DIGITAL FORENSIC PROJECT

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

MALWARE ANALYSIS OF ANDROID PHONE

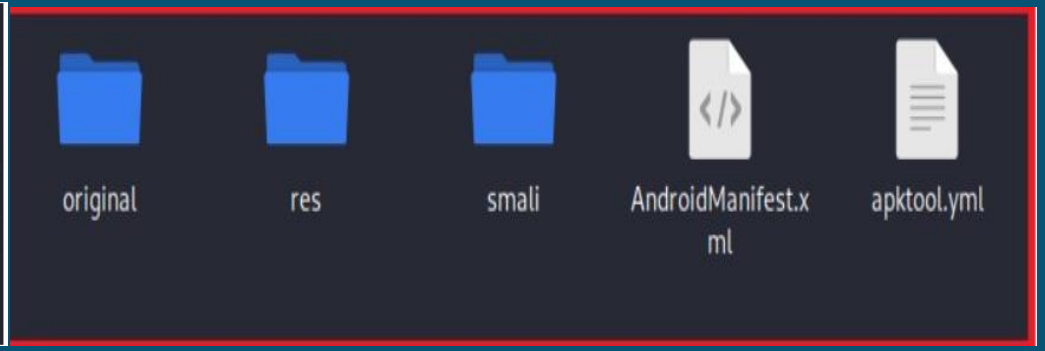
MALWARE ANALYSIS OF ANDROID PHONE

Project Name: Malware Analysis of Android Phone

Tool Used: Dex2Jar (Version 0.0.9.15), JD-GUI (Version 1.6.6), APKTool (Version 2.3.3), Mobile Security Framework (Version 3.2.)

Platform: Windows, Kali Linux

```
$ apktool d 021d55c415ff951c8e7b1ce3f94399bb.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty on 021d55c415ff951c8e7b1ce3f94399bb.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...
```

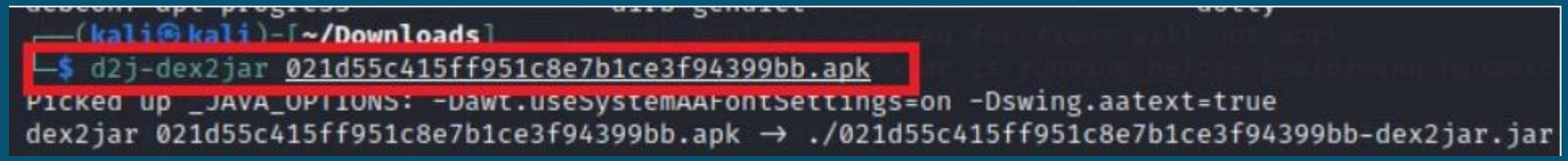


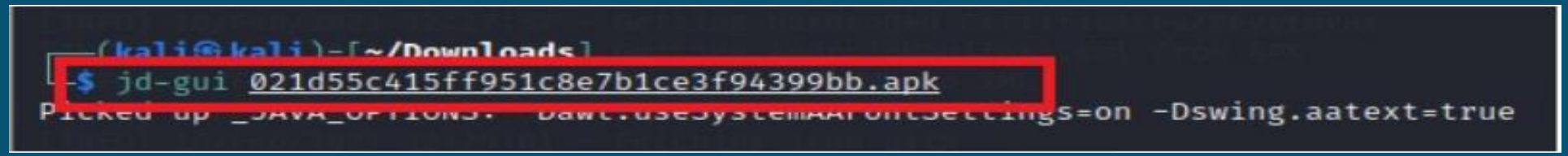
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

MALWARE ANALYSIS OF ANDROID PHONE

DESCRIPTION :

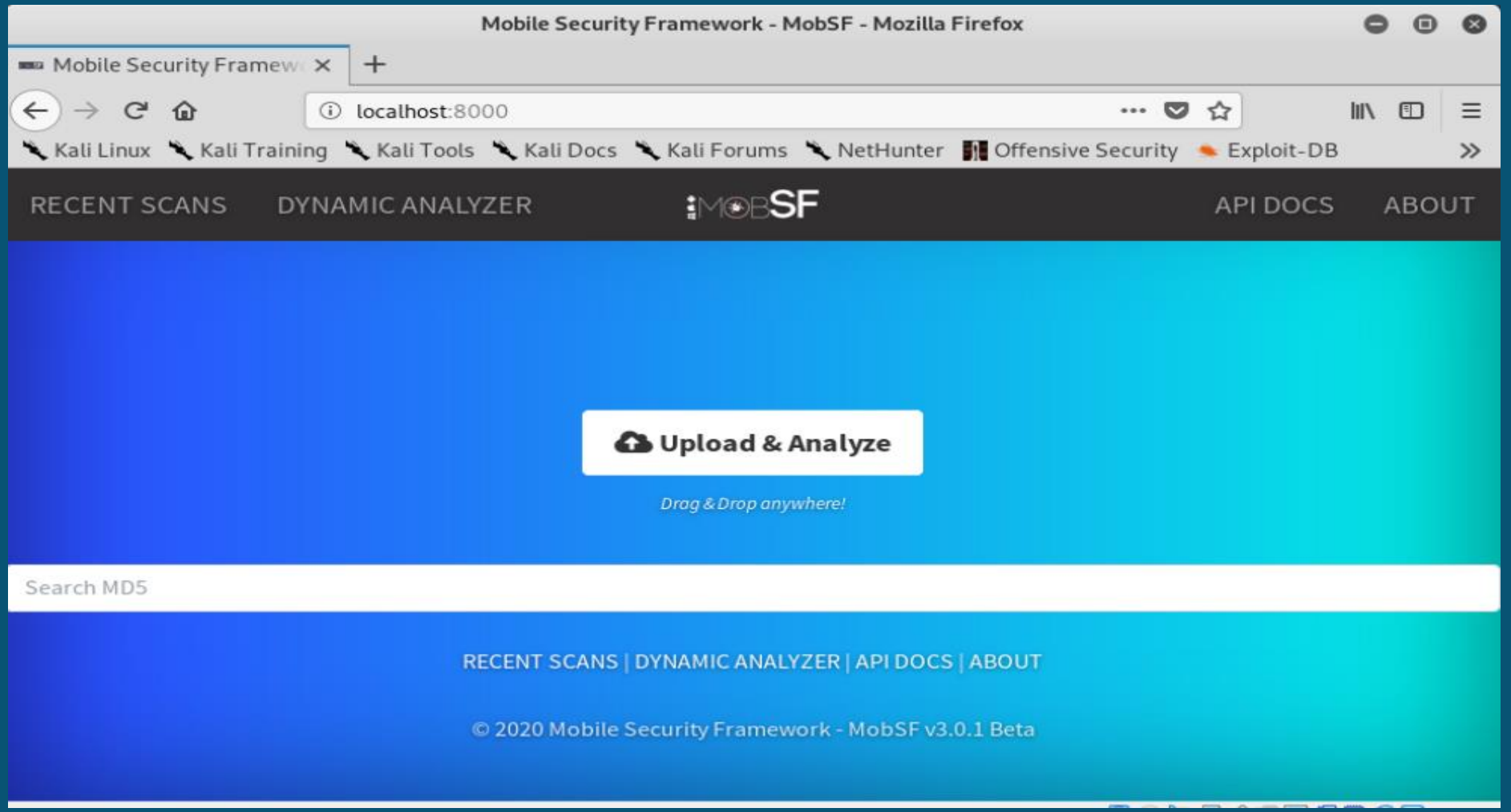
Object of the project is to Analyze malicious code embedded In the APK by reverse engineering the application. And then using static analyzing for malicious code embedded in the APK. Operating system was 'KALI LINUX' and tools used for analysis , reverse engineering and for embedded code are as follows Dex2Jar (Version 0.0.9.15), JD-GUI (Version 1.6.6), APKTool (Version 2.3.3), Mobile Security Framework (version 3.2.)





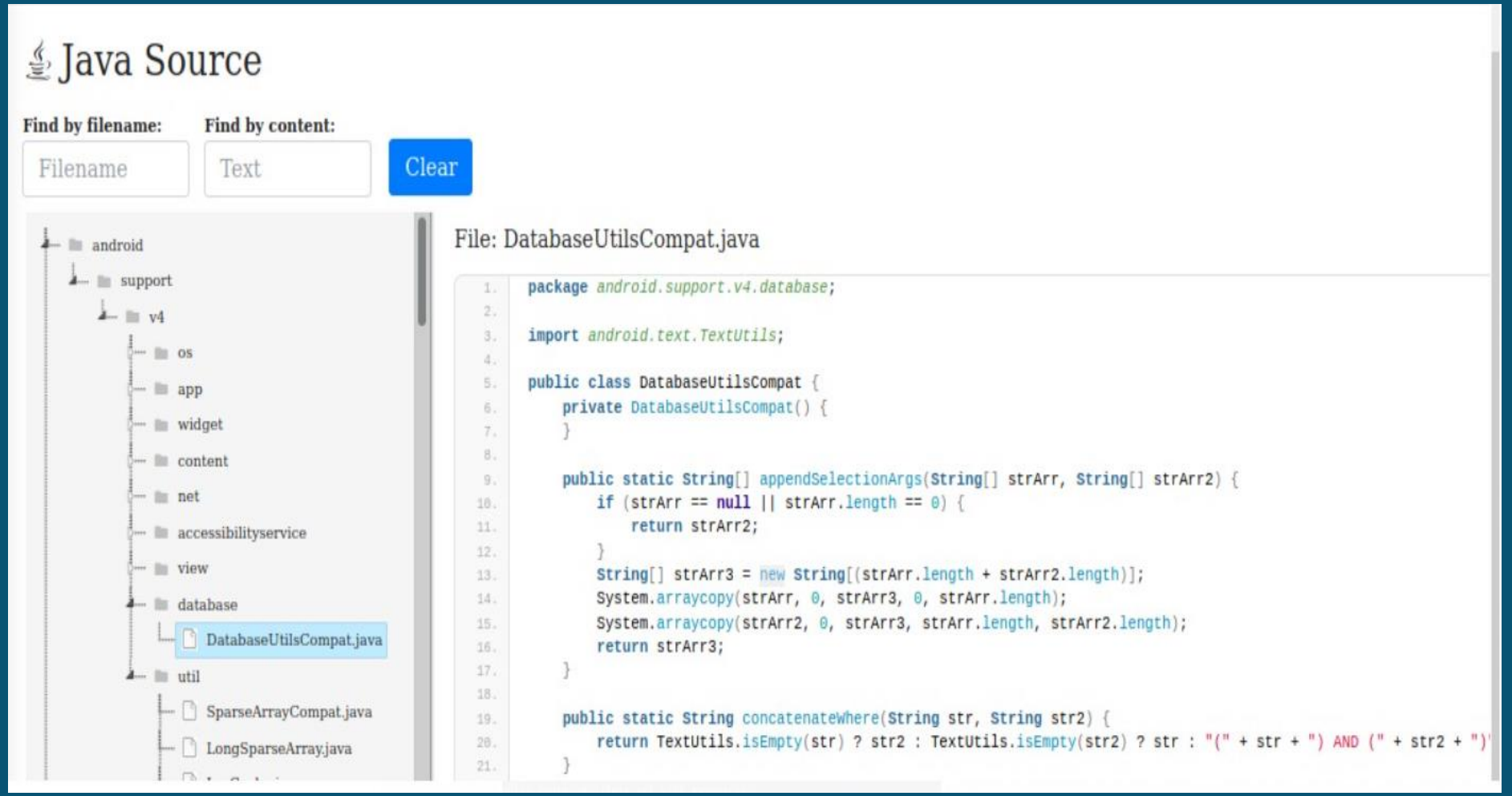
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

MALWARE ANALYSIS OF ANDROID PHONE



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

MALWARE ANALYSIS OF ANDROID PHONE



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.