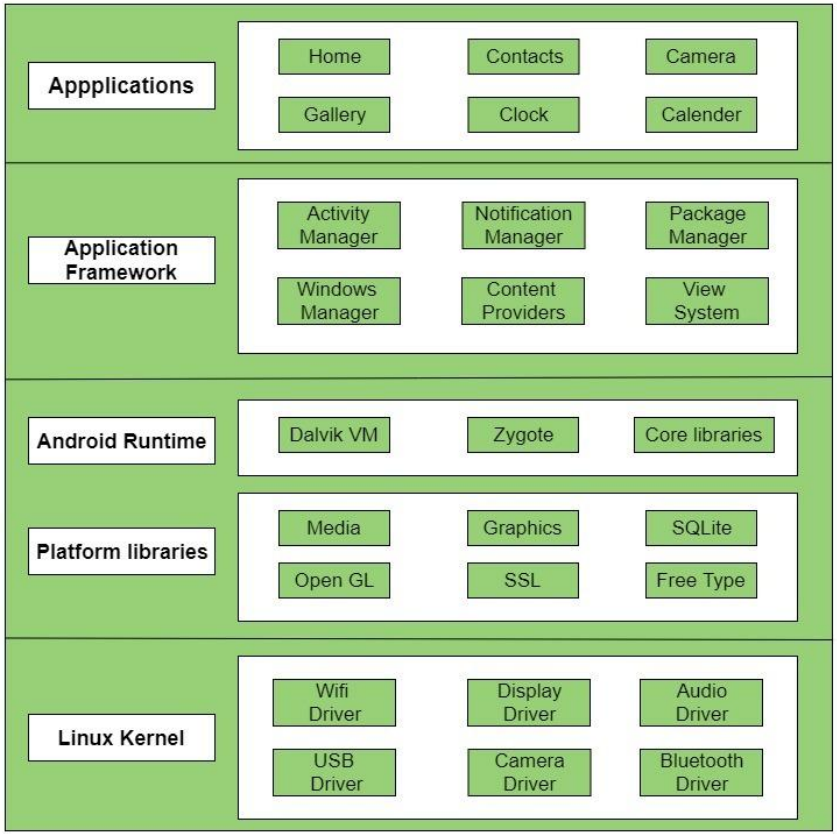
Android App Reverse Engineering

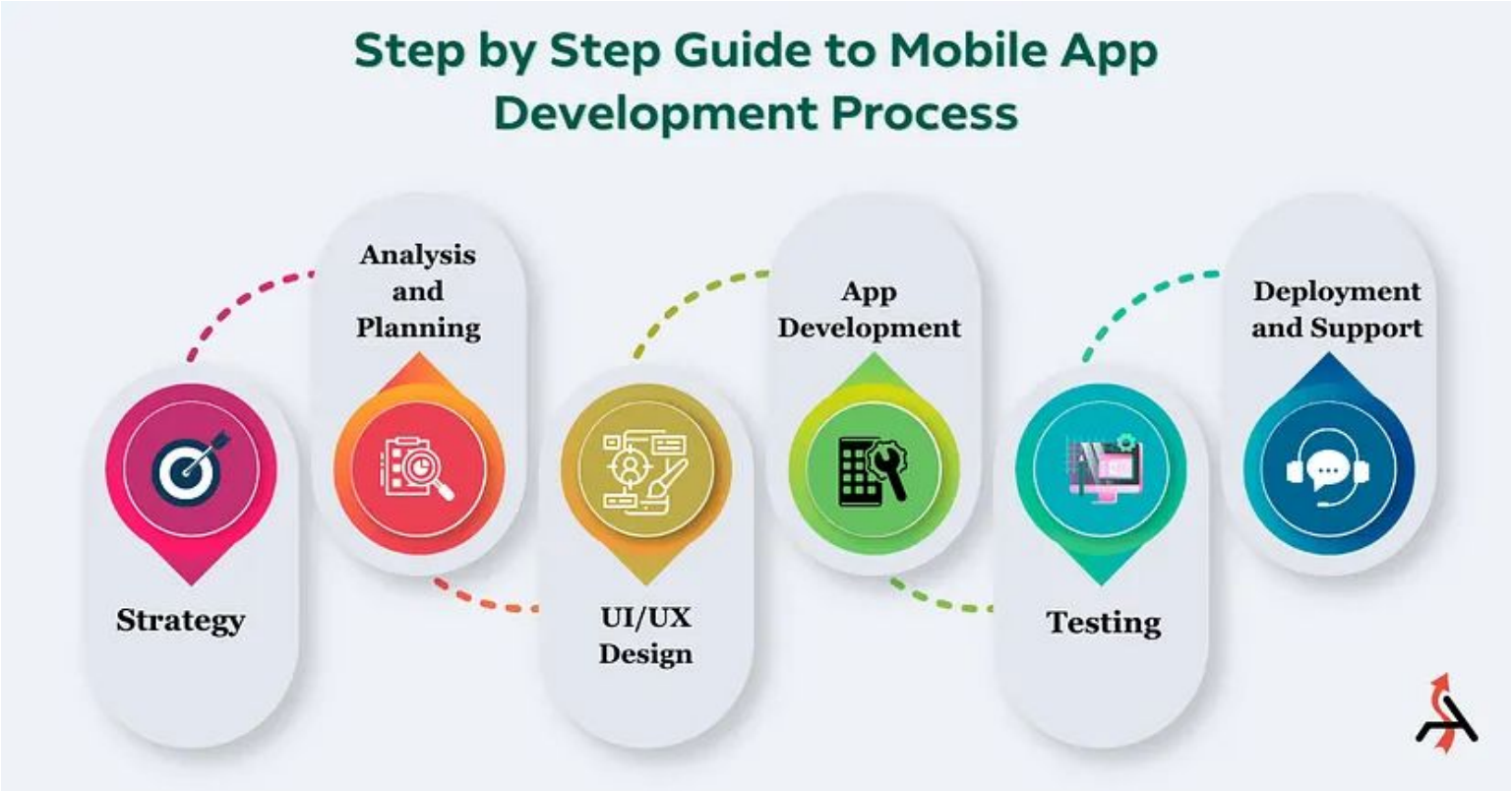
Overview

- **Android Architecture**
  - Kernel
  - APIs
  - Partitions
- **Android App Development Process**
  - Overview of software development and release stages
  - IDEs for Android software development
- **Android Build System**
  - Different parts of an Android app in Android Programming
  - Overview of DVM and Smali
- **Static Analysis**
  - APK Architecture
  - APK Manifests and Resources Analysis
  - DEX Decompilation
- **Automatic Code Analysis**
  - MobSF
  - Ostorlab
  - Nowsecure
- **Obfuscation and Deobfuscation**
  - Intro to Obfuscation
  - Deobfuscation Tools
- **Dynamic Analysis**
  - Setting up Lab Environment
  - Genymotion

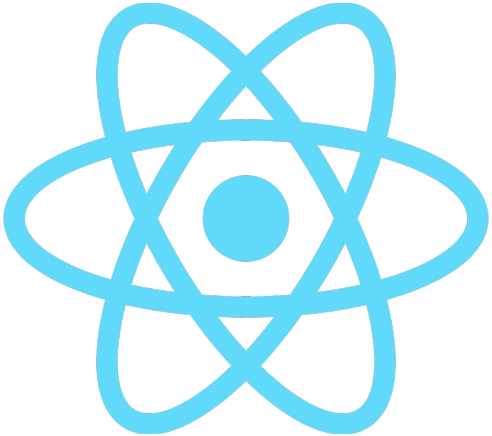
Android Architecture



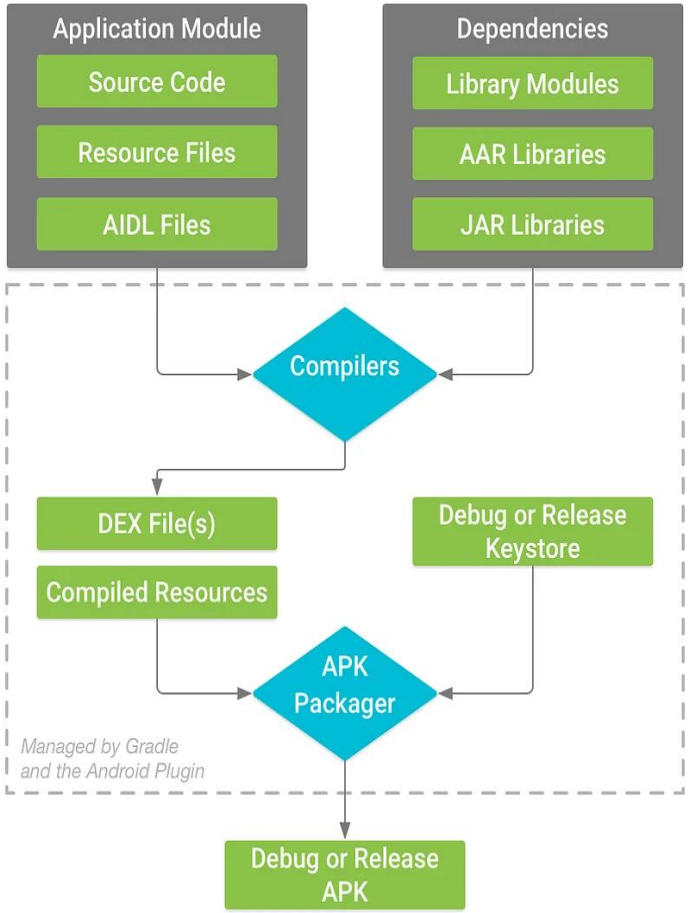
Android App Development Process



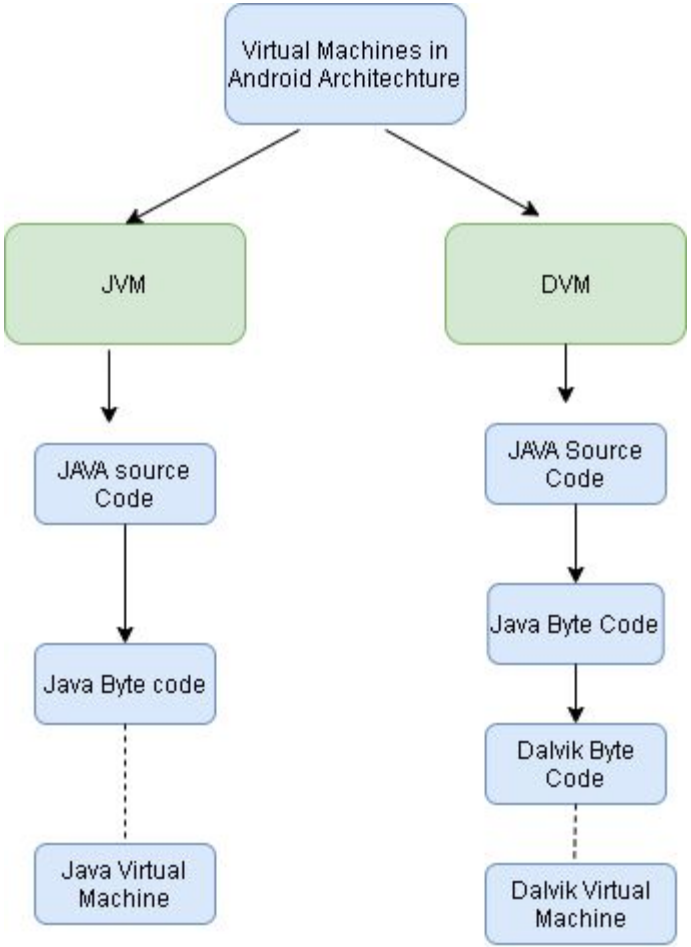
Android App Development IDES



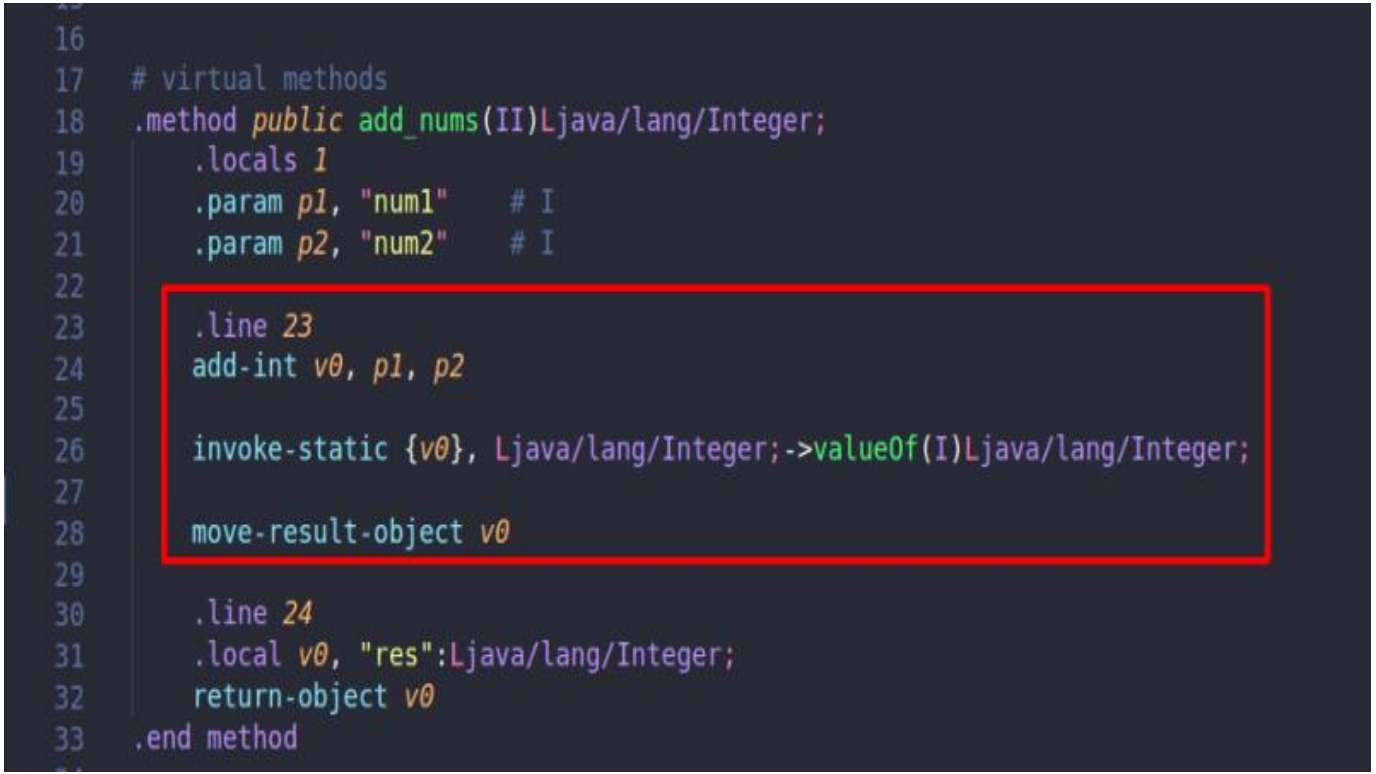
Android Build System



Android Virtual Machine

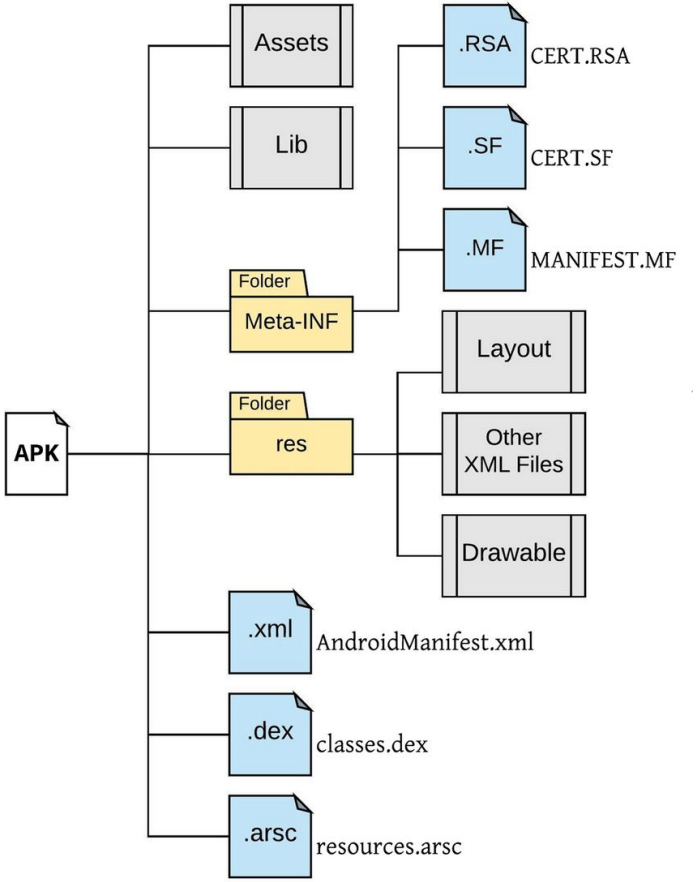


Overview Smali



```
16
17  # virtual methods
18  .method public add_nums(II)Ljava/lang/Integer;
19      .locals 1
20      .param p1, "num1"    # I
21      .param p2, "num2"    # I
22
23      .line 23
24      add-int v0, p1, p2
25
26      invoke-static {v0}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
27
28      move-result-object v0
29
30      .line 24
31      .local v0, "res":Ljava/lang/Integer;
32      return-object v0
33  .end method
```

Static Analysis



Now Open Apk file with Winrar

Static Analysis

ApkTool

Jadx

ApkStudio

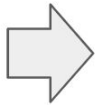
Automatic Code Analysis

Nowsecure

Obfuscation and Deobfuscation

Unprotected

```
class X {
  static String a = "foo";
  static String b = "bar";
  ...
```



Protected

```
class X {
  static {
    Y.restore();
  }
  static String a;
  static String b;
  ...
```

```
class Y {
  static void restore() {
    // perform the following actions
    // in the most complicated way
    //   X.a = "foo";
    //   X.b = "bar";
    ...
  }
  ...
```

Obfuscation and Deobfuscation

Dynamic Analysis

Now Working in the Real World