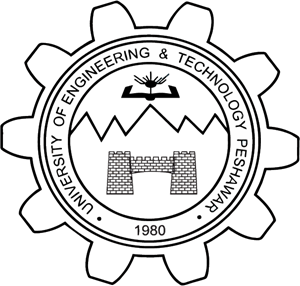
**CSE 303L: Data Communication and Computer Networks**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Demonstration** | **of** | **Poor** | | **(Does** | **not** | **meet** | | **Fair** |  | **(Meet** | | **Good** | | **(Exceeds** | | **Score** |
| **Concepts** |  | **expectation (1))** | | | |  |  | **Expectation (2-3))** | | |  | **Expectation (4-5)** | | |  |  |
|  |  |  |  |  |  |  |
|  |  | The | student | | failed | | to | The student demonstrated a | | | | The student demonstrated a clear | | | |  |
|  |  | demonstrate | | | a |  | clear |  |
|  |  |  | clear understanding of some | | | | understanding of the assignment | | | |  |
|  |  | understanding | | | of |  | the |  |
|  |  |  | of the assignment concepts | | | | concepts | |  |  |  |
|  |  | assignment concepts | | | |  |  |  |  | **30%** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | | | | | |  |  |  | |  |  |  |  |  |
| **Accuracy** |  | The student mis-configured | | | | | | The | student | configured | | The | student | configured | the |  |
|  |  | enough network settings that | | | | | | enough network settings that | | | | network settings that the lab | | | |  |
|  |  | the | lab | computer couldn't | | | | the lab computer partially | | | | computer fully functioned on the | | | |  |
|  |  | function | | properly | | on | the | functioned on the network | | | | network | |  |  |  |
|  |  | network | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **30%** |
|  | |  | | | | | |  | | | |  | | | |  |
| **Following Directions** | | The student clearly failed to | | | | | | The student failed to follow | | | | The student followed the verbal | | | |  |
|  |  | follow the verbal and written | | | | | | the some of the verbal and | | | | and | written | instructions | to |  |
|  |  | instructions to | | | successfully | | | written | instructions | | to | successfully | | complete | |  |
|  |  | complete the lab | | |  |  |  | successfully | | complete | all | requirements of the lab | | |  |  |
|  |  |  |  |  |  |  |  | requirements of the lab | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **20%** |
|  |  |  |  | |  | |  |  |  |  |  |  | | | |  |
| **Time Utilization** |  | The | student | | failed | | to | The | student | failed | to | The student completed the lab in | | | |  |
|  |  | complete even part of the lab | | | | | | complete the entire lab in | | | | its entirety in the allotted | | | |  |
|  |  | in the allotted amount of | | | | | | the allotted amount of time | | | | amount of time | |  |  |  |
|  |  | time |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **20%** |
|  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Credit Hours: 1** | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Lab report 05

**Wireshark**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**304L-Data Communcation and Computer Networks Lab**

**Department of Computer System Engineering**

**University of Engineering and Technology Peshawar**

Submitted to: **Dr. Yasir Saleem Afridi**

Submitted by: **Muhammad Saad**

Reg ID: **21PWCSE1997**

**DCSE, Batch 23, Section “B”**

Date: **Tue, Apr 23, 2024**

**Lab 05**

1. **The Domain Name System (DNS)** translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we’ll take a closer look at the client side of DNS. Recall that the client’s role in the DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back.

The hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client’s DNS query. From the DNS client’s standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

Tracing DNS with Wireshark

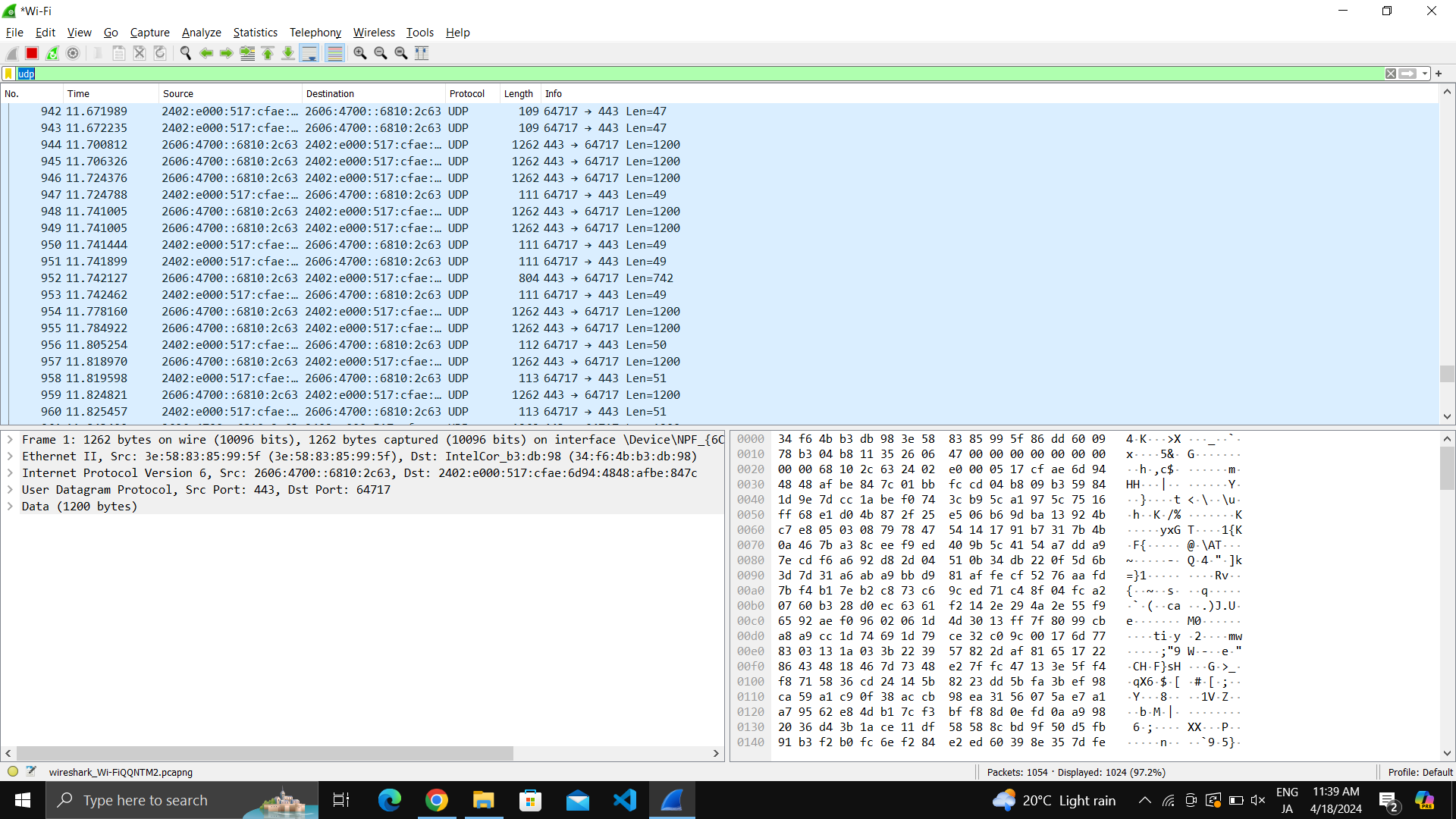
* Open Wireshark and enter “ip.addr == your\_IP\_address” into the filter, where

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.

To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

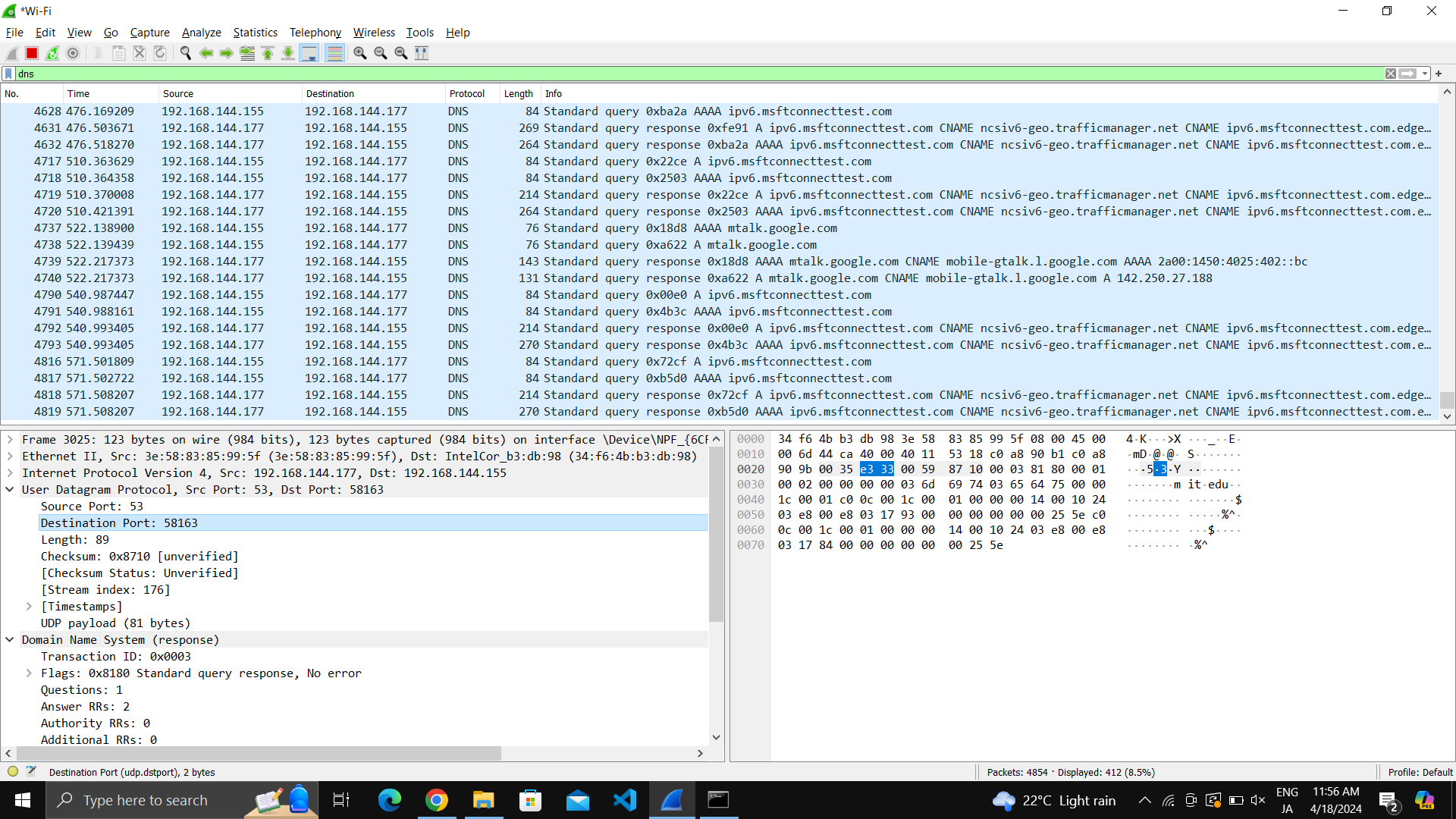
1. Locate the DNS query and response messages. Are then sent over UDP or TCP?



**Ans:** The captured packets from *ietf.com* show that the data is sent over UDP.

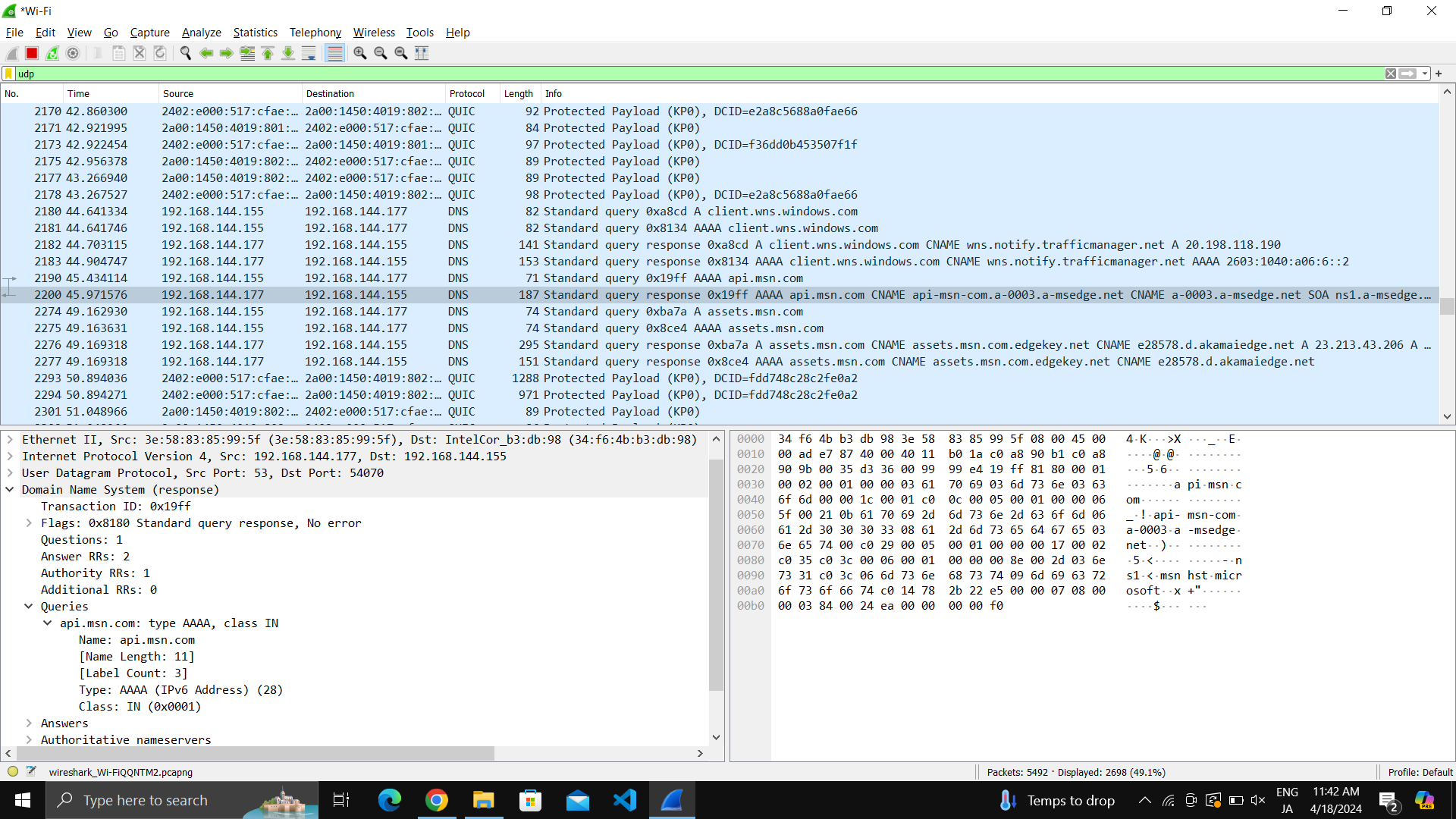
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

**Ans:** Destination port: 58163

 Source port: 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?

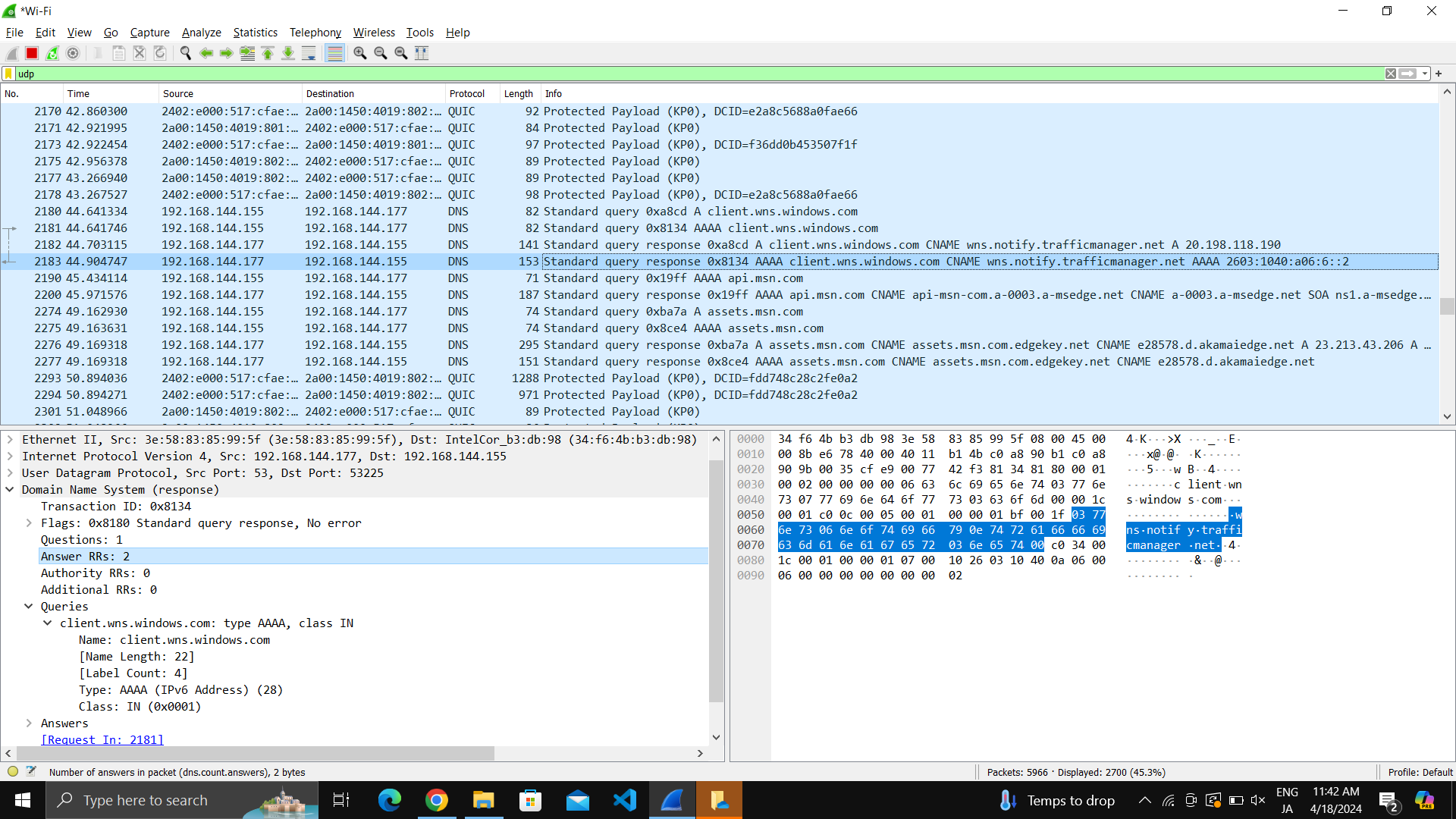
**Ans:** Yes the DNS server’s IP matches IP given in the terminal.



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

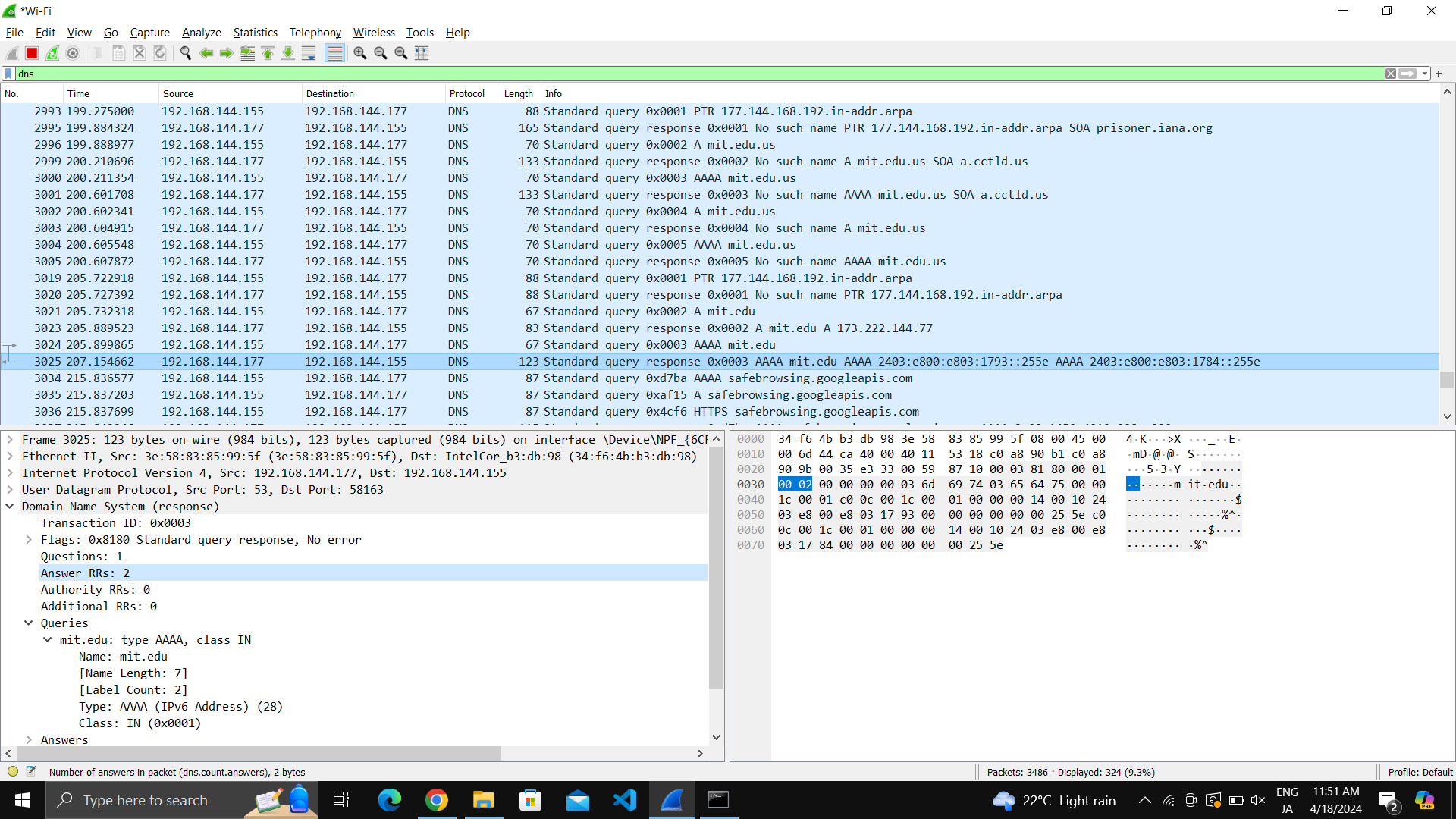
**Ans:** Type of DNS querry: AAAA

And yes the querry does have answers.

****

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

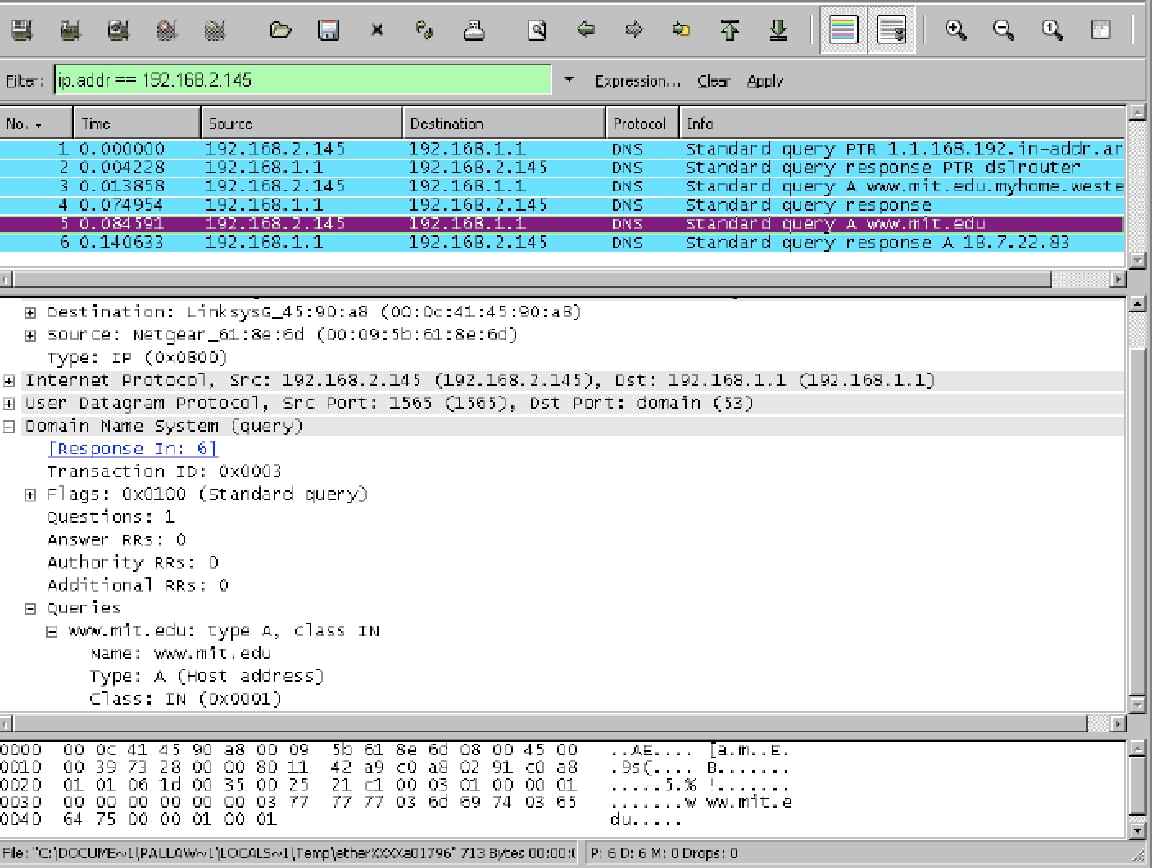
**Ans:** Answers: 2

****

Now let’s play with ***nslookup***.

* Start packet capture.
* Do an ***nslookup*** on www.mit.edu
* Stop packet capture.

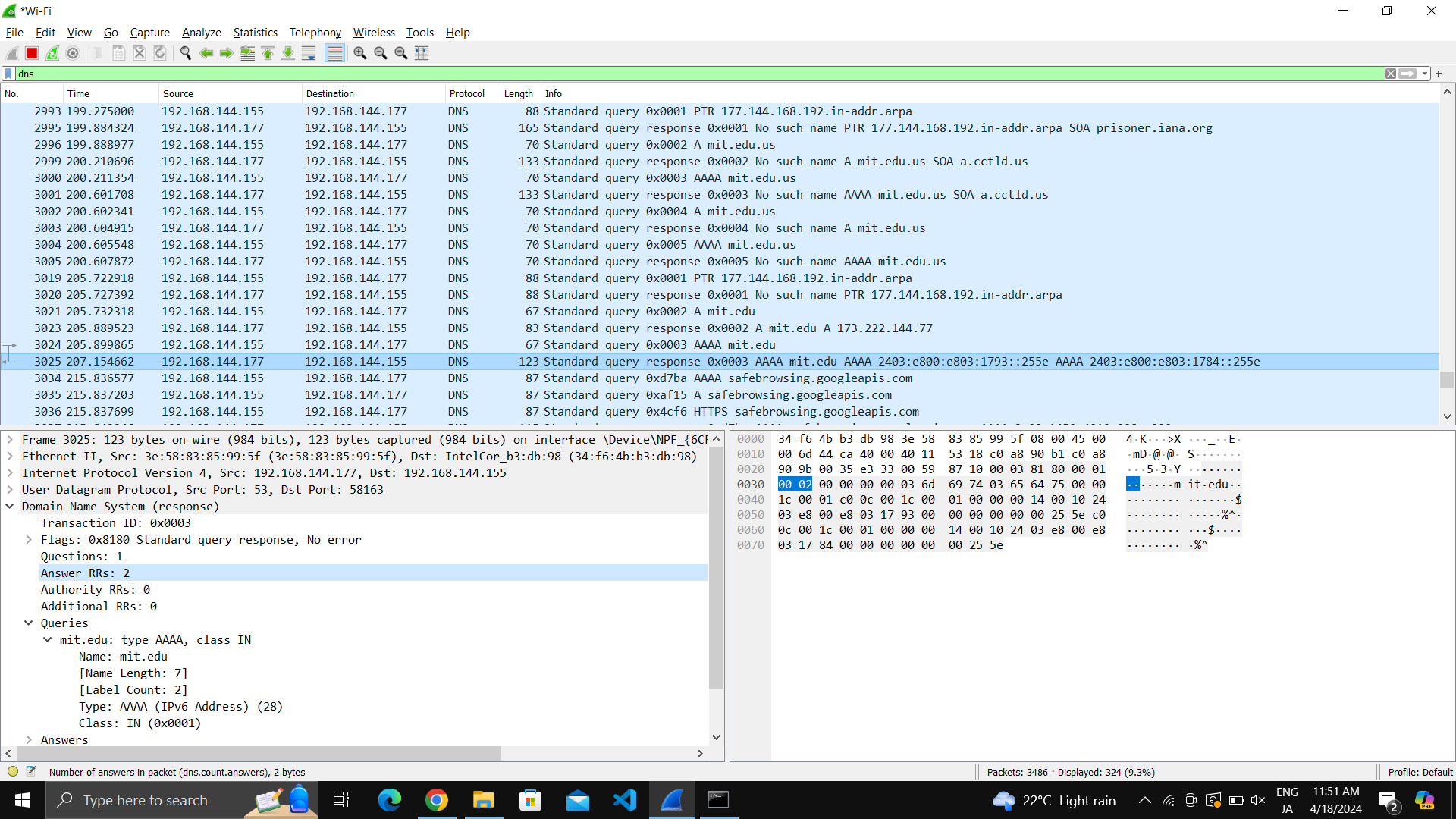
You should get a trace that looks something like the following:



We see from the above screenshot that ***nslookup*** actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to ***nslookup*** and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

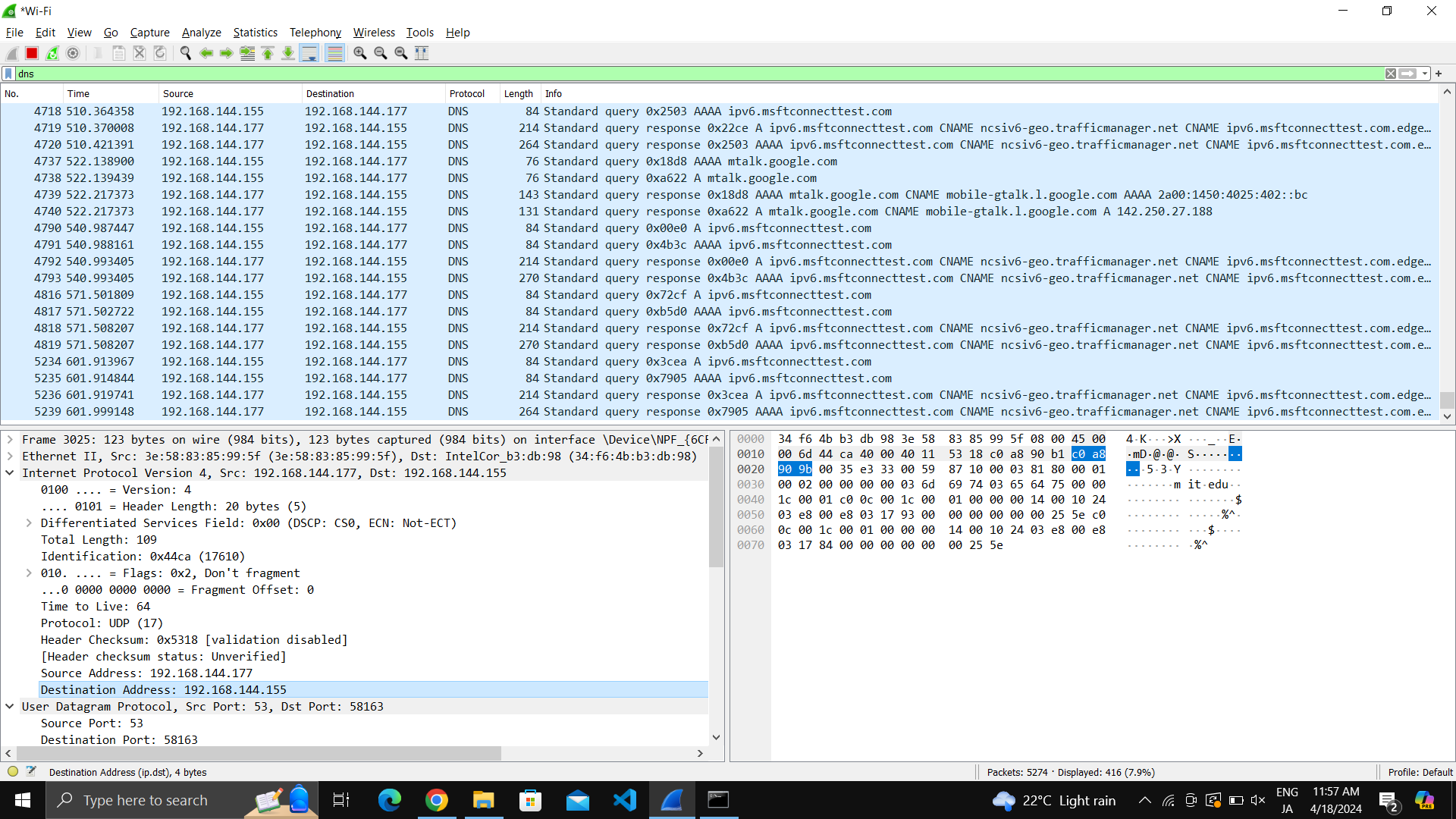
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

**Ans:** Source port: 53, Destination port: 58

****

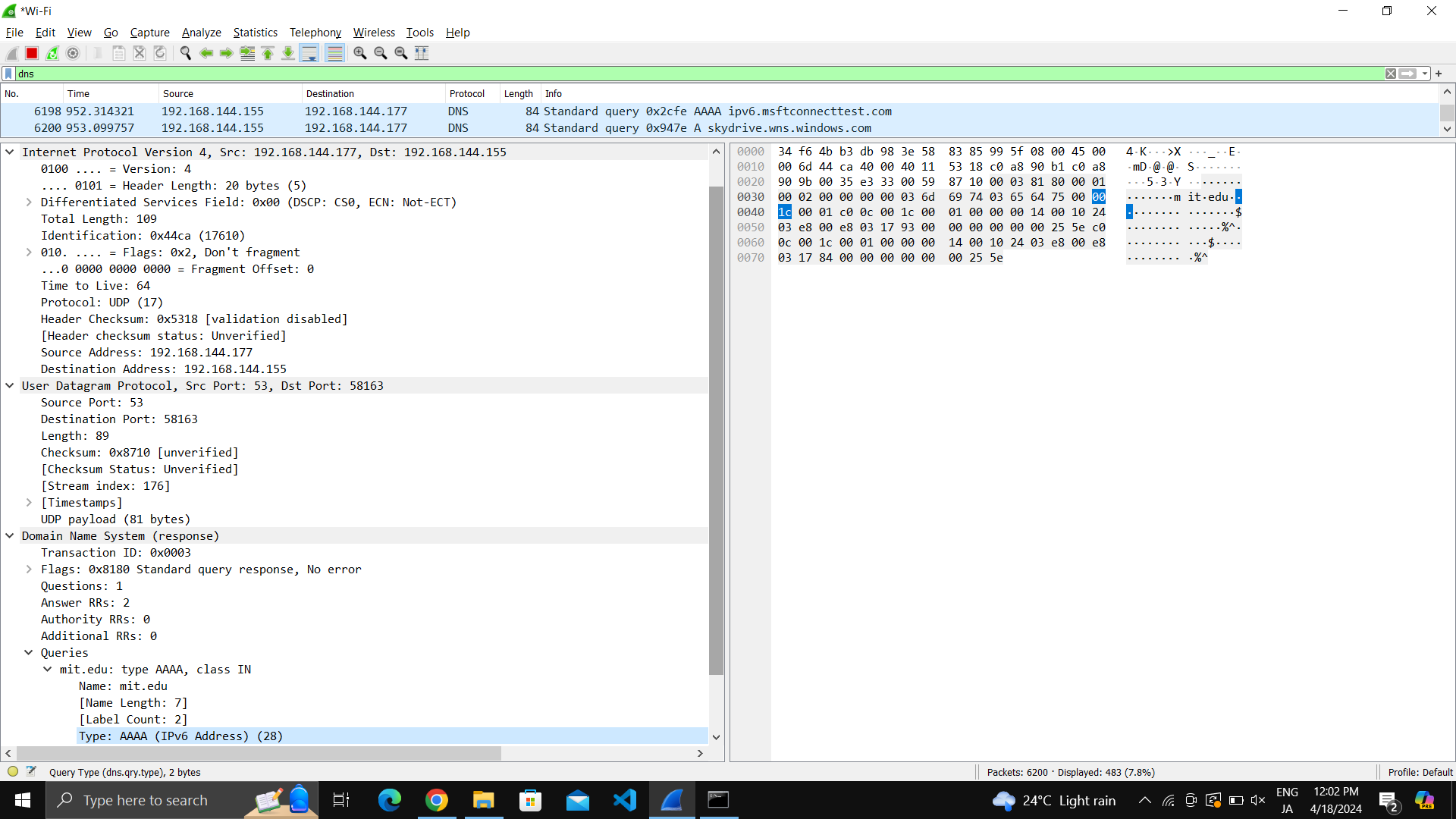
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**Ans:** Yes the IP is the same.



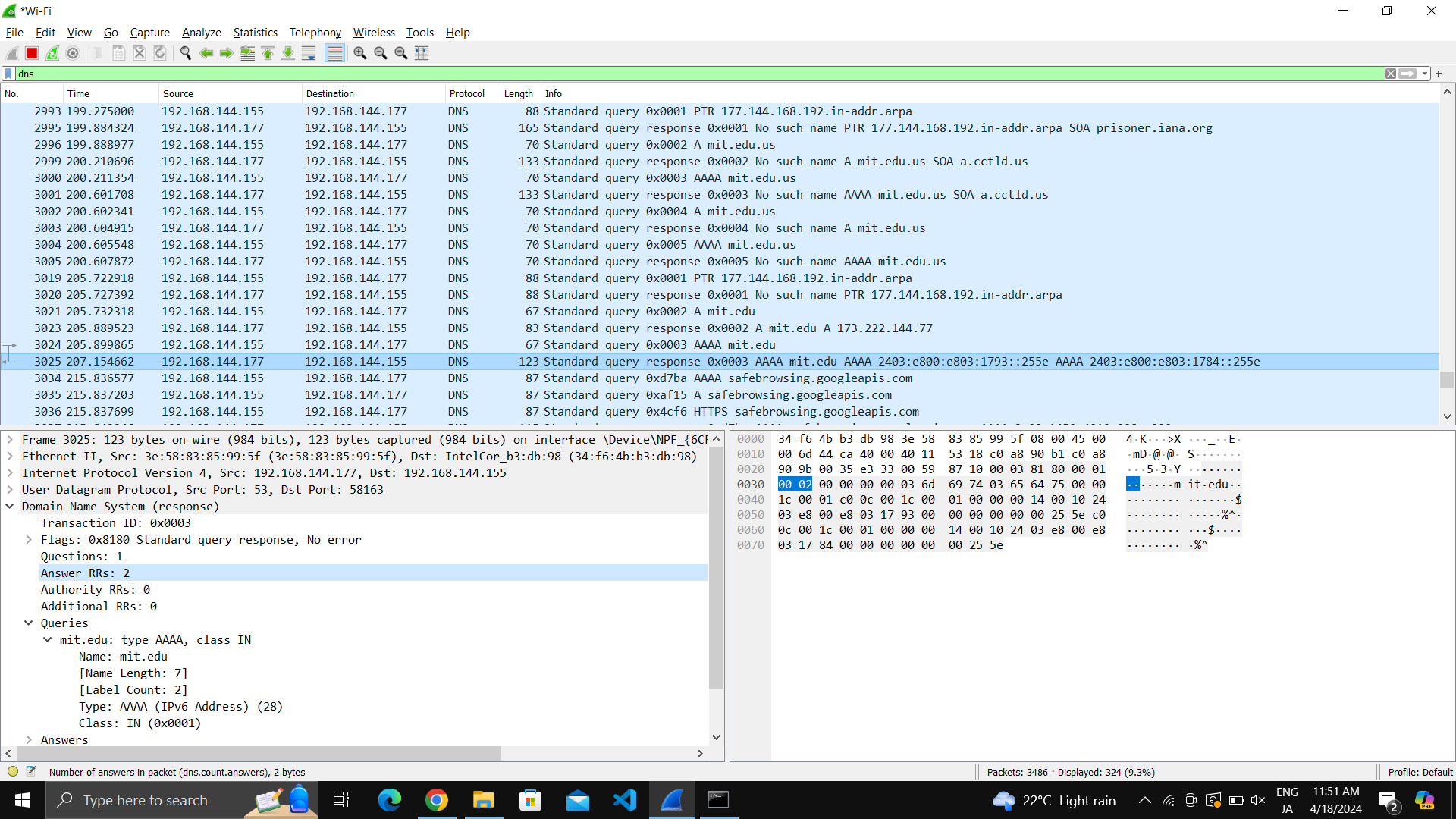
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Ans: Type: AAAA**

****

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

**Ans:** Answer: 2

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_