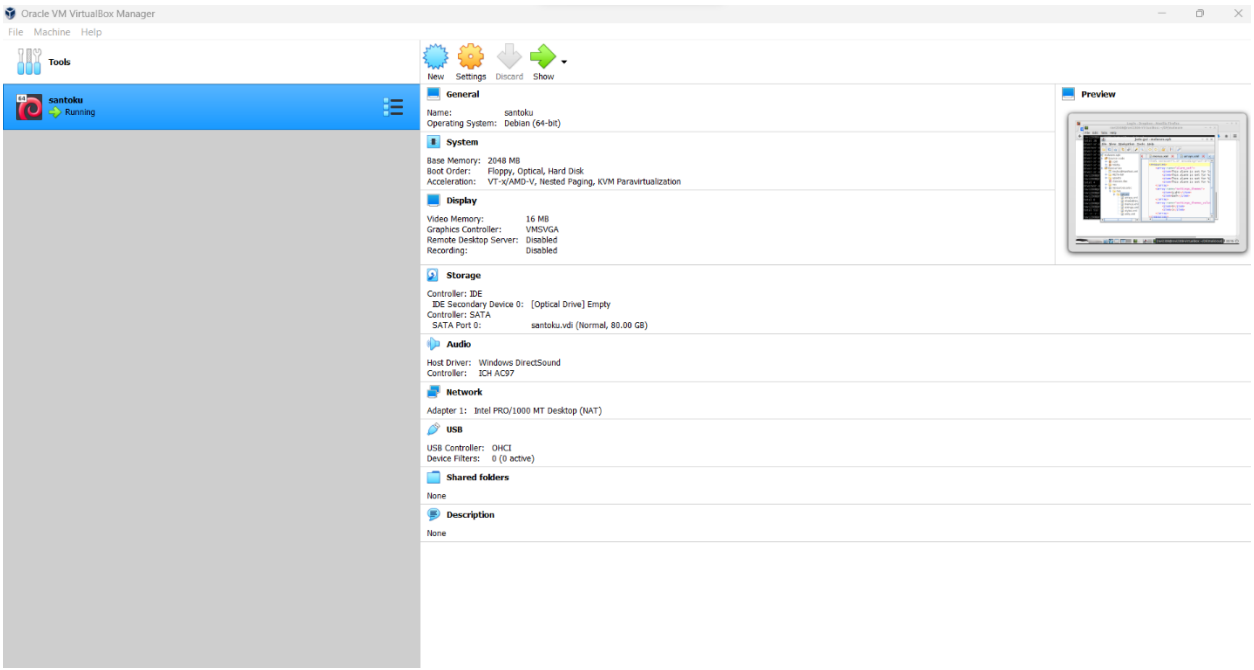
Malicious APK File Creation
No. 16

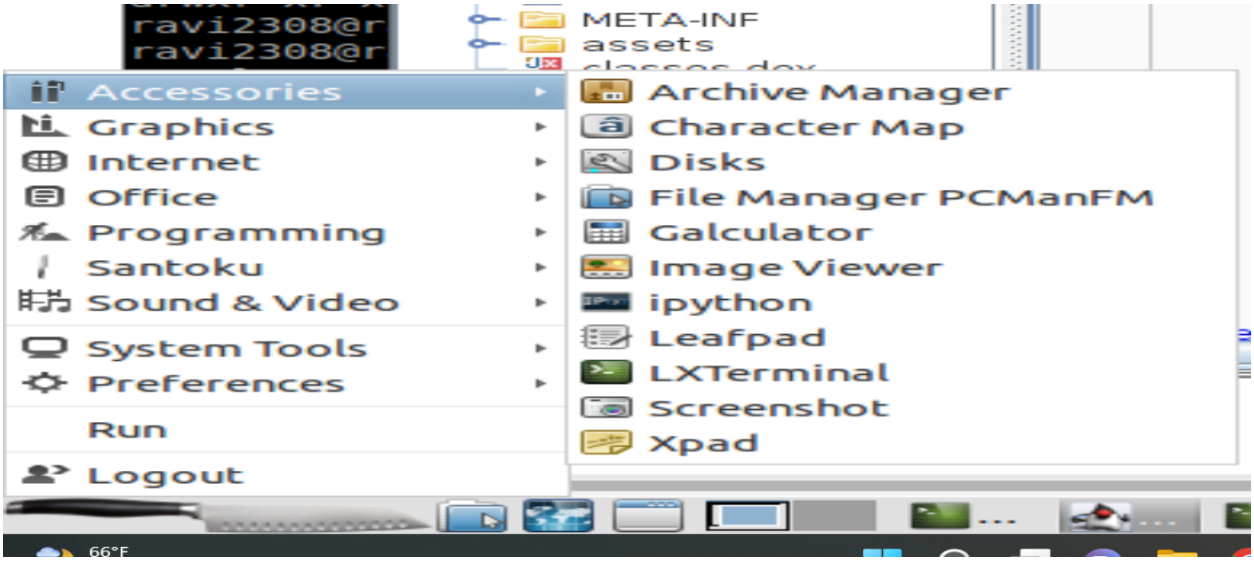
Creating a Malicious Android App using Santoku:

Download and install Virtual box in the system. Create a new virtual machine in virtual box and load the santoku disk image file which was downloaded before.

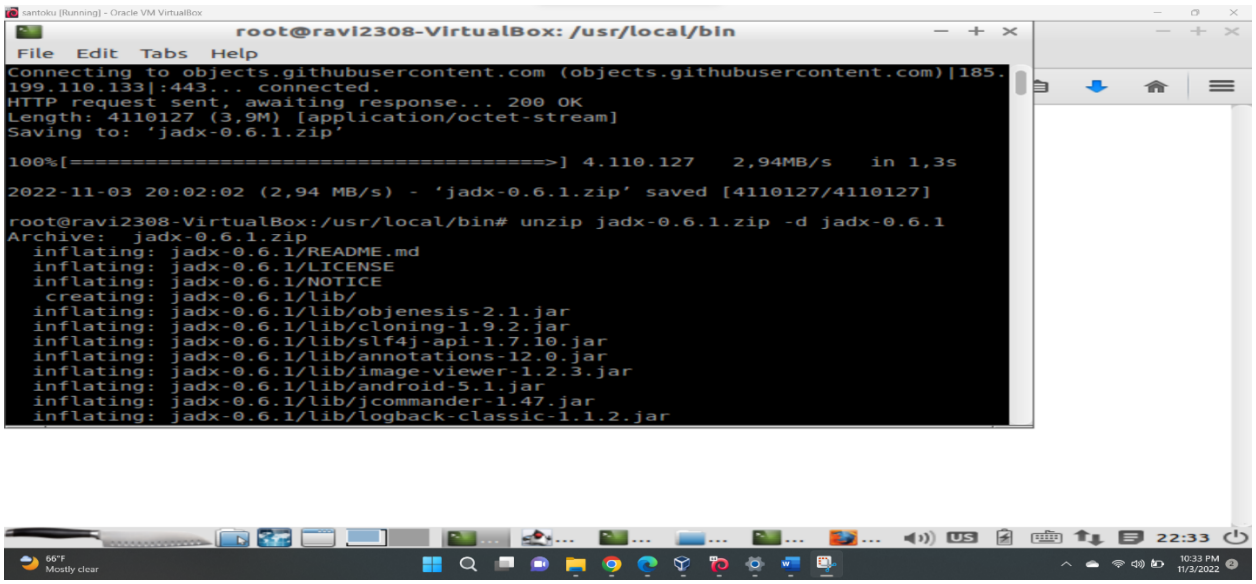
Below picture represents the specifications of the virtual machine:



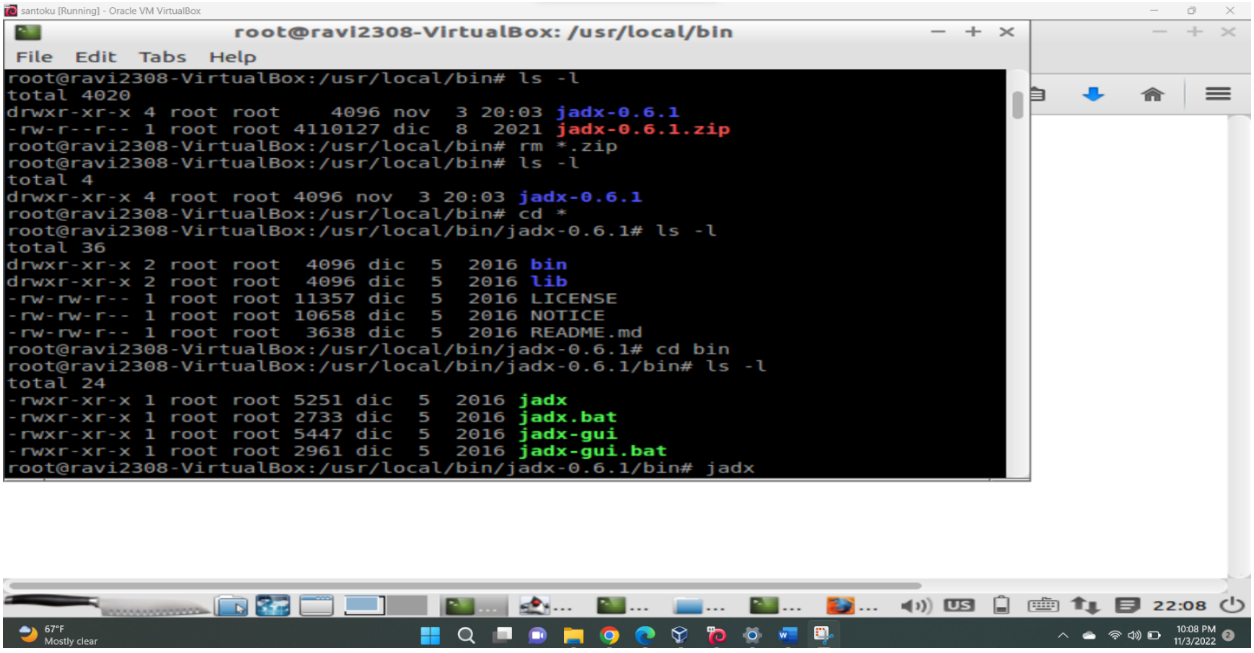
- Open the virtual machine and install Santoku in the virtual machine
- Go to Accessories and open ipython terminal

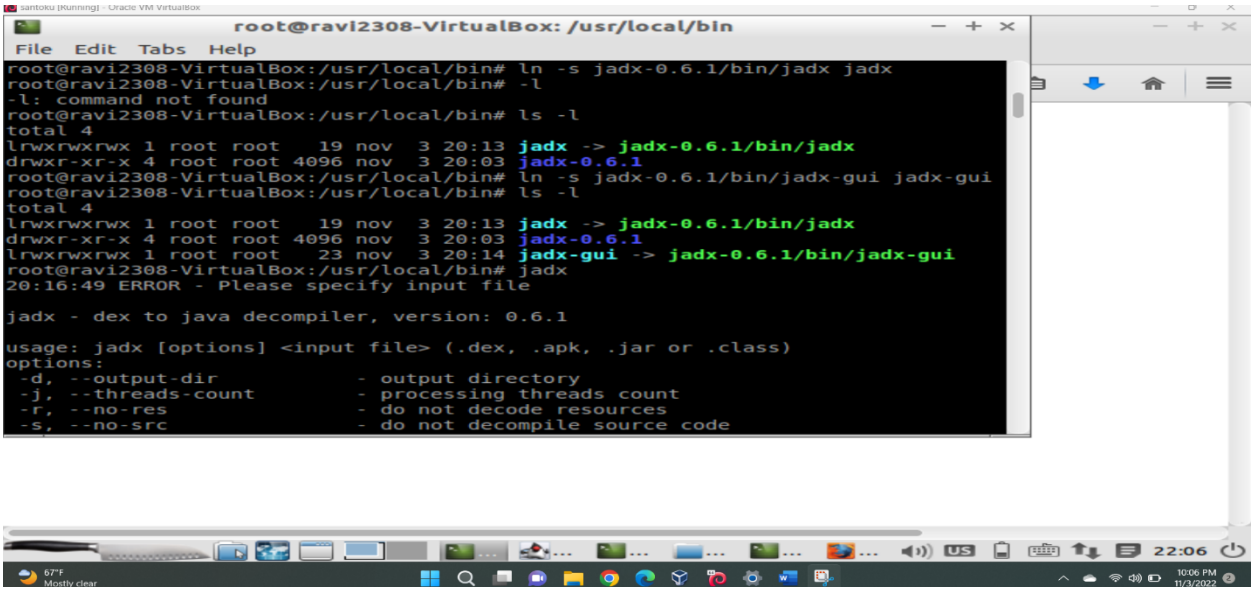


- After opening the ipython terminal using the commands unzip the jadx file
- Jadx is a DEX to Java decompiler

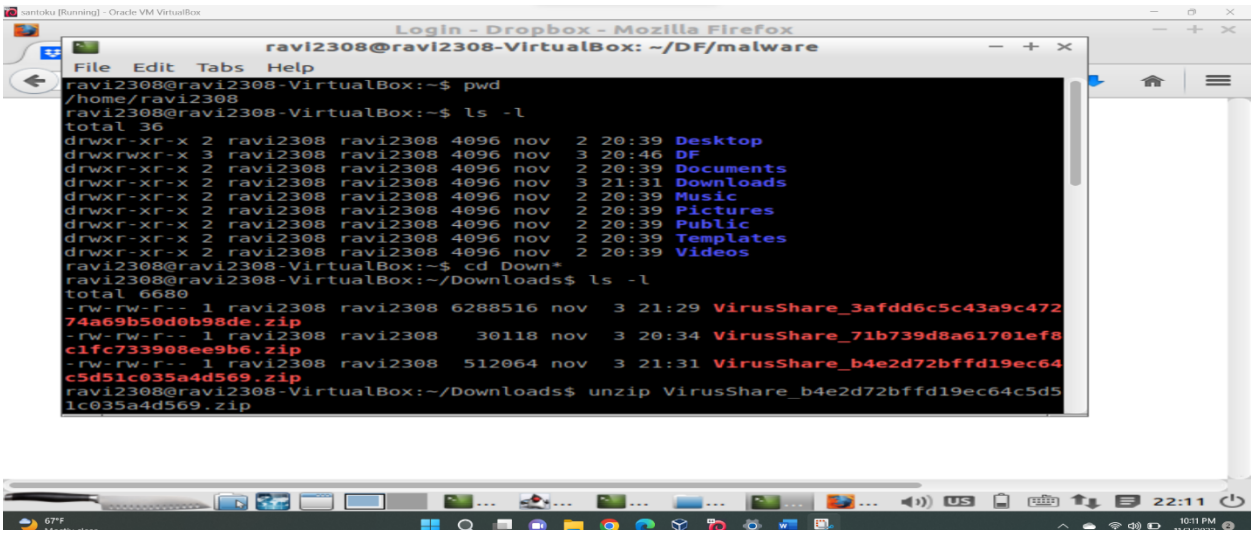


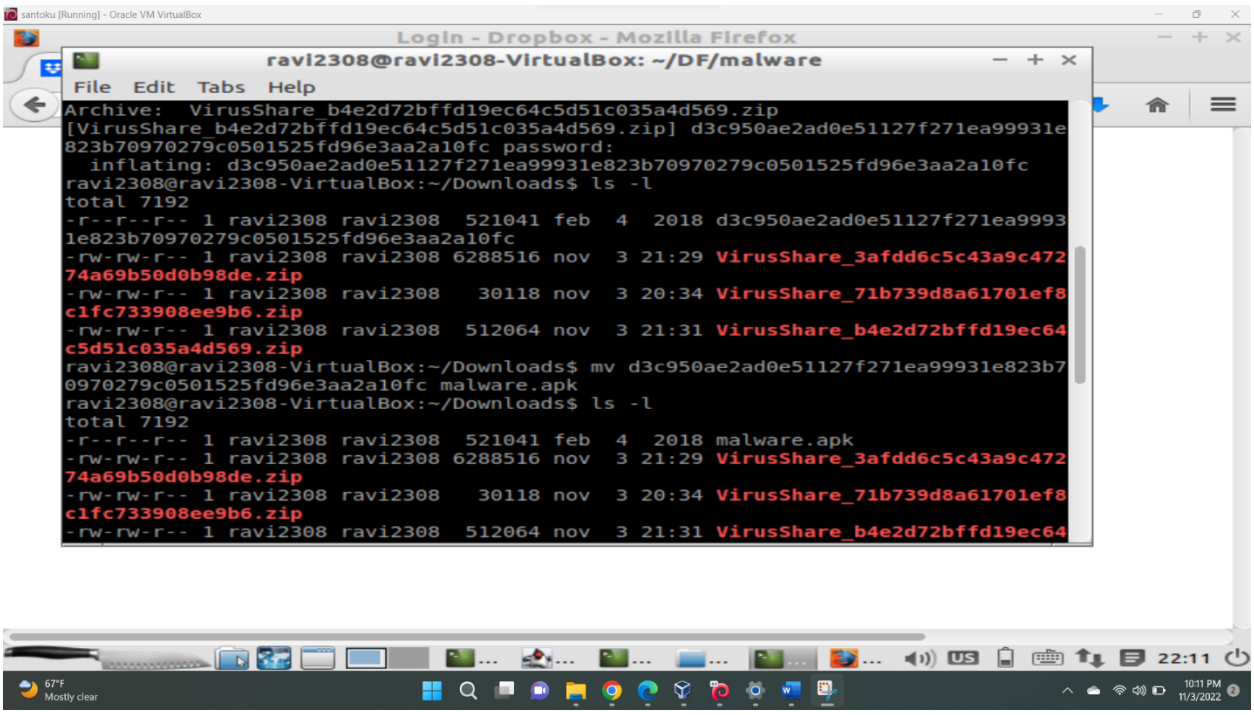
- After unzipping the file remove the zip and list the files



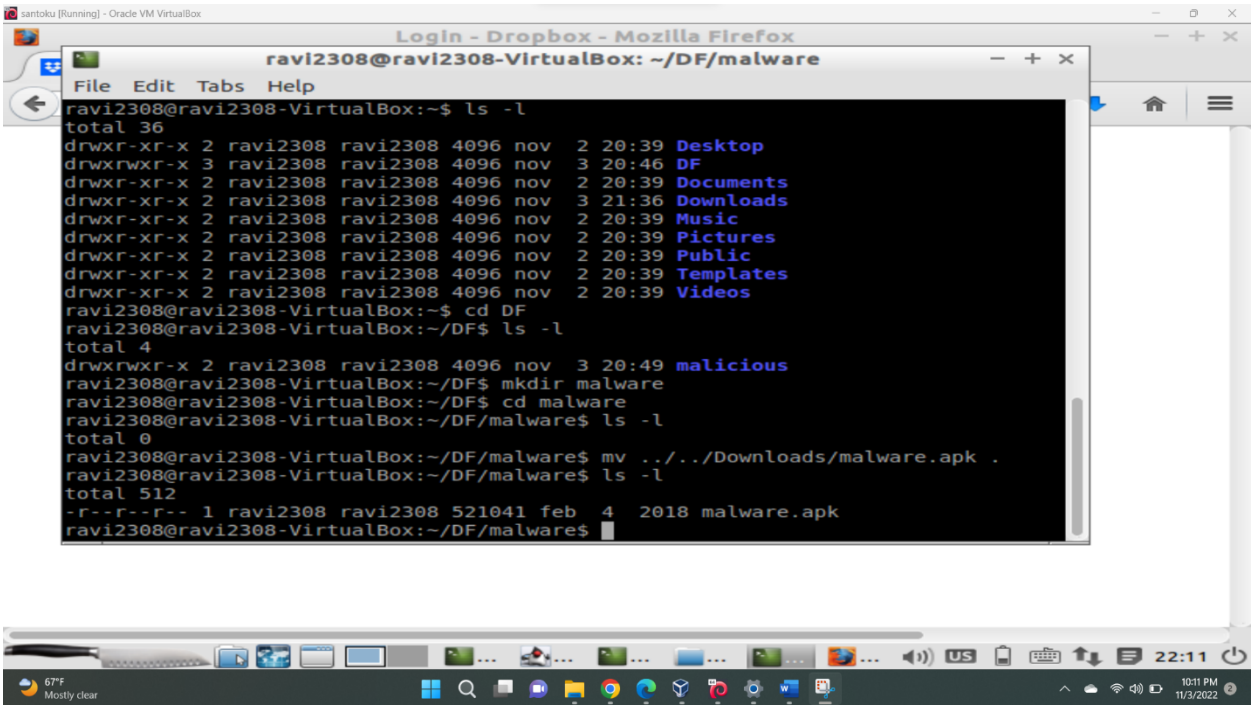


- Download a malicious apk file from the site virusshare.com
- After downloading the file unzip the file using unzip command

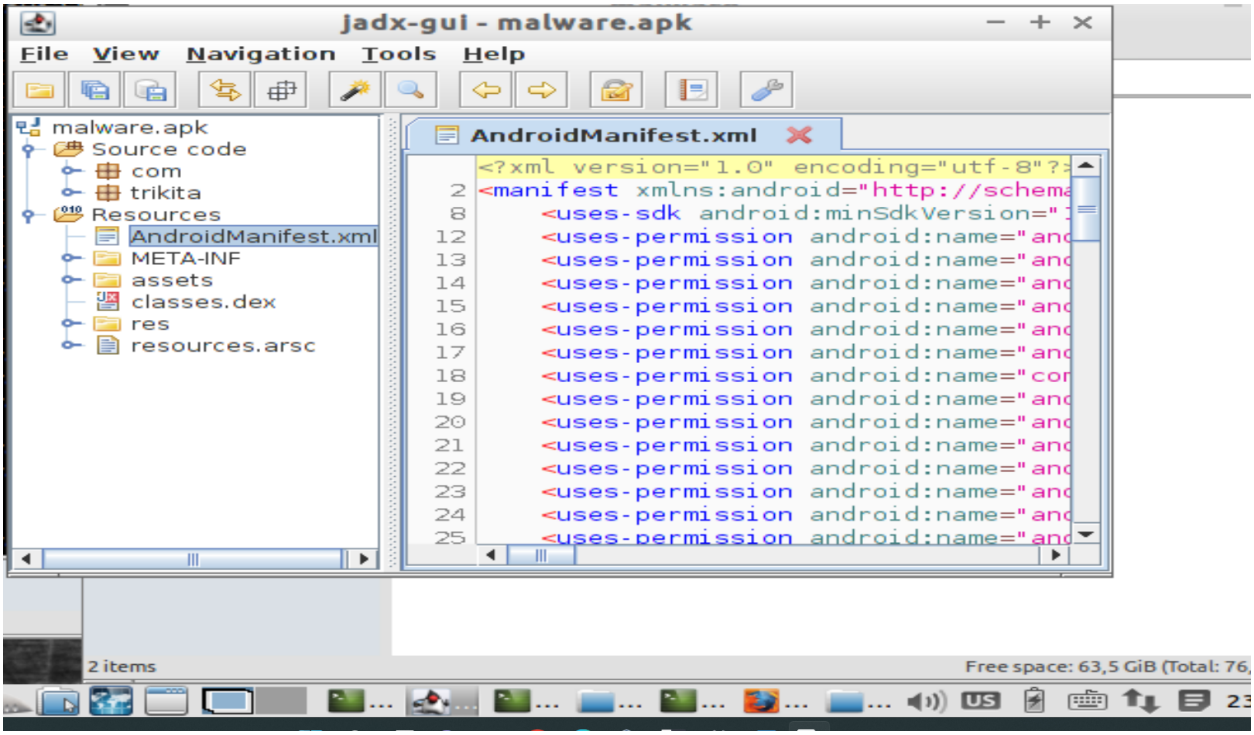




- After unzipping the file rename the file using mv command



- After opening the file, we will get the source code and resources used in the application



- In resources.arsc we have xml files