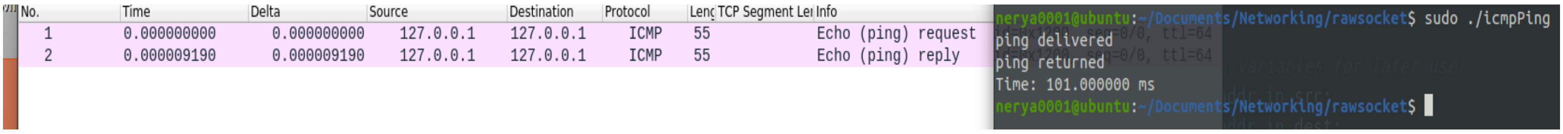
Assignment 5 - ICMP and Sniffing

In this assignment we learned to use raw sockets in order to send ICMP messages (PING), and how to sniff ICMP packets using a raw socket that is used as a monitor.

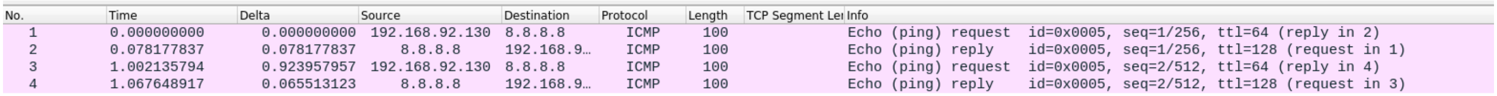
Here is a screenshot of the ping program we've made, in action.
we can see in the right side on the terminal that it took 101ms for the ping to return, and on the left side we recorded this ping on wireshark (the pcap file attached in the submitted folder).



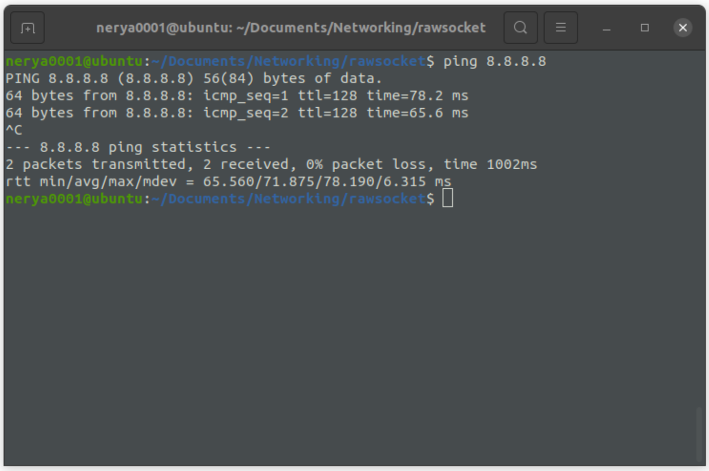
No.	Time	Delta	Source	Destination	Protocol	Leng	TCP Segment Le	Info
1	0.000000000	0.000000000	127.0.0.1	127.0.0.1	ICMP	55		Echo (ping) request
2	0.000009190	0.000009190	127.0.0.1	127.0.0.1	ICMP	55		Echo (ping) reply

```
nerya0001@ubuntu:~/Documents/Networking/rawsocket$ sudo ./icmpPing
ping delivered
ping returned
Time: 101.000000 ms
nerya0001@ubuntu:~/Documents/Networking/rawsocket$
```

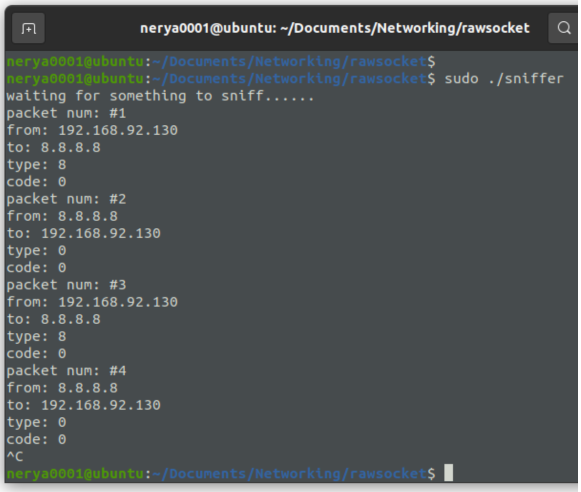
In the following screenshot the sniffing can be seen.
On the right terminal window we can see the siffer run, and on the left terminal window we run a regular ping command (to google - 8.8.8.8) so there will be something for the sniffer to sniff.
on top there is a wireshark recording of all of this, and the pcap file is attached in the submitted folder.



No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Le	Info
1	0.000000000	0.000000000	192.168.92.130	8.8.8.8	ICMP	100		Echo (ping) request id=0x0005, seq=1/256, ttl=64 (reply in 2)
2	0.078177837	0.078177837	8.8.8.8	192.168.9…	ICMP	100		Echo (ping) reply id=0x0005, seq=1/256, ttl=128 (request in 1)
3	1.002135794	0.923957957	192.168.92.130	8.8.8.8	ICMP	100		Echo (ping) request id=0x0005, seq=2/512, ttl=64 (reply in 4)
4	1.067648917	0.065513123	8.8.8.8	192.168.9…	ICMP	100		Echo (ping) reply id=0x0005, seq=2/512, ttl=128 (request in 3)



```
nerya0001@ubuntu:~/Documents/Networking/rawsocket$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=78.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=65.6 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 65.560/71.875/78.190/6.315 ms
nerya0001@ubuntu:~/Documents/Networking/rawsocket$
```



```
nerya0001@ubuntu:~/Documents/Networking/rawsocket$
nerya0001@ubuntu:~/Documents/Networking/rawsocket$ sudo ./sniffer
waiting for something to sniff......
packet num: #1
from: 192.168.92.130
to: 8.8.8.8
type: 8
code: 0
packet num: #2
from: 8.8.8.8
to: 192.168.92.130
type: 0
code: 0
packet num: #3
from: 192.168.92.130
to: 8.8.8.8
type: 8
code: 0
packet num: #4
from: 8.8.8.8
to: 192.168.92.130
type: 0
code: 0
^C
nerya0001@ubuntu:~/Documents/Networking/rawsocket$
```