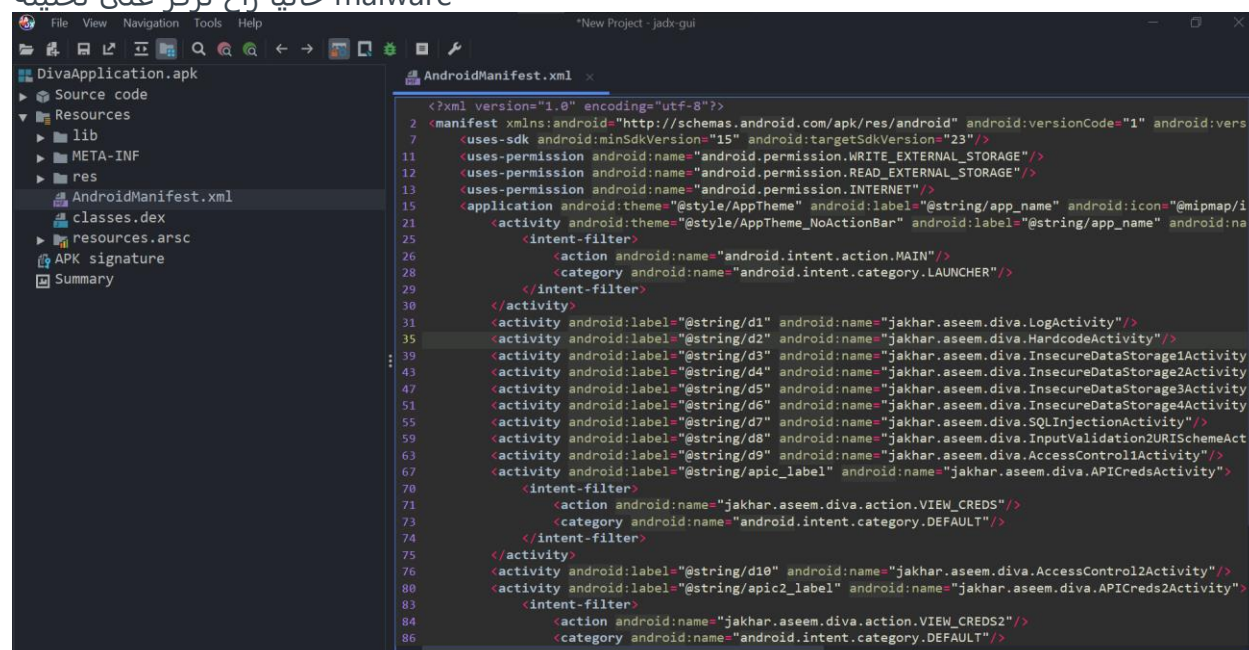


analysis android manifest file

بسم الله الرحمن الرحيم

What is Androidmanifest.xml file

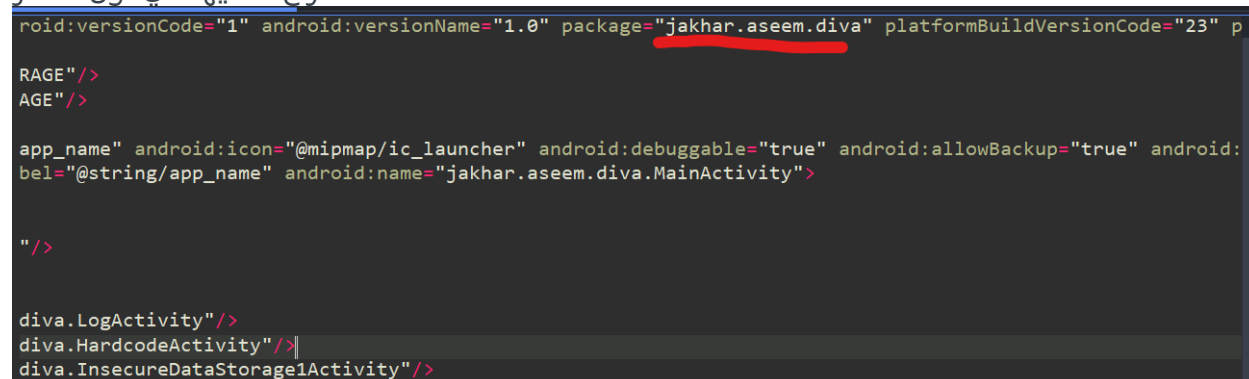
الملف هذا يحتوي على معلومات عن ال apk و يفيدك كثير سواء في penstest او ك analysis malware حاليا راج نركز على تحليله



نرمي ال apk في jadx و ندخل على ال Resources و نفتح AndroidManifest.xml

في البداية كيف نعرف ال package name؟

راج تلاحظها في اول سطر



```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="1" android:versionName="1.0"
    package="jakhar.aseem.diva" platformBuildVersionCode="23"
    platformBuildVersionName="6.0-2166767">
```

اسم ال package مفيد في ال IOC او بعدين اذا بتسوي Dynamic analysis في طرق كثير تعرف ال package name بس هذي اسهلها بالنسبة لي

```
<activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity"
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>
```

الجزئية هذي هي ال main function

```
android:icon="@mipmap/ic_launcher" android:debuggable="true" android:label="@string/app_name"
    android:name="jakhar.aseem.diva.MainActivity">
```

و منها نعرف وين اول فنكشن تشغل ال Main كل اللي عليك تسويه تتبع المسار في jadx و بتحصل ال Main

What is activity

شرح Chatgpt:

An activity is a single, focused thing that the user can do in your application. An activity typically has a user interface (UI), which can consist of a layout file that defines the layout and appearance of the activity's UI elements. Examples of activities in an Android application might include a login screen, a settings screen, or a screen that displays a list of items.

في الويب عندنا صفحات وي index login و غيرها ال activity نفس الفكرة هي الصفحات في التطبيق نفسة و اقصد ال UI

```
<activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity" />
<activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity" />
<activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity" />
<activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity" />
<activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity" />
<activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity" />
<activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity" />
<activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity" />
<activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity" />
<activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity" />
```

و جنب كل activity بتلاقي الفنكشن المسؤولة عنها زي مثلا عندنا في HardcodeActivity مسؤولة عنه هذي الفنكشن

jakhar.aseem.diva.HardcodeActivity

```
/* loaded from: classes.dex */
public class HardcodeActivity extends AppCompatActivity {}
/* JADX INFO: Access modifiers changed from: protected */
@Override // android.support.p003v7.app.AppCompatActivity, android.support.p000v4.app.FragmentA
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(C0319R.layout.activity_hardcode);
}

public void access(View view) {
    EditText hkey = (EditText) findViewById(C0319R.C0321id.hcKey);
    if (hkey.getText().toString().equals("vendorsecretkey")) {
        Toast.makeText(this, "Access granted! See you on the other side :", 0).show();
    } else {
        Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
    }
}
}
```

و اذا دخلت عليها راح تلاقي ال decompiled code و تقدر تحللة راح تستفيد من الشي هذا اذا تبي تفحص صفحة معية مثل login في البرنامج

uses-permission

و هي الصلاحيات اللي يطلبها التطبيق منك لما تشغلة

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INTERNET"/>
```

هذي بعض ال permissions اللي ممكن يتم استخدامها بشكل ضار

```
READ_SMS
SEND_SMS
RECORD_AUDIO
CAMERA
ACCESS_FINE_LOCATION
ACCESS_COARSE_LOCATION
INSTALL_SHORTCUT
READ_CONTACTS
WRITE_CONTACTS
READ_CALL_LOG
RECEIVE_BOOT_COMPLETED
```

مو شرط وجود وحدة من ذول يعني ال البرنامجو malware لأن ممكن البرنامج نفسة يحتاج الصلاحيات هذي عشان يشتغل مثال:

برنامج SMS filter راح يحتاج صلاحيات READ_SMS وعشان يقدر يفلتر و تطبيق تصوير بيحتاج RECORD_AUDIO و CAMERA
و اذا مالقيت شي ضار هذا مايعني ان البرنامج مو ضار ممكن يطلب ال permissions بشكل dynamic و بالطريقة هذي ما يطلع لك في ال manifest file و هذي الحركة تستعمل في تخطي ال AVs

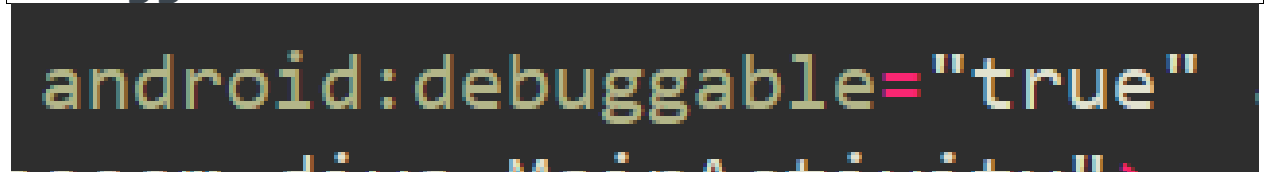
SERVICES

و هي الفنكشنز او الاكواد اللي تشتغل داخل التطبيق و خارجة

```
<service
    android:name=".MyService"
    android:enabled="true"
    android:exported="false">
    <intent-filter>
        <action android:name="com.example.myservice.Location.action.START"
    />
    </intent-filter>
</service>
```

مثلا هذي ال service راح تراقب اللوكيشن حتى لو كنت خارج التطبيق زي برامج google maps او uber يستعملون ال service هذي بحيث يتبعون الموقع حقا حتى خارج التطبيق

debuggable



هذا يعني ان البرنامج تقدر تسوي عليه debug ف وقتها تقدر تسوي Dynamic analysis و حتى لو كان false تقدر تحولها ل true و تسوي debug عالبرنامج ب jdb مثلا

icon & applicaiton name

```
<application android:theme="@style/AppTheme"
    android:label="@string/app_name" android:icon="@mipmap/ic_launcher"
```

```
android:debuggable="true" android:allowBackup="true"  
android:supportsRtl="true">
```

تقدر تلاقي اسم و icon البرنامج من هنا طبعا بتلاحظ انها تبدأ ب @ بس لو تروح ل resources راح تلاقيهم

Androidsdk

```
<uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23"/>
```

هنا بتحصل اقل sdk يشتغل التطبيق عليه و ال target sdK ممكن ما تفيدك كثير بس لازم ترفقها اذا راح تسوي report