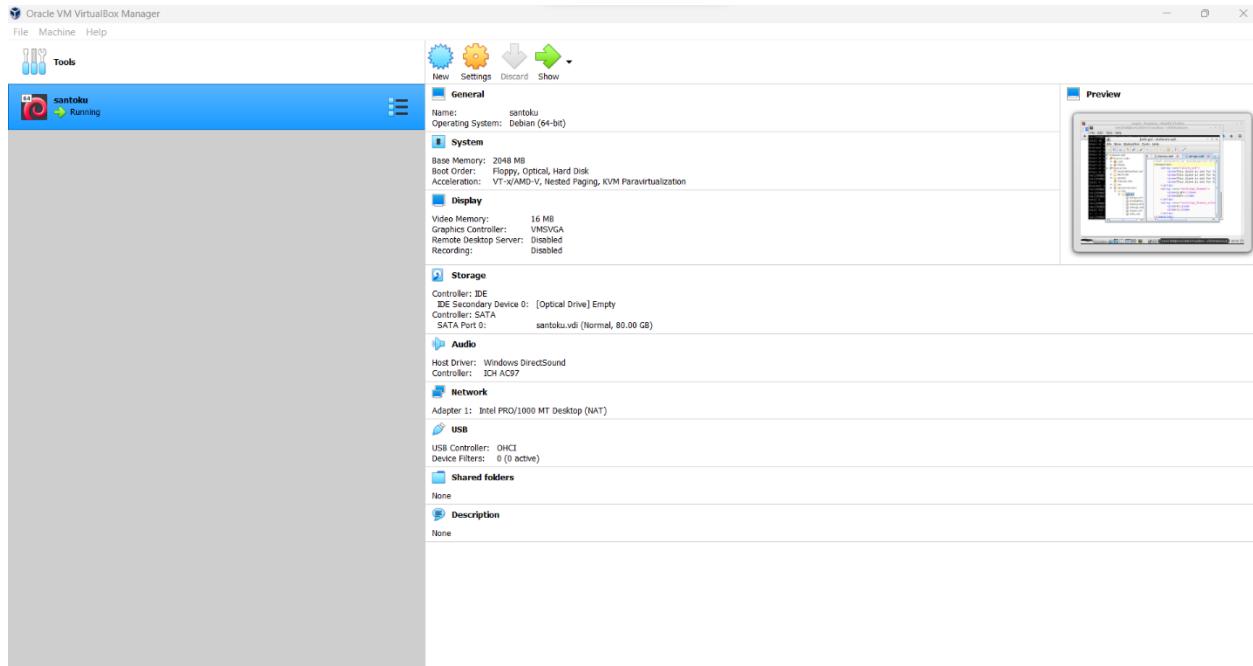


## Malicious APK File Creation No. 16

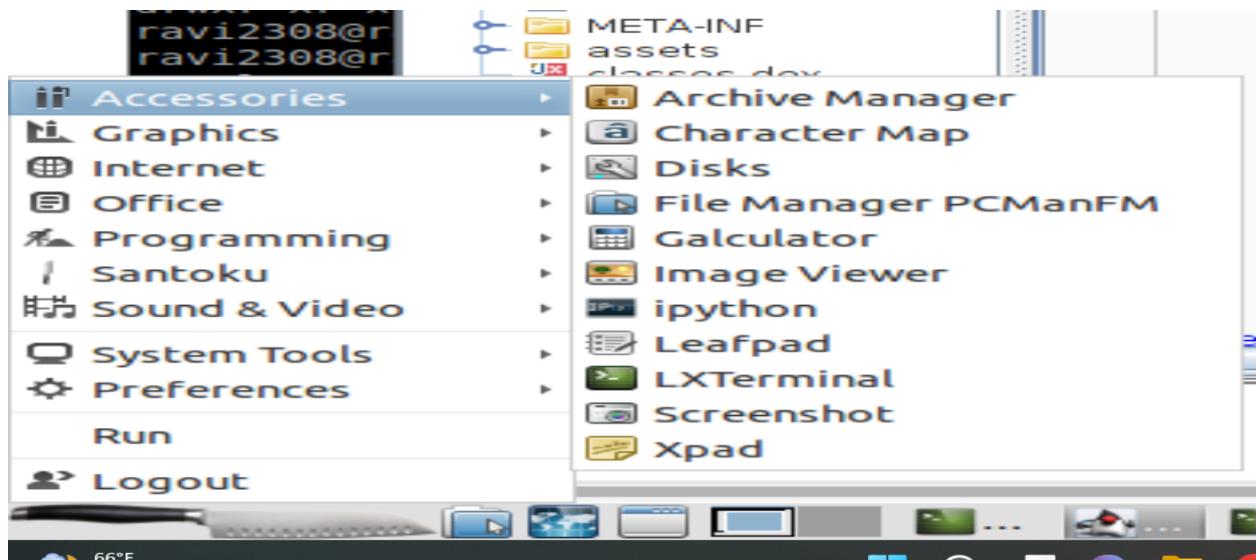
### **Creating a Malicious Android App using Santoku:**

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

```
santoku [Running] - Oracle VM VirtualBox
root@ravi2308-VirtualBox: /usr/local/bin
File Edit Tabs Help
Connecting to objects.githubusercontent.com (objects.githubusercontent.com) | 185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4110127 (3,9M) [application/octet-stream]
Saving to: 'jadx-0.6.1.zip'

100%[=====] 4.110.127 2,94MB/s in 1,3s
2022-11-03 20:02:02 (2,94 MB/s) - 'jadx-0.6.1.zip' saved [4110127/4110127]

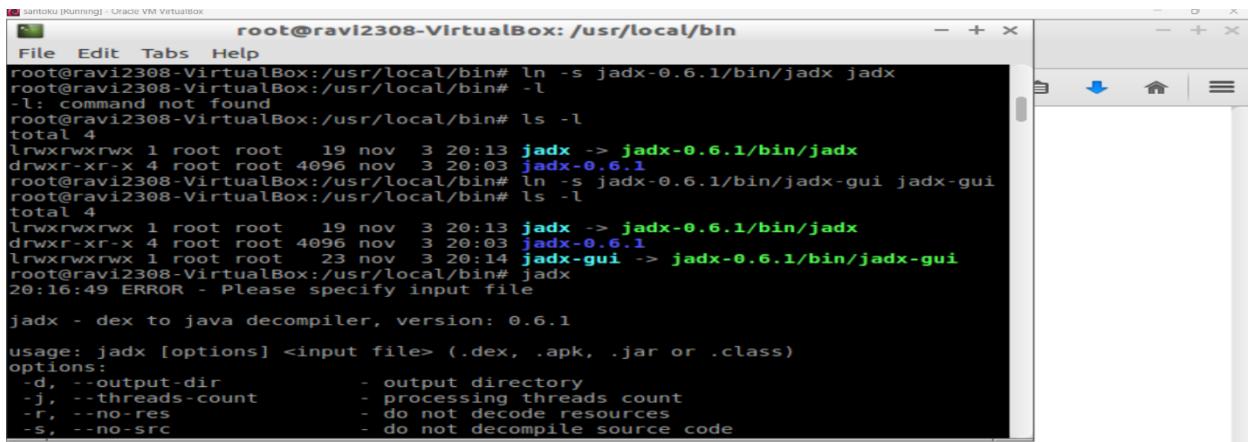
root@ravi2308-VirtualBox:/usr/local/bin# unzip jadx-0.6.1.zip -d jadx-0.6.1
Archive:  jadx-0.6.1.zip
  inflating: jadx-0.6.1/README.md
  inflating: jadx-0.6.1/LICENSE
  inflating: jadx-0.6.1/NOTICE
  creating: jadx-0.6.1/lib/
  inflating: jadx-0.6.1/lib/objenesis-2.1.jar
  inflating: jadx-0.6.1/lib/cloning-1.9.2.jar
  inflating: jadx-0.6.1/lib/slf4j-api-1.7.10.jar
  inflating: jadx-0.6.1/lib/annotations-12.0.jar
  inflating: jadx-0.6.1/lib/image-viewer-1.2.3.jar
  inflating: jadx-0.6.1/lib/android-5.1.jar
  inflating: jadx-0.6.1/lib/jcommander-1.47.jar
  inflating: jadx-0.6.1/lib/logback-classic-1.1.2.jar
```



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

```
santoku [Running] - Oracle VM VirtualBox
root@ravi2308-VirtualBox: /usr/local/bin
File Edit Tabs Help
root@ravi2308-VirtualBox:/usr/local/bin# ls -l
total 4020
drwxr-xr-x 4 root root 4096 nov  3 20:03 jadx-0.6.1
-rw-r--r-- 1 root root 4110127 dic  8 2021 jadx-0.6.1.zip
root@ravi2308-VirtualBox:/usr/local/bin# rm *.zip
root@ravi2308-VirtualBox:/usr/local/bin# ls -l
total 4
drwxr-xr-x 4 root root 4096 nov  3 20:03 jadx-0.6.1
root@ravi2308-VirtualBox:/usr/local/bin# cd *
root@ravi2308-VirtualBox:/usr/local/bin/jadx-0.6.1# ls -l
total 36
drwxr-xr-x 2 root root 4096 dic  5 2016 bin
drwxr-xr-x 2 root root 4096 dic  5 2016 lib
-rw-rw-r-- 1 root root 11357 dic  5 2016 LICENSE
-rw-rw-r-- 1 root root 10658 dic  5 2016 NOTICE
-rw-rw-r-- 1 root root 3638 dic  5 2016 README.md
root@ravi2308-VirtualBox:/usr/local/bin/jadx-0.6.1# cd bin
root@ravi2308-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# ls -l
total 24
-rwxr-xr-x 1 root root 5251 dic  5 2016 jadx
-rwxr-xr-x 1 root root 2733 dic  5 2016 jadx.bat
-rwxr-xr-x 1 root root 5447 dic  5 2016 jadx-gui
-rwxr-xr-x 1 root root 2961 dic  5 2016 jadx-gui.bat
root@ravi2308-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# jadx
```





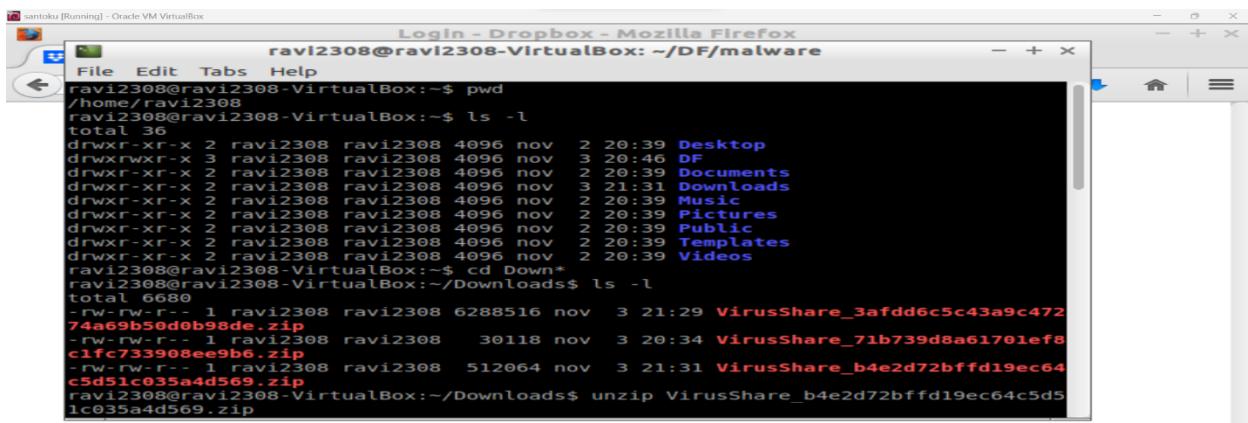
```
santoku [Running] - Oracle VM VirtualBox
root@ravi2308-VirtualBox: /usr/local/bin
File Edit Tabs Help
root@ravi2308-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx jadx
root@ravi2308-VirtualBox:/usr/local/bin# -l
-l: command not found
root@ravi2308-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 nov 3 20:13 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 nov 3 20:03 jadx-0.6.1
root@ravi2308-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx-gui jadx-gui
root@ravi2308-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 nov 3 20:13 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 nov 3 20:03 jadx-0.6.1
lrwxrwxrwx 1 root root 23 nov 3 20:14 jadx-gui -> jadx-0.6.1/bin/jadx-gui
root@ravi2308-VirtualBox:/usr/local/bin# jadx
20:16:49 ERROR - Please specify input file

jadx - dex to java decompiler, version: 0.6.1

usage: jadx [options] <input file> (.dex, .apk, .jar or .class)
options:
-d, --output-dir           - output directory
-j, --threads-count        - processing threads count
-r, --no-res                - do not decode resources
-s, --no-src                - do not decompile source code
```

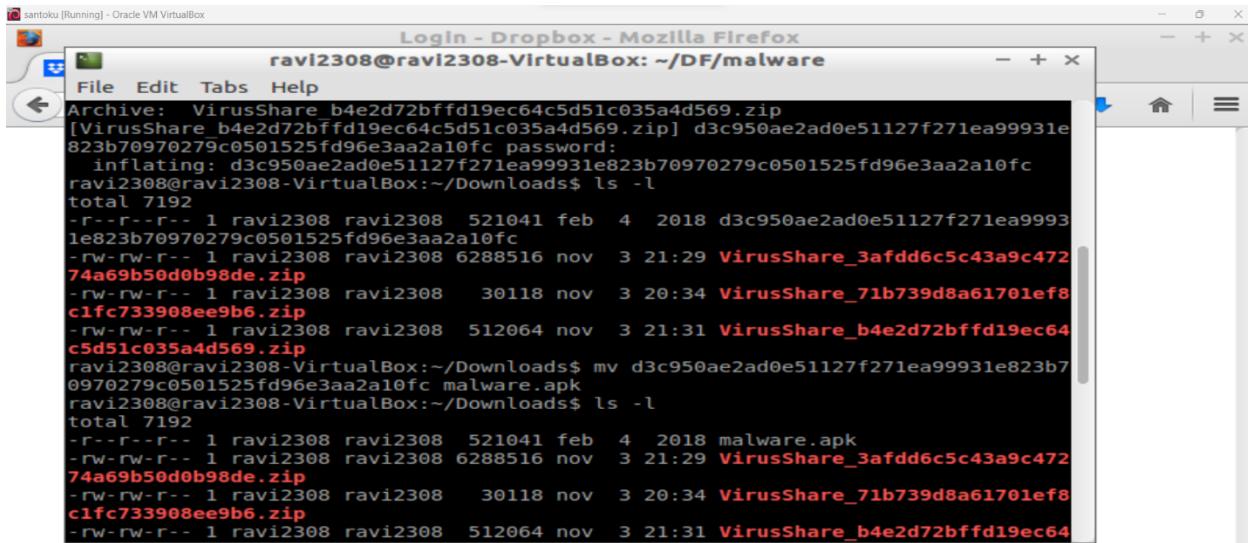


- Download a malicious apk file from the site virusshare.com
- After downloading the file unzip the file using unzip command



```
santoku [Running] - Oracle VM VirtualBox
Login - Dropbox - Mozilla Firefox
ravi2308@ravi2308-VirtualBox: ~/DF/malware
File Edit Tabs Help
ravi2308@ravi2308-VirtualBox:~$ pwd
/home/ravi2308
ravi2308@ravi2308-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Desktop
drwxrwxr-x 3 ravi2308 ravi2308 4096 nov 3 20:46 DF
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Documents
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 3 21:31 Downloads
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Music
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Pictures
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Public
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Templates
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov 2 20:39 Videos
ravi2308@ravi2308-VirtualBox:~$ cd Downloads
ravi2308@ravi2308-VirtualBox:~/Downloads$ ls -l
total 6680
-rw-rw-r-- 1 ravi2308 ravi2308 6288516 nov 3 21:29 VirusShare_3afdd6c5c43a9c472
74a69b50d0b98de.zip
-rw-rw-r-- 1 ravi2308 ravi2308 30118 nov 3 20:34 VirusShare_71b739d8a61701ef8
c1fc733908ee9b6.zip
-rw-rw-r-- 1 ravi2308 ravi2308 512064 nov 3 21:31 VirusShare_b4e2d72bffd19ec64
c5d51c035a4d569.zip
ravi2308@ravi2308-VirtualBox:~/Downloads$ unzip VirusShare_b4e2d72bffd19ec64c5d5
1c035a4d569.zip
```

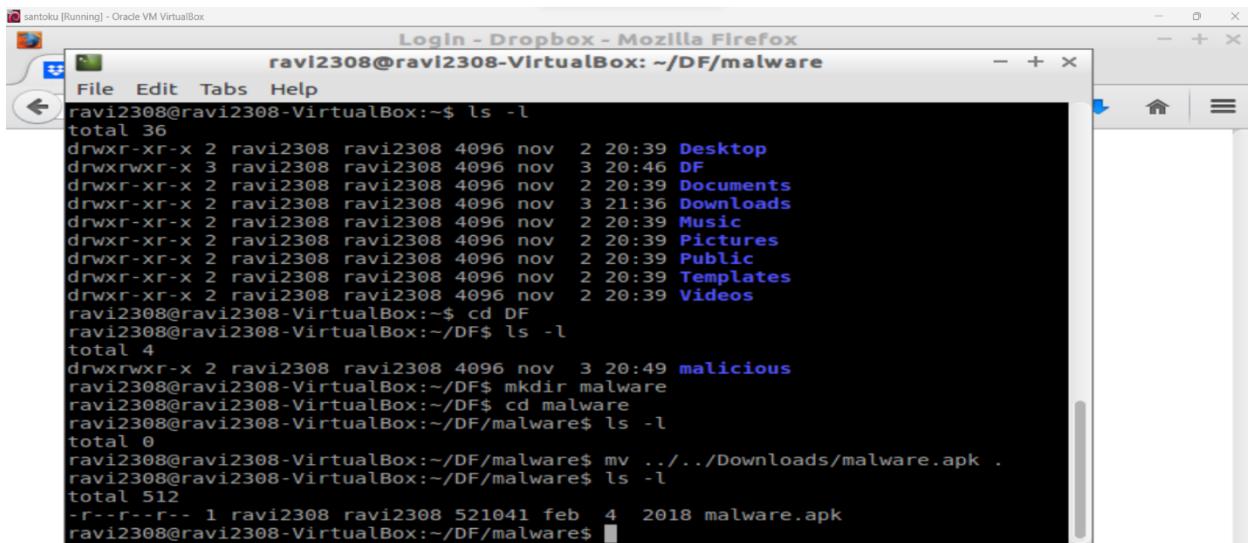




```
ravi2308@ravi2308-VirtualBox: ~/DF/malware
Archive: VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
[VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip] d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc password:
inflating: d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
ravi2308@ravi2308-VirtualBox:~/Downloads$ ls -l
total 7192
-r--r--r-- 1 ravi2308 ravi2308 521041 feb  4 2018 d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
-rw-rw-r-- 1 ravi2308 ravi2308 6288516 nov  3 21:29 VirusShare_3afdd6c5c43a9c47274a69b50d0b98de.zip
-rw-rw-r-- 1 ravi2308 ravi2308 30118 nov  3 20:34 VirusShare_71b739d8a61701ef8c1fc733908ee9b6.zip
-rw-rw-r-- 1 ravi2308 ravi2308 512064 nov  3 21:31 VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
ravi2308@ravi2308-VirtualBox:~/Downloads$ mv d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc malware.apk
ravi2308@ravi2308-VirtualBox:~/Downloads$ ls -l
total 7192
-r--r--r-- 1 ravi2308 ravi2308 521041 feb  4 2018 malware.apk
-rw-rw-r-- 1 ravi2308 ravi2308 6288516 nov  3 21:29 VirusShare_3afdd6c5c43a9c47274a69b50d0b98de.zip
-rw-rw-r-- 1 ravi2308 ravi2308 30118 nov  3 20:34 VirusShare_71b739d8a61701ef8c1fc733908ee9b6.zip
-rw-rw-r-- 1 ravi2308 ravi2308 512064 nov  3 21:31 VirusShare_b4e2d72bffd19ec64
```



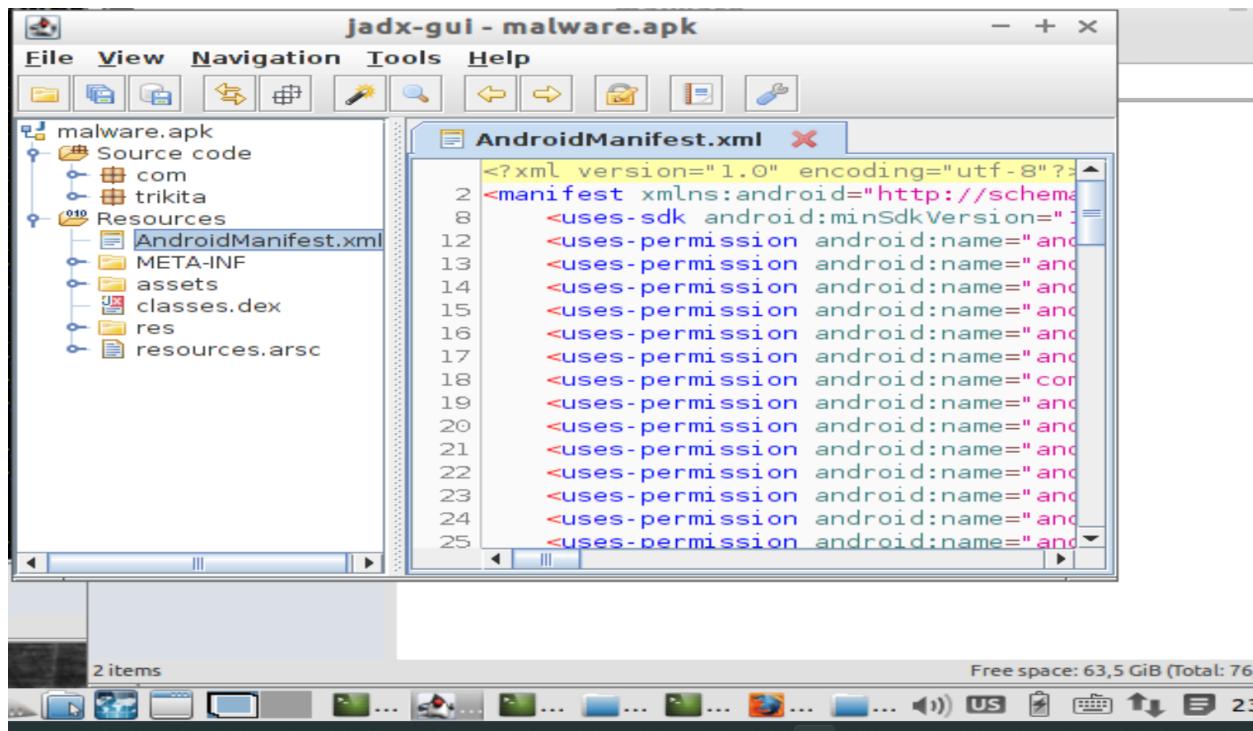
- After unzipping the file rename the file using mv command



```
ravi2308@ravi2308-VirtualBox: ~$ ls -l
total 36
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Desktop
drwxrwxr-x 3 ravi2308 ravi2308 4096 nov  3 20:46 DF
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Documents
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  3 21:36 Downloads
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Music
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Pictures
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Public
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Templates
drwxr-xr-x 2 ravi2308 ravi2308 4096 nov  2 20:39 Videos
ravi2308@ravi2308-VirtualBox: ~$ cd DF
ravi2308@ravi2308-VirtualBox: ~/DF$ ls -l
total 4
drwxrwxr-x 2 ravi2308 ravi2308 4096 nov  3 20:49 malicious
ravi2308@ravi2308-VirtualBox: ~/DF$ mkdir malware
ravi2308@ravi2308-VirtualBox: ~/DF$ cd malware
ravi2308@ravi2308-VirtualBox: ~/DF/malware$ ls -l
total 0
ravi2308@ravi2308-VirtualBox: ~/DF/malware$ mv ../../Downloads/malware.apk .
ravi2308@ravi2308-VirtualBox: ~/DF/malware$ ls -l
total 512
-r--r--r-- 1 ravi2308 ravi2308 521041 feb  4 2018 malware.apk
ravi2308@ravi2308-VirtualBox: ~/DF/malware$
```



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



- In resources.arsc we have xml files

