**21CY681 - INTERNET PROTOCOL LAB - II**

Name: Akhil K J

Register Number: CB.EN.P2CYS22009

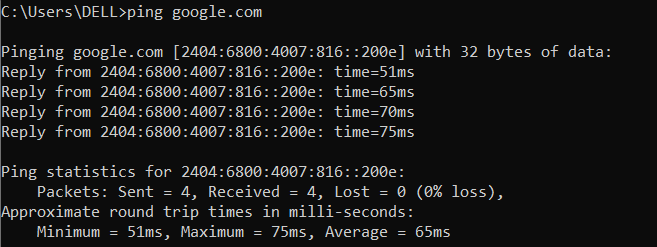
Date: 22th October 2022

Assignment Topic:  Understanding network traffic analysis using wireshark

1. Understand PING and document it, then answer the following question: (3 marks)

Ans:- PING Command is a command to test the ability of the source computer to reach the destination computer. It is done to verify whether a computer can communicate with another computer or not.

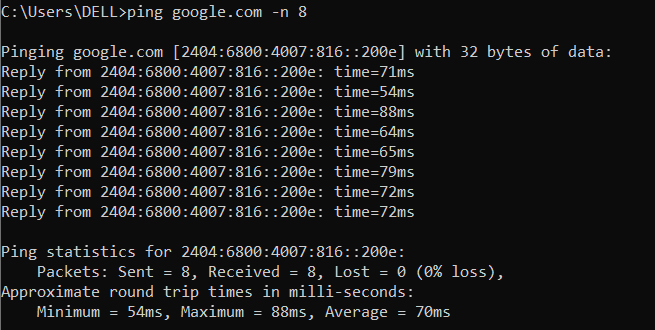
a. Use ping on google.com and document your results on the output you received. [Find the IP address, Time to live value, and round trip time value from the results you got].



IP address: 2404.6800.4007.816::200e

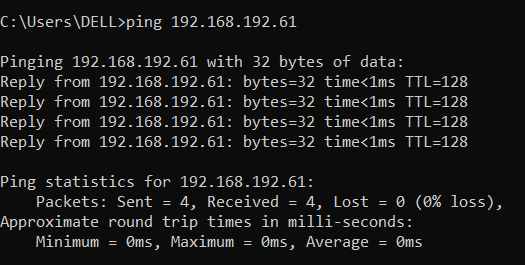
Round trip time:

b. By default, ping will send 4 packets to check the details, here you have to send 8 packets to check the output over google.com. Explain what the purpose of this doing is.



We use –n flag to send no of packets which we desire to send to google.com or any other server.

c. Ping your local host. Explain what the purpose.

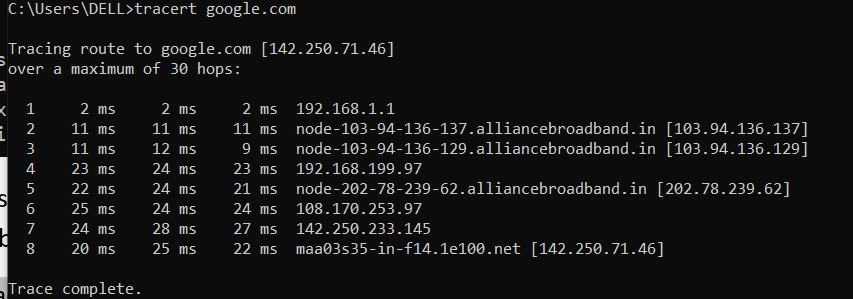


We use ping command to see if localhost is up and running. Localhost is used by developers to test their website in their own browser.

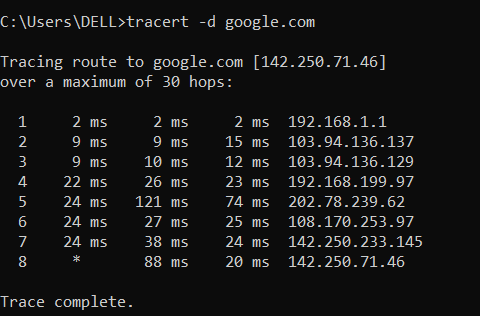
1. Read the Unix manual page for traceroute OR help for tracert. Experiment with the various options. Describe the three things that you found most useful in the result. (2 marks)

Answer the following question:

a. Try tracert over google.com

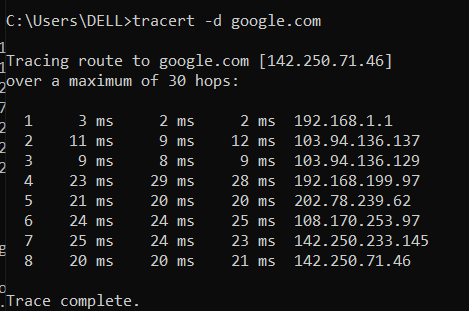


b. Type tracert -d google.com



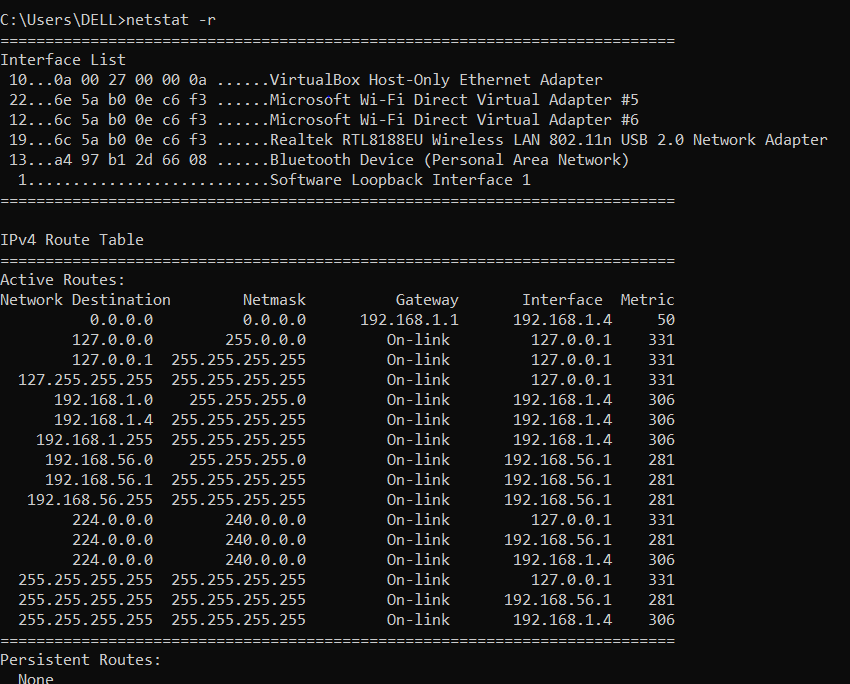
1. How many hops is your machine away from google.com? - 14 Hops

2. Wait for a while and execute the same command again. Is the output the same as the first time? Observe and compare the difference and explain the reason.

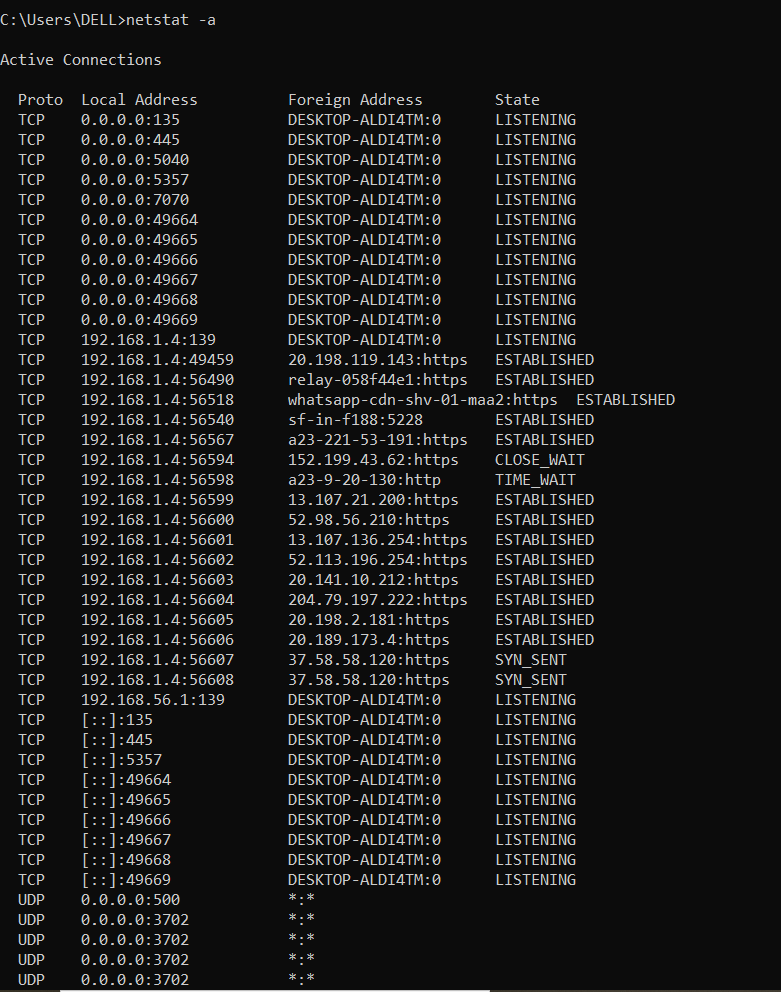


3. You have to read about NETSTAT from the manual page or help before answering the below questions:

a . Use netstat to display information about the routing table.



b. Use netstat to display about ethernet statistics.



4. What is the purpose of NSLOOKUP ?

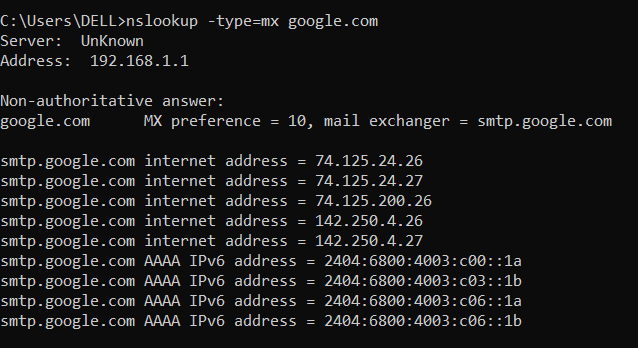
It is a command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System to obtain domain name or IP address mapping or any other specific DNS record.

Answer the following questions below:

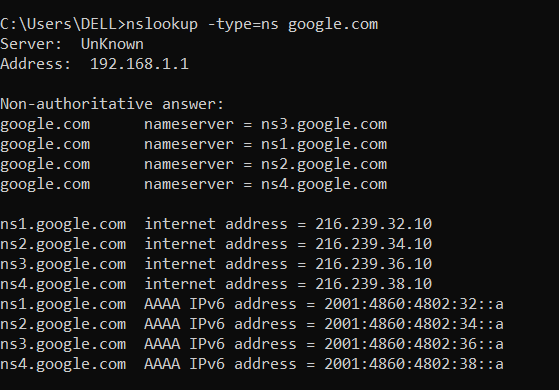
a. Use nslookup to find out the internet address of the domain amrita.edu.

ANS - 3.33.154.67 and 15.197.141.123

b. What is the mail exchanger for the domain google.com.



c. What is the name server for amrita.edu

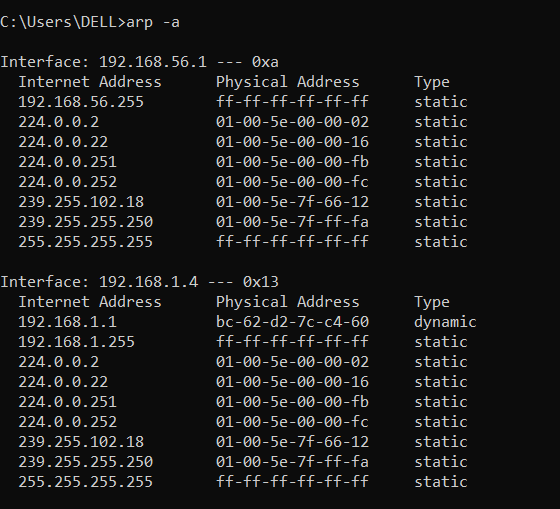


5. What are ARP and RARP?

**ARP stands for Address Resolution protocol .It retrieves the receiver's physical address in a network.** **RARP stands for Reverse Address Resolution Protocol . It retrieves**  logical address for a computer from the server..

Answer the following questions below: (3 marks)

a. Use arp command to find the gateway address and host systems hardware address.



The gateway address is 10.11.128.1 & the hardware address of the host systems are 44-31-92-56-07-97 , 80-91-33-94-5a-3b .

b. How do you find the arp entries for a particular interface?

To find the arp entries for a particular interface we need to use the **–N** flag along with the ip address.

c. How do delete an arp entry?

To delete an arp entry, we need to use the **–d flag** along with the ip address . To delete all the entries we need to use the wildcard flag(\*) .

d. How do you add an arp entry in arpcache?

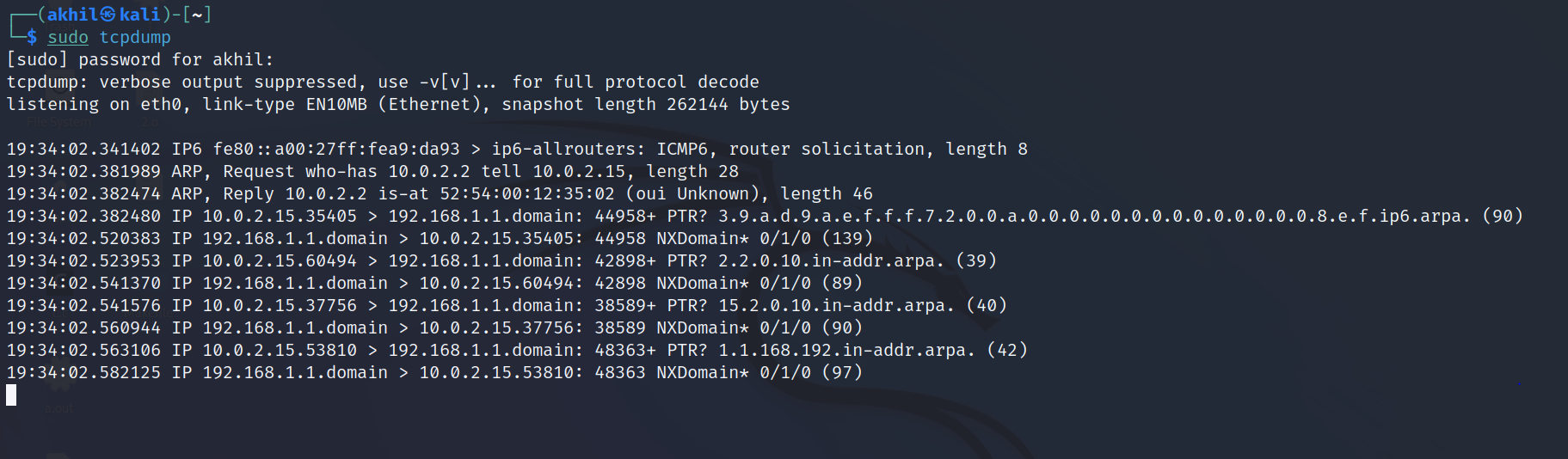
To add an arp entry we need to use –s flag along with IP address and MAC address.

EXAMPLE - arp -s  192.168.43.160  00-aa-00-62-c6-09

6. Read about TCPDUMP tool [use manual page].

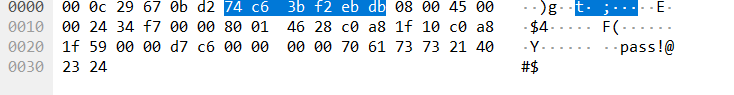
Answer the questions below: (1 marks)

a. Using tcpdump, get the information about the general incoming network traffic with names.

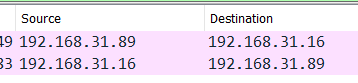


b. Using tcpdump, get the information about the general incoming network traffic with ip address on specific interface.

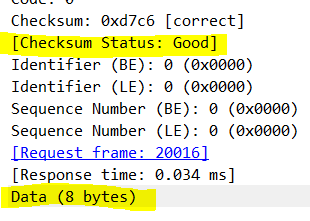
7. Use Wireshark (Latest version) to solve the below scenarios:



b. Find the source and destination IP of that log.



c. Find the Data length (Bytes) and verify the checksum status on destination.



2. Now you have found that some kind of file is been downloaded by insider in unencrypted web traffic. Your task is to

1. Find the name and type of file. – NAME = 1.jpg , Type of file = JPEG JFIF



1. Export that file from that web traffic, then analyze the file for any secret information.



1. c. Find the hostname in which the file is stored. – 192.168.31.113



3. Based upon their activities, auditing team has started investigation against them and found that the insider passed some sensitive information via call to someone. The traffic is been captured.

a. Analyze the traffic and find those conversations and extract the sensitive information in it.

Ans - The password is “LIMBO”

b. Find the call-ID when the status of the call is ringing.

