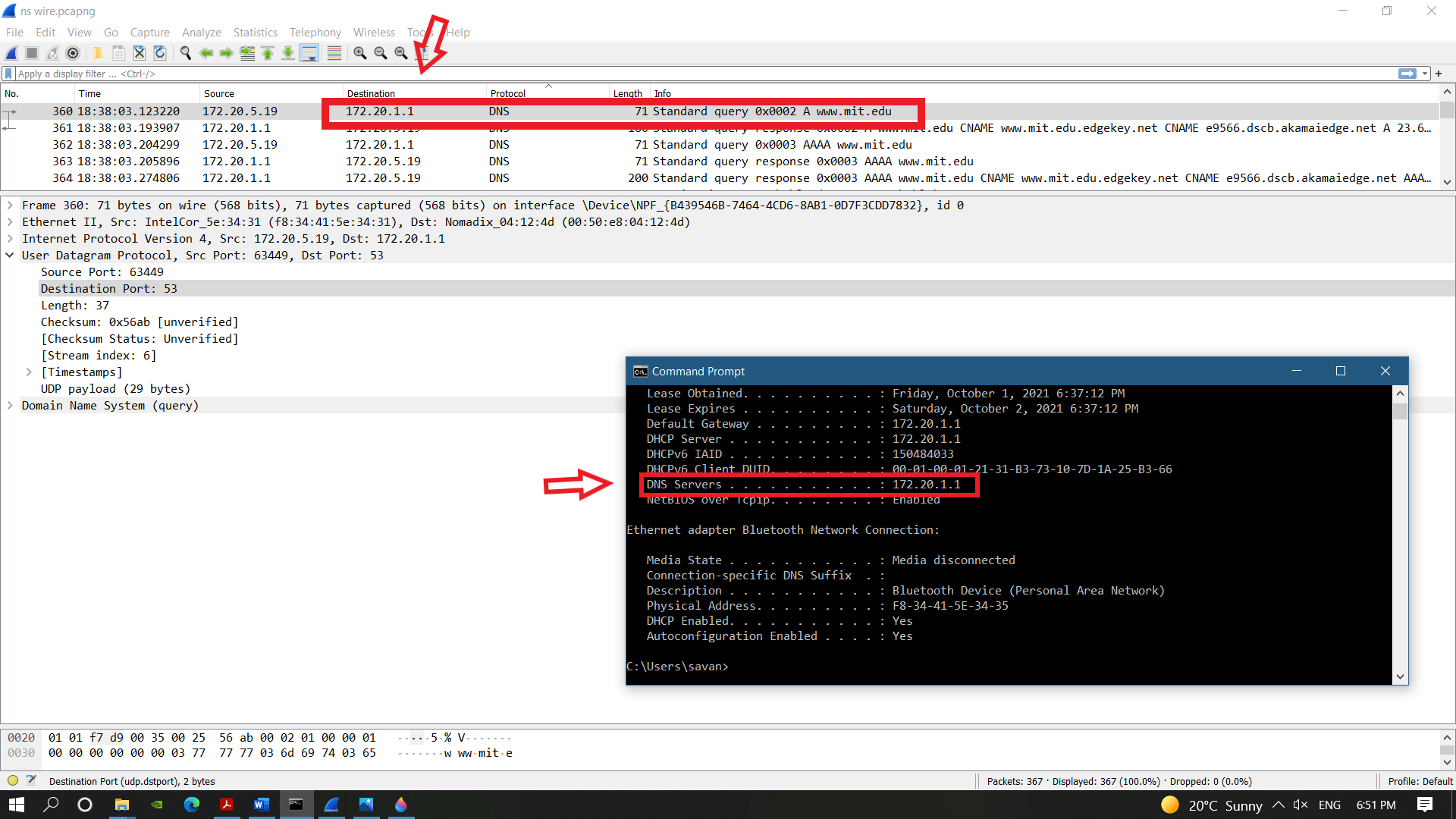
The Ports of DNS response message:

* Source port: 53 and the Destination port: 63449

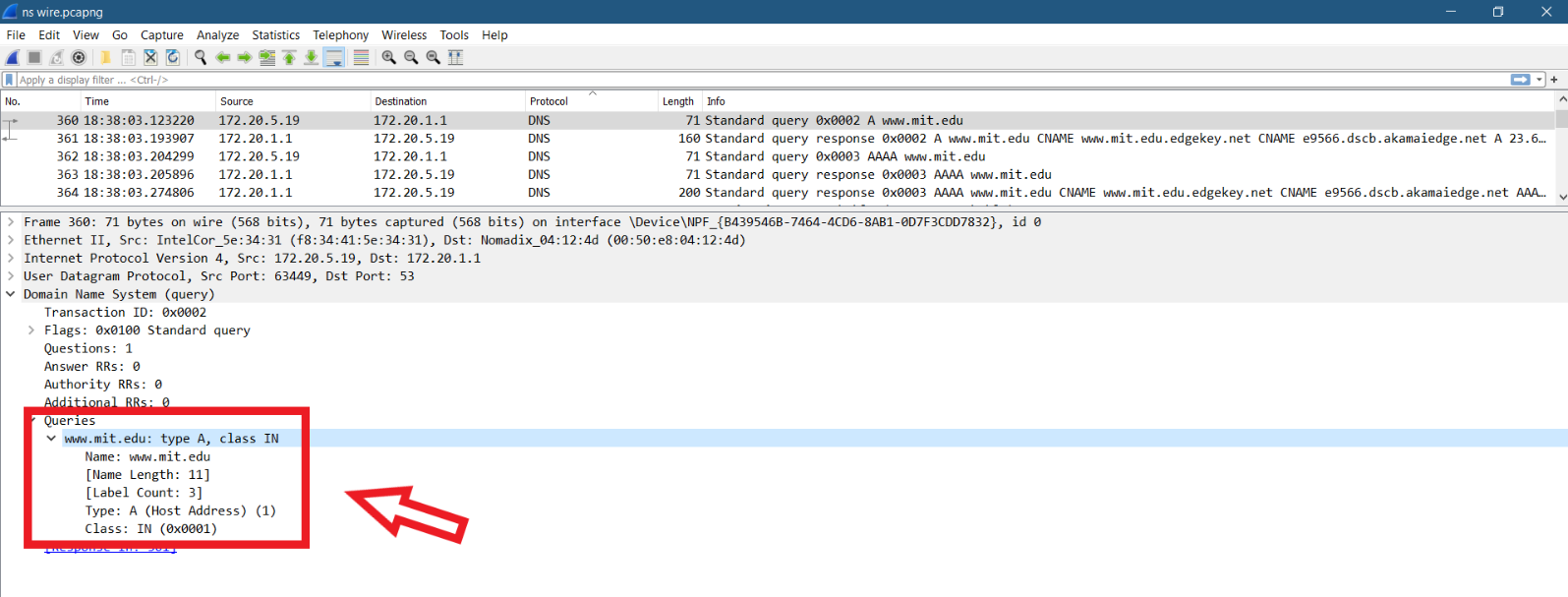


1. The DNS query message was sent to IP address- **172.20.1.1**

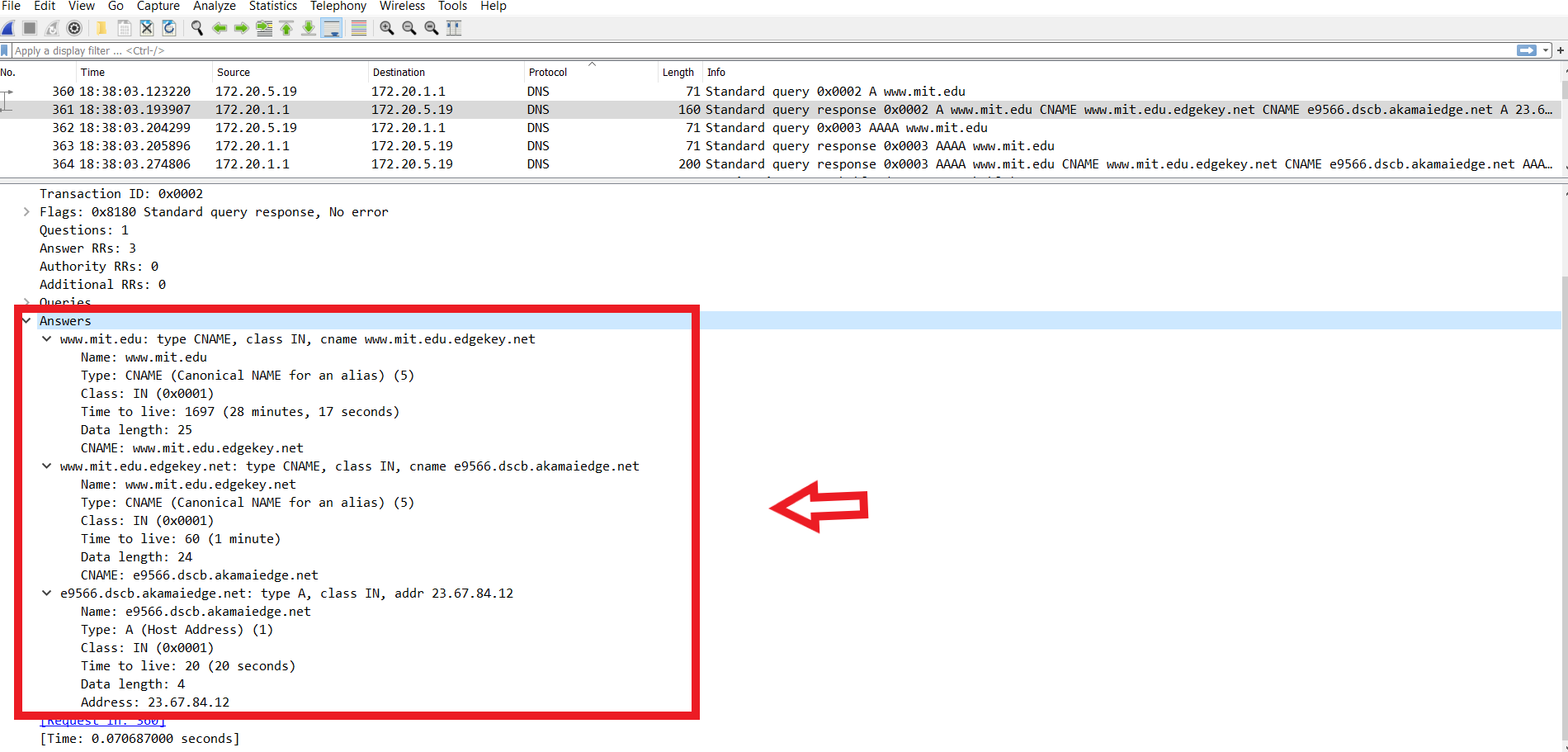
**YES,** both the IP address are same.



1. The DNS query message was a **Type “A”** query and as can see from the screenshot bellow there are **no answers.**

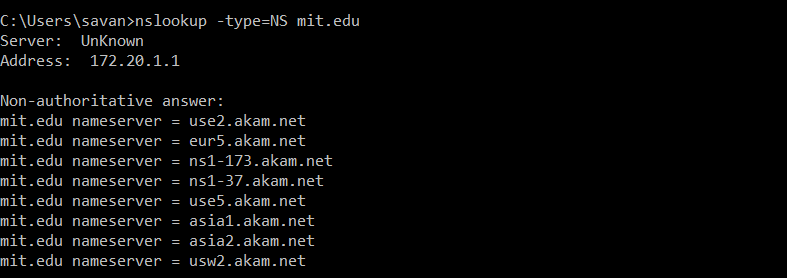


1. There are **3 answers** provided in DNS response message. Each answer contains **Name, Type, Class, Time to live, Data Length, CNAME and** the last answer contains **the Address.**

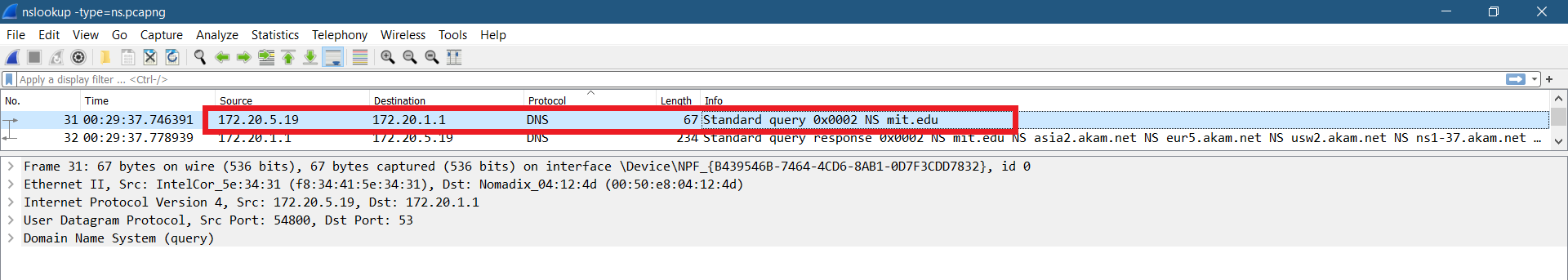


1. Screenshots are provided for each of the answers below.

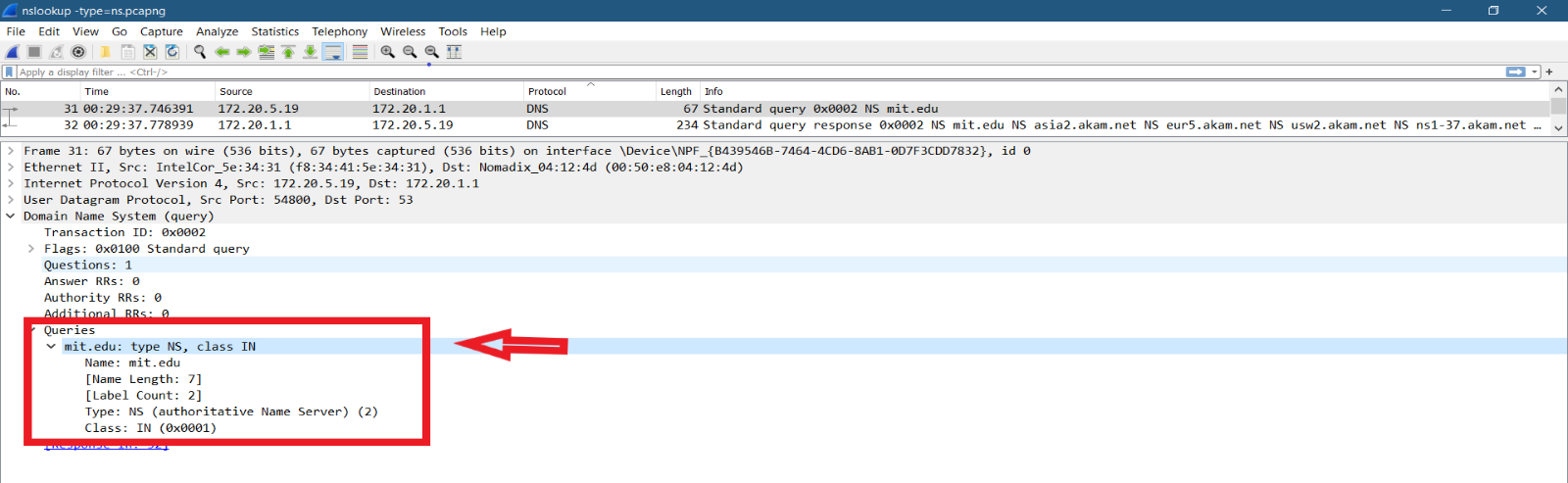
* **Nslookup -type=NS mit.edu**

****

1. The DNS query message was sent to IP address **172.20.1.1** and IP address of my default local DNS server is **172.20.5.19.**

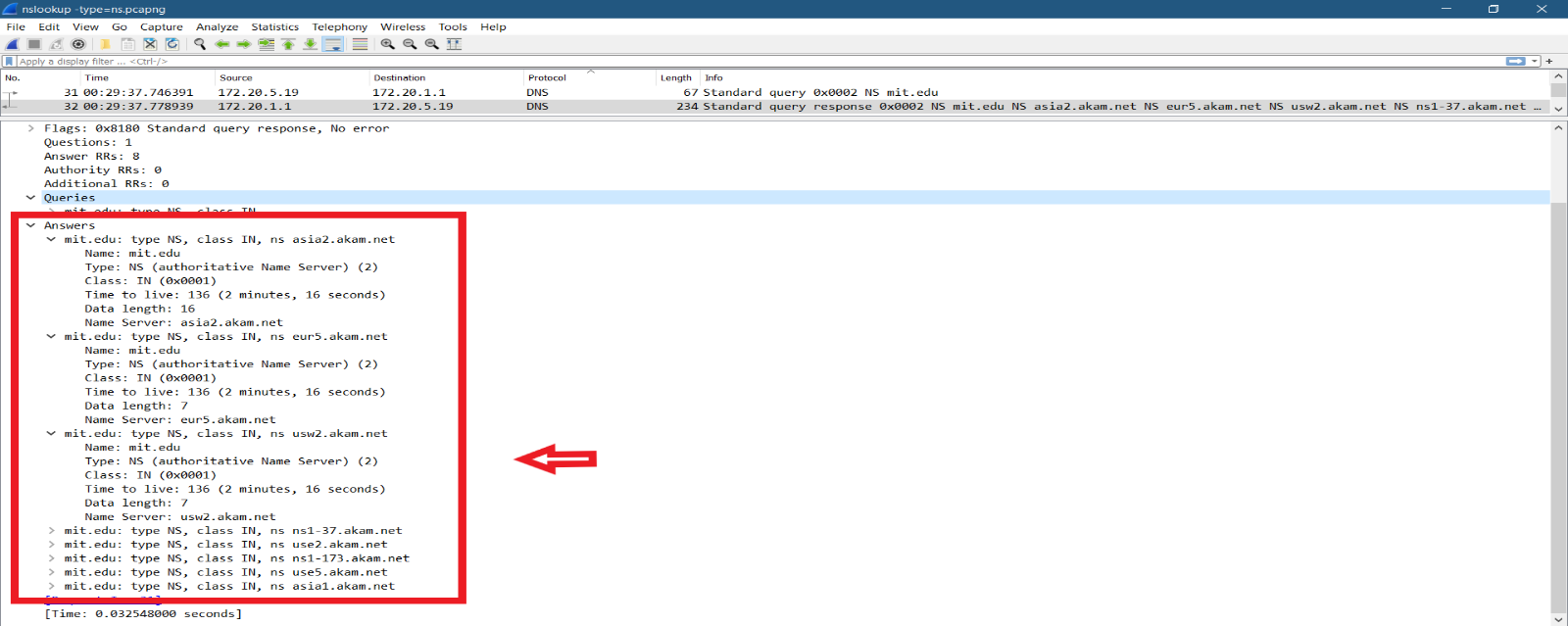


1. The DNS query message was a **Type “NS”** query and the query message has **no answers.**



1. The DNS response message provides 8 MIT nameservers answers which are:

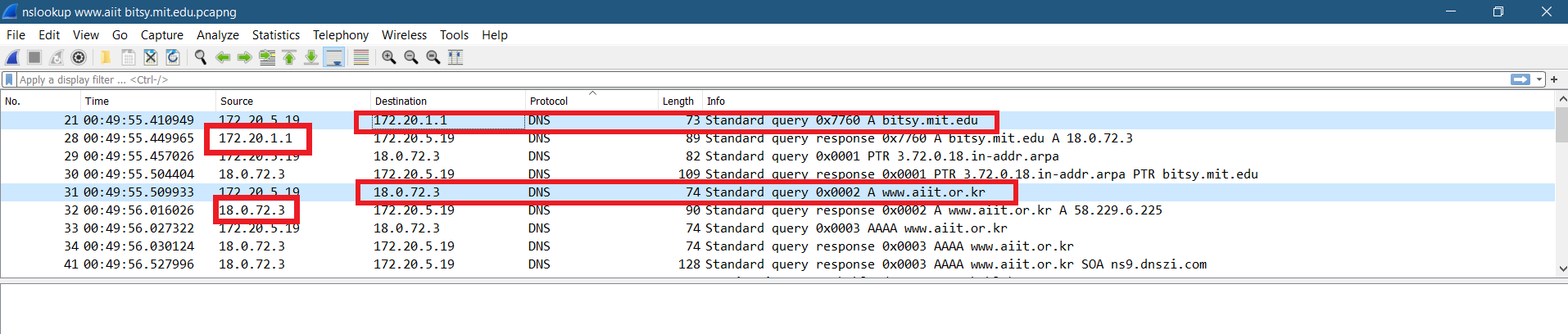
* asia2.akam.net, eur5.akam.net, usw2.akam.net, ns1-37.akam.net, use2.akam.net, ns1-173.akam.net, use5.akam.net, asia1.akam.net.
* NO, as we can see from the screenshot bellow there is no address field or any IP address in any of the MIT nameservers. But it includes name, type, class, time to live, data length, and the name server field.



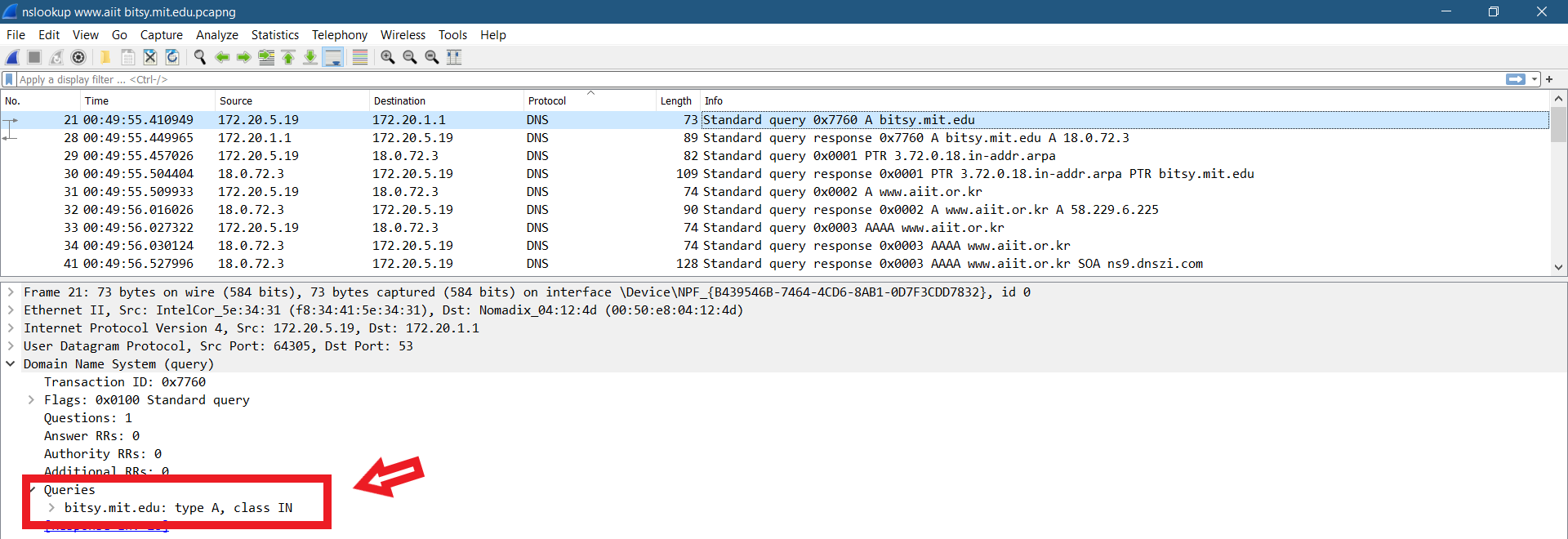
1. Screenshots are provided for each of the answers below.

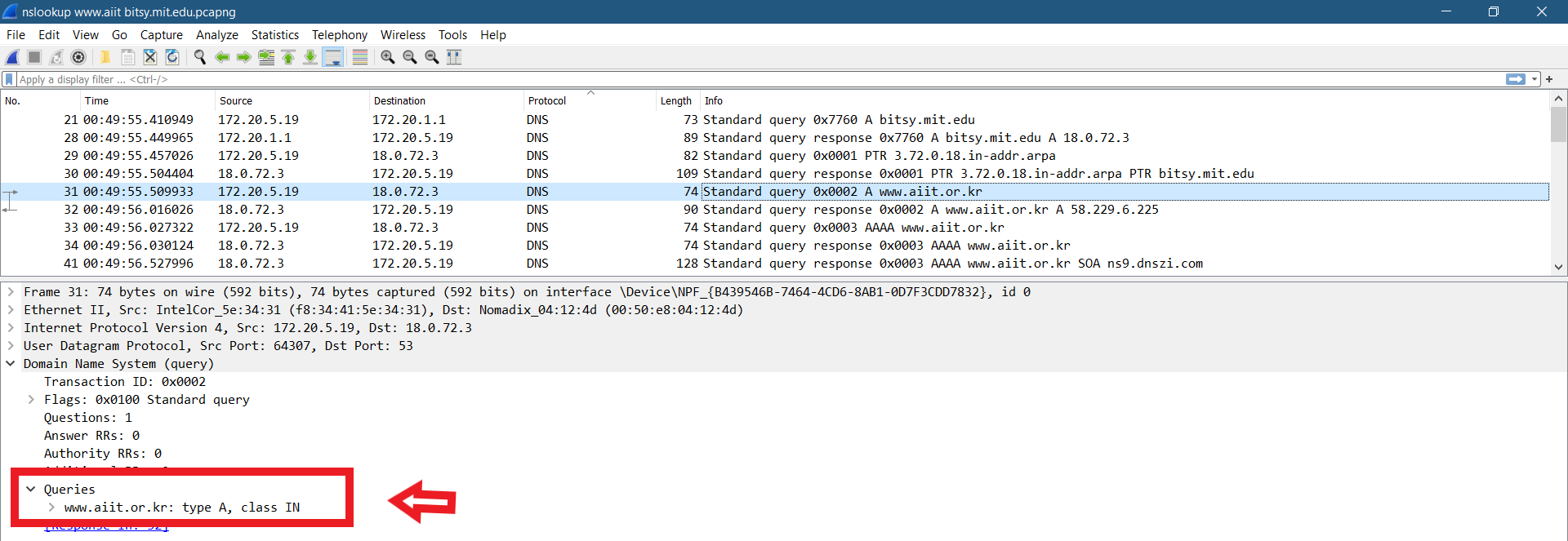
* **nslookup** [**www.aiit.or.kr**](http://www.aiit.or.kr) **bitsy.mit.edu**

1. The DNS query message IP address for bitsy.mit.edu is 172.20.1.1 and for [www.aiit.or.kr](http://www.aiit.or.kr) is 18.0.72.3 which is the IP address of the MIT DNS response sender.

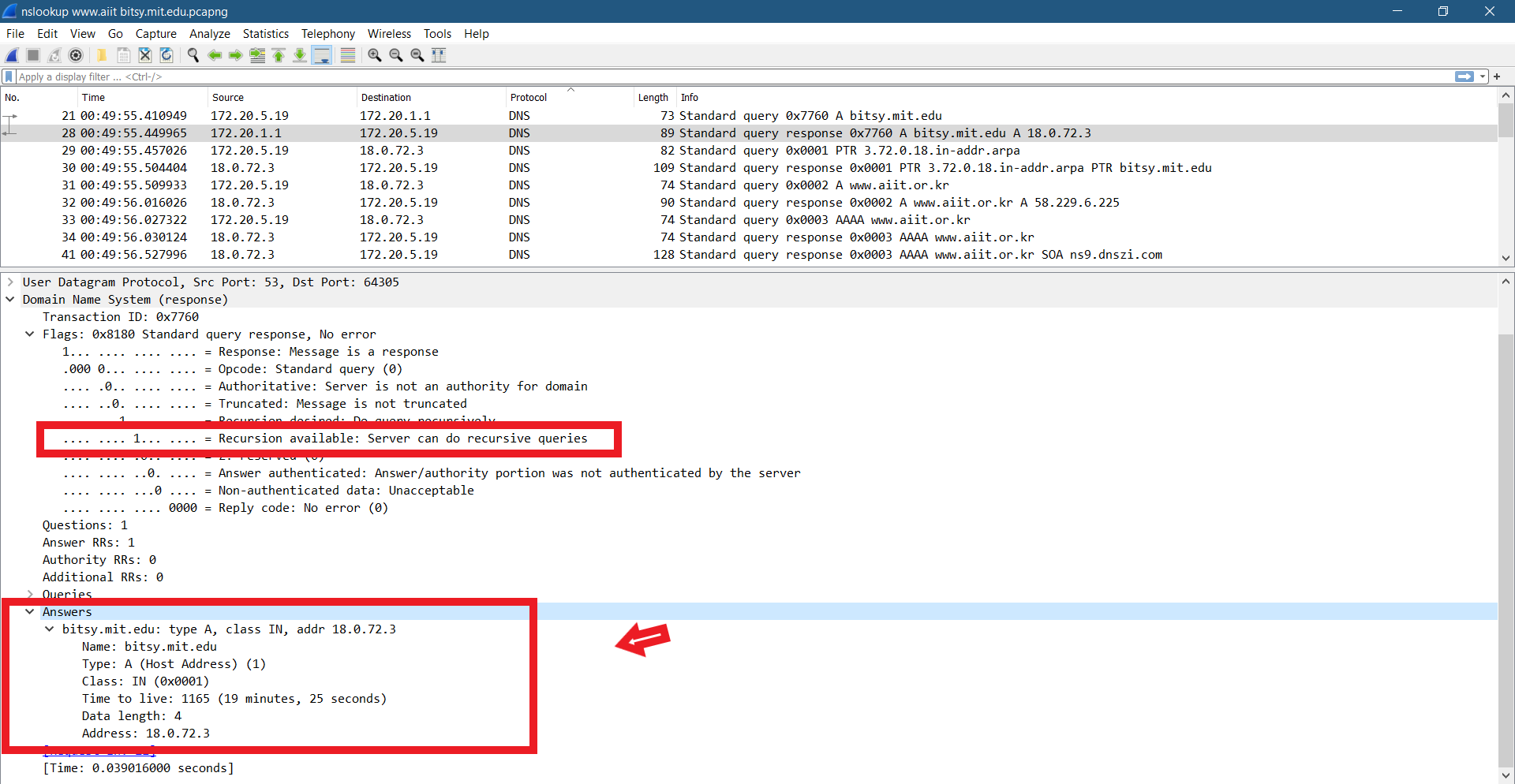


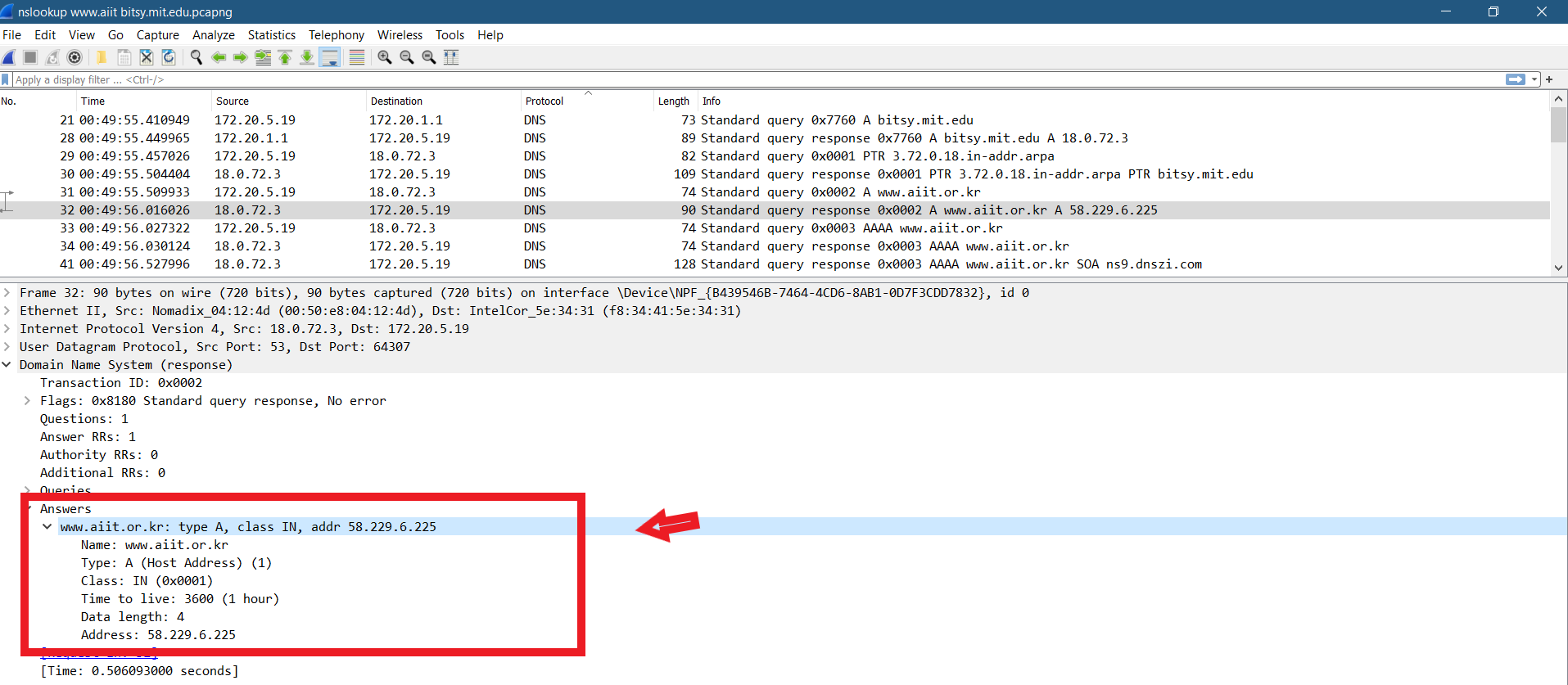
1. The DNS query message was a **Type “A”** query and the query message has **no answers.**





1. The DNS response message provide only **one answer** and each answer contains **name**, **type**, **class, time to live, data length and address**. An also returns a flag where the server can do recursive queries.



****

1. Screenshots are provided bellow for each answers.