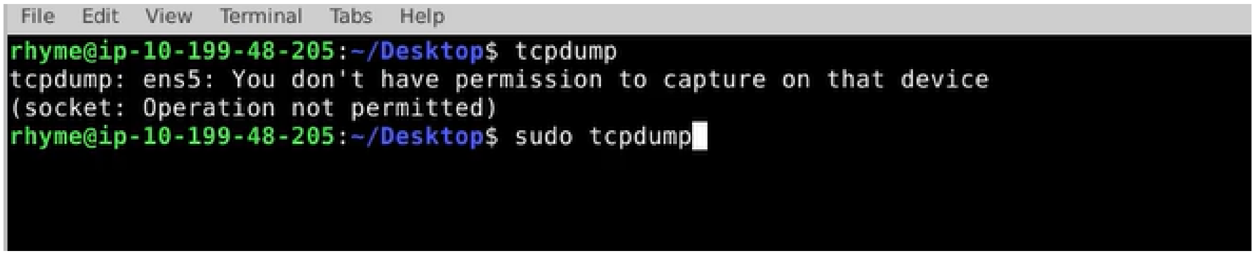
Analyzed Network traffic with TCPDump

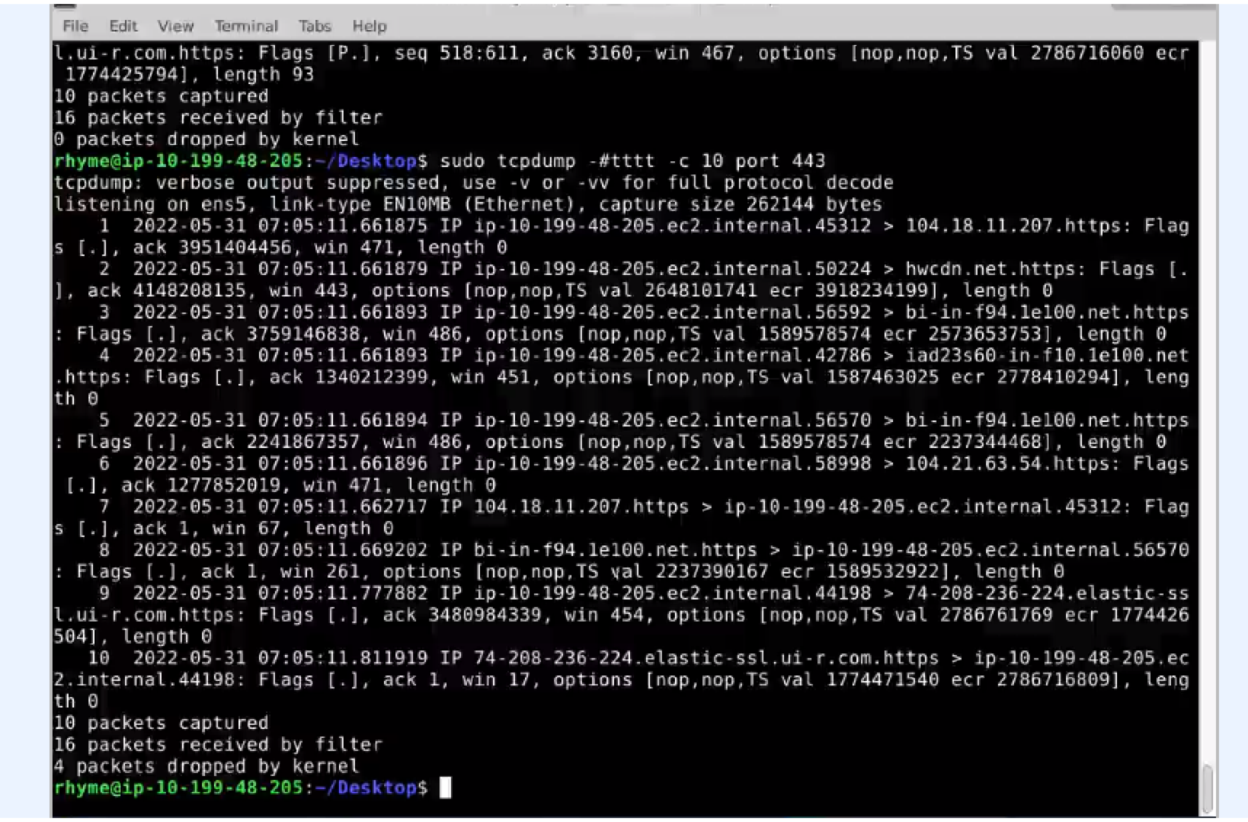
In this project, I learn how to use one of the most networking utilities, tcpdump, to capture and analyze TCP traffic.

- To gain administrative access to use tcpdump, sudo command should be used



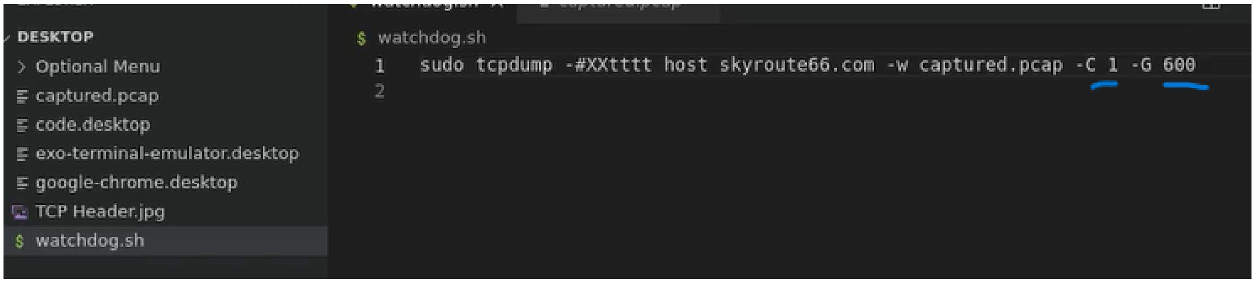
```
rhyme@ip-10-199-48-205:~/Desktop$ tcpdump
tcpdump: ens5: You don't have permission to capture on that device
(socket: Operation not permitted)
rhyme@ip-10-199-48-205:~/Desktop$ sudo tcpdump
```

- Captured 10 packets with numbering commanded out with timestamp commands to port 443



```
l.ui-r.com.https: Flags [P.], seq 518:611, ack 3160, win 467, options [nop,nop,TS val 2786716060 ecr
 1774425794], length 93
10 packets captured
16 packets received by filter
0 packets dropped by kernel
rhyme@ip-10-199-48-205:~/Desktop$ sudo tcpdump -#tttt -c 10 port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens5, link-type EN10MB (Ethernet), capture size 262144 bytes
    1  2022-05-31 07:05:11.661875 IP ip-10-199-48-205.ec2.internal.45312 > 104.18.11.207.https: Flag
s [.], ack 3951404456, win 471, length 0
    2  2022-05-31 07:05:11.661879 IP ip-10-199-48-205.ec2.internal.50224 > hwcdn.net.https: Flags [.
], ack 4148208135, win 443, options [nop,nop,TS val 2648101741 ecr 3918234199], length 0
    3  2022-05-31 07:05:11.661893 IP ip-10-199-48-205.ec2.internal.56592 > bi-in-f94.1e100.net.https
: Flags [.], ack 3759146838, win 486, options [nop,nop,TS val 1589578574 ecr 2573653753], length 0
    4  2022-05-31 07:05:11.661893 IP ip-10-199-48-205.ec2.internal.42786 > iad23s60-in-f10.1e100.net
.https: Flags [.], ack 1340212399, win 451, options [nop,nop,TS val 1587463025 ecr 2778410294], leng
th 0
    5  2022-05-31 07:05:11.661894 IP ip-10-199-48-205.ec2.internal.56570 > bi-in-f94.1e100.net.https
: Flags [.], ack 2241867357, win 486, options [nop,nop,TS val 1589578574 ecr 2237344468], length 0
    6  2022-05-31 07:05:11.661896 IP ip-10-199-48-205.ec2.internal.58998 > 104.21.63.54.https: Flags
 [.], ack 1277852019, win 471, length 0
    7  2022-05-31 07:05:11.662717 IP 104.18.11.207.https > ip-10-199-48-205.ec2.internal.45312: Flag
s [.], ack 1, win 67, length 0
    8  2022-05-31 07:05:11.669202 IP bi-in-f94.1e100.net.https > ip-10-199-48-205.ec2.internal.56570
: Flags [.], ack 1, win 261, options [nop,nop,TS val 2237390167 ecr 1589532922], length 0
    9  2022-05-31 07:05:11.777882 IP ip-10-199-48-205.ec2.internal.44198 > 74-208-236-224.elastic-ss
l.ui-r.com.https: Flags [.], ack 3480984339, win 454, options [nop,nop,TS val 2786761769 ecr 1774426
504], length 0
   10  2022-05-31 07:05:11.811919 IP 74-208-236-224.elastic-ssl.ui-r.com.https > ip-10-199-48-205.ec
2.internal.44198: Flags [.], ack 1, win 17, options [nop,nop,TS val 1774471540 ecr 2786716809], leng
th 0
10 packets captured
16 packets received by filter
4 packets dropped by kernel
rhyme@ip-10-199-48-205:~/Desktop$ 
```

- Created a sequence of dump files with size and time limits, this command will capture packets until 1million bytes or 10 minutes is performed.



```
sudo tcpdump -#XXtttt host skyroute66.com -w captured.pcap -C 1 -G 600
```