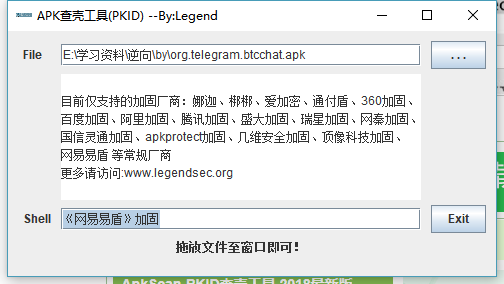
# BiYong自动抢红包插件开发

Git: https://github.com/wawa2222/BiYong-RedPackage-Xposed.git

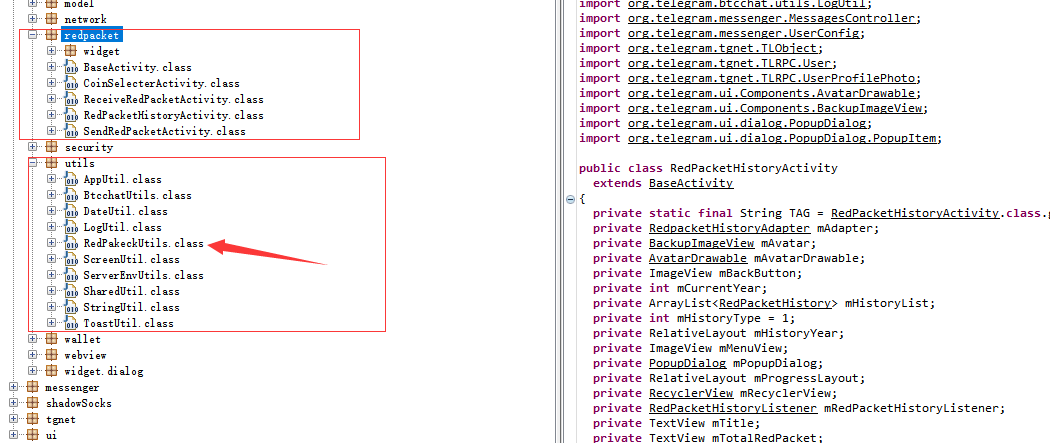
## BiYong聊天工具逆向

第一步查壳



网易易盾加壳,蛋疼。。。

找历史版本,看是否有壳,我这里找到个没壳的,直接反编译,看到些敏感信息的类文件



编写Xposed文件，这里我直接用别人写好的模板

XposedHelpers.*findAndHookMethod*(XposedHelpers.*findClass*(**"java.lang.ClassLoader"**, **loadPackageParam**.**classLoader**), **"loadClass"**, String.**class**, **new** XC\_MethodHook() {  
 @Override  
 **protected void** afterHookedMethod(MethodHookParam param) **throws** Throwable {  
 **super**.afterHookedMethod(param);  
 Class<?> clazz = (Class<?>) param.getResult();  
 **if**( clazz!= **null** && clazz.getName().indexOf(**"org.telegram"**)!=-1){  
 Method[] declaredMethods = clazz.getDeclaredMethods();  
 Log.*e*(**"[执行方法]:"** , **"-------------init--------------"** + Arrays.*toString*(declaredMethods));  
 **for** (**final** Method method : declaredMethods) {  
 **if**(!**set**.contains(method)){  
 **set**.add(method);  
 XposedBridge.*hookMethod*(method, **new** XC\_MethodHook() {  
 @Override  
 **protected void** afterHookedMethod(MethodHookParam param) **throws** Throwable {  
 **super**.afterHookedMethod(param);  
 Log.*e*(**"[执行方法]:"** ,  
 **"class -- "** + param.**thisObject** == **null** ? **null** : param.**thisObject**.getClass()  
 + **"-- methodName -- "** + param.**method**.getName()  
 + **"-- ParameterTypes --"** + Arrays.*toString*(method.getParameterTypes())  
 + **"-- result -- "** + param.getResult()  
 + **"-- param.args -- "** + Arrays.*toString*(param.**args**) + **"--"** );  
 }  
 });  
 }  
 }  
 }  
 }  
});

Hook注入看日志

未领取红包领取红包日志，

领取红包再领取红包的日志

有了这些日志,当然hook到抢红包的方法就是时间问题了

记得用文件差异分析，今天先溜了