**Domain name system (DNS)**

**LAB # 06**

****

**Spring 2022**

**CSE303L-Data Communication & Computer Network**

Submitted by: **Ashfaq Ahmad**

Registration No: **19PWCSE1795**

Class Section: **B**

“On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work.”

Student Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Submitted to:

**Eng: Faizullah**

May 23, 2022

**Department of Computer Systems Engineering**

**University of Engineering and Technology, Peshawar**

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

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

**Credit Hours: 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 and DNS” 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. In this case Wireshark only capture those packets related to given entered IP. For some packets this IP will be source while for some it will be destination. And DNS means Wireshark only capture packets related to DNS and IP entered. If we enter TCP along with IP then Wireshark will capture packets related to TCP and IP.

• Start packet capture in Wireshark.

• With your browser, visit the Web page: http://www.ietf.org

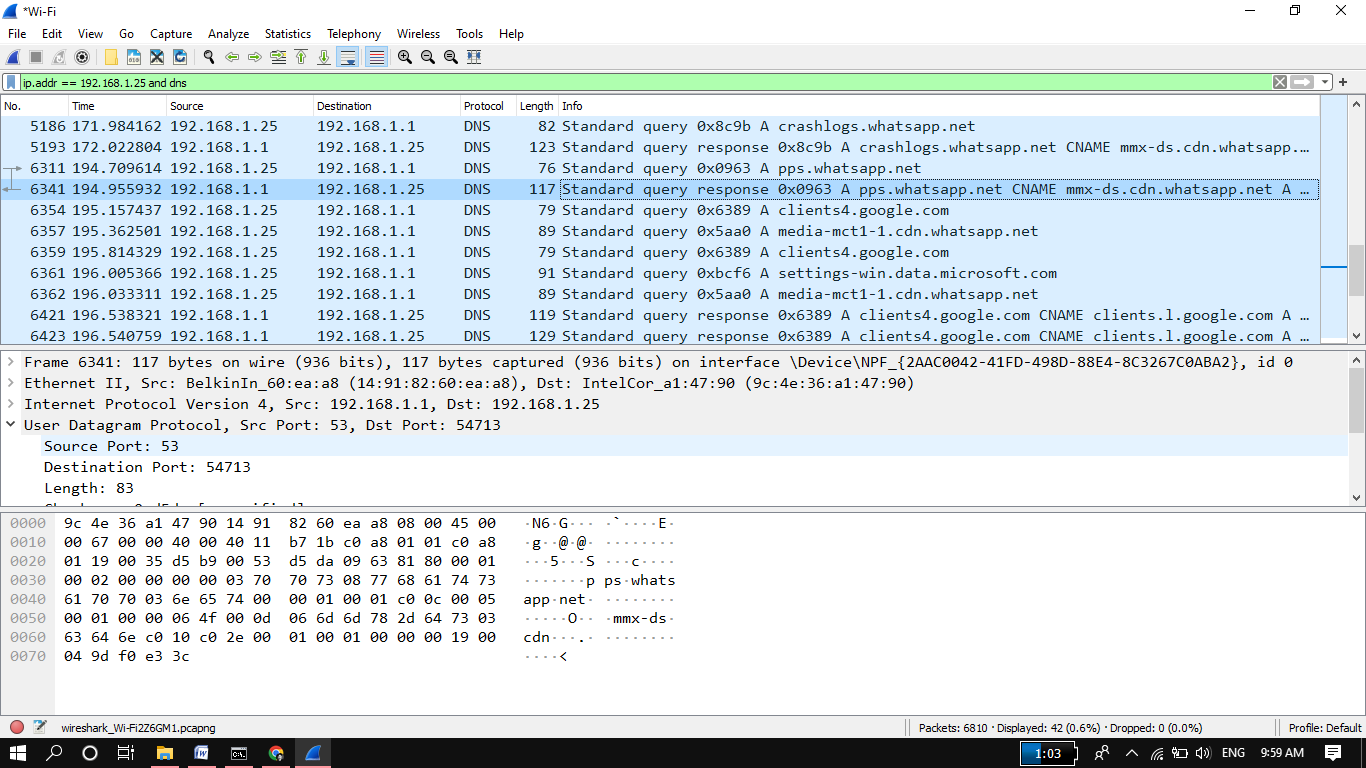
• Stop packet capture.

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?

**Answer:** Yes, this communication occurred over user datagram protocol (UDP).

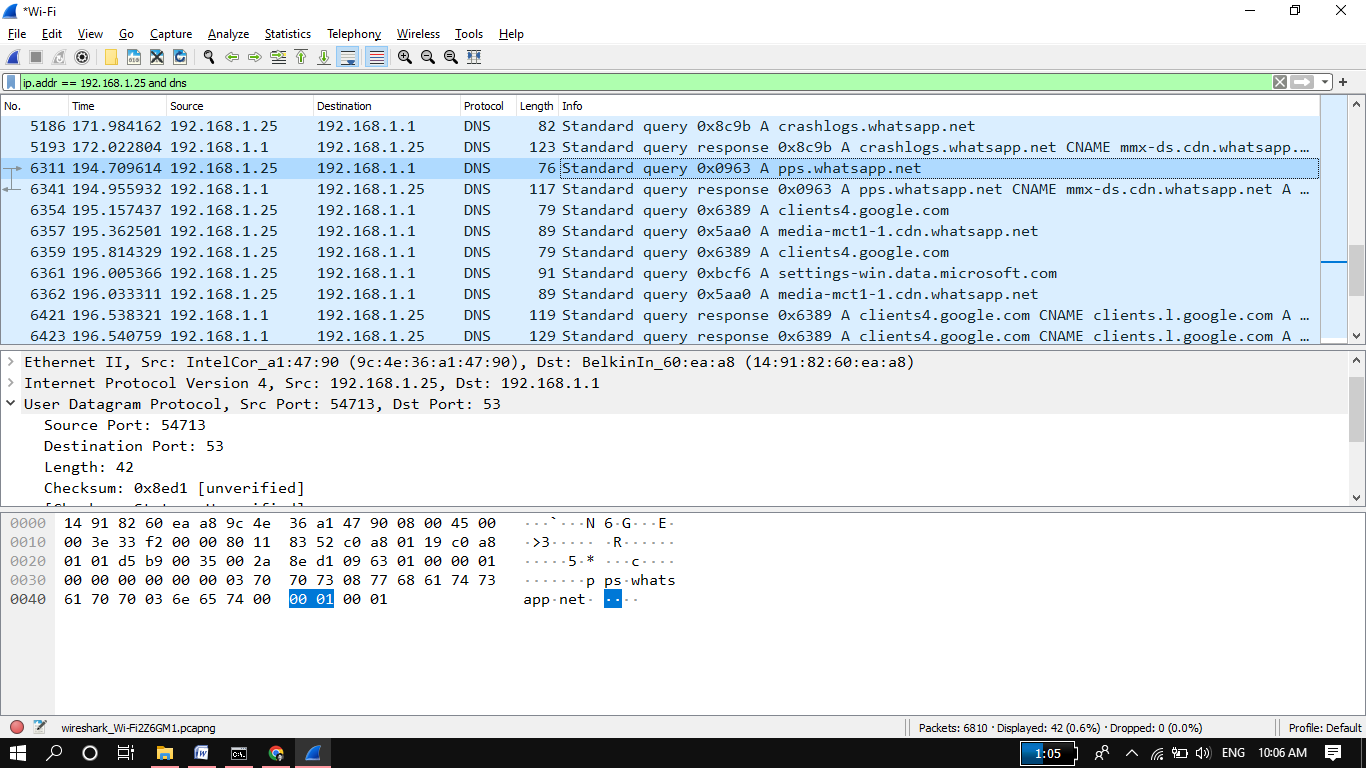
* Communication between servers occurs through TCP and communication between client and server occur through UDP. Both protocols are two ways communication. Only DNS server has both TCP and UDP.

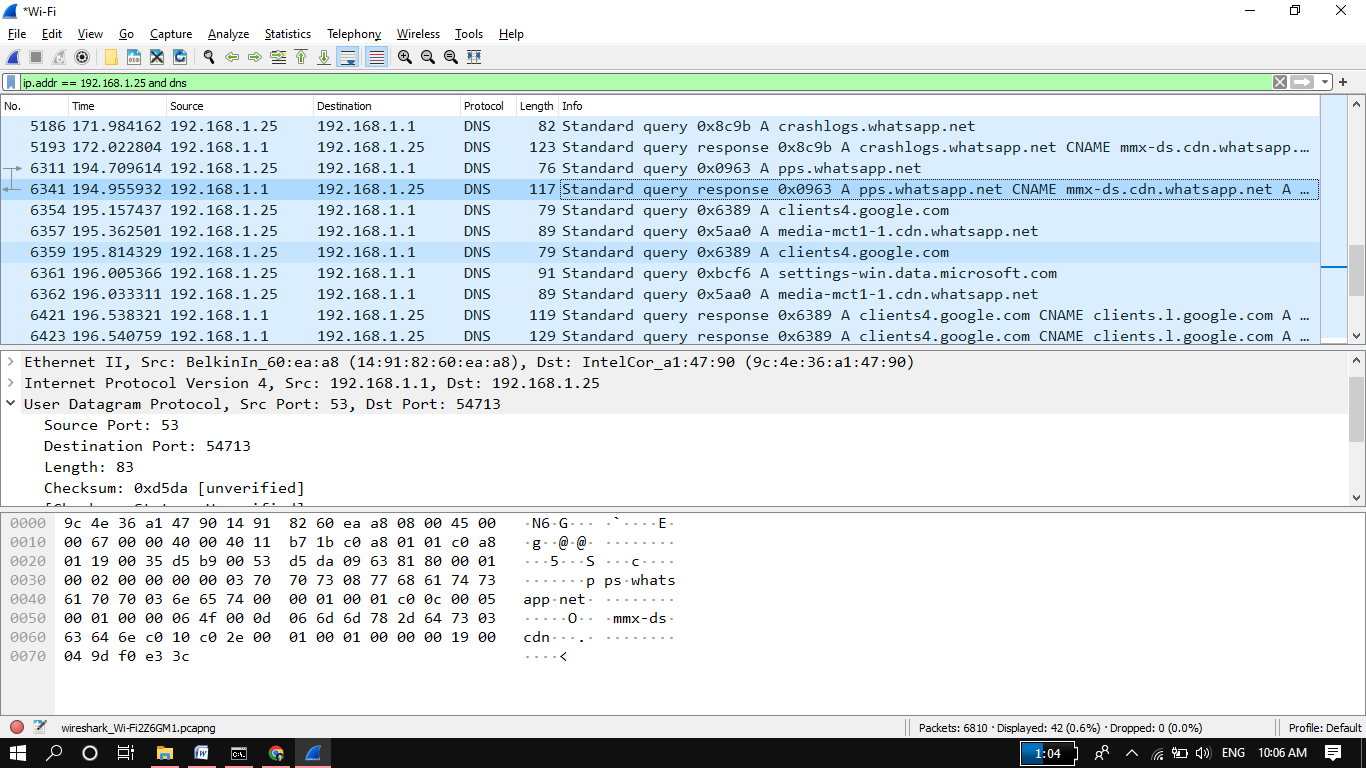


1. What is the destination port for the DNS query message? What is the source port

Of DNS response message?

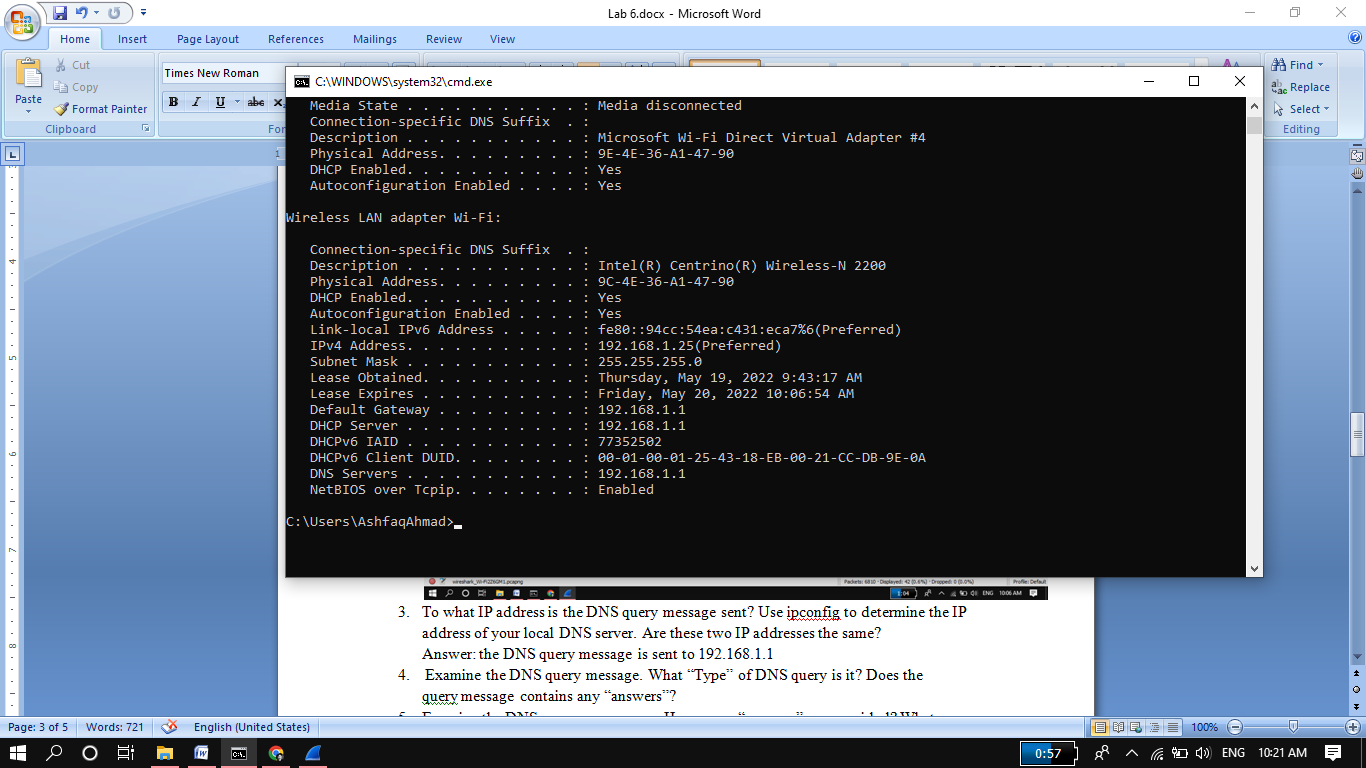
**Answer**: the destination port for the DNS query message is 53.

The source port of DNS response message is 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?

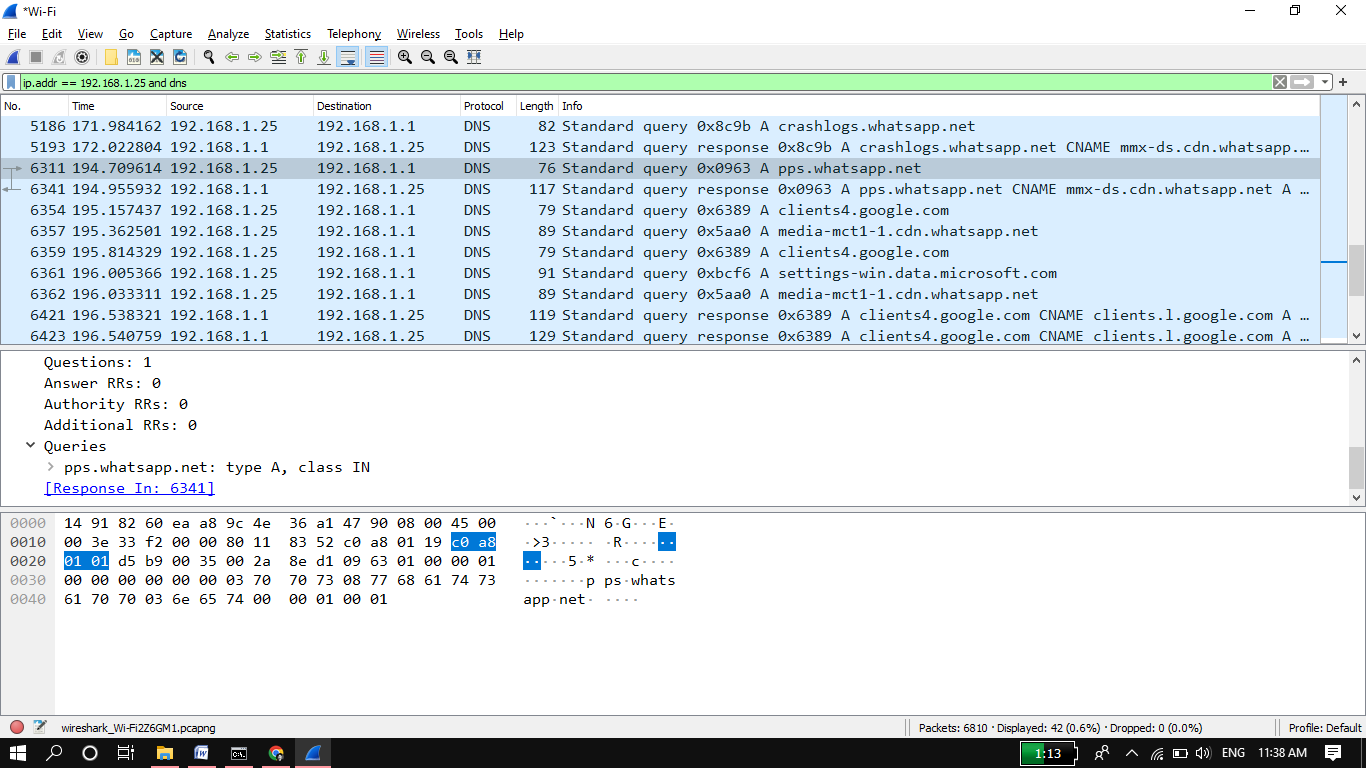
**Answer:** the DNS query message is sent to 192.168.1.1 and yes the IP address to which query message sent and IP of local DNS server both are same.



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

Query message contains any “answers”?

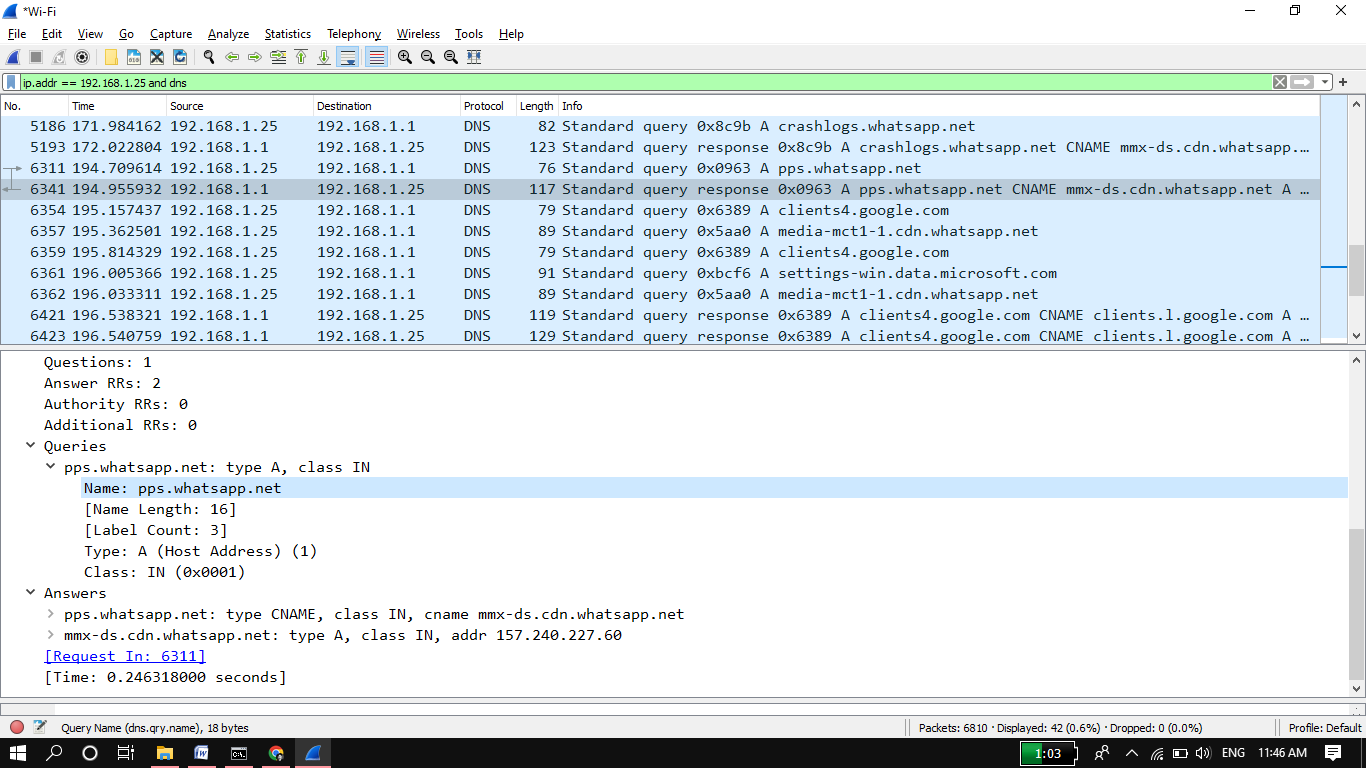
**Answer:** The DNS query message is Type A. it doesn’t contain any answer.



1. Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?

**Answer:** 2 answers are provided. The answers are:



Now let’s play with *nslookup*.

**Nslookup**:

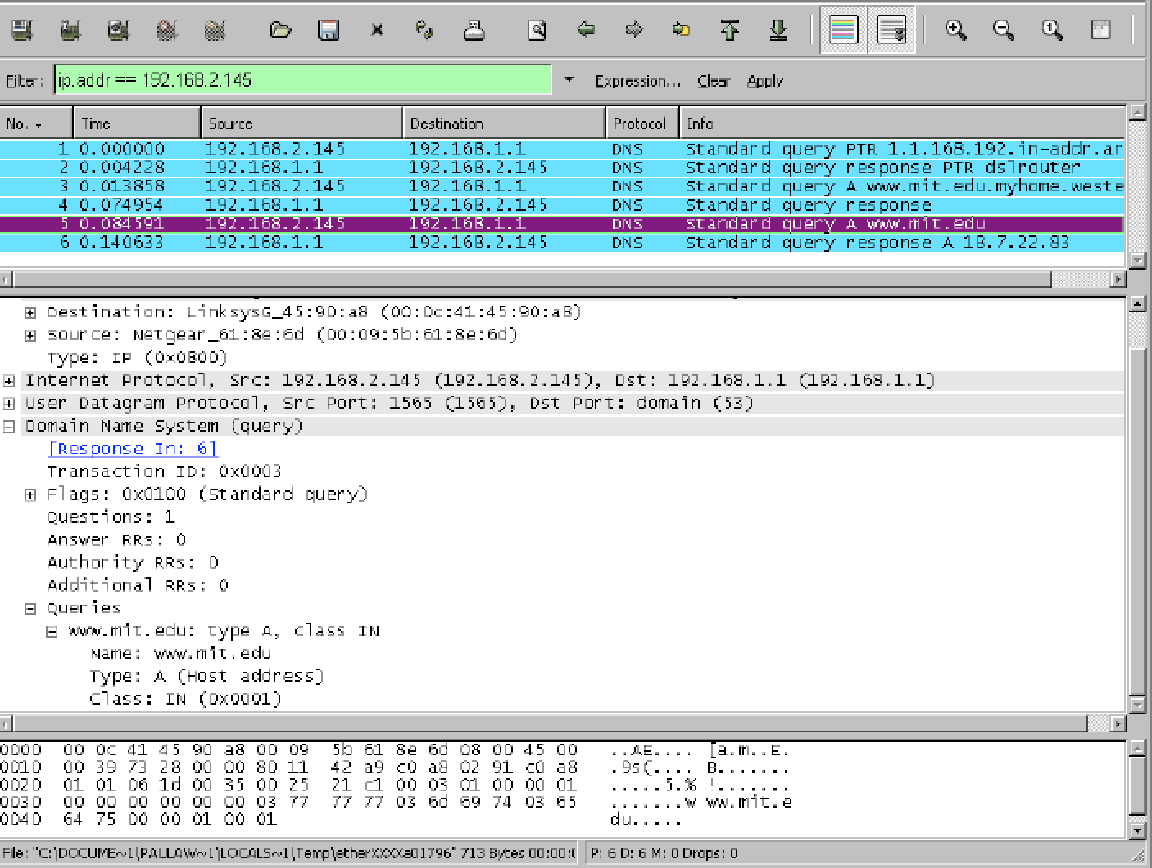
* **Nslookup**(stands for “Name Server Lookup”) is a useful command for getting information from the DNS server.
* It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.
* It is also used to troubleshoot DNS-related problems.

• Start packet capture.

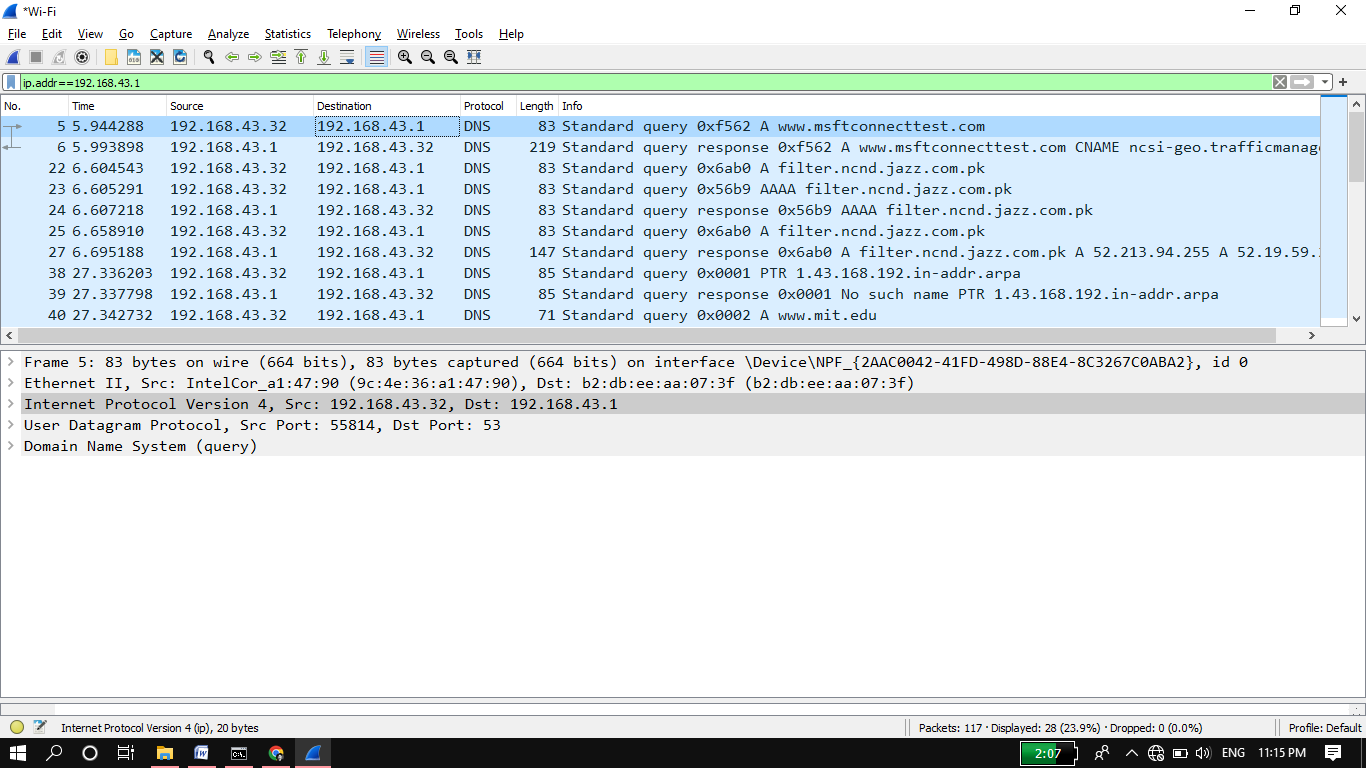
• Do an *nslookup* on www.mit.edu

• Stop packet capture.

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



**In my Case the screenshot is:**



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?

**Answer:** Destination port of DNS query message: 53

Source port of DNS response message: 53.

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

**Answer:** DNS query message is sent to 192.168.43.1. This IP address is our default local DNS server.

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

**Answer:** Type is A and query message doesn’t contain any answer.

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

**Answer:** 5 answers are provided. The answers are given below,

