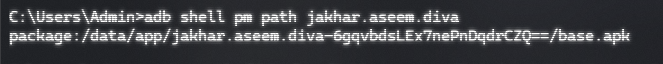
QARK

To analyse DIVA application using QARK we need the apk path first. To get the path using adb we will use adb shell pm path Jakhar.aseem.diva

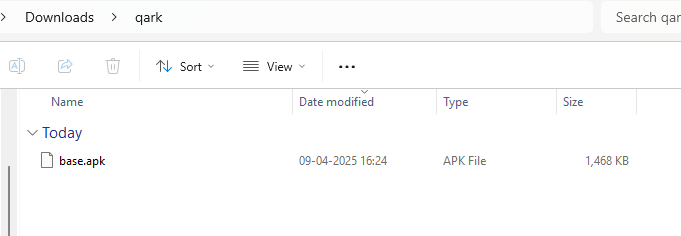


This will give us the complete apk path for DIVA apk.

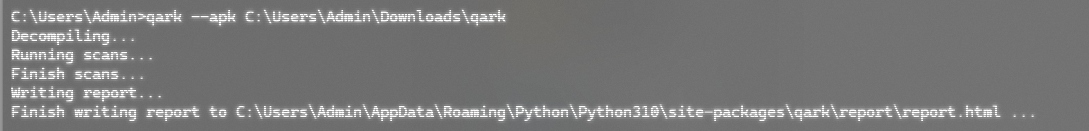
We will pull this apk to our local device or host device



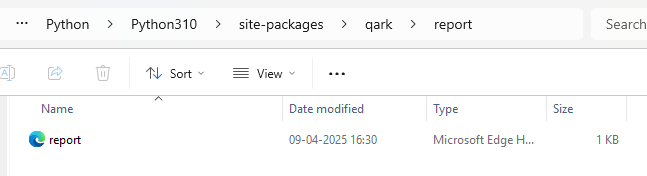
Once we pull the file we can view it manually in downloads folder in our system



Now using qark –apk command we can run a static analysis of our apk file by specifying the path in the command



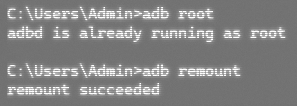
We can see that qark has generated an html page for the report of the analysis that was run on the apk



TCPDUMP

To run tcpdump in androd we will use adb as our cli.

We need to access adb as root first and remount it.

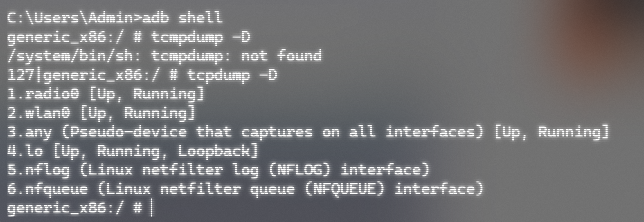


We will download tcpdump online and store it in our local host device

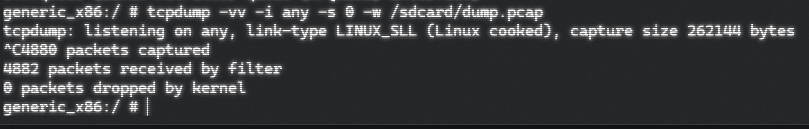
After downloading tcpdump, we will push this file to our emulator using adb



We will then enter the adb shell to run commands in android. We can see the list of processes that can be carried out using tcdump here

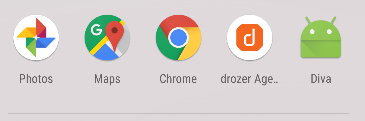


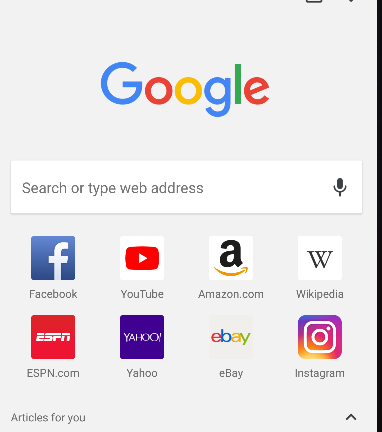
We will start capturing the network packets using the following commands and store it in sdcard as a pcap file using the following command



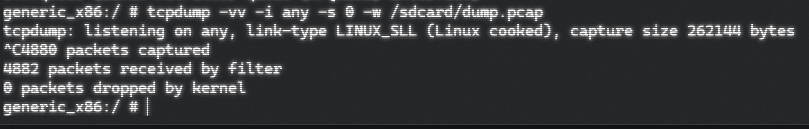
We will try to start an activity in our emulator to check if the packets are being captured

In this lab I have started chrome and visited YouTube

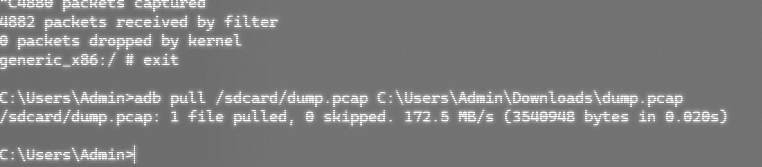




We will stop the process manually and see that we have received 4882 packet through our activity.



Now since this pcap file is in the emulator’s sdcard, we will need to pull it on our local host device. We can use add pull for this.



After pull the pcap file on out local host device we can manually view this in the folder we pulled the file in and view it in wireshark.

On analysing the packets, you can see that youtube activity has been captured in the packets.

