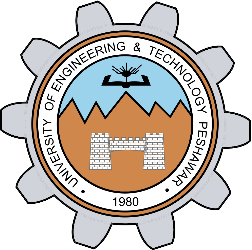
**Lab 07**



Submitted by**:**

**Maaz Habib**

Registration Number**:**

**20pwcse1952**

Section: **C**

Submitted To**:**

**Engr, Yasir Saleem Afridi**

# Department of Computer System Engineering university of Engineering and Technology Peshawar

# Objectives

In this lab we understand the Domain Name System and we’ll make extensive use of the nslookup tool.

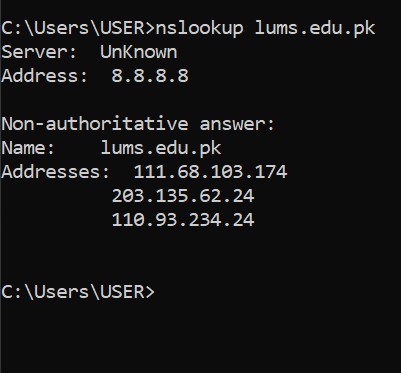
# Domain Name System

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.

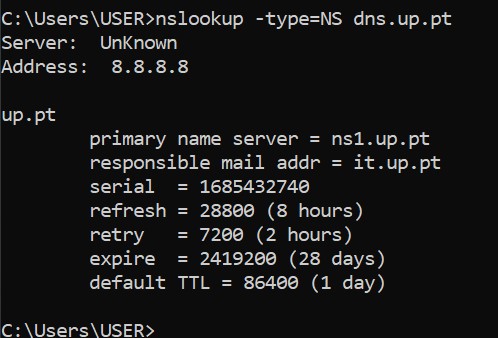
# NSLookup

In this lab, we’ll make extensive use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, you just type the nslookup command on the command line. To run it in Windows, open the Command Prompt and run nslookup on the command line.

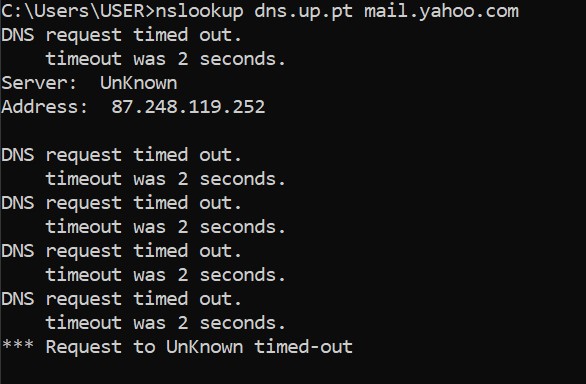
* Run nslookup to obtain the IP address of a Web server in Asia (lums.edu.pk). What is the IP address of that server?



* Run nslookup to determine the authoritative DNS servers for a university in Europe [(dns.up.pt)](http://www.fe.up.pt/).



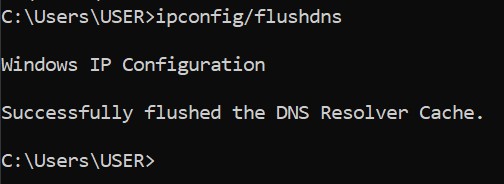
* Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?



# Tracing DNS with Wireshark

Now that we are familiar with *nslookup* and *ipconfig*, we’re ready to get down to some serious business. Let’s first capture the DNS packets that are generated by ordinary Web surfing activity.

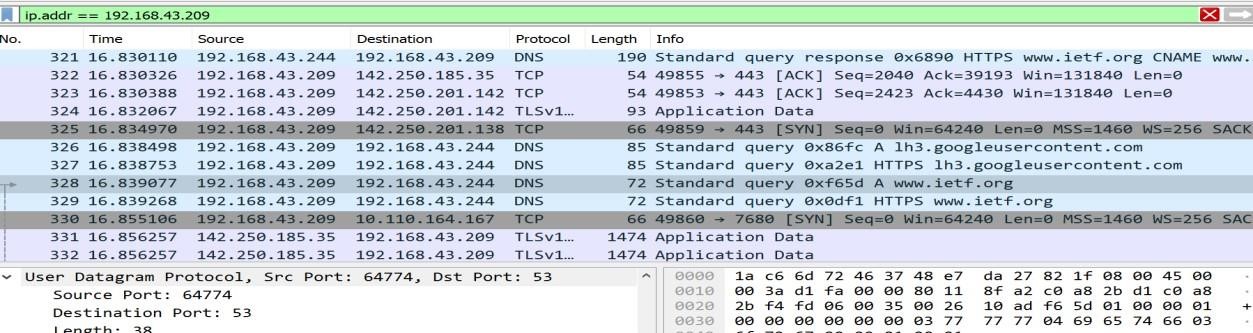
* Use *ipconfig* to empty the DNS cache in your host.



* Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
* 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](http://www.ietf.org/)  Stop packet capture.

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

**They sent over UDP**



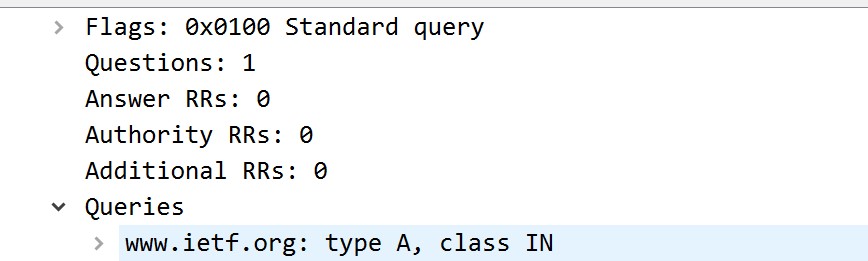
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

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 query was sent to IP address 192.168.43.244. Yes, it is the same IP address as that of my local DNS server.**

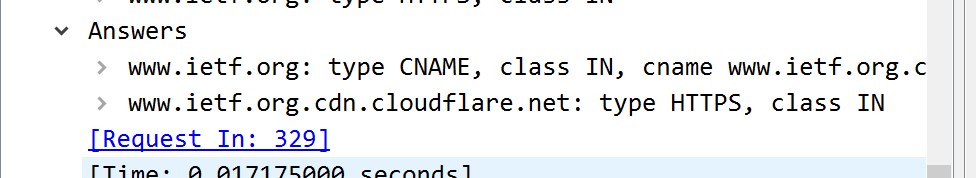
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Type of DNS query is ‘A’ but the query message didn’t contain any answer**



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

**The response message contained two answer to the query.**



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?

**The destination of the SYN packet 10.110.164.167, the same address that was provided in the DNS response message as the type “A” address of the webpage.**

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

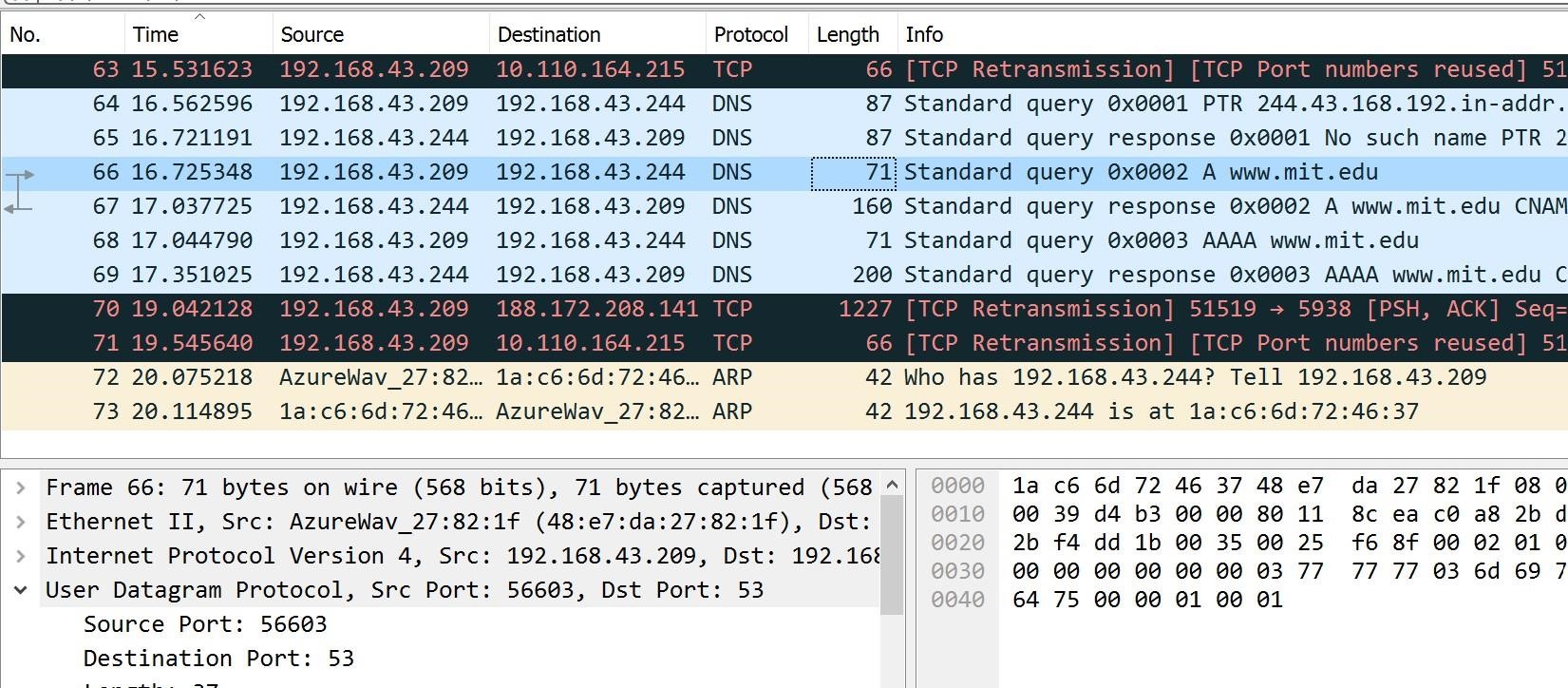
**Yes, my host did issue new DNS queries before the images were retrieved.**

# Task 02

* Start packet capture.

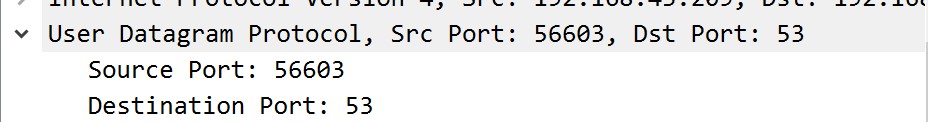
* Do an *nslookup* on [www.mit.edu](http://www.mit.edu/)

* Stop packet capture.



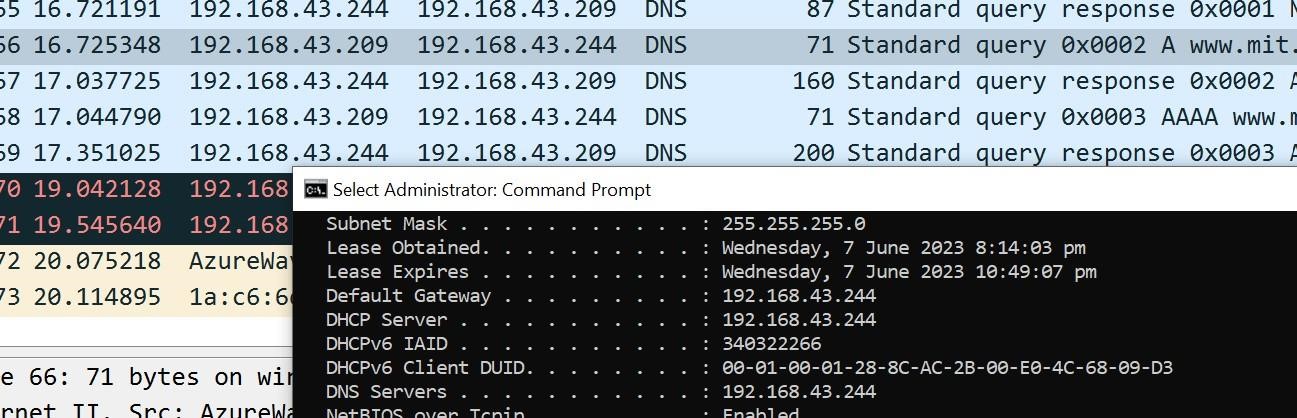
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

**Source port:56603, Dst port: 53**



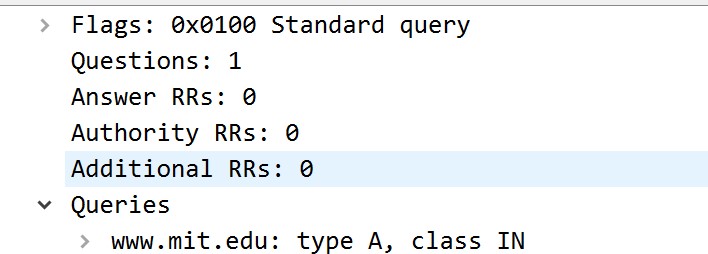
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**The DNS query message is sent to IP address 192.168.43.244, the same address 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”?

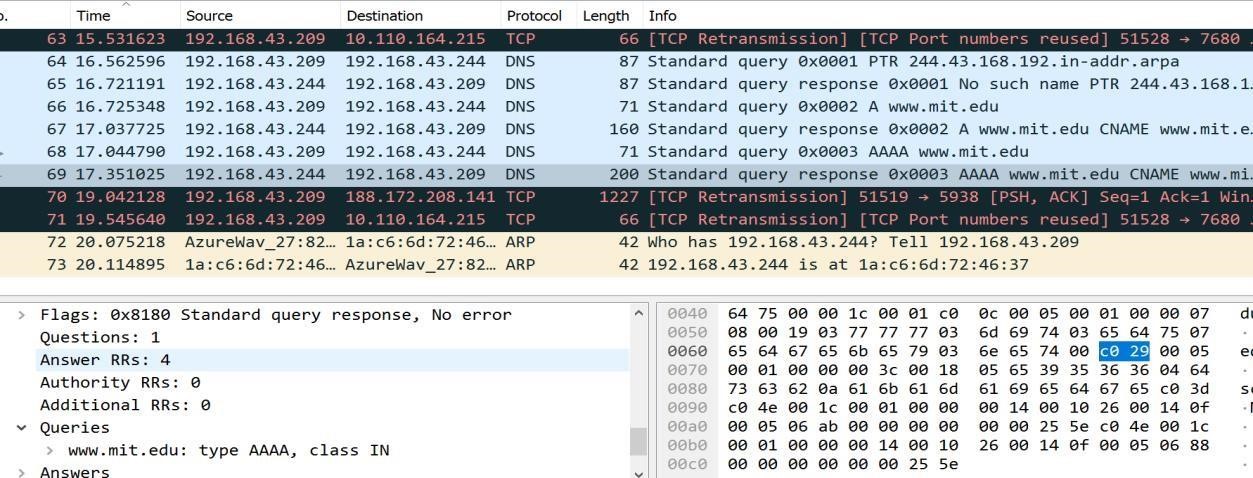
**The DNS query message is a type “A” query, containing only one question and not containing any answers.**



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

**The response message contains four answer to the query and one question.**

1. Provide a screenshot.



**Task**

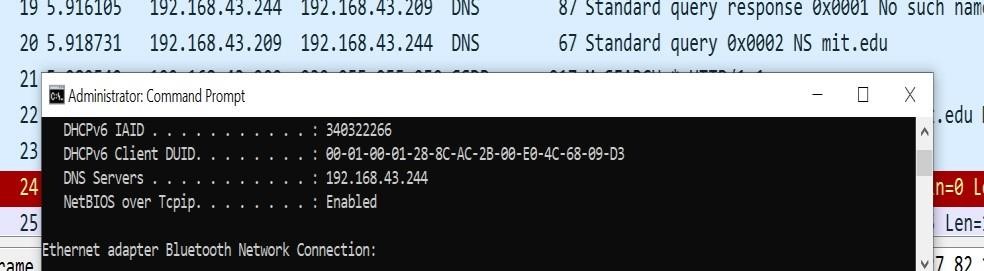
**2.2**

Now repeat the previous experiment, but instead issue the command: nslookup –type=NS mit.edu

Answer the following questions :

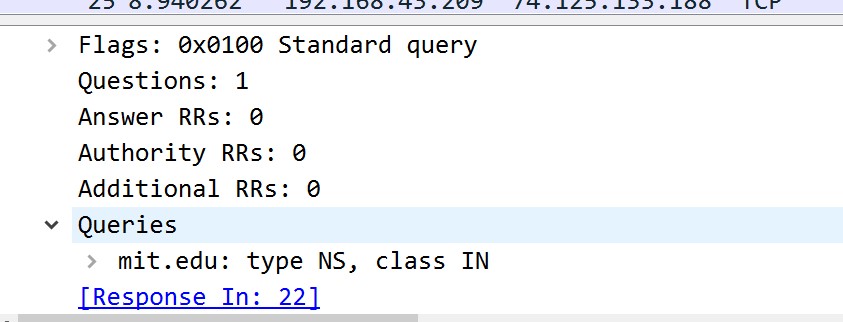
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**The query is sent to 192.168.43.244, the same IP address as that of 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 DNS query is a type “NS” message including one question. The query message did not contain any 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 namesers?

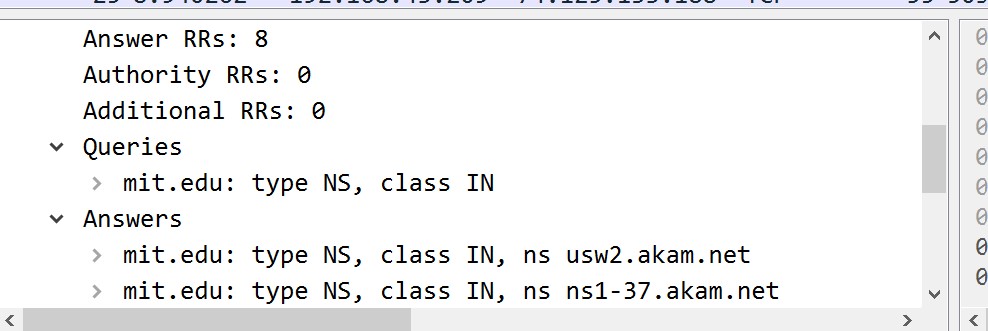
**The response message provided 8 MIT servers. There is no additional record which provide IP addresses of MIT nameservers.**

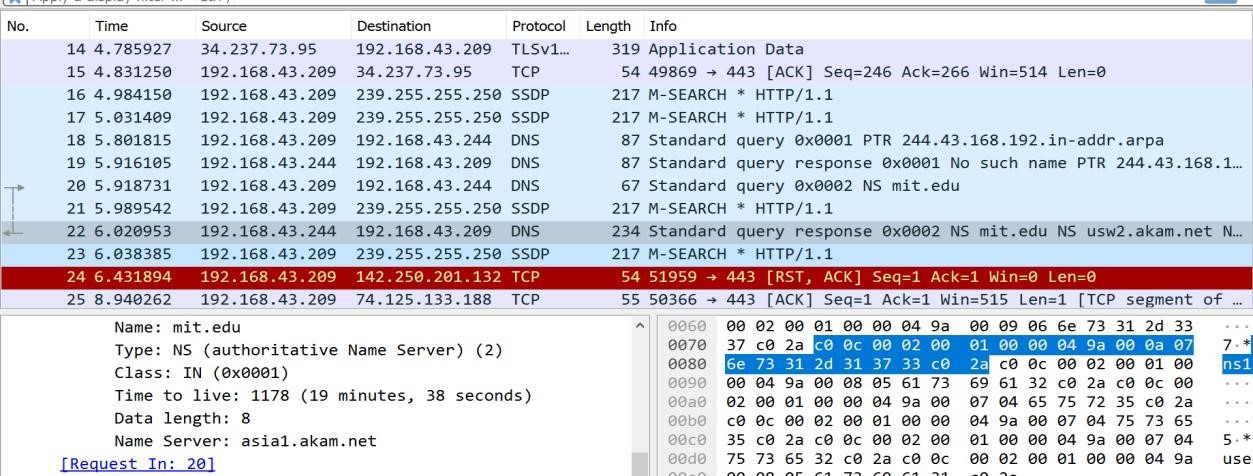
9.

Provide

a

screenshot.





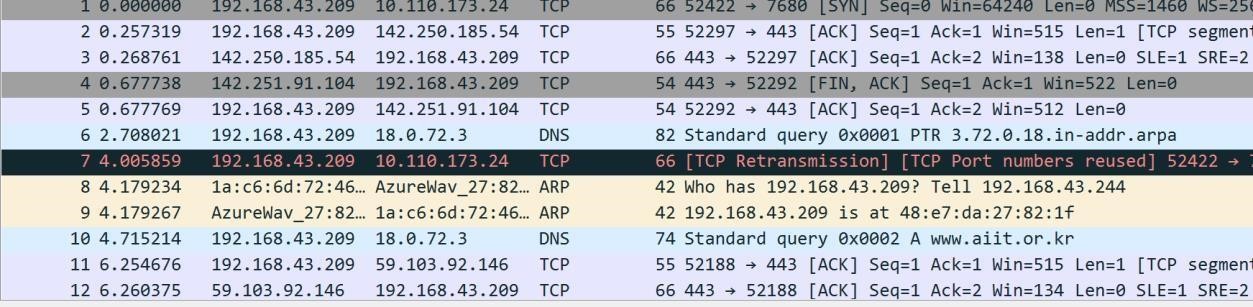
# Task 2.3

Now repeat the previous experiment, but instead issue the command: nslookup [www.aiit.or.kr b](http://www.aiit.or.kr/)itsy.mit.edu

Answer the following questions6:

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?

**This DNS query message is sent to 18.0.72.3 which is the IP address of the MIT DNS response sender.**



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

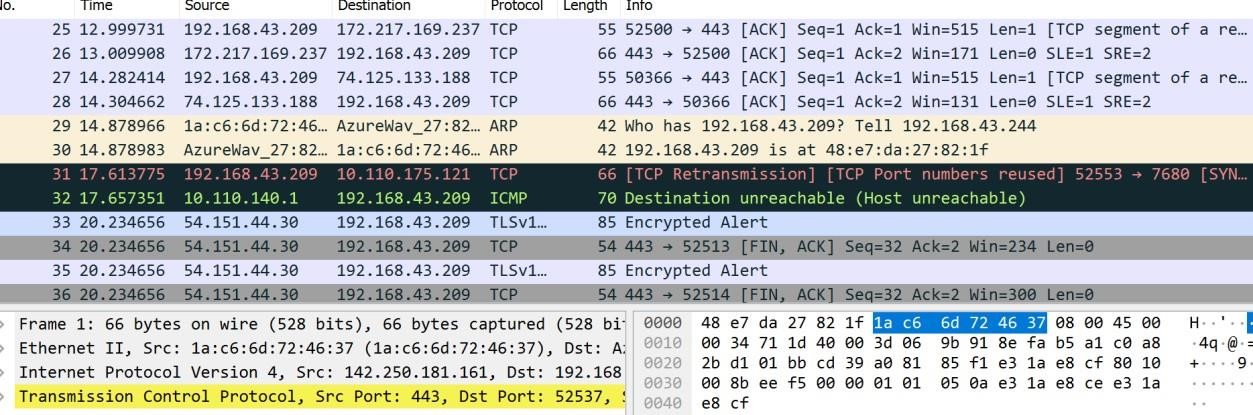
**The type of DNS query is A and it doesn’t contain any answer**

A screenshot of a computer

Description automatically generated with low confidence

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

**There is no response message recieved**



1. Provide a screenshot.

