Daniel Lara - ID: 49651280

Zachary Hart – ID: 70953123

CS 132

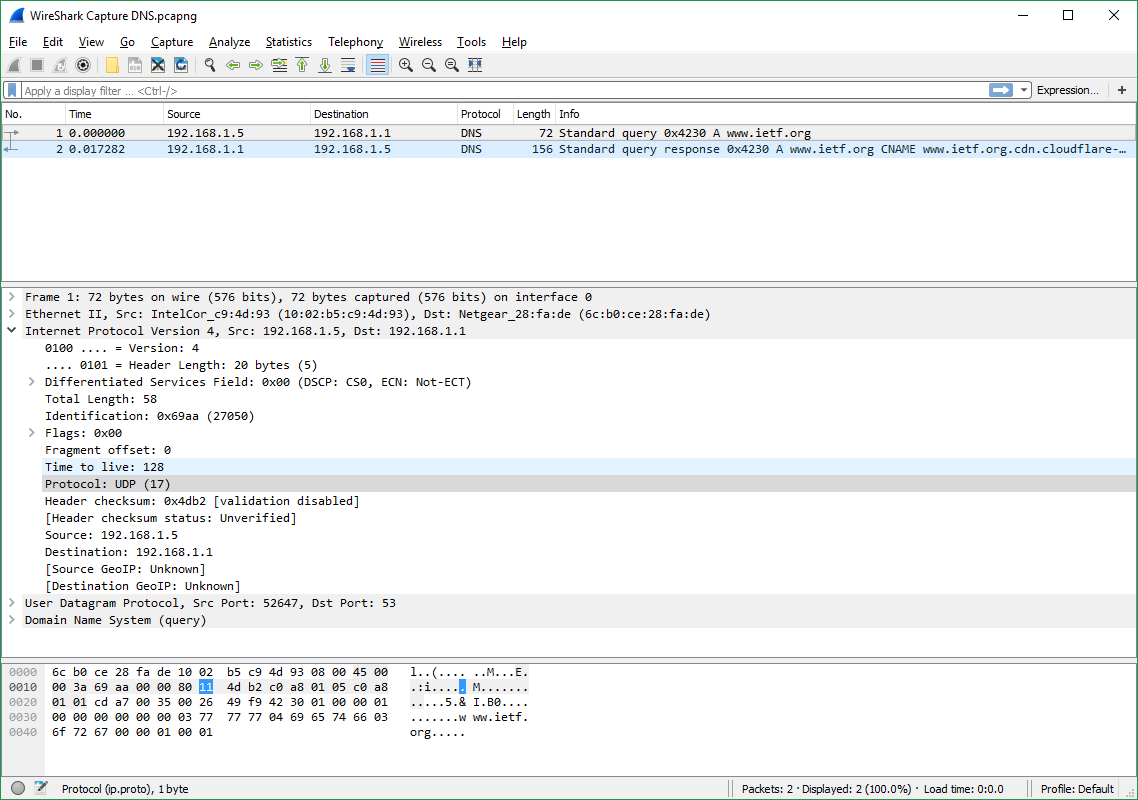
HW 2: Wireshark Labs

# Question 2: Wireshark Labs

## DNS:

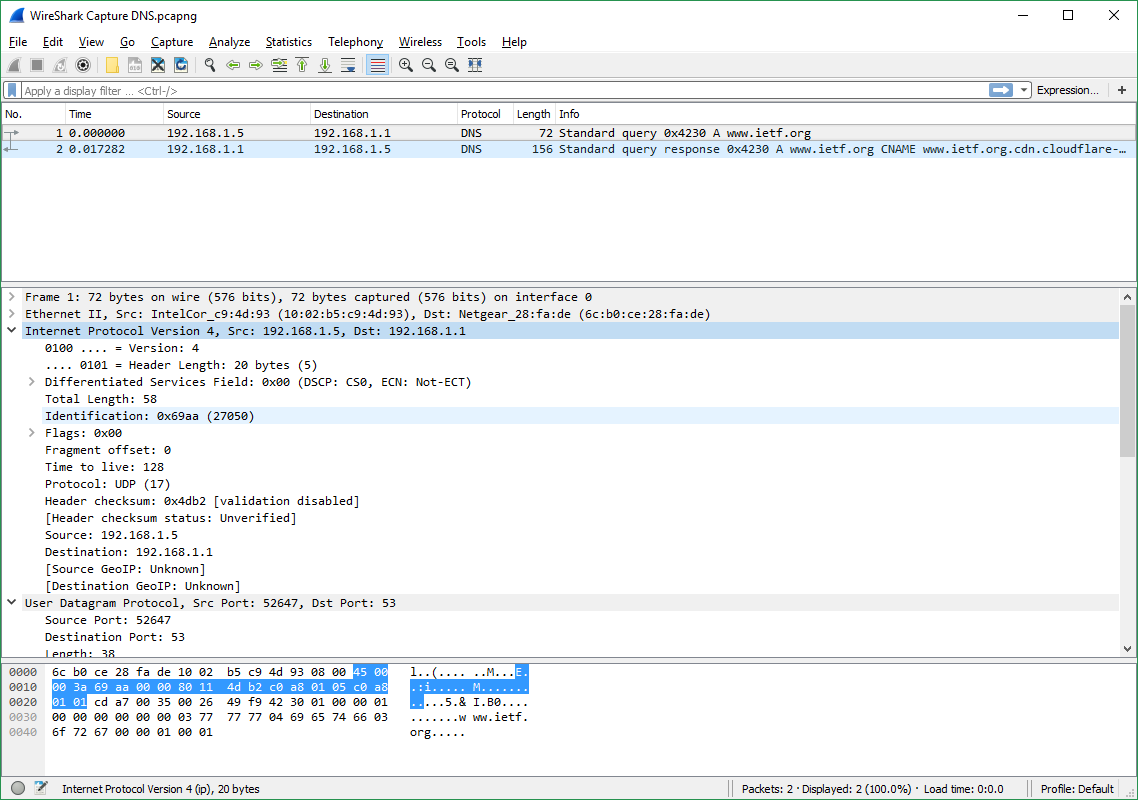
1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

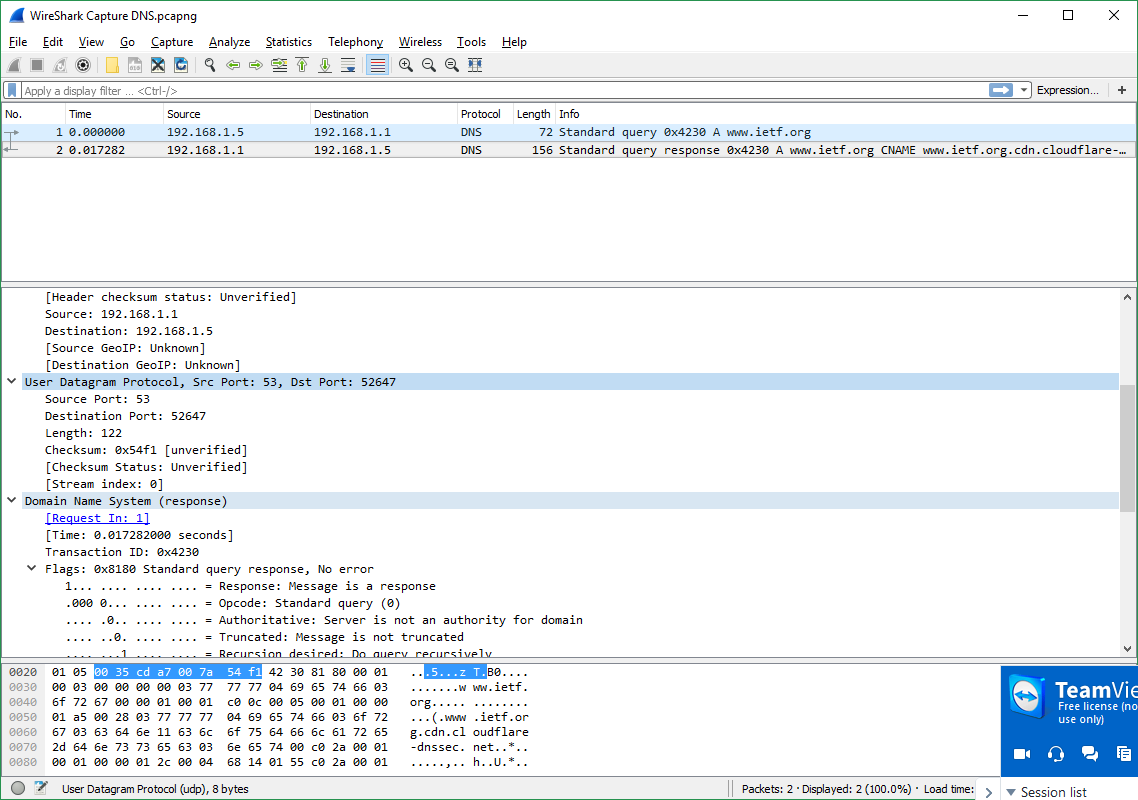
**Answer: Both the query and the query response use UDP**



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

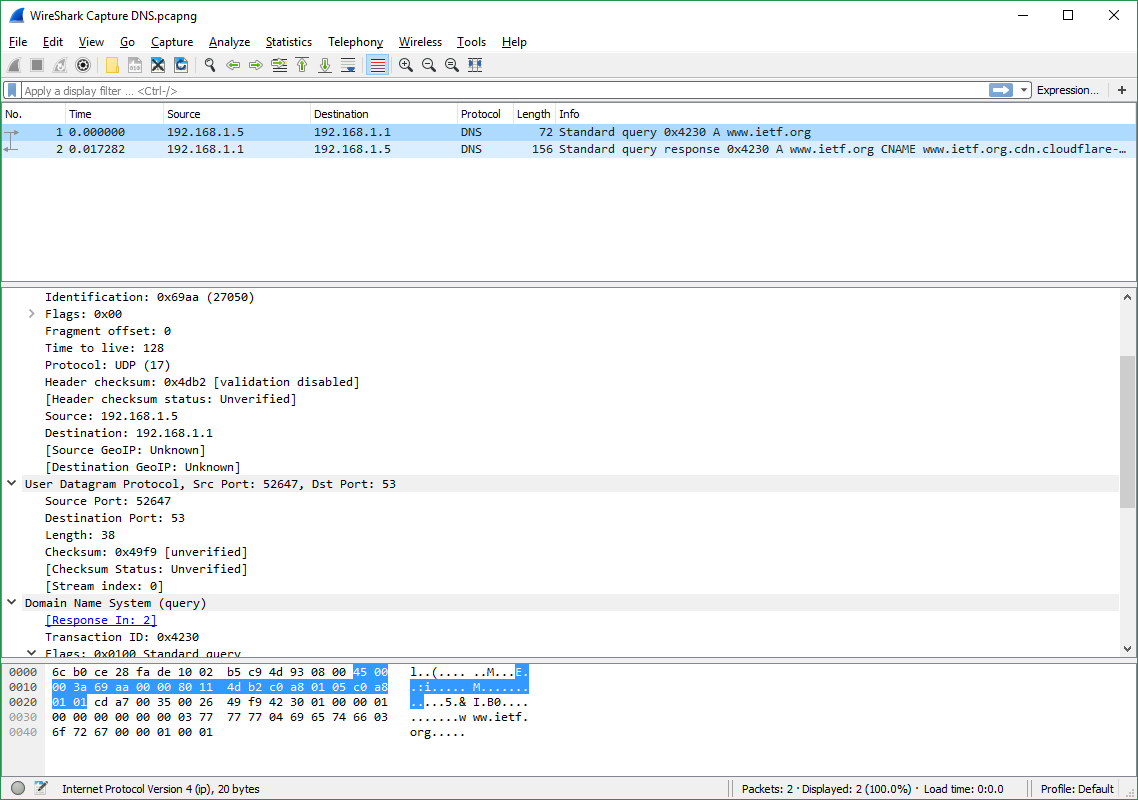
**Answer: Destination Port = 53 and Source Port = 53**

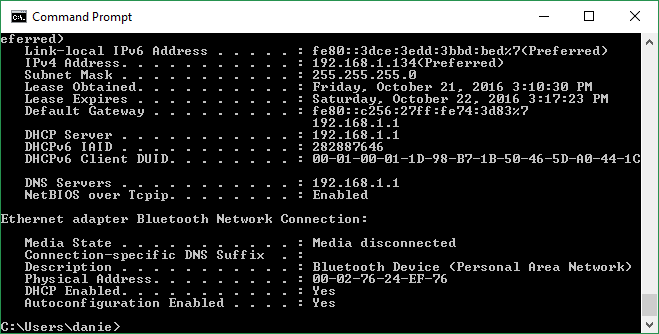




1. To what IP address is the DNS query message sent? Use ipconfig to determine the  
   IP address of your local DNS server. Are these two IP addresses the same?

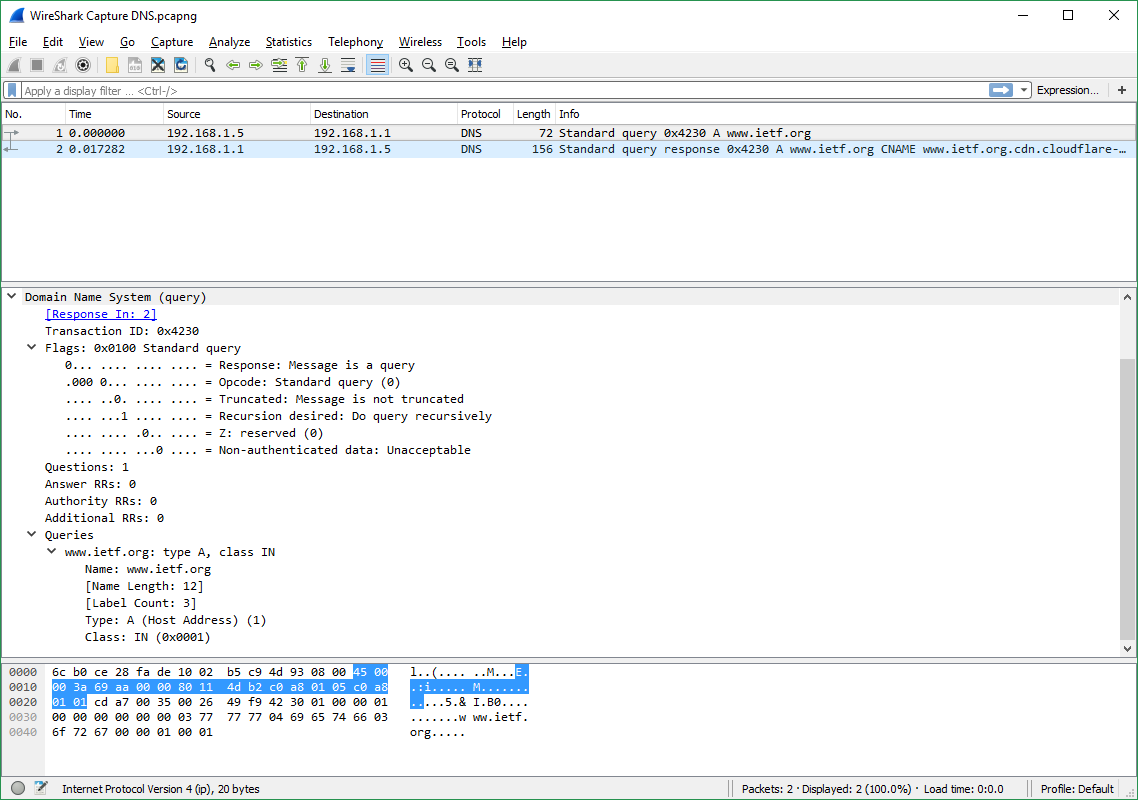
**Answer: IP Address = 192.168.1.1 | Local DNS server IP Address = 192.168.1.1 (Local DNS was found using the command “ipconfig /all”**





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

**Answer: Type-A, class IN. The Query message does not have any answers associated with it.**



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

**Answer: There were 3 answers provided. All of the answers have the following: Name, Type, Class, Time to live, and Data length. The first answer is of type “CName” and its value is** [**www.ietf.org.cdn.cloudflare-dnssec.net**](http://www.ietf.org.cdn.cloudflare-dnssec.net)**. The other two responses are of type A and have addresses associated with them. (2nd: 104.20.1.85, 3rd: 104.20.0.85)**

