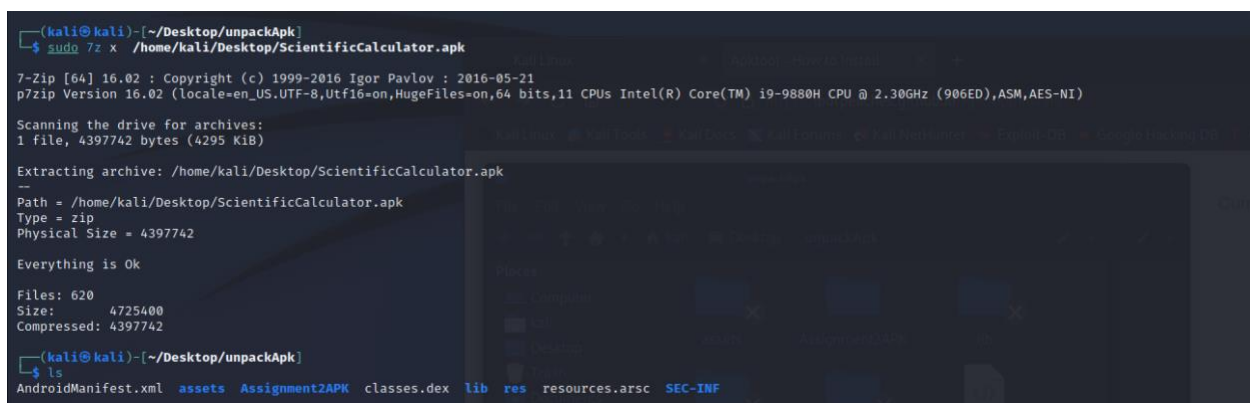


Malicious APK File Analysis No. 2

Your job is to investigate the content of a given malicious Android app. Using the tools given in the above and below link and also the ones presented in the class to learn about analysis of apk file, your job is to analyze the given app and reveal the secret code along with the description of what the malicious part is trying to do:

Step 1: Get malcous apk unzip using password provide and create unpackApk folder.



```
(kali@kali)~[/Desktop/unpackApk]
$ sudo 7z x /home/kali/Desktop/ScientificCalculator.apk

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,11 CPUs Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz (906ED),ASM,AES-NI)

Scanning the drive for archives:
1 file, 4397742 bytes (4295 KiB)

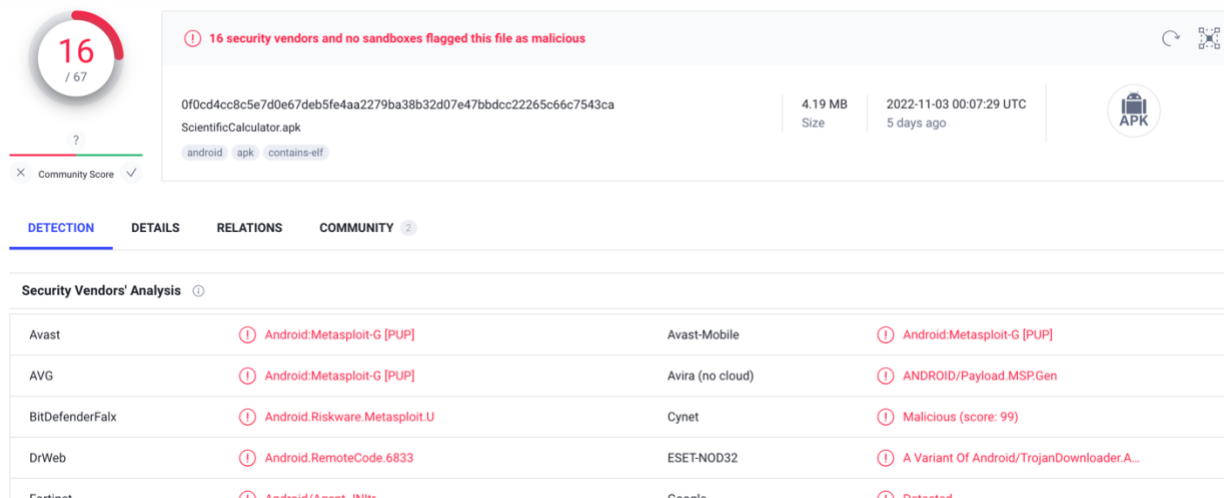
Extracting archive: /home/kali/Desktop/ScientificCalculator.apk
-
Path = /home/kali/Desktop/ScientificCalculator.apk
Type = zip
Physical Size = 4397742

Everything is Ok

Files: 620
Size: 4725400
Compressed: 4397742

(kali@kali)~[/Desktop/unpackApk]
$ ls
AndroidManifest.xml  assets  Assignment2APK  classes.dex  lib  res  resources.arsc  SEC-INF
```

Step 2: Check the apk from virus total to get the details of malware inside.



The screenshot shows the VirusTotal analysis page for the file `ScientificCalculator.apk`. The file is identified as `0f0cd4cc8c5e7d0e67deb5fe4aa2279ba38b32d07e47bbdcc22265c66c7543ca`, with a size of 4.19 MB and was uploaded 5 days ago. It is flagged as malicious by 16 security vendors. The file contains ELF (executable and linkable format) code. The 'DETECTION' tab is active, showing a table of security vendors' analysis.

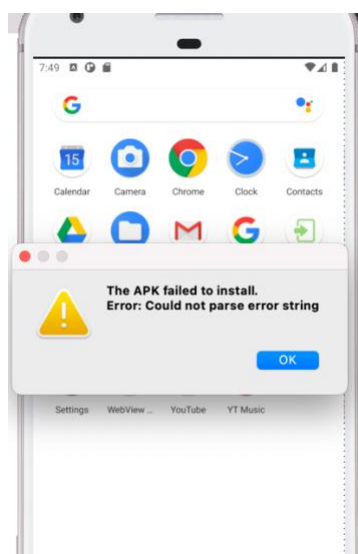
Security Vendors' Analysis			
Avast	Android.Metasploit-G [PUP]	Avast-Mobile	Android.Metasploit-G [PUP]
AVG	Android.Metasploit-G [PUP]	Avira (no cloud)	ANDROID/Payload.MSP.Gen
BitDefenderFalx	Android.Riskware.Metasploit.U	Cynet	Malicious (score: 99)
DrWeb	Android.RemoteCode.6833	ESET-NOD32	A Variant Of Android/TrojanDownloader.A...
Emsisoft	Android/Apexit.BKtr	Panda	Detected

From the virus total.com the apk contains android metasploit, Trojan we can see in above screenshot.

Step 3: Try to install apk in Android Virtual Device , but it cannot install which can see in the screen shots below.

Install apk from Terminal

```
((base) sarojgopali@Sarojs-MacBook-Pro-2 platform-tools % ./adb install /Users/sarojgopali/Downloads/Linux/ScientificCalculator.apk
Performing Streamed Install
adb: failed to install /Users/sarojgopali/Downloads/Linux/ScientificCalculator.apk: Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES: Failed collecting certificates for /data/app/vmdl1301709031.tmp/base.apk: Failed to collect certificates from /data/app/vmdl1301709031.tmp/base.apk: Attempt to get length of null array]
(base) sarojgopali@Sarojs-MacBook-Pro-2 platform-tools %
```



Step 4: Decompile apk using Apktool. "*apktool d ScientificCalculator.apk*"

```
(kali@kali)-[~/Desktop]
$ ls
Assignment2APK.zip  ScientificCalculator.apk  unpackApk

(kali@kali)-[~/Desktop]
$ apktool d ScientificCalculator.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on ScientificCalculator.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 ...

(kali@kali)-[~/Desktop]
$ cd ScientificCalculator

(kali@kali)-[~/Desktop/ScientificCalculator]
$ ls
AndroidManifest.xml  apktool.yml  assets  lib  original  res  smali  unknown
```

Step 5: Details of apk with signature.

buildConfirm cert

Samsung Cert SIGNER

Identity: Samsung Cert SIGNER

Verified by: Samsung Cert INTER

Expires: 05/11/2116

Details

Subject Name

C (Country): KR

ST (State): South Korea

L (Locality): Suwon City

O (Organization): Samsung Corporation

OU (Organizational Unit): Mobile

CN (Common Name): Samsung Cert SIGNER

Issuer Name

C (Country): KR

ST (State): South Korea

L (Locality): Suwon City

O (Organization): Samsung Corporation

OU (Organizational Unit): Mobile

CN (Common Name): Samsung Cert INTER

Issued Certificate

Version: 3

Serial Number: 01 54 A3 D8 04 BF

Not Valid Before: 2016-05-12

Not Valid After: 2116-05-11

Certificate Fingerprints

SHA1: AF 38 4E B7 D7 80 A2 EC 5E 7C 7E C6 41 40 07 1E 60 47 22 E2

MD5: 7A 4A AB 54 95 84 C5 7B D8 F3 AF 11 4C 4A 2E 9E

Public Key Info

Key Algorithm: RSA

Key Parameters: 05 00

Key Size: 4096

Key SHA1 Fingerprint: 3A 16 38 35 EB 3D 25 B3 40 E1 D0 D0 94 97 05 AF BA 23 E5 21

Public Key: 30 82 02 0A 02 82 02 01 00 D7 F5 0F C4 85 D0 62 85 6F 99 D1 B2 79 EB 21 EF 78 B4 C7 D3 BE C6 68 74 0D D9 3C 58 0F 91 3B 97 33 20 91 9C 6C DA E1 30 BE 2F 2E BE F7 49 34 48 98 18 D6 21 A7 D7 09 A5 F0 F1 50 B4 71 71 83 D8 9C EE CF FF D1 F6 87 20 48 B0 0C BB 02 43 ED C9 0F A4 74 FC 47 45 23 26 08 76 31 BF A4 6A E9 FA CF BD 9B 06 97 12 94 50 6A 1F F4 37 05 05 B3 4A D1 07 28 60 6C 20 56 02 DC 15 F0 8E 00 02 86 1F FF E5 03 21 9C 74 87 53 F7 B0 F4 C5 A9 03 CA 55 15 15 BE 2F C6 03 45 DA 93 FE FD F5 E6 02 00 B2 80 4C 55 93 C0 B3 80 4D 48 1B 8A 40 D9 85 4C 1F 0A 88 10 AE 74 C7 9A B1 09 EF 01 06 92 57 0F 69 F6 14 EA 3E 79 E3 2D 61 F4 AC A6 38 92 E9 87 78 BE FA A9 46 07 2C 16 FC 8F A6 05 60 DA 68 D0 7F 2E 5F 86 18 37 E0 EA A6 66 2A 66 E1 A0 46 02 C9 64 34 1B 8F 75 4A 4F 1E 6E F5 78 0F D0 A2 75 C2 43 65 52 BA 96 2A 1E 4A C8 34 1B EA E7 9D BE 36 90 0F 95 31 72 32 26 A8 80 32 04 79 E5 32 07 60 C7 E2 8E 7F DF 18 98 38 08 CE 55 15 29 AE 31 43 48 47 37 A7 A5 13 74 BA 17 8B B6 A3 15 C1 95 BA 35 D5 F5 D5 20 60 50 20 60 05 9E 90 08 04 BE 07 E9 20 74 73 AB 0E 65 49 1C FB 00 1E 50 CB A2 D3 01 06 90 10 13 CB 32 40 38 AF B1 08 28 3F 2E E3 84 64 55 2C 00 44 01 06 03 70 04 03 1F 95 54 CE 9C 88 45 43 70 80 C1 BC 33 02 46 DC EF 5C 96 27 13 1B 0F 6E E1 92 60 80 36 A1 54 F5 19 A4 F2 D7 05 00 B9 5F 49 2B 86 23 D5 BE BC CF 57 EE 2C DD 58 BA 69 A0 81 E5 AC 43 00 44 27 E2 0F F5 CB 82 99 D1 04 10 BA 12 64 74 AD A9 9C 4D E8 D0 EE 6A 69 CA CE 8D 34 EE D6 30 D8 E5 71 51 29 03 16 BF 90 53 0D 48 6C 17 0A 64 D0 B4 6C 00 56 A5 19 0F 0F 36 90 D9 2F 06 49 37 6C AF 78 C1 90 28 07 02 03 01 00 01

Extension

Identifier: 2.5.29.35

Value: 30 81 AA 00 14 6F 65 CD 85 37 6F D2 83 2F 68 03 08 ED E9 C2 4E 59 E5 1E A4 A1 81 89 A4 01 86 30 81 83 31 08 30 09 06 03 55 04 06 13 02 40 52 31 14 30 12 06 03 55 04 08 13 08 53 6F 75 74 08 20 4B 0F 72 65 61 31 13 30 11 06 03 55 04 07 13 BA 53 75 77 6F 6E 20 43 69 74 79 31 1C 30 1A 06 03 55 04 0A 13 13 53 61 60 73 75 6E 67 20 43 6F 72 70 6F 72 61 74 69 6F 6E 31 0F 30 0D 06 03 55 04 08 13 06 4D 6F 62 69 6C 65 31 1A 30 18 06 03 55 04 03 13 11 53 61 60 73 75 6E 67 20 43 65 72 74 20 52 4F 4F 54 82 06 01 54 A3 D8 BA C8

Critical: No

Subject Key Identifier

Key Identifier: BF 4C 47 2E A6 58 A4 51 F0 74 6C 98 E9 A8 1E ED 81 4E EB 45

Critical: No

Key Usage

Usages: Digital signature

Key encipherment

Critical: Yes

Signature

Signature Algorithm: 1.2.840.113549.1.1.1

Signature Parameters: 05 00

Signature: 84 EC E8 01 6F C0 7D 71 0C 73 E4 EC E9 83 60 93 C5 74 66 54 00 C1 3F AF D8 46 10 59 40 D7 08 22 48 C3 AB CC 50 F1 87 17 D8 F9 D8 38 2D 75 45 CF DC 6E F4 CE 62 13 C3 58 9F CB 08 5F AA 25 53 37 63 AA 58 77 87 D0 78 08 49 59 BA 12 0E CA 92 77 96 88 40 7E D8 05 18 D7 7D 59 87 83 7A 37 8A 70 5A 9C 8B DF AB FB 47 44 37 E1 5B 04 A1 53 BC 0D 5C 4C 2E D8 70 E9 AB D8 58 8F 9A 72 8C 72 BA CE 3A 03 66 9A 79 8B A8 59 C6 08 B4 A1 A8 6C 19 71 05 95 E2 22 FA B1 3B E9 EB BA 04 2F AD 3D 18 90 66 C3 DD E1 A0 2F 1E EC 78 38 08 78 2F 57 08 D0 D0 08 F3 08 A8 29 09 33 11 0F E8 23 2D 28 98 4A F3 79 E1 69 06 88 62 03 C2 02 55 01 B4 78 C1 4F 08 74 87 1D C4 EC 88 BA A0 AF 23 7F 39 59 37 0E F2 C7 F9 65 9F C3 3B CF 1E 3E 13 51 7E 4A FF 8D 04 28 5D 08 D2 7D A4 60 35 94 74 01 73 05 3D F7 01 EE F7 C4 C2 97 36 D2 8B D3 D7 40 9A 38 2F 0F 17 76 D3 86 A1 8E 1C C2 D2 E1 8F A9 AF 30 FA 63 08 31 6D 16 F7 90 0A 64 01 26 C2 D1 63 52 A3 46 70 A6 B1 D2 79 29 41 AD AB 3D E8 FE D0 D1 2B 3C 7C 60 58 FC EF EE 9E 46 A4 7A 7A 25 D8 1E 6A 5F 86 04 09 A9 EA 86 AE A6 72 25 BA 6F 90 D8 E1 4E 47 45 03 4F 8E 0F D7 77 3A EF E9 29 15 EA 80 AA B3 82 87 98 34 FD 04 02 FA BC 49 95 25 E8 62 28 18 E2 D8 9C EB 95 C8 D3 A6 9C 64 E4 E7 A5 51 79 F3 CB A2 D9 61 BC 92 F2 0F F1 07 4E CB 6F 87 9C CF 08 A4 96 E9 D3 5B 10 58 81 28 E7 FC F4 63 40 E4 64 5A 36 00 67 E9 11 79 9F 2E 90 F7 54 E0 3E 02 0C FF A9 A3 F0 22 6E 3A D8 0C 9E CC 2D 74 20 28 2A 05 31 52 02 14 81 93 8F 3E 3D 8B 7C 6E 17 F8 59 62 D9 C0 58 38 60 21 31 9C 06 04 64 39 23 28 5B EF 90 1F 9A 55 AC A6 A0 57 4A C3 08

Step 6: Install androguard "sudo apt-get install androguard" .

```
(root@kali)~/home/kali/androguard
# python3 cli.py apkid /home/kali/Desktop/ScientificCalculator.apk

{
  "/home/kali/Desktop/ScientificCalculator.apk": [
    "com.sec.android.app.popupcalculator",
    "1212003000",
    "12.1.20.3"
  ]
}

(root@kali)~/home/kali/androguard
# python3 cli.py sign /home/kali/Desktop/ScientificCalculator.apk

2022-11-14 19:38:14.103 | INFO | androguard.core.apk:_apk_analysis:313 - Starting analysis on AndroidManifest.xml
2022-11-14 19:38:14.147 | INFO | androguard.core.apk:_apk_analysis:370 - APK file was successfully validated!
2022-11-14 19:38:14.149 | WARNING | androguard.core.api_specific_resources:load_permissions:52 - Requested API level 31 is
larger than maximum we have, returning API level 29 instead.
2022-11-14 19:38:14.152 | WARNING | androguard.core.api_specific_resources:load_permissions:52 - Requested API level 30 is
larger than maximum we have, returning API level 29 instead.
ScientificCalculator.apk, package: 'com.sec.android.app.popupcalculator'
Is signed v1: False
Is signed v2: False
Is signed v3: False
```

Get apkid and sign using androguard.

Step 7: Analyze apk using androguard.

"python cli.py analyze /home/kali/Desktop/ScientificCalculator.apk"

```
File Actions Edit View Help
# python3 cli.py analyze /home/kali/Desktop/ScientificCalculator.apk

/home/kali/Desktop/ScientificCalculator
2022-11-14 19:52:28.777 | INFO | androguard.session:__init__:58 - Opening database <Database(sqlite:///androguard.db)>
2022-11-14 19:52:28.788 | INFO | androguard.session:__init__:67 - Creating new session [3]
2022-11-14 19:52:28.788 | INFO | main:androlyze_main:257 - Please be patient, this might take a while.
2022-11-14 19:52:28.789 | INFO | main:androlyze_main:261 - Found the provided file is of type 'APK'
2022-11-14 19:52:28.800 | INFO | androguard.session:addAPK:140 - add APK /home/kali/Desktop/ScientificCalculator.apk:0f0
cd4cc8c5e7d0e67deb5fe4aa2279ba38b32d07e47bbdcc22265c66c7543ca
2022-11-14 19:52:28.821 | INFO | androguard.core.apk:_apk_analysis:313 - Starting analysis on AndroidManifest.xml
2022-11-14 19:52:28.867 | INFO | androguard.core.apk:_apk_analysis:370 - APK file was successfully validated!
2022-11-14 19:52:28.868 | WARNING | androguard.core.api_specific_resources:load_permissions:52 - Requested API level 31 is
larger than maximum we have, returning API level 29 instead.
2022-11-14 19:52:28.870 | WARNING | androguard.core.api_specific_resources:load_permissions:52 - Requested API level 30 is
larger than maximum we have, returning API level 29 instead.
2022-11-14 19:52:28.879 | INFO | androguard.session:addDEX:174 - add DEX:6729491e54bb2056e4f64cabf153db370b383781802ba8c
6bc5d3b99321713fa
2022-11-14 19:52:29.739 | INFO | androguard.session:addDEX:180 - added DEX:6729491e54bb2056e4f64cabf153db370b383781802ba
8c6bc5d3b99321713fa
2022-11-14 19:52:29.739 | INFO | androguard.core.analysis.analysis:add:1435 - Adding DEX file version 39
2022-11-14 19:52:33.186 | INFO | androguard.core.analysis.analysis:add:1458 - Added DEX in the analysis took : 0min 03s
2022-11-14 19:52:34.208 | INFO | androguard.core.analysis.analysis:create_xref:1492 - End of creating cross references (
XREF) run time: 0min 00s
2022-11-14 19:52:34.209 | INFO | androguard.session:addAPK:160 - added APK /home/kali/Desktop/ScientificCalculator.apk:0
f0cd4cc8c5e7d0e67deb5fe4aa2279ba38b32d07e47bbdcc22265c66c7543ca
2022-11-14 19:52:34.209 | INFO | main:androlyze_main:275 - Added file to session: SHA256::0f0cd4cc8c5e7d0e67deb5fe4aa227
9ba38b32d07e47bbdcc22265c66c7543ca
2022-11-14 19:52:34.209 | INFO | main:androlyze_main:278 - Loaded APK file ...
>>> filename
/home/kali/Desktop/ScientificCalculator.apk
>>> a
<androguard.core.apk.APK object at 0x7f0b8b15e350>
>>> d
[<androguard.core.dex.DEX object at 0x7f0b8b1cd210>]
>>> dx
<analysis.Analysis VMs: 1, Classes: 1629, Methods: 12571, Strings: 2564>
Androguard version 4.0 started
```

Step 8: Get Permissions from apk.

```
Androguard version 4.0 started
In [1]: a.get_permissions()
Out[1]:
['android.permission.VIBRATE',
'android.permission.INTERNET',
'android.permission.WRITE_CONTACTS',
'android.permission.WRITE_SETTINGS',
'android.permission.ACCESS_NETWORK_STATE',
'android.permission.CAMERA',
'android.permission.READ_CALL_LOG',
'android.permission.READ_SMS',
'android.permission.ACCESS_FINE_LOCATION',
'android.permission.GET_TASKS',
'android.permission.RECEIVE_BOOT_COMPLETED',
'android.permission.RECORD_AUDIO',
'android.permission.READ_CONTACTS',
'android.permission.SEND_SMS',
'android.permission.WAKE_LOCK',
'android.permission.RECEIVE_SMS',
'com.samsung.keyguard.SHORTCUT_PERMISSION',
'com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY',
'android.permission.WRITE_EXTERNAL_STORAGE',
'android.permission.CALL_PHONE',
'com.sec.spp.permission.TOKEN_b8a82002e8796582a00da99945c0030cbf5b2363606544cbe5839d0ed225f6ab631336df38d03c8f062aef9f4f0b12c876a16353cf9bd4793def6834d2addffa5f34e4b04344a60fa268dd722f793777fab4263f8be781f45a49e1c9362261e00cbd5b159b77455826c585f7f04e66134faca83b6f9e98441dcb54022e7d3e',
'android.permission.WRITE_CALL_LOG',
'android.permission.ACCESS_COARSE_LOCATION',
'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS',
'android.permission.SET_WALLPAPER',
'android.permission.READ_PHONE_STATE',
'com.sec.android.app.parser.permission.SecretCodeIME']
```

Step 9: Get activities from apk.

```
In [2]: a.get_activities()
Out[2]:
['com.sec.android.app.popupcalculator.Calculator',
'com.sec.android.app.popupcalculator.converter.controller.NewUnitConverterActivity',
'com.sec.android.app.popupcalculator.converter.mortgage.controller.MortgageResultActivity',
'com.sec.android.app.popupcalculator.converter.mortgage.controller.BaseMortgageActivity',
'com.sec.android.app.popupcalculator.converter.mortgage.controller.MortgageDetailActivity']
```

Step 10: Create jar from classes.dex. "d2j-dex2jar classes.dex"

```
(root@kali)-[/home/kali/Desktop/unpackApk]
# ls
AndroidManifest.xml  assets  Assignment2APK  classes.dex  lib  res  resources.arsc  SEC-INF

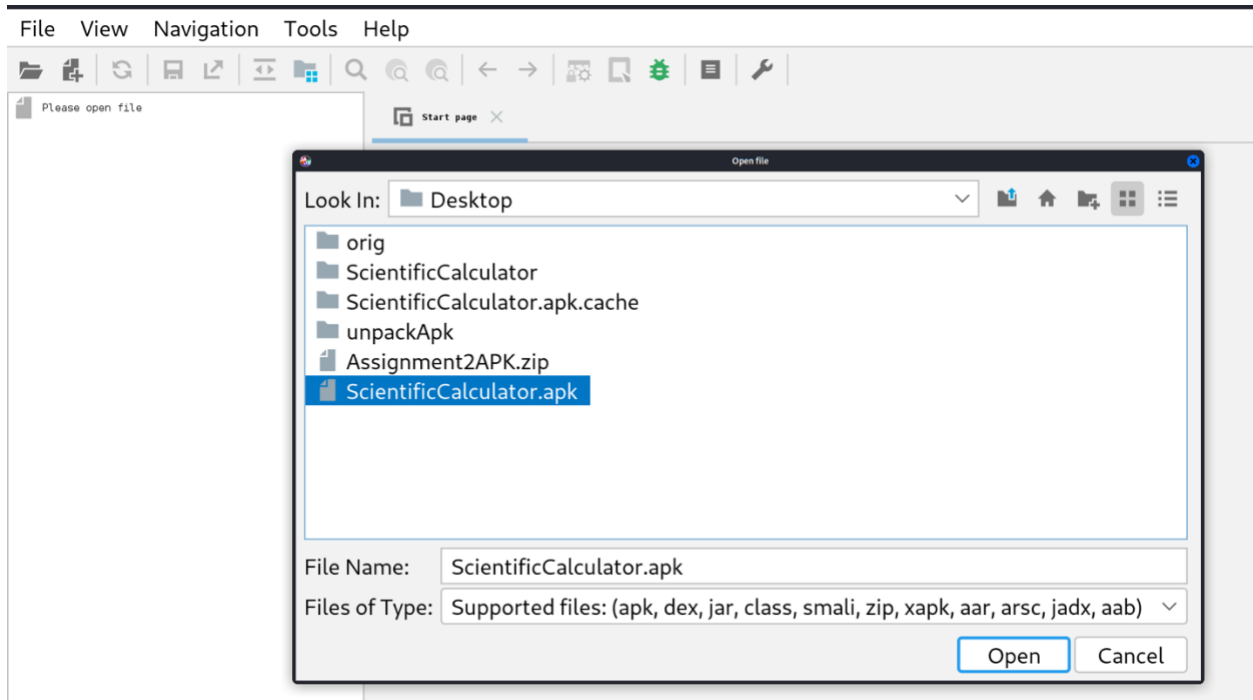
(root@kali)-[/home/kali/Desktop/unpackApk]
# d2j-dex2jar classes.dex

dex2jar classes.dex → ./classes-dex2jar.jar
Detail Error Information in File ./classes-error.zip
Please report this file to one of following link if possible (any one).
https://sourceforge.net/p/dex2jar/tickets/
https://bitbucket.org/pxb1988/dex2jar/issues
https://github.com/pxb1988/dex2jar/issues
dex2jar@googlegroups.com

(root@kali)-[/home/kali/Desktop/unpackApk]
# ls
AndroidManifest.xml  Assignment2APK  classes-dex2jar.jar  lib  resources.arsc
assets             classes.dex      classes-error.zip    res  SEC-INF
```


[illegible]

Step 12: Check secret code from Jadx- GUI.



The secret code we found is "SecretCodeIME" as highlighted in the screen shot below.

