ANDROGUARD ANALYSIS

Androguard documentation link:

https://androguard.readthedocs.io/en/latest/

Installation:

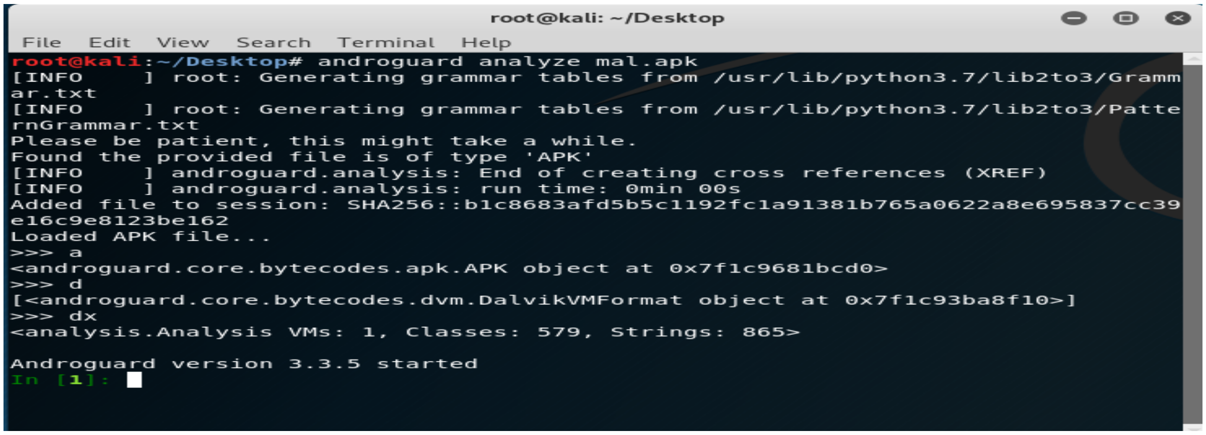
In KALI LINUX cmd type:

```
$ pip install -U androguard[magic,GUI]
```

STEPS TO ANALYSE:

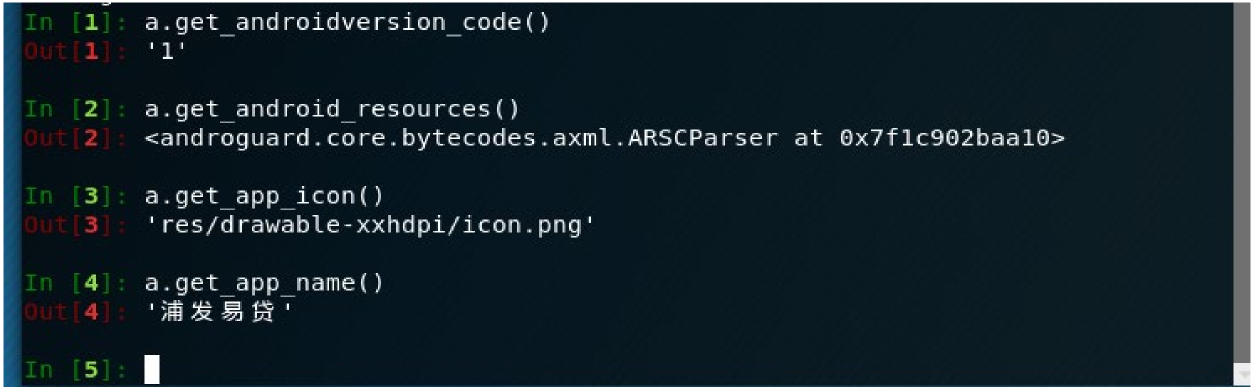
1. Run the following to extract files from apk.

```
androguard analyze mal.apk
```



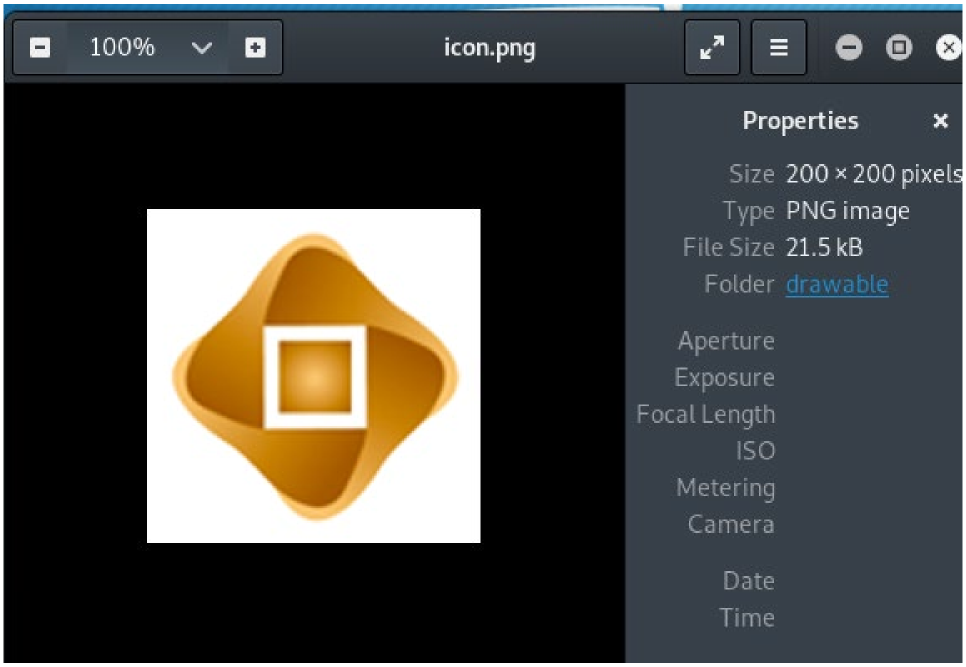
```
root@kali:~/Desktop# androguard analyze mal.apk
[INFO    ] root: Generating grammar tables from /usr/lib/python3.7/lib2to3/Gramm
ar.txt
[INFO    ] root: Generating grammar tables from /usr/lib/python3.7/lib2to3/Patte
rnGrammar.txt
Please be patient, this might take a while.
Found the provided file is of type 'APK'
[INFO    ] androguard.analysis: End of creating cross references (XREF)
[INFO    ] androguard.analysis: run time: 0min 00s
Added file to session: SHA256::b1c8683afd5b5c1192fc1a91381b765a0622a8e695837cc39
e16c9e8123be162
Loaded APK file...
>>> a
<androguard.core.bytecodes.apk.APK object at 0x7f1c9681bcd0>
>>> d
[<androguard.core.bytecodes.dvm.DalvikVMFormat object at 0x7f1c93ba8f10>]
>>> dx
<analysis.Analysis VMs: 1, Classes: 579, Strings: 865>

Androguard version 3.3.5 started
In [1]:
```

2. Run the following commands to get android version , app name and logo.



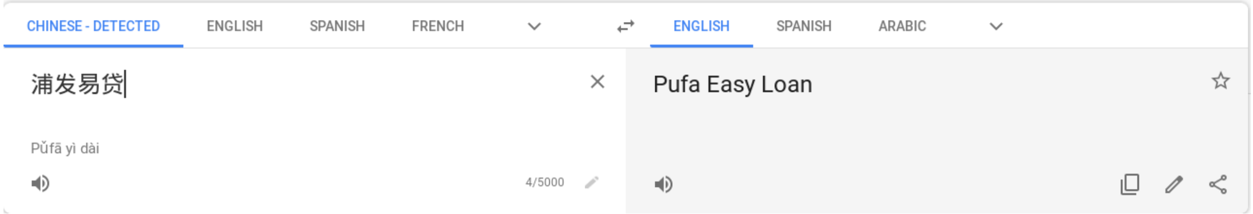
```
In [1]: a.get_androidversion_code()
Out[1]: '1'

In [2]: a.get_android_resources()
Out[2]: <androguard.core.bytecodes.axml.ARSCParser at 0x7f1c902baa10>

In [3]: a.get_app_icon()
Out[3]: 'res/drawable-xxhdpi/icon.png'

In [4]: a.get_app_name()
Out[4]: '浦发易贷'

In [5]:
```

APP LOGO:



Size 200 × 200 pixels
Type PNG image
File Size 21.5 kB
Folder drawable
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

Google translate of the android app name:



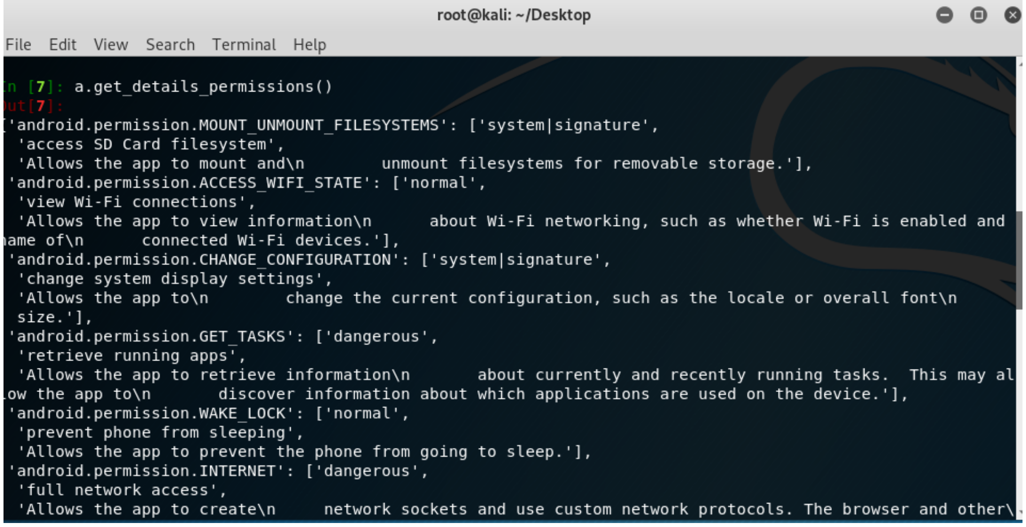
浦发易贷

Pǔfā yì dài

Pufa Easy Loan

3. For detailed permissions used in the apk, we extracted it using the following command:

```
a.get_details_permissions()
```



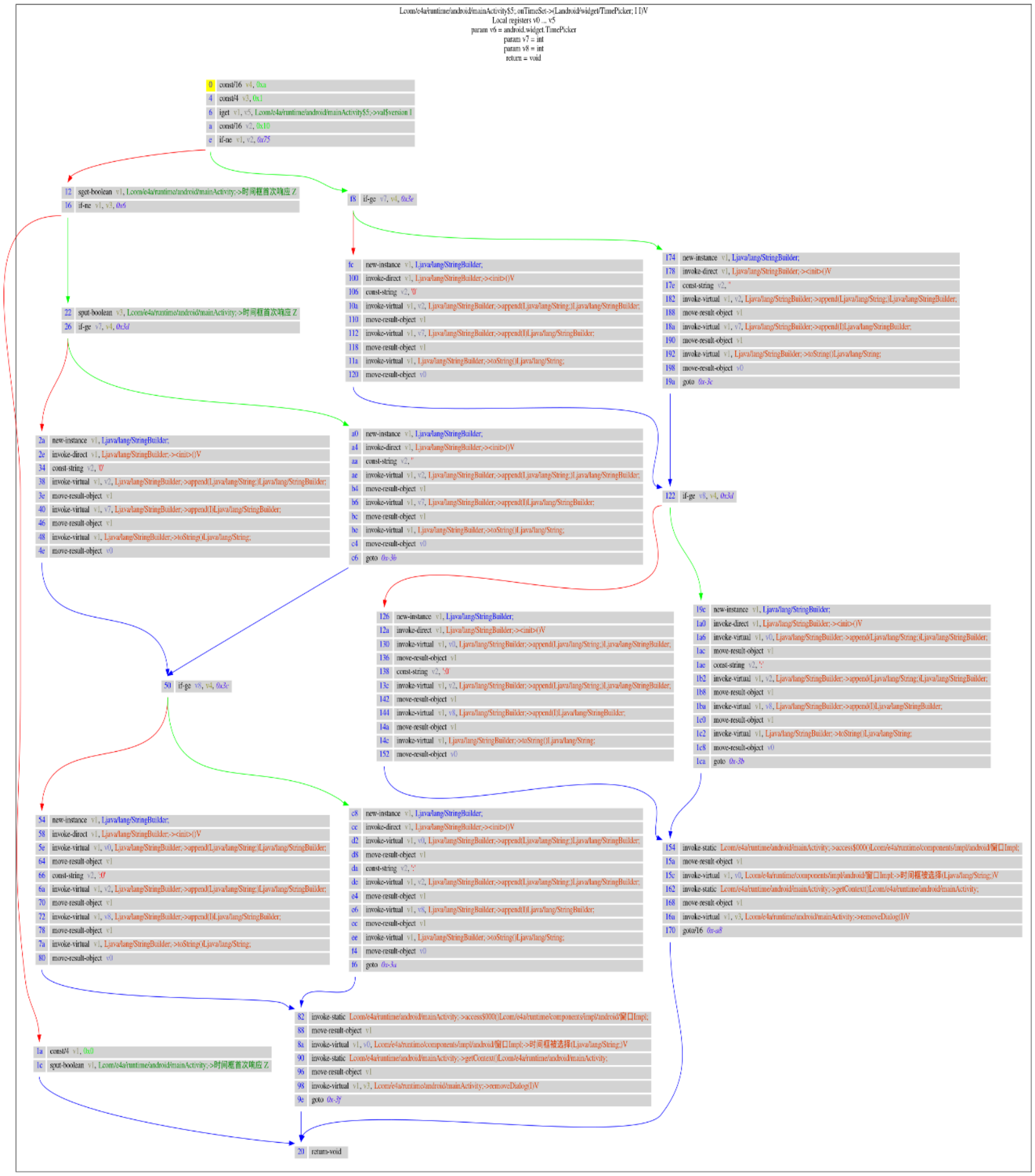
```
n [7]: a.get_details_permissions()
ut[7]:
['android.permission.MOUNT_UNMOUNT_FILESYSTEMS': ['system|signature',
  'access SD Card filesystem',
  'Allows the app to mount and\n        unmount filesystems for removable storage.'],
 'android.permission.ACCESS_WIFI_STATE': ['normal',
  'view Wi-Fi connections',
  'Allows the app to view information\n      about Wi-Fi networking, such as whether Wi-Fi is enabled and
ame of\n      connected Wi-Fi devices.'],
 'android.permission.CHANGE_CONFIGURATION': ['system|signature',
  'change system display settings',
  'Allows the app to\n        change the current configuration, such as the locale or overall font\n
  size.'],
 'android.permission.GET_TASKS': ['dangerous',
  'retrieve running apps',
  'Allows the app to retrieve information\n       about currently and recently running tasks.  This may al
ow the app to\n       discover information about which applications are used on the device.'],
 'android.permission.WAKE_LOCK': ['normal',
  'prevent phone from sleeping',
  'Allows the app to prevent the phone from going to sleep.'],
 'android.permission.INTERNET': ['dangerous',
  'full network access',
  'Allows the app to create\n     network sockets and use custom network protocols. The browser and other\
```

Androguard gives a detailed description of what each permission does and labels them to be either harmful or safe. See below

```
{'android.permission.MOUNT_UNMOUNT_FILESYSTEMS': ['system|signature',
  'access SD Card filesystem',
  'Allows the app to mount and\n        unmount filesystems for removable storage.'],
 'android.permission.ACCESS_WIFI_STATE': ['normal',
  'view Wi-Fi connections',
  'Allows the app to view information\n      about Wi-Fi networking, such as whether Wi-Fi is enabled and name
of\n      connected Wi-Fi devices.'],
 'android.permission.CHANGE_CONFIGURATION': ['system|signature',
  'change system display settings',
  'Allows the app to\n       change the current configuration, such as the locale or overall font\n       size.'],
 'android.permission.GET_TASKS': ['dangerous',
  'retrieve running apps',
  'Allows the app to retrieve information\n       about currently and recently running tasks.  This may allow
the app to\n       discover information about which applications are used on the device.'],
 'android.permission.WAKE_LOCK': ['normal',
  'prevent phone from sleeping',
  'Allows the app to prevent the phone from going to sleep.'],
 'android.permission.INTERNET': ['dangerous',
  'full network access',
  'Allows the app to create\n      network sockets and use custom network protocols. The browser and other\n
applications provide means to send data to the internet, so this\n     permission is not required to send data
to the internet.'],
 'android.permission.READ_PHONE_STATE': ['dangerous',
  'read phone status and identity',
  'Allows the app to access the phone\n      features of the device.  This permission allows the app to determine
the\n       phone number and device IDs, whether a call is active, and the remote number\n      connected by a
call.'],
 'android.permission.SYSTEM_ALERT_WINDOW': ['dangerous',
  'draw over other apps',
  'Allows the app to draw on top of other\n         applications or parts of the user interface.  They may
interfere with your\n         use of the interface in any application, or change what you think you are\n
seeing in other applications.'],
 'android.permission.ACCESS_COARSE_LOCATION': ['dangerous',
  'approximate location\n      (network-based)',
  'Allows the app to get your\n      approximate location. This location is derived by location services using\n
network location sources such as cell towers and Wi-Fi. These location\n       services must be turned on and
available to your device for the app to\n       use them. Apps may use this to determine approximately where
you\n      are.'],
 'android.permission.ACCESS_FINE_LOCATION': ['dangerous',
  'precise location (GPS and\n      network-based)',
  'Allows the app to get your\n       precise location using the Global Positioning System (GPS) or network\n
location sources such as cell towers and Wi-Fi. These location services\n      must be turned on and available
to your device for the app to use them.\n       Apps may use this to determine where you are, and may consume
additional\n      battery power.'],
         'com.android.launcher.permission.INSTALL_SHORTCUT': ['normal',
          'Unknown permission from android reference',
          'Unknown permission from android reference'],
         'android.permission.ACCESS_NETWORK_STATE': ['normal',
          'view network connections',
          'Allows the app to view\n      information about network connections such as which networks exist
        and are\n      connected.'],
         'android.permission.WRITE_EXTERNAL_STORAGE': ['dangerous',
          'modify or delete the contents of your SD card',
          'Allows the app to write to the SD card.'],
         'com.android.launcher.permission.READ_SETTINGS': ['normal',
          'Unknown permission from android reference',
          'Unknown permission from android reference']}
```

4. To better visualize the app, androguard uses the following command to create CFGs (Control Flow graph).(Install grahviz and pydot before running this command)

```
Androgiard decompile -d output_folder -f jpg mal.apk
```

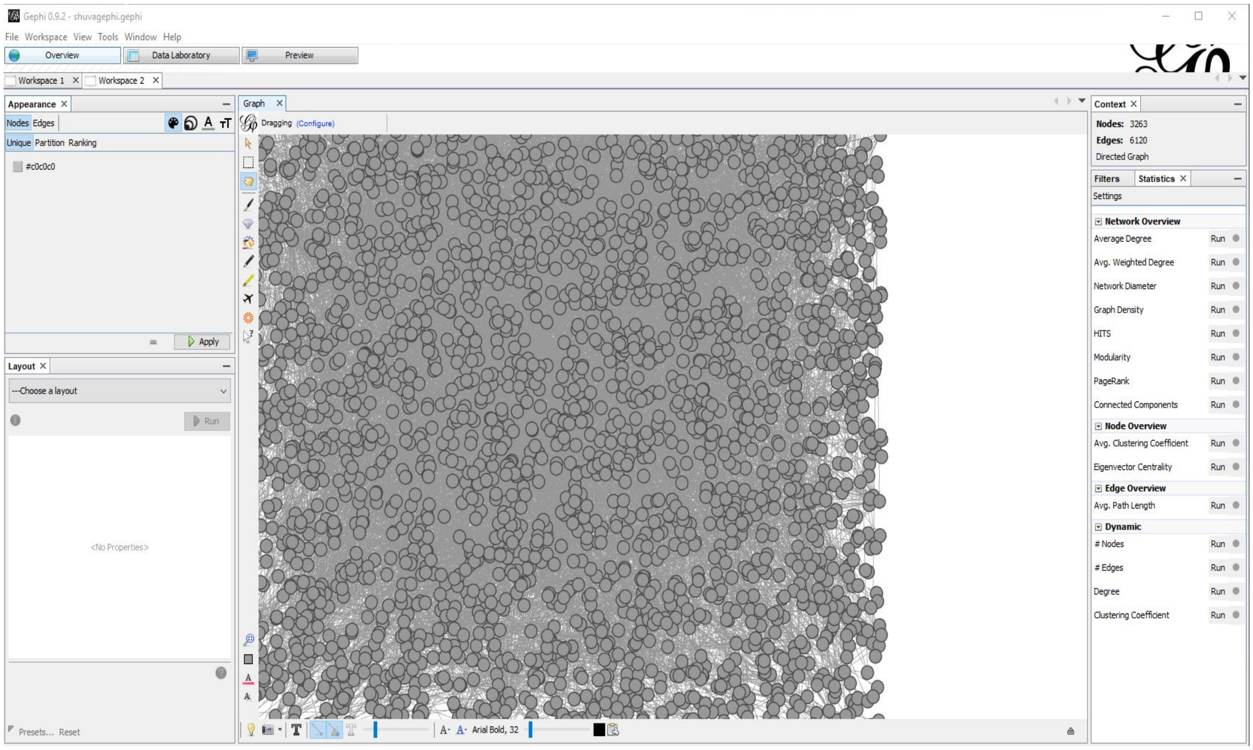


```
Lcom/e4a/runtime/android/mainActivity$5;.onTimeSet->(Landroid/widget/TimePicker; I I)V
Local registers v0 ... v5
param v6 = android.widget.TimePicker
param v7 = int
param v8 = int
return = void

0    const/16 v4, 0xa
4    const/4 v3, 0x1
6    iget v1, v5, Lcom/e4a/runtime/android/mainActivity$5;->val$version I
a    const/16 v2, 0x10
e    if-ne v1, v2, 0x75

12   sget-boolean v1, Lcom/e4a/runtime/android/mainActivity;->时间框首次响应 Z
16   if-ne v1, v3, 0x6

f8   if-ge v7, v4, 0x3e

fc   new-instance v1, Ljava/lang/StringBuilder;
100  invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
106  const-string v2, '0'
10a  invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
110  move-result-object v1
112  invoke-virtual v1, v7, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
118  move-result-object v1
11a  invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
120  move-result-object v0

174  new-instance v1, Ljava/lang/StringBuilder;
178  invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
17e  const-string v2, ''
182  invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
188  move-result-object v1
18a  invoke-virtual v1, v7, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
190  move-result-object v1
192  invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
198  move-result-object v0
19a  goto 0x-3c

22   sput-boolean v3, Lcom/e4a/runtime/android/mainActivity;->时间框首次响应 Z
26   if-ge v7, v4, 0x3d

2a   new-instance v1, Ljava/lang/StringBuilder;
2e   invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
34   const-string v2, '0'
38   invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
3e   move-result-object v1
40   invoke-virtual v1, v7, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
46   move-result-object v1
48   invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
4e   move-result-object v0

a0   new-instance v1, Ljava/lang/StringBuilder;
a4   invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
aa   const-string v2, ''
ae   invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
b4   move-result-object v1
b6   invoke-virtual v1, v7, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
bc   move-result-object v1
be   invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
c4   move-result-object v0
c6   goto 0x-3b

122  if-ge v8, v4, 0x3d

126  new-instance v1, Ljava/lang/StringBuilder;
12a  invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
130  invoke-virtual v1, v0, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
136  move-result-object v1
138  const-string v2, ':0'
13c  invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
142  move-result-object v1
144  invoke-virtual v1, v8, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
14a  move-result-object v1
14c  invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
152  move-result-object v0

19c  new-instance v1, Ljava/lang/StringBuilder;
1a0  invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
1a6  invoke-virtual v1, v0, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
1ac  move-result-object v1
1ae  const-string v2, ':'
1b2  invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
1b8  move-result-object v1
1ba  invoke-virtual v1, v8, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
1c0  move-result-object v1
1c2  invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
1c8  move-result-object v0
1ca  goto 0x-3b

50   if-ge v8, v4, 0x3c

54   new-instance v1, Ljava/lang/StringBuilder;
58   invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
5e   invoke-virtual v1, v0, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
64   move-result-object v1
66   const-string v2, ':0'
6a   invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
70   move-result-object v1
72   invoke-virtual v1, v8, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
78   move-result-object v1
7a   invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
80   move-result-object v0

c8   new-instance v1, Ljava/lang/StringBuilder;
cc   invoke-direct v1, Ljava/lang/StringBuilder;-><init>()V
d2   invoke-virtual v1, v0, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
d8   move-result-object v1
da   const-string v2, ':'
de   invoke-virtual v1, v2, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
e4   move-result-object v1
e6   invoke-virtual v1, v8, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
ec   move-result-object v1
ee   invoke-virtual v1, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
f4   move-result-object v0
f6   goto 0x-3a

154  invoke-static Lcom/e4a/runtime/android/mainActivity;->access$000()Lcom/e4a/runtime/components/impl/android/窗口Impl;
15a  move-result-object v1
15c  invoke-virtual v1, v0, Lcom/e4a/runtime/components/impl/android/窗口Impl;->时间框被选择(Ljava/lang/String;)V
162  invoke-static Lcom/e4a/runtime/android/mainActivity;->getContext()Lcom/e4a/runtime/android/mainActivity;
168  move-result-object v1
16a  invoke-virtual v1, v3, Lcom/e4a/runtime/android/mainActivity;->removeDialog(I)V
170  goto/16 0x-a8

1a   const/4 v1, 0x0
1c   sput-boolean v1, Lcom/e4a/runtime/android/mainActivity;->时间框首次响应 Z

82   invoke-static Lcom/e4a/runtime/android/mainActivity;->access$000()Lcom/e4a/runtime/components/impl/android/窗口Impl;
88   move-result-object v1
8a   invoke-virtual v1, v0, Lcom/e4a/runtime/components/impl/android/窗口Impl;->时间框被选择(Ljava/lang/String;)V
90   invoke-static Lcom/e4a/runtime/android/mainActivity;->getContext()Lcom/e4a/runtime/android/mainActivity;
96   move-result-object v1
98   invoke-virtual v1, v3, Lcom/e4a/runtime/android/mainActivity;->removeDialog(I)V
9e   goto 0x-3f

20   return-void
```

5. To create call graphs (methods as nodes and edge as calls to methods), run the following commands:

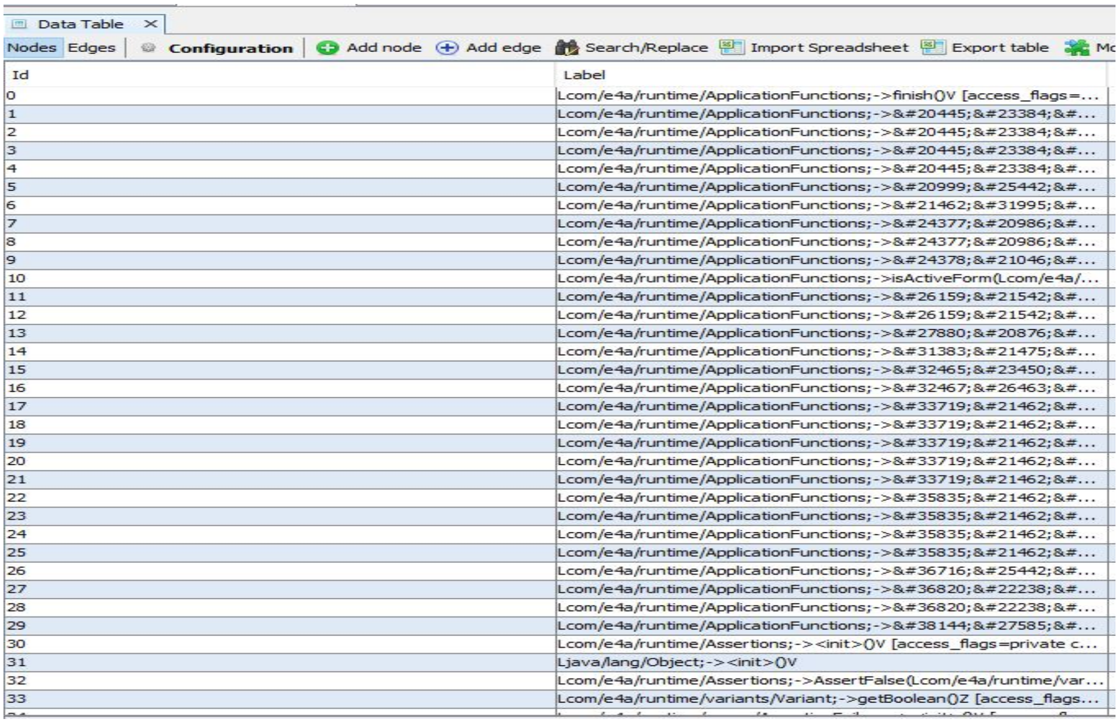
```
androguard cg mal.apk
```

It generates a .gml file which can be viewed using a visualization tool Gephi.



Nodes: 3263
Edges: 6120
Directed Graph

This tool also lists down the methods label and their node ids:



Id	Label
0	Lcom/e4a/runtime/ApplicationFunctions;->finish()V [access_flags=...
1	Lcom/e4a/runtime/ApplicationFunctions;->&#20445;&#23384;&#...
2	Lcom/e4a/runtime/ApplicationFunctions;->&#20445;&#23384;&#...
3	Lcom/e4a/runtime/ApplicationFunctions;->&#20445;&#23384;&#...
4	Lcom/e4a/runtime/ApplicationFunctions;->&#20445;&#23384;&#...
5	Lcom/e4a/runtime/ApplicationFunctions;->&#20999;&#25442;&#...
6	Lcom/e4a/runtime/ApplicationFunctions;->&#21462;&#31995;&#...
7	Lcom/e4a/runtime/ApplicationFunctions;->&#24377;&#20986;&#...
8	Lcom/e4a/runtime/ApplicationFunctions;->&#24377;&#20986;&#...
9	Lcom/e4a/runtime/ApplicationFunctions;->&#24378;&#21046;&#...
10	Lcom/e4a/runtime/ApplicationFunctions;->isActiveForm(Lcom/e4a/...
11	Lcom/e4a/runtime/ApplicationFunctions;->&#26159;&#21542;&#...
12	Lcom/e4a/runtime/ApplicationFunctions;->&#26159;&#21542;&#...
13	Lcom/e4a/runtime/ApplicationFunctions;->&#27880;&#20876;&#...
14	Lcom/e4a/runtime/ApplicationFunctions;->&#31383;&#21475;&#...
15	Lcom/e4a/runtime/ApplicationFunctions;->&#32465;&#23450;&#...
16	Lcom/e4a/runtime/ApplicationFunctions;->&#32467;&#26463;&#...
17	Lcom/e4a/runtime/ApplicationFunctions;->&#33719;&#21462;&#...
18	Lcom/e4a/runtime/ApplicationFunctions;->&#33719;&#21462;&#...
19	Lcom/e4a/runtime/ApplicationFunctions;->&#33719;&#21462;&#...
20	Lcom/e4a/runtime/ApplicationFunctions;->&#33719;&#21462;&#...
21	Lcom/e4a/runtime/ApplicationFunctions;->&#33719;&#21462;&#...
22	Lcom/e4a/runtime/ApplicationFunctions;->&#35835;&#21462;&#...
23	Lcom/e4a/runtime/ApplicationFunctions;->&#35835;&#21462;&#...
24	Lcom/e4a/runtime/ApplicationFunctions;->&#35835;&#21462;&#...
25	Lcom/e4a/runtime/ApplicationFunctions;->&#35835;&#21462;&#...
26	Lcom/e4a/runtime/ApplicationFunctions;->&#36716;&#25442;&#...
27	Lcom/e4a/runtime/ApplicationFunctions;->&#36820;&#22238;&#...
28	Lcom/e4a/runtime/ApplicationFunctions;->&#36820;&#22238;&#...
29	Lcom/e4a/runtime/ApplicationFunctions;->&#38144;&#27585;&#...
30	Lcom/e4a/runtime/Assertions;-><init>()V [access_flags=private c...
31	Ljava/lang/Object;-><init>()V
32	Lcom/e4a/runtime/Assertions;->AssertFalse(Lcom/e4a/runtime/var...
33	Lcom/e4a/runtime/variants/Variant;->getBoolean()Z [access_flags...