# TASK 5

In this task we are going to capture and analyze network traffic using a tool called **WIRESHARK**

Wireshark is a tool that helps us capture and analyze individual packets that travel through a network, this is helpful in the field of cybersecurity as we can now monitor literally everything that is going on with our network. So let's see how the tool works:

1. But first let's install it using a simple command on linux: “ sudo apt install wireshark -y ”.
2. Now that wireshark has been installed on our device lets open it simply by typing wireshark on our terminal or opening it manualy through the application menu in linux. (I would suggest opening it trough the application menu since opening it through the terminal will cause it to shut down if you interrupt the terminal or close it)
3. After open the app the user interface looks something like in fig1

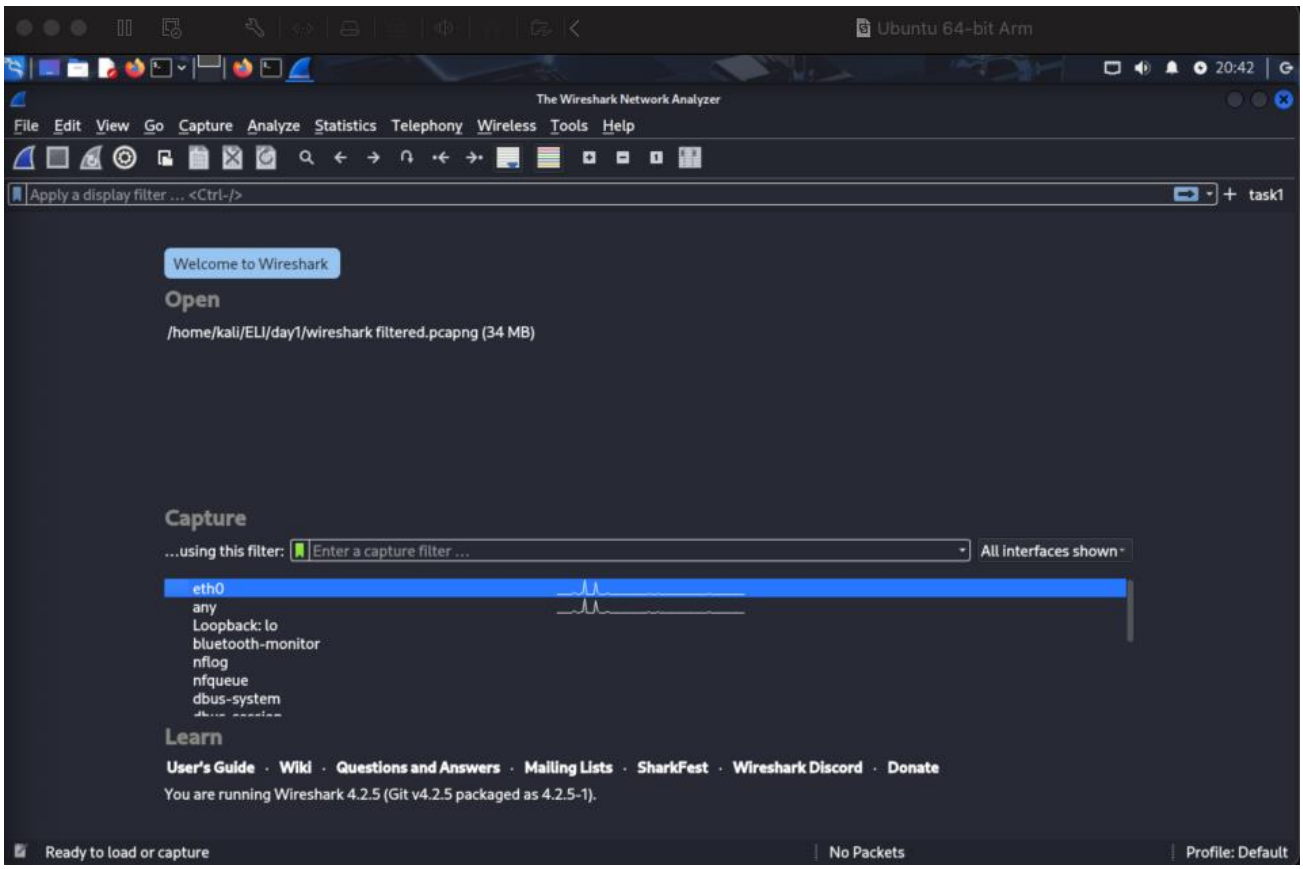


fig1

4. Now that you are in the home screen mkae sure you have selected eth0 (for ethernet) or wlan0 (for wifi) depending on what you are using and just press the blue button which says start capturing packets to start capturing packets

It should look something like this: fig2

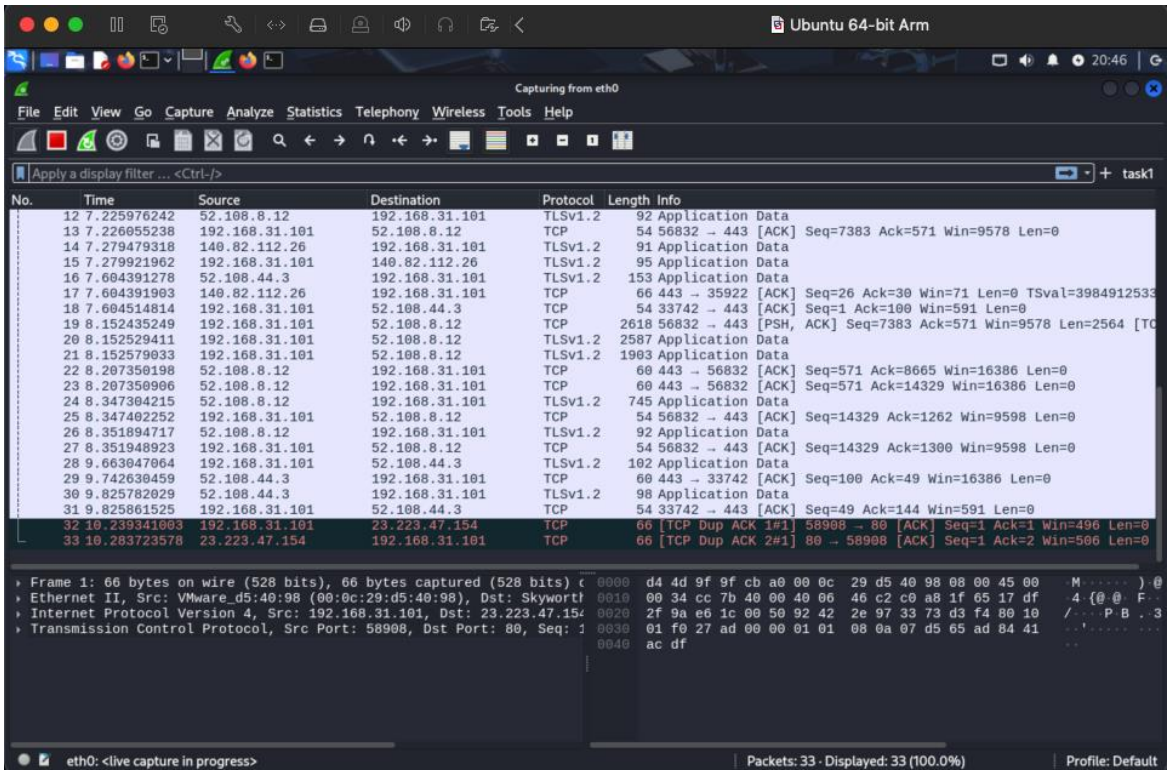


Fig2

5. Now just after you start the scan go back to your terminal and ping something to increase the number of packets you can capture the simple command should be: “ ping –c 4 google.com ” like in fig 3

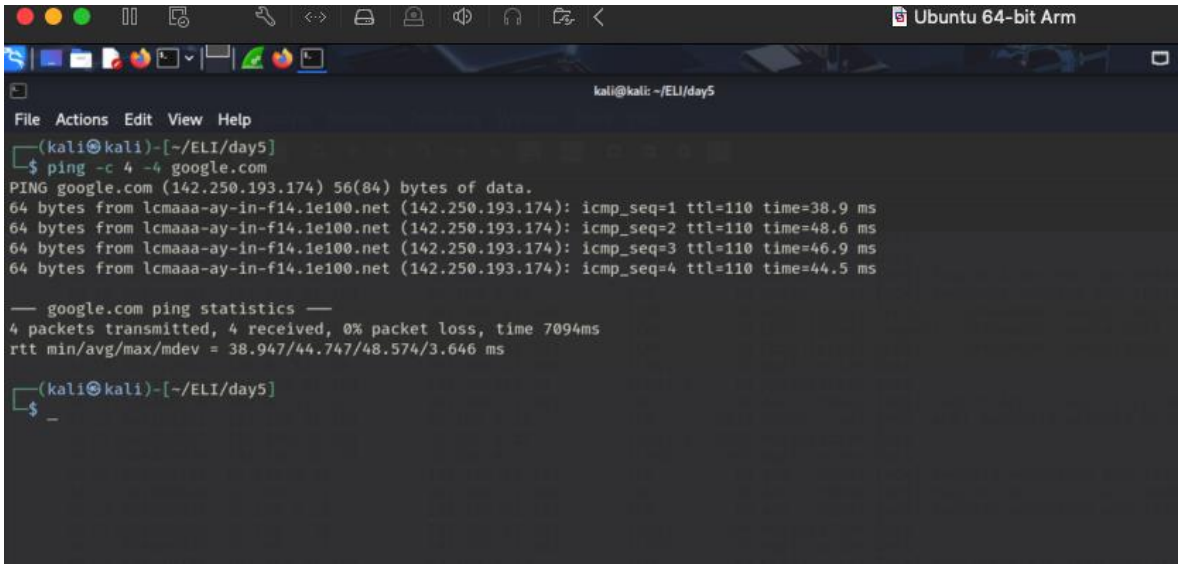


Fig 3

6. Then after the command finishes just stop the capture and go to the options>file>save_as>file_name to save the captured file so it is easy to analyze

7. Then comes the analysis process of it for this task we will be only analyzing based on 4 protocols but there is a lot more you can do with this tool but thats takes a lot of time.
    8. Firstly when you finish the capture your screen will loke something like this: fig4

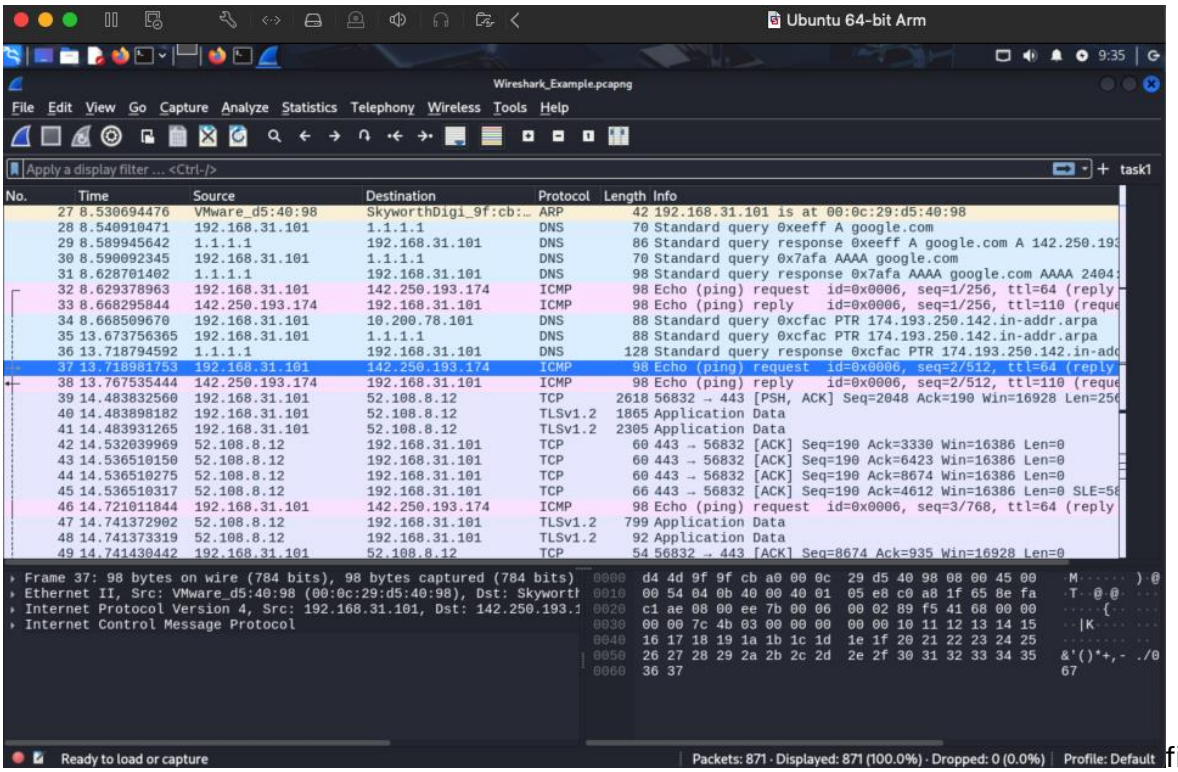

fig 4

9. Now to filter your packets based on protocols is realy simple, in the top menu click on bar that says apply a display filter and write the protocol shortform and it will be filtered for eg. Lets filter all the ICMP packets just by simply typing icmp and pressing enter : fig 5

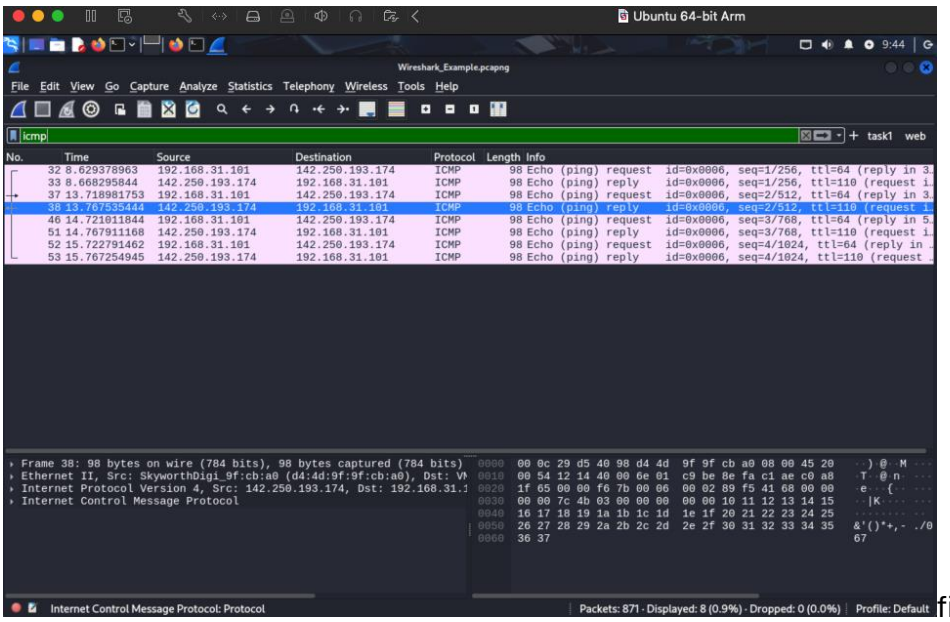

fig5

10. Now to save this specific filtered ranged output go to file select export specified packets and in that select packet range as displayed only so you only save the filtered pakets and give the file name and click save. Like in fig6

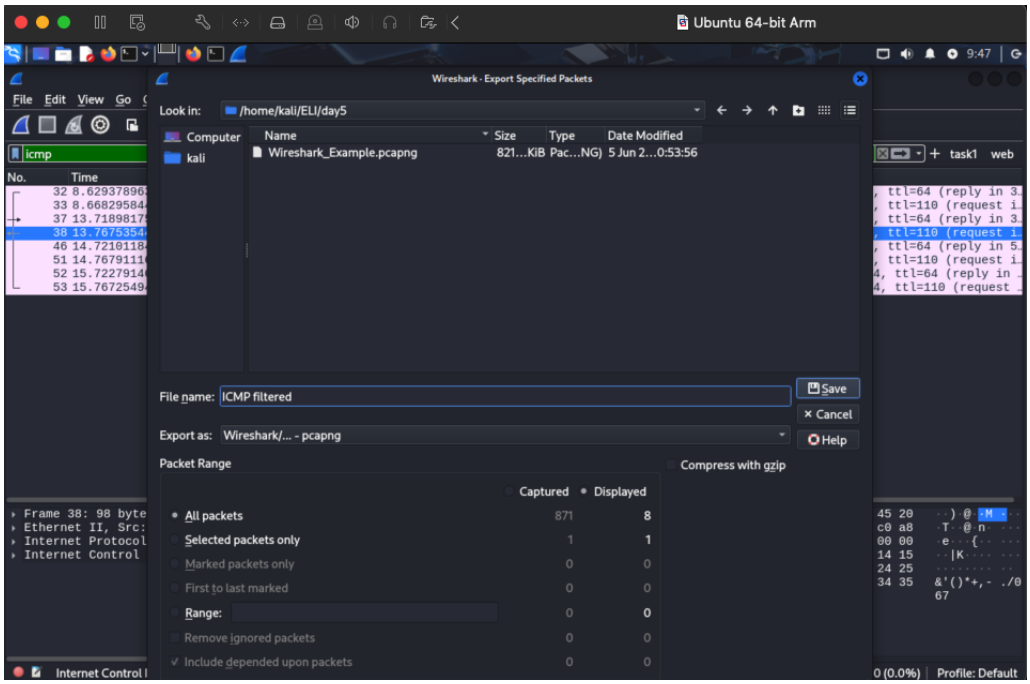


Fig 6

11. Now do thi with every protocol packet you want to and then lets see how to analyze them next:
12. Ok let's understand a little about the protocols we just filtered our wireshark_example.pcapng file
    - DNS: the protocol is DNS which is Domain name system which is used to allot domain names to their IP's and check if the selected domain name is present in the preconfigured DNS list or not
      Its port is 53
    - ICMP: the protocol is called internet control message protocol Its is mostly used for when we try to ping a website or traceroute it in our terminal which is mostly used by devices like routers to communicate.
      Its does use port rather it used type and code
      In short type and code are used for echo request and echo reply where 8 is echo request and 0 is echo reply.
    - TCP: TCP or rather transmission control protocol is one of the most used protocols and it's used case is really simple where it is a protocol that is used to establish a stable and secure connection between 2 devices/services, it's main part is the TCP handshake where the device A sends SYN and then device B sends SYN/ACK and the the sender again sends a ACK to establish a connection.

It has a lot of ports but the most common one's are 80,443 which is used by HTTP,HTTPS respectively.

- TLS: Transport layer security is a protocol that used TCP as its base and then enhances it for security purposes, it's simplest example would be the https protocol which uses the same method as http but does it more securly.
  THats the reason why majority of websites uses HTTPS instead of HTTP.
  Its port mostly is 443

Overall, the pakets I found on my network were nothing super detailed or fetch much information from it. The most important packet type on my network would maybe be ICMP since it is responsible for the network routing and trafficking.