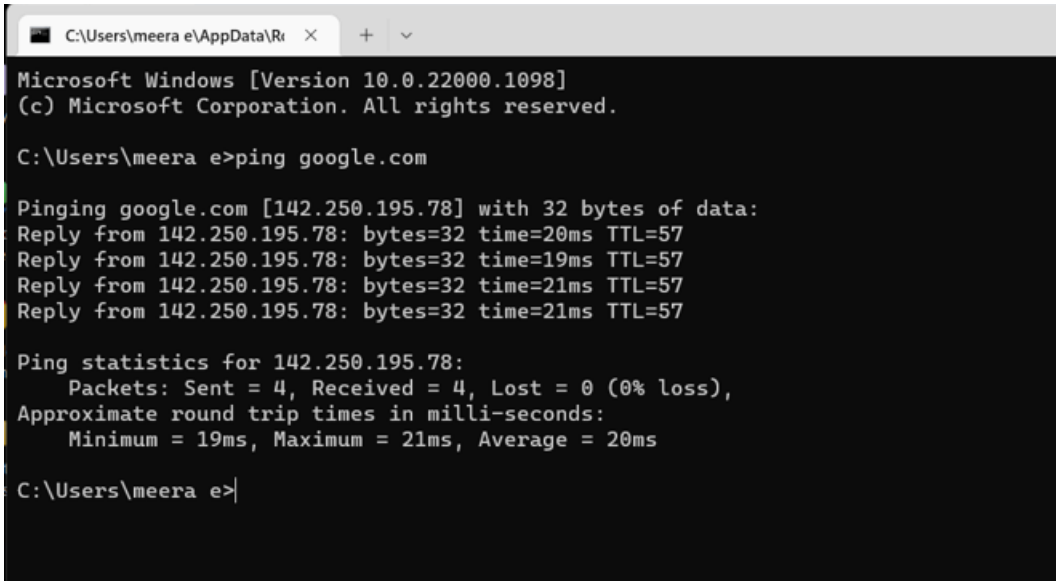
CYS 681 IP Lab Assignment -II

Name : Meera E Thimothy Date: 22nd October 2022

Roll no: CB.EN.P2CYS22002

1. Understand PING and document it, then answer the following question:

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].

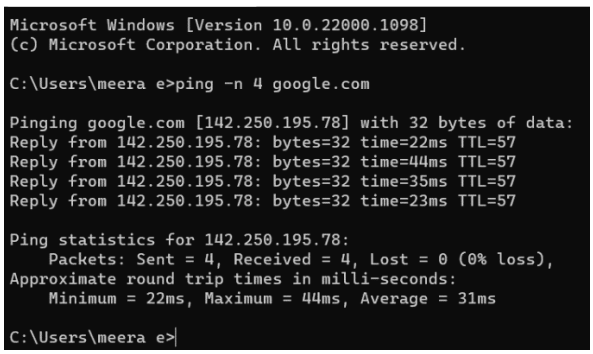


IP Address - 142.250.195.78

TTL - 57 ms

Round trip time – 20 msb.

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.



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.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\meera e> ping localhost

Pinging LAPTOP-QA1841BC [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\meera e>
```

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.

2. 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

```
PS C:\Users\meera e> tracert google.com

Tracing route to google.com [142.250.195.78]
over a maximum of 30 hops:

  1     6 ms     2 ms     1 ms  192.168.1.1
  2     6 ms     4 ms     3 ms  172.16.231.1
  3    97 ms    14 ms     5 ms  81.227.88.202.asianet.co.in [202.88.227.81]
  4     6 ms     4 ms     4 ms  45.243.88.202.asianet.co.in [202.88.243.45]
  5     *        7 ms     *     57.243.88.202.asianet.co.in [202.88.243.57]
  6    21 ms    21 ms    24 ms  130.230.88.202.asianet.co.in [202.88.230.130]
  7    20 ms    20 ms    23 ms  21.252.88.202.asianet.co.in [202.88.252.21]
  8    25 ms    22 ms    22 ms  216.239.43.133
  9    21 ms    22 ms    22 ms  142.251.55.75
 10    21 ms    21 ms    20 ms  maa03s38-in-f14.1e100.net [142.250.195.78]

Trace complete.
```

b. Type tracert -d google.com

```
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\meera e>tracert d google.com
Unable to resolve target system name d.

C:\Users\meera e>tracert -d google.com

Tracing route to google.com [142.250.195.78]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2    29 ms     4 ms     4 ms  172.16.231.1
  3     7 ms     5 ms     6 ms  202.88.227.81
  4     7 ms     4 ms     4 ms  202.88.243.45
  5     *        *        *     Request timed out.
  6  1561 ms    53 ms     *     202.88.230.130
  7     *       21 ms    31 ms  202.88.252.21
  8   171 ms    29 ms    22 ms  216.239.43.133
  9   190 ms     *      426 ms  142.251.55.75
 10    20 ms    21 ms    89 ms  142.250.195.78

Trace complete.
```

i) How many hops is your machine away from google.com? - 10 Hops

ii) 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.

```
PS C:\Users\meera e> tracert -d google.com

Tracing route to google.com [142.250.195.78]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     4 ms     3 ms     4 ms  172.16.231.1
  3     5 ms     4 ms     5 ms  202.88.227.81
  4     4 ms     5 ms     7 ms  202.88.243.45
  5     *        4 ms     *     202.88.243.57
  6    21 ms    22 ms    20 ms  202.88.230.130
  7    23 ms    22 ms    22 ms  202.88.252.21
  8   146 ms    30 ms   167 ms  216.239.43.133
  9     *       22 ms    21 ms  142.251.55.75
 10    21 ms    21 ms    22 ms  142.250.195.78

Trace complete.
```

In networking, there are several routes to reach the destination router. So each time when we run tracert command with google, it gives us different path i.e no. of hops is different.

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.

```
PS C:\Users\meera e> netstat -r
===========================================================================
Interface List
 21...a8 b1 3b 13 e0 75 ......Realtek Gaming GbE Family Controller
 19...00 ff c6 1d e6 c3 ......ExpressVPN TAP Adapter
 17.........................ExpressVPN Wintun Driver
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter
  3...52 c2 e8 4a b1 21 ......Microsoft Wi-Fi Direct Virtual Adapter
 10...d2 c2 e8 4a b1 21 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 15...50 c2 e8 4a b1 21 ......Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
  1...........................Software Loopback Interface 1
 60...00 15 5d 85 87 51 ......Hyper-V Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.8     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
      172.29.16.0    255.255.240.0         On-link       172.29.16.1   5256
      172.29.16.1  255.255.255.255         On-link       172.29.16.1   5256
    172.29.31.255  255.255.255.255         On-link       172.29.16.1   5256
      192.168.1.0    255.255.255.0         On-link       192.168.1.8    306
      192.168.1.8  255.255.255.255         On-link       192.168.1.8    306
    192.168.1.255  255.255.255.255         On-link       192.168.1.8    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
```

b. Use netstat to display about ethernet statistics.

```
PS C:\Users\meera e> netstat -e
Interface Statistics

                           Received            Sent

Bytes                     101291832        15588734
Unicast packets              242408           93808
Non-unicast packets           24848           27668
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
PS C:\Users\meera e>
```

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.

```
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\meera e>nslookup amrita.edu
Server:  UnKnown
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    amrita.edu
Addresses:  3.33.154.67
          15.197.141.123
```

ANS - 3.33.154.67 and 15.197.141.123

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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\meera e> 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
PS C:\Users\meera e>
```

ANS - smtp.google.com

c. What is the name server for amrita.edu

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\meera e> nslookup -type=ns google.com
Server:  UnKnown
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns3.google.com
PS C:\Users\meera e>
```

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 a computer from server**.**

Answer the following questions below: (3 marks)

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

```
PS C:\Users\meera e> arp -a

Interface: 192.168.56.1 --- 0xc
  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
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.3.22          01-00-5e-7f-03-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.1.8 --- 0xf
  Internet Address      Physical Address      Type
  192.168.1.1           bc-62-d2-24-85-60     dynamic
  192.168.1.2           2c-e0-32-a6-7e-37     dynamic
  192.168.1.3           60-02-b4-eb-ae-54     dynamic
  192.168.1.4           c2-14-dc-4a-c3-7a     dynamic
  192.168.1.6           14-c1-4e-1a-a6-bd     dynamic
  192.168.1.7           f0-a3-b2-40-4b-29     dynamic
  192.168.1.9           ea-74-59-5d-db-57     dynamic
  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
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

The gateway address is 192.168.56.1 & the hardware address of the host systems are 192.168.56.2, 192.168.56.3, 192.168.56.4, 192.168.56.5, 192.168.56.6, 192.168.56.7, 192.168.56.9.

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.

Ex - 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.

```
sh3bu@shebu:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:26:25.325332 IP shebu.mshome.net.54298 > 239.255.255.250.1900: UDP, length 175
22:26:25.381105 IP 172.17.219.180.42213 > shebu.mshome.net.domain: 47834+ PTR? 250.255.255.239.i
22:26:25.389984 IP shebu.mshome.net.54303 > 239.255.255.250.1900: UDP, length 175
22:26:25.392448 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr
22:26:25.393672 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local.
22:26:25.470137 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr
22:26:25.474530 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local.
22:26:26.325771 IP shebu.mshome.net.54298 > 239.255.255.250.1900: UDP, length 175
22:26:26.379917 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr
22:26:26.383321 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local.
22:26:26.394464 IP shebu.mshome.net.54303 > 239.255.255.250.1900: UDP, length 175
22:26:26.457120 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr
22:26:26.458050 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local.
22:26:27.326640 IP shebu.mshome.net.54298 > 239.255.255.250.1900: UDP, length 175
22:26:27.398416 IP shebu.mshome.net.54303 > 239.255.255.250.1900: UDP, length 175
22:26:28.332455 IP shebu.mshome.net.54298 > 239.255.255.250.1900: UDP, length 175
22:26:28.402566 IP shebu.mshome.net.54303 > 239.255.255.250.1900: UDP, length 175
```

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

```
meera@meera:~$ tcpdump - i enp0s3
tcpdump: enp0s3: You don't have permission to capture on that device
(socket: Operation not permitted)
meera@meera:~$
```

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

1. You, as a SOC analyst noted that someone try to send information (PING) to unknown IP address and you are suspecting some malicious information might transferred in it. Analyze the log file.

a. Find the data transferred. – The data that is transferred in the packet is “pass!@#$”

```
3b f2 eb db 08 00 45 00   ··)g··t· ;·····E·
46 28 c0 a8 1f 10 c0 a8   ·$4····· F(······
00 00 70 61 73 73 21 40   ·Y····· ··pass!@
                          #$
```

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

```
Source Address: 192.168.31.89
Destination Address: 192.168.31.16
```

Source IP = 192.168.31.89, Destination IP = 192.168.31.16

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

```
Internet Protocol Version 4, Src: 192.168.31.89, Dst: 192.168.31.16
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 36
   Identification: 0x0001 (1)
 > 000. .... = Flags: 0x0
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 64
   Protocol: ICMP (1)
   Header Checksum: 0xbb1e [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.31.89
   Destination Address: 192.168.31.16
```

ANS - The data length is 36 bytes and the header checksum status is unverified

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

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

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

b. 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

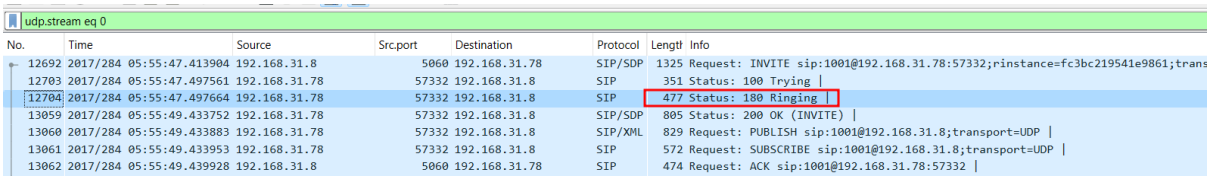
```
Destination      Protocol  Length  Info
192.168.31.67    HTTP       209 GET /1.jpg HTTP/1.1
192.168.31.113   HTTP     22234 HTTP/1.1 200 OK  (JPEG JFIF image)
```

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.



```
INVITE sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.31.8:5060;branch=z9hG4bK30e63862
Max-Forwards: 70
From: "1002" <sip:1002@192.168.31.8>;tag=as1d95fb93
To: <sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP>
Contact: <sip:1002@192.168.31.8:5060>
Call-ID: 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060
CSeq: 102 INVITE
User-Agent: FPBX-2.11.0(11.13.0)
Date: Tue, 10 Oct 2017 16:25:46 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH,
```

CALLER-ID = 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060