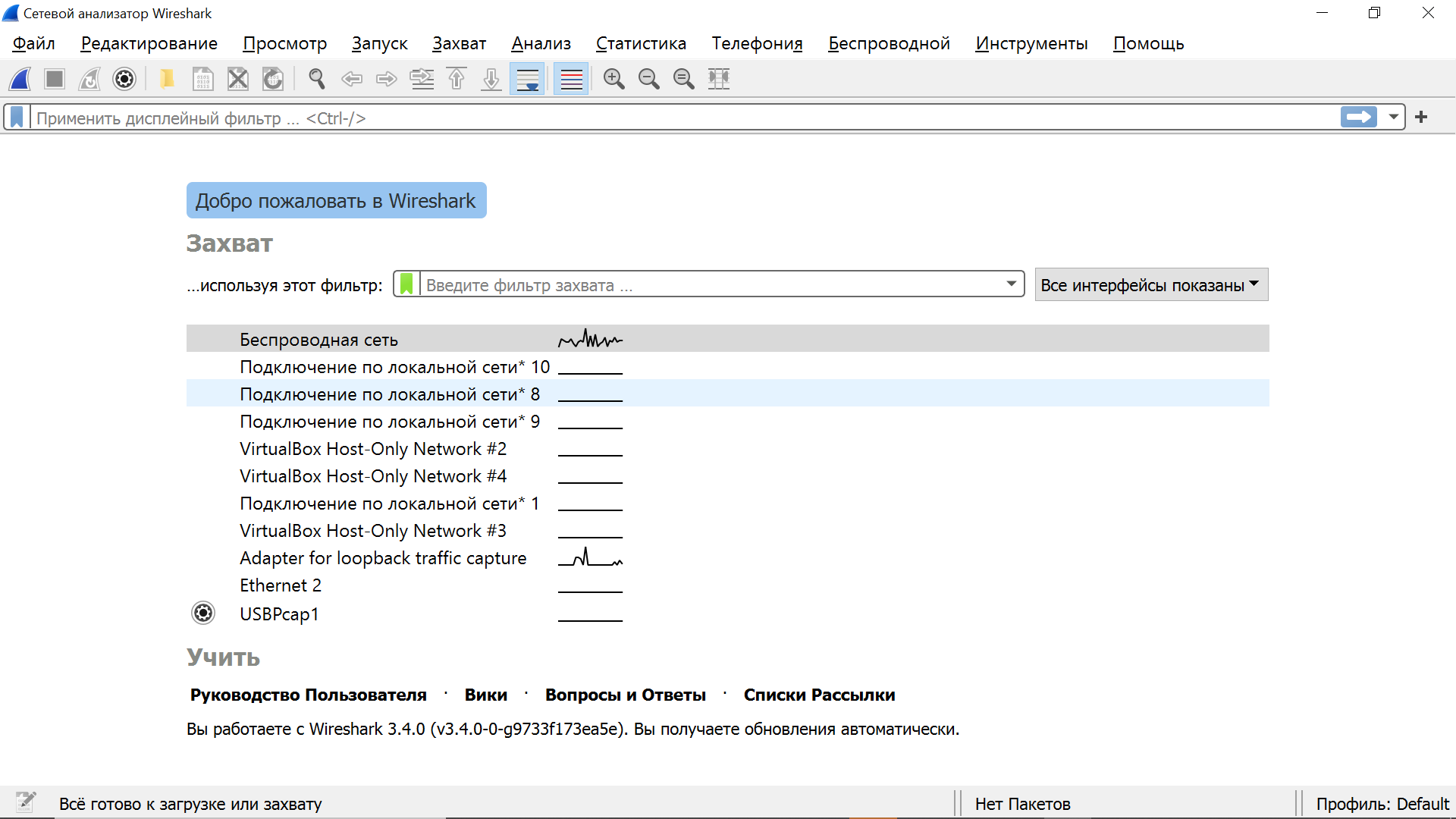
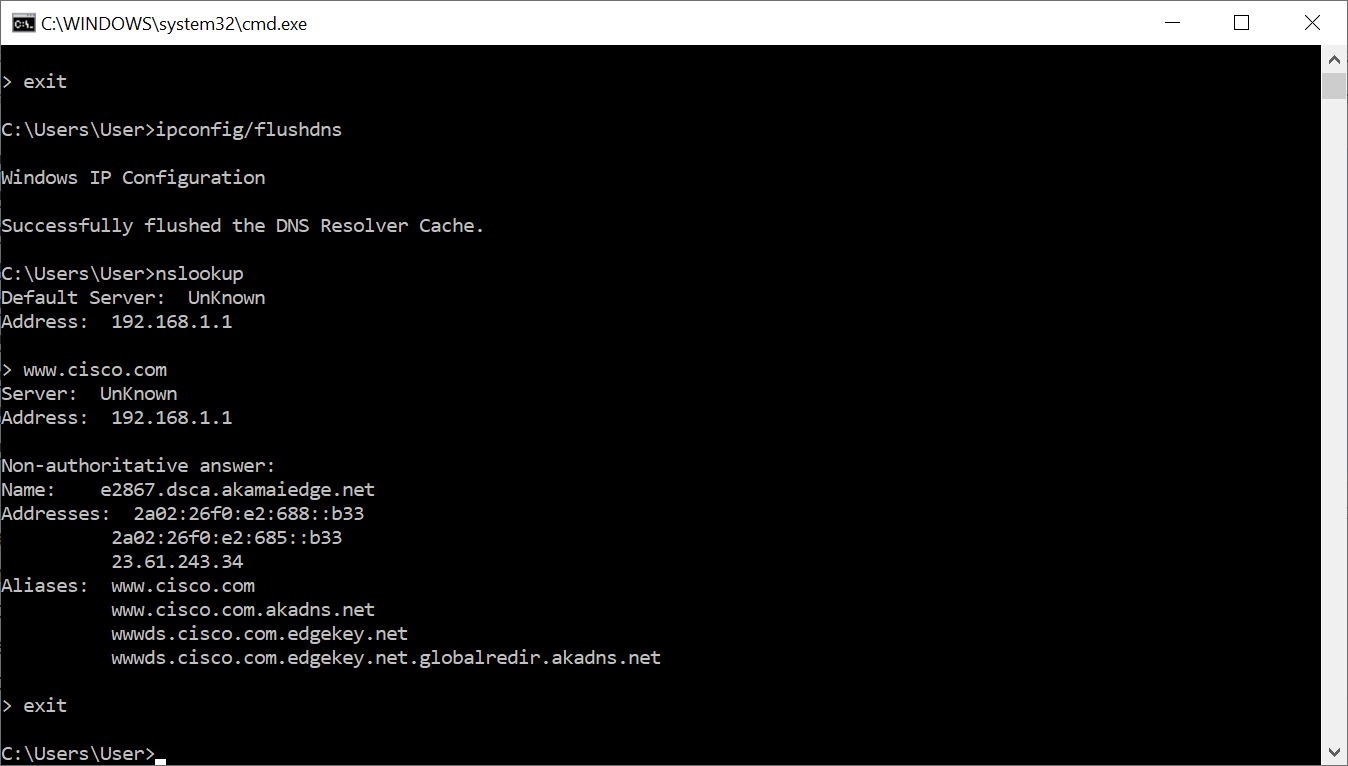
**Lab – Exploring DNS Traffic**

**Part 1: Capture DNS Traffic**

**Step 2: Capture DNS traffic.**

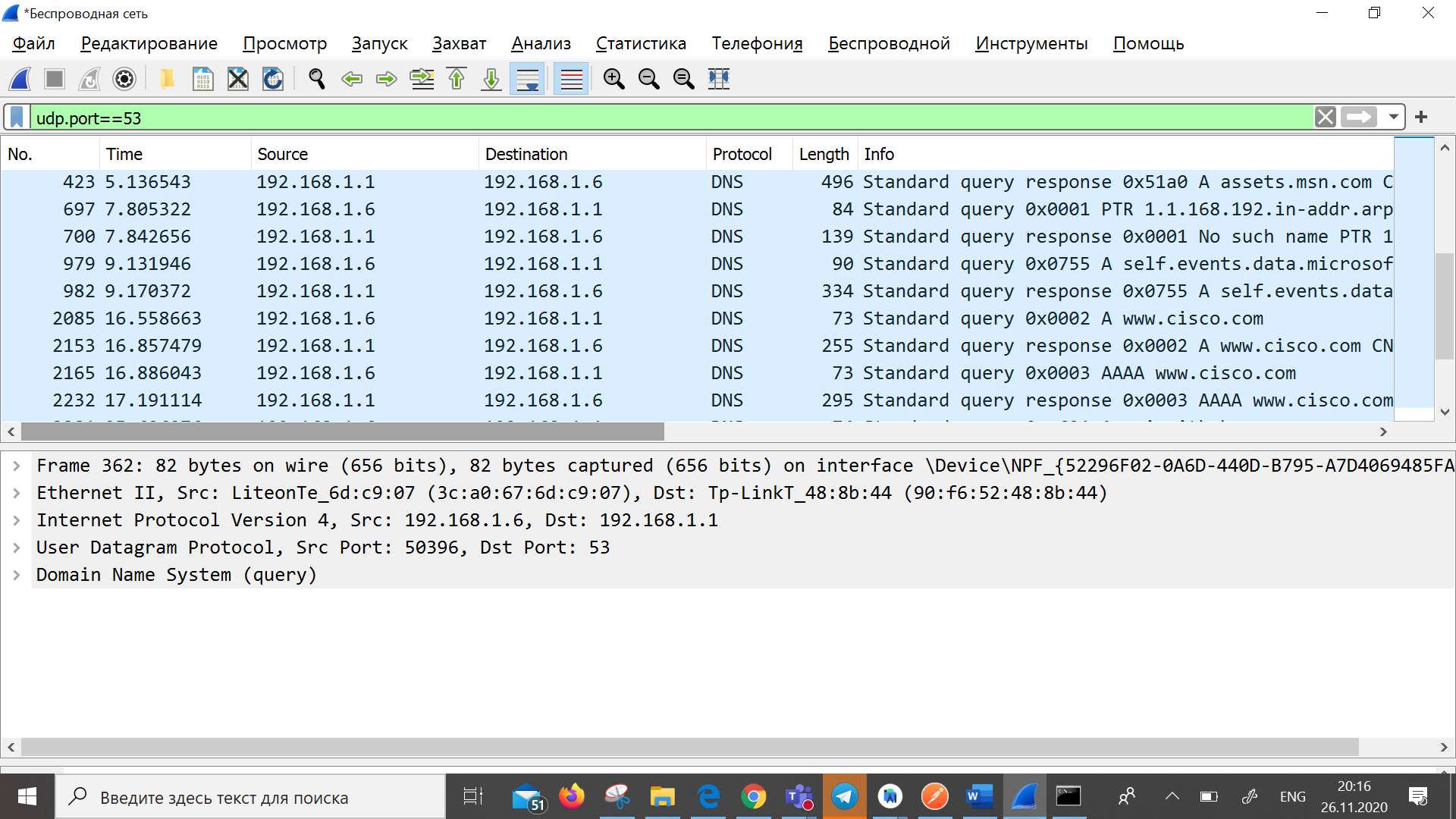


Wireshark welcome page

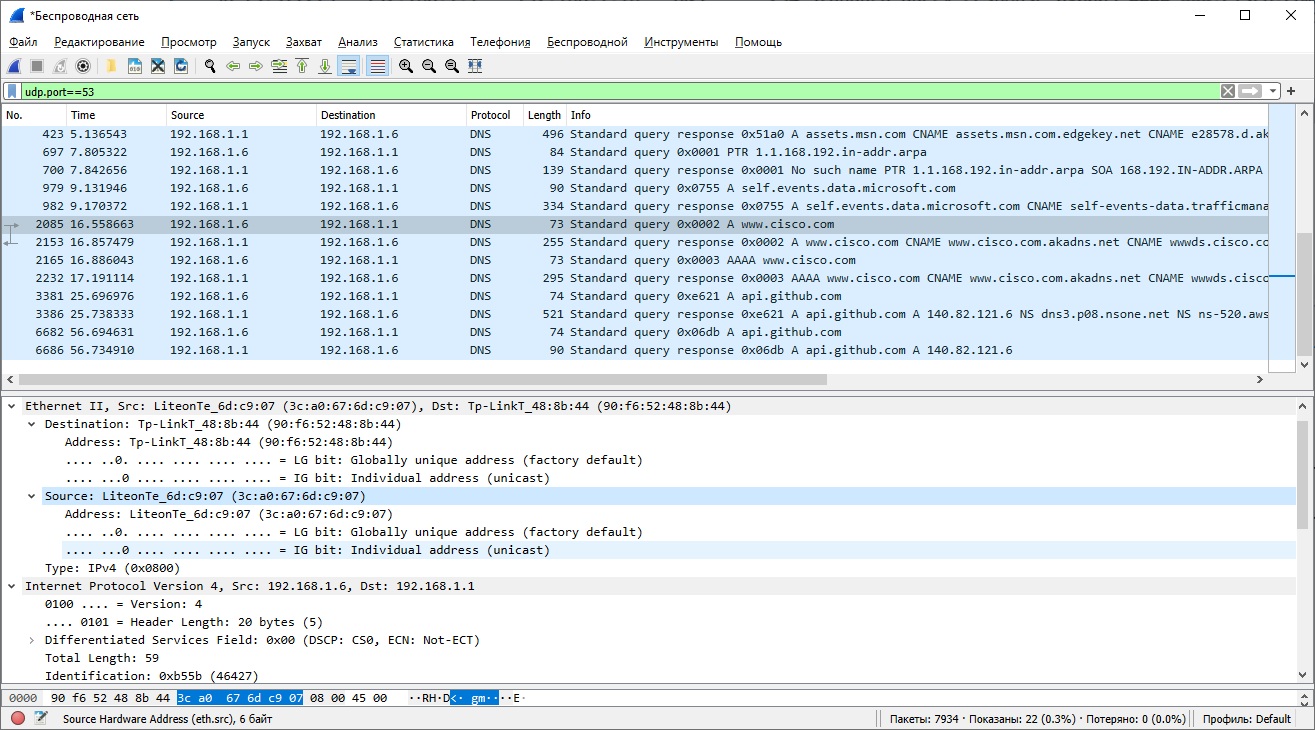


Nslookup [www.cisco.com](http://www.cisco.com)

**Part 2: Explore DNS Query Traffic**



Traffic captured in the Wireshark Packet list pane

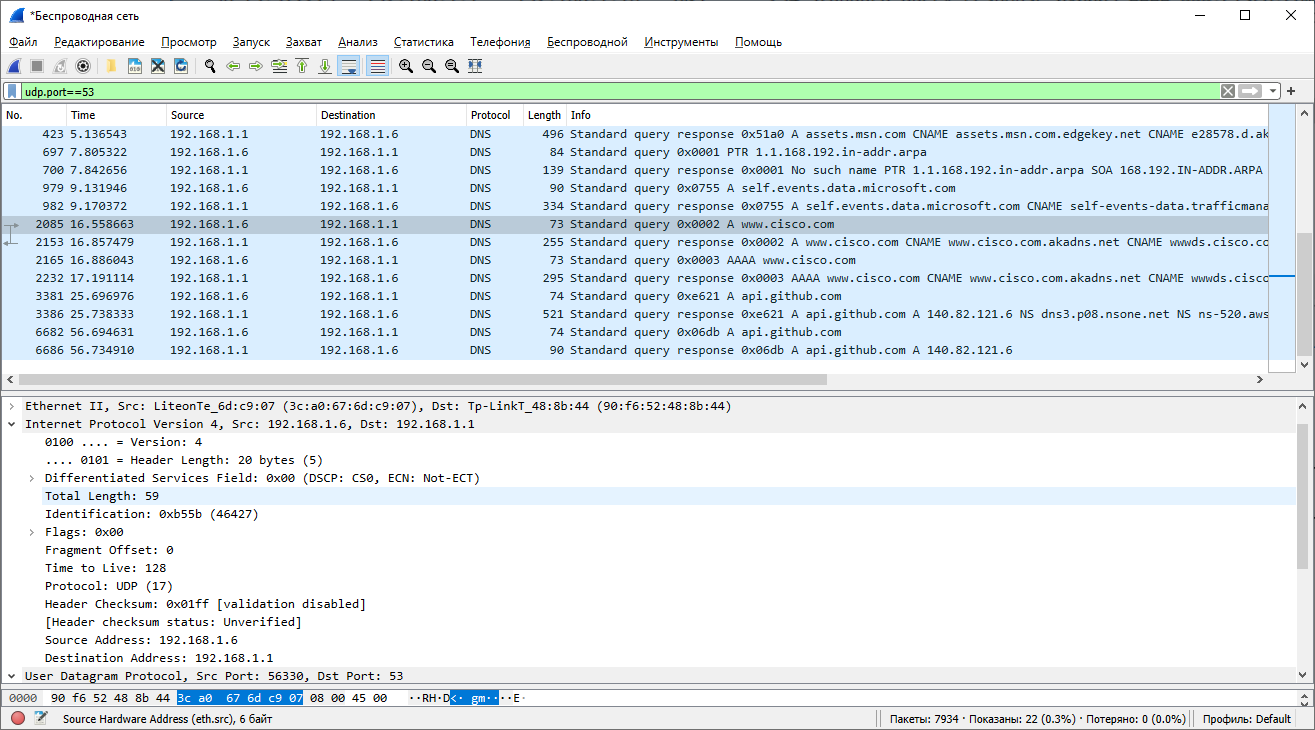


**What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?**

Source: 3c:a0:67:6d:c9:07

Destination: 90:f6:52:48:8b:44

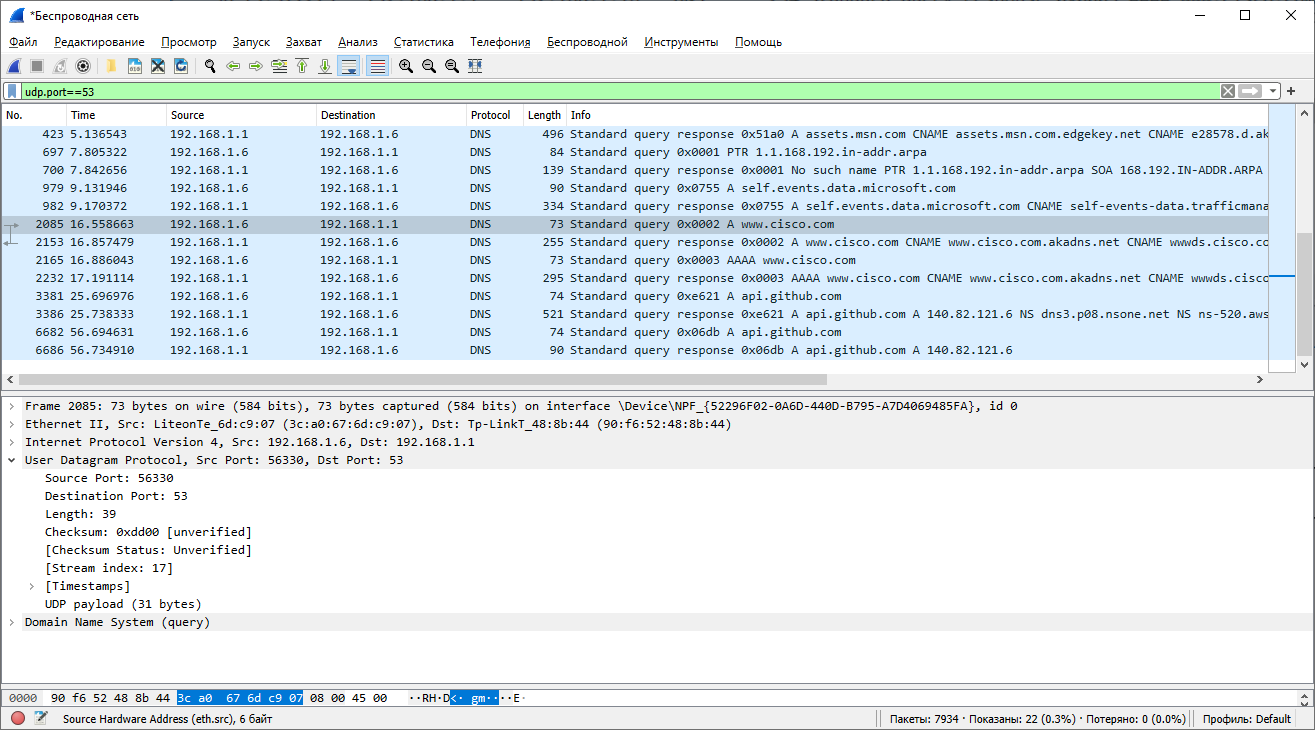
Source MAC address is associated with the NIC on the PC, destination MAC addeess is associated with the DNS server



**What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?**

Source: 192.168.1.6

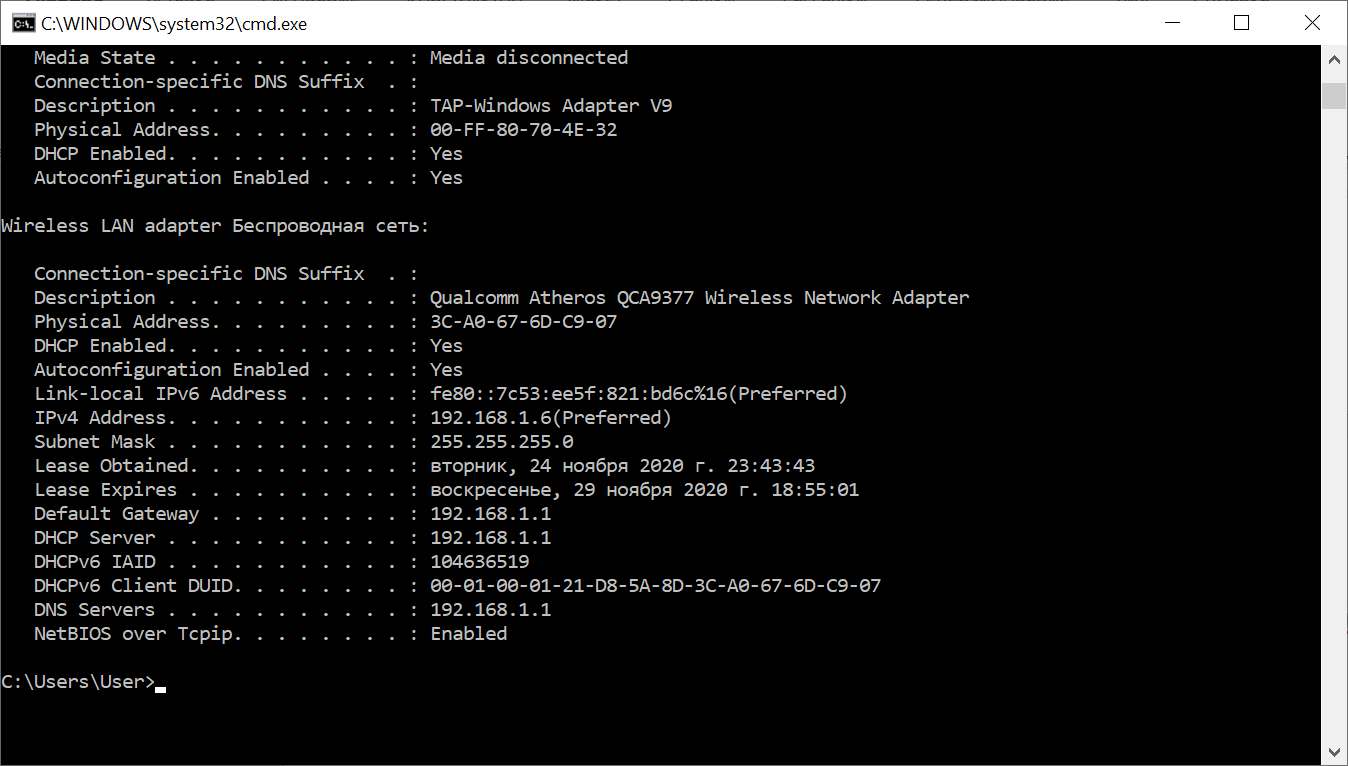
Destination: 192.168.1.1



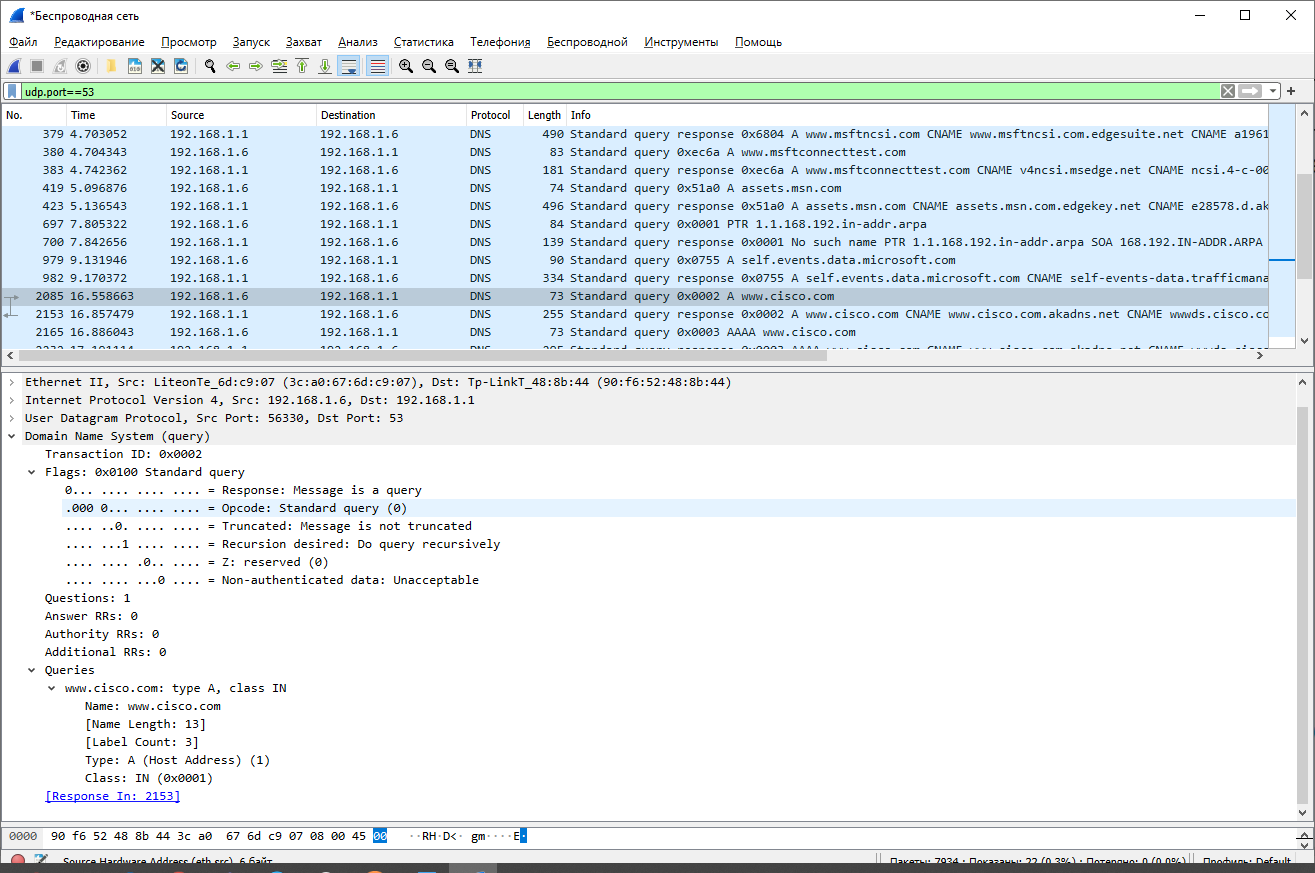
**What are the source and destination ports? What is the default DNS port number?**

Destination, DNS port number 53, Source port 56330

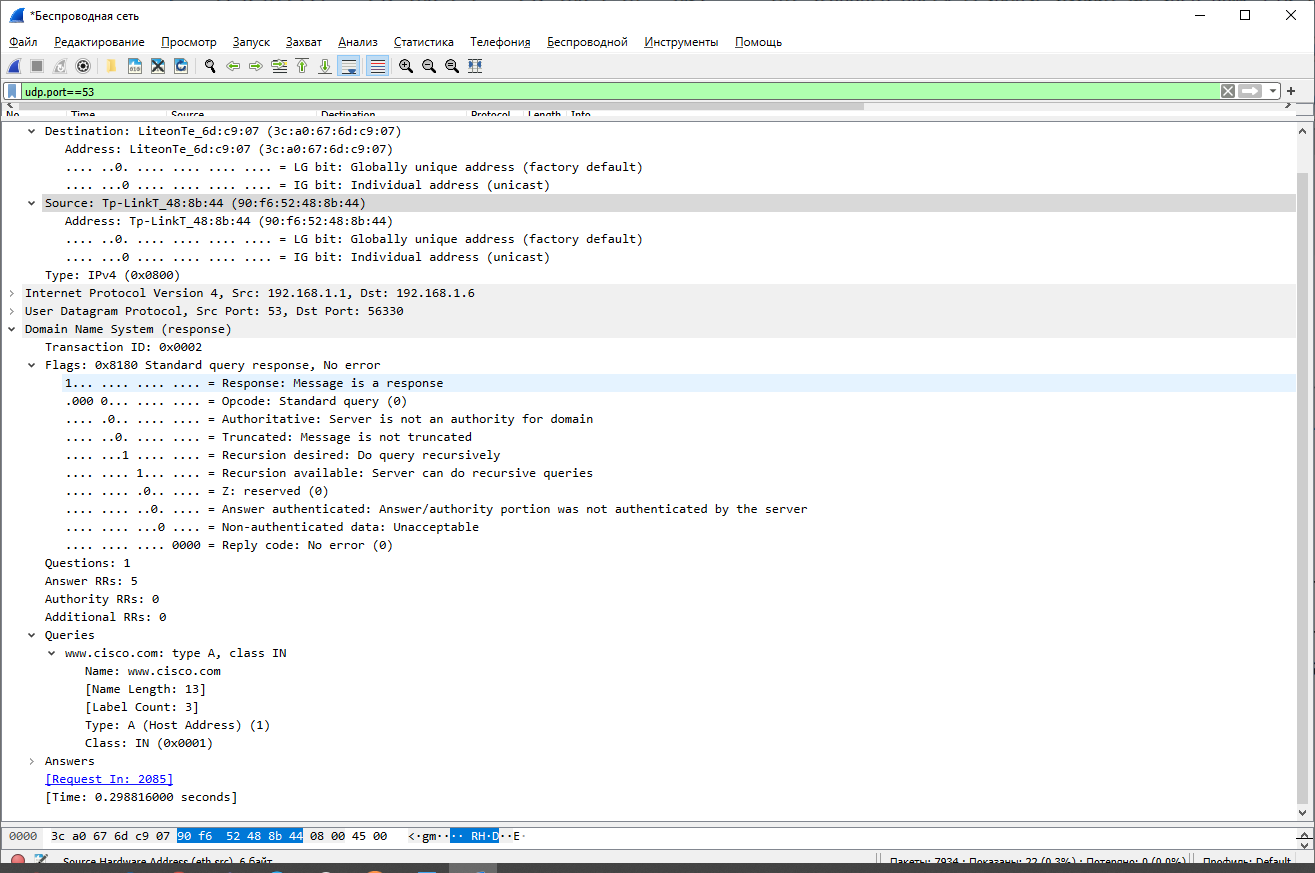
**Compare the MAC and IP addresses in the Wireshark results to the results from the ipconfig /all results. What is your observation?**



IP address and MAC address in Wireshark results similar with the ipconfig/all results.

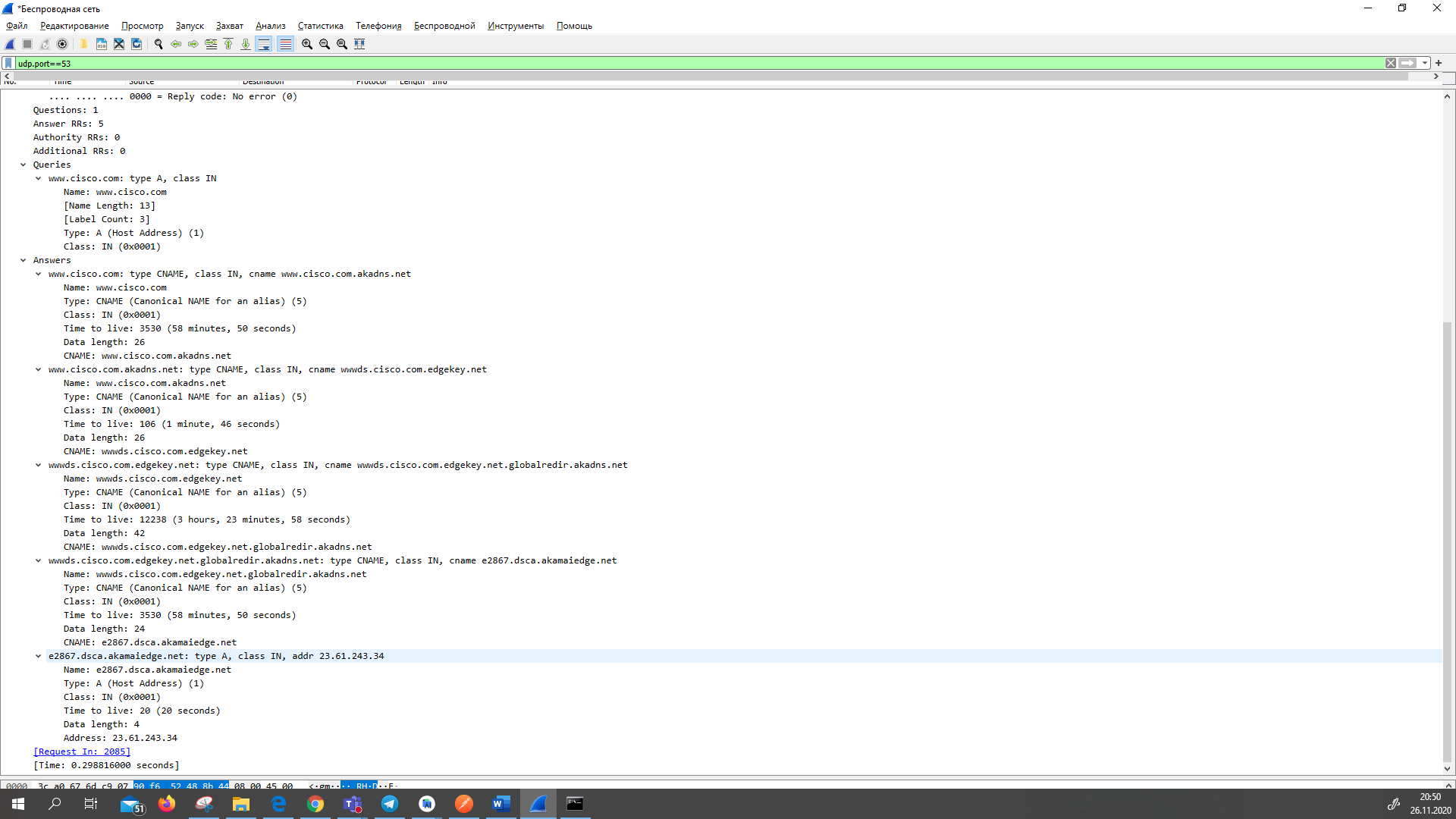


**Part 3: Explore DNS Response Traffic**



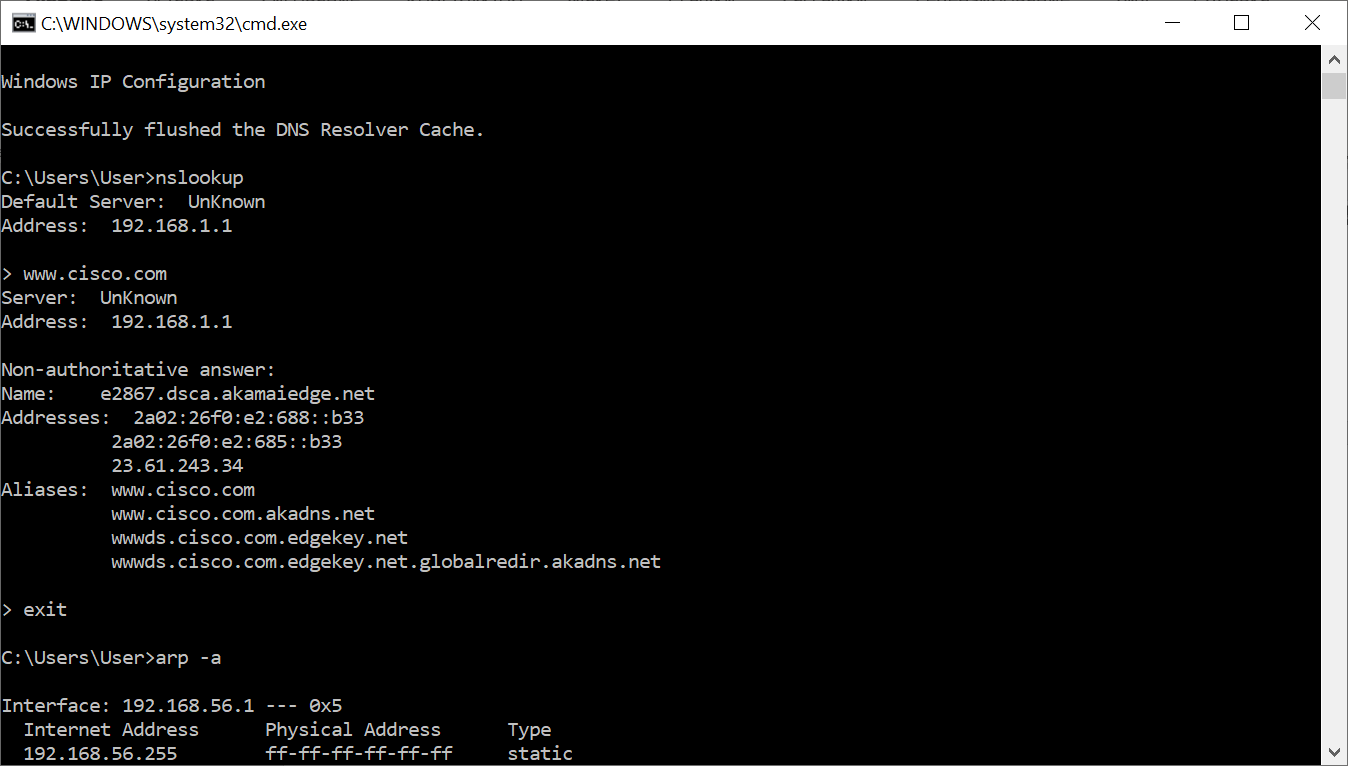
Source: MAC address(90:f6:52:48:8b:44), IP address(192.168.1.1), 53 port

Destination: MAC address3c:a0:67:6d:c9:07), IP address(192.168.1.6), 56330 port. They interchanged



**Observe the results. Can the DNS server do recursive queries?** Yes

**Observe the CNAME and A records in the Answers details. How do the results compare to nslookup results?**



They are similar in nslookup and Wireshark Answers type A

**Reflection**

1. **From the Wireshark results, what else can you learn about the network when you remove the filter?**

Without filter it shows all packets and we can observe other devices traffic in LAN

1. **How can an attacker use Wireshark to compromise your network security?**

If traffic does not encrypted attacker on the LAN can get information which contains in packet details