21CY681– Internet Protocol lab

ASSIGNMENT -2

Name: B.Shebu

Register Number : CYS22005

Title: Analyzing HTTP requests and responses using wireshark

Date of Assignment provided: 9/10/2022

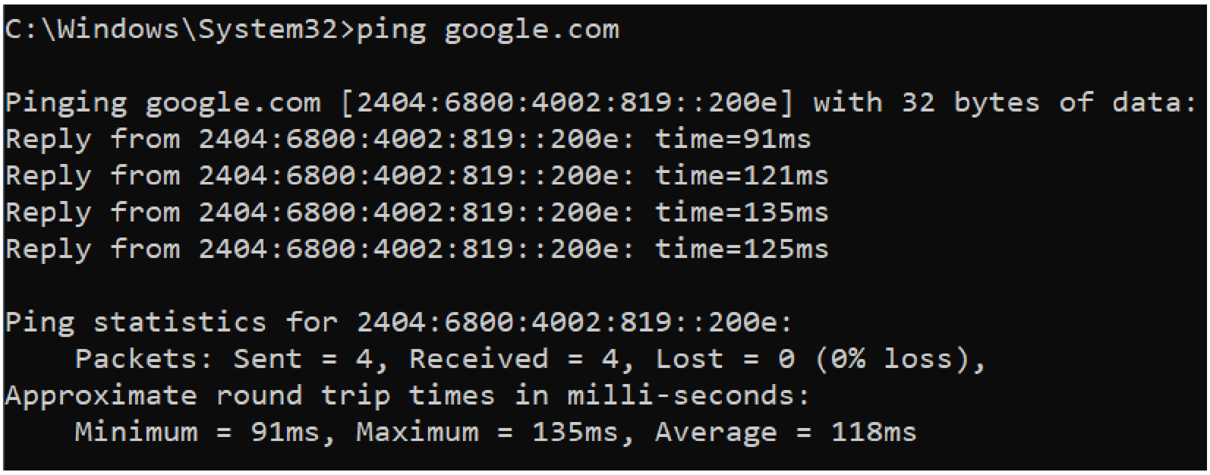
Aim: Understanding Network traffic analysis using wireshark

PROCEDURE -

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

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a ICMP echo packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency.

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].



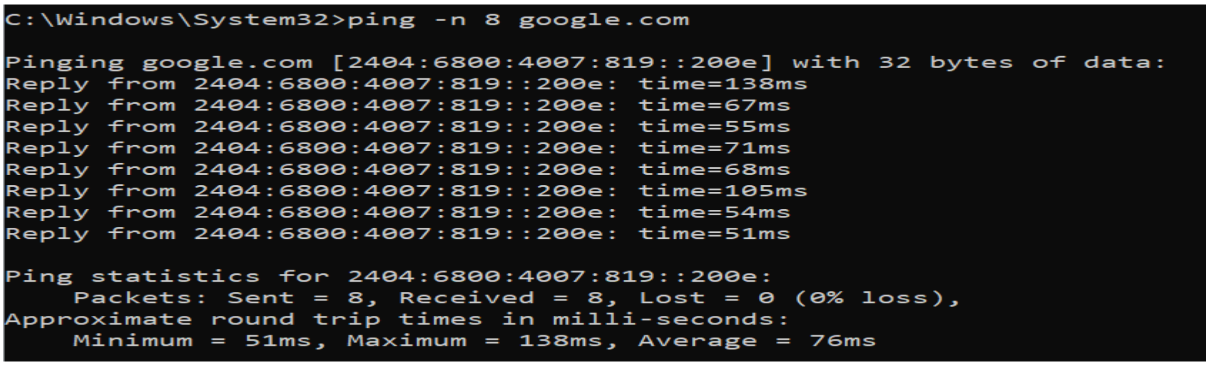
```
C:\Windows\System32>ping google.com

Pinging google.com [2404:6800:4002:819::200e] with 32 bytes of data:
Reply from 2404:6800:4002:819::200e: time=91ms
Reply from 2404:6800:4002:819::200e: time=121ms
Reply from 2404:6800:4002:819::200e: time=135ms
Reply from 2404:6800:4002:819::200e: time=125ms

Ping statistics for 2404:6800:4002:819::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 91ms, Maximum = 135ms, Average = 118ms
```

IP Address - 2404:6800:4002:819::200e

TTL - 121 ms

Round trip time – 118 ms

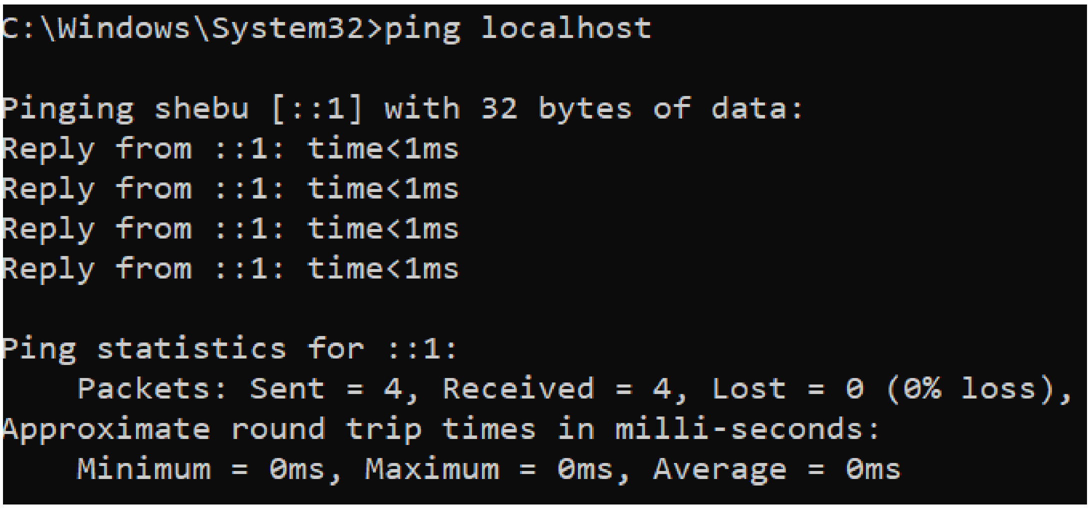
b. By default, ping will send 4 packets to check the details, here you have to send 8 packets to check the output over google.com. Explain what the purpose of this doing is.



```
C:\Windows\System32>ping -n 8 google.com

Pinging google.com [2404:6800:4007:819::200e] with 32 bytes of data:
Reply from 2404:6800:4007:819::200e: time=138ms
Reply from 2404:6800:4007:819::200e: time=67ms
Reply from 2404:6800:4007:819::200e: time=55ms
Reply from 2404:6800:4007:819::200e: time=71ms
Reply from 2404:6800:4007:819::200e: time=68ms
Reply from 2404:6800:4007:819::200e: time=105ms
Reply from 2404:6800:4007:819::200e: time=54ms
Reply from 2404:6800:4007:819::200e: time=51ms

Ping statistics for 2404:6800:4007:819::200e:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 138ms, Average = 76ms
```

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:\Windows\System32>ping localhost

Pinging shebu [::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
```

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.

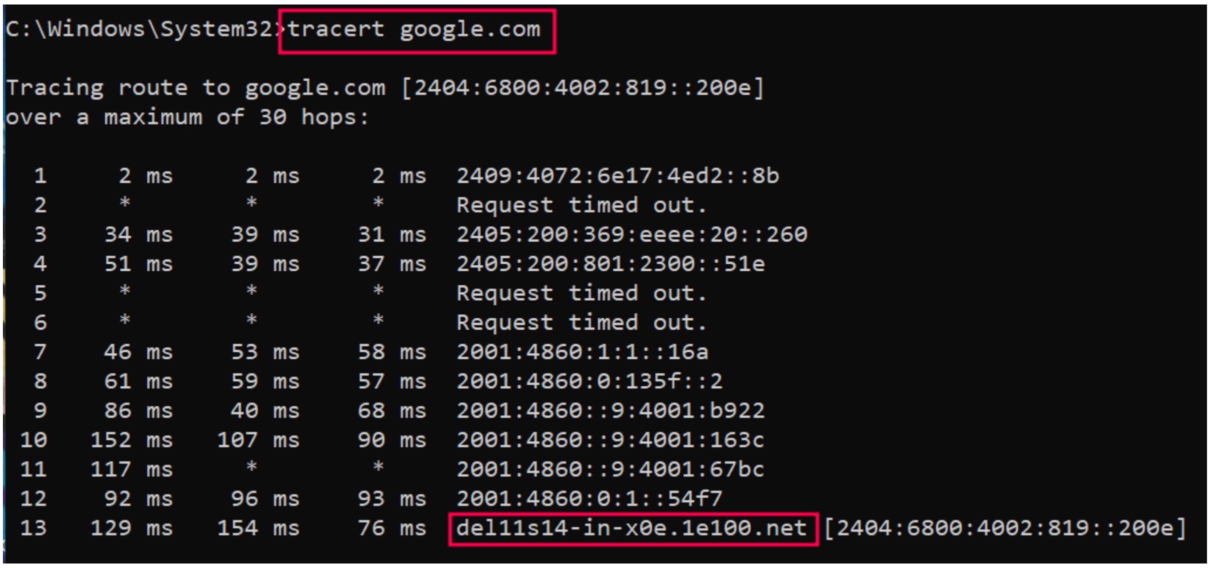
2. Read the Unix manual page for traceroute OR help for tracert. Experiment with the various options. Describe the three things that you found most useful in the result. (2 marks)

- Tracert command helps us to trace the path through which our packet is sent

- It helps us to know how many hops the packet took to reach the destination

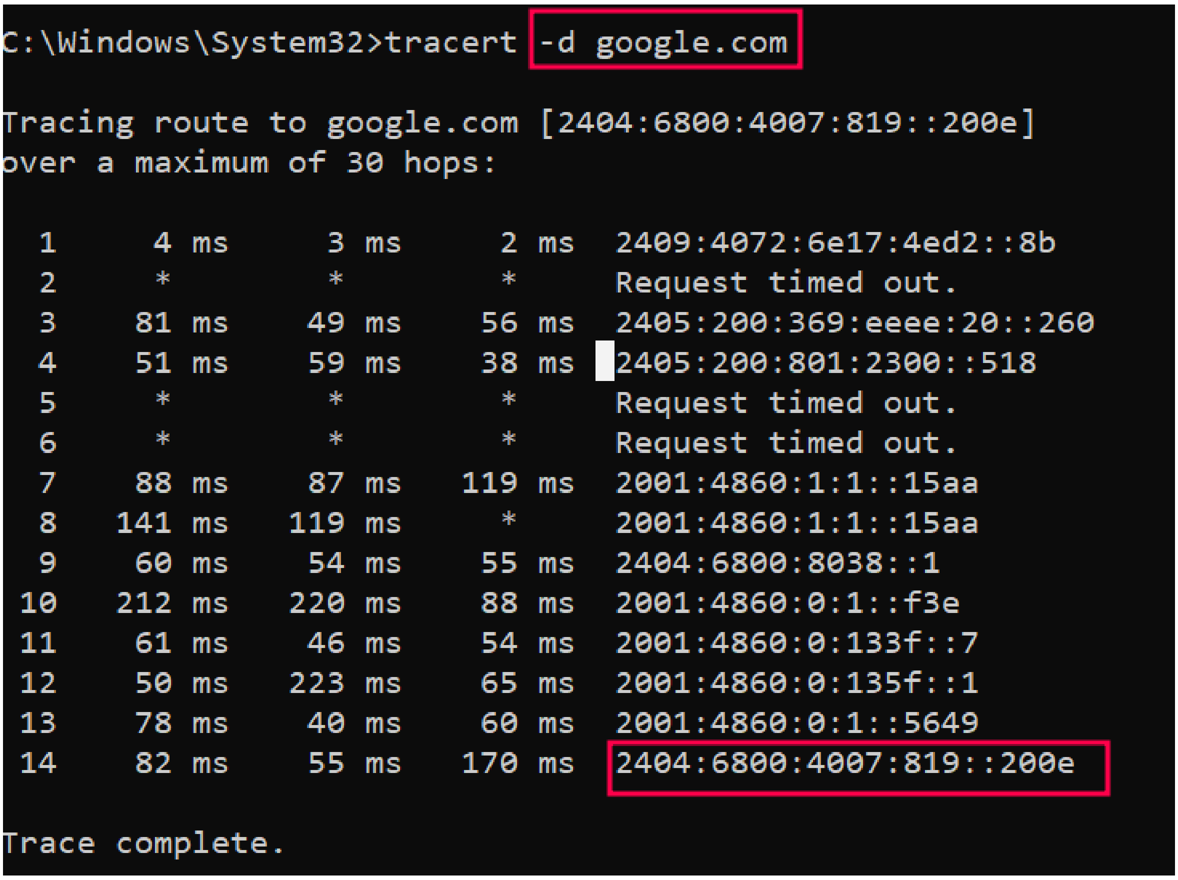
Answer the following question:

a. Try tracert over google.com



```
C:\Windows\System32>tracert google.com

Tracing route to google.com [2404:6800:4002:819::200e]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  2409:4072:6e17:4ed2::8b
  2     *        *        *     Request timed out.
  3    34 ms    39 ms    31 ms  2405:200:369:eeee:20::260
  4    51 ms    39 ms    37 ms  2405:200:801:2300::51e
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    46 ms    53 ms    58 ms  2001:4860:1:1::16a
  8    61 ms    59 ms    57 ms  2001:4860:0:135f::2
  9    86 ms    40 ms    68 ms  2001:4860::9:4001:b922
 10   152 ms   107 ms    90 ms  2001:4860::9:4001:163c
 11   117 ms     *        *     2001:4860::9:4001:67bc
 12    92 ms    96 ms    93 ms  2001:4860:0:1::54f7
 13   129 ms   154 ms    76 ms  del11s14-in-x0e.1e100.net [2404:6800:4002:819::200e]
```

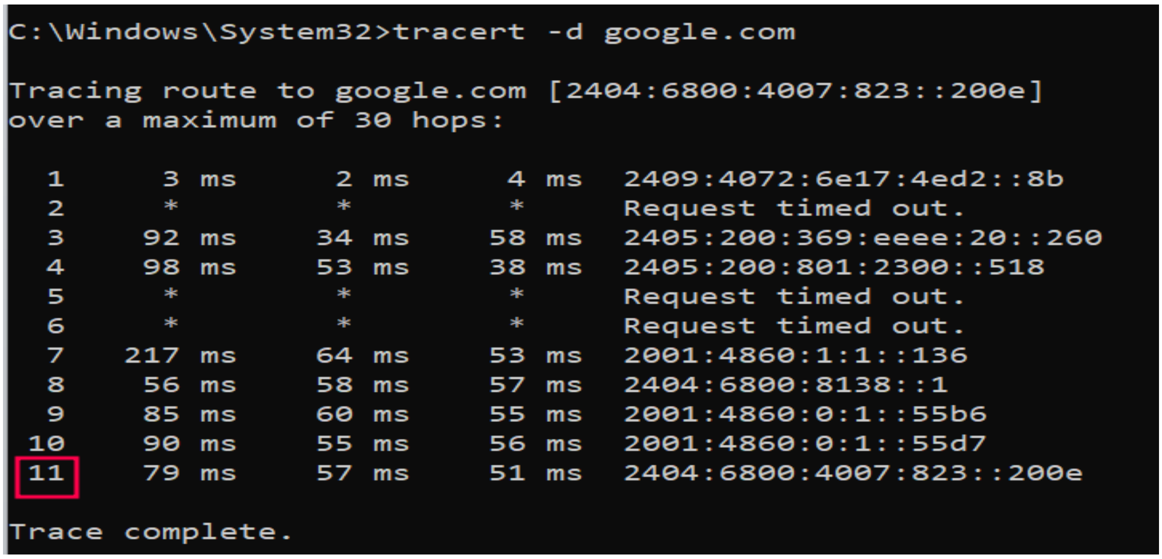
b. Type tracert -d google.com



```
C:\Windows\System32>tracert -d google.com

Tracing route to google.com [2404:6800:4007:819::200e]
over a maximum of 30 hops:

  1     4 ms     3 ms     2 ms  2409:4072:6e17:4ed2::8b
  2     *        *        *     Request timed out.
  3    81 ms    49 ms    56 ms  2405:200:369:eeee:20::260
  4    51 ms    59 ms    38 ms  2405:200:801:2300::518
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    88 ms    87 ms   119 ms  2001:4860:1:1::15aa
  8   141 ms   119 ms     *     2001:4860:1:1::15aa
  9    60 ms    54 ms    55 ms  2404:6800:8038::1
 10   212 ms   220 ms    88 ms  2001:4860:0:1::f3e
 11    61 ms    46 ms    54 ms  2001:4860:0:133f::7
 12    50 ms   223 ms    65 ms  2001:4860:0:135f::1
 13    78 ms    40 ms    60 ms  2001:4860:0:1::5649
 14    82 ms    55 ms   170 ms  2404:6800:4007:819::200e

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.

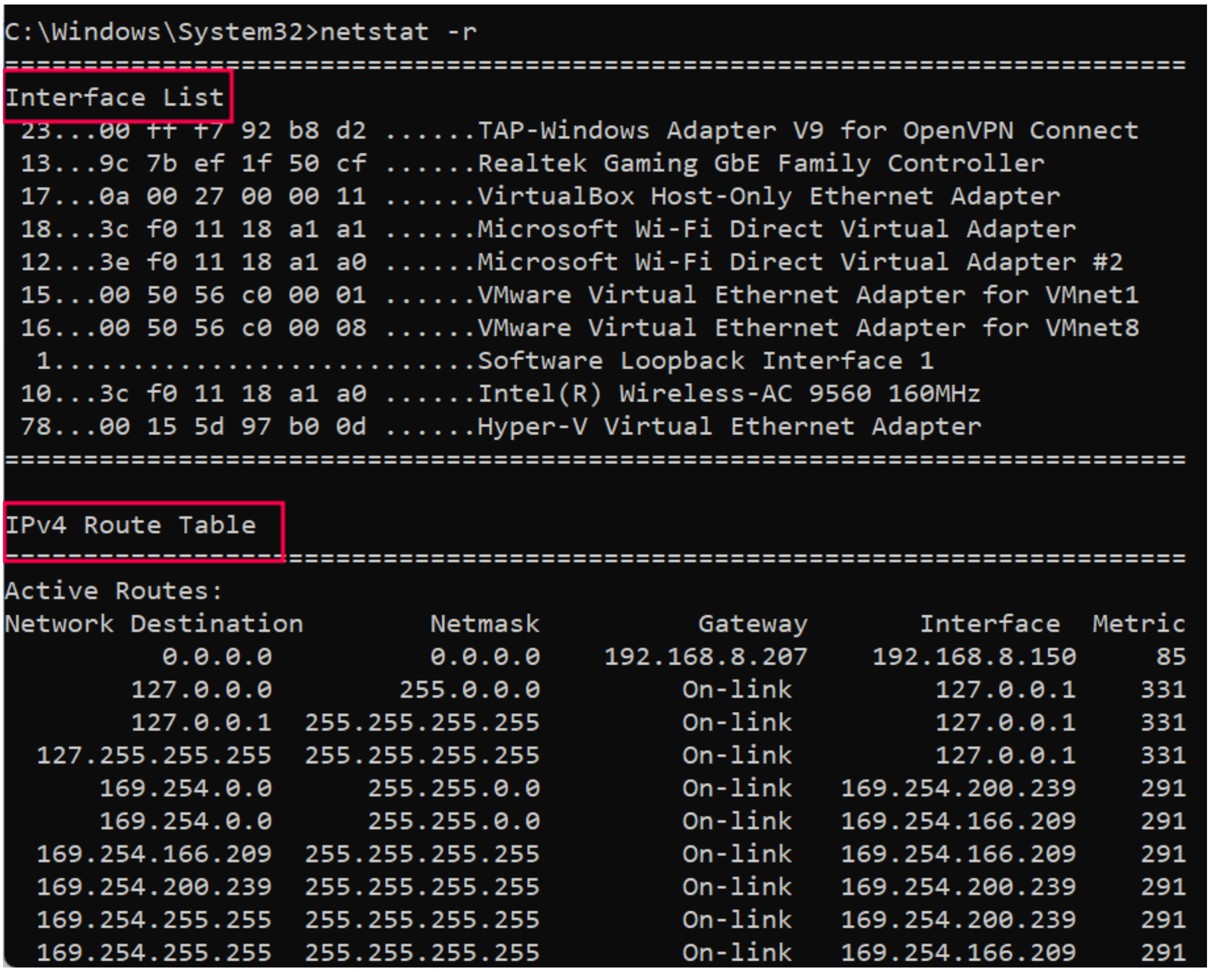


```
C:\Windows\System32>tracert -d google.com

Tracing route to google.com [2404:6800:4007:823::200e]
over a maximum of 30 hops:

  1     3 ms     2 ms     4 ms  2409:4072:6e17:4ed2::8b
  2     *        *        *     Request timed out.
  3    92 ms    34 ms    58 ms  2405:200:369:eeee:20::260
  4    98 ms    53 ms    38 ms  2405:200:801:2300::518
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7   217 ms    64 ms    53 ms  2001:4860:1:1::136
  8    56 ms    58 ms    57 ms  2404:6800:8138::1
  9    85 ms    60 ms    55 ms  2001:4860:0:1::55b6
 10    90 ms    55 ms    56 ms  2001:4860:0:1::55d7
 11    79 ms    57 ms    51 ms  2404:6800:4007:823::200e

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 ie. No of hops is different .

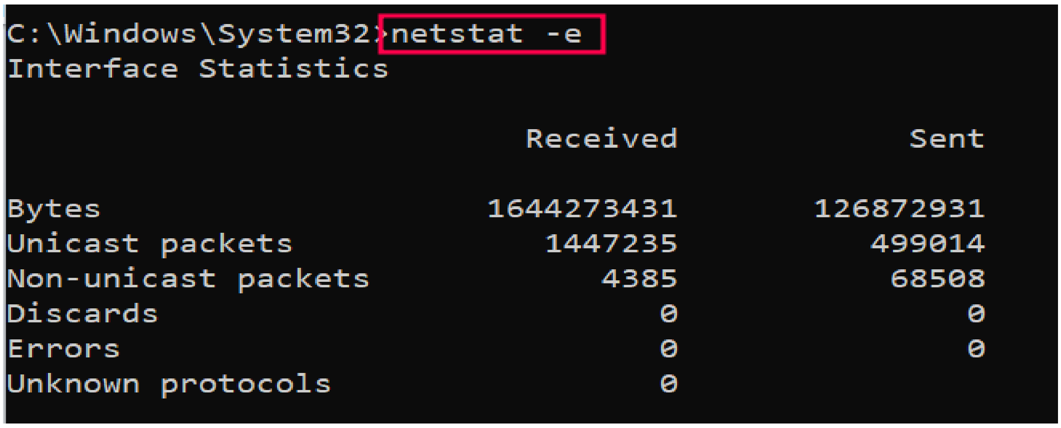
3. You have to read about NETSTAT from the manual page or help before answering the below questions:

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



```
C:\Windows\System32>netstat -r
===========================================================================
Interface List
 23...00 ff f7 92 b8 d2 ......TAP-Windows Adapter V9 for OpenVPN Connect
 13...9c 7b ef 1f 50 cf ......Realtek Gaming GbE Family Controller
 17...0a 00 27 00 00 11 ......VirtualBox Host-Only Ethernet Adapter
 18...3c f0 11 18 a1 a1 ......Microsoft Wi-Fi Direct Virtual Adapter
 12...3e f0 11 18 a1 a0 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 15...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 16...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
 10...3c f0 11 18 a1 a0 ......Intel(R) Wireless-AC 9560 160MHz
 78...00 15 5d 97 b0 0d ......Hyper-V Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.8.207    192.168.8.150     85
        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
      169.254.0.0      255.255.0.0         On-link   169.254.200.239    291
      169.254.0.0      255.255.0.0         On-link   169.254.166.209    291
  169.254.166.209  255.255.255.255         On-link   169.254.166.209    291
  169.254.200.239  255.255.255.255         On-link   169.254.200.239    291
  169.254.255.255  255.255.255.255         On-link   169.254.200.239    291
  169.254.255.255  255.255.255.255         On-link   169.254.166.209    291
```

b. Use netstat to display about ethernet statistics.



```
C:\Windows\System32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    1644273431       126872931
Unicast packets             1447235          499014
Non-unicast packets            4385           68508
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

4. What is the purpose of NSLOOKUP ?

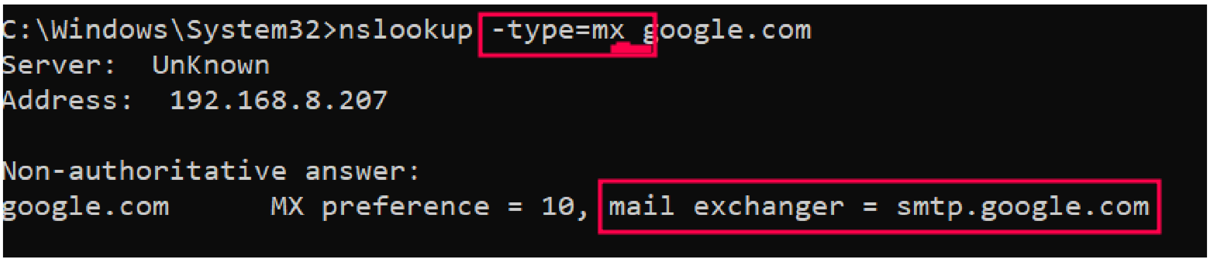
It is a command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System to obtain domain name or IP address mapping or any other specific DNS record.

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

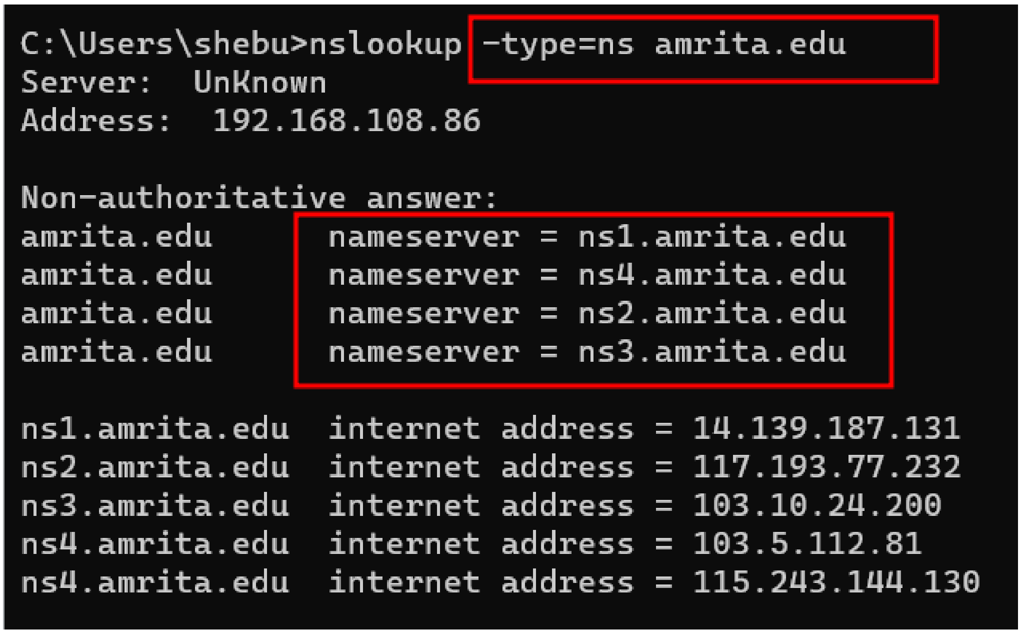
b. What is the mail exchanger for the domain google.com.



```
C:\Windows\System32>nslookup -type=mx google.com
Server:  UnKnown
Address:  192.168.8.207

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

ANS - smtp.google.com

c. What is the name server for amrita.edu



```
C:\Users\shebu>nslookup -type=ns amrita.edu
Server:  UnKnown
Address:  192.168.108.86

Non-authoritative answer:
amrita.edu      nameserver = ns1.amrita.edu
amrita.edu      nameserver = ns4.amrita.edu
amrita.edu      nameserver = ns2.amrita.edu
amrita.edu      nameserver = ns3.amrita.edu

ns1.amrita.edu  internet address = 14.139.187.131
ns2.amrita.edu  internet address = 117.193.77.232
ns3.amrita.edu  internet address = 103.10.24.200
ns4.amrita.edu  internet address = 103.5.112.81
ns4.amrita.edu  internet address = 115.243.144.130
```

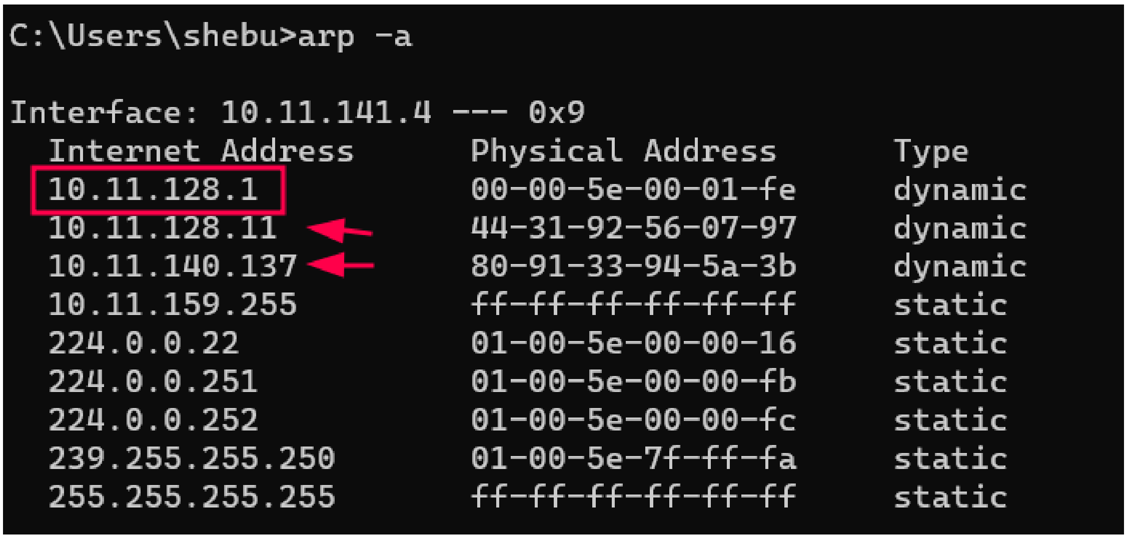
The name servers are ns1.amrita.edu , ns2.amrita.edu , ns3.amrita.edu , ns4.amrita.edu

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.



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

Interface: 10.11.141.4 --- 0x9
  Internet Address      Physical Address      Type
  10.11.128.1           00-00-5e-00-01-fe     dynamic
  10.11.128.11          44-31-92-56-07-97     dynamic
  10.11.140.137         80-91-33-94-5a-3b     dynamic
  10.11.159.255         ff-ff-ff-ff-ff-ff     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
  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?

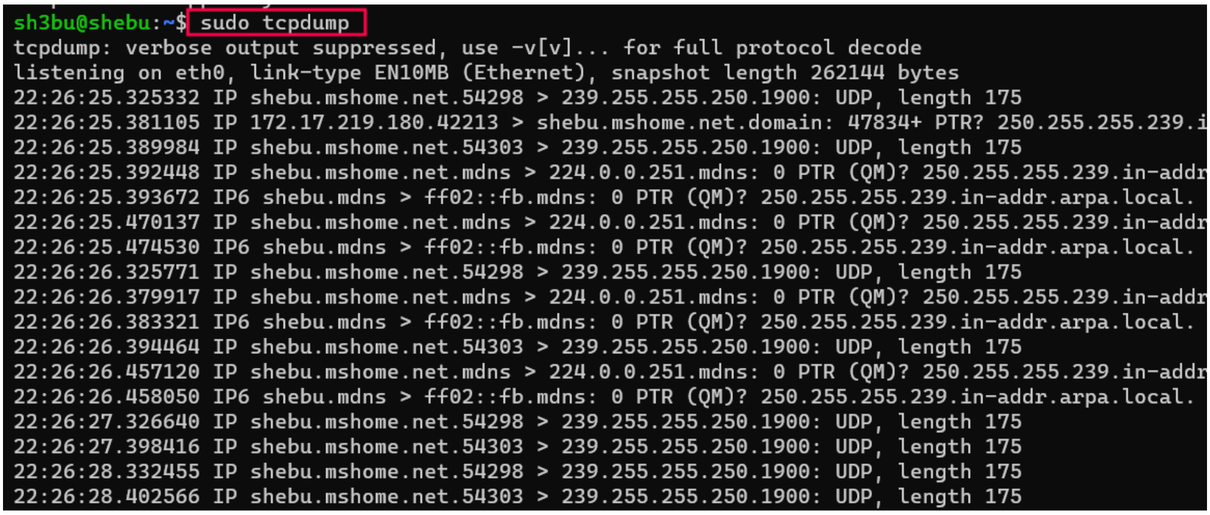
To add an arp entry we need to use –s flag along with IP address and MAC address.

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

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

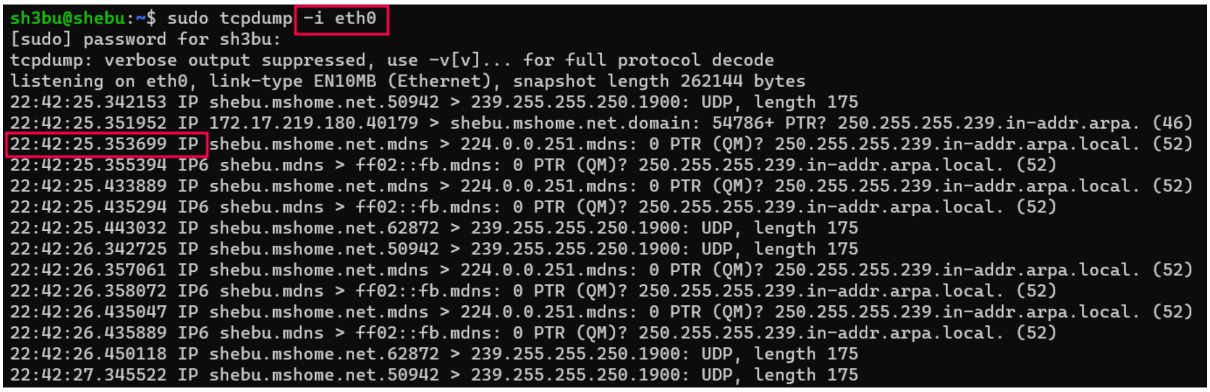
Answer the questions below: (1 marks)

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



```
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.



```
sh3bu@shebu:~$ sudo tcpdump -i eth0
[sudo] password for sh3bu:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:42:25.342153 IP shebu.mshome.net.50942 > 239.255.255.250.1900: UDP, length 175
22:42:25.351952 IP 172.17.219.180.40179 > shebu.mshome.net.domain: 54786+ PTR? 250.255.255.239.in-addr.arpa. (46)
22:42:25.353699 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:25.355394 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:25.433889 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:25.435294 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:25.443032 IP shebu.mshome.net.62872 > 239.255.255.250.1900: UDP, length 175
22:42:26.342725 IP shebu.mshome.net.50942 > 239.255.255.250.1900: UDP, length 175
22:42:26.357061 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:26.358072 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:26.435047 IP shebu.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:26.435889 IP6 shebu.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
22:42:26.450118 IP shebu.mshome.net.62872 > 239.255.255.250.1900: UDP, length 175
22:42:27.345522 IP shebu.mshome.net.50942 > 239.255.255.250.1900: UDP, length 175
```

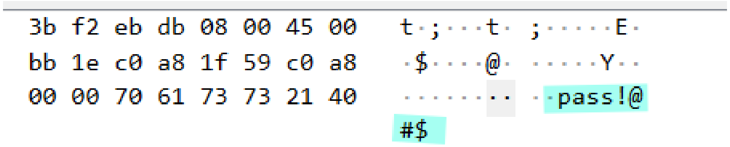
-I flag helps us to specify the desired interface

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.

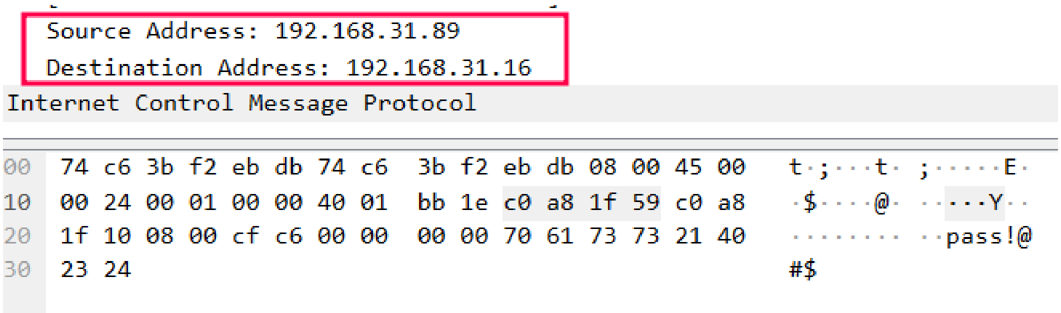
a. Find the data transferred.

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



```
3b f2 eb db 08 00 45 00   t·;···t· ;·····E·
bb 1e c0 a8 1f 59 c0 a8   ·$····@· ·····Y··
00 00 70 61 73 73 21 40   ········ ··pass!@
                          #$
```

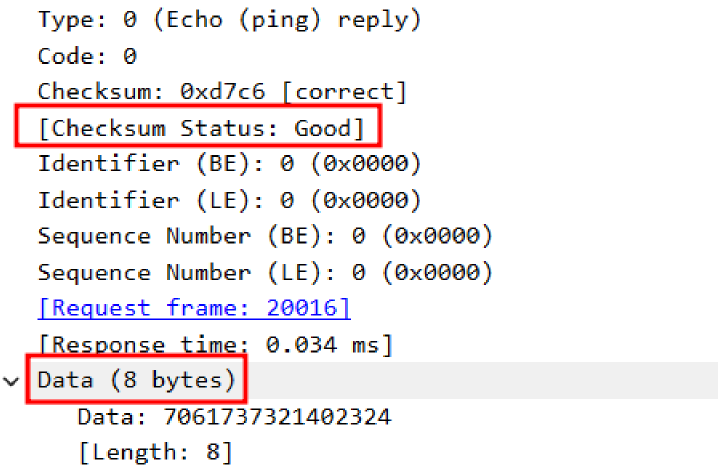
b. Find the source and destination IP of that log.



```
Source Address: 192.168.31.89
Destination Address: 192.168.31.16
Internet Control Message Protocol

00  74 c6 3b f2 eb db 74 c6  3b f2 eb db 08 00 45 00   t·;···t· ;·····E·
10  00 24 00 01 00 00 40 01  bb 1e c0 a8 1f 59 c0 a8   ·$····@· ·····Y··
20  1f 10 08 00 cf c6 00 00  00 00 70 61 73 73 21 40   ········ ··pass!@
30  23 24                                              #$
```

Source IP = 192.168.31.89, Destination IP = 192.168.31.16

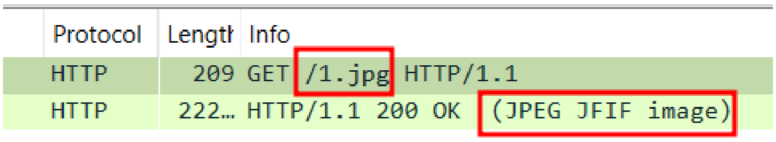
c. Find the Data length (Bytes) and verify the checksum status on destination.



```
Type: 0 (Echo (ping) reply)
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)
    Data: 7061737321402324
    [Length: 8]
```

ANS - The data length is 8 bytes and the header checksum status is GOOD

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

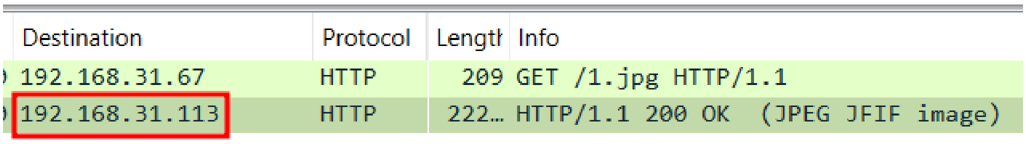


Protocol	Length	Info
HTTP	209	GET /1.jpg HTTP/1.1
HTTP	222…	HTTP/1.1 200 OK (JPEG JFIF image)

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

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



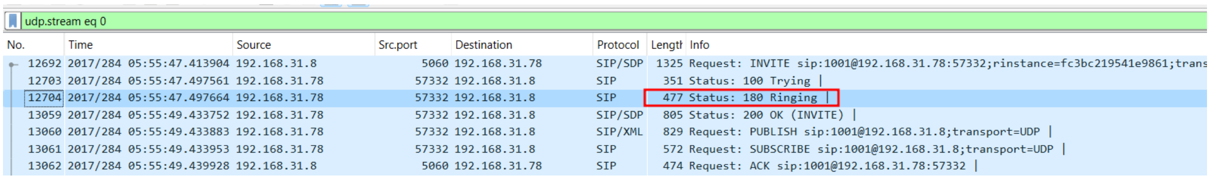
Destination	Protocol	Length	Info
192.168.31.67	HTTP	209	GET /1.jpg HTTP/1.1
192.168.31.113	HTTP	222…	HTTP/1.1 200 OK (JPEG JFIF image)

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.

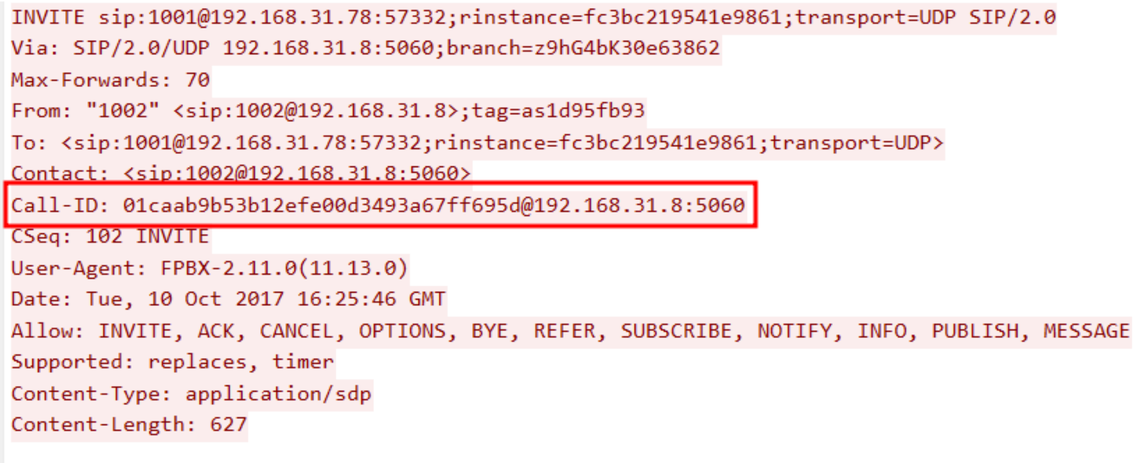
Ans - The password is “LIMBO”

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



udp.stream eq 0

No.	Time	Source	Src.port	Destination	Protocol	Length	Info
12692	2017/284 05:55:47.413904	192.168.31.8	5060	192.168.31.78	SIP/SDP	1325	Request: INVITE sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;trans
12703	2017/284 05:55:47.497561	192.168.31.78	57332	192.168.31.8	SIP	351	Status: 100 Trying |
12704	2017/284 05:55:47.497664	192.168.31.78	57332	192.168.31.8	SIP	477	Status: 180 Ringing |
13059	2017/284 05:55:49.433752	192.168.31.78	57332	192.168.31.8	SIP/SDP	805	Status: 200 OK (INVITE) |
13060	2017/284 05:55:49.433883	192.168.31.78	57332	192.168.31.8	SIP/XML	829	Request: PUBLISH sip:1001@192.168.31.8;transport=UDP |
13061	2017/284 05:55:49.433953	192.168.31.78	57332	192.168.31.8	SIP	572	Request: SUBSCRIBE sip:1001@192.168.31.8;transport=UDP |
13062	2017/284 05:55:49.439928	192.168.31.8	5060	192.168.31.78	SIP	474	Request: ACK sip:1001@192.168.31.78:57332 |



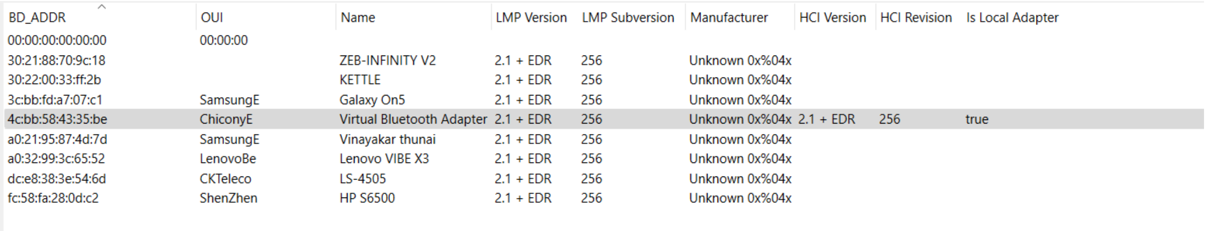
```
INVITE sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.31.8:5060;branch=z9hG4bK30e63862
Max-Forwards: 70
From: "1002" <sip:1002@192.168.31.8>;tag=as1d95fb93
To: <sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP>
Contact: <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, MESSAGE
Supported: replaces, timer
Content-Type: application/sdp
Content-Length: 627
```

CALLER-ID = 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060

4. On further investigation, you have a suspect on some wireless device communications. List out the Bluetooth devices communications from this traffic and find the details about native Bluetooth adapter.

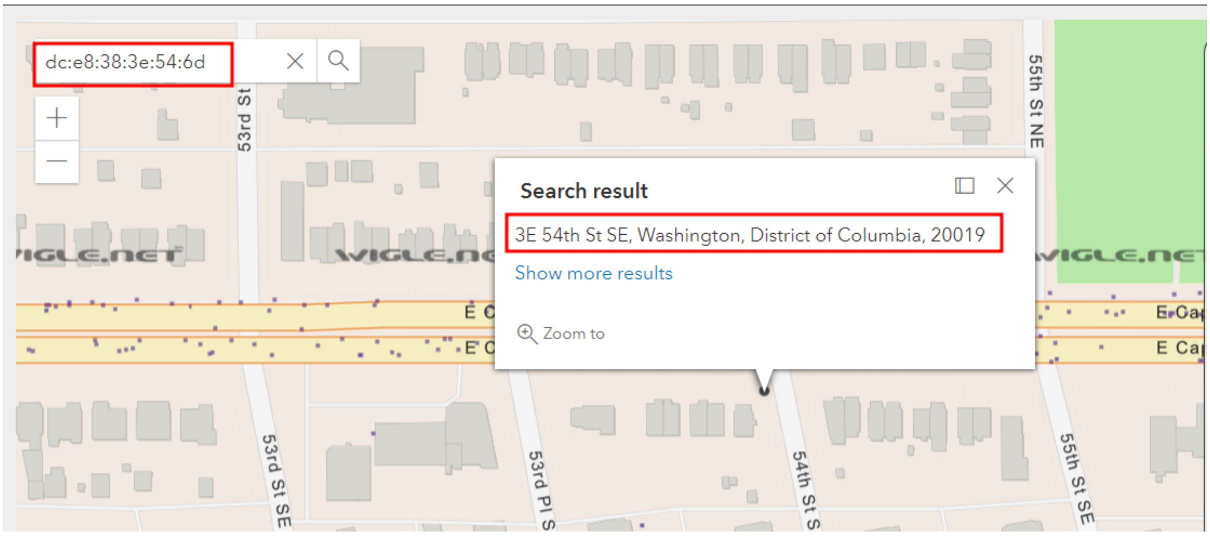
a. Analyze the captured WPA handshake from this traffic and report in detail about it to your administrator.

b. Geo locate all the endpoint of wireless devices.



BD_ADDR	OUI	Name	LMP Version	LMP Subversion	Manufacturer	HCI Version	HCI Revision	Is Local Adapter
00:00:00:00:00:00	00:00:00							
30:21:88:70:9c:18		ZEB-INFINITY V2	2.1 + EDR	256	Unknown 0x%04x			
30:22:00:33:ff:2b		KETTLE	2.1 + EDR	256	Unknown 0x%04x			
3c:bb:fd:a7:07:c1	SamsungE	Galaxy On5	2.1 + EDR	256	Unknown 0x%04x			
4c:bb:58:43:35:be	ChiconyE	Virtual Bluetooth Adapter	2.1 + EDR	256	Unknown 0x%04x	2.1 + EDR	256	true
a0:21:95:87:4d:7d	SamsungE	Vinayakar thunai	2.1 + EDR	256	Unknown 0x%04x			
a0:32:99:3c:65:52	LenovoBe	Lenovo VIBE X3	2.1 + EDR	256	Unknown 0x%04x			
dc:e8:38:3e:54:6d	CKTeleco	LS-4505	2.1 + EDR	256	Unknown 0x%04x			
fc:58:fa:28:0d:c2	ShenZhen	HP S6500	2.1 + EDR	256	Unknown 0x%04x			

We can find the following device's geolocation by using Wigle.net



dc:e8:38:3e:54:6d

Search result

3E 54th St SE, Washington, District of Columbia, 20019

Show more results

4c:bb:58:43:35:be - Straße 43 35, 13125, Berlin, Karow, Berlin

30:22:00:33:ff:2b - Tromilja, Šibenik, Šibensko-kninska županija

30:21:88:70:9c:18 - Zakučac, Omiš, Splitsko-dalmatinska županija

dc:e8:38:3e:54:6d - 3E 54th St SE, Washington, District of Columbia, 20019

c. Analyze the protocol level information transfer between wireless devices