Malicious APK File Analysis
No. 11

Install androguard:

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/androguard/androguard.git
Cloning into 'androguard' ...
remote: Enumerating objects: 19244, done.
remote: Counting objects: 100% (542/542), done.
remote: Compressing objects: 100% (249/249), done.
remote: Total 19244 (delta 282), reused 466 (delta 245), pack-reused 18702
Receiving objects: 100% (19244/19244), 90.65 MiB | 2.20 MiB/s, done.
Resolving deltas: 100% (13571/13571), done.

┌──(kali㉿kali)-[~]
```

Analyze:

Python3 cli.py analyse siva.apk

```
└─$ python3 cli.py analyze siva.apk
2022-11-14 23:02:02.280 | INFO     | androguard.session:__init__:58 - Opening database <Database(sqlite:///androguard.db)>
2022-11-14 23:02:02.301 | INFO     | androguard.session:__init__:67 - Creating new session [2]
2022-11-14 23:02:02.301 | INFO     | main:androlyze_main:257 - Please be patient, this might take a while.
2022-11-14 23:02:02.301 | INFO     | main:androlyze_main:261 - Found the provided file is of type 'APK'
2022-11-14 23:02:02.303 | INFO     | androguard.session:addAPK:140 - add APK siva.apk:d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
2022-11-14 23:02:02.308 | INFO     | androguard.core.apk:_apk_analysis:313 - Starting analysis on AndroidManifest.xml
2022-11-14 23:02:02.344 | INFO     | androguard.core.apk:_apk_analysis:370 - APK file was successfully validated!
2022-11-14 23:02:02.355 | INFO     | androguard.session:addDEX:174 - add DEX:7e685b2e0d1d03d9edaf414c6ea576a635675bbce39998959dee64da2250404c
2022-11-14 23:02:02.643 | INFO     | androguard.session:addDEX:180 - added DEX:7e685b2e0d1d03d9edaf414c6ea576a635675bbce39998959dee64da2250404c
2022-11-14 23:02:02.643 | INFO     | androguard.core.analysis.analysis:add:1435 - Adding DEX file version 35
2022-11-14 23:02:04.069 | INFO     | androguard.core.analysis.analysis:add:1458 - Added DEX in the analysis took : 0min 01s
2022-11-14 23:02:04.481 | INFO     | androguard.core.analysis.analysis:create_xref:1492 - End of creating cross references (XREF) run time: 0min 00s
2022-11-14 23:02:04.481 | INFO     | androguard.session:addAPK:160 - added APK siva.apk:d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
2022-11-14 23:02:04.481 | INFO     | main:androlyze_main:275 - Added file to session: SHA256::d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
2022-11-14 23:02:04.481 | INFO     | main:androlyze_main:278 - Loaded APK file...
>>> filename
siva.apk
>>> a
<androguard.core.apk.APK object at 0x7fe1e1709e10>
>>> d
[<androguard.core.dex.DEX object at 0x7fe1e1785510>]
>>> dx
<analysis.Analysis VMs: 1, Classes: 1267, Methods: 6809, Strings: 2176>

Androguard version 4.0 started
```

```
Androguard version 4.0 started
In [1]: a.get_signature_name()
Out[1]: 'META-INF/CERT.RSA'
```

permissions this app needs:

We can see in this screenshot that the app has various permissions .

```
In [2]: a.get_permissions()
Out[2]:
['android.permission.VIBRATE',
 'android.permission.ACCESS_WIFI_STATE',
 'com.android.launcher.permission.INSTALL_SHORTCUT',
 'android.permission.SYSTEM_ALERT_WINDOW',
 'android.permission.RECEIVE_BOOT_COMPLETED',
 'android.permission.WRITE_SETTINGS',
 'android.permission.READ_PHONE_STATE',
 'android.permission.CHANGE_NETWORK_STATE',
 'android.permission.WRITE_EXTERNAL_STORAGE',
 'android.permission.CHANGE_WIFI_STATE',
 'android.permission.INTERNET',
 'android.permission.MOUNT_UNMOUNT_FILESYSTEMS',
 'android.permission.WAKE_LOCK',
 'android.permission.READ_EXTERNAL_STORAGE',
 'android.permission.ACCESS_NETWORK_STATE',
 'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS',
 'android.permission.GET_TASKS']
```

a.get_detailed_permission():

```
In [3]: a.get_details_permissions()
Out[3]:
{'android.permission.VIBRATE': ['normal',
  'control vibration',
  'Allows the app to control the vibrator.'],
 'android.permission.ACCESS_WIFI_STATE': ['normal',
  'view Wi-Fi connections',
  'Allows the app to view information\n      about Wi-Fi networking, such as whether Wi-Fi is enabled and name of\n      connected Wi-Fi devices.'],
 'com.android.launcher.permission.INSTALL_SHORTCUT': ['dangerous',
  'install shortcuts',
  'Allows an application to add\n       Homescreen shortcuts without user intervention.'],
 'android.permission.SYSTEM_ALERT_WINDOW': ['dangerous',
  'draw over other apps',
  'Allows the app to draw on top of other\n       applications or parts of the user interface.  They may interfere with your\n       use of the interface in any application, or change what you think you are\n       seeing in other ap
plications.'],
 'android.permission.RECEIVE_BOOT_COMPLETED': ['normal',
  'run at startup',
  'Allows the app to\n       have itself started as soon as the system has finished booting.\n       This can make it take longer to start the phone and allow the\n       app to slow down the overall phone by always running.'],
 'android.permission.WRITE_SETTINGS': ['normal',
  'modify system settings',
  "Allows the app to modify the\n       system's settings data. Malicious apps may corrupt your system's\n       configuration."],
 'android.permission.READ_PHONE_STATE': ['dangerous',
  'read phone status and identity',
  'Allows the app to access the phone\n      features of the device.  This permission allows the app to determine the\n      phone number and device IDs, whether a call is active, and the remote number\n      connected by a call.'],
 'android.permission.CHANGE_NETWORK_STATE': ['normal',
  'change network connectivity',
  'Allows the app to change the state of network connectivity.'],
 'android.permission.WRITE_EXTERNAL_STORAGE': ['dangerous',
  'modify or delete the contents of your SD card',
  'Allows the app to write to the SD card.'],
 'android.permission.CHANGE_WIFI_STATE': ['dangerous',
  'connect and disconnect from Wi-Fi',
  'Allows the app to connect to and\n      disconnect from Wi-Fi access points and to make changes to device\n      configuration for Wi-Fi networks.'],
 'android.permission.INTERNET': ['dangerous',
  'full network access',
  'Allows the app to create\n     network sockets and use custom network protocols. The browser and other\n     applications provide means to send data to the internet, so this\n     permission is not required to send data to the intern
et.'],
 'android.permission.MOUNT_UNMOUNT_FILESYSTEMS': ['system|signature',
  'access SD Card filesystem',
  'Allows the app to mount and\n       unmount filesystems for removable storage.'],
 'android.permission.WAKE_LOCK': ['normal',
  'prevent phone from sleeping',
  'Allows the app to prevent the phone from going to sleep.'],
 'android.permission.READ_EXTERNAL_STORAGE': ['normal',
  'read the contents of your SD card',
  'Allows the app to read the contents of your SD card.'],
 'android.permission.ACCESS_NETWORK_STATE': ['normal',
  'view network connections',
  'Allows the app to view\n      information about network connections such as which networks exist and are\n      connected.'],
 'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.GET_TASKS': ['normal',
  'retrieve running apps',
```

Obfuscation:

```
santoku@santoku:~/Desktop$ unzip siva.apk
Archive:  siva.apk
  inflating: AndroidManifest.xml
  inflating: META-INF/CERT.RSA
  inflating: META-INF/CERT.SF
  inflating: META-INF/MANIFEST.MF
  inflating: META-INF/services/javax.ws.rs.ext.MessageBodyReader
  inflating: META-INF/services/javax.ws.rs.ext.MessageBodyWriter
  inflating: assets/armeabi-v7a/skysea
  inflating: assets/armeabi/skysea
  inflating: classes.dex
 extracting: res/drawable-hdpi-v4/ic_launcher.png
 extracting: res/drawable-mdpi-v4/ic_launcher.png
 extracting: res/drawable-xhdpi-v4/ic_launcher.png
 extracting: res/drawable-xxhdpi-v4/app_icon.png
 extracting: res/drawable-xxhdpi-v4/close_m.png
 extracting: res/drawable-xxhdpi-v4/ic_launcher.png
 extracting: res/drawable-xxxhdpi-v4/ic_launcher.png
  inflating: res/drawable/dialog_bg_m.xml
  inflating: res/layout/activity_browser.xml
  inflating: res/layout/activity_main.xml
  inflating: res/layout/rect_dialog.xml
  inflating: res/menu/overflow_popup.xml
 extracting: res/mipmap-hdpi-v4/ic_launcher.png
 extracting: res/mipmap-mdpi-v4/ic_launcher.png
 extracting: res/mipmap-xhdpi-v4/ic_launcher.png
 extracting: res/mipmap-xxhdpi-v4/ic_launcher.png
 extracting: res/mipmap-xxxhdpi-v4/ic_launcher.png
  inflating: res/xml/preferences.xml
```

Apktool d siva.apk -f: This command creates a folder of siva in the desktop folder which contains all the files present in the apk.

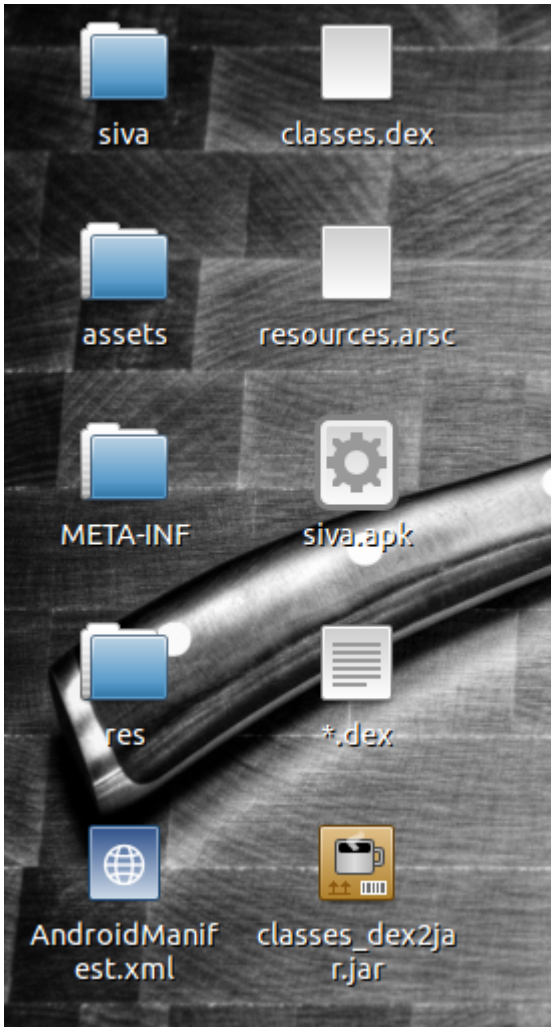
```
santoku@santoku:~/Desktop$ apktool d siva.apk -f
I: Baksmaling...
I: Loading resource table...
Exception in thread "main" brut.androlib.AndrolibException: Could not decode arsc file
        at brut.androlib.res.decoder.ARSCDecoder.decode(ARSCDecoder.java:56)
        at brut.androlib.res.AndrolibResources.getResPackagesFromApk(AndrolibResources.java:491)
        at brut.androlib.res.AndrolibResources.loadMainPkg(AndrolibResources.java:74)
        at brut.androlib.res.AndrolibResources.getResTable(AndrolibResources.java:66)
        at brut.androlib.Androlib.getResTable(Androlib.java:50)
        at brut.androlib.ApkDecoder.getResTable(ApkDecoder.java:189)
        at brut.androlib.ApkDecoder.decode(ApkDecoder.java:114)
        at brut.apktool.Main.cmdDecode(Main.java:146)
        at brut.apktool.Main.main(Main.java:77)
Caused by: java.io.IOException: Expected: 0x001c0001, got: 0x00000000
        at brut.util.ExtDataInput.skipCheckInt(ExtDataInput.java:48)
        at brut.androlib.res.decoder.StringBlock.read(StringBlock.java:44)
        at brut.androlib.res.decoder.ARSCDecoder.readPackage(ARSCDecoder.java:102)
        at brut.androlib.res.decoder.ARSCDecoder.readTable(ARSCDecoder.java:83)
        at brut.androlib.res.decoder.ARSCDecoder.decode(ARSCDecoder.java:49)
        ... 8 more
santoku@santoku:~/Desktop$
```

Here we are removing the dex and html files to get the main content to be examined .

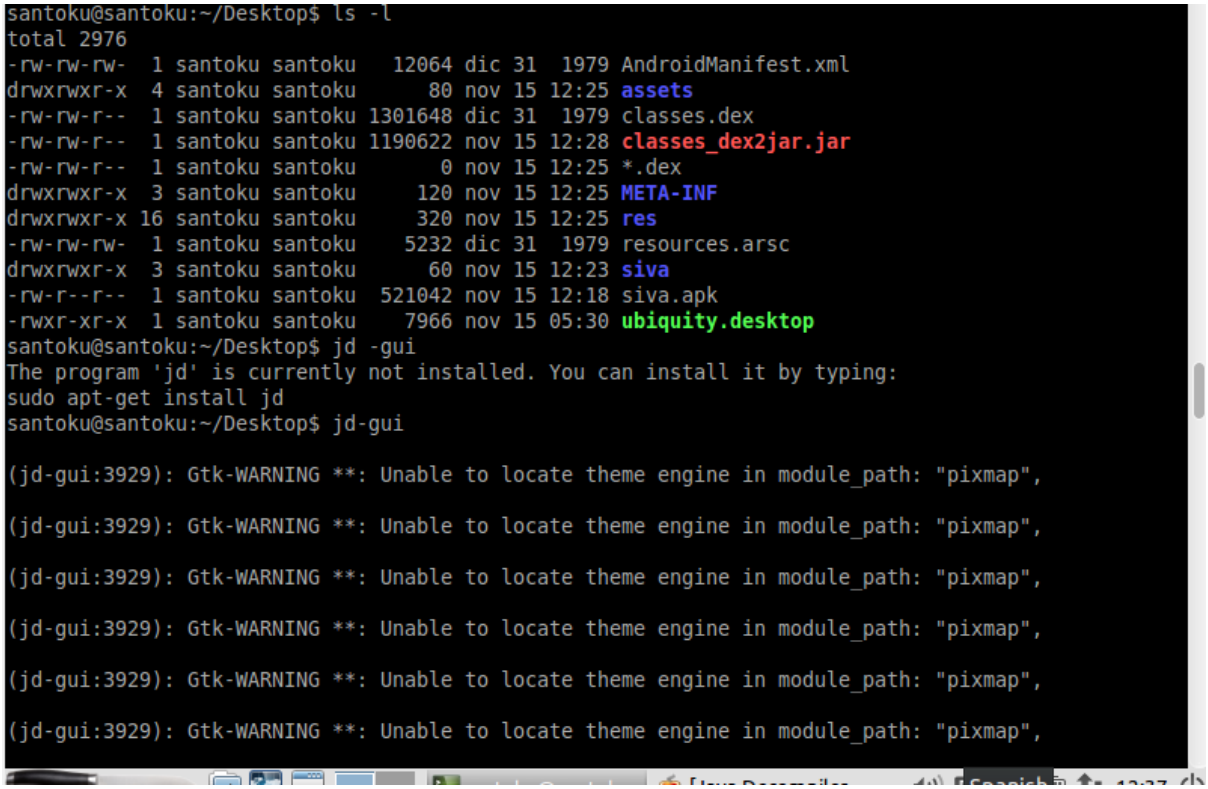
```
santoku@santoku:~/Desktop$ vi siva.apk
santoku@santoku:~/Desktop$ rm *.xml
santoku@santoku:~/Desktop$ rm *.dex
santoku@santoku:~/Desktop$ rm *.arsc
santoku@santoku:~/Desktop$ ls 'l
> ^C
santoku@santoku:~/Desktop$ ls -l
total 520
drwxrwxr-x  4 santoku santoku     80 nov 15 12:12 assets
drwxrwxr-x  3 santoku santoku     60 nov 15 12:15 -f
drwxrwxr-x  3 santoku santoku    120 nov 15 12:12 META-INF
drwxrwxr-x 16 santoku santoku    320 nov 15 12:12 res
drwxrwxr-x  3 santoku santoku     60 nov 15 07:36 siva
-rw-r--r--  1 santoku santoku 521042 nov 15 12:18 siva.apk
-rwxr-xr-x  1 santoku santoku   7966 nov 15 05:30 ubiquity.desktop
santoku@santoku:~/Desktop$ rm -r ./assets
santoku@santoku:~/Desktop$ rm -r ./META-INF
santoku@santoku:~/Desktop$ rm -r ./res
santoku@santoku:~/Desktop$ ls -l
total 520
drwxrwxr-x 3 santoku santoku     60 nov 15 12:15 -f
drwxrwxr-x 3 santoku santoku     60 nov 15 07:36 siva
-rw-r--r-- 1 santoku santoku 521042 nov 15 12:18 siva.apk
-rwxr-xr-x 1 santoku santoku   7966 nov 15 05:30 ubiquity.desktop
```

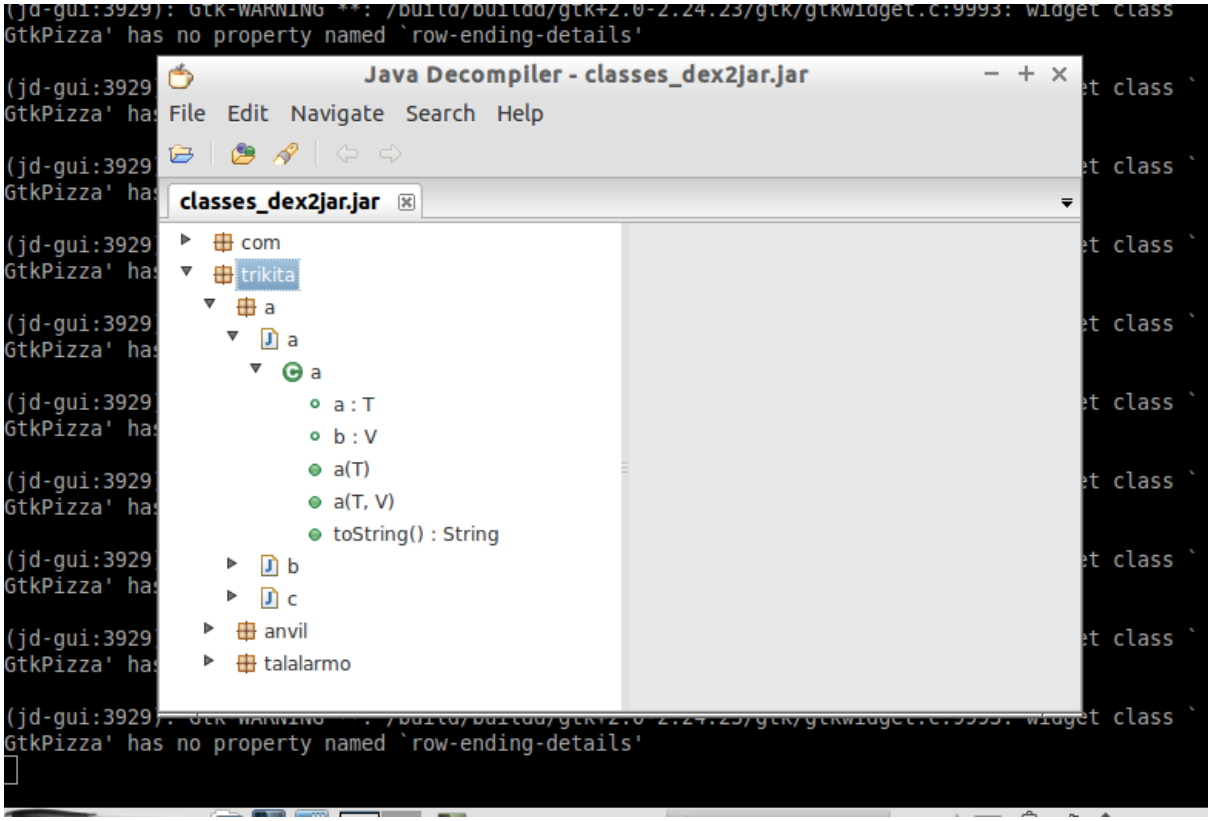
dex2jar classes.dex:

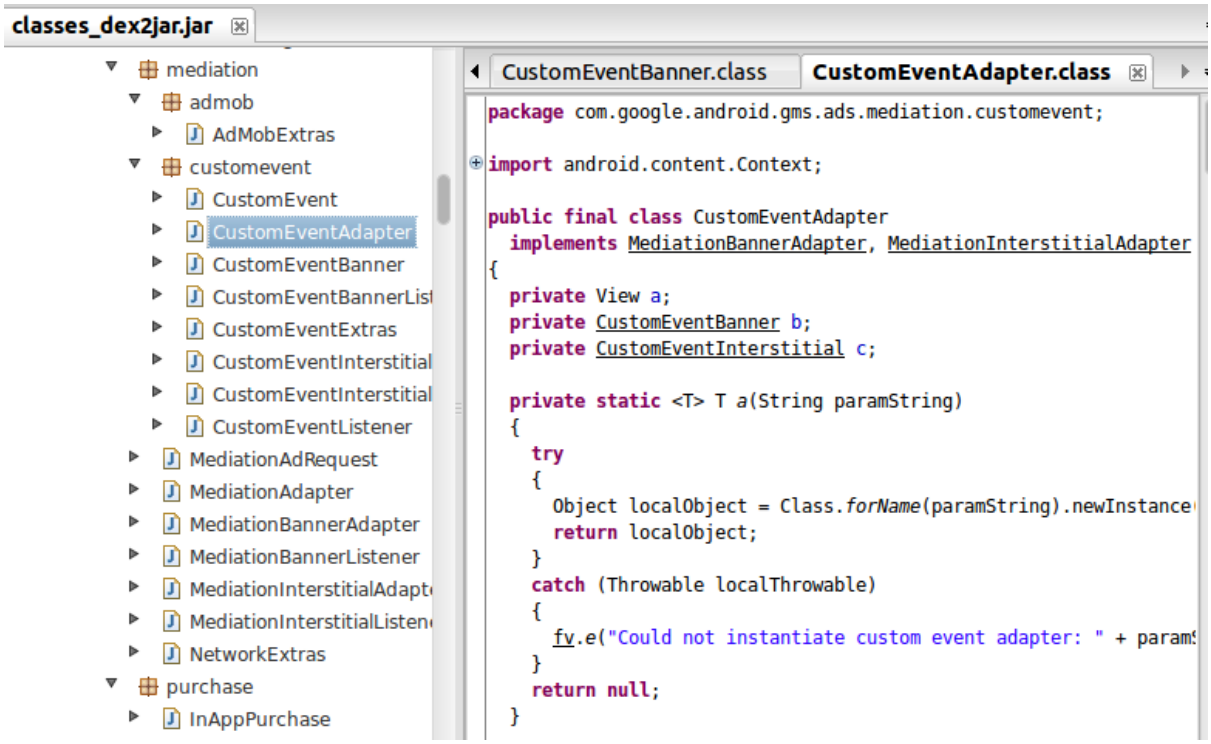
```
santoku@santoku:~/Desktop$ dex2jar classes.dex
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.15
dex2jar classes.dex -> classes_dex2jar.jar

Done.
santoku@santoku:~/Desktop$
santoku@santoku:~/Desktop$ ls -l
total 2976
-rw-rw-rw-  1 santoku santoku   12064 dic 31  1979 AndroidManifest.xml
drwxrwxr-x  4 santoku santoku      80 nov 15 12:25 assets
-rw-rw-r--  1 santoku santoku 1301648 dic 31  1979 classes.dex
-rw-rw-r--  1 santoku santoku 1190622 nov 15 12:28 classes_dex2jar.jar
-rw-rw-r--  1 santoku santoku       0 nov 15 12:25 *.dex
drwxrwxr-x  3 santoku santoku     120 nov 15 12:25 META-INF
drwxrwxr-x 16 santoku santoku     320 nov 15 12:25 res
-rw-rw-rw-  1 santoku santoku    5232 dic 31  1979 resources.arsc
drwxrwxr-x  3 santoku santoku      60 nov 15 12:23 siva
-rw-r--r--  1 santoku santoku  521042 nov 15 12:18 siva.apk
-rwxr-xr-x  1 santoku santoku    7966 nov 15 05:30 ubiquity.desktop
santoku@santoku:~/Desktop$
```



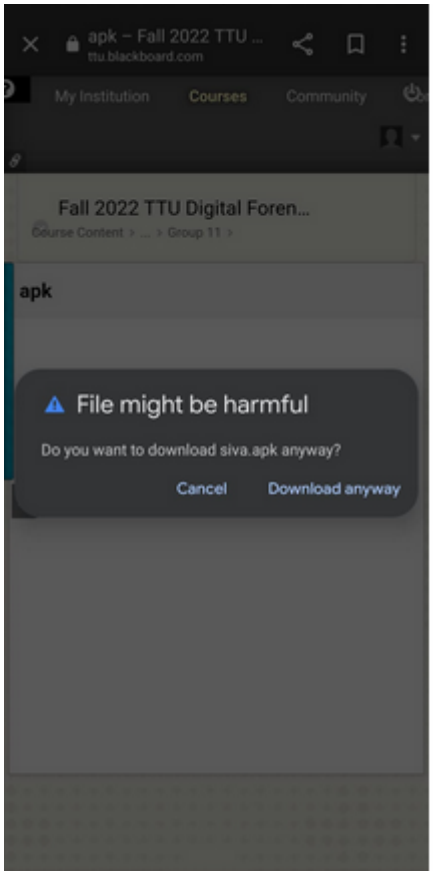
dissected Java code using JD-GUI

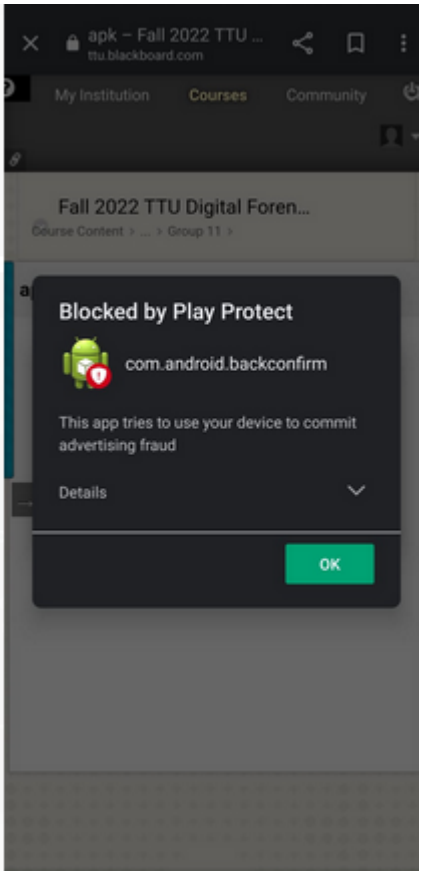

santoku@santoku:~/Desktop$ ls -l
total 2976
-rw-rw-rw- 1 santoku santoku   12064 dic 31 1979 AndroidManifest.xml
drwxrwxr-x 4 santoku santoku   80 nov 15 12:25 assets
-rw-rw-r-- 1 santoku santoku 1301648 dic 31 1979 classes.dex
-rw-rw-r-- 1 santoku santoku 1190622 nov 15 12:28 classes_dex2jar.jar
-rw-rw-r-- 1 santoku santoku   0 nov 15 12:25 *.dex
drwxrwxr-x 3 santoku santoku   120 nov 15 12:25 META-INF
drwxrwxr-x 16 santoku santoku   320 nov 15 12:25 res
-rw-rw-rw- 1 santoku santoku   5232 dic 31 1979 resources.arsc
drwxrwxr-x 3 santoku santoku   60 nov 15 12:23 siva
-rw-r--r-- 1 santoku santoku 521042 nov 15 12:18 siva.apk
-rwxr-xr-x 1 santoku santoku   7966 nov 15 05:30 ubiquity.desktop
santoku@santoku:~/Desktop$ jd -gui
The program 'jd' is currently not installed. You can install it by typing:
sudo apt-get install jd
santoku@santoku:~/Desktop$ jd-gui
(jd-gui:3929): Gtk-WARNING **: Unable to locate theme engine in module_path: "pixmap",
(jd-gui:3929): Gtk-WARNING **: Unable to locate theme engine in module_path: "pixmap",
(jd-gui:3929): Gtk-WARNING **: Unable to locate theme engine in module_path: "pixmap",
(jd-gui:3929): Gtk-WARNING **: Unable to locate theme engine in module_path: "pixmap",
(jd-gui:3929): Gtk-WARNING **: Unable to locate theme engine in module_path: "pixmap",
(jd-gui:3929): Gtk-WARNING **: Unable to locate theme engine in module_path: "pixmap",


GtkPizza' has no property named `row-ending-details'
Java Decompiler - classes_dex2jar.jar
File Edit Navigate Search Help
classes_dex2jar.jar
com
trikita
a
a
a
a : T
b : V
a(T)
a(T, V)
toString() : String
b
c
anvil
talalarmo
GtkPizza' has no property named `row-ending-details'



Dynamic Analysis:





In dynamic analysis ,we are not even able to install the given apk.

Secret code in the file: Texas tech