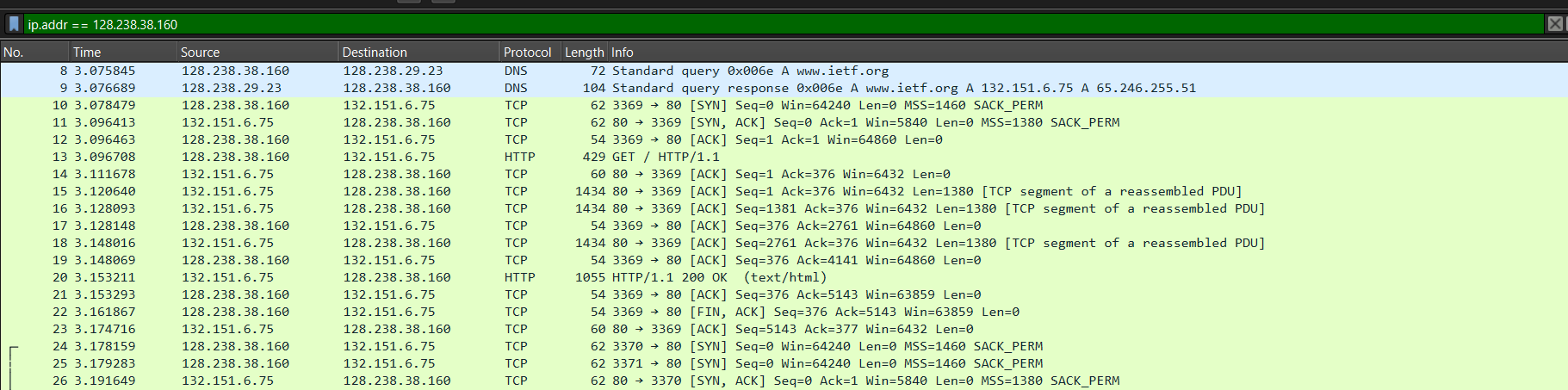
PARSHWA HERWADE 22510064,S4

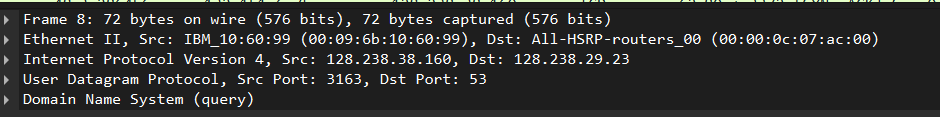
CN 12 : WIRESHARK LAB :DNS

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

Ans. They are sent over UDP

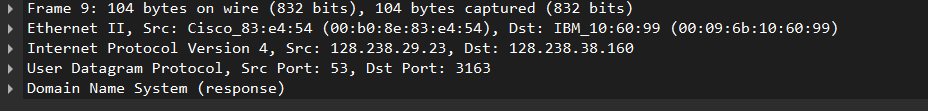


1. What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans. 

The destination port for the DNS query :53

The source port of the DNS response : 53



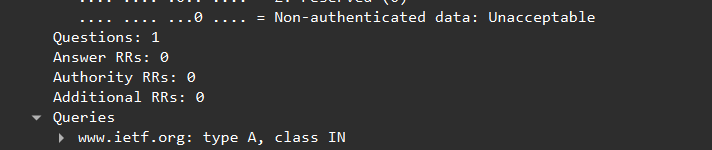
1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans. Destination: 128.238.29.23

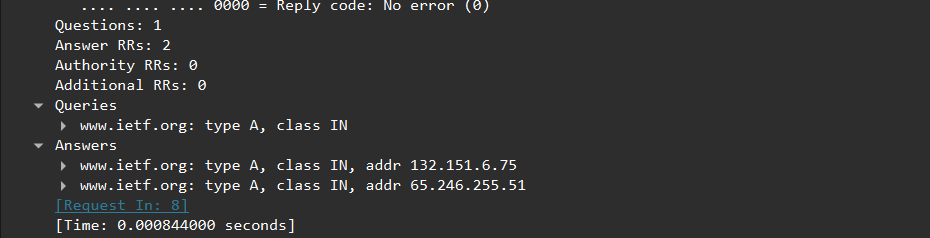
No, they are not same.

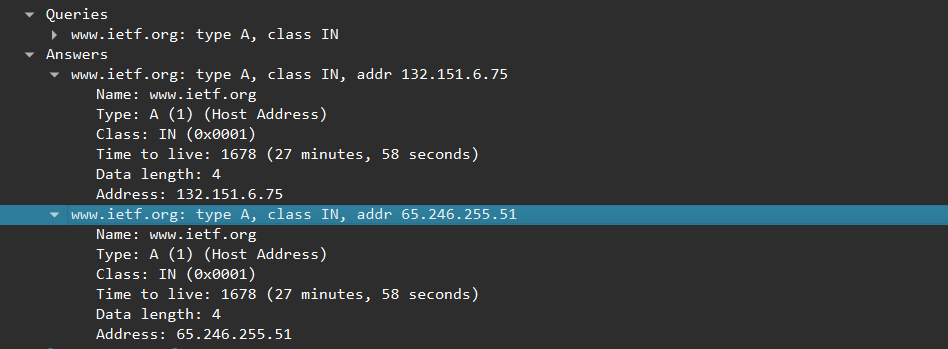
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans. Standard query with no messages.



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

Ans. Yea 2 answers, it contains TTL,type,class,address,name.



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?

Ans.

The first SYN packet was sent to 132.151.6.75 which corresponding to the first IP address provided in the DNS response message.

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

Ans. No.

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

Ans. Both are 53.

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

Ans. Destination: 128.238.29.23.Yes, it is of the DNS server to which request was sent.