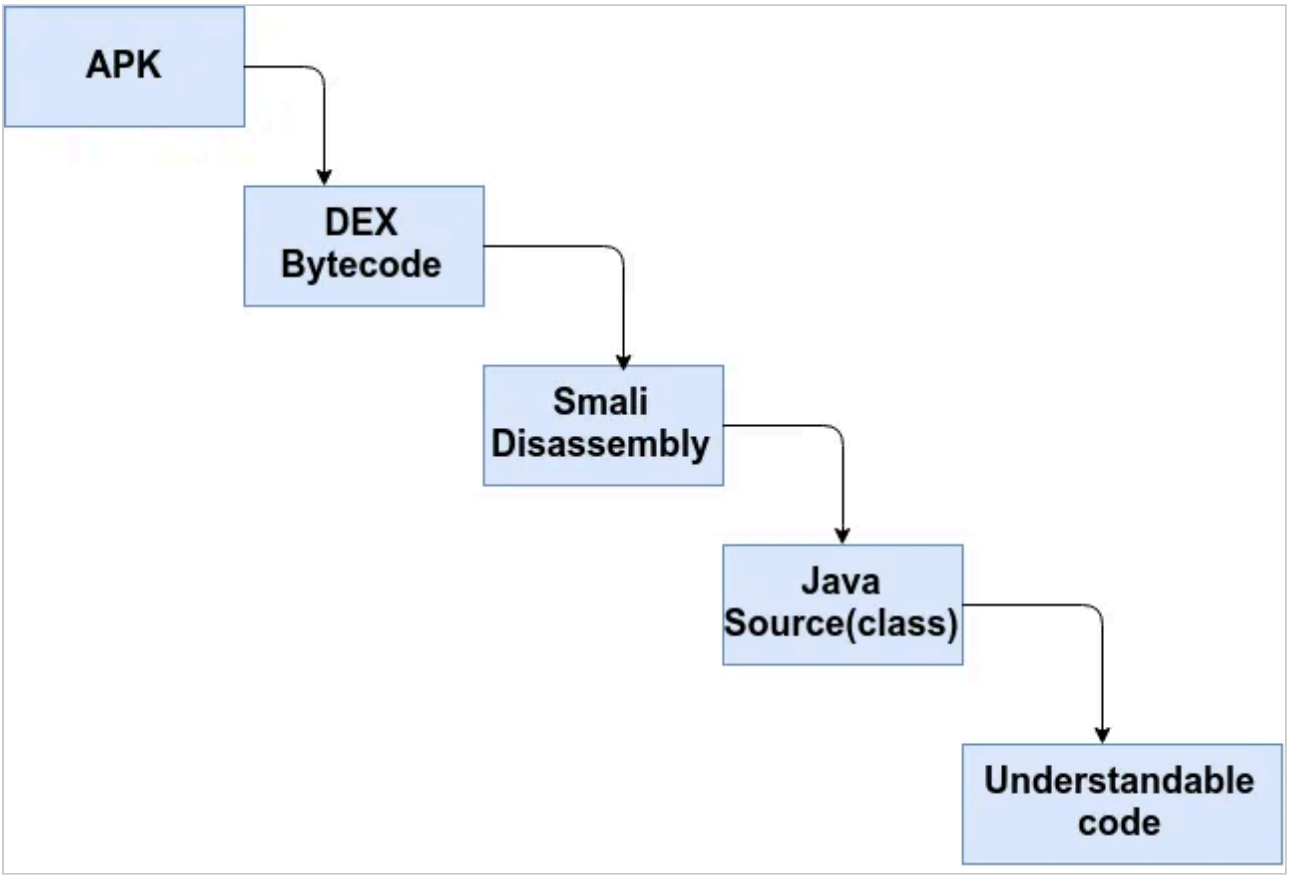
FIELD NOTE / REVERSE ENGINEERING

Decompile Android APK/DEX Lebih Mudah Dengan JADX

Petruknisme · 7 Mar, 2018 · 2 min to read

Bagi rekan-rekan yang berkecimpung dalam dunia Reverse Engineering mungkin sudah tidak asing dengan istilah decompiler ataupun proses decompile. Secara simpelnya, proses decompile adalah sebuah proses yang melakukan pembongkaran terhadap suatu aplikasi untuk mendapatkan source code agar bisa dibaca/dipahami, sedangkan untuk decompiler sendiri merupakan sebuah alat yang dipakai dalam proses decompile.

Dalam proses pembongkaran android package, diperlukan beberapa proses seperti berikut:



Pada diagram tersebut, diperlukan beberapa proses dalam reverse engineering sebuah apk. Dimulai dengan membongkar APK itu sendiri karena APK bersifat archive yang bisa kita extract dengan tool archive extractor semacam rar dan lain sebagainya. Lalu berkas dex tersebut disassembly dan didecompile menjadi java source yang masih merupakan class file. Source code tersebut bisa dibaca menggunakan java decompiler seperti JD-GUI.

Oh iya, saya pernah bahas soal Java Bytecodes Decompiler dengan Procyon pada tulisan ini https://petruknisme.com/2017/04/08/procyon-powerful-java-bytecode-decompiler/

Licensed under CC BY-SA 4.0

(https://petruknisme.com/2017/04/08/procyon-powerful-java-bytecode-decompiler/)

Oke, sesuai dengan judul pada tulisan kali ini, saya akan membahas JADX. Sebuah tool yang saya pikir membuat proses reverse engineering sebuah apk menjadi lebih mudah karena beberapa step yang saya jelaskan diatas sudah otomatis dilakukan oleh JADX. Jadi kita hanya perlu memberikan sebuah berkas apk yang akan didecompile saja.

Instalasi JADX

JADX sendiri masih bertahan pada versi v0.6.1 untuk stable, dan untuk unstable build atau bleeding edge langsung melalui github sudah mencapai versi v0.7.0-xxx. Unduh JADX pada laman https://github.com/skylot/jadx/releases (https://github.com/skylot/jadx/releases)

Setelahnya lakukan unzip terhadap berkas tersebut

```
↳ unzip jadx-0.6.1.zip
Archive:  jadx-0.6.1.zip
  inflating: README.md
  inflating: LICENSE
  inflating: NOTICE
   creating: lib/
  inflating: lib/objenesis-2.1.jar
  inflating: lib/cloning-1.9.2.jar
  inflating: lib/slf4j-api-1.7.10.jar
  inflating: lib/annotations-12.0.jar
  inflating: lib/image-viewer-1.2.3.jar
  inflating: lib/android-5.1.jar
  inflating: lib/jcommander-1.47.jar
  inflating: lib/logback-classic-1.1.2.jar
  inflating: lib/jadx-cli-0.6.1.jar
  inflating: lib/commons-io-2.4.jar
  inflating: lib/jfontchooser-1.0.5.jar
  inflating: lib/asm-5.0.3.jar
  inflating: lib/jadx-core-0.6.1.jar
  inflating: lib/rsyntaxtextarea-2.5.8.jar
  inflating: lib/gson-2.3.1.jar
  inflating: lib/logback-core-1.1.2.jar
  inflating: lib/jadx-gui-0.6.1.jar
  inflating: lib/dx-1.10.jar
   creating: bin/
  inflating: bin/jadx
```

Licensed under CC BY-SA 4.0

```
27     inflating: bin/jadx-gui.bat
28     inflating: bin/jadx-gui
29     inflating: bin/jadx.bat
```

Bagi pengguna Archlinux/Blackarch, cukup menggunakan command berikut untuk instalasi jadx:

```
1  pacman -S jadx
```

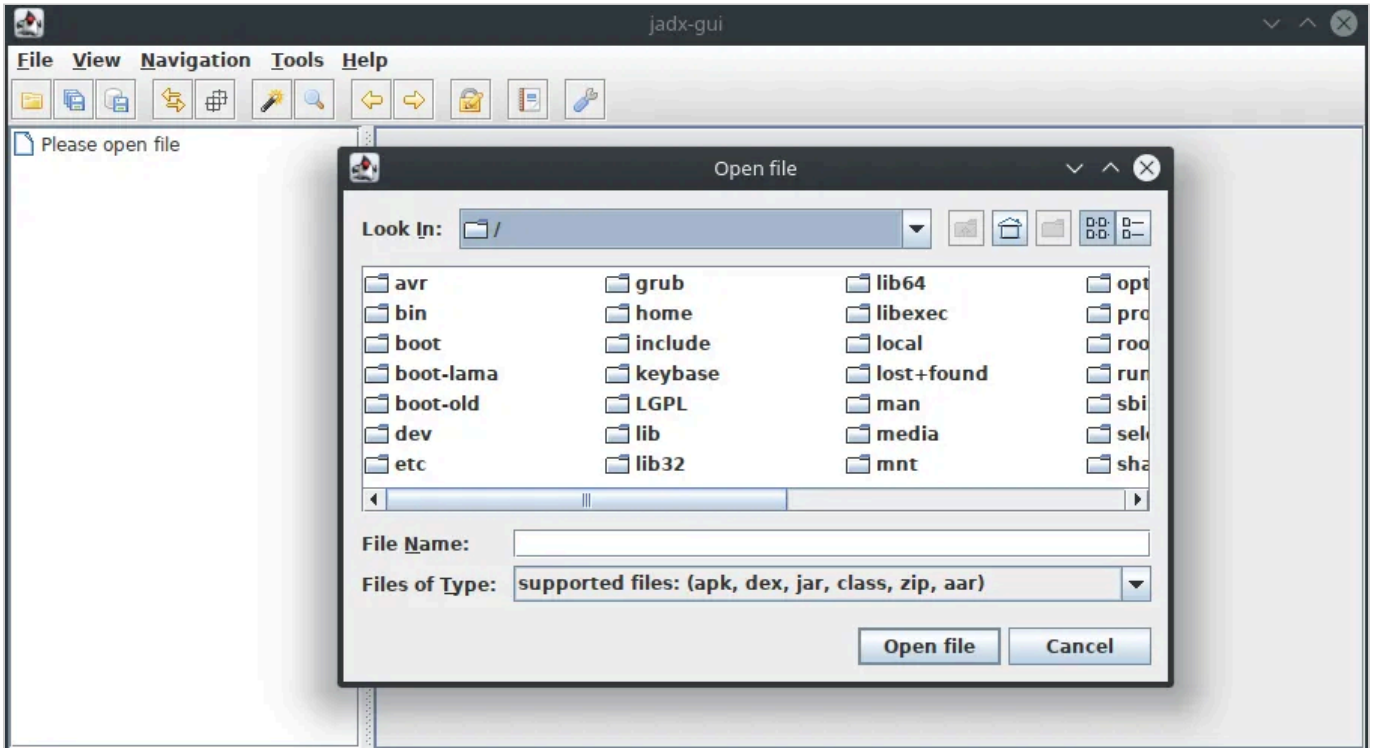
Perlu diingat bahwa JADX ini cross-platform, jadi bisa jalan pada sistem operasi windows, linux dan *NIX selama java sudah terpasang.

Menjalankan JADX

Untuk menjalankan jadx, cukup dengan menjalankan jadx-gui ataupun jadx yang ada didalam direktori bin. Bagi pengguna Archlinux, cukup dengan:

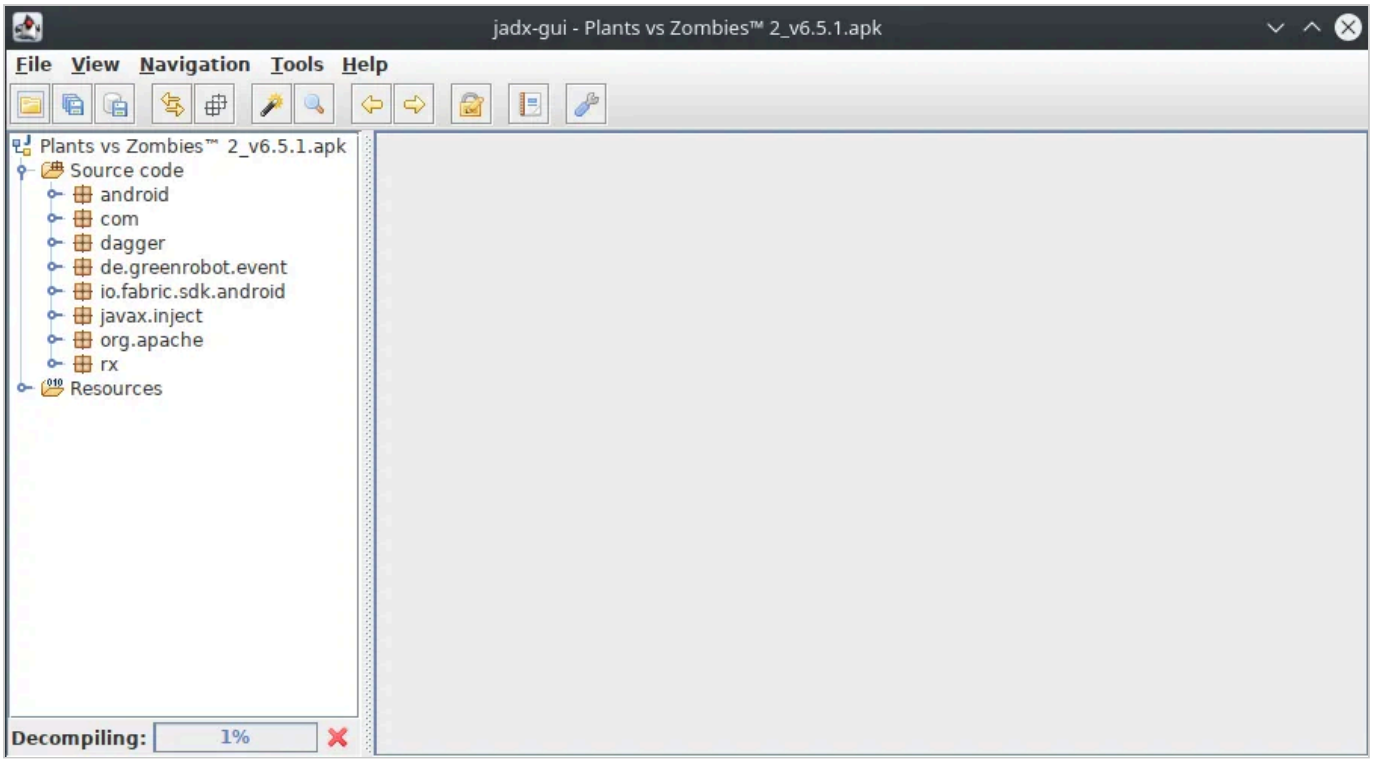
```
1  jadx-gui
```

Maka akan muncul dialog untuk open file seperti pada gambar berikut:

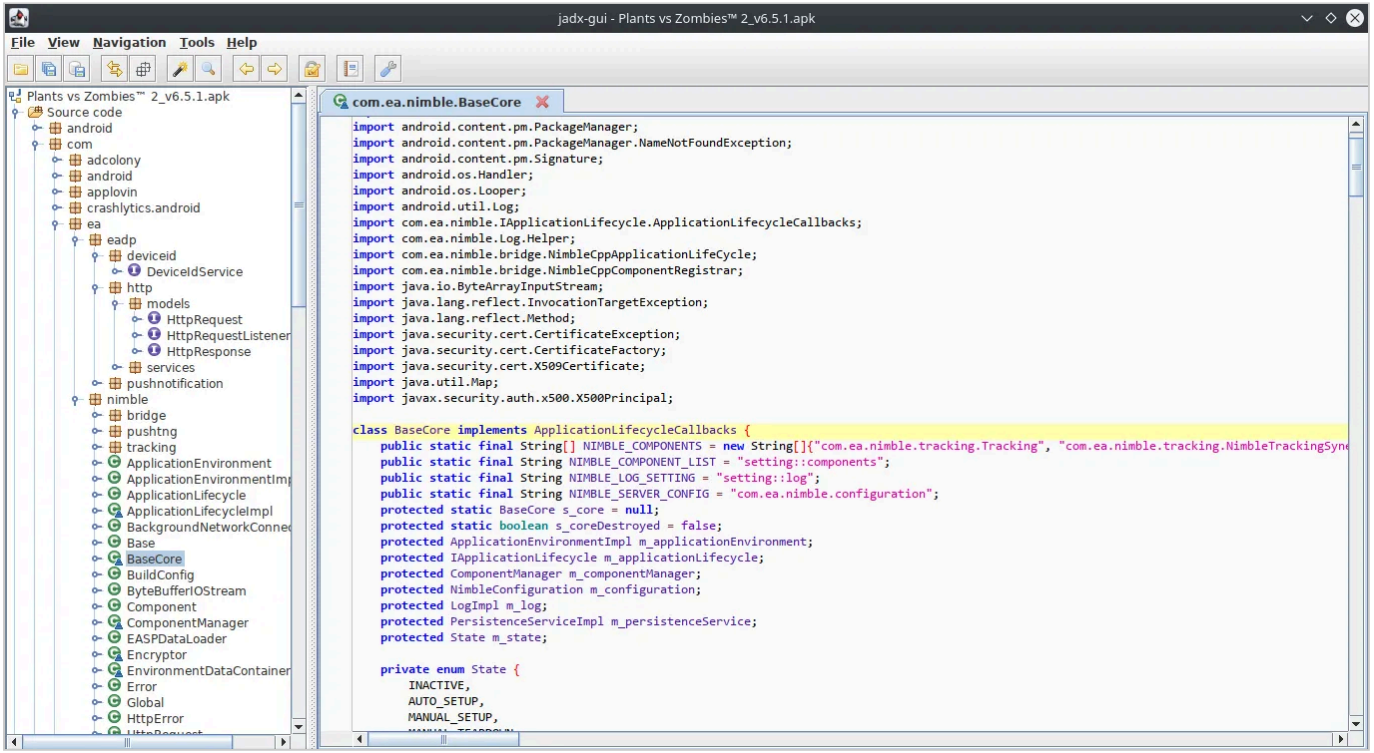


Licensed under CC BY-SA 4.0

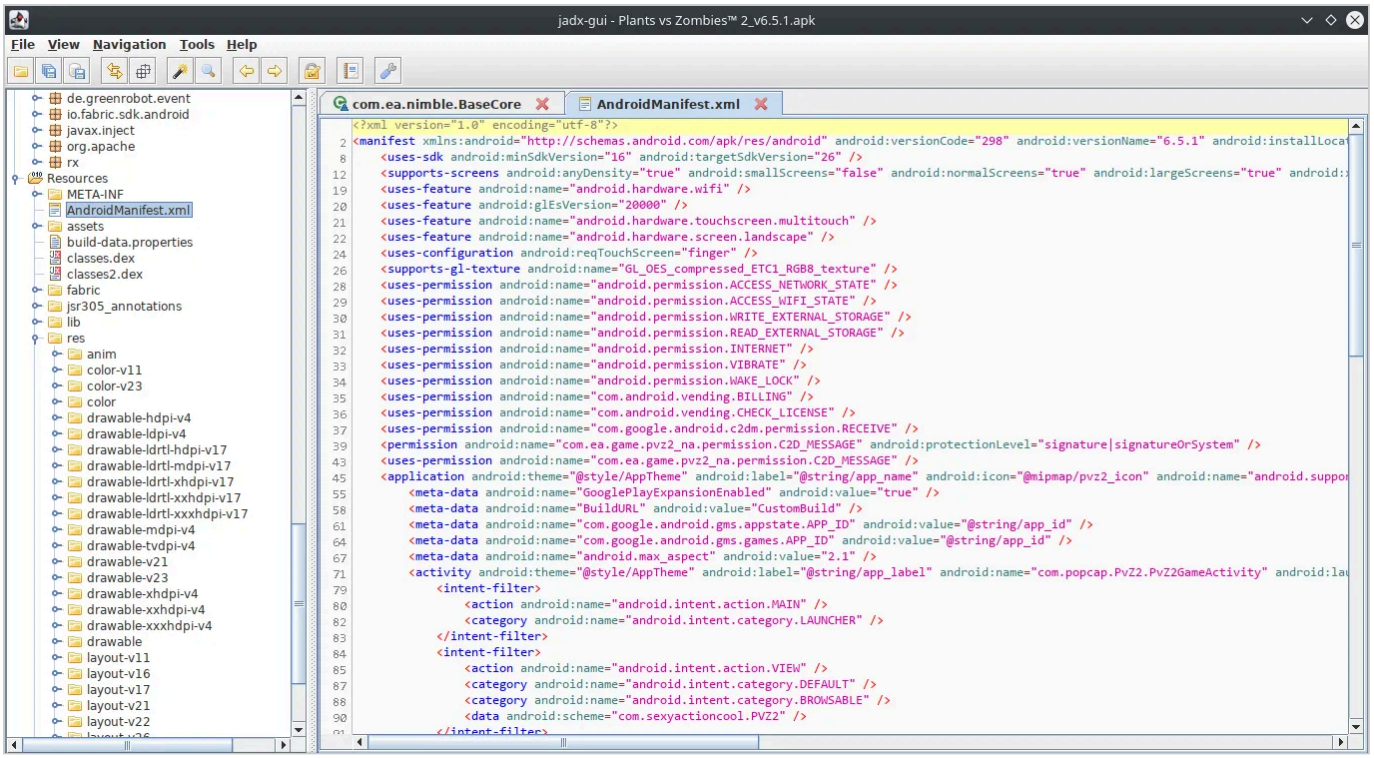
Misal pada contoh tulisan kali ini saya menggunakan APK dari Plants vs Zombie 2. Jadx akan melakukan proses decompiling terlebih dahulu, biasanya agak memakan banyak memory(java :p)



Nah seperti ini hasil dari decompile ketika selesai:



jadx juga menyediakan untuk androidmanifest dan resource yang ada dalam apk.



Bagaimana? Mudah kan? Tapi, perlu diingat bahwa setiap tool pasti memiliki kelemahan dan kekurangan, nantinya kita sendiri yang menentukan mana tool terbaik untuk kondisi yang sedang dialami hehe

Akhir kata, semoga tulisan ini bermanfaat.

Reverse Engineering # Security # Tutorial

Licensed under CC BY-SA 4.0