命令：

1.反编译： java -jar apktool_2.3.4.jar d *.apk

2.编译： java -jar apktool_2.3.4.jar b 文件夹

3.编译成功后在dist文件中生成编译后的apk

4.签名： jarsigner -digestalg SHA1 -sigalg SHA1withRSA -verbose -keystore mihui.key -signedjar app-release.encrypted.apk com.alibaba.android.rimet_4.6.3_497.apk 蜜惠

输出string类型日志

```
#test Log
const-string v1, "0.0"
const-string v2, "钉钉：getEntry_111111"
invoke-static {v1, v2}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I
```

输出boolean类型日志

```
#test Log 钉钉日志
const-string v1, "0.0"
invoke-static {p1}, Ljava/lang/String;->valueOf(Z)Ljava/lang/String;
move-result-object v2
invoke-static {v1, v2}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I
```

```
#test boolean
invoke-static {v12}, Ljava/lang/Boolean;->valueOf(Z)Ljava/lang/Boolean;
move-result-object v5
invoke-static {v5}, Lcom/langzu/baozha/ddutil/DDUtil;->testLog(Ljava/lang/Boolean;)V
```

输出int类型日志

```
#test int 旋转方向degree
invoke-static {v10}, Lcom/langzu/baozha/ddutil/DDUtil;->testLog(I)V
```

输出字符串拼接整型日志

```
#test Log
const-string v1, "0.0"
const-string v2, "钉钉：定位经纬度———31 31 31 getErrorCode:"
new-instance v3, Ljava/lang/StringBuilder;
invoke-direct {v3}, Ljava/lang/StringBuilder;-><init>()V
invoke-virtual {v3, v2}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
invoke-virtual {v3, v0}, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
invoke-virtual {v3}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v3
invoke-static {v1, v3}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I
```

toast输出

```
#test toast
const/4 v2, 0x1
```

```
const-string/jumbo v3, "欢迎使用爆炸版钉钉～～"
invoke-static {p0, v3, v2}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;I)Landroid/widget/Toast;
move-result-object v2
invoke-virtual {v2}, Landroid/widget/Toast;->show()V
```

钉钉模块注册 hdl.smali

```
.class public final Lhdl;
日志报文解析 service为hdl.smali中的模块名，action为模块中的方法名，例子：
```

service=internal.request, action=lwp

钉钉数据请求日志输入
修改涉及文件：
.class public Lcom/alibaba/lightapp/runtime/monitor/RuntimeTrace;

```
修改trace方法
打印日志
#test Log 钉钉日志
invoke-static {v1}, Lcom/langzu/baozha/ddutil/DDUtil;->testLog(Ljava/lang/String;)V
```

一. 植入工具类 DDUtil.smali
二. wifi修改

修改涉及文件：

.class public Lcom/alibaba/lightapp/runtime/plugin/device/Base;

.class Lcom/alibaba/lightapp/runtime/plugin/device/Base$1;

1.Landroid/net/wifi/WifiInfo;->getBSSID

```
#修改wifi
invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getMybssid()Ljava/lang/String;
move-result-object v0
```

2.Landroid/net/wifi/WifiInfo;->getSSID

```
Lcom/langzu/baozha/ddutil/DDUtil;->getMyssid
```

```
例子：
#修改wifi
invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getMyssid()Ljava/lang/String;
move-result-object v5
```

```
#修改wifi
invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getMybssid()Ljava/lang/String;
move-result-object v5
```

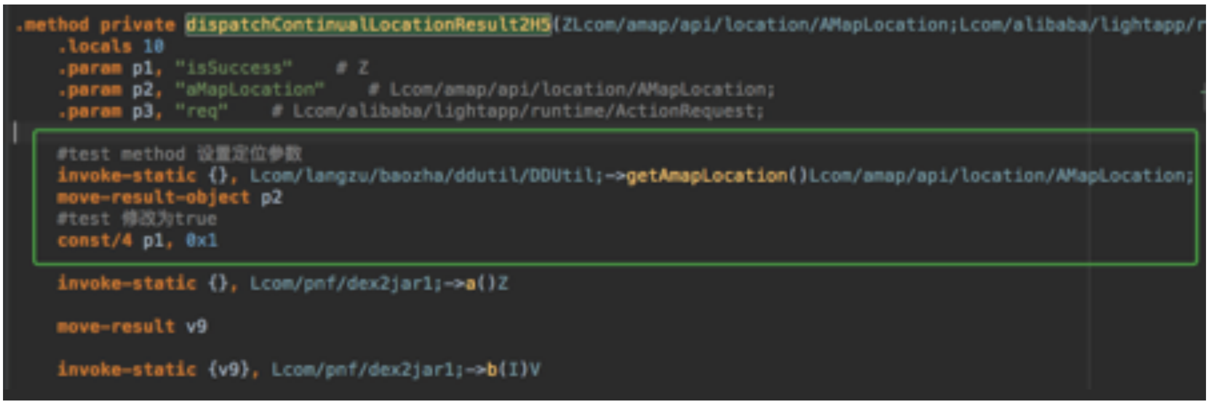
三. 定位修改

修改AndroidManifest.xml高德定位com.amap.api.v2.apikey

修改涉及文件：.class public Lcom/alibaba/lightapp/runtime/plugin/device/Geolocation;

```
修改dispatchContinualLocationResult2H5方法
```

```
修改入参 p1为true p2为自定义定位信息
#test method 设置定位参数
invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getAmapLocation()Lcom/amap/api/location/AMapLocation;
move-result-object p2
#test 修改为true
const/4 p1, 0x1
```



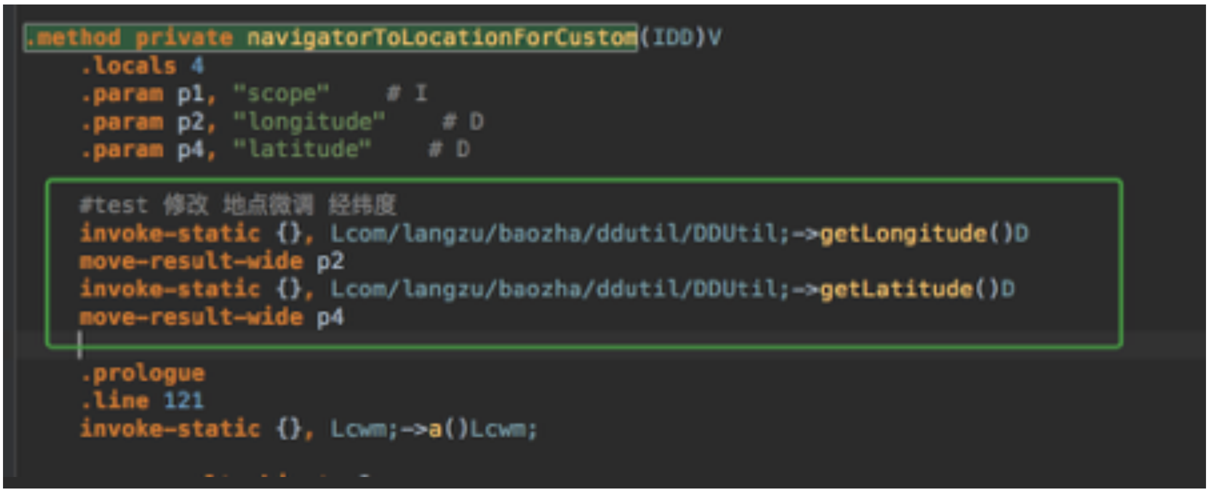
```
.method private dispatchContinualLocationResult2H5(ZLcom/amap/api/location/AMapLocation;Lcom/alibaba/lightapp/r
    .locals 10
    .param p1, "isSuccess"    # Z
    .param p2, "aMapLocation"    # Lcom/amap/api/location/AMapLocation;
    .param p3, "req"    # Lcom/alibaba/lightapp/runtime/ActionRequest;

    #test method 设置定位参数
    invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getAmapLocation()Lcom/amap/api/location/AMapLocation;
    move-result-object p2
    #test 修改为true
    const/4 p1, 0x1

    invoke-static {}, Lcom/pnf/dex2jar1;->a()Z

    move-result v9

    invoke-static {v9}, Lcom/pnf/dex2jar1;->b(I)V
```

签到 地点微调 设置

修改涉及文件 **.class public** Lcom/alibaba/lightapp/runtime/plugin/biz/Map;

修改方法**.method private** navigatorToLocationForCustom

```
#test 修改 地点微调 经纬度
invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getLongitude()D
move-result-wide p2
invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getLatitude()D
move-result-wide p4
```



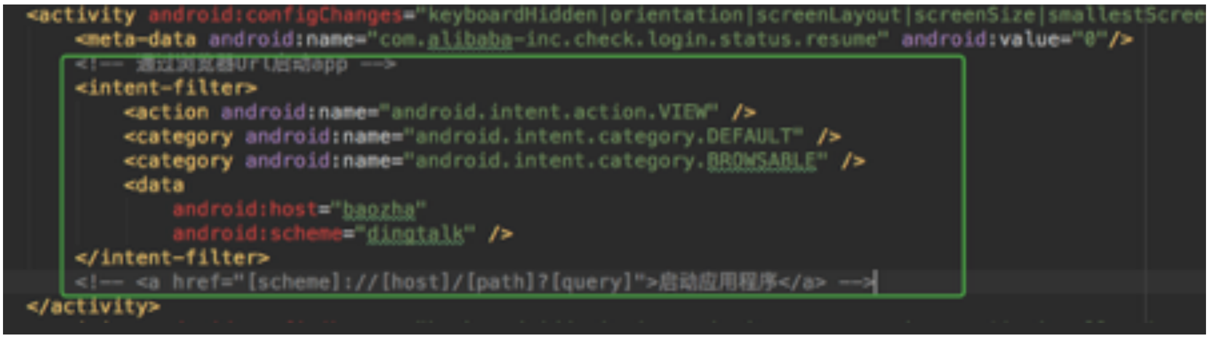
```
.method private navigatorToLocationForCustom(IDD)V
    .locals 4
    .param p1, "scope"    # I
    .param p2, "longitude"    # D
    .param p4, "latitude"    # D

    #test 修改 地点微调 经纬度
    invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getLongitude()D
    move-result-wide p2
    invoke-static {}, Lcom/langzu/baozha/ddutil/DDUtil;->getLatitude()D
    move-result-wide p4

    .prologue
    .line 121
    invoke-static {}, Lcwm;->a()Lcwm;
```

四.启动设置Activity

1.修改AndroidManifest.xml

com.alibaba.android.rimet.biz.SplashActivity

```
<!-- 通过浏览器Url启动app -->
<intent-filter>
<action
android:name="android.intent.action.VIEW"
/>
<category
android:name="android.intent.category.DEFAULT" />
<category
android:name="android.intent.category.BROWSABLE" />
<data
    android:host="baozha"
    android:scheme="dingtalk" />
</intent-filter>
```



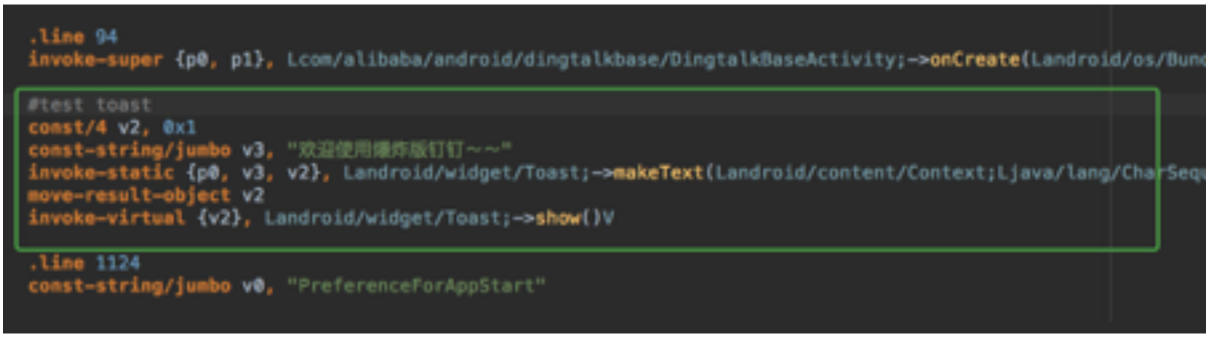
```
<activity android:configChanges="keyboardHidden|orientation|screenLayout|screenSize|smallestScree
    <meta-data android:name="com.alibaba-inc.check.login.status.resume" android:value="0"/>
    <!-- 通过浏览器Url启动app -->
    <intent-filter>
        <action android:name="android.intent.action.VIEW" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.BROWSABLE" />
        <data
            android:host="baozha"
            android:scheme="dingtalk" />
    </intent-filter>
    <!-- <a href="[scheme]://[host]/[path]?[query]">启动应用程序</a> -->
</activity>
```

2.修改文件

.class public Lcom/alibaba/android/rimet/biz/SplashActivity;

```
onCreate方法中
```

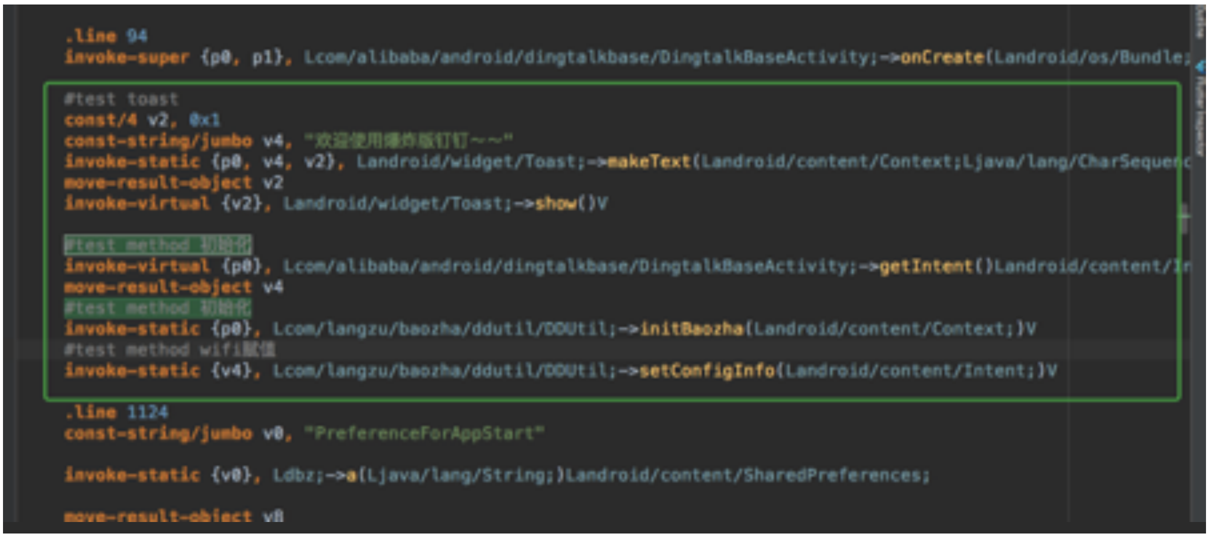
```
#test toast
const/4 v2, 0x1
const-string/jumbo v3, "欢迎使用爆炸版钉钉～～"
invoke-static {p0, v3, v2}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;I)Landroid/widget/Toast;
move-result-object v2
invoke-virtual {v2}, Landroid/widget/Toast;->show()V
```



```
.line 94
invoke-super {p0, p1}, Lcom/alibaba/android/dingtalkbase/DingtalkBaseActivity;->onCreate(Landroid/os/Bun

#test toast
const/4 v2, 0x1
const-string/jumbo v3, "欢迎使用爆炸版钉钉~~"
invoke-static {p0, v3, v2}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSeq
move-result-object v2
invoke-virtual {v2}, Landroid/widget/Toast;->show()V

.line 1124
const-string/jumbo v0, "PreferenceForAppStart"
```

```
#test method 初始化
invoke-virtual {p0}, Lcom/alibaba/
android/dingtalkbase/
DingtalkBaseActivity;-
>getIntent()Landroid/content/Intent;
move-result-object v4
```

```
#test method 初始化
invoke-static {p0}, Lcom/langzu/baozha/
ddutil/DDUtil;->initBaozha(Landroid/
content/Context;)V
#test method wifi赋值
invoke-static {v4}, Lcom/langzu/baozha/
ddutil/DDUtil;->setConfigInfo(Landroid/
content/Intent;)V
```



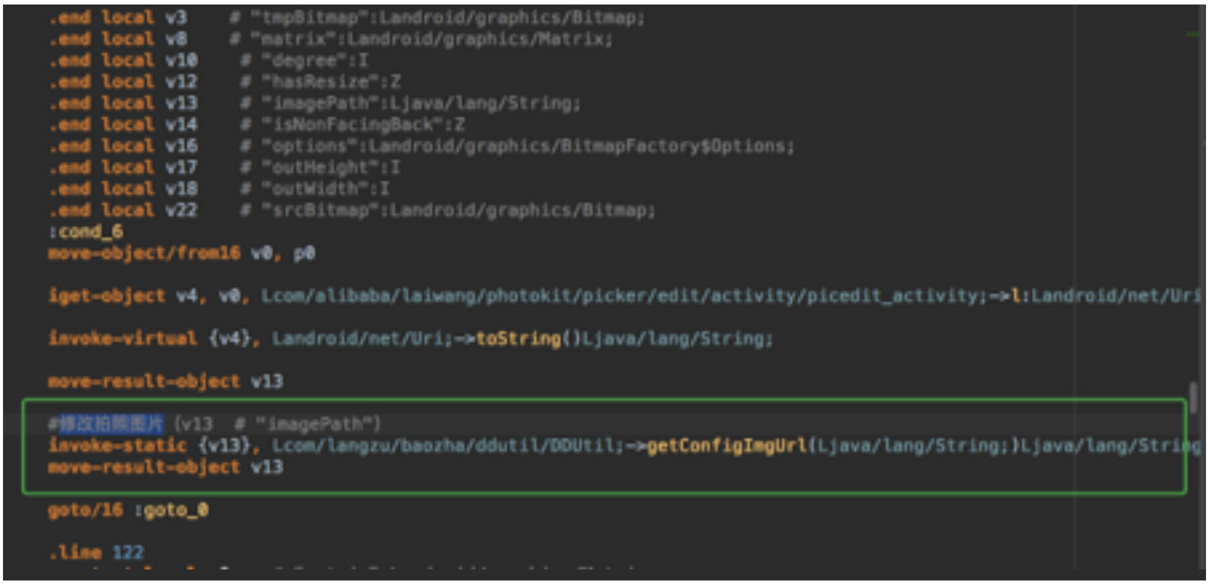
```
    .line 94
    invoke-super {p0, p1}, Lcom/alibaba/android/dingtalkbase/DingtalkBaseActivity;->onCreate(Landroid/os/Bundle;

    #test toast
    const/4 v2, 0x1
    const-string/jumbo v4, "欢迎使用爆炸版钉钉~~~"
    invoke-static {p0, v4, v2}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequenc
    move-result-object v2
    invoke-virtual {v2}, Landroid/widget/Toast;->show()V

    #test method 初始化
    invoke-virtual {p0}, Lcom/alibaba/android/dingtalkbase/DingtalkBaseActivity;->getIntent()Landroid/content/In
    move-result-object v4
    #test method 初始化
    invoke-static {p0}, Lcom/langzu/baozha/ddutil/DDUtil;->initBaozha(Landroid/content/Context;)V
    #test method wifi赋值
    invoke-static {v4}, Lcom/langzu/baozha/ddutil/DDUtil;->setConfigInfo(Landroid/content/Intent;)V

    .line 1124
    const-string/jumbo v0, "PreferenceForAppStart"

    invoke-static {v0}, Ldbz;->a(Ljava/lang/String;)Landroid/content/SharedPreferences;

    move-result-object v0
```

五.签到拍照图片配置

1.修改.class public Lcom/alibaba/laiwang/photokit/picker/edit/activity/picedit_activity;

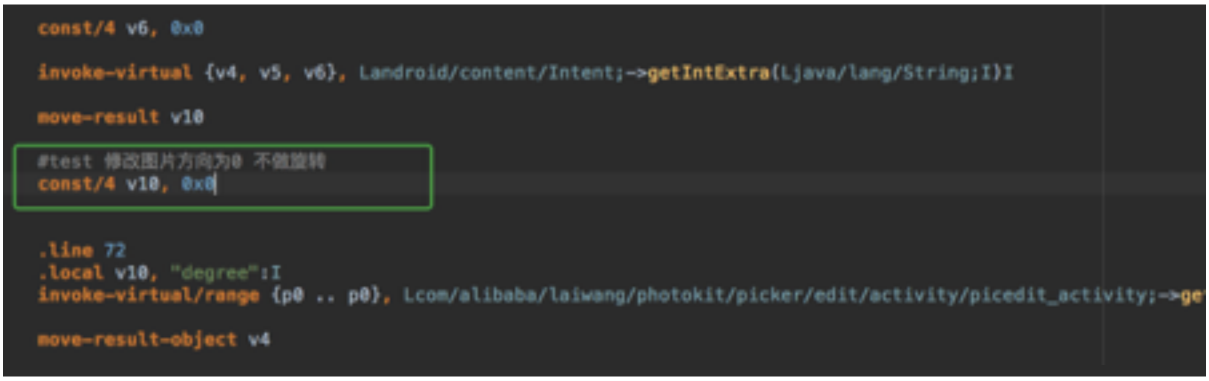
修改onCreate方法

```
#修改拍照图片 (v13  # "imagePath")
invoke-static {v13}, Lcom/langzu/baozha/ddutil/DDUtil;->getConfigImgUrl(Ljava/lang/String;)Ljava/lang/String;
move-result-object v13
```



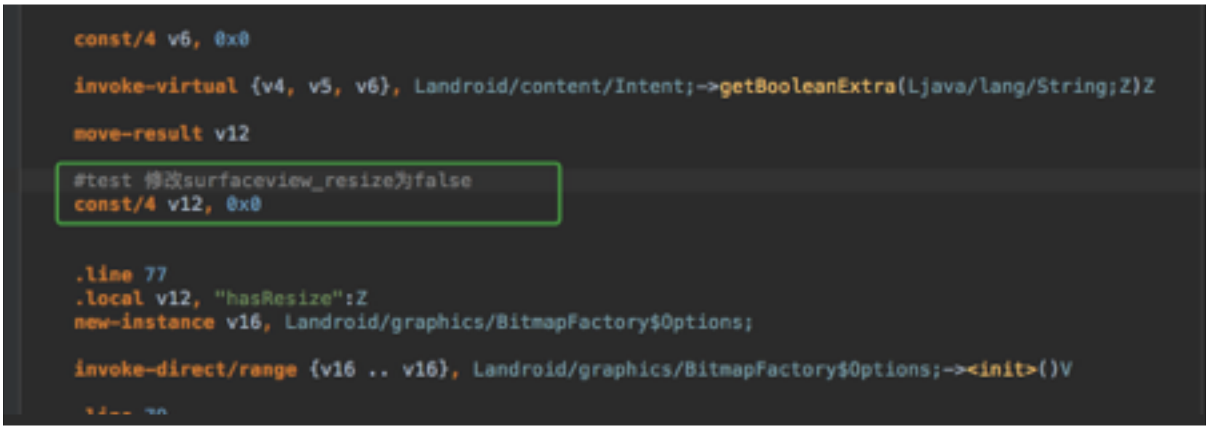
```
    .end local v3    # "tmpBitmap":Landroid/graphics/Bitmap;
    .end local v8    # "matrix":Landroid/graphics/Matrix;
    .end local v10    # "degree":I
    .end local v12    # "hasResize":Z
    .end local v13    # "imagePath":Ljava/lang/String;
    .end local v14    # "isNonFacingBack":Z
    .end local v16    # "options":Landroid/graphics/BitmapFactory$Options;
    .end local v17    # "outHeight":I
    .end local v18    # "outWidth":I
    .end local v22    # "srcBitmap":Landroid/graphics/Bitmap;
    :cond_6
    move-object/from16 v0, p0

    iget-object v4, v0, Lcom/alibaba/laiwang/photokit/picker/edit/activity/picedit_activity;->l:Landroid/net/Uri

    invoke-virtual {v4}, Landroid/net/Uri;->toString()Ljava/lang/String;

    move-result-object v13

    #修改拍照图片 (v13  # "imagePath")
    invoke-static {v13}, Lcom/langzu/baozha/ddutil/DDUtil;->getConfigImgUrl(Ljava/lang/String;)Ljava/lang/String
    move-result-object v13

    goto/16 :goto_0

    .line 122
```

```
#test 修改图片方向为0 不做旋转 注意修改地方
const/4 v10, 0x0
```



```
    const/4 v6, 0x0

    invoke-virtual {v4, v5, v6}, Landroid/content/Intent;->getIntExtra(Ljava/lang/String;I)I

    move-result v10

    #test 修改图片方向为0 不做旋转
    const/4 v10, 0x0

    .line 72
    .local v10, "degree":I
    invoke-virtual/range {p0 .. p0}, Lcom/alibaba/laiwang/photokit/picker/edit/activity/picedit_activity;->ge

    move-result-object v4
```

```
#test 修改surfaceview_resize为false 注意修改地方
const/4 v12, 0x0
```



```
const/4 v6, 0x0

invoke-virtual {v4, v5, v6}, Landroid/content/Intent;->getBooleanExtra(Ljava/lang/String;Z)Z

move-result v12

#test 修改surfaceview_resize为false
const/4 v12, 0x0


.line 77
.local v12, "hasResize":Z
new-instance v16, Landroid/graphics/BitmapFactory$Options;

invoke-direct/range {v16 .. v16}, Landroid/graphics/BitmapFactory$Options;-><init>()V
```

六.考勤打卡拍照图片配置

1.修改AndroidManifest.xml文件中的Activity的配置

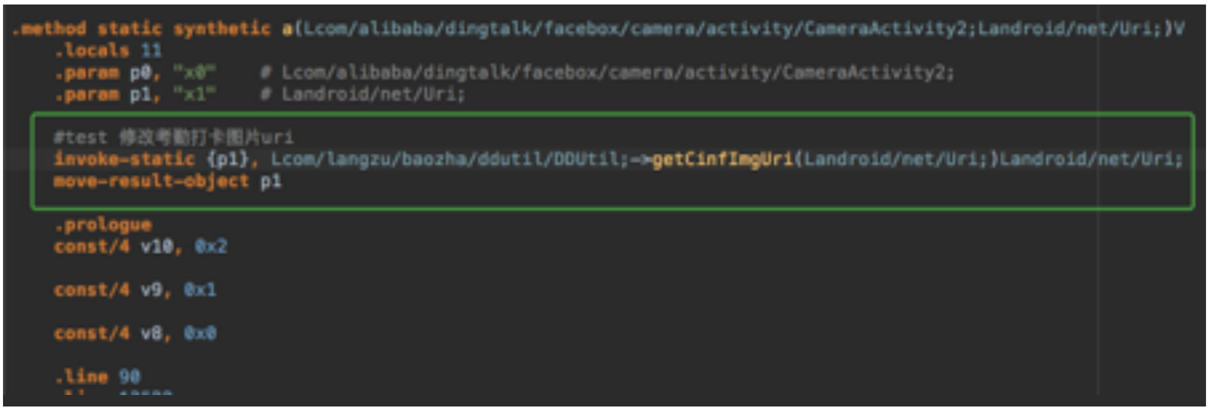
```
com.alibaba.dingtalk.facebox.camera.activity.CameraActivity2 和
com.alibaba.dingtalk.facebox.camera.activity.PiceditActivity2
```

删除不同进程的配置android:process=":tools"

2.修改**.class public** Lcom/alibaba/dingtalk/facebox/camera/activity/CameraActivity2;

修改的方法**.method static synthetic** a(Lcom/alibaba/dingtalk/facebox/camera/activity/CameraActivity2;Landroid/net/Uri;)V

```
#test 修改考勤打卡图片uri
invoke-static {p1}, Lcom/langzu/baozha/ddutil/DDUtil;->getCinfImgUri(Landroid/net/Uri;)Landroid/net/Uri;
move-result-object p1
```



```
.method static synthetic a(Lcom/alibaba/dingtalk/facebox/camera/activity/CameraActivity2;Landroid/net/Uri;)V
    .locals 11
    .param p0, "x0"    # Lcom/alibaba/dingtalk/facebox/camera/activity/CameraActivity2;
    .param p1, "x1"    # Landroid/net/Uri;

    #test 修改考勤打卡图片uri
    invoke-static {p1}, Lcom/langzu/baozha/ddutil/DDUtil;->getCinfImgUri(Landroid/net/Uri;)Landroid/net/Uri;
    move-result-object p1

    .prologue
    const/4 v10, 0x2

    const/4 v9, 0x1

    const/4 v8, 0x0

    .line 90
```

七.包名修改 还没有破解成功

修改AndroidManifest.xml

```
1.package="com.alibaba.android.rimet2"
2.修改自定义权限
<permission android:name="com.alibaba.android.rimet2.permission.MIPUSH_RECEIVE" android:protectionLevel="signature"/>
<permission android:name="com.alibaba.android.rimet2.permission.C2D_MESSAGE" android:protectionLevel="signature"/>
```

```
3.所有<provider>标签中的authorities属性相关包名
```