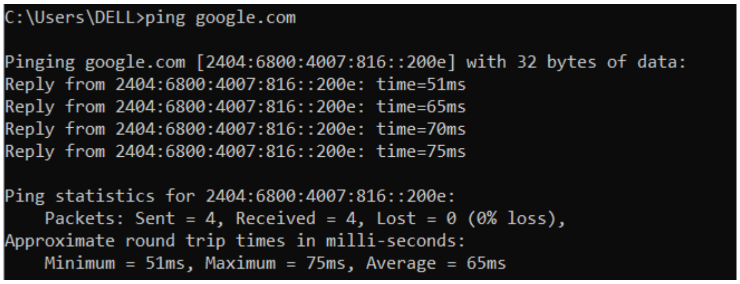
21CY681 - INTERNET PROTOCOL LAB - II

Name: Rahul Raj
Register Number: CB.EN.P2CYS22011
Date: 22th October 2022
Assignment Topic: Understanding network traffic analysis using wireshark

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].

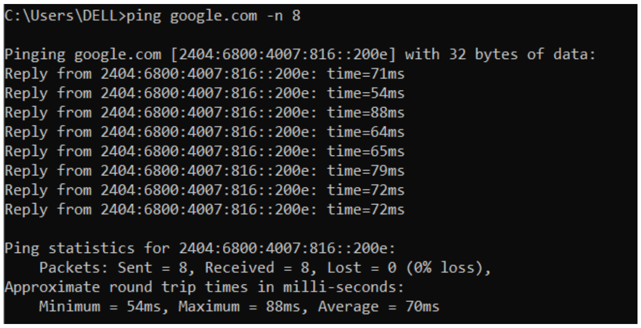


```
C:\Users\DELL>ping google.com

Pinging google.com [2404:6800:4007:816::200e] with 32 bytes of data:
Reply from 2404:6800:4007:816::200e: time=51ms
Reply from 2404:6800:4007:816::200e: time=65ms
Reply from 2404:6800:4007:816::200e: time=70ms
Reply from 2404:6800:4007:816::200e: time=75ms

Ping statistics for 2404:6800:4007:816::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 75ms, Average = 65ms
```

IP address: 2404.6800.4007.816::200e

Round trip time:

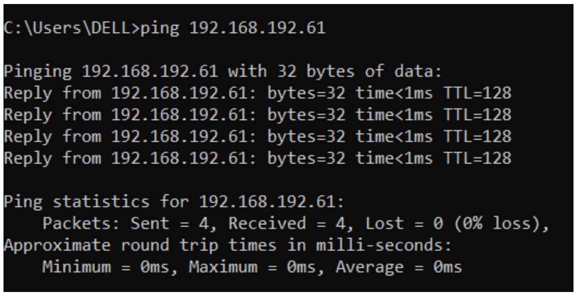
b. By default, ping will send 4 packets to check the details, here you have to send 8 packets to check the output over google.com. Explain what the purpose of this doing is.



```
C:\Users\DELL>ping google.com -n 8

Pinging google.com [2404:6800:4007:816::200e] with 32 bytes of data:
Reply from 2404:6800:4007:816::200e: time=71ms
Reply from 2404:6800:4007:816::200e: time=54ms
Reply from 2404:6800:4007:816::200e: time=88ms
Reply from 2404:6800:4007:816::200e: time=64ms
Reply from 2404:6800:4007:816::200e: time=65ms
Reply from 2404:6800:4007:816::200e: time=79ms
Reply from 2404:6800:4007:816::200e: time=72ms
Reply from 2404:6800:4007:816::200e: time=72ms

Ping statistics for 2404:6800:4007:816::200e:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 88ms, Average = 70ms
```

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.



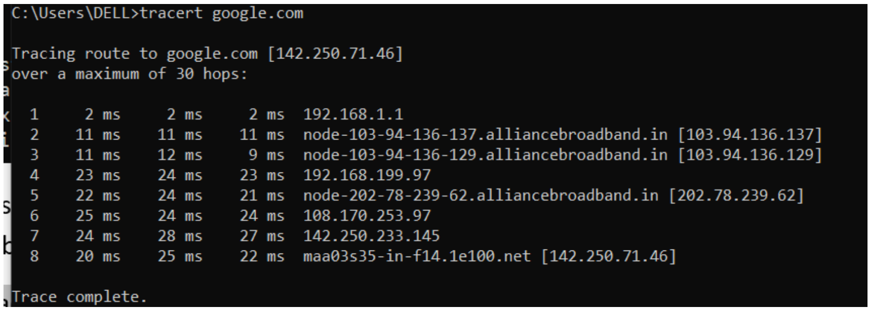
```
C:\Users\DELL>ping 192.168.192.61

Pinging 192.168.192.61 with 32 bytes of data:
Reply from 192.168.192.61: bytes=32 time<1ms TTL=128
Reply from 192.168.192.61: bytes=32 time<1ms TTL=128
Reply from 192.168.192.61: bytes=32 time<1ms TTL=128
Reply from 192.168.192.61: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.192.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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.

- 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)

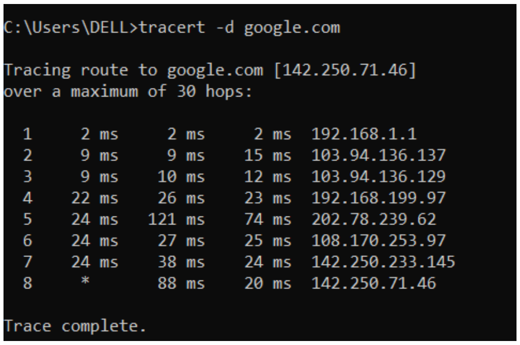
  Answer the following question:

  a. Try tracert over google.com



```
C:\Users\DELL>tracert google.com

Tracing route to google.com [142.250.71.46]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.1.1
  2    11 ms    11 ms    11 ms  node-103-94-136-137.alliancebroadband.in [103.94.136.137]
  3    11 ms    12 ms     9 ms  node-103-94-136-129.alliancebroadband.in [103.94.136.129]
  4    23 ms    24 ms    23 ms  192.168.199.97
  5    22 ms    24 ms    21 ms  node-202-78-239-62.alliancebroadband.in [202.78.239.62]
  6    25 ms    24 ms    24 ms  108.170.253.97
  7    24 ms    28 ms    27 ms  142.250.233.145
  8    20 ms    25 ms    22 ms  maa03s35-in-f14.1e100.net [142.250.71.46]

Trace complete.
```

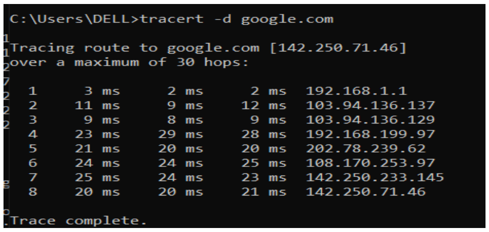
b. Type tracert -d google.com



```
C:\Users\DELL>tracert -d google.com

Tracing route to google.com [142.250.71.46]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.1.1
  2     9 ms     9 ms    15 ms  103.94.136.137
  3     9 ms    10 ms    12 ms  103.94.136.129
  4    22 ms    26 ms    23 ms  192.168.199.97
  5    24 ms   121 ms    74 ms  202.78.239.62
  6    24 ms    27 ms    25 ms  108.170.253.97
  7    24 ms    38 ms    24 ms  142.250.233.145
  8     *       88 ms    20 ms  142.250.71.46

Trace complete.
```

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

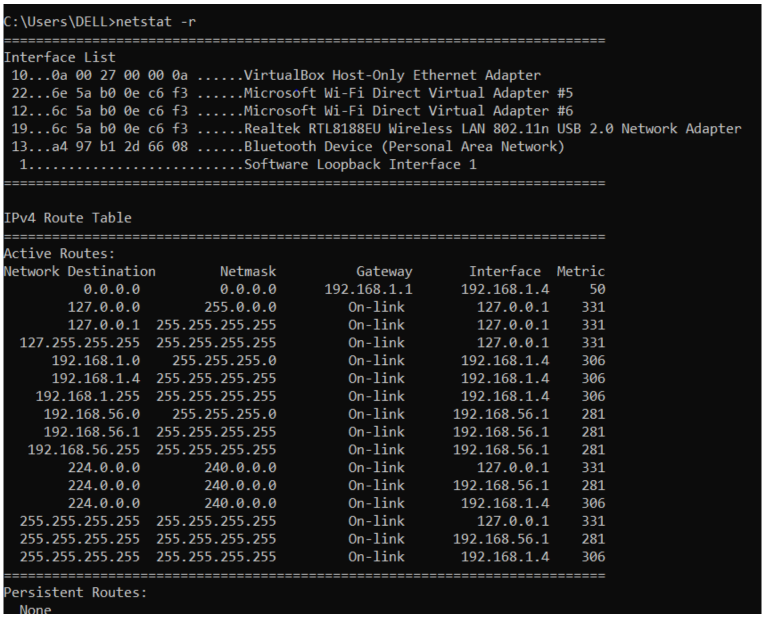
2. Wait for a while and execute the same command again. Is the output the same as the first time? Observe and compare the difference and explain the reason.



```
C:\Users\DELL>tracert -d google.com

Tracing route to google.com [142.250.71.46]
over a maximum of 30 hops:

  1     3 ms     2 ms     2 ms  192.168.1.1
  2    11 ms     9 ms    12 ms  103.94.136.137
  3     9 ms     8 ms     9 ms  103.94.136.129
  4    23 ms    29 ms    28 ms  192.168.199.97
  5    21 ms    20 ms    20 ms  202.78.239.62
  6    24 ms    24 ms    25 ms  108.170.253.97
  7    25 ms    24 ms    23 ms  142.250.233.145
  8    20 ms    20 ms    21 ms  142.250.71.46

Trace complete.
```

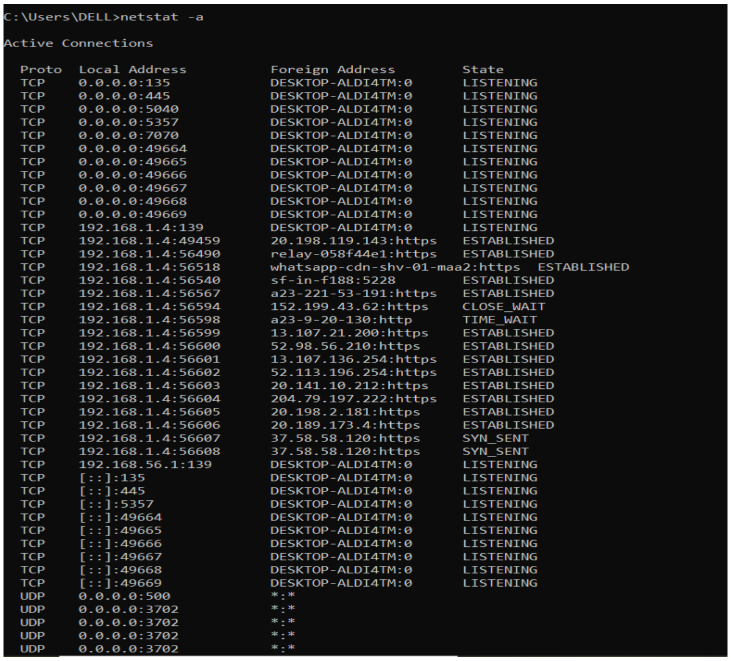
3. You have to read about NETSTAT from the manual page or help before answering the below questions:

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



```
C:\Users\DELL>netstat -r
===========================================================================
Interface List
 10...0a 00 27 00 00 0a ......VirtualBox Host-Only Ethernet Adapter
 22...6e 5a b0 0e c6 f3 ......Microsoft Wi-Fi Direct Virtual Adapter #5
 12...6c 5a b0 0e c6 f3 ......Microsoft Wi-Fi Direct Virtual Adapter #6
 19...6c 5a b0 0e c6 f3 ......Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
 13...a4 97 b1 2d 66 08 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.4     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link       192.168.1.4    306
      192.168.1.4  255.255.255.255         On-link       192.168.1.4    306
    192.168.1.255  255.255.255.255         On-link       192.168.1.4    306
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link       192.168.1.4    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link       192.168.1.4    306
===========================================================================
Persistent Routes:
  None
```

b. Use netstat to display about ethernet statistics.



```
C:\Users\DELL>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:7070           DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-ALDI4TM:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-ALDI4TM:0      LISTENING
  TCP    192.168.1.4:139        DESKTOP-ALDI4TM:0      LISTENING
  TCP    192.168.1.4:49459      20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.4:56490      relay-058f44e1:https   ESTABLISHED
  TCP    192.168.1.4:56518      whatsapp-cdn-shv-01-maa2:https  ESTABLISHED
  TCP    192.168.1.4:56540      sf-in-f188:5228        ESTABLISHED
  TCP    192.168.1.4:56567      a23-221-53-191:https   ESTABLISHED
  TCP    192.168.1.4:56594      152.199.43.62:https    CLOSE_WAIT
  TCP    192.168.1.4:56598      a23-9-20-130:http      TIME_WAIT
  TCP    192.168.1.4:56599      13.107.21.200:https    ESTABLISHED
  TCP    192.168.1.4:56600      52.98.56.210:https     ESTABLISHED
  TCP    192.168.1.4:56601      13.107.136.254:https   ESTABLISHED
  TCP    192.168.1.4:56602      52.113.196.254:https   ESTABLISHED
  TCP    192.168.1.4:56603      20.141.10.212:https    ESTABLISHED
  TCP    192.168.1.4:56604      204.79.197.222:https   ESTABLISHED
  TCP    192.168.1.4:56605      20.198.2.181:https     ESTABLISHED
  TCP    192.168.1.4:56606      20.189.173.4:https     ESTABLISHED
  TCP    192.168.1.4:56607      37.58.58.120:https     SYN_SENT
  TCP    192.168.1.4:56608      37.58.58.120:https     SYN_SENT
  TCP    192.168.56.1:139       DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:135               DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:445               DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:5357              DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:49664             DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:49665             DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:49666             DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:49667             DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:49668             DESKTOP-ALDI4TM:0      LISTENING
  TCP    [::]:49669             DESKTOP-ALDI4TM:0      LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
```

4. What is the purpose of NSLOOKUP ?

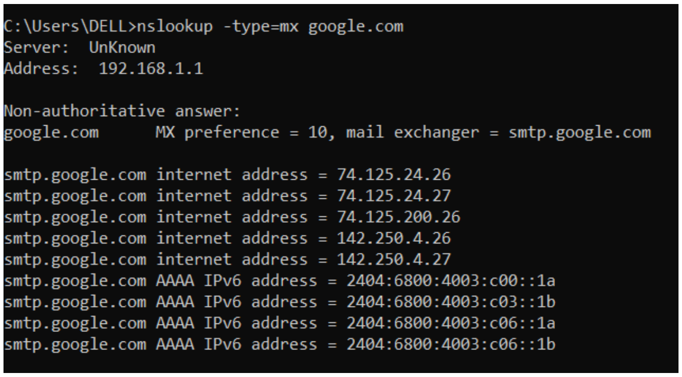
It is a command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System to obtain domain name or IP address mapping or any other specific DNS record.

Answer the following questions below:

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

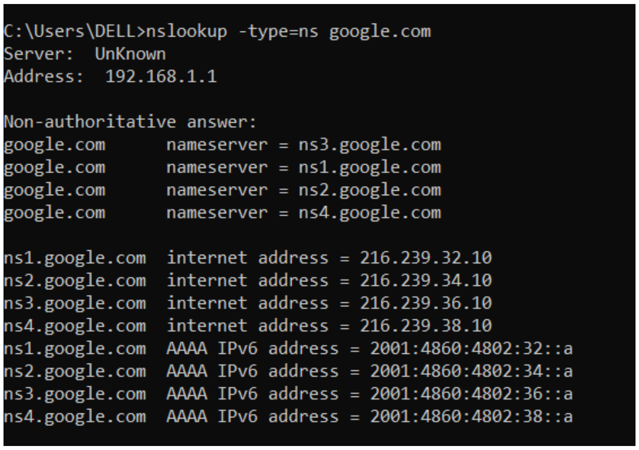
ANS - 3.33.154.67 and 15.197.141.123

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



```
C:\Users\DELL>nslookup -type=mx google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com

smtp.google.com internet address = 74.125.24.26
smtp.google.com internet address = 74.125.24.27
smtp.google.com internet address = 74.125.200.26
smtp.google.com internet address = 142.250.4.26
smtp.google.com internet address = 142.250.4.27
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c00::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c03::1b
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c06::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c06::1b
```

c. What is the name server for amrita.edu



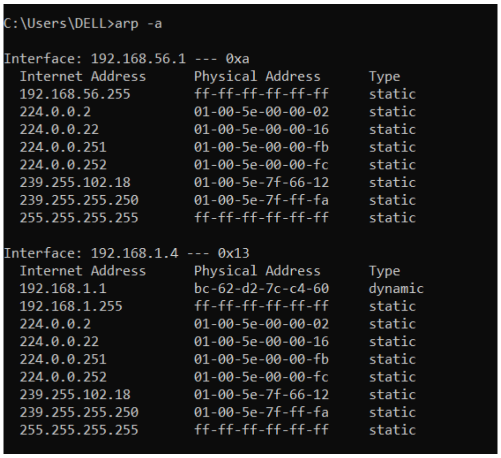
```
C:\Users\DELL>nslookup -type=ns google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
google.com      nameserver = ns3.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns4.google.com

ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
```

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.



```
C:\Users\DELL>arp -a

Interface: 192.168.56.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.1.4 --- 0x13
  Internet Address      Physical Address      Type
  192.168.1.1           bc-62-d2-7c-c4-60     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

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?

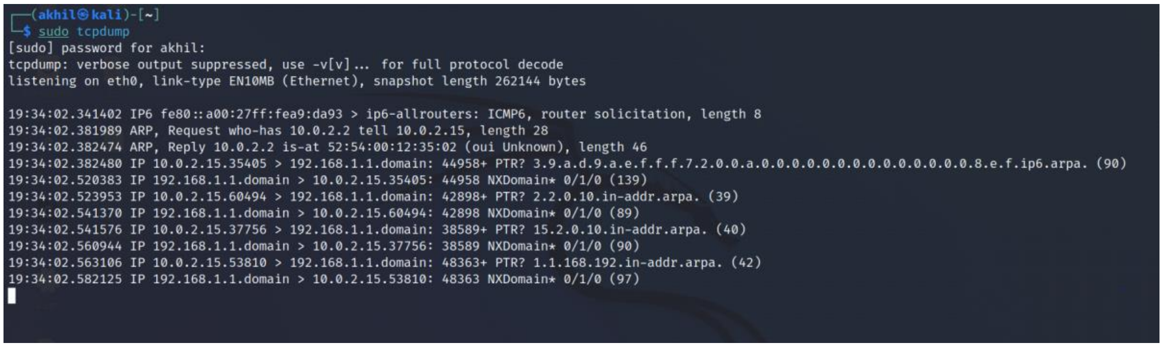
To add an arp entry we need to use –s flag along with IP address and MAC address.

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)

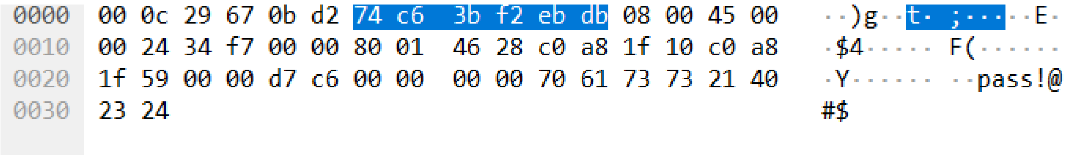
a. Using tcpdump, get the information about the general incoming network traffic with names.



```
┌──(akhil㉿kali)-[~]
└─$ sudo tcpdump
[sudo] password for akhil:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

19:34:02.341402 IP6 fe80::a00:27ff:fea9:da93 > ip6-allrouters: ICMP6, router solicitation, length 8
19:34:02.381989 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
19:34:02.382474 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02 (oui Unknown), length 46
19:34:02.382480 IP 10.0.2.15.35405 > 192.168.1.1.domain: 44958+ PTR? 3.9.a.d.9.a.e.f.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
19:34:02.520383 IP 192.168.1.1.domain > 10.0.2.15.35405: 44958 NXDomain* 0/1/0 (139)
19:34:02.523953 IP 10.0.2.15.60494 > 192.168.1.1.domain: 42898+ PTR? 2.2.0.10.in-addr.arpa. (39)
19:34:02.541370 IP 192.168.1.1.domain > 10.0.2.15.60494: 42898 NXDomain* 0/1/0 (89)
19:34:02.541576 IP 10.0.2.15.37756 > 192.168.1.1.domain: 38589+ PTR? 15.2.0.10.in-addr.arpa. (40)
19:34:02.560944 IP 192.168.1.1.domain > 10.0.2.15.37756: 38589 NXDomain* 0/1/0 (90)
19:34:02.563106 IP 10.0.2.15.53810 > 192.168.1.1.domain: 48363+ PTR? 1.1.168.192.in-addr.arpa. (42)
19:34:02.582125 IP 192.168.1.1.domain > 10.0.2.15.53810: 48363 NXDomain* 0/1/0 (97)
█
```

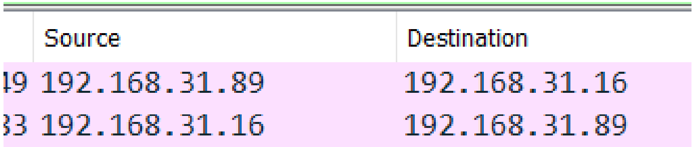
b. Using tcpdump, get the information about the general incoming network traffic with ip address on specific interface.

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



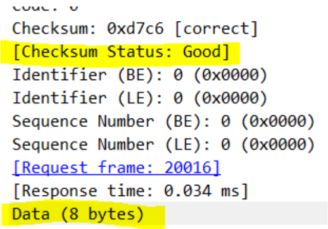
```
0000   00 0c 29 67 0b d2 74 c6  3b f2 eb db 08 00 45 00    ··)g··t· ;·····E·
0010   00 24 34 f7 00 00 80 01  46 28 c0 a8 1f 10 c0 a8    ·$4·····  F(······
0020   1f 59 00 00 d7 c6 00 00  00 00 70 61 73 73 21 40    ·Y······  ··pass!@
0030   23 24                                               #$
```

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



	Source	Destination
19	192.168.31.89	192.168.31.16
33	192.168.31.16	192.168.31.89

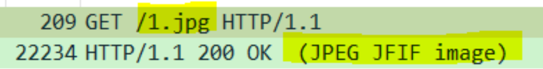
c. Find the Data length (Bytes) and verify the checksum status on destination.



```
Code: 0
Checksum: 0xd7c6 [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 20016]
[Response time: 0.034 ms]
Data (8 bytes)
```

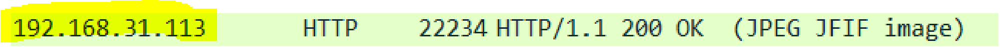
2. Now you have found that some kind of file is been downloaded by insider in unencrypted web traffic. Your task is to

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



```
  209 GET /1.jpg HTTP/1.1
22234 HTTP/1.1 200 OK  (JPEG JFIF image)
```

- Export that file from that web traffic, then analyze the file for any secret information.
- c. Find the hostname in which the file is stored. – 192.168.31.113



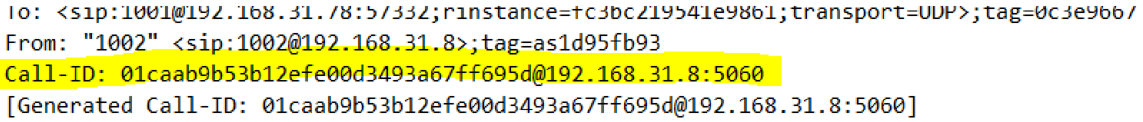
```
192.168.31.113        HTTP     22234 HTTP/1.1 200 OK  (JPEG JFIF image)
```

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.



```
To: <sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP>;tag=0c3e9667
From: "1002" <sip:1002@192.168.31.8>;tag=as1d95fb93
Call-ID: 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060
[Generated Call-ID: 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060]
```