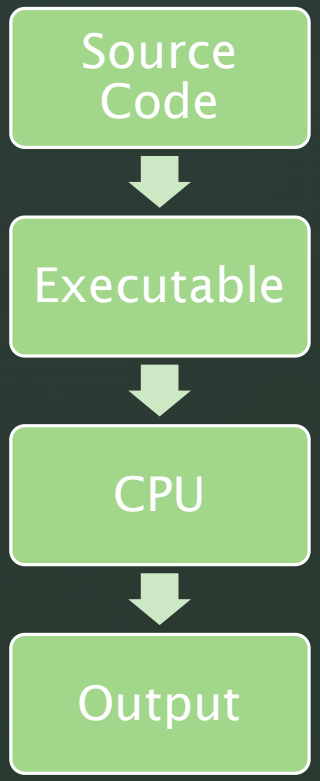
Introduction to Reverse Engineering

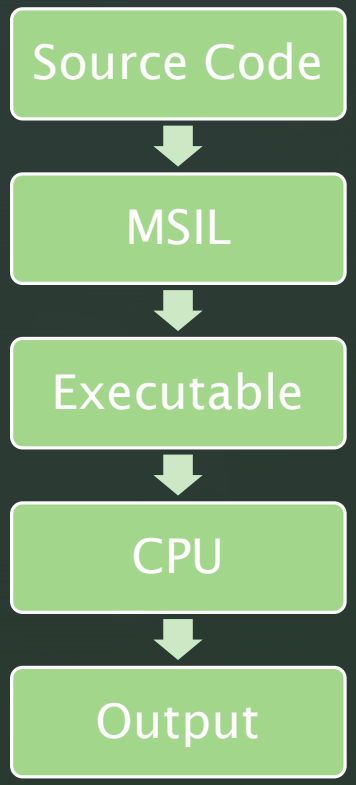
Unmanaged Code



Unmanaged code compiles straight to machine code. For example, traditional C/C++ compilers output 'unmanaged code'. Also, since it compiles to machine code and not an intermediate language it is non-portable (i.e. it is machine dependent).

The code runs directly on the operating system which means it has no runtime services such as garbage collection

Managed Code



Visual Basic .NET and C# compilers create managed code. It runs on the CLR (Common Language Runtime), which offers services like garbage collection, runtime type checking, exception handling and reference checking.

The source code is compiled in an intermediate language known as MSIL. It helps prevent memory buffer overflows. But it does not provide low-level access to the programmer.

References:
Managed v/s Unmanaged code in .NET | GeeksforGeeks
Full Managed code and Unmanaged code in .NET | GeeksforGeeks

.NET Decompilation

.NET is a family of programming languages comprising of:

- C#
- F#
- Visual Basic

Tools to decompile .NET applications:

- dotPeek : https://www.jetbrains.com/decompiler/
- ILSpy : https://github.com/icsharpcode/ILSpy
- dnSpy : https://github.com/dnSpy/dnSpy

Exeinfo PE

- A tool that shows you information such as the entry point, file offset, linker information, file size, EP section, first bytes, sub-system and overlay of an executable file including compiler type and underlying obfuscations.

- Download link : http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/ExEinfo-PE.shtml

Python

Python Source file: .py

Python byte code : .pyc

Uncompyle 6:

```
pip install uncompyle6
```

Java Decompilation

Types of Java bytecode:

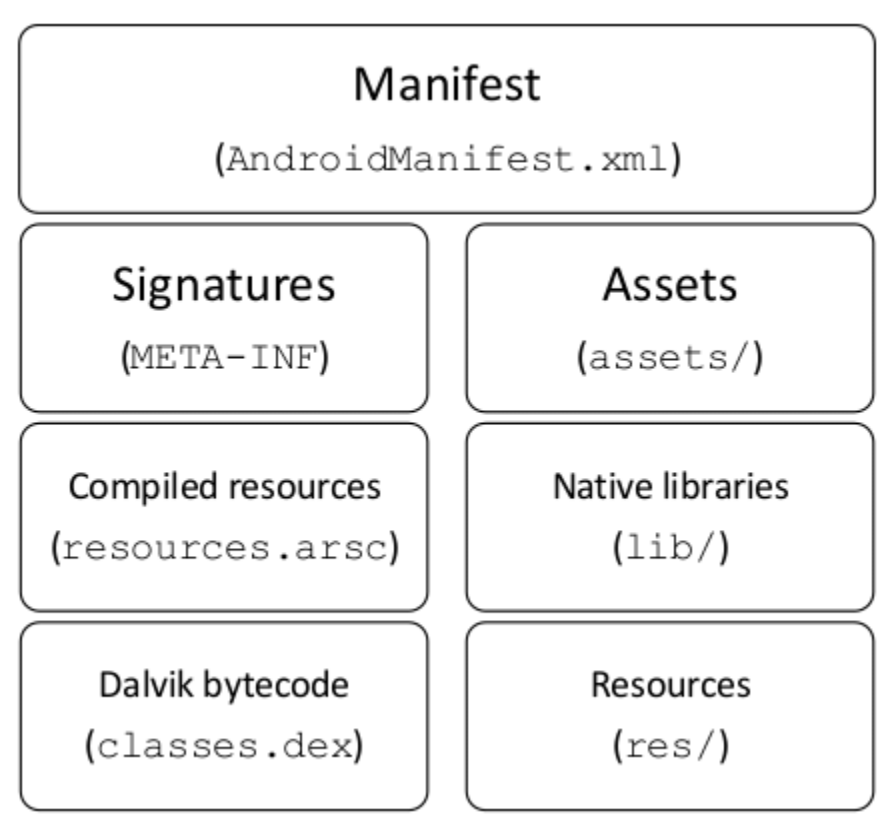
- .class
- .dex

Tools to decompile Java bytecode:

- JD-GUI : https://java-decompiler.github.io/
- Jadx-GUI : https://github.com/skylot/jadx

APK Decompilation

APK file composed of:



Reference: Inspecting APK Files | PSPDFKit

APK Decompilation

- Apk file can be easily unpacked by either unzipping or using tools like apktool etc.
- After receiving .dex and other resources, we can use tools like dex2jar to convert Dalvik bytecode to jar file and then convert jar to java file for complete de-compilation.
- Another way can be by simply using tool like JADX or Android Studio's Apk Analyzer to analyze contents of apk file.

Apktool: https://ibotpeaches.github.io/Apktool/

Dex2jar: https://github.com/pxb1988/dex2jar.git/

JADX: https://github.com/skylot/jadx

ELF and PE reversing

Part 2 coming soon...