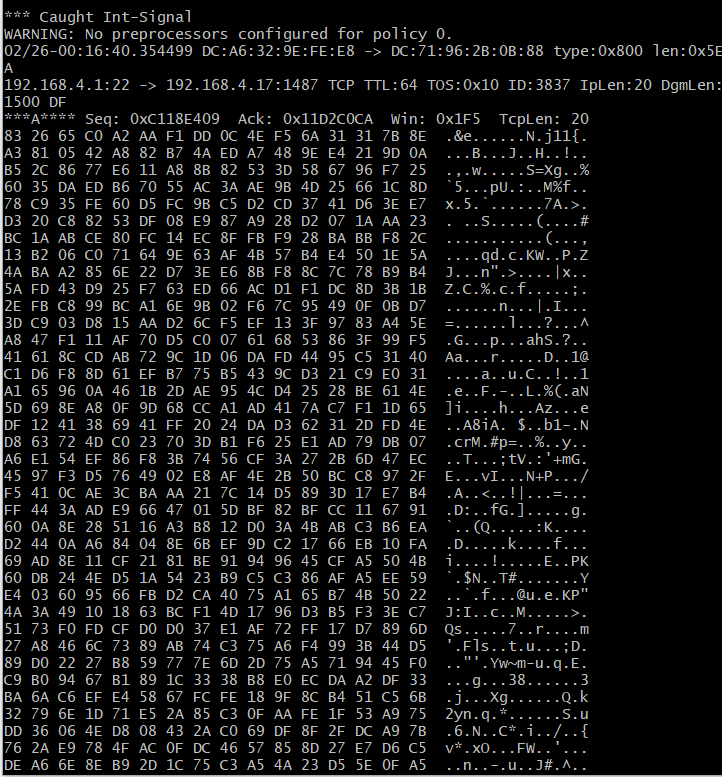
Task 1:

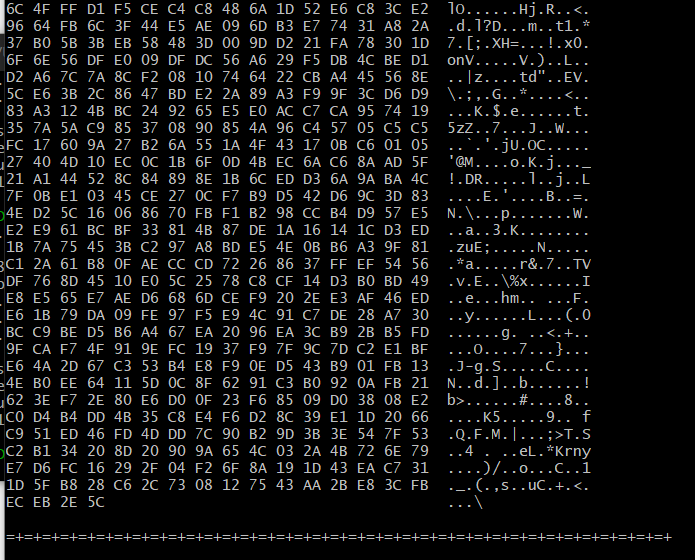
sudo snort -d -e -i wlan0

-d let you see the application data

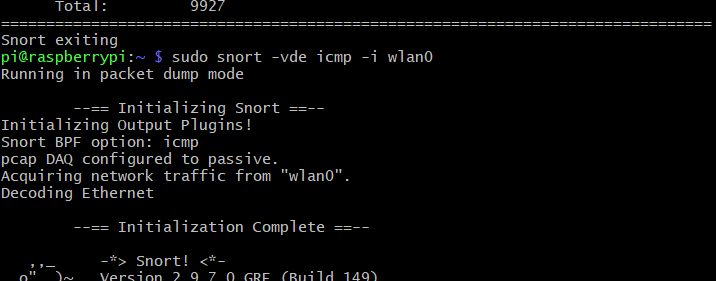
-e showing the data link layer headers

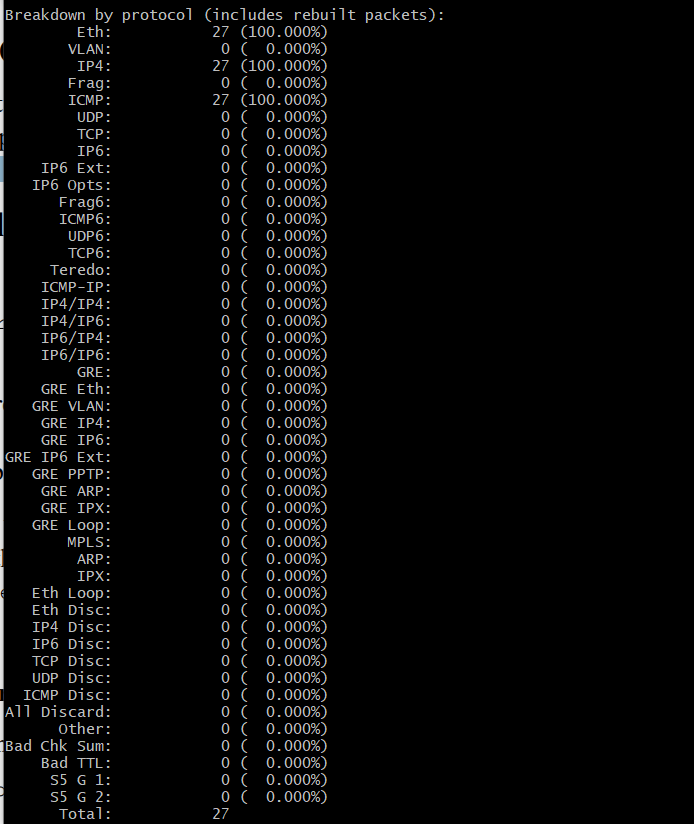




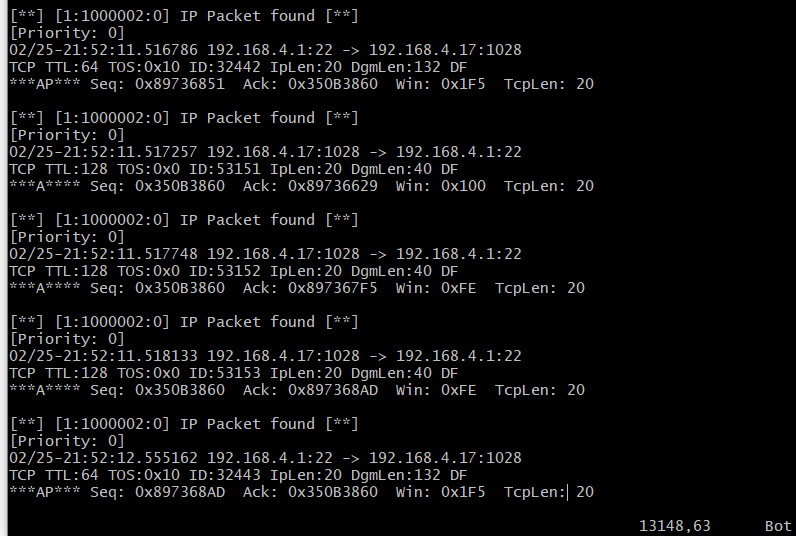
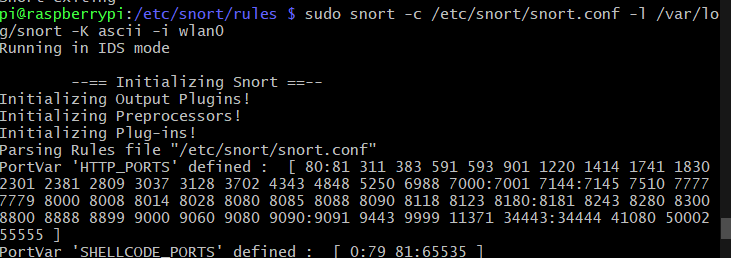


Task 2:





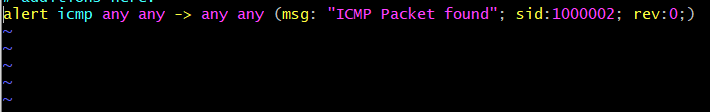
Task 3:



Yes , I see tons of “IP packet found”

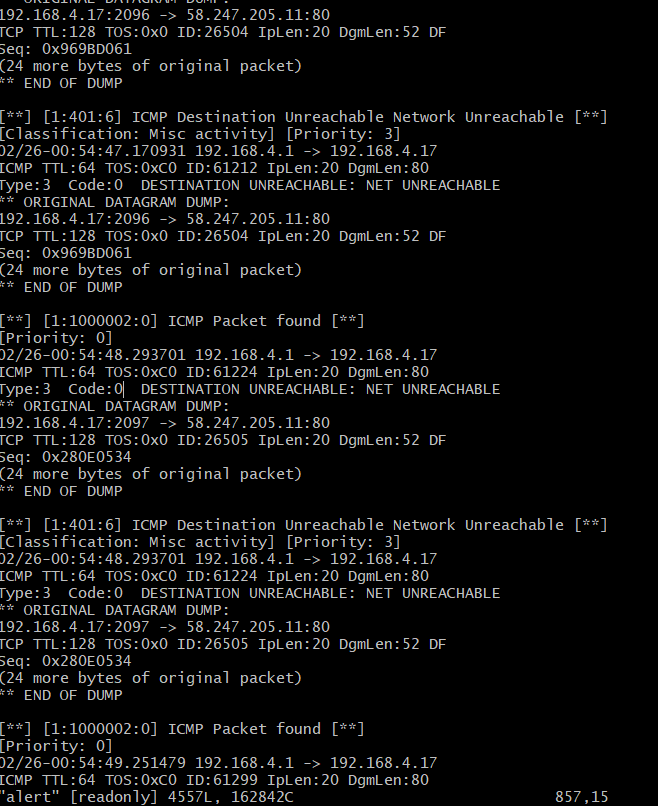
This rule will capture every IP packet. They are so many that it is different to find something wrong. Therefore, we can say that this rule is useless and it will waste the space of disk.

Task 4



I just change the previous command from “ip” to “icmp” , IP to ICMP





Task 5:

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 !:1024

it will alert every tcp traffic (except coming from 192.168.1.0/24) to 192.168.1.0/24 except send to port less and equal than 1024

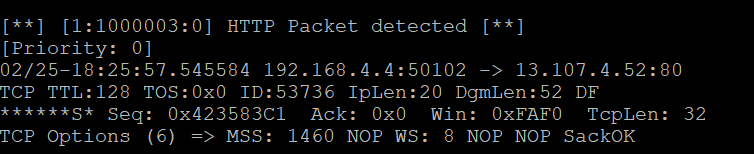
TASK 6: Alert on HTTP Get

Use this rule

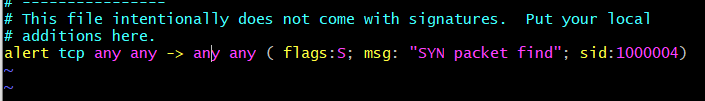


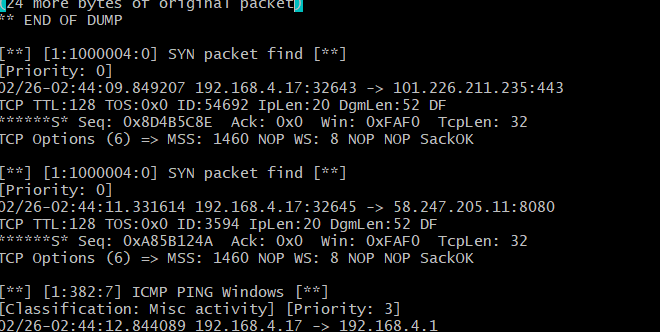
Run the same command





Task 7:





Task 8:

