**Tracing DNS with Wireshark**

**LAB # 08**



**Spring 2025**

Submitted by: **Mohsin Sajjad**

Registration No: **22pwsce2149**

Class Section: **A**

“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:

**Dr. Yasir Saleem Afridi**

Month Day, Year (21 05, 2025)

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 al | **20%** |

**Credit Hours: 1**

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

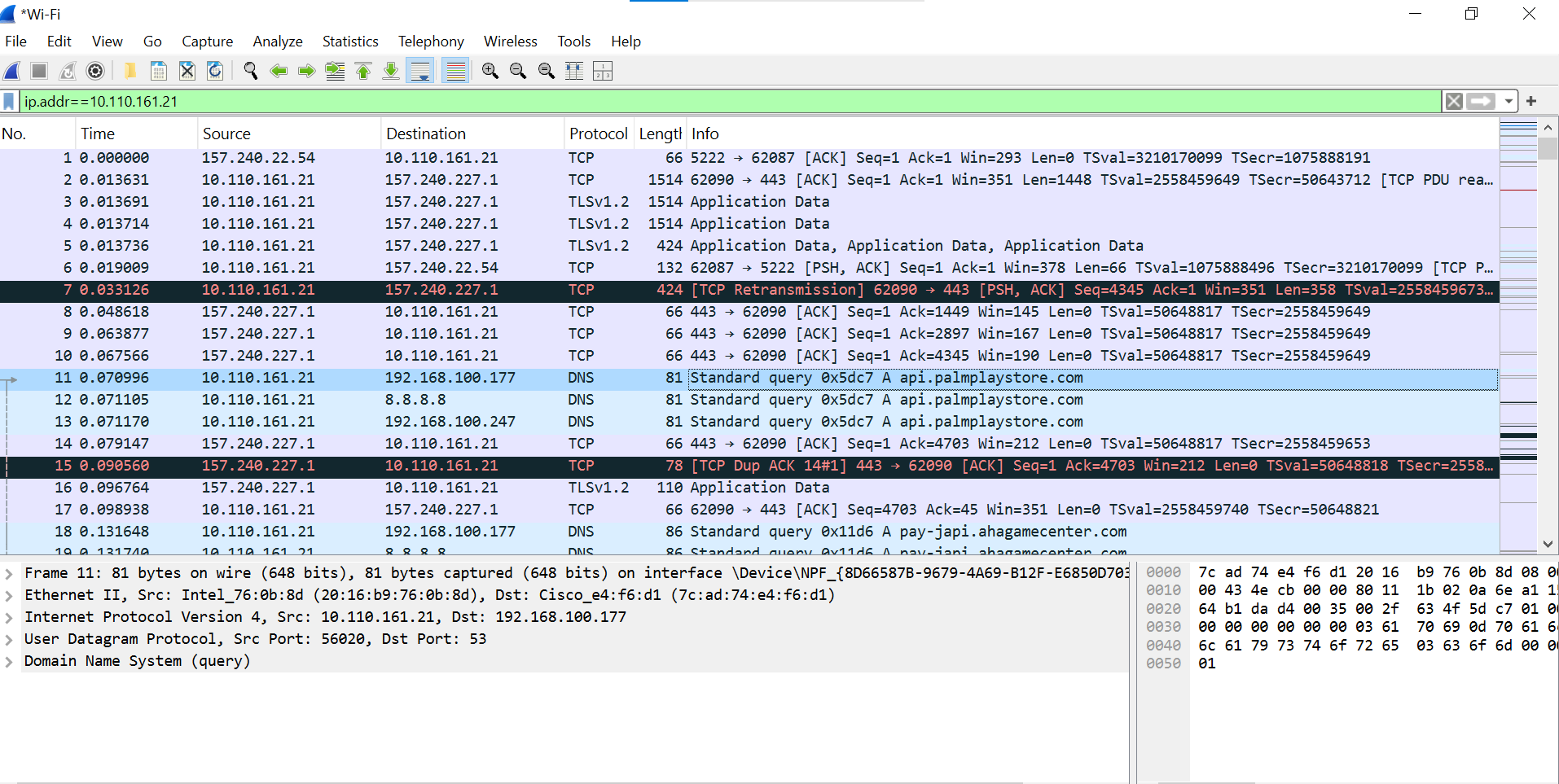
neither originate nor are destined to your host.

• 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.



**Question 1:**

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

Answer:  
**The DNS message sent over UDP not TCP.**

**Question 02:**What is the destination port for the DNS query message? What is the source port

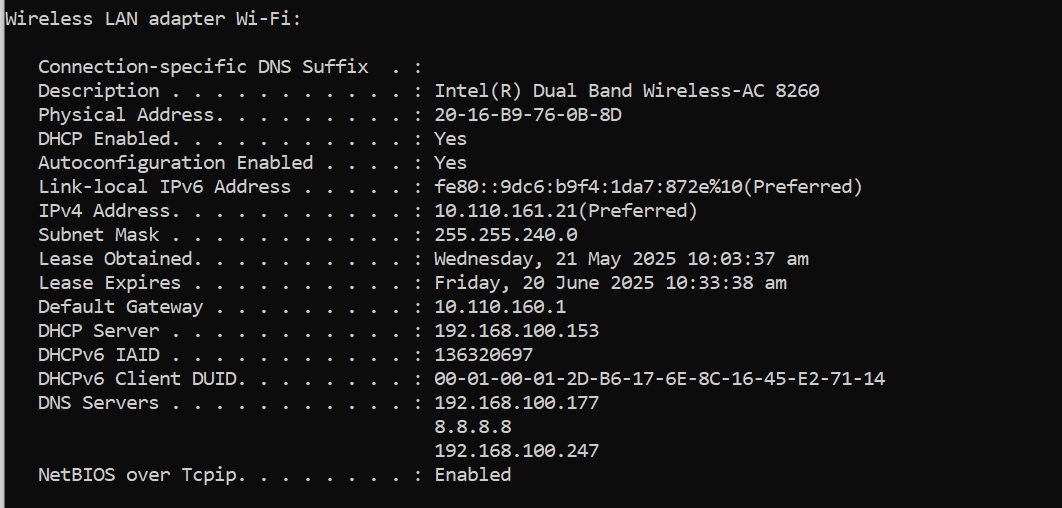
of DNS response message?

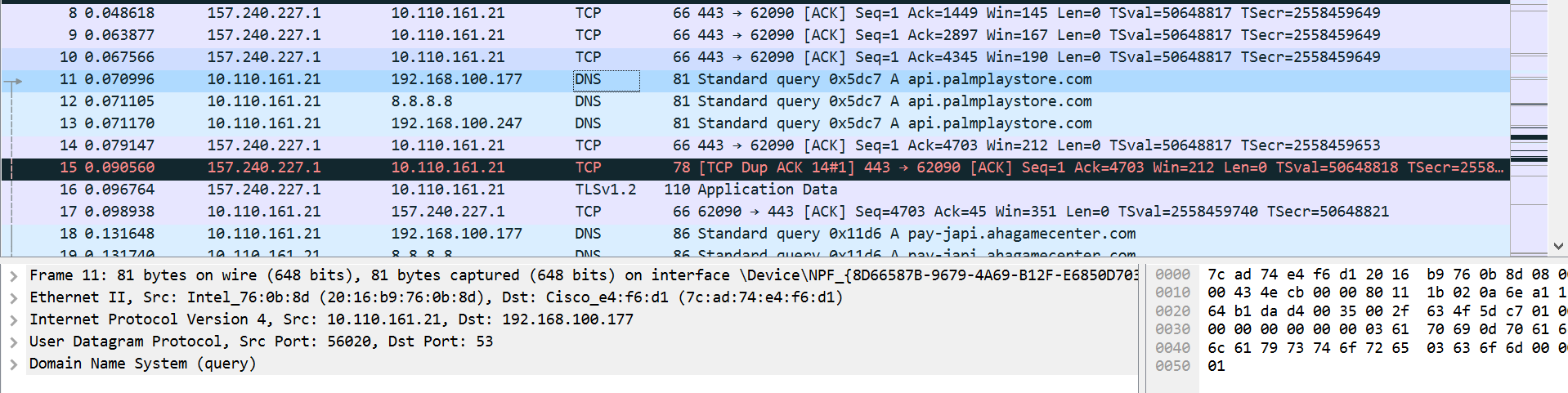
**Answer:**

Destination port for DNS query: 56020.

Source port of DNS response: 53.

**Question 03:**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:  
**

****

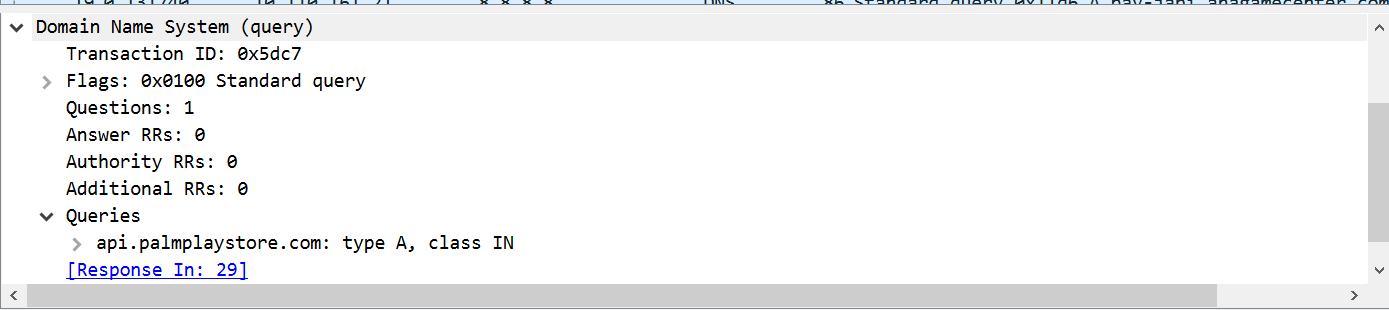
**Answer:**

Yes, the ip address of DNS server is same as in packet.

**Question 04:**

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

query message contains any “answers”?

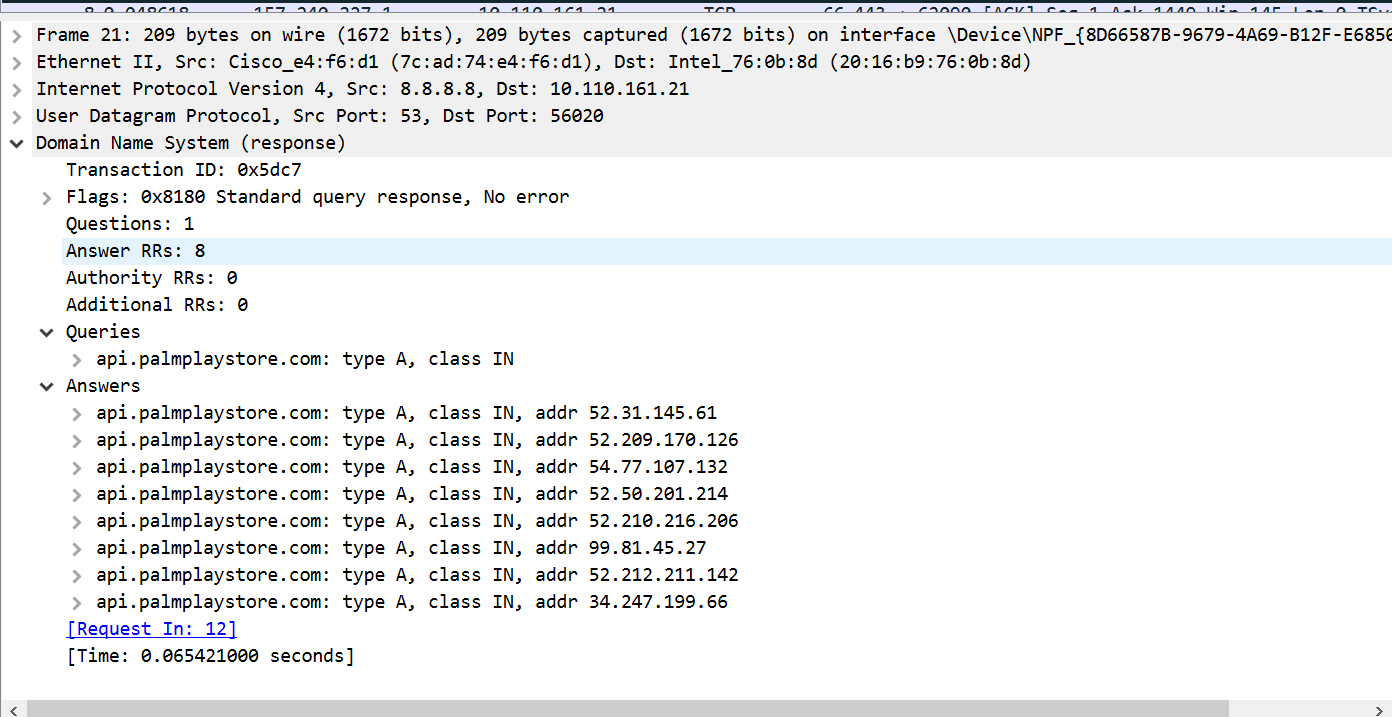
**Answer:  
**

The query is of Type A (requesting IPv4 address for a domain, e.g., api.palmplaystore.com).

No, the query message does not contain any answers—it's only a request.

**Question 05:**Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?



**Answer:**

For api.palmplaystore.com, DNS responses included multiple answers. For example:

Packet 21 contained 8 answers:

A records like 52.31.145.61, 52.209.170.126, etc.

Packet 29 contained more than 8 answers including A records (IP addresses) and NS records (name servers).

**Each answer includes:**

A Records: IP addresses associated with the queried domain.

NS Records (in some cases): Name server domain names (and sometimes A records for them too).

**NSLOOKUP**

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

Destination port of DNS query: 53 (standard for DNS).

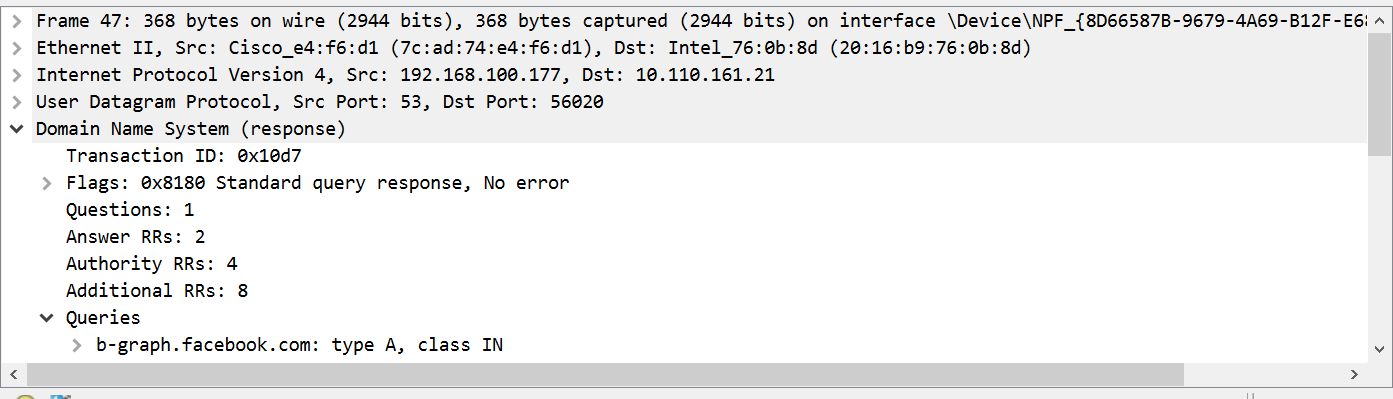
Source port of DNS response: 56020

**Question 02:**To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**Answer:**

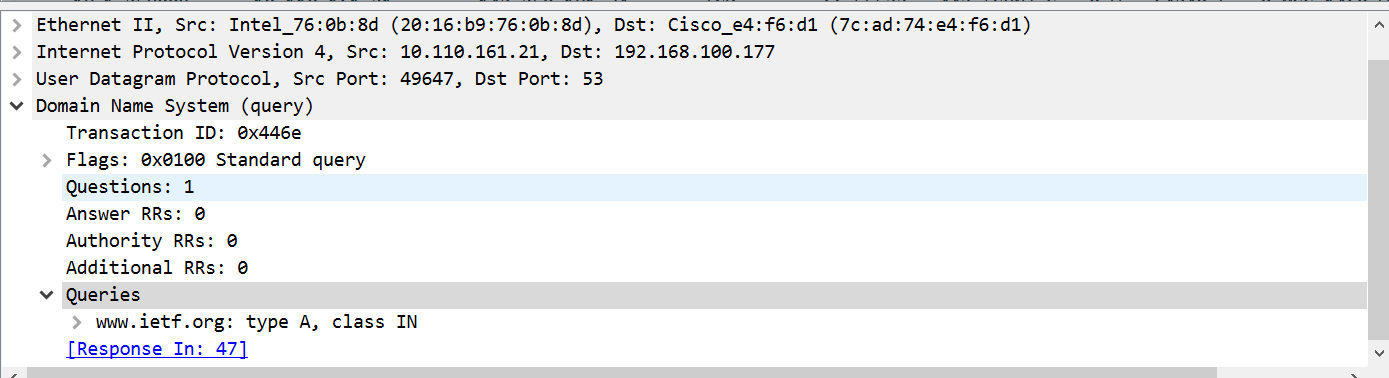
The DNS query is likely sent to your local DNS server 192.168.100.177.

Run ipconfig /all and check the “DNS Servers” line. That IP should match the destination IP in your DNS query.

****

**Question 03:**Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Answer:**

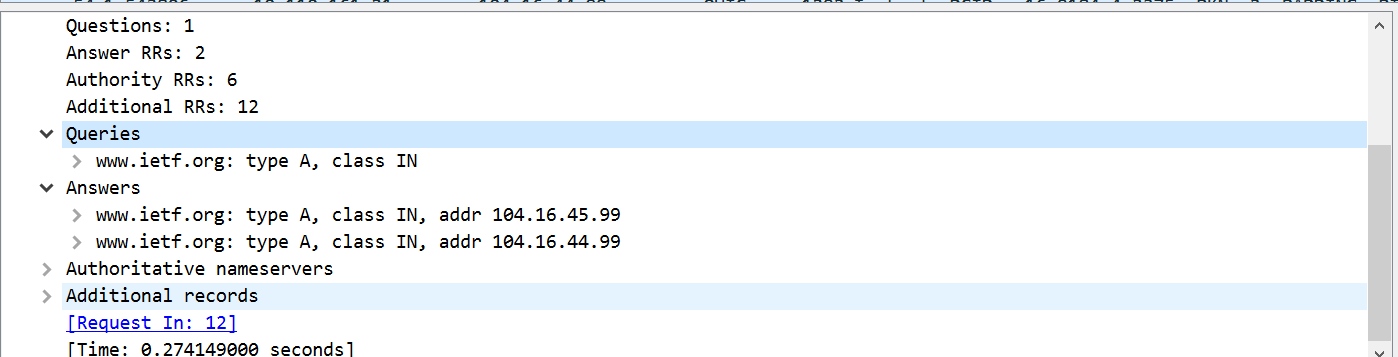
****

**Answer to Question 3:**

**Type of DNS Query:  
Type A**, which means it is requesting the IPv4 address for the domain www.ietf.org.

**Does the Query Message Contain Any Answers?**No, the DNS query message does not contain any answers.  
It only includes the question section, asking for the A record of www.mit.edu.  
The answers come only in the response message, not in the query.

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

****

**Answer:**2 answers are provided in the DNS response.

**Each Answer Contains:**

**Answer 1:**

* + - **Name: www.ietf.org**
    - **Type: A (IPv4 address)**
    - **Address: 104.16.45.99**

**Answer 2:**

* + - **Name: www.ietf.org**
    - **Type: A (IPv4 address)**
    - **Address: 104.16.44.99**

These are two A records, meaning www.ietf.org resolves to two different IP addresses, likely for load balancing or redundancy.