(Beta)

Overview

- APK
- Androguard

Installation

- option 1
  https://github.com/DploY707/static-apk-analyzer.git

How to use

Install the project

- clone the project
- move to cloned directory

```
$ cd [root directory of this project]
```

- build the docker image

```
$ docker build -t android-analyzer ./
```

Getting start

> *"Sequence 3, 4 will be removed in the future you can analyze the APKs with just running the docker image)"*

- Copy the APKs that you want to analysis to "**[root directory of this project]/data**"
- Run the docker image

```
$ docker run -it --rm -v [host APK directory path]:/root/workDir/data
android-analyzer
```

- Run the program that analysis APKs

```
$ python3 main.py
```

- Extract analysis result (**In this version, methodList Log**)

```
$ docker cp [CONTAINER_ID]:/root/results/methodLists/
[host_dir_path_to_save_extracted_data]
```

- Use the extracted Log
  - Extracted Log file is a binary file, so you can use it with "**python pickle**"

```
$ python3
>>> import pickle
>>> f = open('[log_path]', 'rb')
>>> p = pickle.load(f)

# now you can use extracted MethodLis
```

MethodList Log format

```
OrderedDict([
        ('className', 'LAAa;'),
        ('methodName', '<init>'),
        ('returnType', 'void'),
        ('registers', OrderedDict([('begin', 0), ('size', 1)])),
        ('paramList', [(1, 'yAa')]),
        ('accessFlagList', ['public', 'constructor']),
        ('methodIndex', 1),
        ('codeSize', 6),
        ('instructions',
                        [OrderedDict([('bytecode', '7010808b0000'),
                                ('smali', 'invoke-directv0, Ljava/lang
/Object;-><init>()V')]),
                        OrderedDict([('bytecode', '5b011700'),
                                ('smali', 'iput-objectv1, v0, LAAa;-
>ESbLyAa;')]),
                        OrderedDict([('bytecode', '0e00'),
                                ('smali', 'return-void')]
                )]
        )
        ('javaSource', 'v0 = new LAAa(); \n return
void')
])
```

- className : (string)
- methodName : (string)
- returnType : (string)
- registers : (OrderedDict) params

        - begin :
        - size : begin
        - EX) begin = 1, size = 4 v1, v2, v3, v4

- paramList : (tuple list) tuple .
    - EX) [(1, 'yAa')] v1 yAa

- accessFlagList : (list) access flaghttps://source.android.com/devices/tech/dalvik/dex-format#access-flags

- methodIndex : (int) DEX index

- codeSize : (int) bytecode byte

- instructions : (OrderedDict list)
    - bytecode : bytecode
    - smali : smali baksmali

- javaSource : Java level decompile str

TODO

Code Extraction

- Single DEX
    - Goals & Achievement
        - All methods in DEX File
            - Androguard virtual, direct method
        - Perfect information should be in Log
            - decompile 2 issue
                1. exception method decompile (DAD error)
                1. DAD decompile ,

```
Multiple exit nodes found !
```

- Multi DEX

- Extern DEX / Jar / etc . . .

- Native Library

Call Reference parsing

- Invoke Instruction
    - Goals & Achievement
        - Invoke inst call chain
- Android Component Relation