Introduction to Computer Networks Labsheet2

Analyzing the Web pages accessed using Wireshark

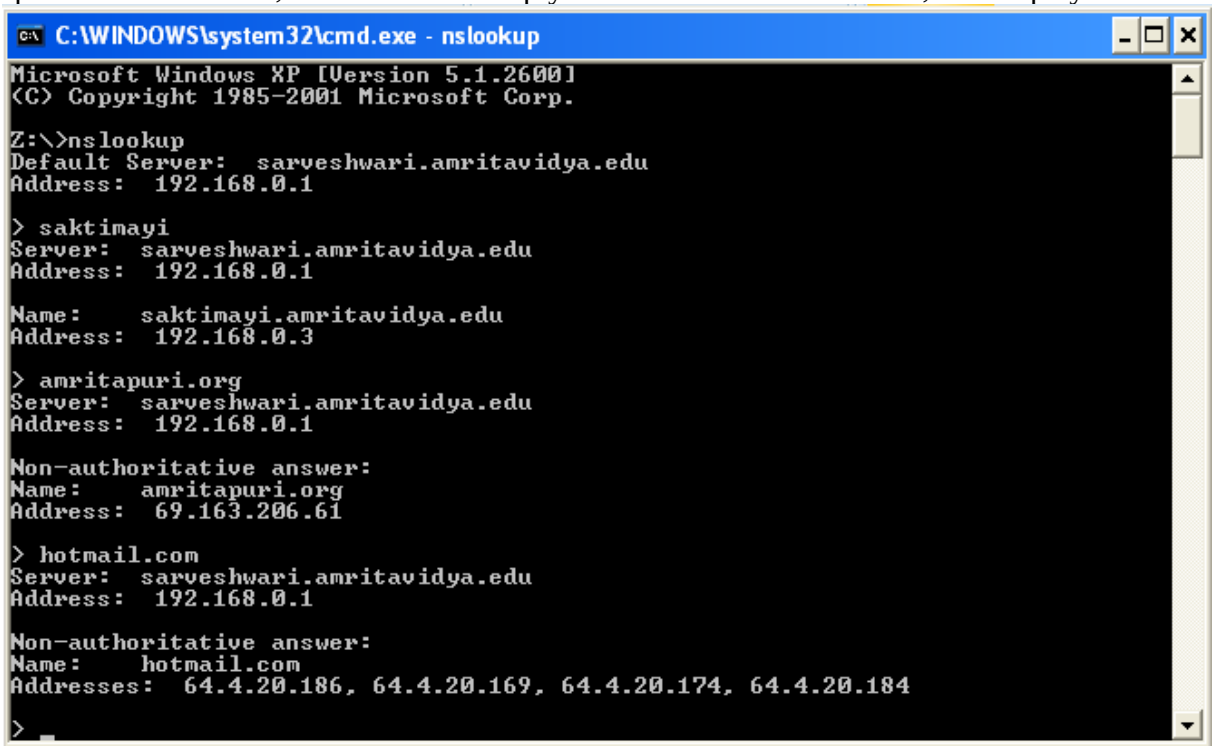
Name: Girish S

Roll: AM.EN.U4AIE22044

Part1: Mapping the given URL to IP address using nslookup

To run *nslookup* in Linux/Unix, you just type the *nslookup* command on the command line. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.
We as humans usually use the website address known as Uniform Resource Locator (URL) to identify the destination host. But IP address is used by the devices to identify the server in the network. Domain Name System (DNS) service by the DNS server helps the client to translate an unknown URL to an IP address and also cache it in the device itself for subsequent access. The local cache maintains DNS record having a map between URL and IP address.

In it is most basic operation, *nslookup* tool allows the host running the tool to query any specified DNS server for a DNS record. To accomplish this task, *nslookup* sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.



The IP address of abc.com is 18.67.161.122

The IP address of google.com is 142.250.182.142

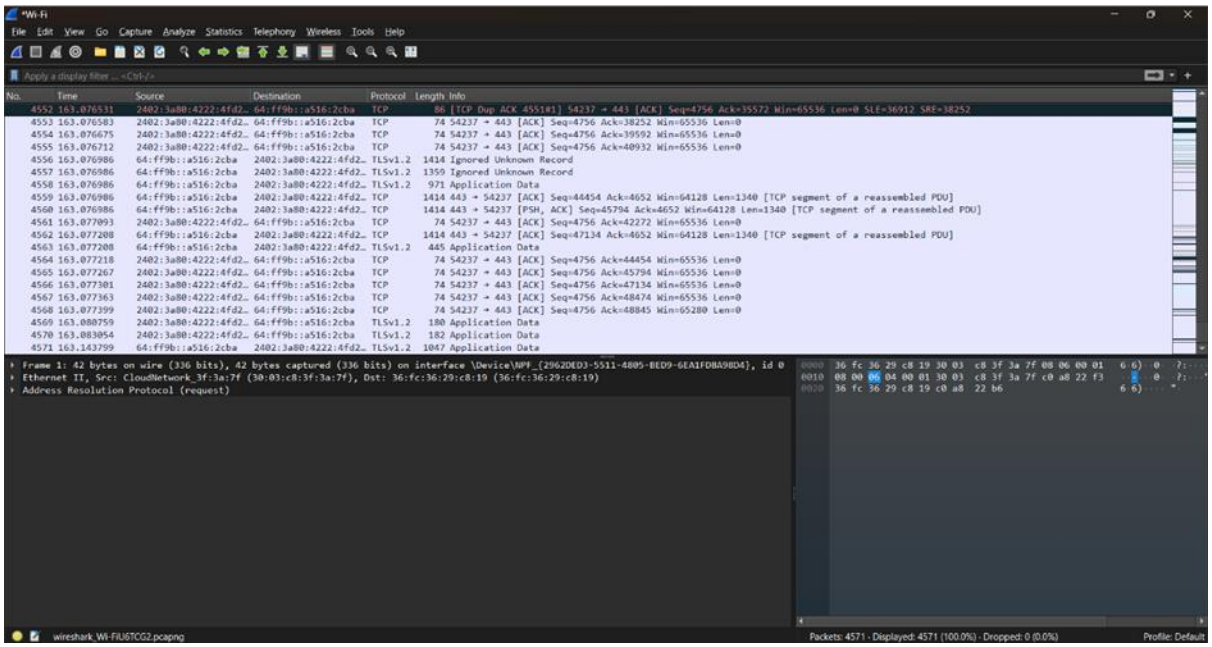
```
C:\Users\giri0>nslookup
Default Server:  UnKnown
Address:  192.168.0.250

> amritapuri.org
Server:  UnKnown
Address:  192.168.0.250

Non-authoritative answer:
Name:    amritapuri.org
Address:  10.0.0.80

> gmail.com
Server:  UnKnown
Address:  192.168.0.250

Non-authoritative answer:
Name:    gmail.com
Addresses:  2404:6800:4007:81e::2005
          142.250.193.133

> hotmail.com
Server:  UnKnown
Address:  192.168.0.250

Non-authoritative answer:
Name:    hotmail.com
Address:  204.79.197.212
```

Find the IP address of all websites that you are using for Part2.

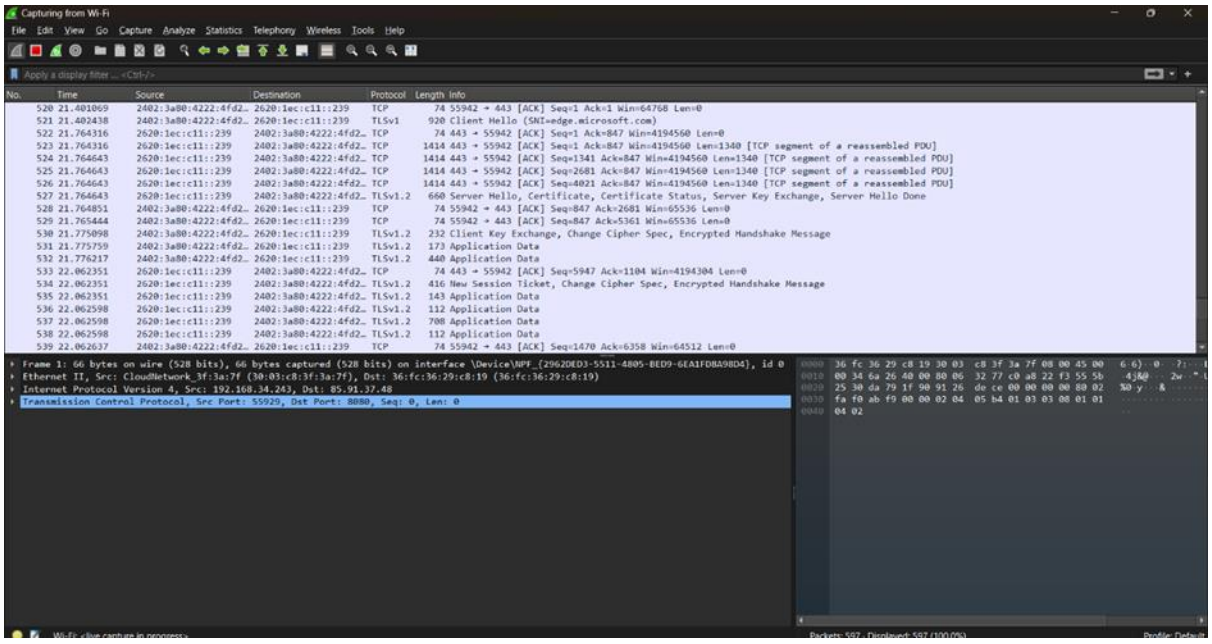
```
> example.org
Server:  UnKnown
Address:  192.168.0.250

Non-authoritative answer:
Name:    example.org
Addresses:  2606:2800:220:1:248:1893:25c8:1946
          93.184.216.34
```

Part2: Understanding the TCP/IP protocol stack using Wireshark

1. **Open Packet sniffer [Wireshark] Application and Capture the Wi-Fi/ Ethernet Interface**



2. **Do this activity and capture frames.**
   a. Request for a web page by typing the least used URL in the webserver



3. **Briefly explain the Encapsulation process in at least one http request frame of the protocol analyzed. Also complete the table below by PDU contents and details requested in each layer. Also try to provide proof in the form of a relevant screenshot.**

Ans - When a request is sent from the application layer, the data (message) can be divided and split into capsules called TCP segments. These segments are further packeted into IP

packets which have source and destination address. This is further covered in an ethernet frame which has the source and destination MAC addresses. These packets are now transmitted to other networks by the router. Finally, the data converts from electrical signals to optical signals in the physical layer**.**

Layer	Protocol	Important Contents (You can get details on clicking on a packet)	Purpose of the content specified in the Layer
Application	HTTP	GET request	To provide network services to end services
Transport	TCP	Provides source and destination port	Segmenting data into packets and managing the flow of transport
Internet	IPV4	Provides source and destination IP addresses of the request	Helps with routing the packets to appropriate destination
Data Link	Ethernet	Provides source and destination MAC address and provides the frame size (in bits)	Enables routing and packet forwarding to aid effective transmission of data across networks