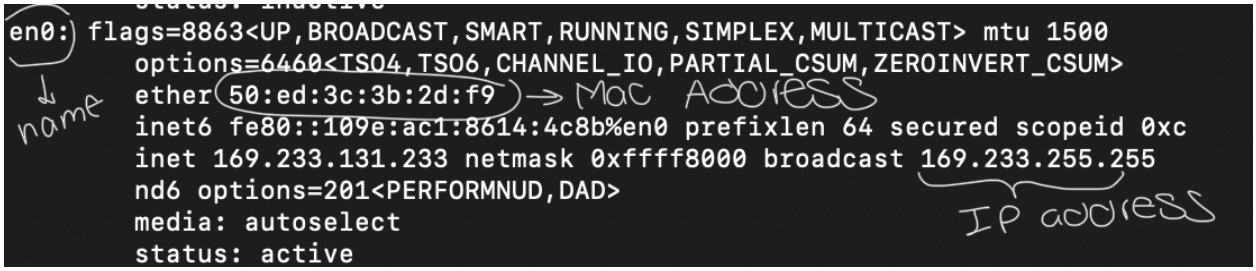
Pre-Lab 2:

a.) Network Interface is the point of connection between a computer and the network

[2 pts] In your own words, define Network Interface. On your laptop, look at your system settings and find your Ethernet or Wireless interface. List the interface name, MAC address, and IP Address. Attach a **screenshot** with the information highlighted or circled.



b.) What is the command to get details on all the processes running on the system?

- ps aux

c.) What is the complete command to find the pid of a process named “testing”?

- ps aux | grep -i testing,

What is the command to kill this process?

- kill testing

d.) What does it mean to run a process in “the background”?

- Running a process in the background means executing it that it runs independently from the terminal interface, meaning that other commands can be ran without the process disrupting them

What is the command to run a process “testing” in the background?

-./testing &

Q2.) Mininet Commands

a.) What command do you use to find the host interface?

- hostName ifconfig

b.) What are 2 different ways to test connectivity between hosts

- h1 ping h2
- Iperf

what is the difference between them?

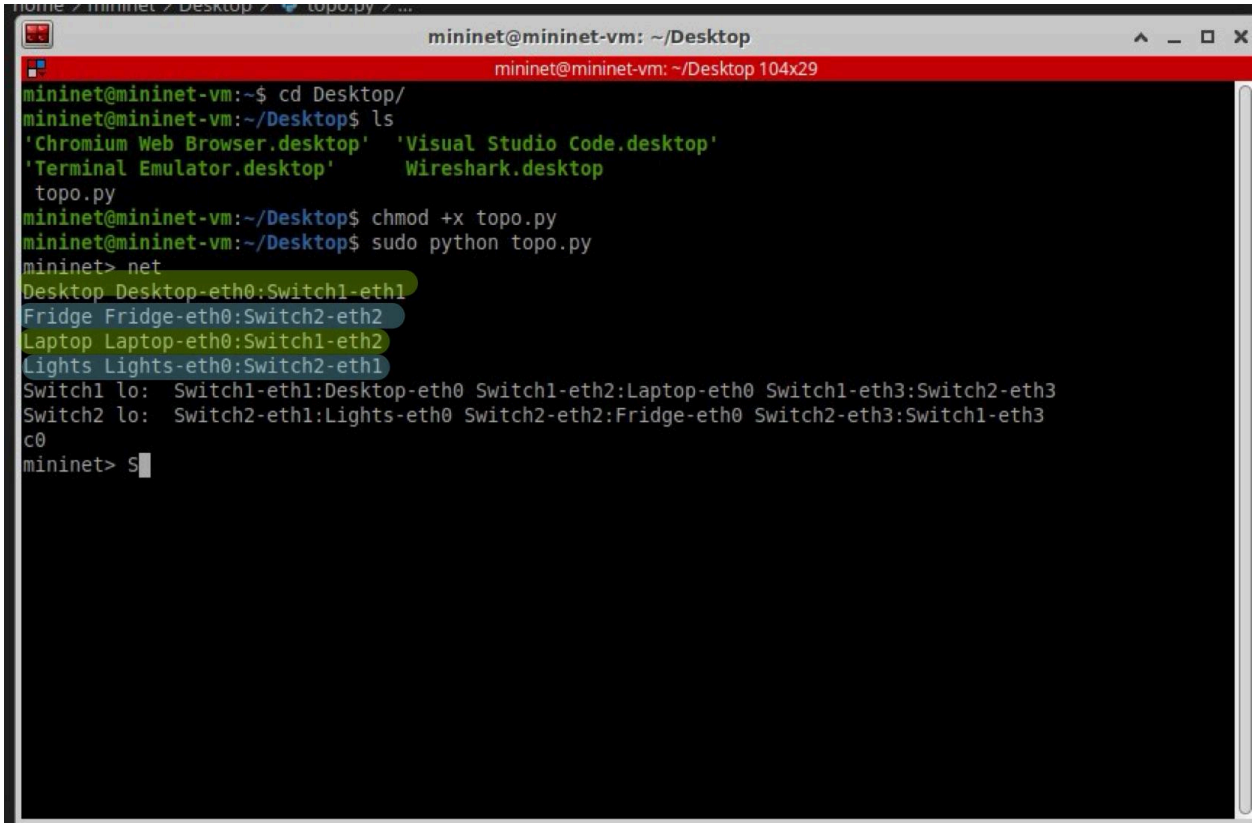
- Ping tests the network reachability, whether the host can communicate with each other, if the host is functioning on the network.
- While, iperf measures the bandwidth between the 2 hosts, the performance of the connection

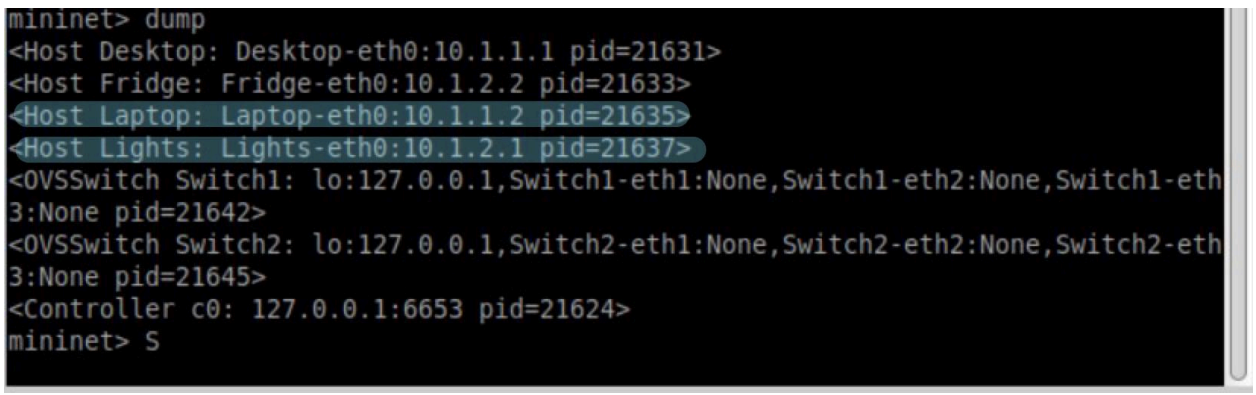
c.)What command do you use in Mininet to opne a terminal on a host?

- xterm h1

Q3.)

a.)


mininet@mininet-vm: ~/Desktop
mininet@mininet-vm: ~/Desktop 104x29
mininet@mininet-vm:~$ cd Desktop/
mininet@mininet-vm:~/Desktop$ ls
'Chromium Web Browser.desktop' 'Visual Studio Code.desktop'
'Terminal Emulator.desktop'   Wireshark.desktop
 topo.py
mininet@mininet-vm:~/Desktop$ chmod +x topo.py
mininet@mininet-vm:~/Desktop$ sudo python topo.py
mininet> net
Desktop Desktop-eth0:Switch1-eth1
Fridge Fridge-eth0:Switch2-eth2
Laptop Laptop-eth0:Switch1-eth2
Lights Lights-eth0:Switch2-eth1
Switch1 lo: Switch1-eth1:Desktop-eth0 Switch1-eth2:Laptop-eth0 Switch1-eth3:Switch2-eth3
Switch2 lo: Switch2-eth1:Lights-eth0 Switch2-eth2:Fridge-eth0 Switch2-eth3:Switch1-eth3
c0
mininet> S


mininet> dump
<Host Desktop: Desktop-eth0:10.1.1.1 pid=21631>
<Host Fridge: Fridge-eth0:10.1.2.2 pid=21633>
<Host Laptop: Laptop-eth0:10.1.1.2 pid=21635>
<Host Lights: Lights-eth0:10.1.2.1 pid=21637>
<OVSSwitch Switch1: lo:127.0.0.1,Switch1-eth1:None,Switch1-eth2:None,Switch1-eth
3:None pid=21642>
<OVSSwitch Switch2: lo:127.0.0.1,Switch2-eth1:None,Switch2-eth2:None,Switch2-eth
3:None pid=21645>
<Controller c0: 127.0.0.1:6653 pid=21624>
mininet> S

b.)

```
mininet> pingallfull
*** Ping: testing ping reachability
Desktop -> Fridge Laptop Lights
Fridge -> Desktop Laptop Lights
Laptop -> Desktop Fridge Lights
Lights -> Desktop Fridge Laptop
*** Results:
 Desktop->Fridge: 1/1, rtt min/avg/max/mdev 5.041/5.041/5.041/0.000 ms
 Desktop->Laptop: 1/1, rtt min/avg/max/mdev 1.216/1.216/1.216/0.000 ms
 Desktop->Lights: 1/1, rtt min/avg/max/mdev 1.678/1.678/1.678/0.000 ms
 Fridge->Desktop: 1/1, rtt min/avg/max/mdev 0.736/0.736/0.736/0.000 ms
 Fridge->Laptop: 1/1, rtt min/avg/max/mdev 1.766/1.766/1.766/0.000 ms
 Fridge->Lights: 1/1, rtt min/avg/max/mdev 0.983/0.983/0.983/0.000 ms
 Laptop->Desktop: 1/1, rtt min/avg/max/mdev 0.561/0.561/0.561/0.000 ms
 Laptop->Fridge: 1/1, rtt min/avg/max/mdev 1.042/1.042/1.042/0.000 ms
 Laptop->Lights: 1/1, rtt min/avg/max/mdev 2.071/2.071/2.071/0.000 ms
 Lights->Desktop: 1/1, rtt min/avg/max/mdev 0.946/0.946/0.946/0.000 ms
 Lights->Fridge: 1/1, rtt min/avg/max/mdev 2.871/2.871/2.871/0.000 ms
 Lights->Laptop: 1/1, rtt min/avg/max/mdev 1.640/1.640/1.640/0.000 ms
```

4.) Explain what you understand from the output

- The output is showing each host pinging every other host in the network outputting the response time for each host, showing each host is successful in reaching connection the other hosts

Q5.) What is ICMP?

- The internet control message (ICMP) protocol is used by hosts and routers to communicate network layer information with each other
- Applications Usage;
  - Traceroute:
    - Send ICMP package to the nth router, once it reaches the nth router and has expired will send a ICMP message to the sender host
  - Ping:
    - Sender send an ICMP Type 8(echo request) to destination host, and destination host sends an 0 code (echo reply)

No.	Time	Source	Destination	Protocol	Length	Info
7	0.903839468	10.1.1.1	10.1.1.2	ICMP	100	Echo (ping) request id
8	0.904010172	10.1.1.1	10.1.1.2	OpenFl…	184	Type: OFPT_PACKET_IN
9	0.904125140	10.1.1.1	10.1.1.2	OpenFl…	190	Type: OFPT_PACKET_OUT
11	0.904188060	10.1.1.1	10.1.1.2	ICMP	100	Echo (ping) request id
12	0.904190128	10.1.1.1	10.1.1.2	ICMP	100	Echo (ping) request id
13	0.904190651	10.1.1.1	10.1.1.2	ICMP	100	Echo (ping) request id
14	0.904202618	10.1.1.2	10.1.1.1	ICMP	100	Echo (ping) reply id
15	0.904296073	10.1.1.1	10.1.1.2	OpenFl…	184	Type: OFPT_PACKET_IN
16	0.904341754	10.1.1.2	10.1.1.1	OpenFl…	184	Type: OFPT_PACKET_IN
19	0.904405651	10.1.1.2	10.1.1.1	OpenFl…	190	Type: OFPT_PACKET_OUT
21	0.904416617	10.1.1.1	10.1.1.2	OpenFl…	190	Type: OFPT_PACKET_OUT
23	0.904471801	10.1.1.2	10.1.1.1	ICMP	100	Echo (ping) reply id

b.)Ping:

- When a sender sends an ICMP Type 8 (Echo Request) to a destination host, it's asking if the host is reachable. The destination host responds with an ICMP Type 0 (Echo Reply), confirming its availability.

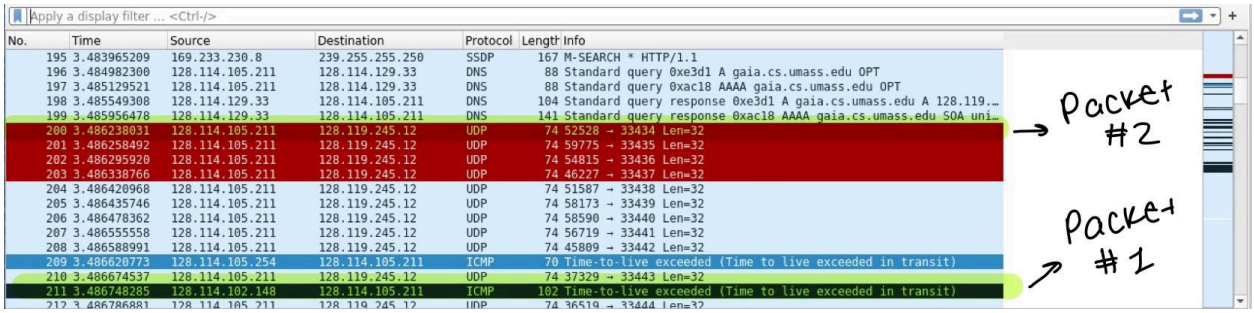
c.)

```
Frame 7: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interfa
  Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Oct  9, 2024 14:00:13.446143425 PDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1728507613.446143425 seconds
    [Time delta from previous captured frame: 0.903361115 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.903839468 seconds]
    Frame Number: 7
    Frame Length: 100 bytes (800 bits)
    Capture Length: 100 bytes (800 bits)
    [Frame is marked: False]
```

Q6.)

a.) What is the meaning of the -q flag in the traceroute command

- The q flag is utilized to specify the number of probe queries sent to each hop (router)

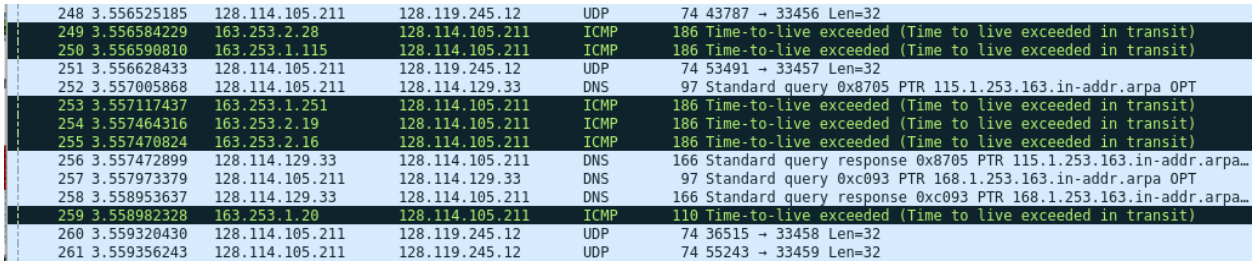


2.) According to your wireshark output, how many probes in total were Transmitted?

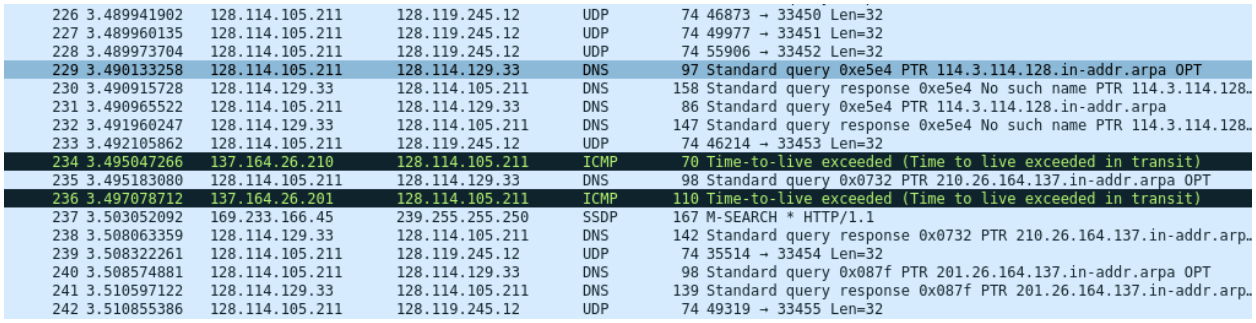
- 26 were transmitted

Does each generate a TTL-Exceeded Message?

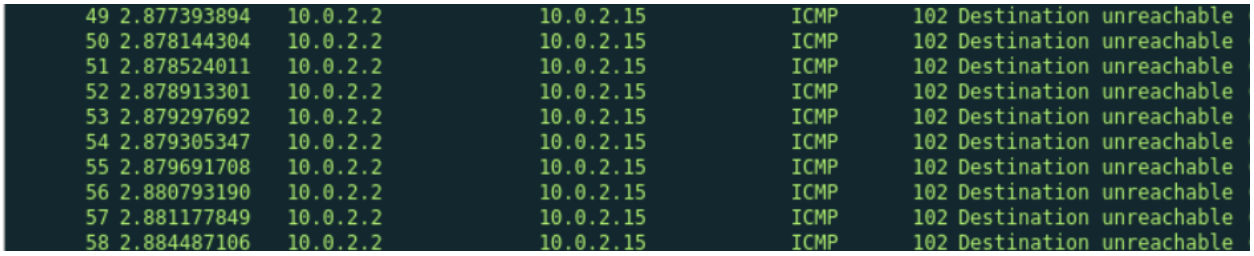
```
200 3.486238031  128.114.105.211  128.119.245.12  UDP   74 52528 → 33434 Len=32
201 3.486258492  128.114.105.211  128.119.245.12  UDP   74 59775 → 33435 Len=32
202 3.486295920  128.114.105.211  128.119.245.12  UDP   74 54815 → 33436 Len=32
203 3.486338766  128.114.105.211  128.119.245.12  UDP   74 46227 → 33437 Len=32
204 3.486420968  128.114.105.211  128.119.245.12  UDP   74 51587 → 33438 Len=32
205 3.486435746  128.114.105.211  128.119.245.12  UDP   74 58173 → 33439 Len=32
206 3.486478362  128.114.105.211  128.119.245.12  UDP   74 58590 → 33440 Len=32
207 3.486555558  128.114.105.211  128.119.245.12  UDP   74 56719 → 33441 Len=32
208 3.486588991  128.114.105.211  128.119.245.12  UDP   74 45809 → 33442 Len=32

209 3.486620773  128.114.105.254  128.114.105.211  ICMP  70 Time-to-live exceeded (Time to live exceeded in transit)
210 3.486674537  128.114.105.211  128.119.245.12  UDP   74 37329 → 33443 Len=32
211 3.486748285  128.114.102.148  128.114.105.211  ICMP  102 Time-to-live exceeded (Time to live exceeded in transit)
212 3.486786881  128.114.105.211  128.119.245.12  UDP   74 36519 → 33444 Len=32
213 3.486859147  128.114.3.105    128.114.105.211  ICMP  70 Time-to-live exceeded (Time to live exceeded in transit)
214 3.486871820  128.114.105.211  128.119.245.12  UDP   74 54103 → 33445 Len=32
215 3.486903233  128.114.105.211  128.119.245.12  UDP   74 56860 → 33446 Len=32
216 3.486916665  128.114.105.211  128.119.245.12  UDP   74 40287 → 33447 Len=32
217 3.486993194  128.114.105.211  128.119.245.12  UDP   74 55483 → 33448 Len=32
218 3.487006436  128.114.105.211  128.119.245.12  UDP   74 42950 → 33449 Len=32
```



248	3.556525185	128.114.105.211	128.119.245.12	UDP	74 43787 → 33456 Len=32
249	3.556584229	163.253.2.28	128.114.105.211	ICMP	186 Time-to-live exceeded (Time to live exceeded in transit)
250	3.556590810	163.253.1.115	128.114.105.211	ICMP	186 Time-to-live exceeded (Time to live exceeded in transit)
251	3.556628433	128.114.105.211	128.119.245.12	UDP	74 53491 → 33457 Len=32
252	3.557005868	128.114.105.211	128.114.129.33	DNS	97 Standard query 0x8705 PTR 115.1.253.163.in-addr.arpa OPT
253	3.557117437	163.253.1.251	128.114.105.211	ICMP	186 Time-to-live exceeded (Time to live exceeded in transit)
254	3.557464316	163.253.2.19	128.114.105.211	ICMP	186 Time-to-live exceeded (Time to live exceeded in transit)
255	3.557470824	163.253.2.16	128.114.105.211	ICMP	186 Time-to-live exceeded (Time to live exceeded in transit)
256	3.557472899	128.114.129.33	128.114.105.211	DNS	166 Standard query response 0x8705 PTR 115.1.253.163.in-addr.arpa…
257	3.557973379	128.114.105.211	128.114.129.33	DNS	97 Standard query 0xc093 PTR 168.1.253.163.in-addr.arpa OPT
258	3.558953637	128.114.129.33	128.114.105.211	DNS	166 Standard query response 0xc093 PTR 168.1.253.163.in-addr.arpa…
259	3.558982328	163.253.1.20	128.114.105.211	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
260	3.559320430	128.114.105.211	128.119.245.12	UDP	74 36515 → 33458 Len=32
261	3.559356243	128.114.105.211	128.119.245.12	UDP	74 55243 → 33459 Len=32

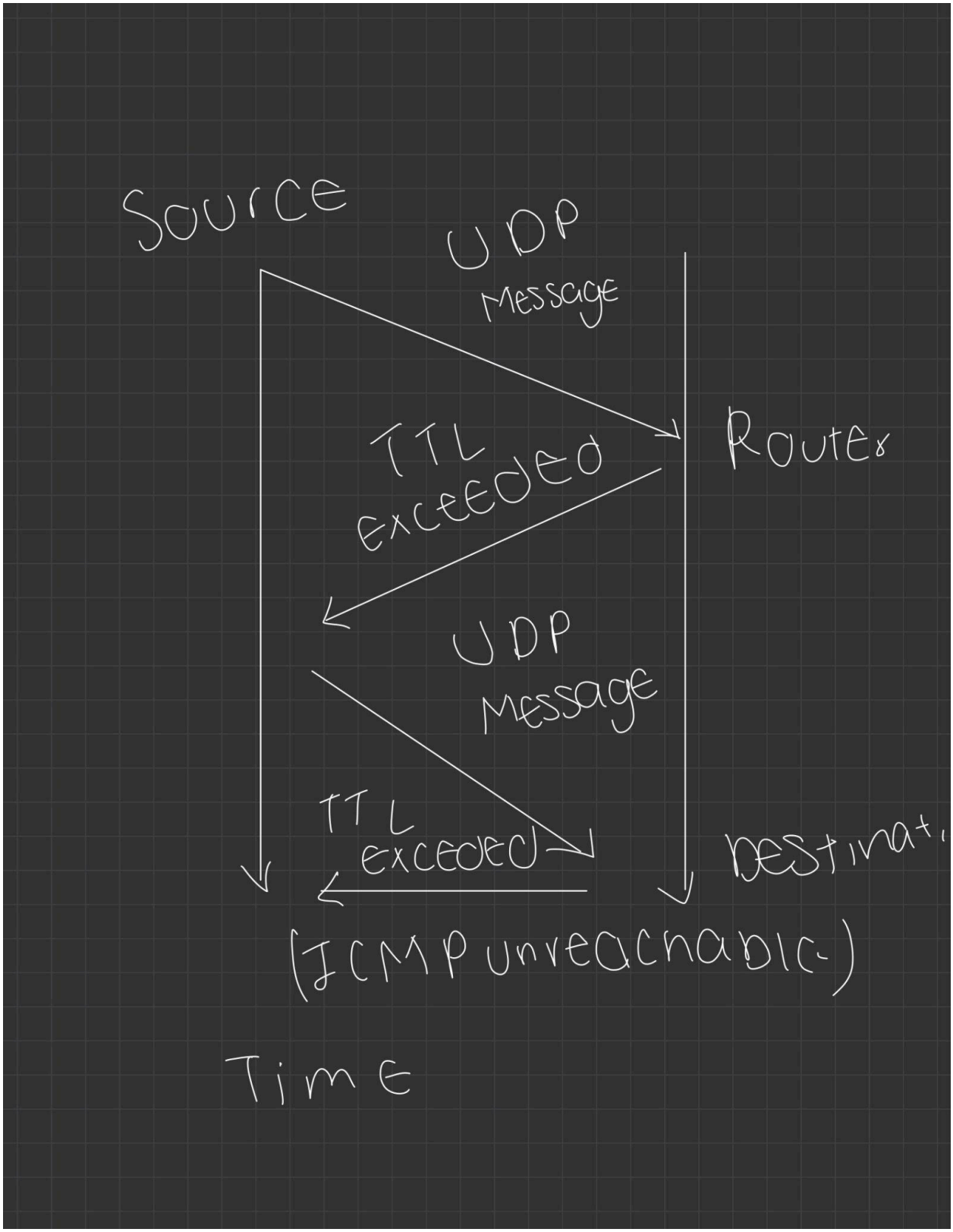


226	3.489941902	128.114.105.211	128.119.245.12	UDP	74 46873 → 33450 Len=32
227	3.489960135	128.114.105.211	128.119.245.12	UDP	74 49977 → 33451 Len=32
228	3.489973704	128.114.105.211	128.119.245.12	UDP	74 55906 → 33452 Len=32
229	3.490133258	128.114.105.211	128.114.129.33	DNS	97 Standard query 0xe5e4 PTR 114.3.114.128.in-addr.arpa OPT
230	3.490915728	128.114.129.33	128.114.105.211	DNS	158 Standard query response 0xe5e4 No such name PTR 114.3.114.128…
231	3.490965522	128.114.105.211	128.114.129.33	DNS	86 Standard query 0xe5e4 PTR 114.3.114.128.in-addr.arpa
232	3.491960247	128.114.129.33	128.114.105.211	DNS	147 Standard query response 0xe5e4 No such name PTR 114.3.114.128…
233	3.492105862	128.114.105.211	128.119.245.12	UDP	74 46214 → 33453 Len=32
234	3.495047266	137.164.26.210	128.114.105.211	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
235	3.495183080	128.114.105.211	128.114.129.33	DNS	98 Standard query 0x0732 PTR 210.26.164.137.in-addr.arpa OPT
236	3.497078712	137.164.26.201	128.114.105.211	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
237	3.503052092	169.233.166.45	239.255.255.250	SSDP	167 M-SEARCH * HTTP/1.1
238	3.508063359	128.114.129.33	128.114.105.211	DNS	142 Standard query response 0x0732 PTR 210.26.164.137.in-addr.arp…
239	3.508322261	128.114.105.211	128.119.245.12	UDP	74 35514 → 33454 Len=32
240	3.508574881	128.114.105.211	128.114.129.33	DNS	98 Standard query 0x087f PTR 201.26.164.137.in-addr.arpa OPT
241	3.510597122	128.114.129.33	128.114.105.211	DNS	139 Standard query response 0x087f PTR 201.26.164.137.in-addr.arp…
242	3.510855386	128.114.105.211	128.119.245.12	UDP	74 49319 → 33455 Len=32



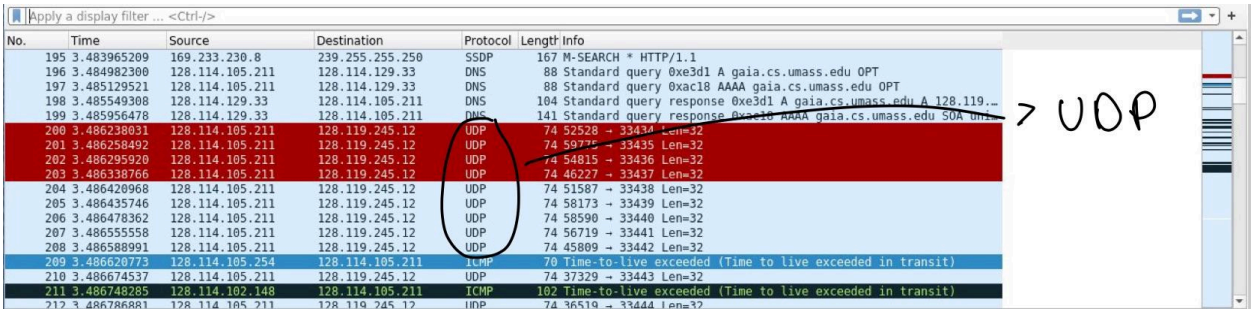
49	2.877393894	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
50	2.878144304	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
51	2.878524011	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
52	2.878913301	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
53	2.879297692	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
54	2.879305347	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
55	2.879691708	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
56	2.880793190	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
57	2.881177849	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable
58	2.884487106	10.0.2.2	10.0.2.15	ICMP	102 Destination unreachable

c.) Draw a small diagram



Q7.) What 2 protocols can Traceroute use for its probes

- Traceroute can use
  - UDP
  - ICMP Echo Request Message



b.) What protocol is being used to send the probe in Q6.

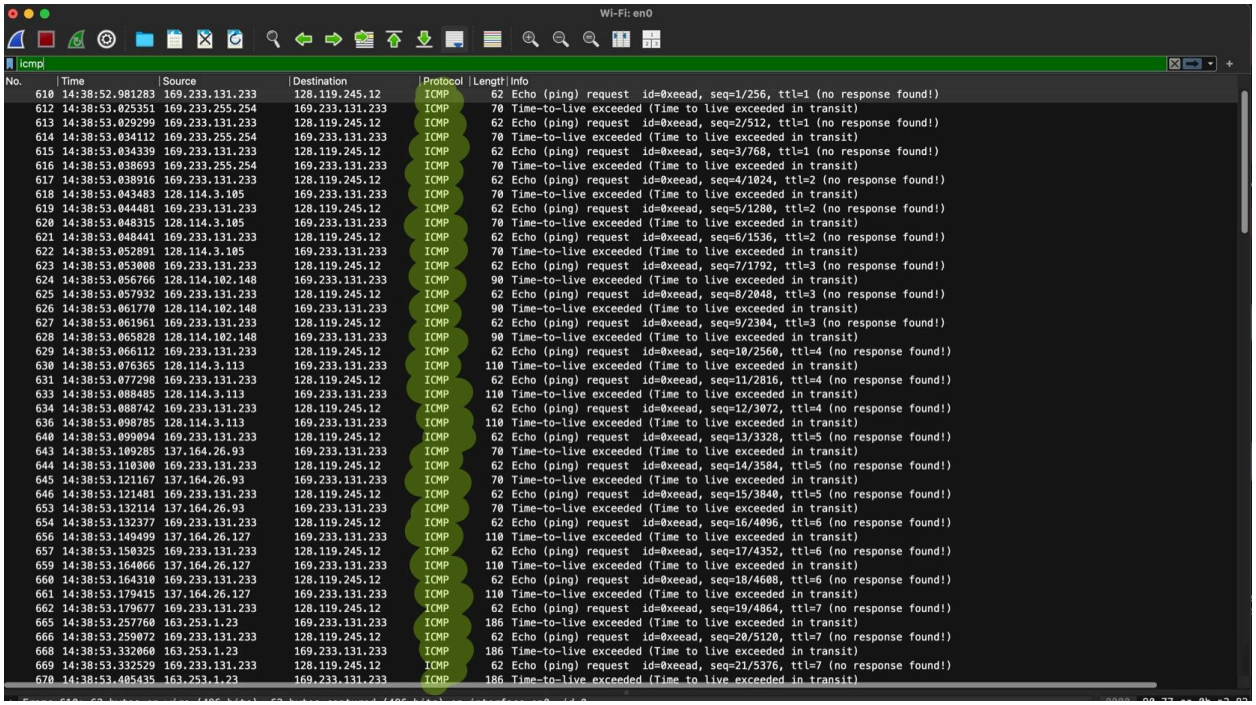
- The protocol being used is UDP as shown in the screenshot, as UDP is connectionless protocol allowing traceroute to reach routers and response without increased delay of connection setup

Q8.)

a.) What flag would you need to force traceroute to use the ICMP Protocol?

- traceroute -I <destination>

b.)



b.) Provide an explanation

- ICMP allows for an immediate responses from each router when the TTL (Time To Live) expires. Many firewalls permit ICMP traffic but block UDP, making it easier for traceroute to get through restrictive network environments.

Q9.) From the Displayed ID Header Information:

a.) What is the source (src) and destination (dst) IP Address

- Source : 128.114.105.254
- Destination: 128.114.105.211

b.) What is the size (in bytes) of the IP Header's Length Field

- 20 bytes

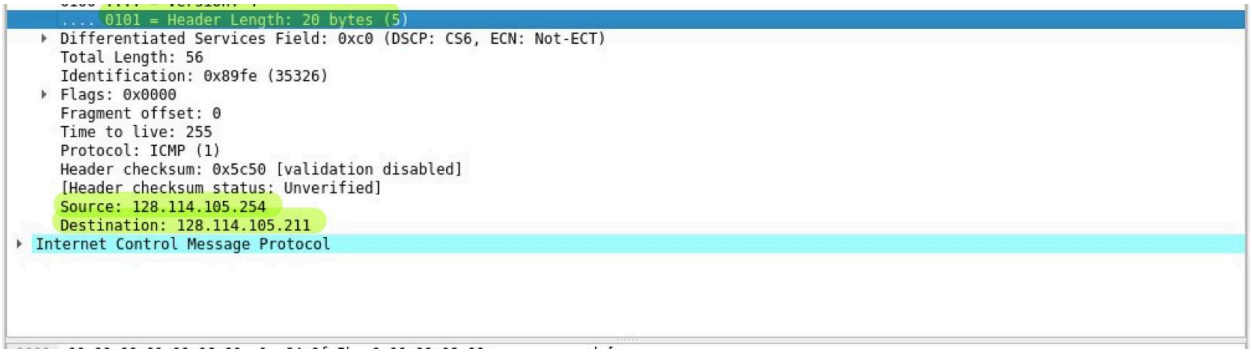
c.) How many bytes are in the payload of the IP Datagram?

-Total Length: 36 bytes

Explain how you determined the number of payload bytes:

- The length of the payload bytes is achieved, by subtracting the header length from the total length

Attach a screenshot and circle your answers a,b,c



Extra Credit:

Think about the probes you observed in Q6. Find the response from the server that causes Traceroute to terminate.

Attach a screenshot of your results in Wireshark and describe what type of packets you have found that causes Tracerouce to finish.