逆向gfx tool 第一天

笔记本:	gfx逆向		
创建时间:	2019/10/9 20:00	**更新时间:**	2019/11/16 21:06
作者:	381643188@qq.com		

先使用jeb导出反编译的java文件，res文件反编译失败了。

反编译Gfx Tool

主流程

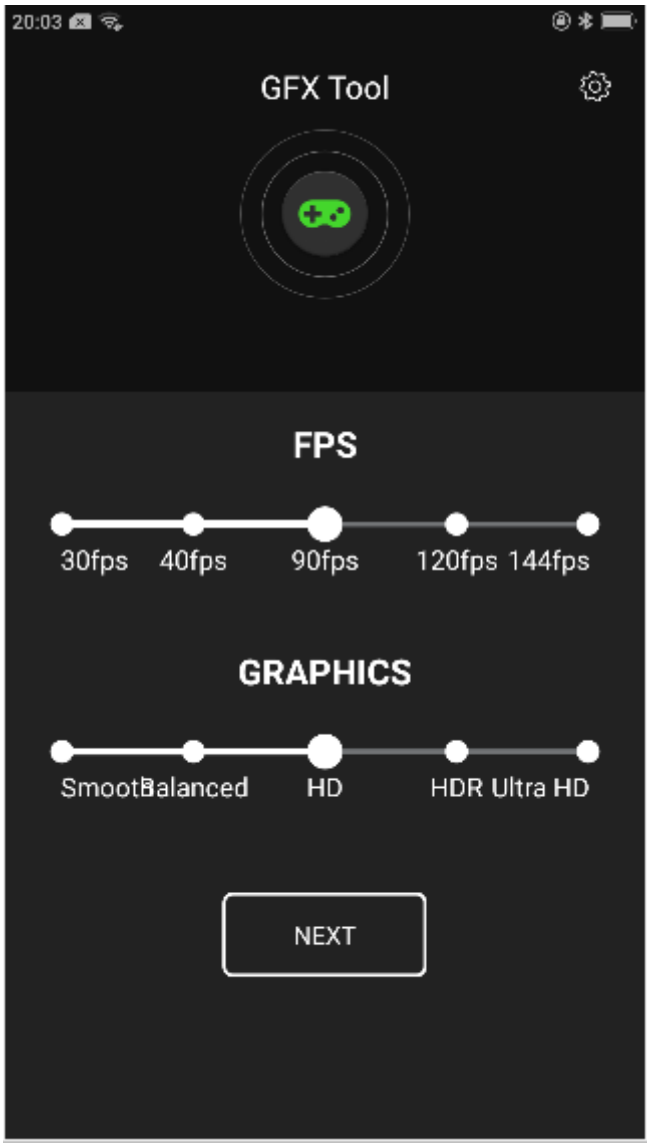
apk获取

```
adb shell pm path com.ayanne.gamebooster
package:/data/app/com.ayanne.gamebooster-tpXCqRa5nhhjpX-r3SuF5Q==/base.apk
package:/data/app/com.ayanne.gamebooster-tpXCqRa5nhhjpX-
r3SuF5Q==/split_config.xxhdpi.apk
package:/data/app/com.ayanne.gamebooster-tpXCqRa5nhhjpX-
r3SuF5Q==/split_config.zh.apk
```

使用apktool 2.4进行逆向
https://ibotpeaches.github.io/Apktool/
代码使用jeb和jadx1.0进行逆向。
https://github.com/skylot/jadx/releases

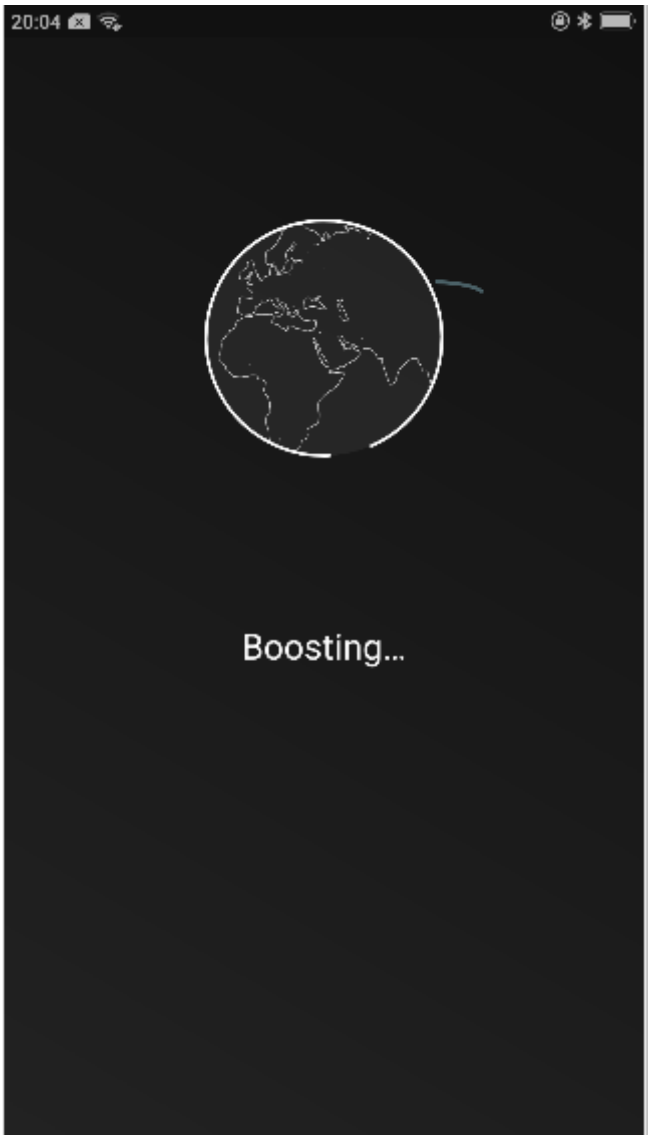
进入主界面进行dump，显示GameTrayActivity。
进度gfx tool进行dump：
第一个界面resolution为com.ayanne.gamebooster.gfxtool.SelectResolutionActivity

第二个界面fps、graphics为com.ayanne.gamebooster.gfxtool.QualityActivity

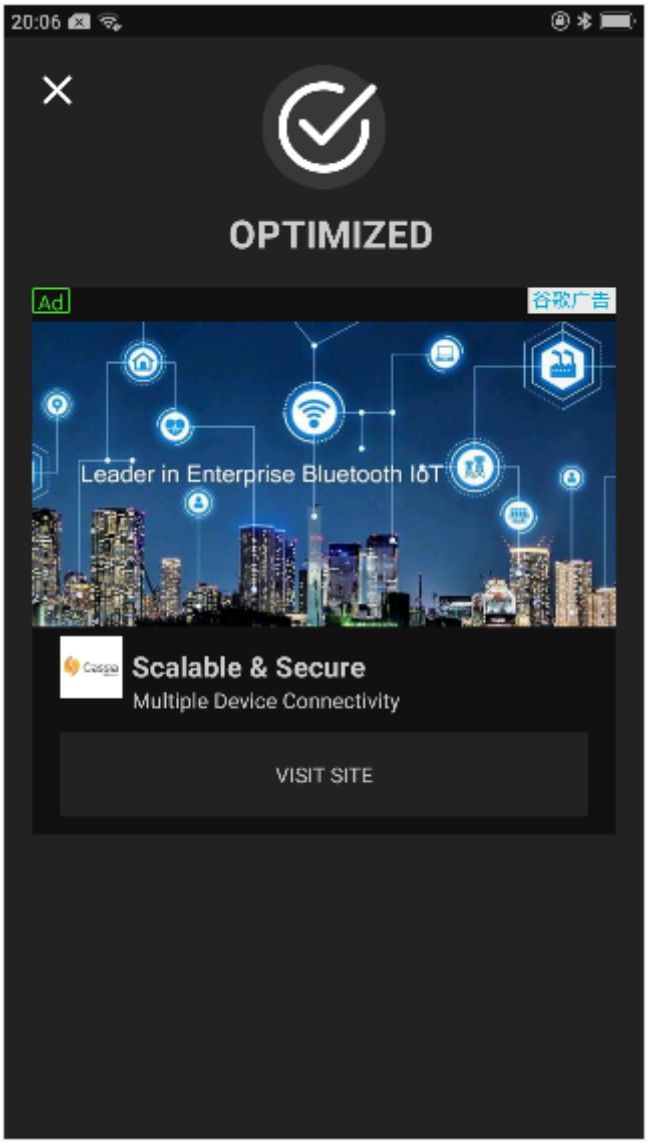


第三个界面game booster为com.ayanne.gamebooster.gfxtool.BoostOptionActivity

第四个界面boosting为com.ayanne.gamebooster.gfxtool.GFXBoostActivity



第五个界面optimized为com.ayanne.gamebooster.gfxtool.BoostCompletedActivity



resolution

SelectResolutionActivity的布局id为2131,361831，换算为16进制后为0x7f0a0027，activity_select_resolution。
其中名为next的button的id为nextBtn，0x7f0800bd，2131230909，对应反编译代码this.r，点击后直接启动QualityActivity，没有做其他事情，所以在com.warkiz.widget.IndicatorSeekBar上找寻处理逻辑。

```
<string-array name="resolution_array">
        <item>960</item>
        <item>1280</item>
        <item>1440</item>
        <item>1600</item>
        <item>1920</item>
        <item>2560</item>
</string-array>
```

id为seekBar，0x7f0800f4，2131230964，为r控件。
实际控制代码为

```
import com.ayanne.gamebooster.b.c;
this.r.setOnSeekChangeListener(new e() {
    public void a(IndicatorSeekBar arg1) {
    }
    public void a(g arg2) {
        c.a(this.a).d(arg2.b);
    }
    public void b(IndicatorSeekBar arg1) {
    }
});
```

在c中的代码应该是将分辨率数据写入了文件中

```
this.b.edit().putInt("NUMBER_OF_USAGE_FOR_RATE_APP_PREFS", arg3).apply();
```

开始优化

BoostOptionActivity中的nextButton，名为r。执行后跳转到GFXBoostActivity，继承com.ayanne.gamebooster.a。
GFXBoostActivity在onResume的时候调用了

```
if(this.n != null) {
    this.n.a();
}
```

这个n是父类com.ayanne.gamebooster.a中的，是类型com.ayanne.gamebooster.b.d，然后发现了实际的优化代码为

```
public int a() {
    try {
        this.b = ((int)a.a(this.a.getApplicationContext()));
        b.a.a.a("clearRAM: free memory ram before boost = " + this.b, new
Object[0]);
        e.a().a(this.a);
        this.b = ((int)a.a(this.a.getApplicationContext()));
        b.a.a.a("clearRAM: free memory ram after boost = " + this.b, new
Object[0]);
    }
```

```
    catch(Throwable v1) {
        this.b = 0;
        b.a.a.a(v1);
    }
    return this.b;
}
```

其中e.a().a(this.a);会调用代码

```
public void a(Context arg5) {
    ActivityManager.killBackgroundProcesses
    ……
    System.runFinalization();
    Runtime.getRuntime().gc();
    System.gc();

}
```

功能为杀进程，并进行gc。

如下代码块的功能为打印当前的内存状态。是通过获取/proc/meminfo
中的信息，和ActivityManager.getMemoryInfo。

```
this.b = ((int)a.a(this.a.getApplicationContext()));
b.a.a.a("clearRAM: free memory ram before boost = " + this.b, new
Object[0]);
```