**WIRE SHARK**

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

ping is used for checking connectivity and identifying network issues.

-w : it adjusts the timeout setting for a ping command

-l: it adjusts the packet size.

-f: it sets do not fragment flag

-n : pings the give ip address n number of times.

1a**. ping on google.com**

Ipv6 address: 2404:6800:4003:c0f::71

Time to live is not shown as it is ipv6 address.

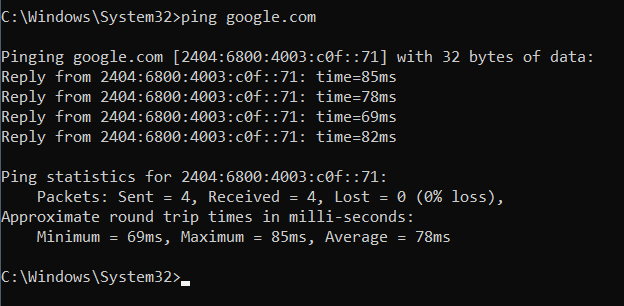
Round-trip time values

RTT1:85ms

RTT2:78ms

RTT3:69ms

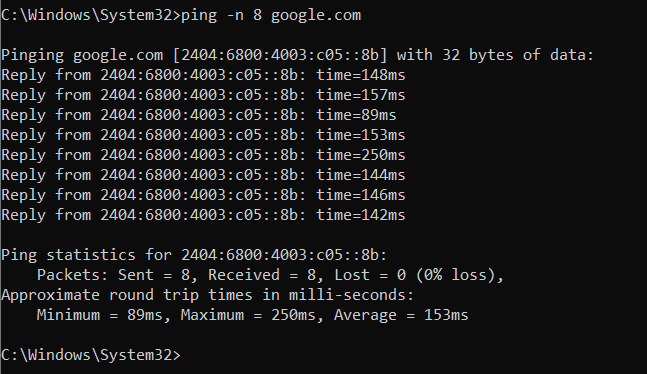
RTT4:82ms



b. **sending 8 packets:**

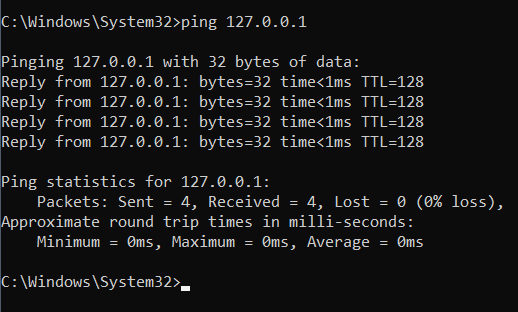
by sending 8 packets it helps to provide a reliable assessment of a network

performance.



c. **Ping your local host. Explain the purpose of doing it.**

It is used on the local host to troubleshoot if the network interface is up and running.

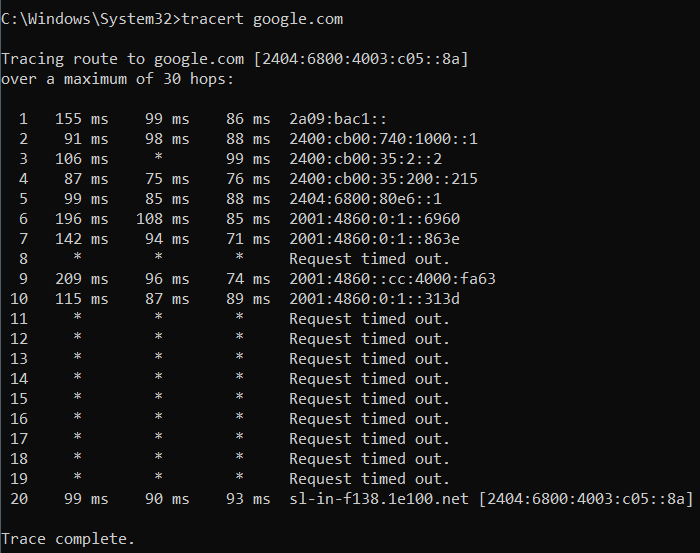


Tracert:-

By transmitting an ICMP(internet control message protocol) echo, the tracert command finds the path to a give ip address location.

Tracert is useful for determining response durations as data moves between nodes and the routing hops it must pass through.

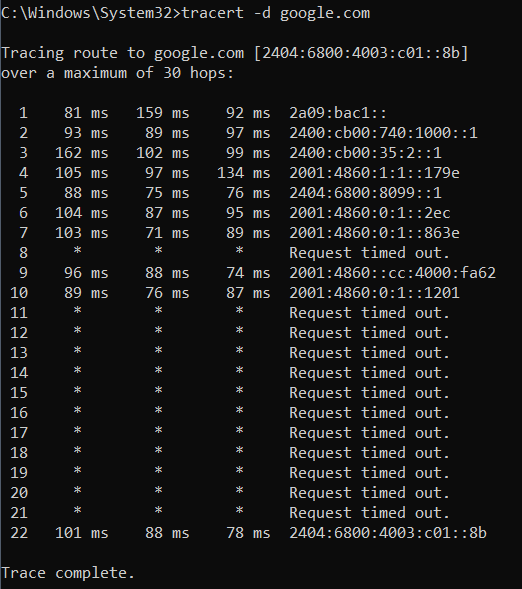
a. **Try tracert over google.com**



b.i.

**How many hops is your machine away from google.com?**

My machine is 22 hops away from google.com

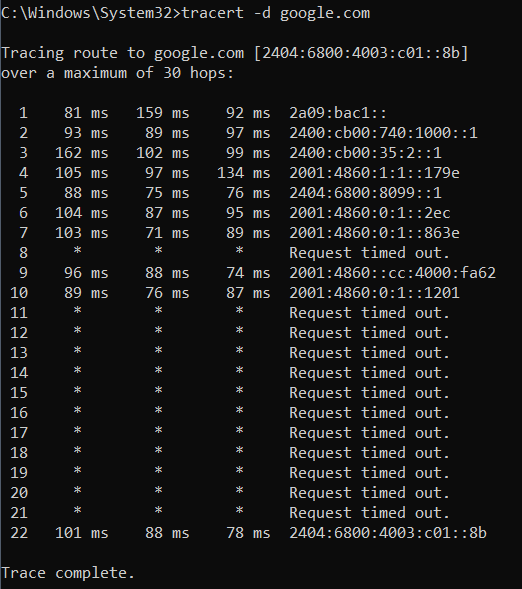


b.ii.

**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.**

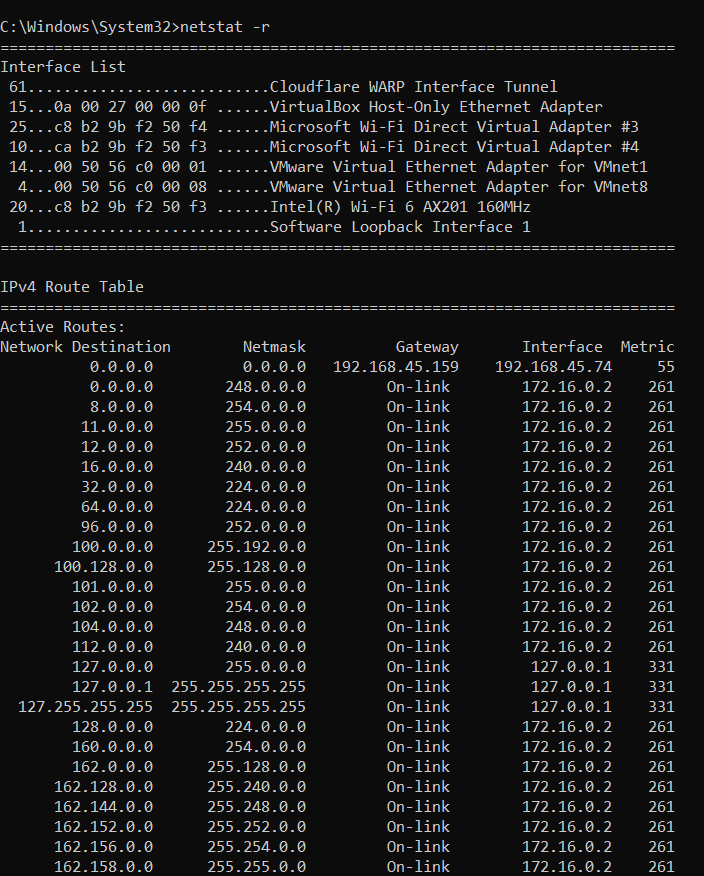
The new output does not seem very different from the previous output except for the latency.

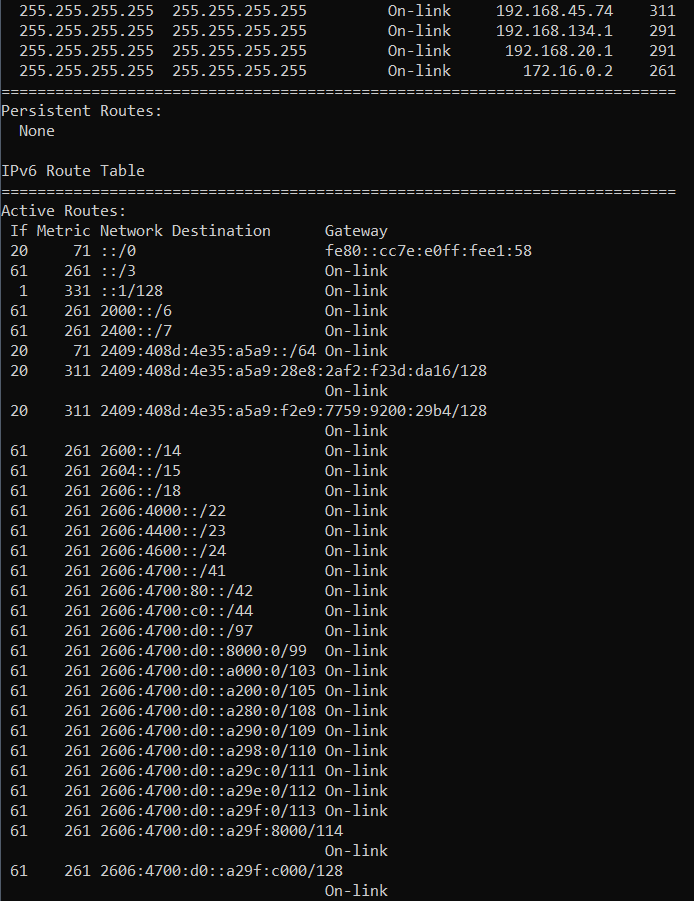
This could be because the network is already using the shortest path.



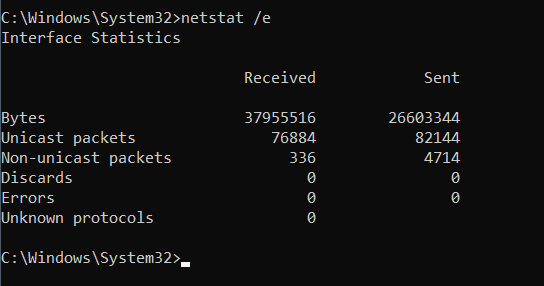
Netstat

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





b. **Use netstat to display about ethernet statistics.**

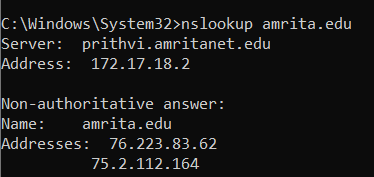


**4. What is the purpose of NSLOOKUP?**

We can enter a host name and find out the corresponding ip address or domain name system(DNS) record.

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

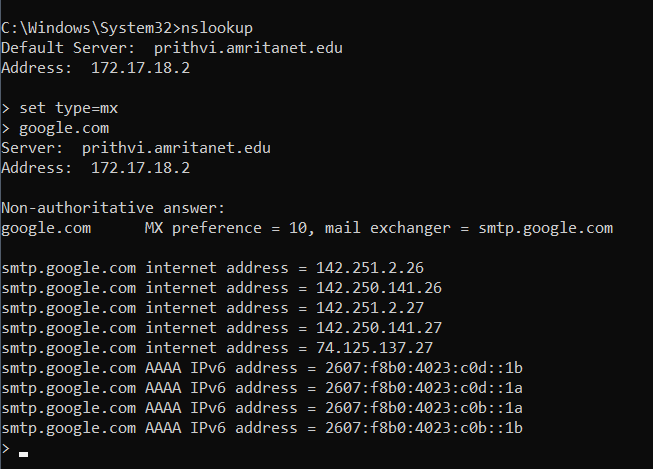
Intrenet address is 76.223.83.62



b.

**What is the mail exchanger for the domain google.com?**

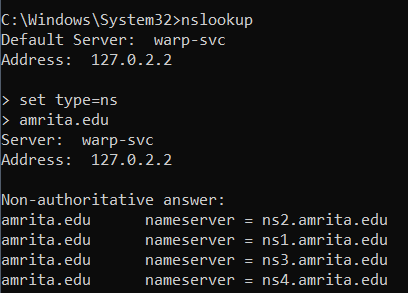
it is smtp.google.com



c.

**What is the name server for amrita.edu.**

Nameserver for amrita.edu is ns1.amrita.edu



5. **What is ARP and RARP? Answer the following questions below:**

ARP(Address resolution protocol):

To get the mac address of a network device when we only have IP address of that network device.

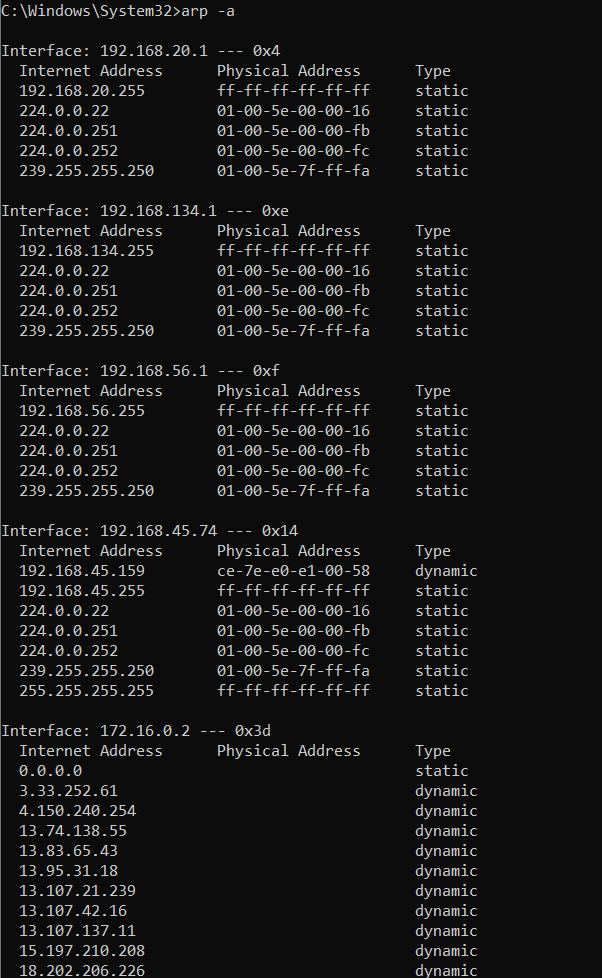
RARP( Reverse Address resolution protocol):

To get the IP address of a network device when we only have mac address of that network device.

5a.

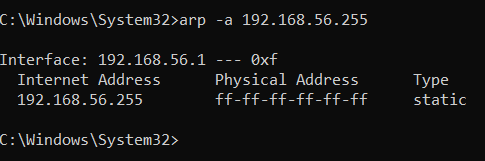
**Use arp command to find the gateway address and host systems hardware address.**

Gateway address: 192.168.56.255



B

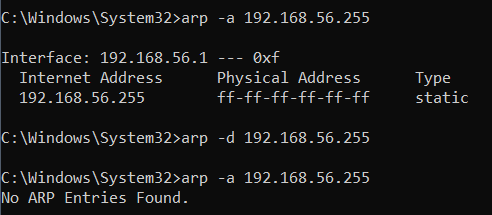
**How do you find the arp entries for a particular interface?**



C.

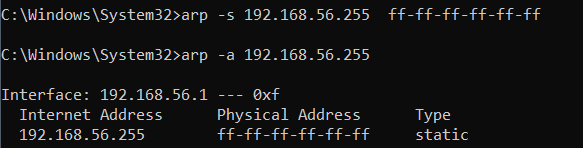
**How do delete an arp entry?**

By using arp –d command



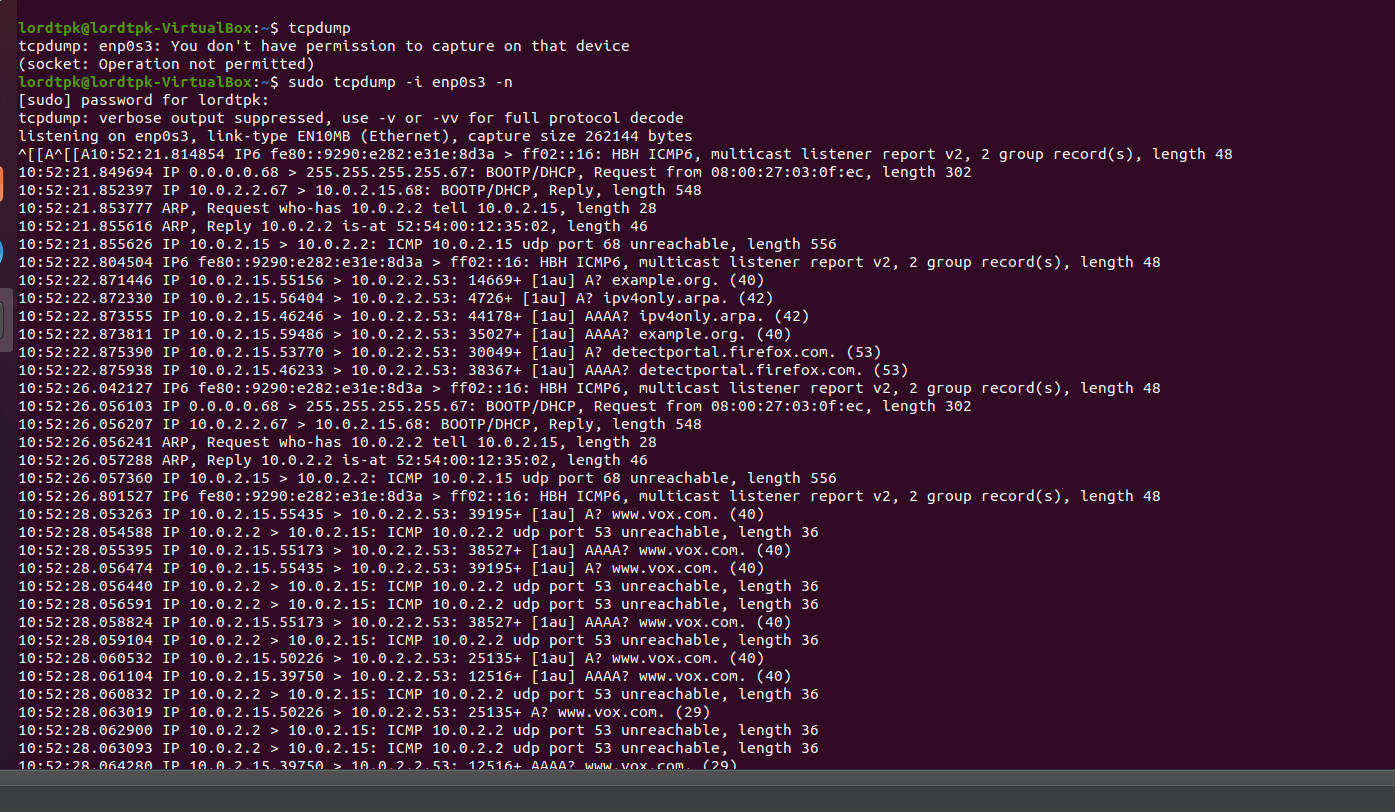
D. **How do you add and arp entry in arpcache?**

by using arp –s command

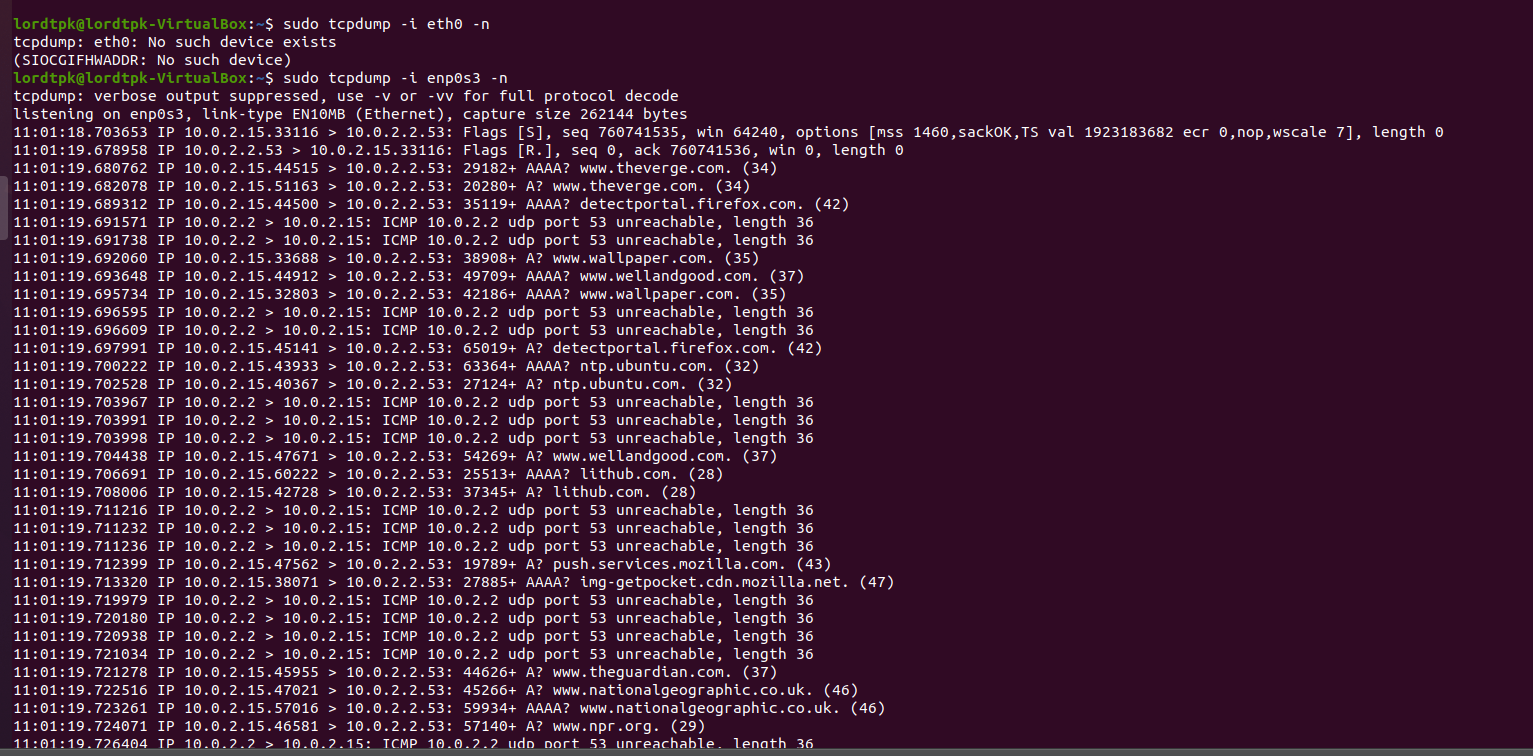


**6. Read about TCPDUMP tool :**

**6.a) Using tcpdump, get the information about the general incoming network traffic with domain names**.



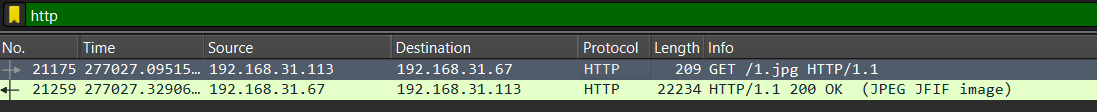
**6.b) Using tcpdump, get the information about the general incoming network traffic with ip address on specific interface**

****

7. **Use Wireshark (Latest version) to solve the below scenarios Use Evidence.pcapng as evidence file to answer the below questions.**

a. **Find the data transferred.**

.jpg file is transferred



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

The Source IP address : 192.168.31.113

the destination IP address : 192.168.31.67

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

data length : 22234 bytes.

Checksum status: unverified.



**7.2**

**Now you have found that some kind of file has been downloaded by insider in unencrypted web traffic.**

1. **Find the name and type of file**

Name : 1.jpg

Type: image/jpeg



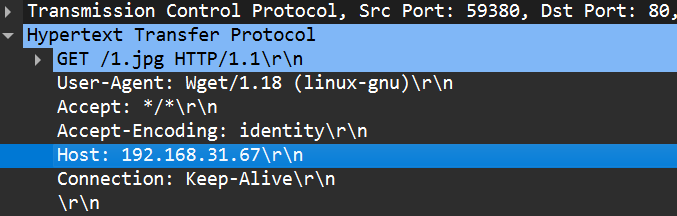
**b. Export that file from that web traffic, then analyze the file for any secret information.**

Secret information: Anthem



**b.Find the hostname in which the file is stored**.

The hostname is 192.168.31.67

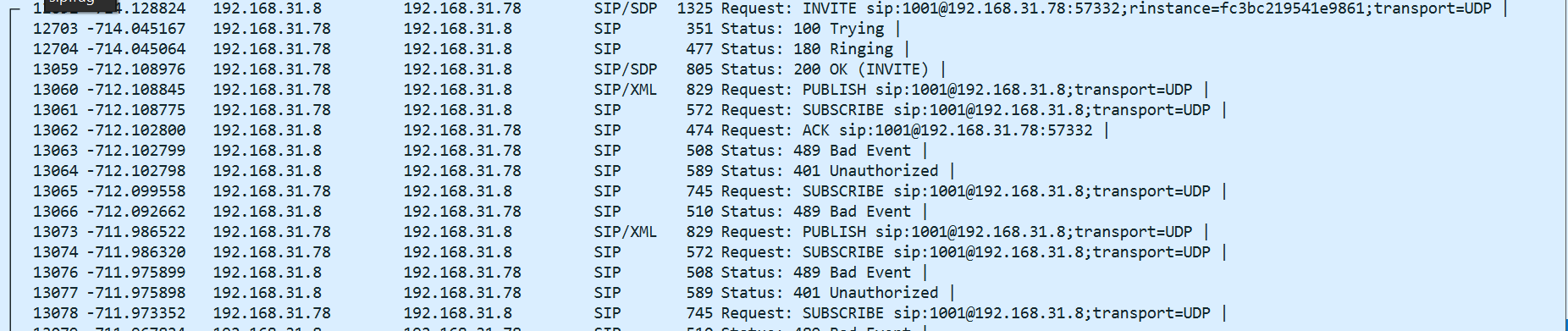


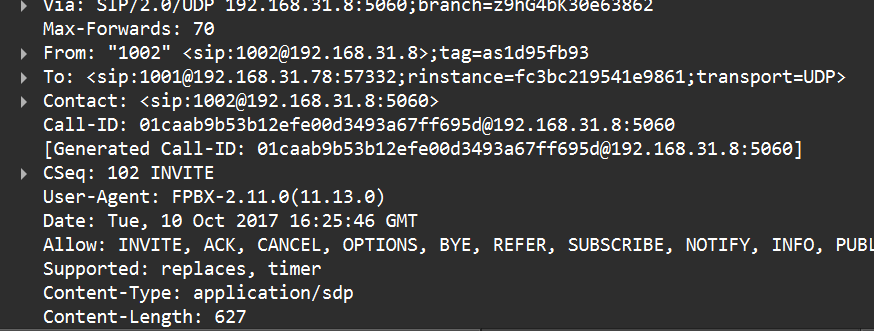
7. 3

**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 has been captured.**

**a.**

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





We can see the From, To, and call ID in the above screenshot.

We are also able to listen to the VOIP call in which a password is being shared.By listening to the call we can find out that the password is “LIMBO”.

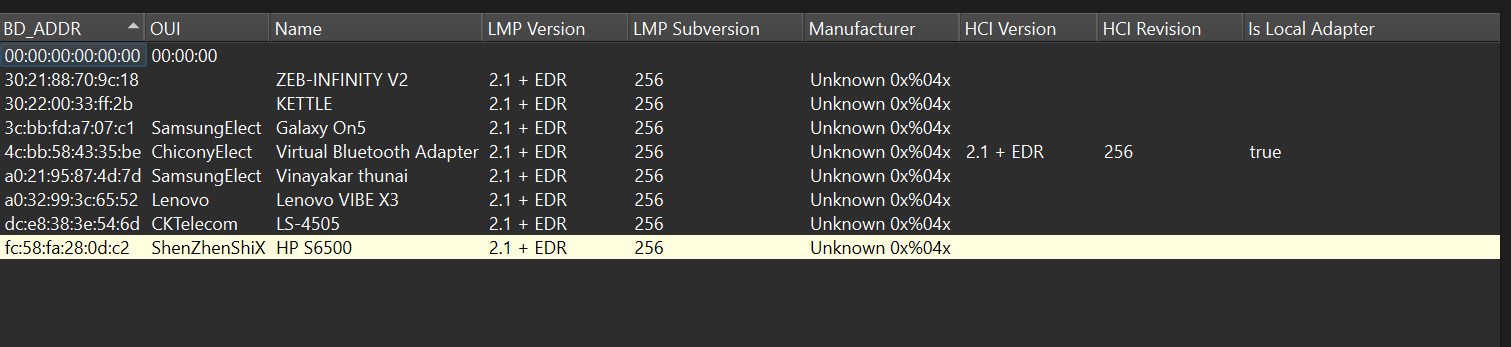
**b.**

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

call ID is [01caab9b53b12efe00d3493a67ff6956@192.168.31.8:5060](mailto:01caab9b53b12efe00d3493a67ff6956@192.168.31.8:5060)

**7.4**

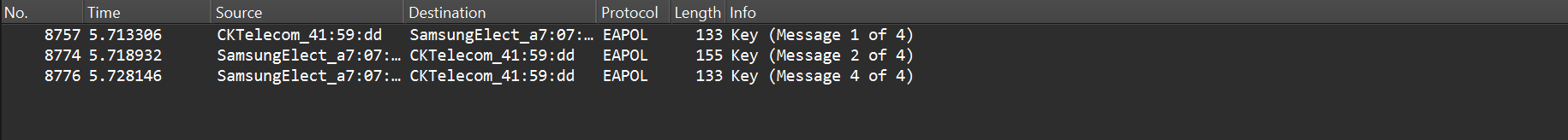
**On further investigation, you have a suspect on some wireless device communications. List out the Bluetooth devices communications from this traffic and find the details about native Bluetooth adapter.**



**a.**

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

3 WPA handshakes have been captured and the handshake are incomplete.



b.

**Geo locate all the endpoint of wireless devices.**

