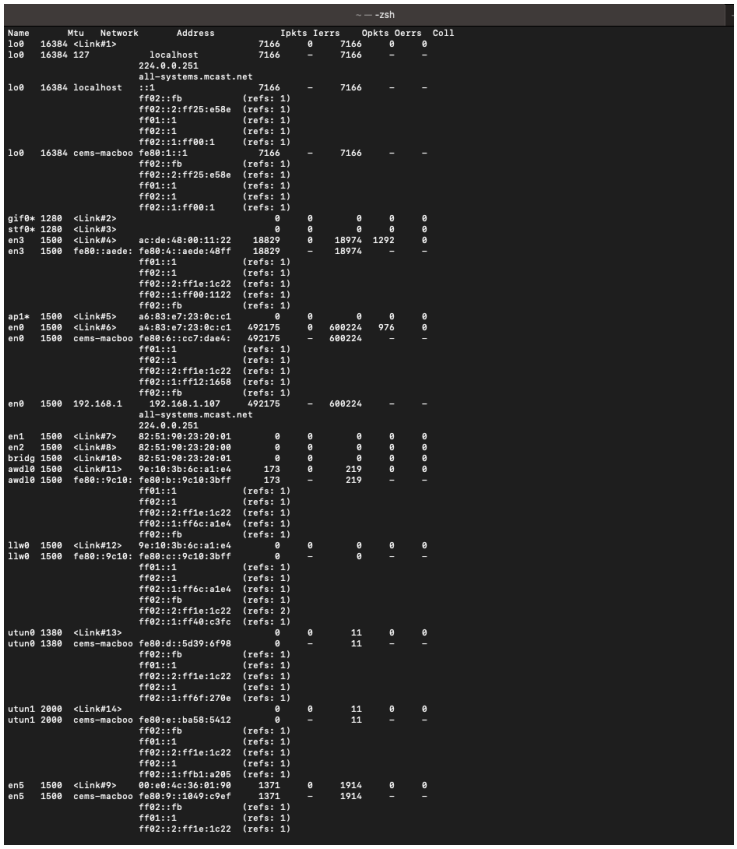
PROJECT 3

PART-1

1. Use ‘netstat -ai’ command to view the interface information. Differentiate the interfaces that you see and explain the parameters provided in the output.



```
~ — -zsh
Name       Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16384 <Link#1>                            7166     0     7166     0     0
lo0   16384 127           localhost            7166     -     7166     -     -
                          224.0.0.251
                          all-systems.mcast.net
lo0   16384 localhost     ::1                  7166     -     7166     -     -
                          ff02::fb           (refs: 1)
                          ff02::2:ff25:e58e  (refs: 1)
                          ff01::1            (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::1:ff00:1     (refs: 1)
lo0   16384 cems-macboo fe80:1::1              7166     -     7166     -     -
                          ff02::fb           (refs: 1)
                          ff02::2:ff25:e58e  (refs: 1)
                          ff01::1            (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::1:ff00:1     (refs: 1)
gif0* 1280  <Link#2>                             0     0        0     0     0
stf0* 1280  <Link#3>                             0     0        0     0     0
en3   1500  <Link#4>    ac:de:48:00:11:22    18829     0    18974  1292     0
en3   1500  fe80::aede: fe80:4::aede:48ff     18829     -    18974     -     -
                          ff01::1            (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 1)
                          ff02::1:ff00:1122  (refs: 1)
                          ff02::fb           (refs: 1)
ap1*  1500  <Link#5>    a6:83:e7:23:0c:c1        0     0        0     0     0
en0   1500  <Link#6>    a4:83:e7:23:0c:c1   492175     0   600224   976     0
en0   1500  cems-macboo fe80:6::cc7:dae4:   492175     -   600224     -     -
                          ff01::1            (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 1)
                          ff02::1:ff12:1658  (refs: 1)
                          ff02::fb           (refs: 1)
en0   1500  192.168.1    192.168.1.107       492175     -   600224     -     -
                          all-systems.mcast.net
                          224.0.0.251
en1   1500  <Link#7>    82:51:90:23:20:01        0     0        0     0     0
en2   1500  <Link#8>    82:51:90:23:20:00        0     0        0     0     0
bridg 1500  <Link#10>   82:51:90:23:20:01        0     0        0     0     0
awdl0 1500  <Link#11>   9e:10:3b:6c:a1:e4      173     0      219     0     0
awdl0 1500  fe80::9c10: fe80:b::9c10:3bff      173     -      219     -     -
                          ff01::1            (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 1)
                          ff02::1:ff6c:a1e4  (refs: 1)
                          ff02::fb           (refs: 1)
llw0  1500  <Link#12>   9e:10:3b:6c:a1:e4        0     0        0     0     0
llw0  1500  fe80::9c10: fe80::9c10:3bff          0     -        0     -     -
                          ff01::1            (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::1:ff6c:a1e4  (refs: 1)
                          ff02::fb           (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 2)
                          ff02::1:ff40:c3fc  (refs: 1)
utun0 1380  <Link#13>                            0     0       11     0     0
utun0 1380  cems-macboo fe80:d::5d39:6f98         0     -       11     -     -
                          ff02::fb           (refs: 1)
                          ff01::1            (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::1:ff6f:270e  (refs: 1)
utun1 2000  <Link#14>                            0     0       11     0     0
utun1 2000  cems-macboo fe80:e::ba58:5412         0     -       11     -     -
                          ff02::fb           (refs: 1)
                          ff01::1            (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 1)
                          ff02::1            (refs: 1)
                          ff02::1:ffb1:a205  (refs: 1)
en5   1500  <Link#9>    00:e0:4c:36:01:90     1371     0     1914     0     0
en5   1500  cems-macboo fe80:9::1049:c9ef      1371     -     1914     -     -
                          ff02::fb           (refs: 1)
                          ff01::1            (refs: 1)
                          ff02::2:ff1e:1c22  (refs: 1)
```

INTERFACES:

1-)lo0: loopback interface that includes the messages whose sender and the receiver addressed to the same computer.

2-) gif0: software network interface

3-)en0: Wi-Fi interface

4-)awdl0: apple wireless direct link , which is used for peer to peer connection in apple devices.

5-)stf0: ipv6 to ipv4 tunnel interface.

6-)en1, en2, en3: thunderbolt interfaces.

7-)ap1: access point interface

8-)bridge: thunderbolt bridge interface.

9-)llw0: low-latency wlan interface.

10-)utun0, utun1:the interfaces used for vpn connections.

11-)en5: iBridge adapter

PARAMETERS:

Name: Name of the interface

Mtu: Maximum transmission Unit is the size of the largest protocol data unit that can be communicated in a single network layer transaction (Source: wikipedia)

Ipkts: Total number of packets received.

Ierrs: Total number of input errors.

Opkts: Total number of packets transmitted.

Oerrs: Total number of output errors.

Coll: Number of packet collisions detected.

2. Use ‘netstat -nr’ or ‘netstat -r’ to find the local routing (forwarding) table. Examine the output and explain the following categories from the output: Destination, Gateway, GenMask, Flags and the meanings of various flags which are set, MSS, Window and ‘irtt’.

```
cemkilinc@Cems-MacBook-Pro ~ % netstat -nr
Routing tables

Internet:
Destination        Gateway            Flags        Netif Expire
default            192.168.1.1        UGScg          en0
127                127.0.0.1          UCS            lo0
127.0.0.1          127.0.0.1          UH             lo0
169.254            link#6             UCS            en0      !
192.168.1          link#6             UCS            en0      !
192.168.1.1/32     link#6             UCS            en0      !
192.168.1.1        5c:63:bf:ac:46:f4  UHLWIir        en0   1189
192.168.1.107/32   link#6             UCS            en0      !
192.168.1.108      50:bc:96:d6:65:85  UHLWIi         en0   1196
192.168.1.110      8e:26:54:aa:65:19  UHLWIi         en0   1011
224.0.0/4          link#6             UmCS           en0      !
224.0.0.251        1:0:5e:0:0:fb      UHmLWI         en0
239.255.255.250    1:0:5e:7f:ff:fa    UHmLWI         en0
255.255.255.255/32 link#6             UCS            en0      !

Internet6:
Destination                             Gateway                         Flags         Net
if Expire
default                                 fe80::%utun0                    UGcIg         utu
n0
default                                 fe80::%utun1                    UGcIg         utu
n1
default                                 fe80::%utun2                    UGcIg         utu
n2
default                                 fe80::%utun3                    UGcIg         utu
n3
::1                                     ::1                             UHL             l
o0
fe80::%lo0/64                           fe80::1%lo0                     UcI             l
o0
fe80::1%lo0                             link#1                          UHLI            l
o0
fe80::%en3/64                           link#4                          UCI             e
n3
fe80::aede:48ff:fe00:1122%en3           ac:de:48:0:11:22                UHLI            l
o0
fe80::aede:48ff:fe33:4455%en3           ac:de:48:33:44:55               UHLWIi          e
n3
fe80::%en0/64                           link#6                          UCI             e
n0
fe80::cc7:dae4:f512:1658%en0            a4:83:e7:23:c:c1                UHLI            l
o0
fe80::%awdl0/64                         link#11                         UCI           awd
l0
fe80::9c10:3bff:fe6c:a1e4%awdl0         9e:10:3b:6c:a1:e4               UHLI            l
o0
fe80::%llw0/64                          link#12                         UCI            ll
w0
fe80::9c10:3bff:fe6c:a1e4%llw0          9e:10:3b:6c:a1:e4               UHLI            l
o0
fe80::%utun0/64                         fe80::5d39:6f98:5d6f:270e%utun0 UcI           utu
n0
fe80::5d39:6f98:5d6f:270e%utun0         link#13                         UHLI            l
```

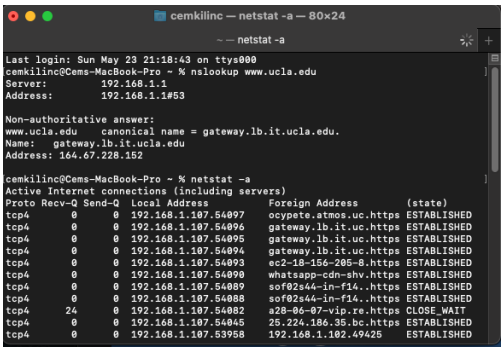
Although I did not receive all of the categories, I also included their explanation below.

Destination**:** It represents the destination network.
Gateway: The address of the outgoing interface.
GenMask: It shows the generality of the route.
Flags: The flags are used to describe the route each U, G, H… describe a situation such as

- G: The route is to a gateway
- U: The interface to be used is up.
- H: Only the single host can be reached through the route
- M: This route is modified.
- L: The link-level address is present
- C: Access to this route creates a cloned route

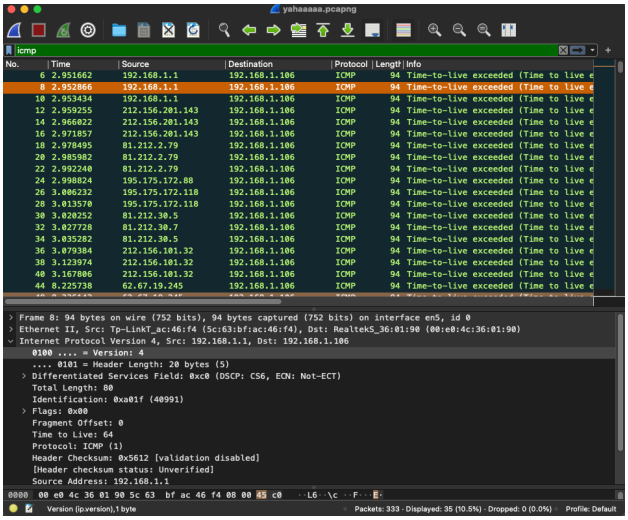
MSS: Maximum segment size which is the size of the largest datagram will be constructed for transmission via this route.
Window: is the maximum amount of data the system will accept in a single burst from a remote host.
Irtt: initial round trip time that is determined by looking at the TCP Three Way Handshake.
(Source : https://tldp.org/LDP/nag2/x-087-2-iface.netstat.html)

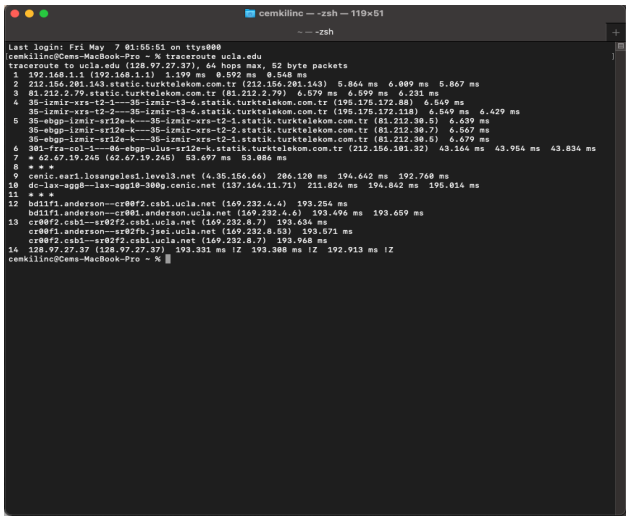
3. Open your assigned URL in the web browser. Find out the corresponding TCP socket using the netstat command with the appropriate command line options/arguments.



I used nslookup command to learn the name of my URL, then by using netstat -a command and saw 192.168.1.107.54094 socket is assigned to this.

4. What is TTL and its significance? Under which layer header can you find the value of TTL?



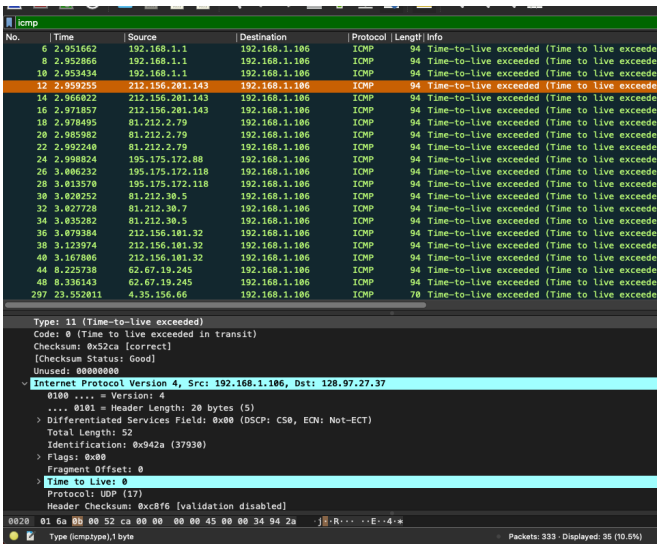


TTL (Time to live) represents the maximum number of hops that a packet can exist before being discarded. It limits the lifespan of data. One can find the TTL value under the internet protocol version 4 header.

5. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP packets does not have source and destination port numbers because they are not designed to communicate network-layer data between application layers of two hosts but rather they are designed to transfer data between hosts and routers. Thus, no port numbers are required.

6. Find the minimum TTL below which the traceroute messages do not reach your particular URL destination.



In the packet with number 12 which is an ICMP type message, TTL value is 0 which is the minimum.

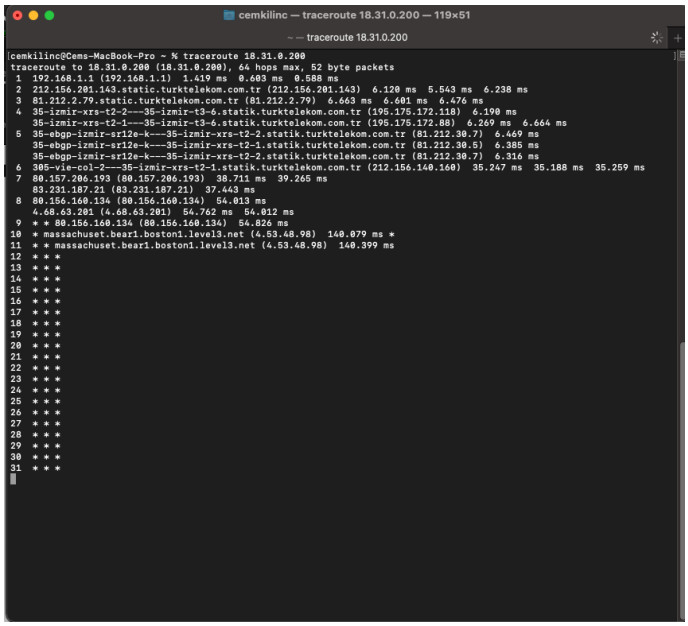
7. How does your computer (the source) learn the IP address of a router along the path from a TTL exceeded packet?

The source makes echo message request to the destination whose path is probed. Thanks to the TTL exceeded messages which are sent from routers to the source as a response, source can learn the IP address of a router by checking ipv4 header.

8. How many times is each router along the path probed by traceroute?

Traceroute generally probes each router 3 times in case of packet loss.

9. Find the route to the IP Address: 18.31.0.200. What is different about the results for this address?



As can be seen from the image it does not return anything, it is called black hole in the networking terminology.

10. What is a Routing Blackhole? Provide a scenario where Routing Blackholes may be used beneficially.

Routing Blackhole term is used when incoming or outgoing network is being eliminated without sending a response message to the sender, thus sender does not receive ICMP error (I execute wireshark and saw no ICMP messages when it entered the blackhole). Blackholes can be used to mitigate DDos attacks. When an attack is detected, all attack traffic can be discarded by routing Blackholes.

11. Use 'mtr *yourURL*' to find continuous statistics of the traceroute. Run the mtr command with three different of 4 fields each (you can find the information from 'man' pages) and explain the output.

For these two question my laptop does not even execute mtr command with my URL even if I brew reinstall.

12. Record the packets using ‘mtr yourURL’ through Wireshark. What is the difference between the Wireshark capture of traceroute and ‘mtr’?

Traceroute is an util which prints the route packages go through their destination in a connection. With mtr we can also trace the route for destination but also we can use it to see where exactly the packet loss happen in realtime, also it shows the loss percentage on hosts. Due to MTR using ICMP ECHO requests, it can work where traceroute command is not working. (Source: https://blog.zenlab.it/traceroute-vs-ping-vs-mtr/)