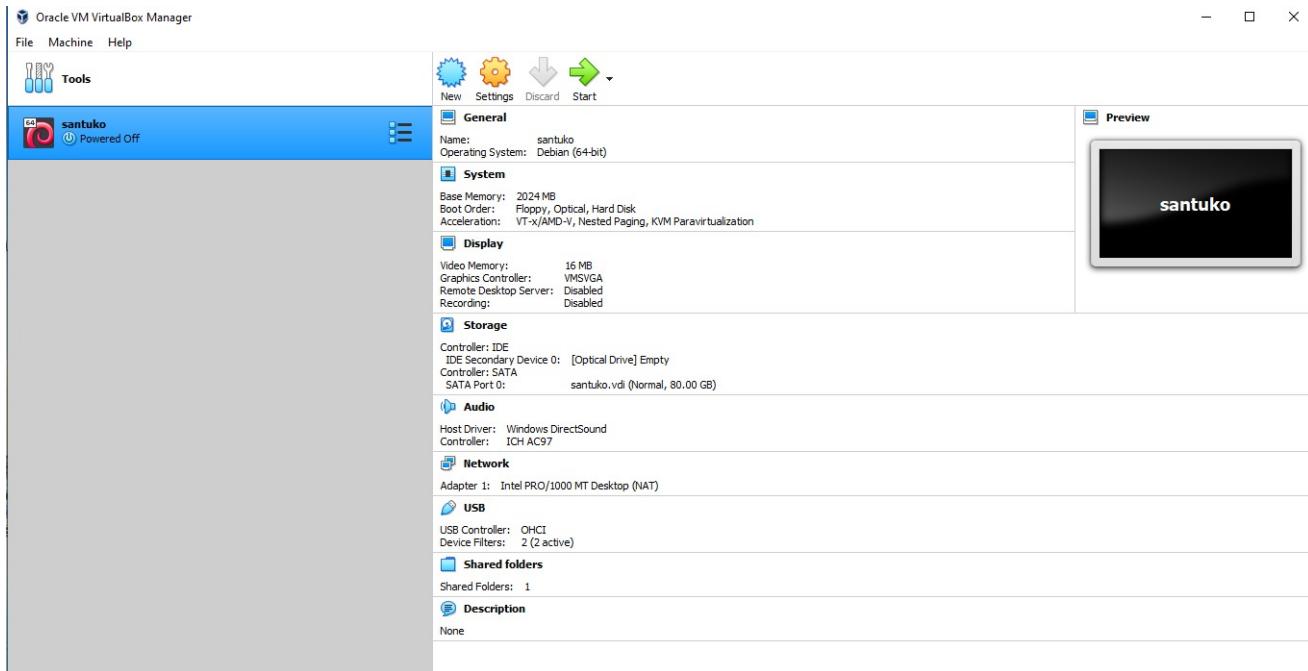


Malicious APK File Creation No. 11

The installation and the creation of malicious android application are as follows:

Step-1: Installation of Santoku in the Virtual Machine.



Step-2:

Open the terminal and enter the command

pwd

and then enter the command

cd/usr/local/bin

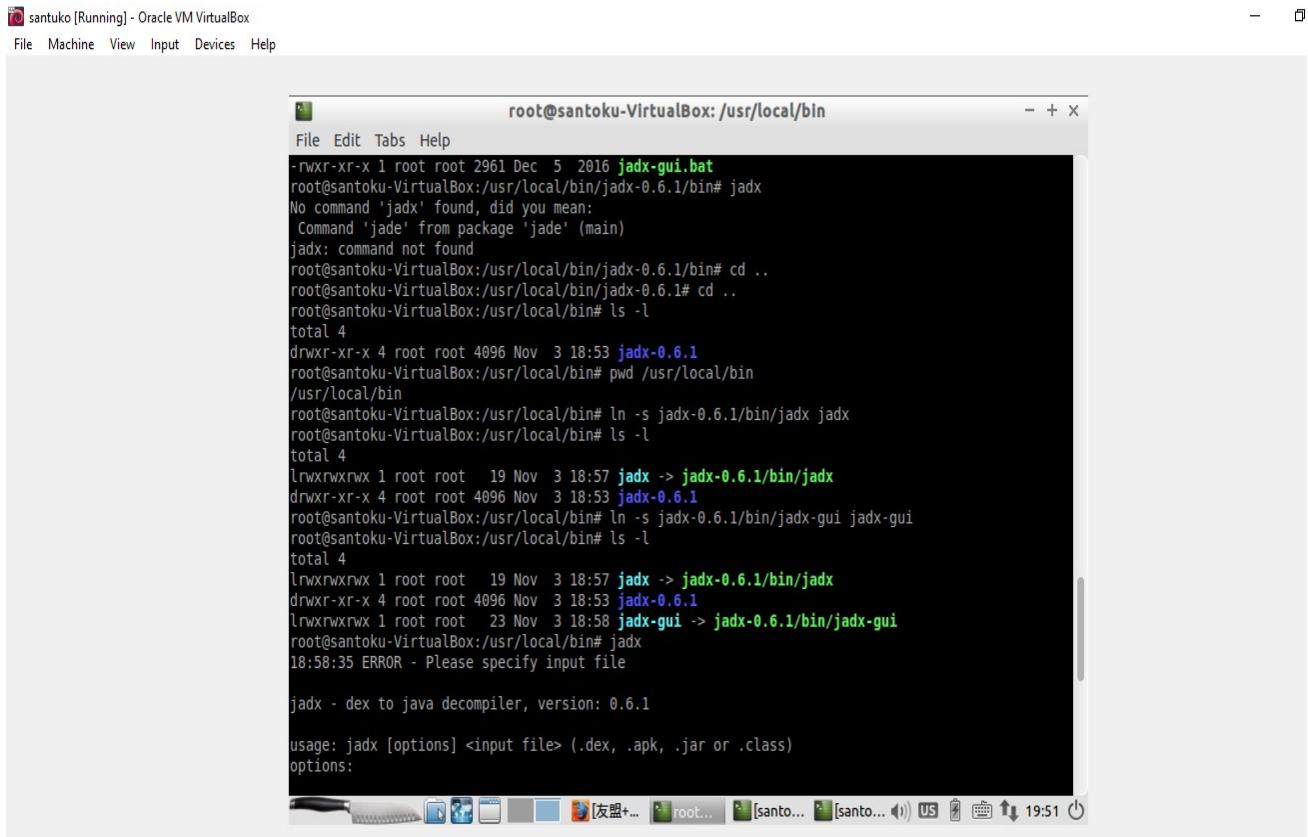
This will create a folder in the above path.

Step-3: Dex to Java Decompiler

We need to install jadx-gui. This is to decompile the application.

This operation will let us know about the application permissions, details of the blocks, information leakage etc. The operation result is as shown below.

The link <https://github.com/skylot/jadx/releases/download/v1.4.5/jadx-1.4.5.zip> is used to wget https://github.com/skylot/jadx/releases/download/v1.4.5/jadx-1.4.5.zip.
This will lead us to get the application installation in terminal.



A screenshot of a Linux terminal window titled "santoku [Running] - Oracle VM VirtualBox". The window shows a root shell session. The user is installing the jadx-0.6.1 binary. The terminal output is as follows:

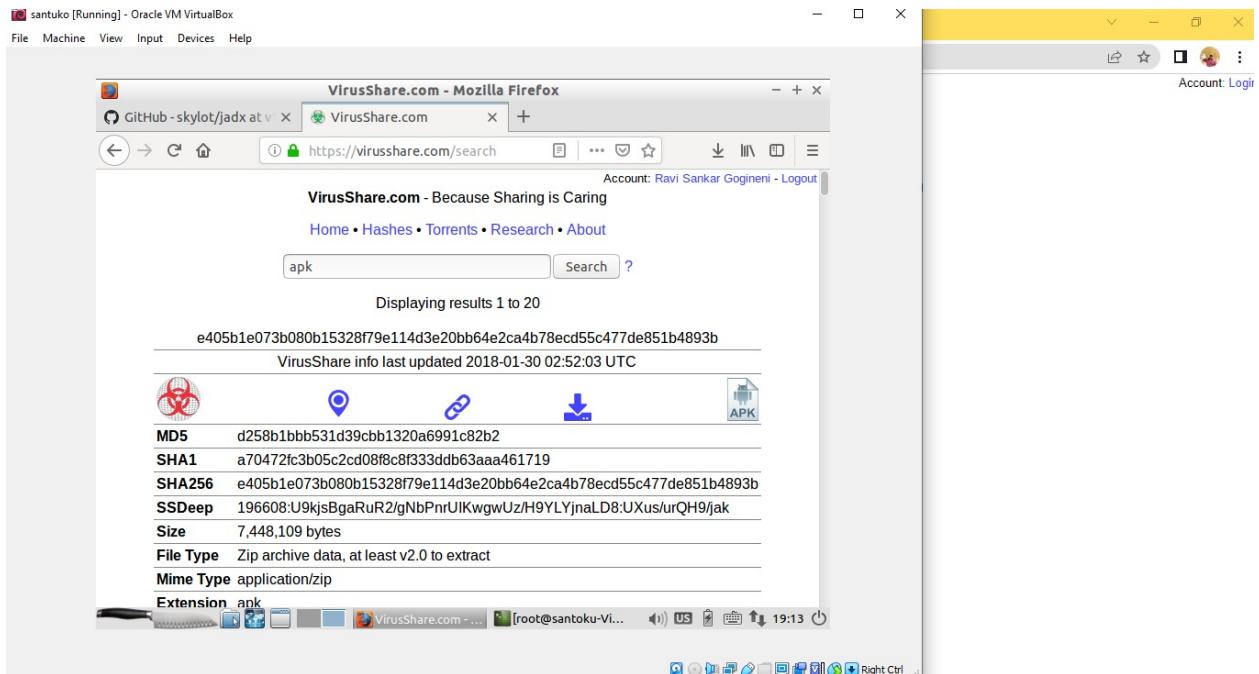
```
root@santoku-VirtualBox: /usr/local/bin
File Edit Tabs Help
-rwxr-xr-x 1 root root 2961 Dec  5 2016 jadx-gui.bat
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# jadx
No command 'jadx' found, did you mean:
  Command 'jade' from package 'jade' (main)
jadx: command not found
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# cd ..
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1# cd ..
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
drwxr-xr-x 4 root root 4096 Nov  3 18:53 jadx-0.6.1
root@santoku-VirtualBox:/usr/local/bin# pwd /usr/local/bin
/usr/local/bin
root@santoku-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx jadx
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 Nov  3 18:57 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 Nov  3 18:53 jadx-0.6.1
root@santoku-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx-gui jadx-gui
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 Nov  3 18:57 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 Nov  3 18:53 jadx-0.6.1
lrwxrwxrwx 1 root root 23 Nov  3 18:58 jadx-gui -> jadx-0.6.1/bin/jadx-gui
root@santoku-VirtualBox:/usr/local/bin# jadx
18:58:35 ERROR - Please specify input file

jadx - dex to java decompiler, version: 0.6.1

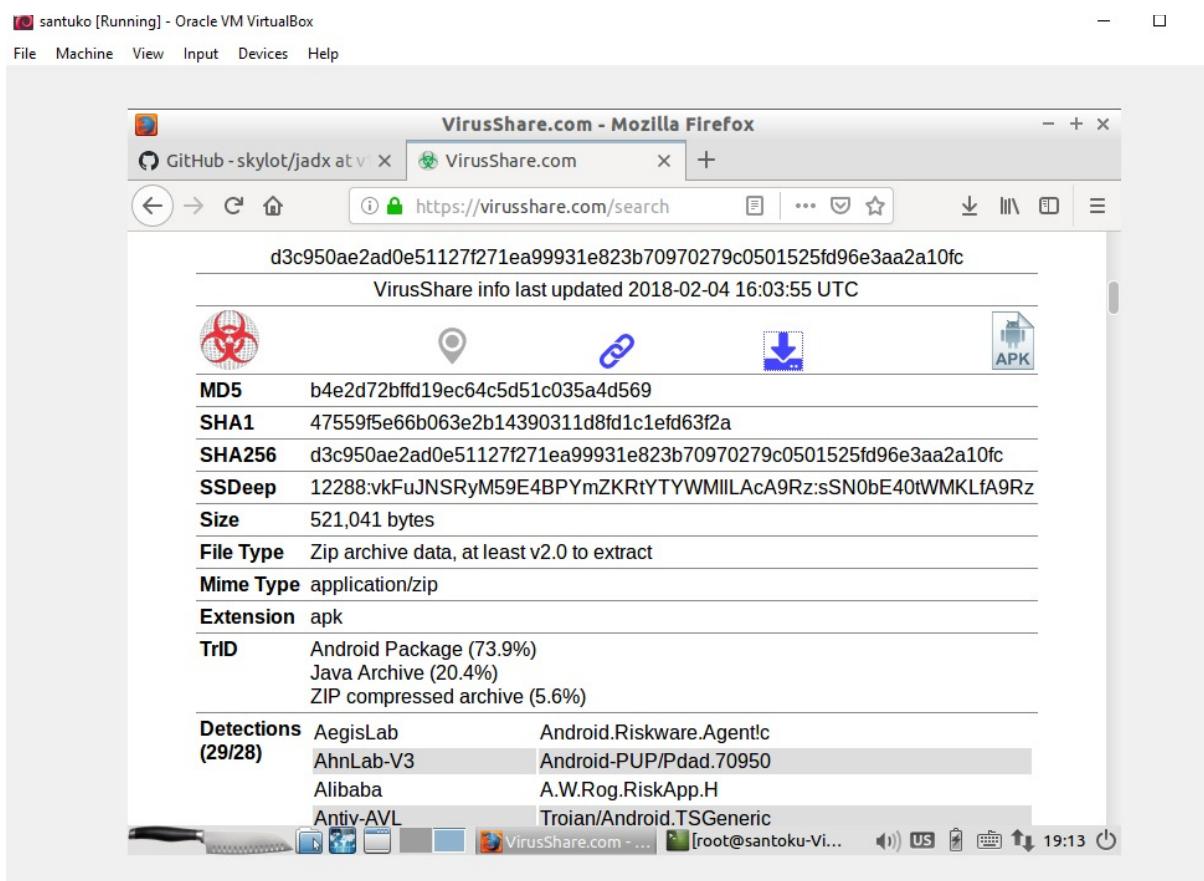
usage: jadx [options] <input file> (.dex, .apk, .jar or .class)
options:
```

Step-4:

By using the <https://virusshare.com/> we will download the malicious application.

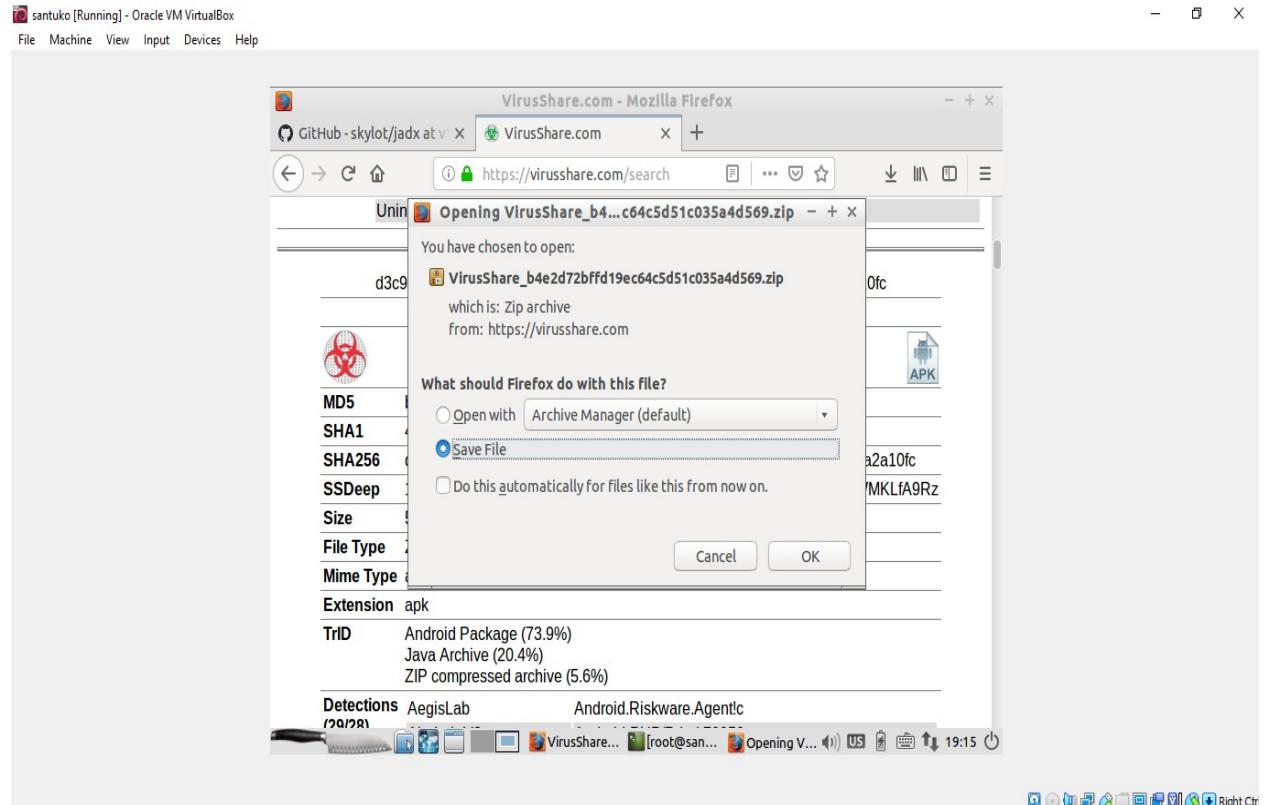


The resultant application details will be as follows:



The malicious part of the application is MD5
B4e2d72bffd19ec64c51c035a4d569

The application is saved as zip file as shown in below snapshot:



Step 5:

By entering the command

ls -l

we will get the folders that are inside the application.

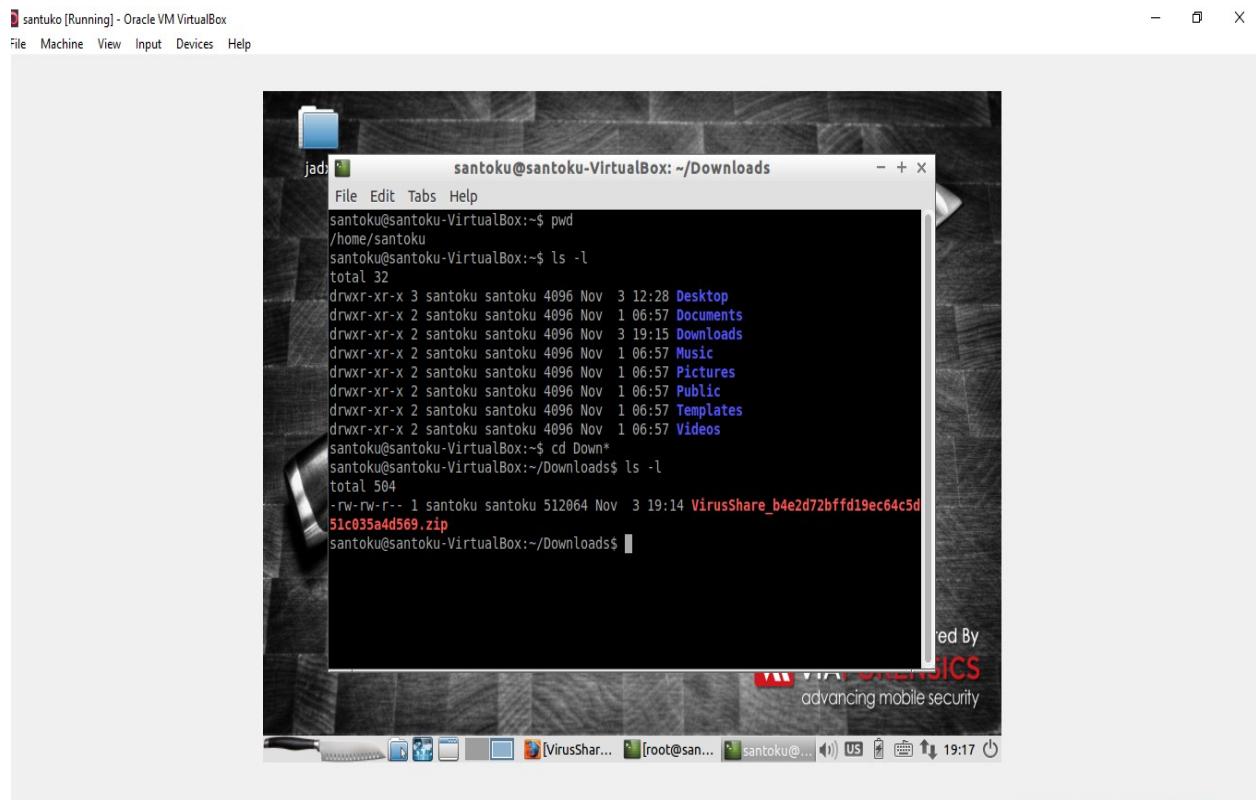
By using the command

cd Down*

we will get directed to the path by which the virus is downloaded. After that command, we enter

ls -l

we will get the list of the virus zip file. It appears as shown below:



The screenshot shows a terminal window titled "jad" running on a Linux system named "santoku". The window displays the following command-line session:

```
santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ pwd
/home/santoku
santoku@santoku-VirtualBox:~$ ls -l
total 32
drwxr-xr-x 3 santoku santoku 4096 Nov  3 12:28 Desktop
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Documents
drwxr-xr-x 2 santoku santoku 4096 Nov  3 19:15 Downloads
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Music
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Pictures
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Public
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Templates
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Videos
santoku@santoku-VirtualBox:~/Downloads$ cd Down*
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 504
-rw-rw-r-- 1 santoku santoku 512064 Nov  3 19:14 VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
santoku@santoku-VirtualBox:~/Downloads$
```

The terminal window is part of a desktop environment, with a taskbar at the bottom showing icons for various applications like a browser, file manager, and terminal. A watermark for "SICS advancing mobile security" is visible in the background of the desktop.

Step 6:

We unzip the folder by using the command

unzip folder_name

The password for the folder is infected.

Now it will display the virus inflating as shown in below image:

A screenshot of a terminal window titled "santoku@santoku-VirtualBox: ~/Downloads". The terminal shows the following command and its execution:

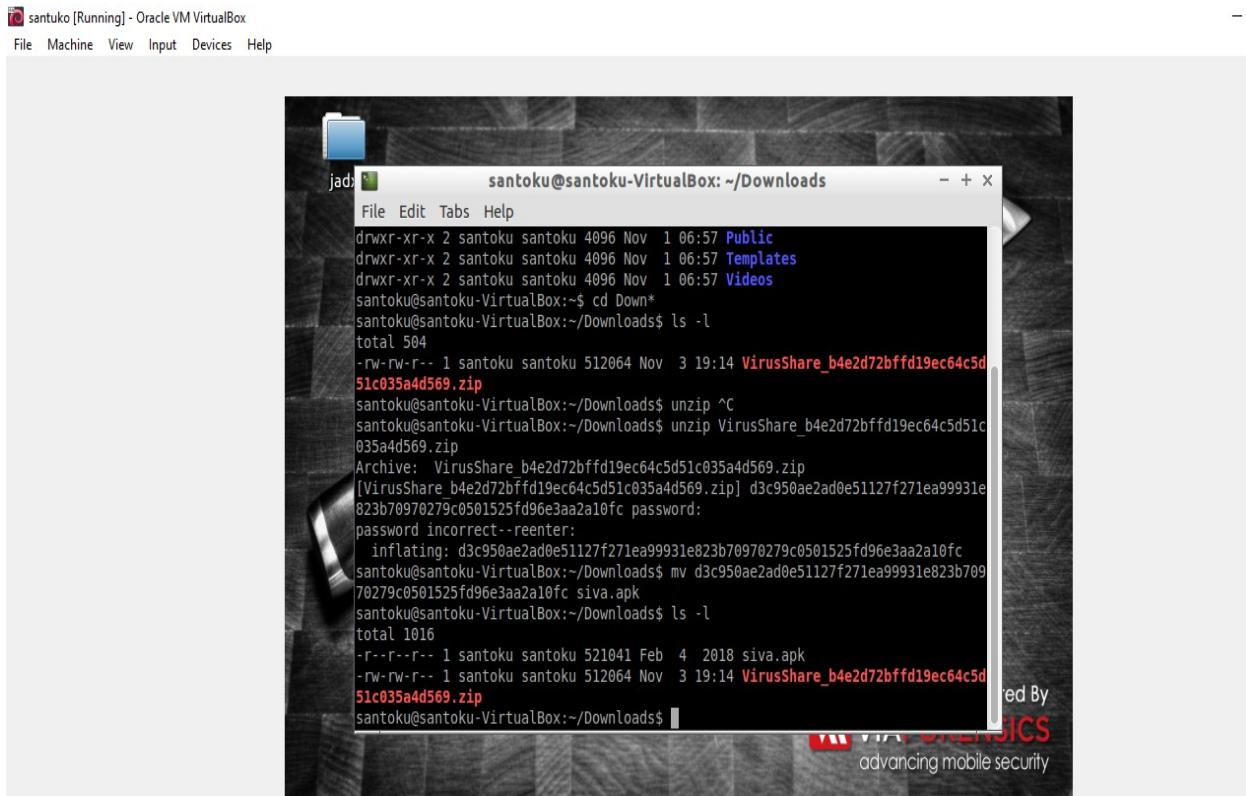
```
total 32
drwxr-xr-x 3 santoku santoku 4096 Nov  3 12:28 Desktop
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Documents
drwxr-xr-x 2 santoku santoku 4096 Nov  3 19:15 Downloads
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Music
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Pictures
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Public
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Templates
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Videos
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 504
-rw-rw-r-- 1 santoku santoku 512064 Nov  3 19:14 VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
santoku@santoku-VirtualBox:~/Downloads$ unzip ^C
santoku@santoku-VirtualBox:~/Downloads$ unzip VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
Archive:  VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
[VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip] d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc password:
password incorrect - reenter:
      inflating: d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
santoku@santoku-VirtualBox:~/Downloads$ mv d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc siva.apk
```

The terminal window has a dark background and light-colored text. The title bar says "santoku@santoku-VirtualBox: ~/Downloads". The bottom status bar shows the date and time as "19:21". There is also a watermark for "SIVAJIICS" and "advancing mobile security" in the bottom right corner of the terminal window.

Step 7:

After unzipping the application, we will create a new folder named ravi and we move the malicious application to that folder. And we also change the malicious application name to siva.apk.

The snapshot of the created folder and the application are shown below:



A screenshot of a terminal window titled "santoku [Running] - Oracle VM VirtualBox". The window shows a Linux command-line interface. The user has navigated to the Downloads directory and listed files. They then unzipped a file named "51c035a4d569.zip". After extracting the contents, they moved the file "VirusShare_b4e2d72bffd19ec64c5d51c035a4d569" to "siva.apk". The terminal window has a dark background with light-colored text. A watermark for "advancing mobile security" is visible at the bottom right of the terminal window.

```
santoku@ santoku@VirtualBox: ~/Downloads
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Public
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Templates
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Videos
santoku@ santoku@VirtualBox: ~$ cd Downloads
santoku@ santoku@VirtualBox: ~/Downloads$ ls -l
total 504
-rw-rw-r-- 1 santoku santoku 512064 Nov  3 19:14 VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
santoku@ santoku@VirtualBox: ~/Downloads$ unzip ^
santoku@ santoku@VirtualBox: ~/Downloads$ unzip VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
Archive:  VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
[VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip] d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc password:
password incorrect--reenter:
    inflating: d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc
santoku@ santoku@VirtualBox: ~/Downloads$ mv d3c950ae2ad0e51127f271ea99931e823b70970279c0501525fd96e3aa2a10fc siva.apk
santoku@ santoku@VirtualBox: ~/Downloads$ ls -l
total 1016
-r--r--r-- 1 santoku santoku 521041 Feb  4 2018 siva.apk
-rw-rw-r-- 1 santoku santoku 512064 Nov  3 19:14 VirusShare_b4e2d72bffd19ec64c5d51c035a4d569.zip
santoku@ santoku@VirtualBox: ~/Downloads$
```

Step 8:

Using <https://www.virustotal.com/gui/home/upload>, we will get to know what trojans it has and what kind of permissions does it need and logos, activities, services and receivers.

Security analysis:

The screenshot displays two tabs of a VirusTotal analysis interface. The top tab, "Security Vendors' Analysis", shows a list of 15 vendors and their findings for the file. The bottom tab, "Symantec", shows a list of 17 Symantec products and their findings. Both tabs include columns for vendor name, detection status, and a detailed description.

Security Vendors' Analysis

Vendor	Description	Vendor	Description
AhnLab-V3	PUP/Android.Pdad.461136	Alibaba	AdWare.Android.HiddenAd.607ea382
Antiy-AVL	Trojan/Generic.ASMalwAD.54	Avast	Android.HiddenAds-MW [Adw]
Avast-Mobile	Android.Evo-gen [Trj]	AVG	Android.HiddenAds-MW [Adw]
Avira (no cloud)	ANDROID/Hiddad.FAZ.Gen	BitDefenderFalk	Android.Trojan.HiddenAds.ZA
Comodo	Malware#@#b030kr24zx4	Cynet	Malicious (score: 99)
DrWeb	Android.HiddenAds.238.origin	ESET-NOD32	A Variant Of Android/Hiddad.FQ
F-Secure	Malware ANDROID/Hiddad.FAZ.Gen	Fortinet	Android/Generic.Z.8EF5AAIt
Google	Detected	Ikarus	Trojan.AndroidOS.Hiddad
Jiangmin	AdWare.AndroidOS.fvhi	K7GW	Trojan (0053e0c31)
Kaspersky	HEUR:Trojan.AndroidOS.Hiddad.er	Kingsoft	Android.MALWARE.at_ghideads.ip.(kclo...)
Lionic	Trojan.AndroidOS.Hiddad.Clc	MAX	Malware (ai Score=99)
McAfee	ArtemisIB4E2D72BFFD1	Microsoft	Adware.AndroidOS/Multiverze

Symantec

Product	Description	Product	Description
Symantec Mobile Insight	AppRisk:Generisk	Tencent	Dos.Trojan.Hiddad.Timw
Trustlook	Android Malware General	Zillya	Trojan.Hiddad.Android.8980
ZoneAlarm by Check Point	HEUR:Trojan.AndroidOS.Hiddad.er	Acronis (Static ML)	Undetected
Add-Aware	Undetected	ALYac	Undetected
Arcabit	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	Cyren	Undetected
Elastic	Undetected	Emsisoft	Undetected
eScan	Undetected	GData	Undetected
Gridinsoft (no cloud)	Undetected	K7AntiVirus	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected
Panda	Undetected	Rising	Undetected

Application permissions:

Certificate Attributes

Valid From	2017-09-20 14:29:02
Valid To	2042-09-14 14:29:02
Serial Number	2464693e
Thumbprint	7b6ebb8503e59fce22de0a91ea3491326451ea1d

Certificate Subject

Distinguished Name	CN:TXM25000302
Common Name	TXM25000302

Certificate Issuer

Distinguished Name	CN:TXM25000302
Common Name	TXM25000302

Permissions

- ⚠ android.permission.INTERNET
- ⚠ com.android.launcher.permission.INSTALL_SHORTCUT
- ⚠ android.permission.SYSTEM_ALERT_WINDOW
- ⚠ android.permission.CHANGE_WIFI_STATE
- ⚠ android.permission.READ_PHONE_STATE
- ⚠ android.permission.WRITE_EXTERNAL_STORAGE
- ⓘ android.permission.CHANGE_NETWORK_STATE
- ⓘ android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
- ⓘ android.permission.READ_EXTERNAL_STORAGE
- ⓘ android.permission.RECEIVE_BOOT_COMPLETED

Main activity:

Activities

- trikitatalalaro.MainActivity
- trikitatalalaro.AgentActivity
- trikitatalalaro.SettingsActivity
- trikitatalalaro.alarm.AlarmActivity
- com.google.android.gms.ads.AdActivity
- com.tiffany.webbtech.core.WebViewActivity

Services

- trikitatalalaro.alarm.AlarmService
- com.tiffany.webbtech.core.UpdateService
- com.xdandroid.hellobdaemon.AbsWorkService\$WorkNotificationService
- com.xdandroid.hellobdaemon.JobSchedulerService
- com.xdandroid.hellobdaemon.WatchDogService
- com.xdandroid.hellobdaemon.WatchDogService\$WatchDogNotificationService

Receivers

- trikitatalalaro.alarm.AlarmReceiver
- trikitatalalaro.alarm.BootReceiver
- com.tiffany.webbtech.core.ScreenReceiver
- com.tiffany.webbtech.core.BootReceiver
- com.xdandroid.hellobdaemon.WakeUpReceiver
- com.xdandroid.hellobdaemon.WakeUpReceiver\$WakeUpAutoStartReceiver

Step 9:

Strings are as shown below:

The screenshot shows a browser window with three tabs open: 'VirusShare.com', 'VirusTotal - File - d3c950ae2ad0...', and 'VirusShare Account Created! - g...'. The main content area displays the file analysis results.

Intent Filters By Category

- + android.intent.category.DEFAULT
- + android.intent.category.LAUNCHER

Interesting Strings

```
http://alog.umeng.com/app_logs
http://alog.umengcloud.com/app_logs
http://plus.google.com/
http://schemas.android.com/apk/lib/com.google.android.gms.plus
http://www.google.com
https://cmmsguideryunos.com:443/genDeviceToken
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_banner.js
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_expanded_banner.js
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_interstitial.js
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40.html
https://googleads.g.doubleclick.net/mads/static/sdk/native/sdk-core-v40.html
https://uop.umeng.com
```

Bundle Info ⓘ

Warnings

⚠ Contains one or more Linux executables.

Contents Metadata

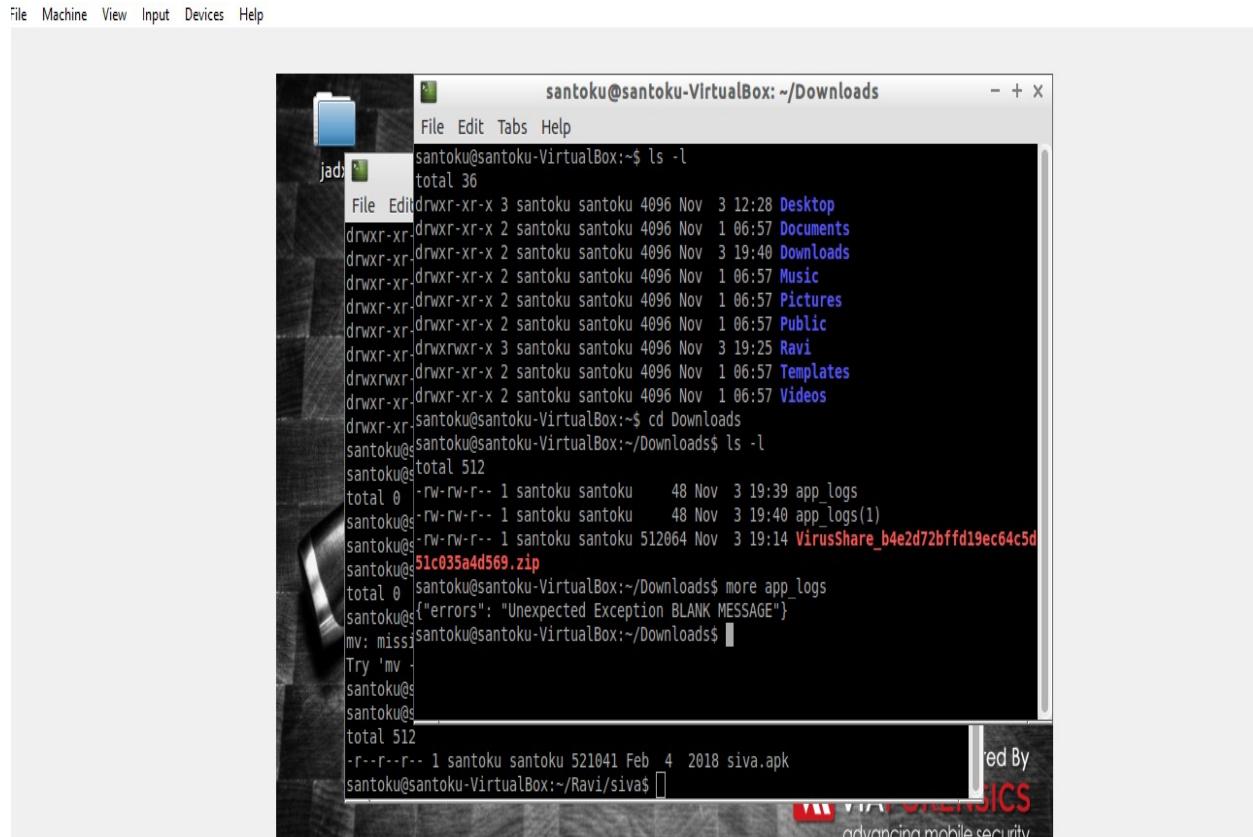
Step 10:

Installation of application logos:

We create the application logos by downloading from the links below:

http://alog.umeng.com/app_logs

http://alog.umengcloud.com/app_logs



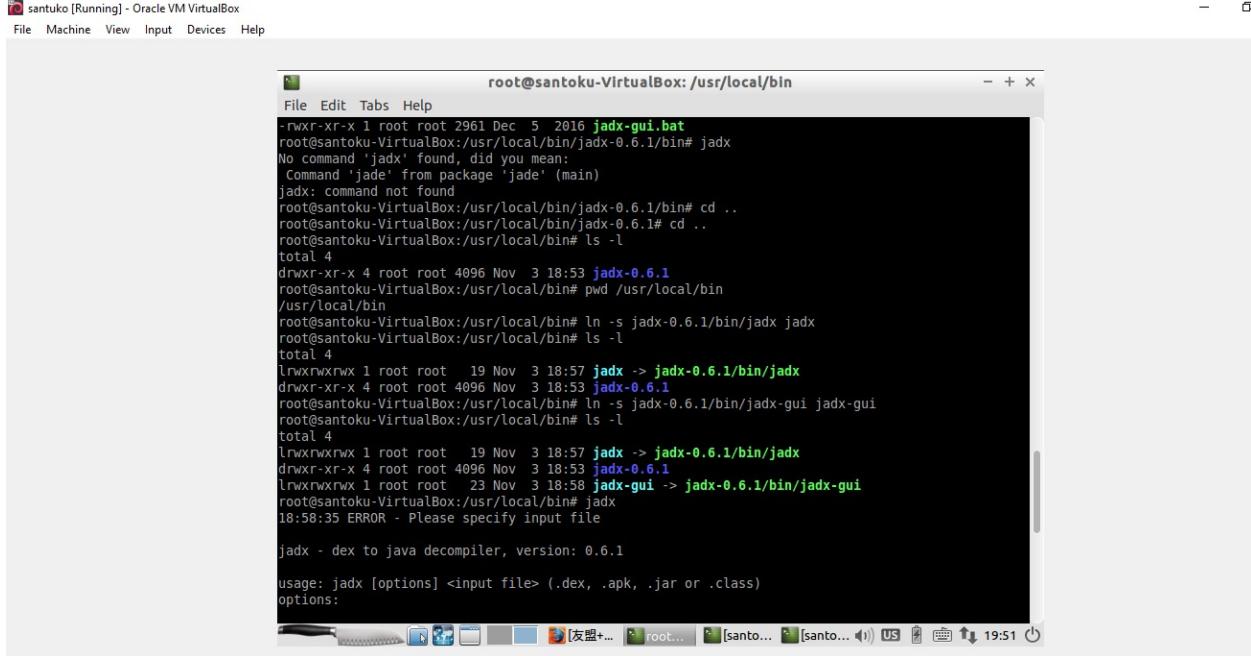
The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~/Downloads". The terminal displays the following command and its output:

```
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 36
drwxr-xr-x 3 santoku santoku 4096 Nov  3 12:28 Desktop
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Documents
drwxr-xr-x 2 santoku santoku 4096 Nov  3 19:40 Downloads
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Music
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Pictures
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Public
drwxr-xr-x 3 santoku santoku 4096 Nov  3 19:25 Ravi
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Templates
drwxr-xr-x 2 santoku santoku 4096 Nov  1 06:57 Videos
santoku@santoku-VirtualBox:~/Downloads$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 512
total 0
-rw-r--r-- 1 santoku santoku     48 Nov  3 19:39 app_logs
santoku@santoku-VirtualBox:~/Downloads$ more app_logs
santoku@santoku-VirtualBox:~/Downloads$ {"errors": "Unexpected Exception BLANK MESSAGE"}
mv: missing destination file operand after 'app_logs'
Try 'mv --help' for more information.
santoku@santoku-VirtualBox:~/Downloads$ mv app_logs 51c035a4d569.zip
santoku@santoku-VirtualBox:~/Downloads$ total 512
-rw-r--r-- 1 santoku santoku 521041 Feb  4  2018 siva.apk
santoku@santoku-VirtualBox:~/Downloads$ mv siva.apk Ravi/siva$
```

The terminal window has a watermark at the bottom right that reads "ADVANCED FORENSICS" and "advancing mobile security".

Step 11:

By using the command jadx-gui, we get the siva.apk application. In that application we see the source code and resources, androidmanifest.xml, classes.dex, resources.arsc.

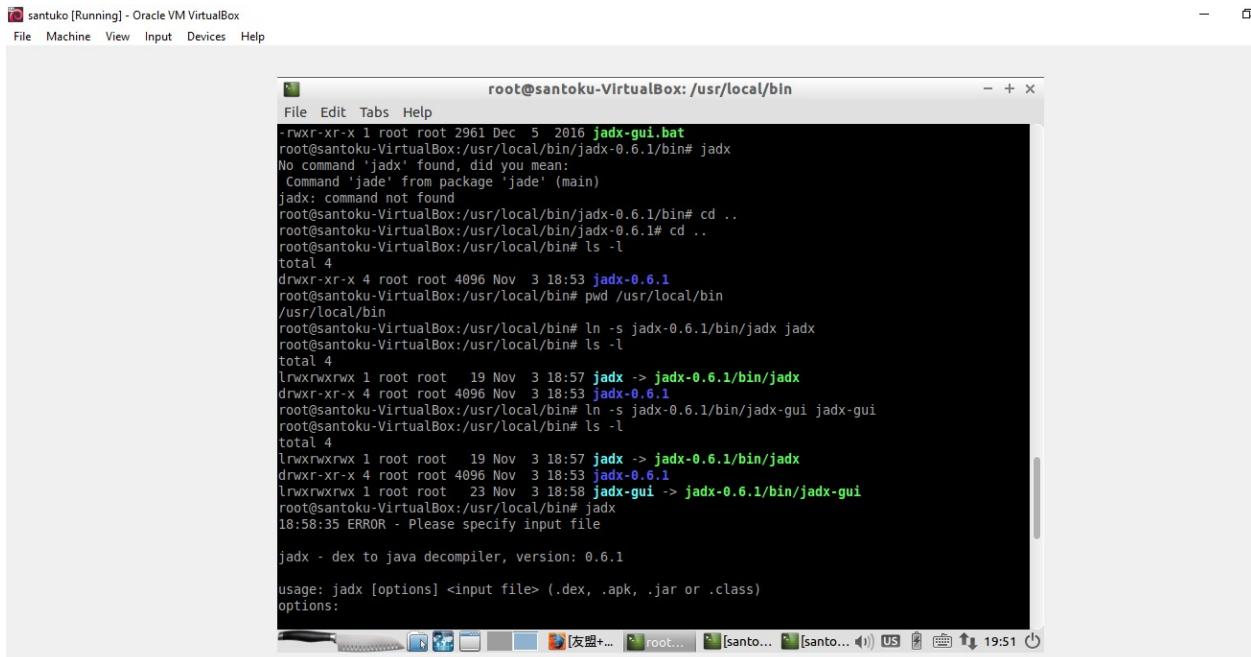


```
root@santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@santoku-VirtualBox: /usr/local/bin
root@...: ~ % jadx-gui.bat
-rwxr-xr-x 1 root root 2961 Dec 5 2016 jadx-gui.bat
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# jadx
No command 'jadx' found, did you mean:
  Command 'jade' from package 'jade' (main)
jadx: command not found
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# cd ..
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1# cd ..
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
drwxr-xr-x 4 root root 4096 Nov 3 18:53 jadx-0.6.1
root@santoku-VirtualBox:/usr/local/bin# pwd /usr/local/bin
/usr/local/bin
root@santoku-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx jadx
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 Nov 3 18:57 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 Nov 3 18:53 jadx-0.6.1
root@santoku-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx-gui jadx-gui
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 Nov 3 18:57 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 Nov 3 18:53 jadx-0.6.1
lrwxrwxrwx 1 root root 23 Nov 3 18:58 jadx-gui -> jadx-0.6.1/bin/jadx-gui
root@santoku-VirtualBox:/usr/local/bin# jadx-gui
18:58:35 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:
```



```
root@santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@santoku-VirtualBox: /usr/local/bin
root@...: ~ % jadx-gui.bat
-rwxr-xr-x 1 root root 2961 Dec 5 2016 jadx-gui.bat
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# jadx
No command 'jadx' found, did you mean:
  Command 'jade' from package 'jade' (main)
jadx: command not found
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1/bin# cd ..
root@santoku-VirtualBox:/usr/local/bin/jadx-0.6.1# cd ..
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
drwxr-xr-x 4 root root 4096 Nov 3 18:53 jadx-0.6.1
root@santoku-VirtualBox:/usr/local/bin# pwd /usr/local/bin
/usr/local/bin
root@santoku-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx jadx
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 Nov 3 18:57 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 Nov 3 18:53 jadx-0.6.1
root@santoku-VirtualBox:/usr/local/bin# ln -s jadx-0.6.1/bin/jadx-gui jadx-gui
root@santoku-VirtualBox:/usr/local/bin# ls -l
total 4
lrwxrwxrwx 1 root root 19 Nov 3 18:57 jadx -> jadx-0.6.1/bin/jadx
drwxr-xr-x 4 root root 4096 Nov 3 18:53 jadx-0.6.1
lrwxrwxrwx 1 root root 23 Nov 3 18:58 jadx-gui -> jadx-0.6.1/bin/jadx-gui
root@santoku-VirtualBox:/usr/local/bin# jadx-gui
18:58:35 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:
```

santuko [Running] - Oracle VM VirtualBox

jadx-gui - siva.apk

File View Navigation Tools Help

siva.apk

- Source code
 - com
 - trikita
- Resources
 - AndroidManifest.xml
 - META-INF
 - assets
 - classes.dex
 - res
 - resources.arsc

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.oscadr.nehemlia" platformBuildVersionCode="1">
<uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.GET_TASKS" />
<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_LOW" />
<application android:label="@string/app_name_p" android:icon="@drawable/icon" android:theme="@style/AppTheme">
<meta-data android:name="UMENG_APPKEY" android:value="599ee798f43e3a2d"/>
<meta-data android:name="UMENG_CHANNEL" android:value="TXM250003"/>
<activity android:theme="@style/AppTheme" android:label="@string/app_name">
<intent-filter>
<action android:name="android.intent.action.MAIN" />
```

santuko [Running] - Oracle VM VirtualBox

jadx-gui - siva.apk

File View Navigation Tools Help

siva.apk

- Source code
 - com
 - trikita
- Resources
 - AndroidManifest.xml
 - META-INF
 - assets
 - classes.dex
 - res
 - resources.arsc

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.oscadr.nehemlia" platformBuildVersionCode="1">
<uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.GET_TASKS" />
<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_LOW" />
<application android:label="@string/app_name_p" android:icon="@drawable/icon" android:theme="@style/AppTheme">
<meta-data android:name="UMENG_APPKEY" android:value="599ee798f43e3a2d"/>
<meta-data android:name="UMENG_CHANNEL" android:value="TXM250003"/>
<activity android:theme="@style/AppTheme" android:label="@string/app_name">
<intent-filter>
<action android:name="android.intent.action.MAIN" />
```

santuko [Running] - Oracle VM VirtualBox

Jadx-gui - siva.apk

File View Navigation Tools Help

AndroidManifest.xml

```
54
55
56    bel="@string/settings" android:name="trikita.talalarmo.AgentActivit
57
58    oid:name="com.oscadr.nehemliah" />
59    droid:name="android.intent.category.DEFAULT" />
60
61
62    bel="@string/settings" android:name="trikita.talalarmo.SettingsActi
63    me=@style/AppTheme" android:name="trikita.talalarmo.alarm.AlarmAc
64    me="trikita.talalarmo.alarm.AlarmReceiver" />
65    me="trikita.talalarmo.alarm.BootReceiver">
66
67    oid:name="android.intent.action.BOOT_COMPLETED" />
68
69
70    e="trikita.talalarmo.alarm.AlarmService" />
71    eme="@*android:style/Theme.Translucent" android:name="com.google.an
72    ne="com.tiffany.webbtech.core.UpdateService" android:exported="true"
73    me="com.tiffany.webbtech.core.ScreenReceiver" android:enabled="true
74
75    oid:name="android.intent.action.PACKAGE_ADDED" />
76    oid:name="android.intent.action.PACKAGE_REMOVED" />
77
78    d="trikita.talalarmo" />
```

santuko [Running] - Oracle VM VirtualBox

Jadx-gui - siva.apk

File View Navigation Tools Help

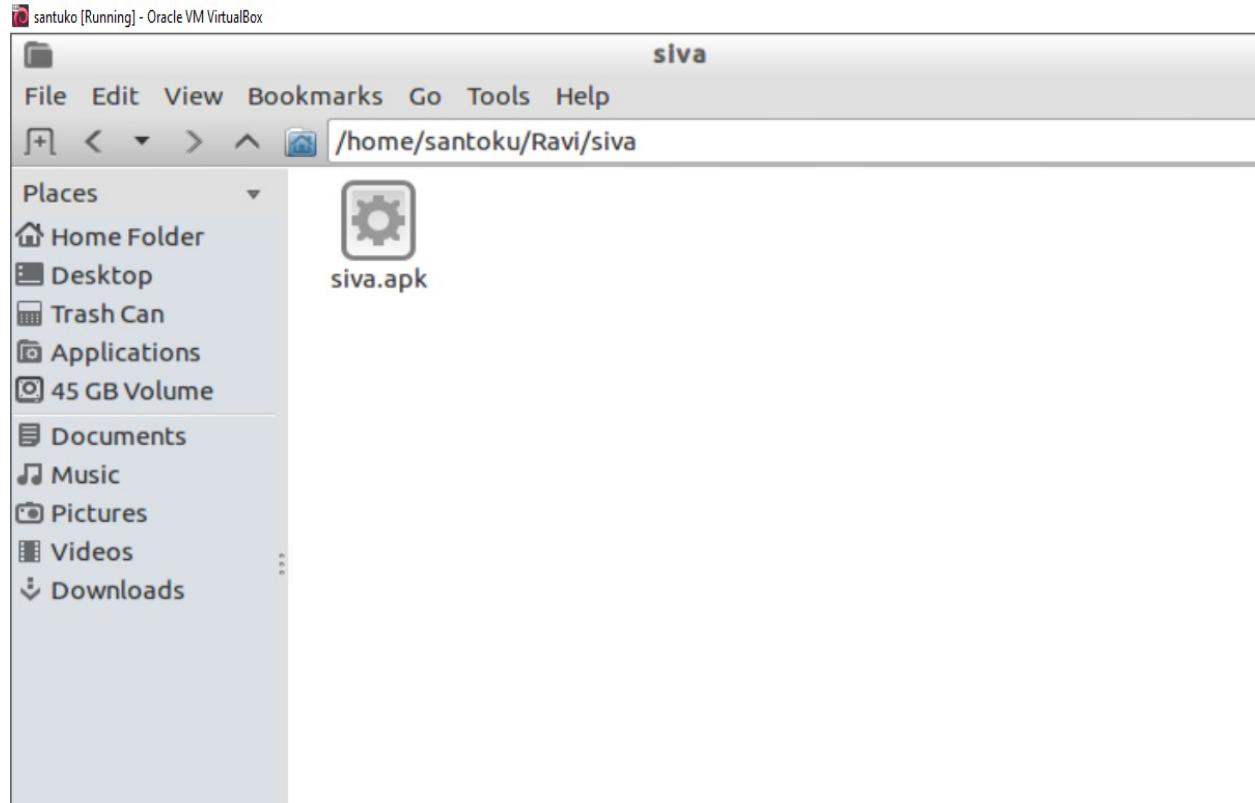
fest.xml resources.arsc com.a.a com.a.a.c

```
package com.a.a;

public class c {
    public static boolean a = true;
    public static String b = "";
    public static String c = "http://alog.umeng.com/app_logs";
    public static String d = "http://alog.umengcloud.com/app_logs";
    public static String[] e = new String[]{c, d};
    public static long f = 2097152;
}
```

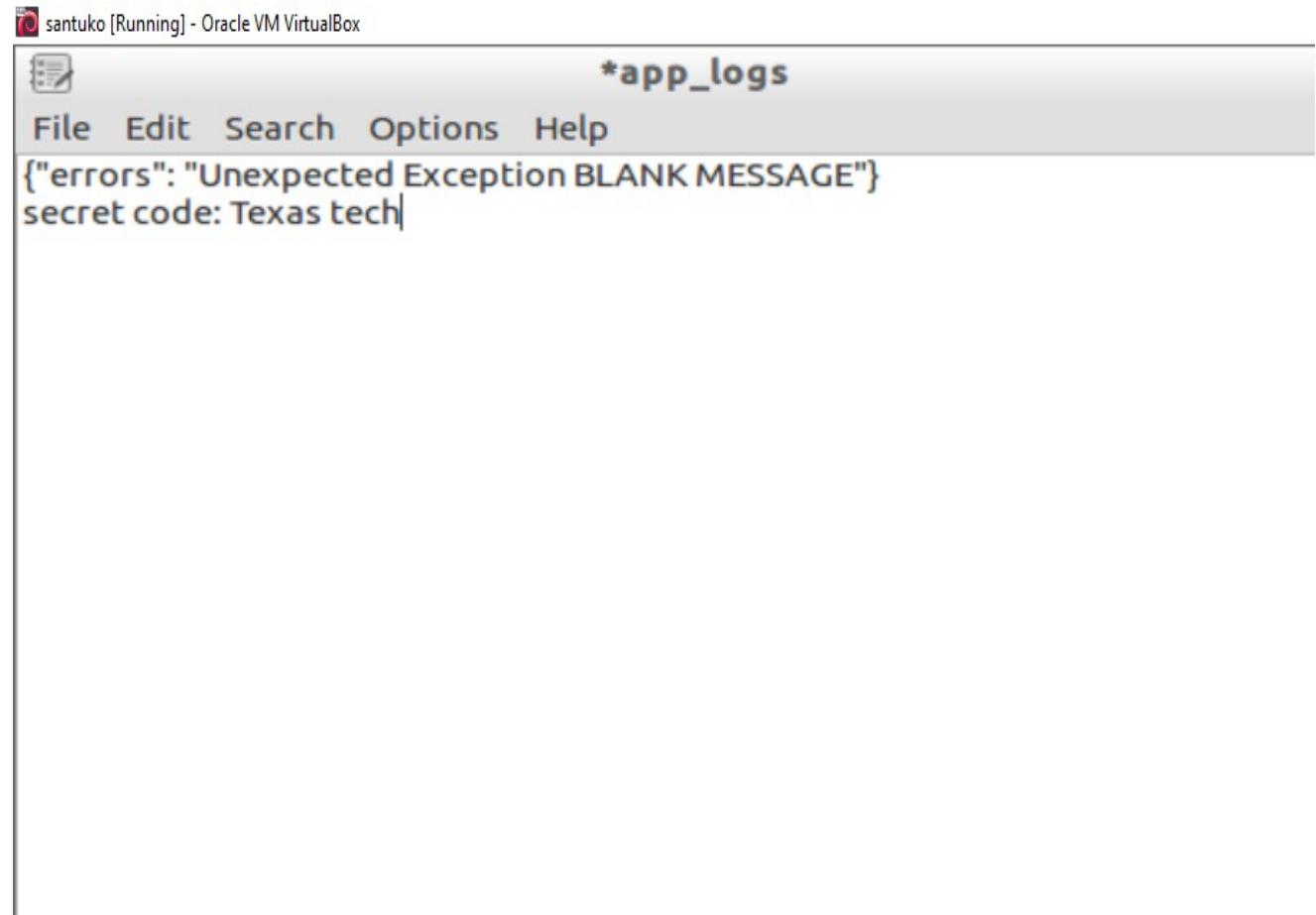
Step 12:

The created malicious application is:



Step 13:

The secret code is **Texas tech**



santuko [Running] - Oracle VM VirtualBox

*app_logs

File Edit Search Options Help

```
{"errors": "Unexpected Exception BLANK MESSAGE"}  
secret code: Texas tech|
```