Lab 4

Team Members:

Alan Tony (191CS207)

Aashish Prateek (191CS225)

Computer Networks Lab (CS302)

Computer Networks Lab (CS302)

Computer Networks Lab (CS302)

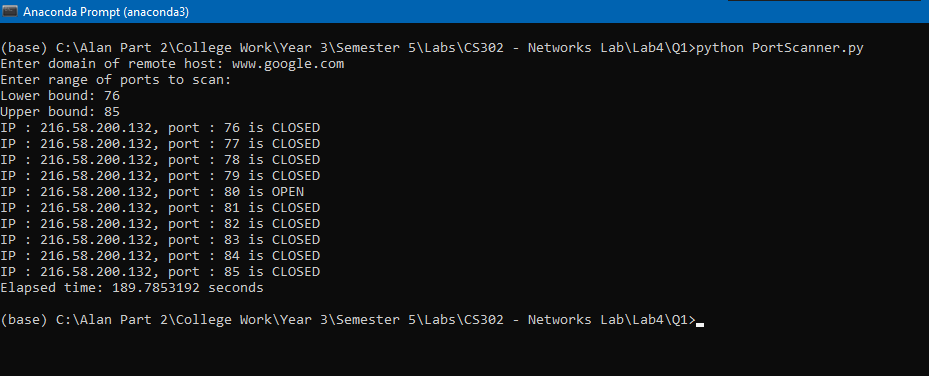


Question 1

Code:



Output:



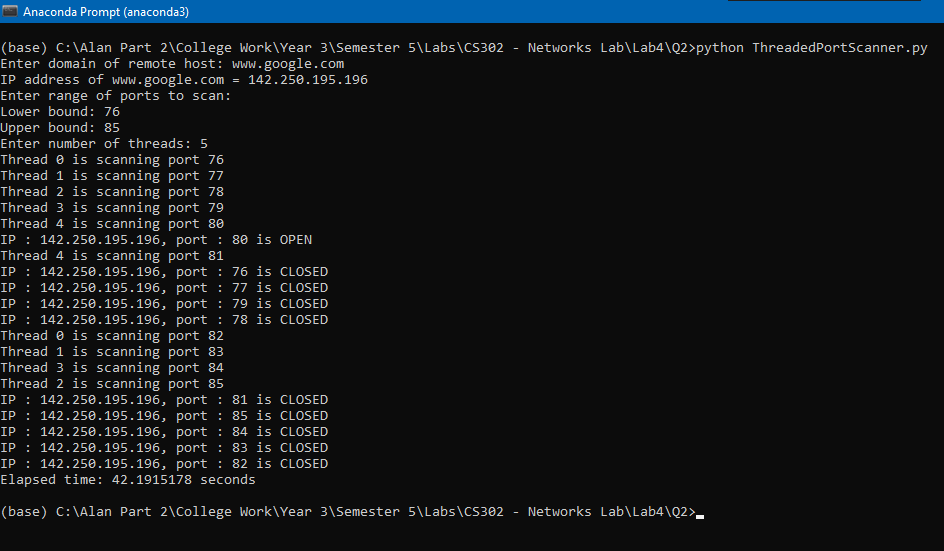
*P.T.O*

Question 2

Code:



Output:



The non-threaded solution (in Q1) took 109s whereas the threaded solution took only 42s for the same task. This shows the improved performance in scanning for multiple ports using multi-threading.

Question 3

To capture DNS traffic, the following steps were followed:

1. Start a Wireshark capture.
2. Commands entered on the Command Prompt:
3. ***ipconfig /renew***

(Renews DHCP assigned IP address)

1. ***ipconfig /flushdns***

(Clears DNS cache)

1. ***nslookup 8.8.8.8***

(Looks up the hostname for the specified IP address)

1. Stop the Wireshark capture.

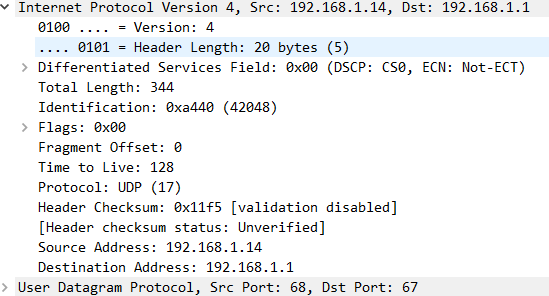
Part a) Analyze DHCP traffic

To analyze the DHCP traffic produced in the steps followed for DNS capture, we applied a filter **udp.port == 68.** We can use port 67 also, because port 68 is a destination port whereas port 67 is a source port. We will see 2 packets filtered out which are of types **DHCP Request** and **DHCP ACK** respectively.

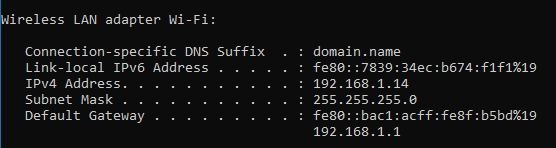
**Observations:**

* 1. In the **Ethernet II layer,** MAC address of the destination in the **DHCP request packet** matches the one obtained from the *Physical Address* field after entering the command *ipconfig /all.*
  2. The next layer is **Internet Protocol (IPV4)**. From here we can obtain the IP address of the client and server.

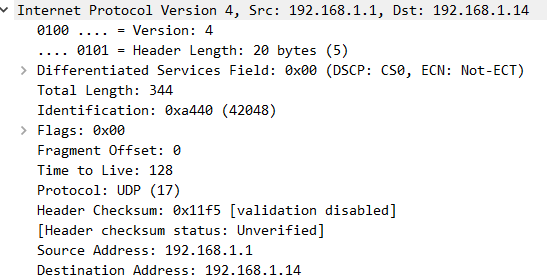
**In DHCP Request Packet:**



Our IP can be confirmed with the *ipconfig* command:

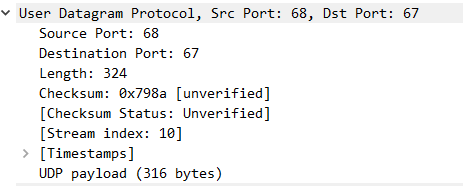


**In DHCP ACK Packet:**

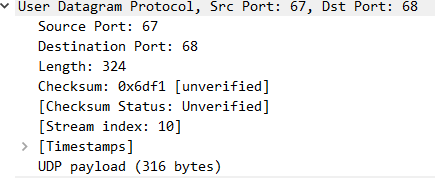
****

* 1. The next layer is **UDP.**

**In DHCP Request Packet:**

****

**In DHCP ACK Packet:**

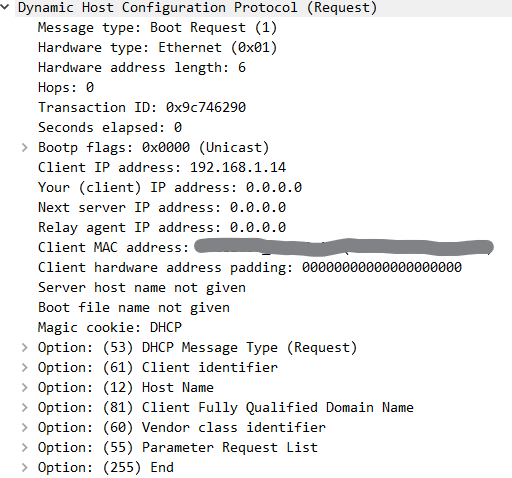
****

As we can see, in the DHCP Request, Source is 68 (Source port) as client sends this packet and Destination is port 67 (Destination port) and vice versa for DHCP ACK packet (Response form server).

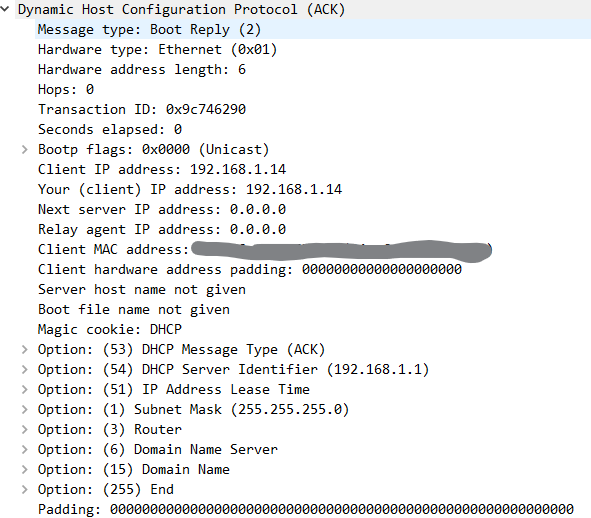
We can also see the checksum field, which is used to check if packets are received correctly.

* 1. The next layer is different for DHCP Request and DHCP ACK packets:

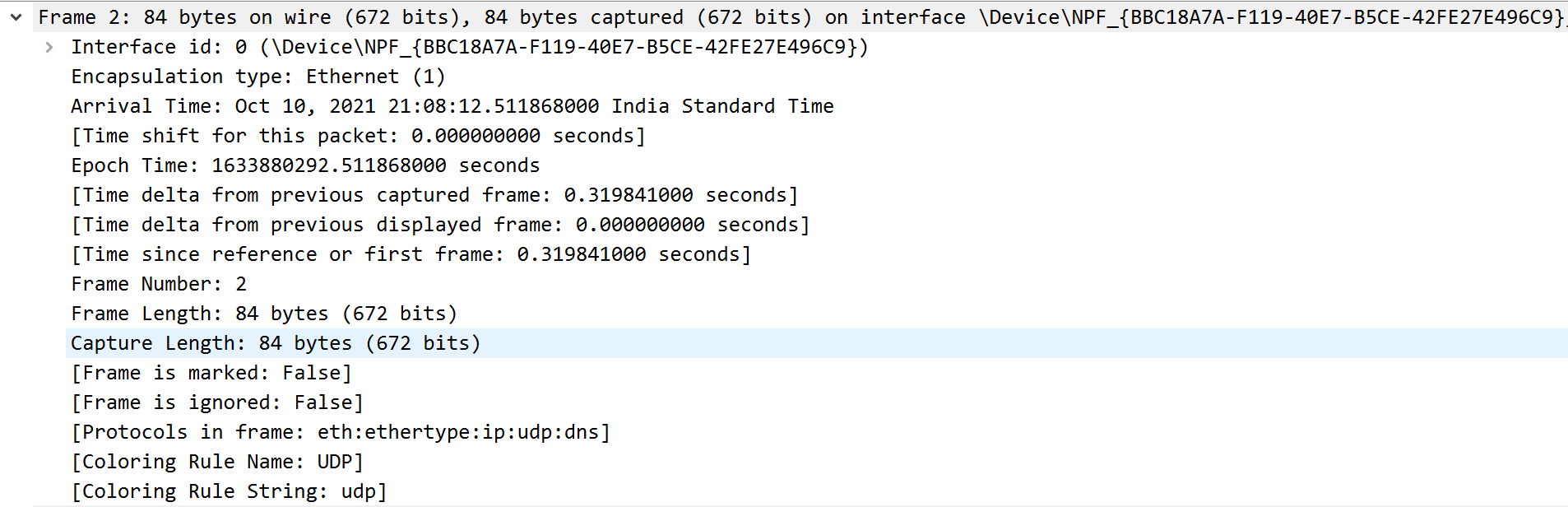
**In request packet: Dynamic Host Configuration Protocol (DHCP)**

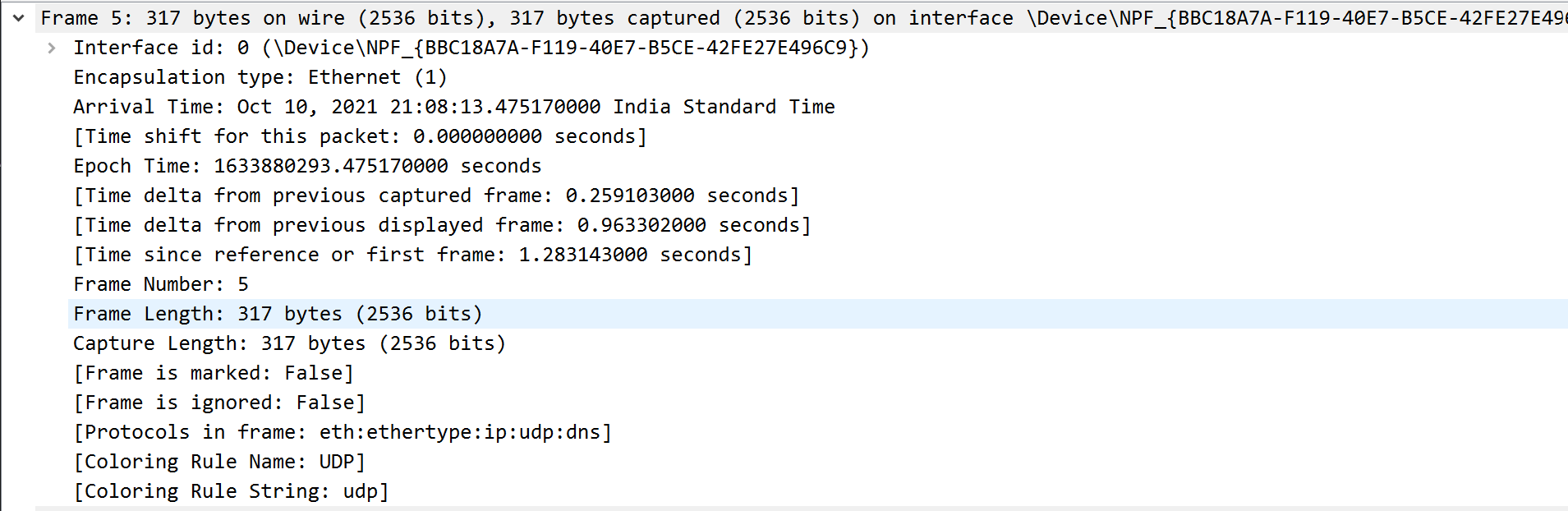
****

**In ACK Packet: Dynamic Host Configuration Protocol (ACK)**

****

Part b) Analyze DNS Traffic

We observe all the details of the packet along with its frame number=2, frame length=84 bytes, time shift of the packet in seconds and also time since first reference and many such details.

The response for the query yields the following packet results:

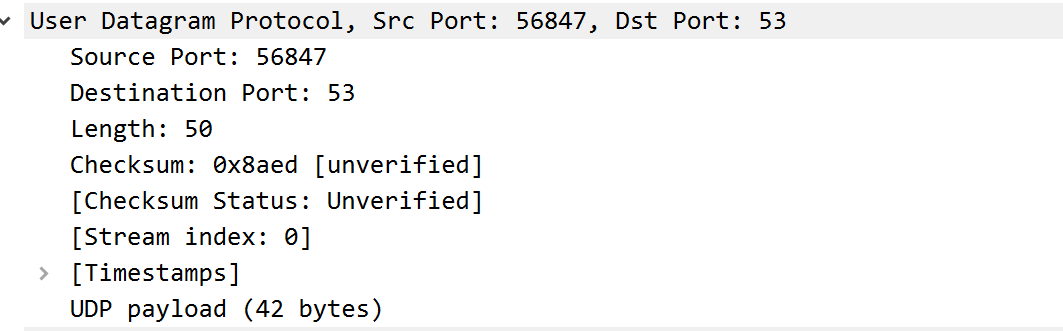
1. 

Here we observe that the source IP address for the query made by the client is 192.168.1.14 and its destination address(server) is 192.168.1.1

The response to the query has the following fields for source and destination IP addresses:

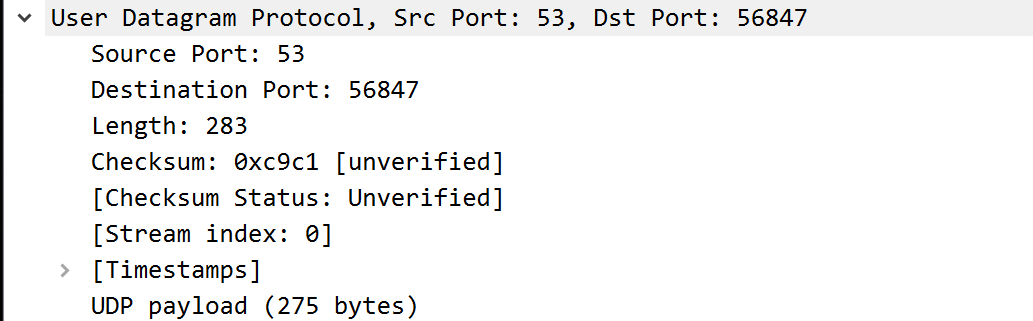


Here we observe that the source and destination IP addresses compared to the query are basically swapped.



Here we observe that the query made by the client uses source port 56847 and the destination port used is port 53.

The response to the query and its corresponding source and destination ports are:



**\*\*\*\*\***