**CS 6345 Digital Forensics**

**Assignment -2**

**Stage -1**

**Creating A Malicious Android Application**

Ravi Sankar Gogineni-R11788968

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

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

Graphical user interface, text, application

Description automatically generated

**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

wgethttps://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.

Graphical user interface, text

Description automatically generated

**Step-4**:

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

Graphical user interface, text, application, email

Description automatically generated

The resultant application details will be as follows:

Graphical user interface, text, application

Description automatically generated

The malicious part of the application is MD5

B4e2d72bffd19ec64c51c035a4d569

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

Graphical user interface, text, application

Description automatically generated

**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:

Graphical user interface

Description automatically generated

**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:

Graphical user interface, text

Description automatically generated

**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:

Text

Description automatically generated

**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:**

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

**Application permissions:**

Graphical user interface, text, application, email

Description automatically generated

**Main activity:**

Graphical user interface, text, application

Description automatically generated

**Step 9**:

Strings are as shown below:

Graphical user interface, text, application

Description automatically generated

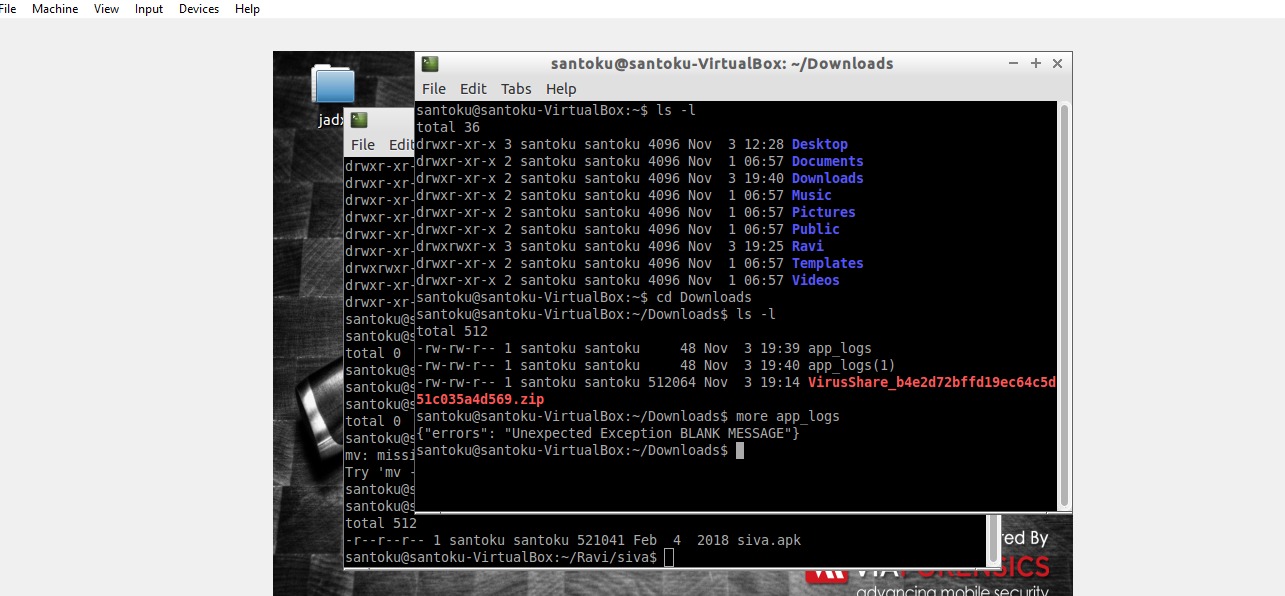
**Step 10:**

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>



**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, clsses.dex, resources.arsc.

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**Step 12**:

The created malicious application is:

Graphical user interface, text, application, email

Description automatically generated

**Step 13**:

The secret code is **Texas tech**

Graphical user interface, text, application, email

Description automatically generated