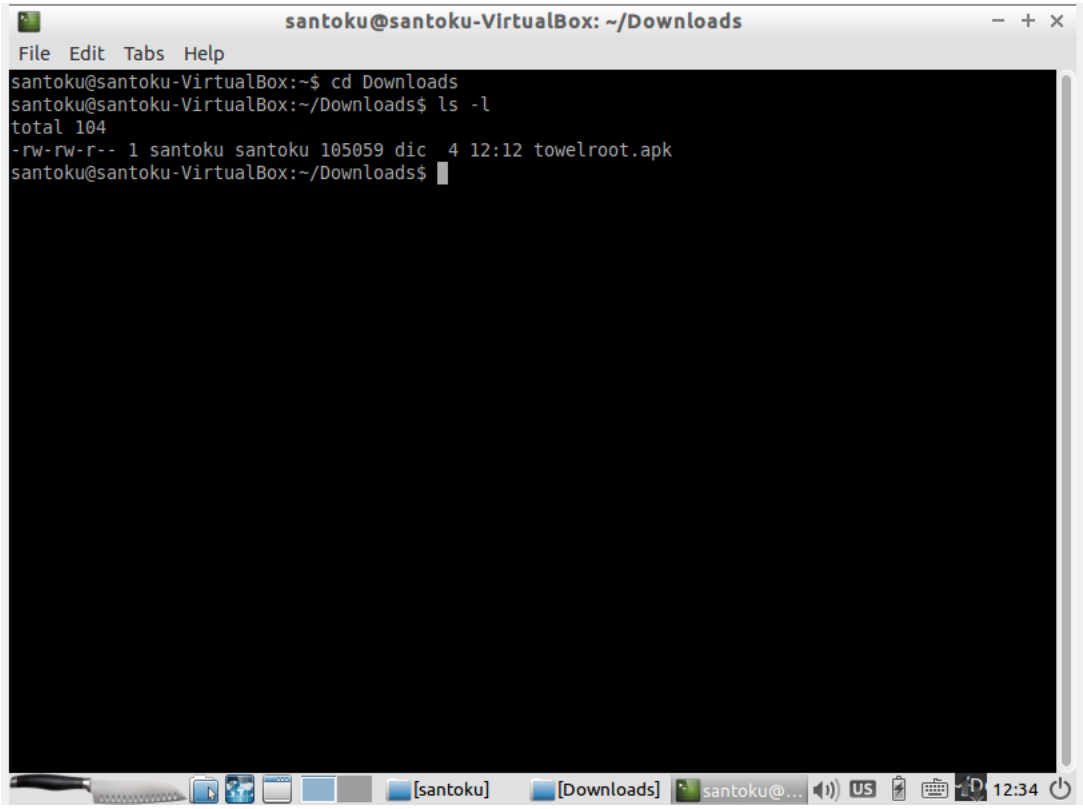
Digital Forensics (Security on Android applications)

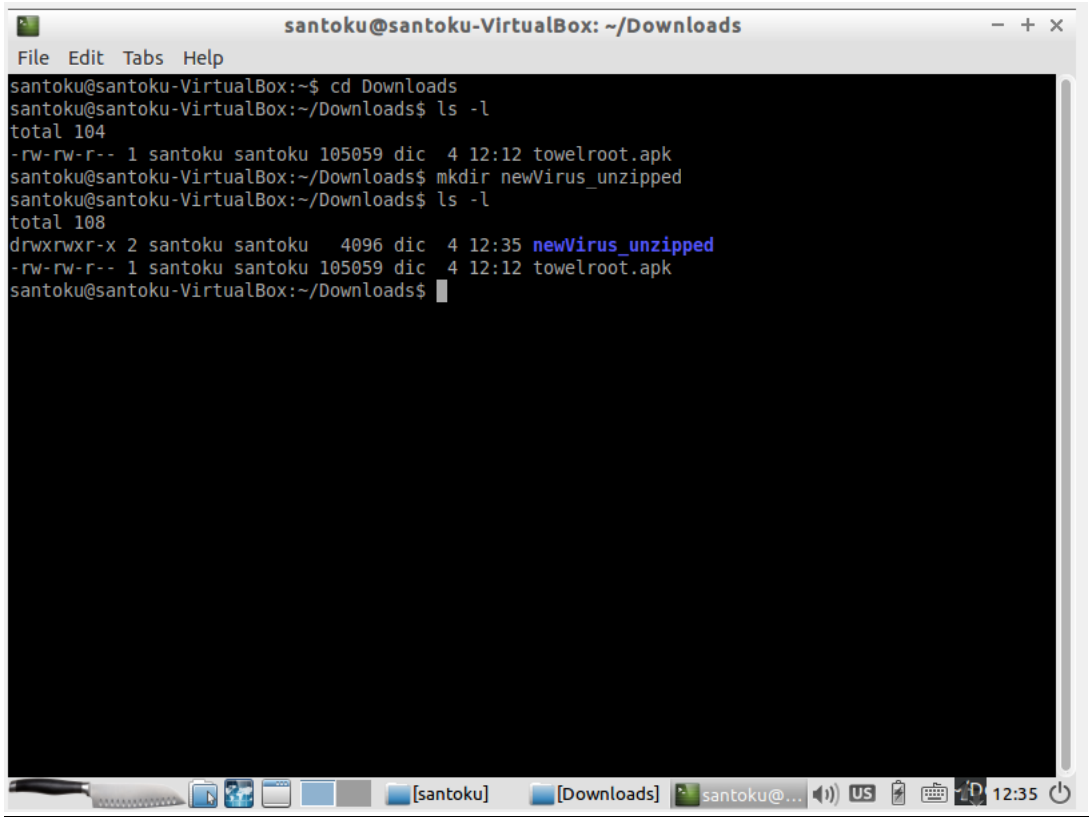
Report

Malware Type:

http://github.com/ashishb/android-malware/blob/master/towelroot/towelroot.apk



We made new directory



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

```
santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File  Edit  Tabs  Help
  inflating: META-INF/MANIFEST.MF
  inflating: META-INF/GEOHOT.SF
  inflating: META-INF/GEOHOT.RSA
  inflating: res/layout/mainlayout.xml
  inflating: AndroidManifest.xml
 extracting: resources.arsc
 extracting: res/drawable-xxhdpi/icon.png
  inflating: classes.dex
  inflating: lib/armeabi/libexploit.so
santoku@santoku-VirtualBox:~/Downloads$ unzip towelroot.apk -d newVirus_unzipped
Archive:  towelroot.apk
  inflating: newVirus_unzipped/META-INF/MANIFEST.MF
  inflating: newVirus_unzipped/META-INF/GEOHOT.SF
  inflating: newVirus_unzipped/META-INF/GEOHOT.RSA
  inflating: newVirus_unzipped/res/layout/mainlayout.xml
  inflating: newVirus_unzipped/AndroidManifest.xml
 extracting: newVirus_unzipped/resources.arsc
 extracting: newVirus_unzipped/res/drawable-xxhdpi/icon.png
  inflating: newVirus_unzipped/classes.dex
  inflating: newVirus_unzipped/lib/armeabi/libexploit.so
santoku@santoku-VirtualBox:~/Downloads$ cd newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ls -l
total 28
-rw-rw-r-- 1 santoku santoku 1836 jun 20  2014 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku 5532 jun 20  2014 classes.dex
drwxrwxr-x 3 santoku santoku 4096 dic  4 12:38 lib
drwxrwxr-x 2 santoku santoku 4096 dic  4 12:38 META-INF
drwxrwxr-x 4 santoku santoku 4096 dic  4 12:38 res
-rw-rw-r-- 1 santoku santoku 1480 jun 20  2014 resources.arsc
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$
```

santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped

File Edit Tabs Help

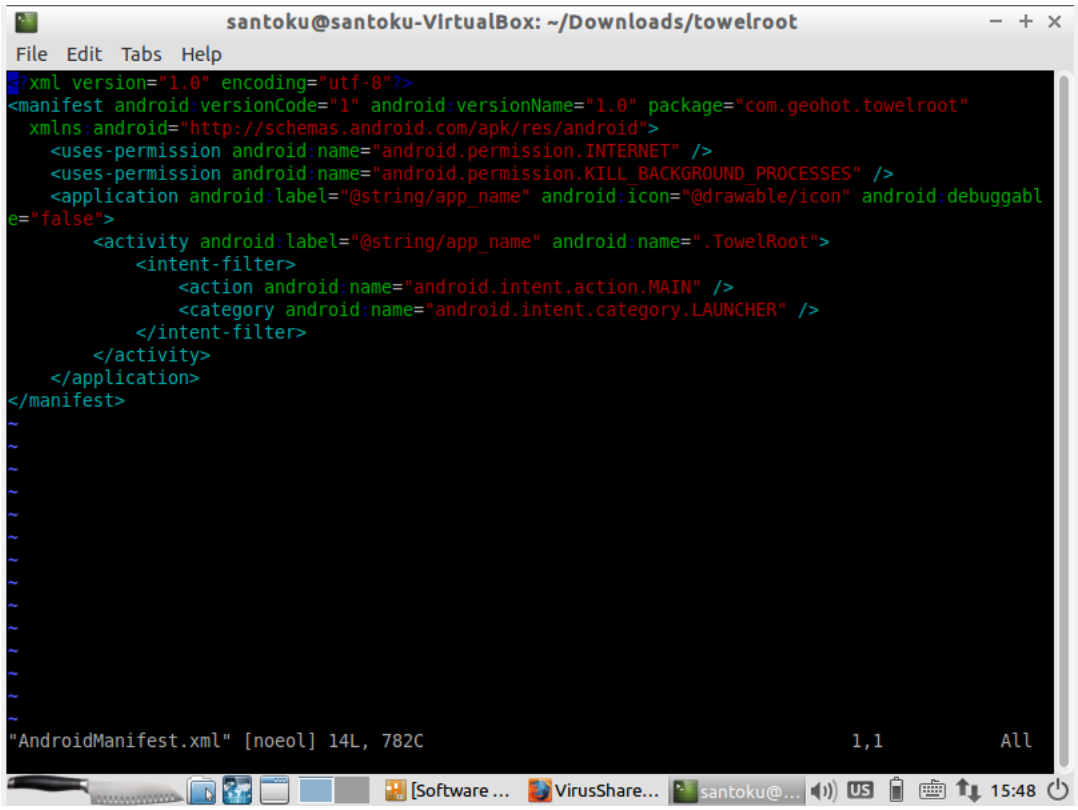
```
Archive:  towelroot.apk
  inflating: newVirus_unzipped/META-INF/MANIFEST.MF
  inflating: newVirus_unzipped/META-INF/GEOHOT.SF
  inflating: newVirus_unzipped/META-INF/GEOHOT.RSA
  inflating: newVirus_unzipped/res/layout/mainlayout.xml
  inflating: newVirus_unzipped/AndroidManifest.xml
 extracting: newVirus_unzipped/resources.arsc
 extracting: newVirus_unzipped/res/drawable-xxhdpi/icon.png
  inflating: newVirus_unzipped/classes.dex
  inflating: newVirus_unzipped/lib/armeabi/libexploit.so
santoku@santoku-VirtualBox:~/Downloads$ cd newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ls -l
total 28
-rw-rw-r-- 1 santoku santoku 1836 jun 20  2014 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku 5532 jun 20  2014 classes.dex
drwxrwxr-x 3 santoku santoku 4096 dic  4 12:38 lib
drwxrwxr-x 2 santoku santoku 4096 dic  4 12:38 META-INF
drwxrwxr-x 4 santoku santoku 4096 dic  4 12:38 res
-rw-rw-r-- 1 santoku santoku 1480 jun 20  2014 resources.arsc
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ll
total 36
drwxrwxr-x 5 santoku santoku 4096 dic  4 12:38 ./
drwxr-xr-x 6 santoku santoku 4096 dic  4 12:36 ../
-rw-rw-r-- 1 santoku santoku 1836 jun 20  2014 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku 5532 jun 20  2014 classes.dex
drwxrwxr-x 3 santoku santoku 4096 dic  4 12:38 lib/
drwxrwxr-x 2 santoku santoku 4096 dic  4 12:38 META-INF/
drwxrwxr-x 4 santoku santoku 4096 dic  4 12:38 res/
-rw-rw-r-- 1 santoku santoku 1480 jun 20  2014 resources.arsc
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$
```

[santoku] Downloads santoku@... US 12:51

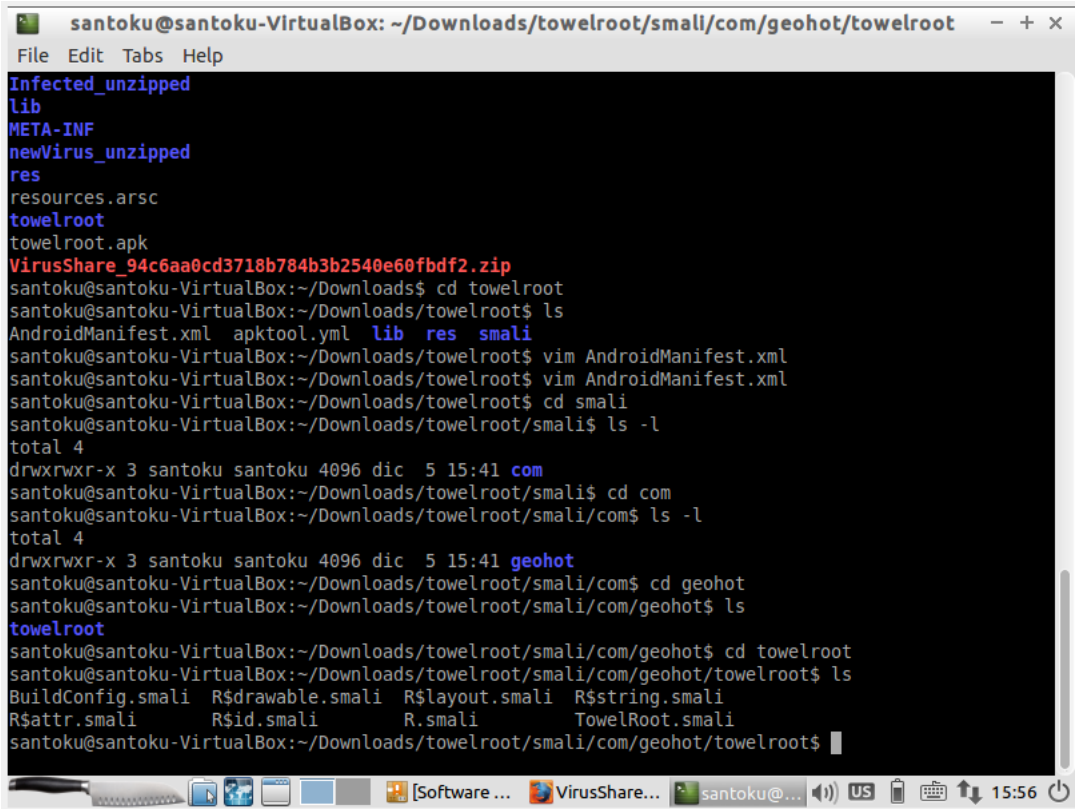
We try to decompile the file using apk tool

```
santoku@santoku-VirtualBox: ~/Downloads/towelroot
File  Edit  Tabs  Help
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/santoku/apktool/framework/1.apk
I: Loaded.
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Done.
I: Copying assets and libs...
santoku@santoku-VirtualBox:~/Downloads$ ls
AndroidManifest.xml
classes.dex
-f
f4c9715b4dbcfa893ee439699c81a933912759a20822fc6a5352d494d2afe2bd
Infected_unzipped
lib
META-INF
newVirus_unzipped
res
resources.arsc
towelroot
towelroot.apk
VirusShare_94c6aa0cd3718b784b3b2540e60fbdf2.zip
santoku@santoku-VirtualBox:~/Downloads$ cd towelroot
santoku@santoku-VirtualBox:~/Downloads/towelroot$ ls
AndroidManifest.xml  apktool.yml  lib  res  smali
santoku@santoku-VirtualBox:~/Downloads/towelroot$ vim AndroidManifest.xml
santoku@santoku-VirtualBox:~/Downloads/towelroot$
```

Using vim command, we try to open the Android manifest.xml file which shows the permission the malware used.



We can see in side the smali which is assembly language code which may contain several files



All the file inside smali files seems to contain empty files

```
santoku@santoku-VirtualBox: ~/Downloads/towelroot/smali/com/geohot/towelroot
File  Edit  Tabs  Help
total 4
drwxrwxr-x 3 santoku santoku 4096 dic  5 15:41 geohot
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com$ cd geohot
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot$ ls
towelroot
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot$ cd towelroot
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ ls
BuildConfig.smali  R$drawable.smali  R$layout.smali  R$string.smali
R$attr.smali       R$id.smali        R.smali         TowelRoot.smali
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd BuildConfig.smali
bash: cd: BuildConfig.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R$drawable.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R$layout.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R$string.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ R$attr.smali
R.smali: command not found
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R$sttr.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R$id.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd R.smali
bash: cd: R.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$ cd TowelRoot.smali
bash: cd: TowelRoot.smali: Not a directory
santoku@santoku-VirtualBox:~/Downloads/towelroot/smali/com/geohot/towelroot$
```

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

```
santoku@santoku-VirtualBox: ~/Downloads/towelroot/res/values
File  Edit  Tabs  Help
total 13940
-rw-rw-r-- 1 santoku santoku    1836 jun 20  2014 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku    5532 jun 20  2014 classes.dex
drwxrwxr-x 5 santoku santoku    4096 dic  4 13:17 -f
-rw-r--r-- 1 santoku santoku 7343494 oct  3 10:33 f4c9715b4dbcfa893ee439699c81a933912759a20822fc6
a5352d494d2afe2bd
drwxrwxr-x 2 santoku santoku    4096 dic  5 15:37 Infected_unzipped
drwxrwxr-x 3 santoku santoku    4096 dic  4 12:36 lib
drwxrwxr-x 2 santoku santoku    4096 dic  4 12:36 META-INF
drwxrwxr-x 5 santoku santoku    4096 dic  5 15:41 newVirus_unzipped
drwxrwxr-x 4 santoku santoku    4096 dic  4 12:36 res
-rw-rw-r-- 1 santoku santoku    1480 jun 20  2014 resources.arsc
drwxrwxr-x 5 santoku santoku    4096 dic  5 15:52 towelroot
-rw-rw-r-- 1 santoku santoku  105059 dic  4 12:12 towelroot.apk
-rw-rw-r-- 1 santoku santoku 6774805 dic  5 10:43 VirusShare_94c6aa0cd3718b784b3b2540e60fbdf2.zip
santoku@santoku-VirtualBox:~/Downloads$ cd towelroot
santoku@santoku-VirtualBox:~/Downloads/towelroot$ ls -l
total 20
-rw-rw-r-- 1 santoku santoku  782 dic  5 15:41 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku  231 dic  5 15:41 apktool.yml
drwxrwxr-x 3 santoku santoku 4096 dic  5 15:41 lib
drwxrwxr-x 5 santoku santoku 4096 dic  5 15:41 res
drwxrwxr-x 3 santoku santoku 4096 dic  5 15:41 smali
santoku@santoku-VirtualBox:~/Downloads/towelroot$ cd res
santoku@santoku-VirtualBox:~/Downloads/towelroot/res$ ls
drawable-xxhdpi  layout  values
santoku@santoku-VirtualBox:~/Downloads/towelroot/res$ cd values
santoku@santoku-VirtualBox:~/Downloads/towelroot/res/values$ ls
ids.xml  public.xml  strings.xml
santoku@santoku-VirtualBox:~/Downloads/towelroot/res/values$
```

santoku@santoku-VirtualBox: ~/Downloads/towelroot/res/values

File Edit Tabs Help

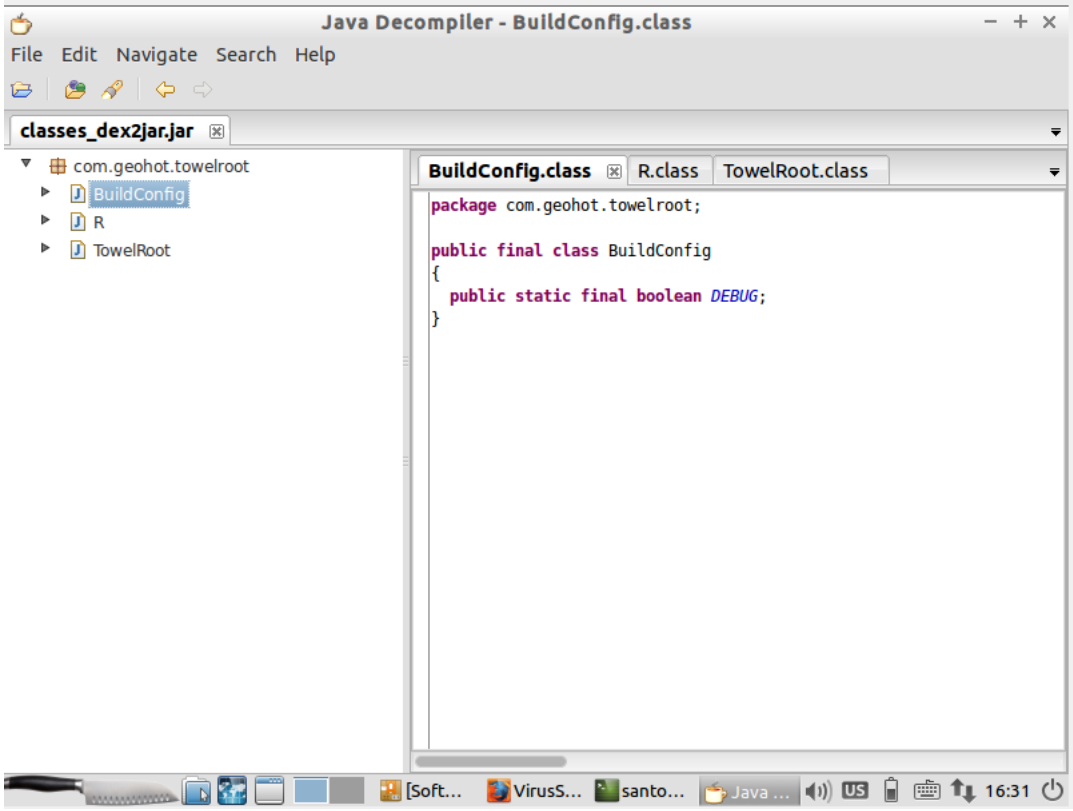
```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">towelroot</string>
    <string name="starting">"Click the button to root
No more reboot required

Phone version is sent to server
To improve device support"</string>
</resources>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"strings.xml" 9L, 258C                                    1,1           All
```

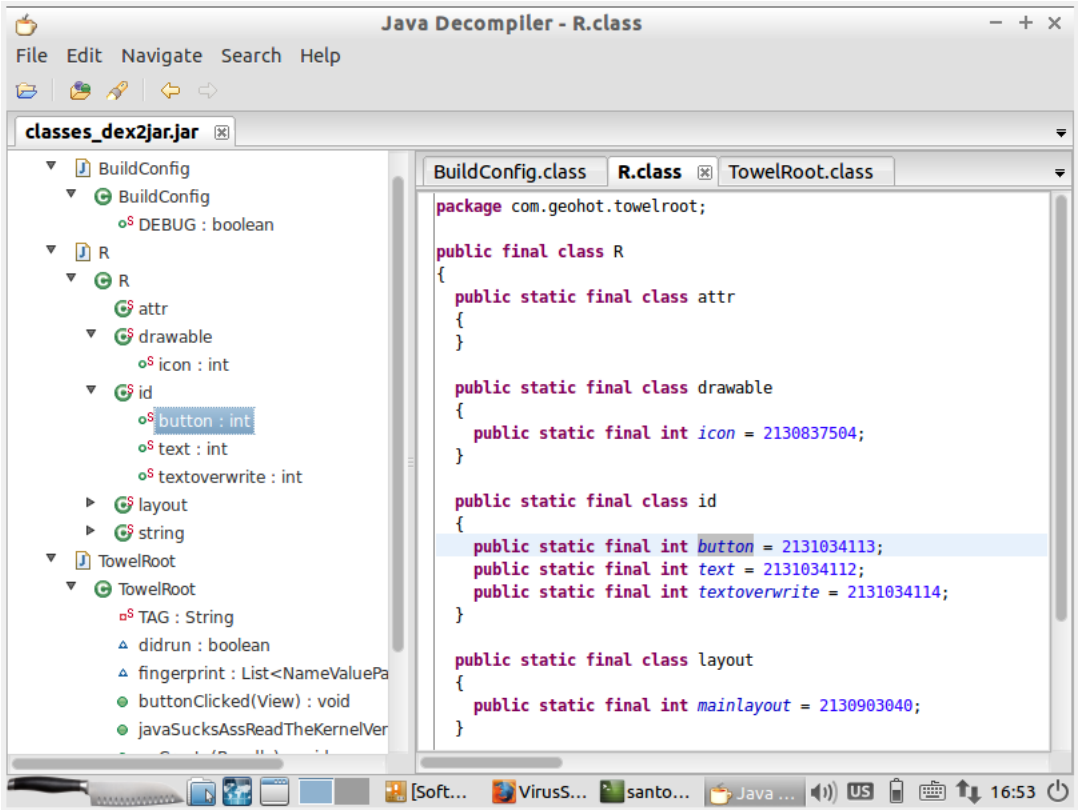
[Software ... VirusShare... santoku@... 16:14

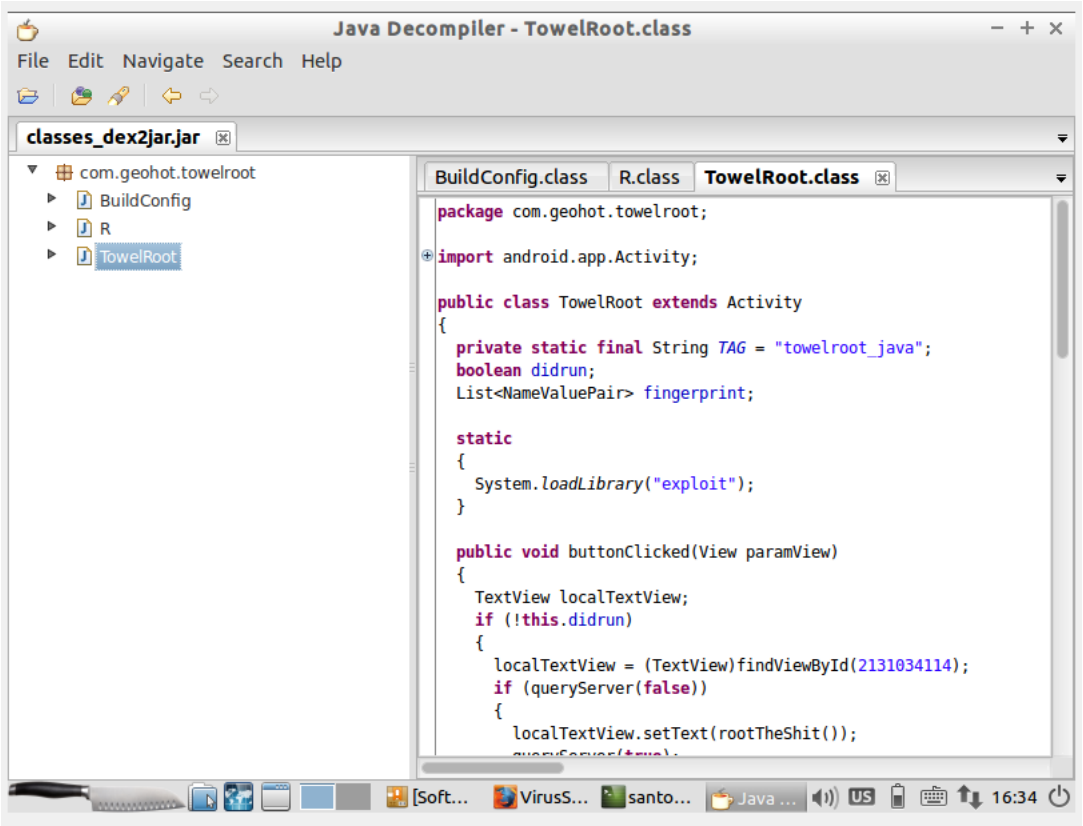
Now we can convert the classes.dex file to jar in the original unzipped file in the malware, which allow us to access the source file. (using JD-GUI inside Santuko)

```
santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File  Edit  Tabs  Help
santoku@santoku-VirtualBox:~/Downloads$ cd towelroot
santoku@santoku-VirtualBox:~/Downloads/towelroot$ ls -l
total 20
-rw-rw-r-- 1 santoku santoku  782 dic  5 15:41 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku  231 dic  5 15:41 apktool.yml
drwxrwxr-x 3 santoku santoku 4096 dic  5 15:41 lib
drwxrwxr-x 5 santoku santoku 4096 dic  5 15:41 res
drwxrwxr-x 3 santoku santoku 4096 dic  5 15:41 smali
santoku@santoku-VirtualBox:~/Downloads/towelroot$ cd res
santoku@santoku-VirtualBox:~/Downloads/towelroot/res$ ls
drawable-xxhdpi  layout  values
santoku@santoku-VirtualBox:~/Downloads/towelroot/res$ cd values
santoku@santoku-VirtualBox:~/Downloads/towelroot/res/values$ ls
ids.xml  public.xml  strings.xml
santoku@santoku-VirtualBox:~/Downloads/towelroot/res/values$ vim strings.xml
santoku@santoku-VirtualBox:~/Downloads/towelroot/res/values$ cd ..
santoku@santoku-VirtualBox:~/Downloads/towelroot/res$ cd ..
santoku@santoku-VirtualBox:~/Downloads/towelroot$ cd ..
santoku@santoku-VirtualBox:~/Downloads$ cd newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ls
AndroidManifest.xml  classes.dex  lib  META-INF  res  resources.arsc
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ 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-VirtualBox:~/Downloads/newVirus_unzipped$ ls
AndroidManifest.xml  classes.dex  classes_dex2jar.jar  lib  META-INF  res  resources.arsc
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$
```

The jar file we created contains lots of random classes and sub classes




Java Decompiler - R.class
File Edit Navigate Search Help
classes_dex2jar.jar
BuildConfig
BuildConfig
DEBUG : boolean
R
R
attr
drawable
icon : int
id
button : int
text : int
textoverwrite : int
layout
string
TowelRoot
TowelRoot
TAG : String
didrun : boolean
fingerprint : List<NameValuePa
buttonClicked(View) : void
javaSucksAssReadTheKernelVer
BuildConfig.class
R.class
TowelRoot.class
package com.geohot.towelroot;
public final class R
{
public static final class attr
{
}
public static final class drawable
{
public static final int icon = 2130837504;
}
public static final class id
{
public static final int button = 2131034113;
public static final int text = 2131034112;
public static final int textoverwrite = 2131034114;
}
public static final class layout
{
public static final int mainlayout = 2130903040;
}
[Soft...
VirusS...
santo...
Java ...
16:53



The programmer is using localTextView method which is used to perform sensitive operation and data processing on the server side.

Also, We see List and keys on the source code which are part of Hash function , here programmer is trying to interfere the hash function to collide the hash bins.

Clientprotocol is being used which represents the client network and allows to communicate with with SQL server.

Conclusion :

This Application looks suspicious