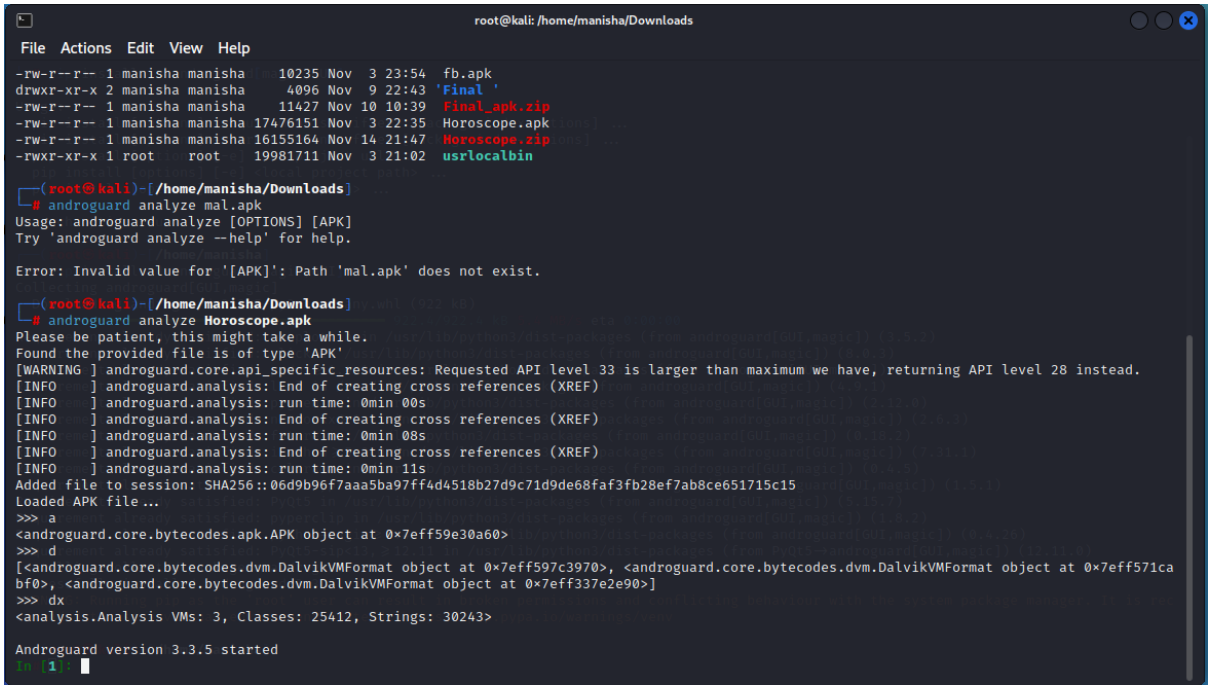
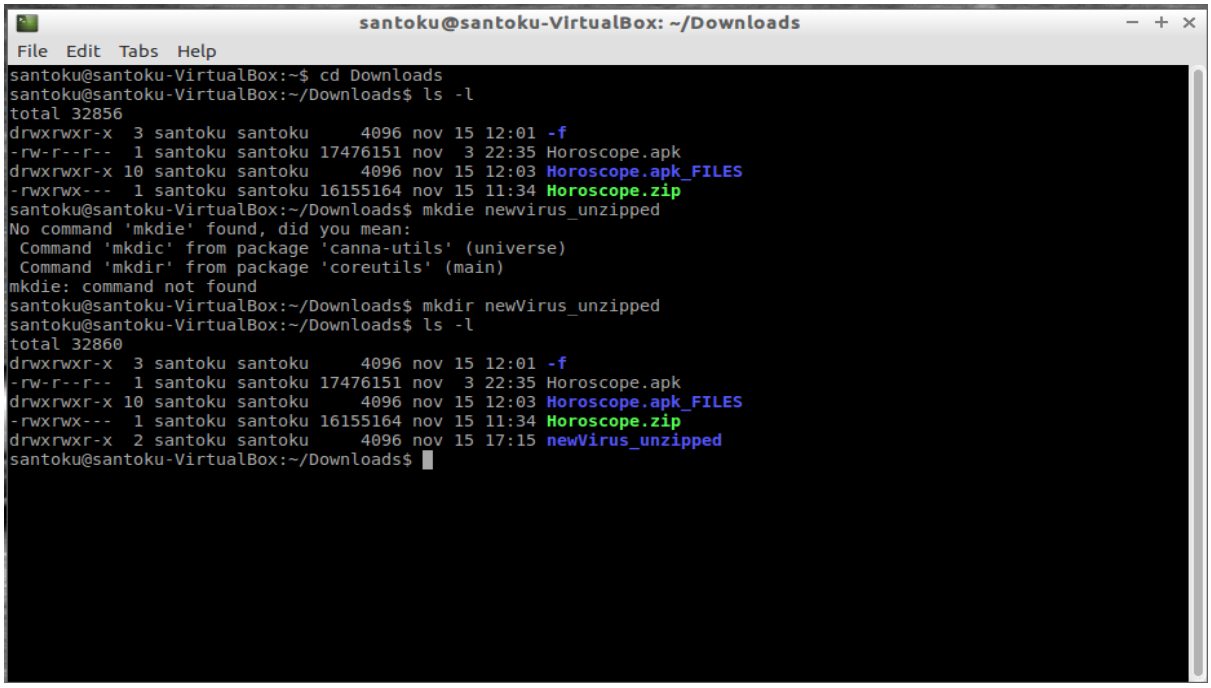
Malicious APK File Analysis
No. 17

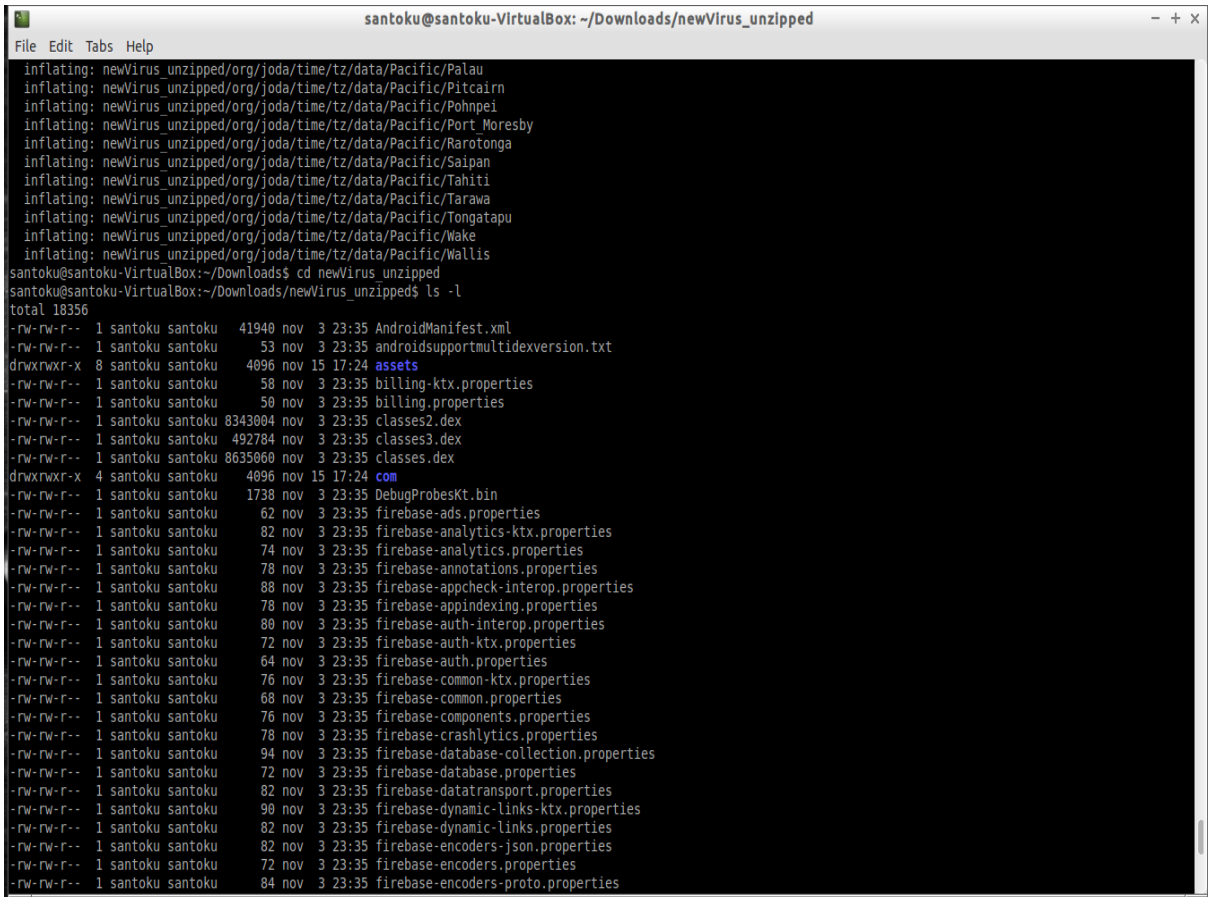
We use androgurd to analyse given Horoscope.apk from group 17.



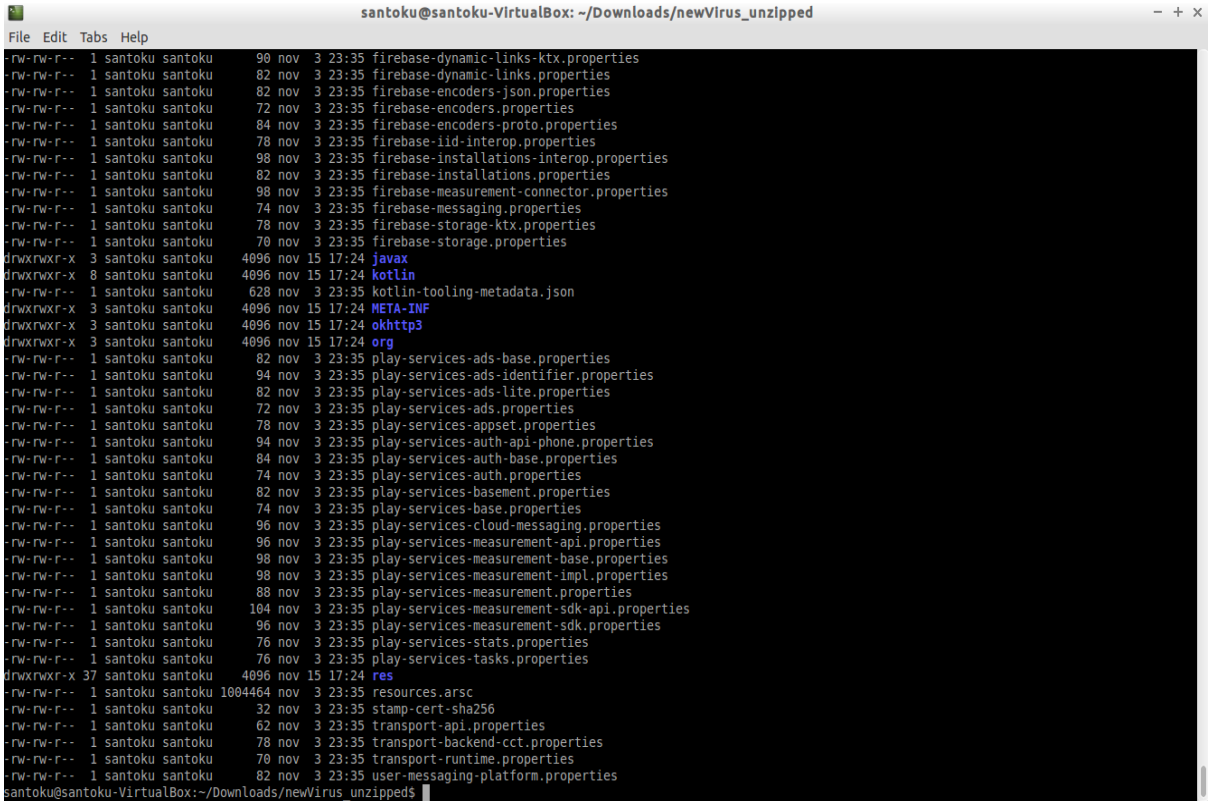
By using androgurd we find the android version ,android resources ,android applications icon ,android applications name and which are the permissions for android applications.

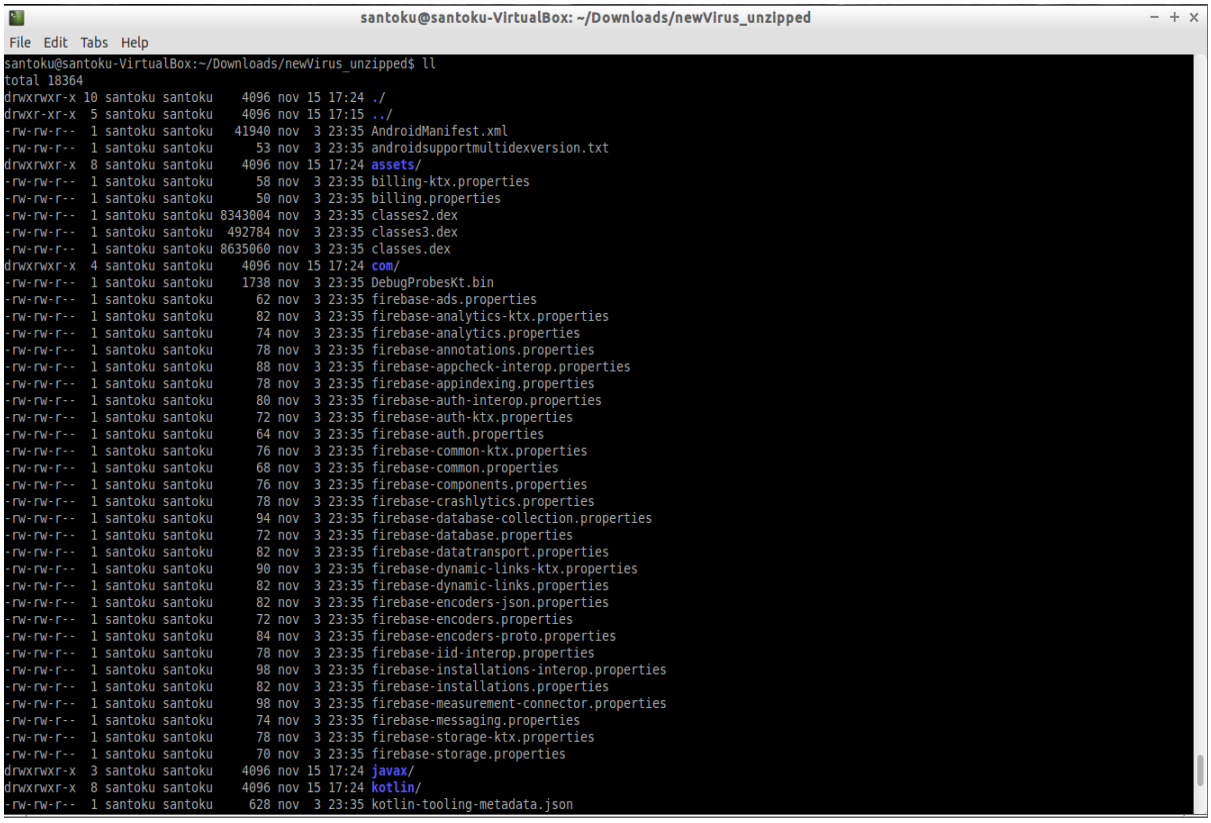
We downloaded given apk in santoku and created new directory

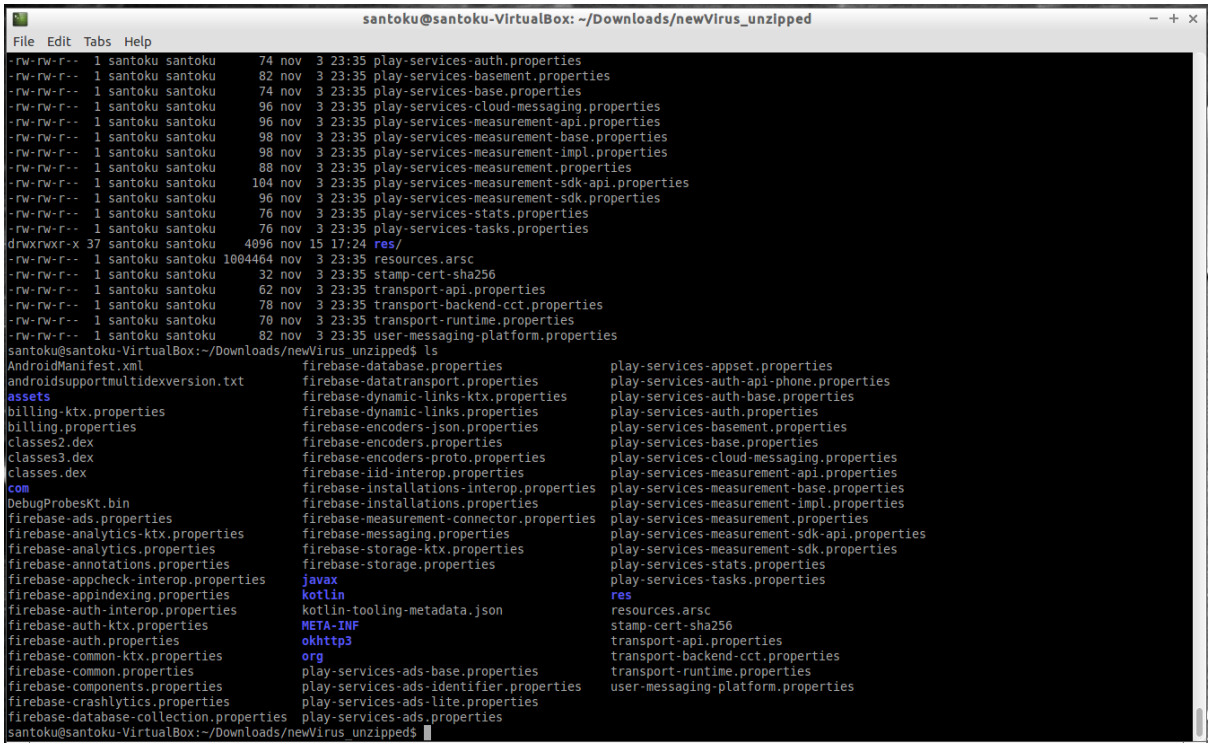

santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 32856
drwxrwxr-x 3 santoku santoku   4096 nov 15 12:01 -f
-rw-r--r-- 1 santoku santoku 17476151 nov 3 22:35 Horoscope.apk
drwxrwxr-x 10 santoku santoku   4096 nov 15 12:03 Horoscope.apk_FILES
-rwxrwx--- 1 santoku santoku 16155164 nov 15 11:34 Horoscope.zip
santoku@santoku-VirtualBox:~/Downloads$ mkdie newvirus_unzipped
No command 'mkdie' found, did you mean:
 Command 'mkdic' from package 'canna-utils' (universe)
 Command 'mkdir' from package 'coreutils' (main)
mkdie: command not found
santoku@santoku-VirtualBox:~/Downloads$ mkdir newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 32860
drwxrwxr-x 3 santoku santoku   4096 nov 15 12:01 -f
-rw-r--r-- 1 santoku santoku 17476151 nov 3 22:35 Horoscope.apk
drwxrwxr-x 10 santoku santoku   4096 nov 15 12:03 Horoscope.apk_FILES
-rwxrwx--- 1 santoku santoku 16155164 nov 15 11:34 Horoscope.zip
drwxrwxr-x 2 santoku santoku   4096 nov 15 17:15 newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads$


santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File Edit Tabs Help
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Palau
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Pitcairn
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Pohnpei
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Port_Moresby
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Rarotonga
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Saipan
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Tahiti
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Tarawa
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Tongatapu
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Wake
  inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Wallis
santoku@santoku-VirtualBox:~/Downloads$ cd newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ls -l
total 18356
-rw-rw-r-- 1 santoku santoku   41940 nov 3 23:35 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku   53 nov 3 23:35 androidsupportmultidexversion.txt
drwxrwxr-x 8 santoku santoku   4096 nov 15 17:24 assets
-rw-rw-r-- 1 santoku santoku   58 nov 3 23:35 billing-ktx.properties
-rw-rw-r-- 1 santoku santoku   50 nov 3 23:35 billing.properties
-rw-rw-r-- 1 santoku santoku 8343004 nov 3 23:35 classes2.dex
-rw-rw-r-- 1 santoku santoku 492784 nov 3 23:35 classes3.dex
-rw-rw-r-- 1 santoku santoku 8635060 nov 3 23:35 classes.dex
drwxrwxr-x 4 santoku santoku   4096 nov 15 17:24 com
-rw-rw-r-- 1 santoku santoku   1738 nov 3 23:35 DebugProbesKt.bin
-rw-rw-r-- 1 santoku santoku   62 nov 3 23:35 firebase-ads.properties
-rw-rw-r-- 1 santoku santoku   82 nov 3 23:35 firebase-analytics-ktx.properties
-rw-rw-r-- 1 santoku santoku   74 nov 3 23:35 firebase-analytics.properties
-rw-rw-r-- 1 santoku santoku   78 nov 3 23:35 firebase-annotations.properties
-rw-rw-r-- 1 santoku santoku   88 nov 3 23:35 firebase-appcheck-interop.properties
-rw-rw-r-- 1 santoku santoku   78 nov 3 23:35 firebase-appindexing.properties
-rw-rw-r-- 1 santoku santoku   80 nov 3 23:35 firebase-auth-interop.properties
-rw-rw-r-- 1 santoku santoku   72 nov 3 23:35 firebase-auth-ktx.properties
-rw-rw-r-- 1 santoku santoku   64 nov 3 23:35 firebase-auth.properties
-rw-rw-r-- 1 santoku santoku   76 nov 3 23:35 firebase-common-ktx.properties
-rw-rw-r-- 1 santoku santoku   68 nov 3 23:35 firebase-common.properties
-rw-rw-r-- 1 santoku santoku   76 nov 3 23:35 firebase-components.properties
-rw-rw-r-- 1 santoku santoku   78 nov 3 23:35 firebase-crashlytics.properties
-rw-rw-r-- 1 santoku santoku   94 nov 3 23:35 firebase-database-collection.properties
-rw-rw-r-- 1 santoku santoku   72 nov 3 23:35 firebase-database.properties
-rw-rw-r-- 1 santoku santoku   82 nov 3 23:35 firebase-datatransport.properties
-rw-rw-r-- 1 santoku santoku   90 nov 3 23:35 firebase-dynamic-links-ktx.properties
-rw-rw-r-- 1 santoku santoku   82 nov 3 23:35 firebase-dynamic-links.properties
-rw-rw-r-- 1 santoku santoku   82 nov 3 23:35 firebase-encoders-json.properties
-rw-rw-r-- 1 santoku santoku   72 nov 3 23:35 firebase-encoders.properties
-rw-rw-r-- 1 santoku santoku   84 nov 3 23:35 firebase-encoders-proto.properties

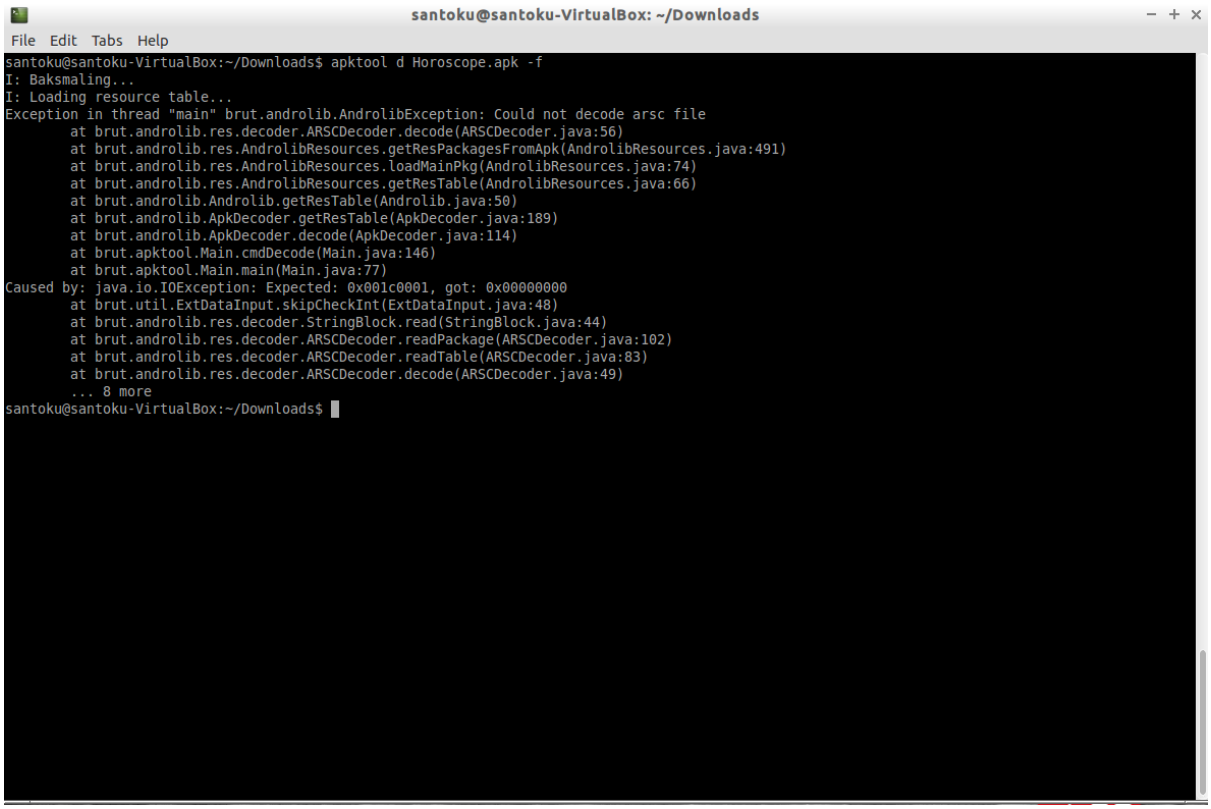
We unzip the apk file and copy that unzipped file to new directory we created



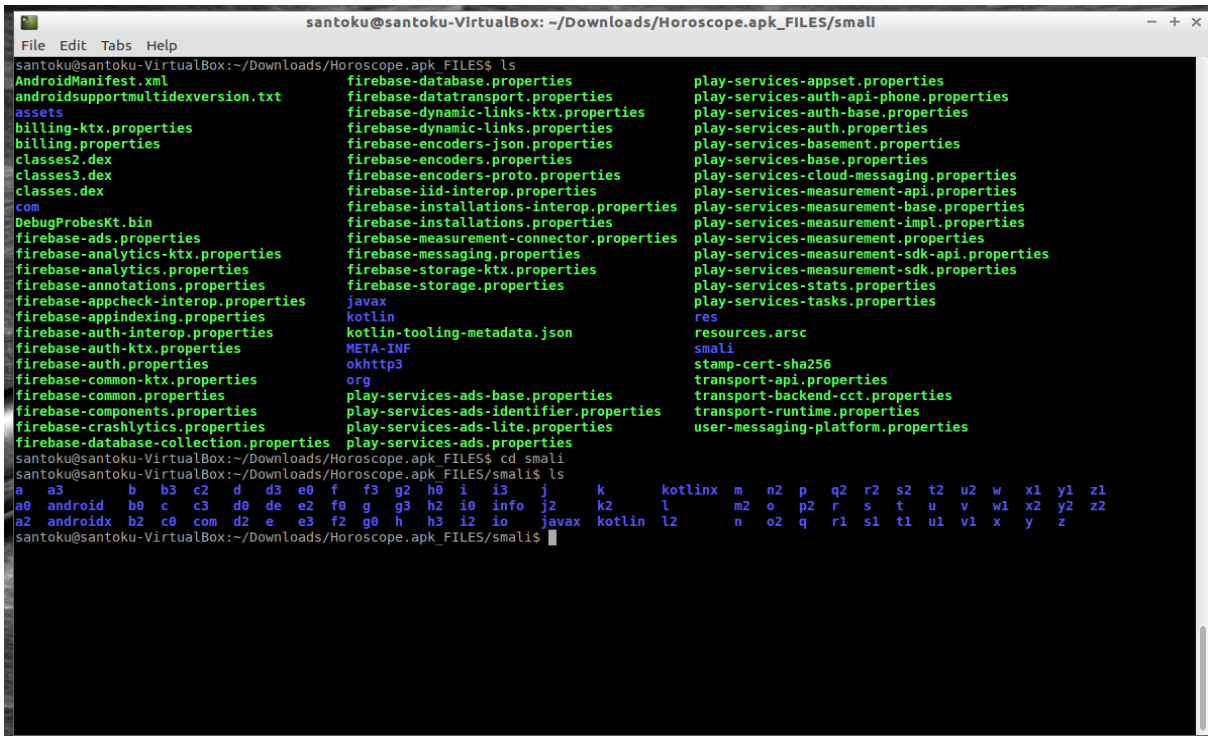




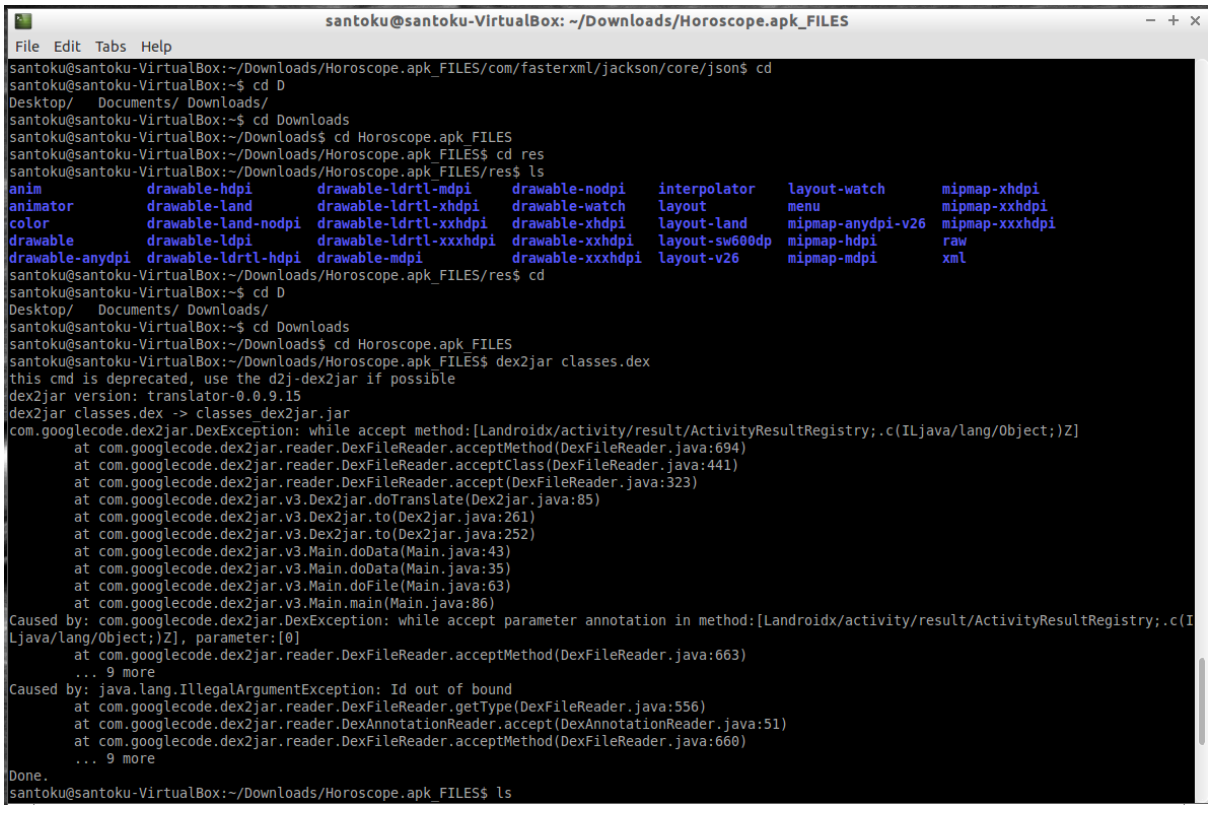
We try to decompile the file using apk tool

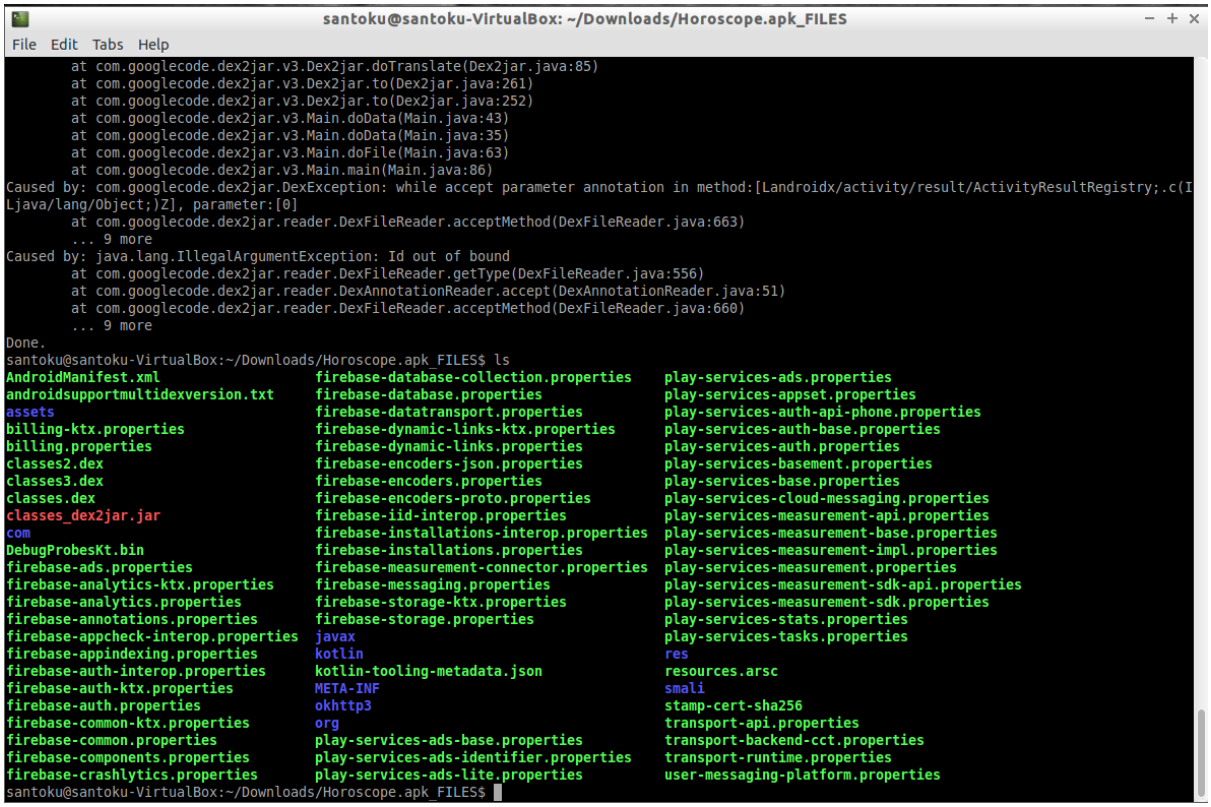


Using ls command, we try to find all files containing in the Horoscope.apk

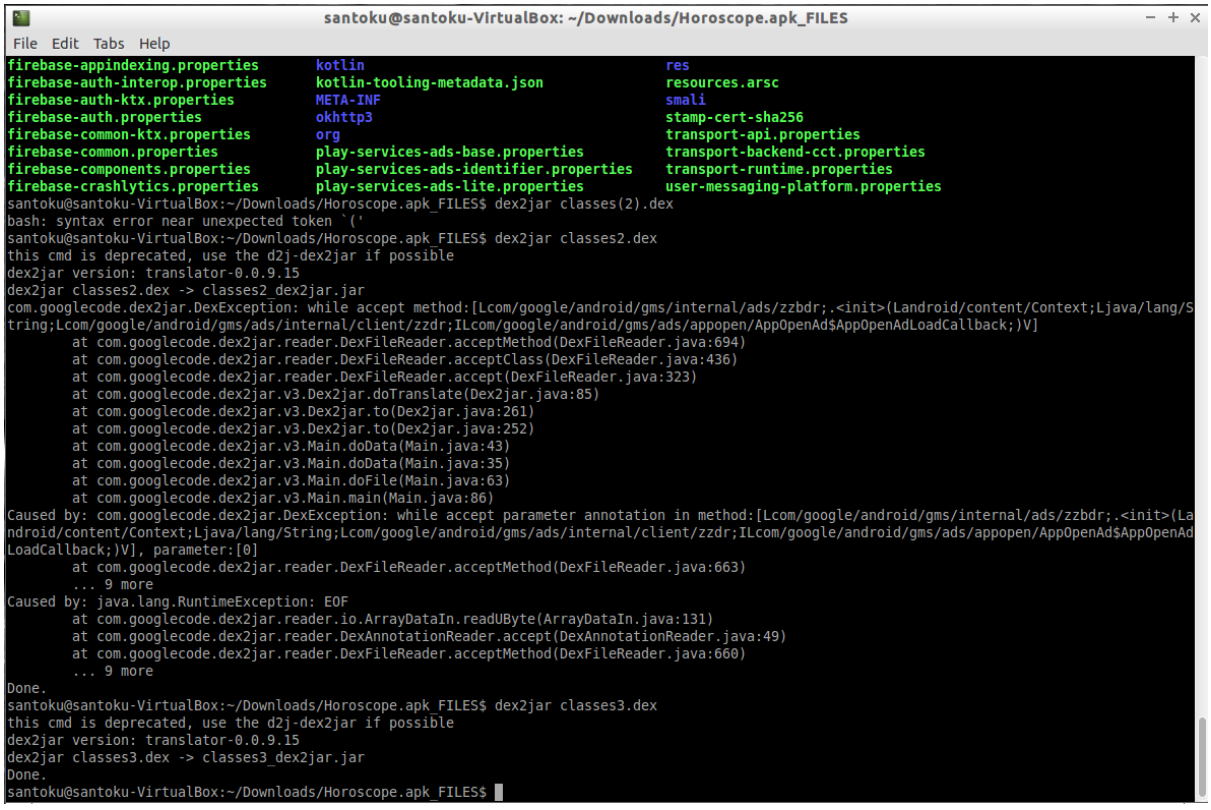


Now We can check the resource folder under the decompiled apk file which may tell what the application is intended to do

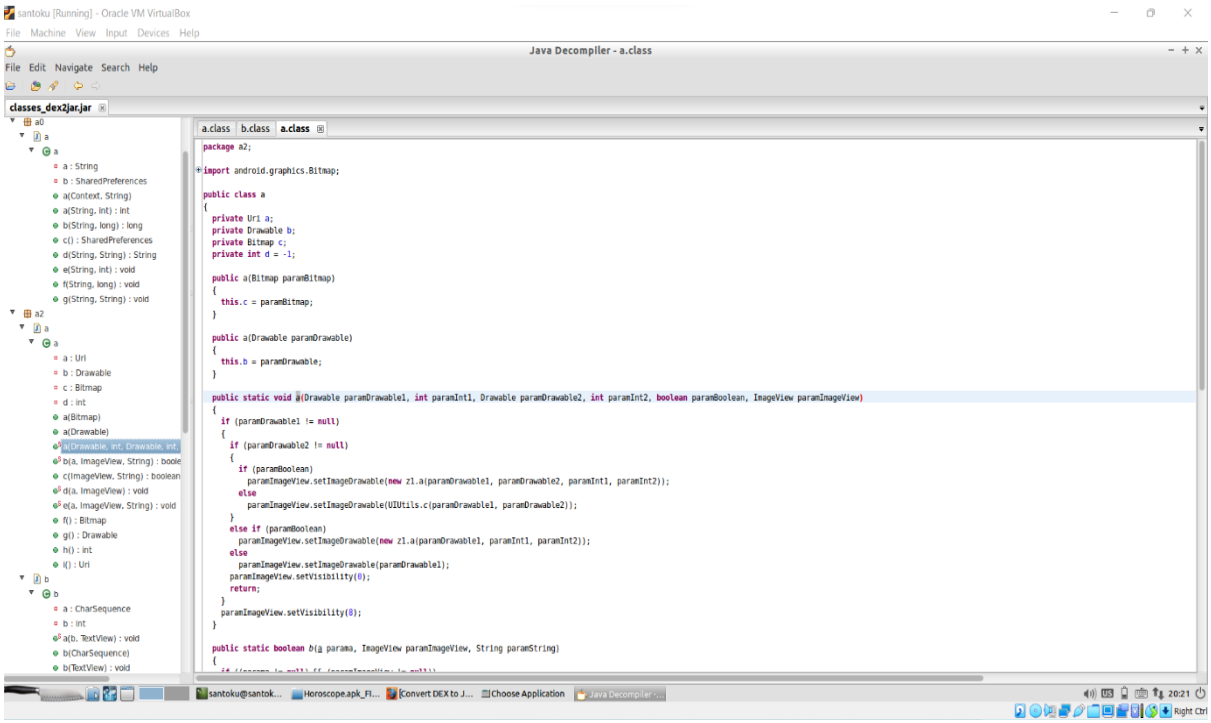




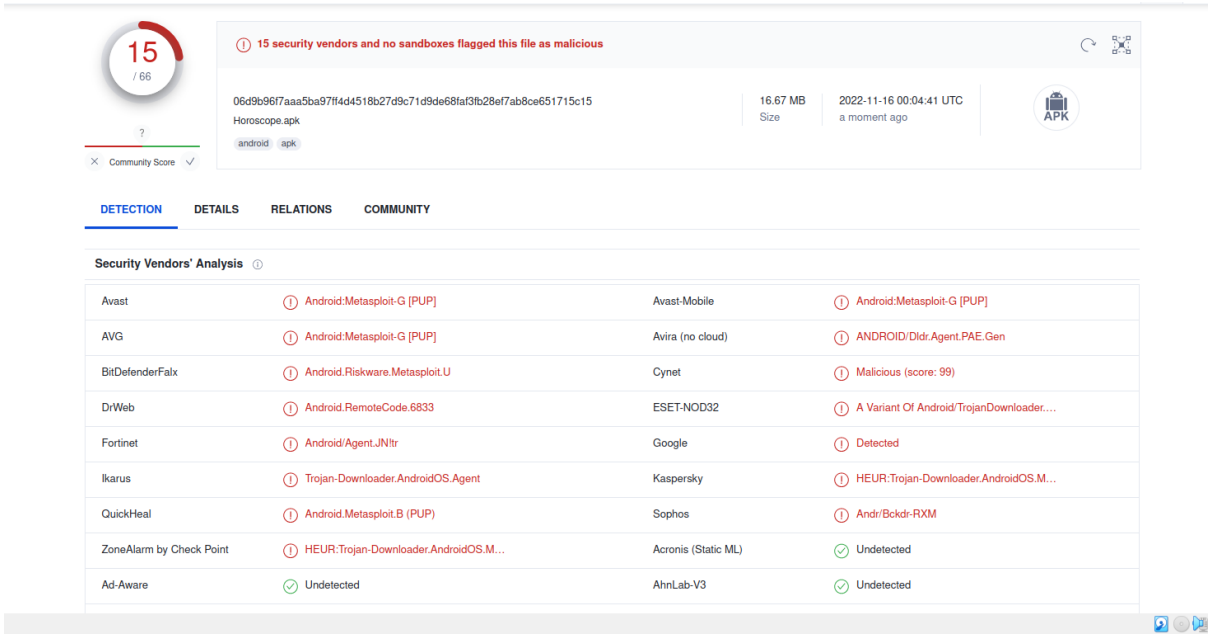
This application contains three classes.dex files. Now we can convert the classes.dex file to jar in the original unzipped file in the malware, which allow us to access the source file. (using JD-GUI inside Santuko



The jar file we created contains lots of random classes and sub classes. d we can see that it has a bunch of obfuscated and disassembled classes from the “jar” file.



Also we analyzed application by following way:



ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	Cyren	Undetected
Emsisoft	Undetected	eScan	Undetected
F-Secure	Undetected	GData	Undetected
Gridinsoft (no cloud)	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kingsoft	Undetected	Lionic	Undetected
Malwarebytes	Undetected	MAX	Undetected
MaxSecure	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	Microsoft	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
Rising	Undetected	Sangfor Engine Zero	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
Symantec Mobile Insight	Undetected	TACHYON	Undetected
Tencent	Undetected	Trellix (FireEye)	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
Trustlook	Undetected	VBA32	Undetected
VIPRE	Undetected	VirIT	Undetected
ViRobot	Undetected	Yandex	Undetected
Zillya	Undetected	Zoner	Undetected
CrowdStrike Falcon	Unable to process file type	Cybereason	Unable to process file type
Cylance	Unable to process file type	Elastic	Unable to process file type
Palo Alto Networks	Unable to process file type	SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type	TEHTRIS	Unable to process file type
Trapmine	Unable to process file type	Webroot	Unable to process file type

Conclusion

This Application looks suspicious. most of the code was obfuscated.