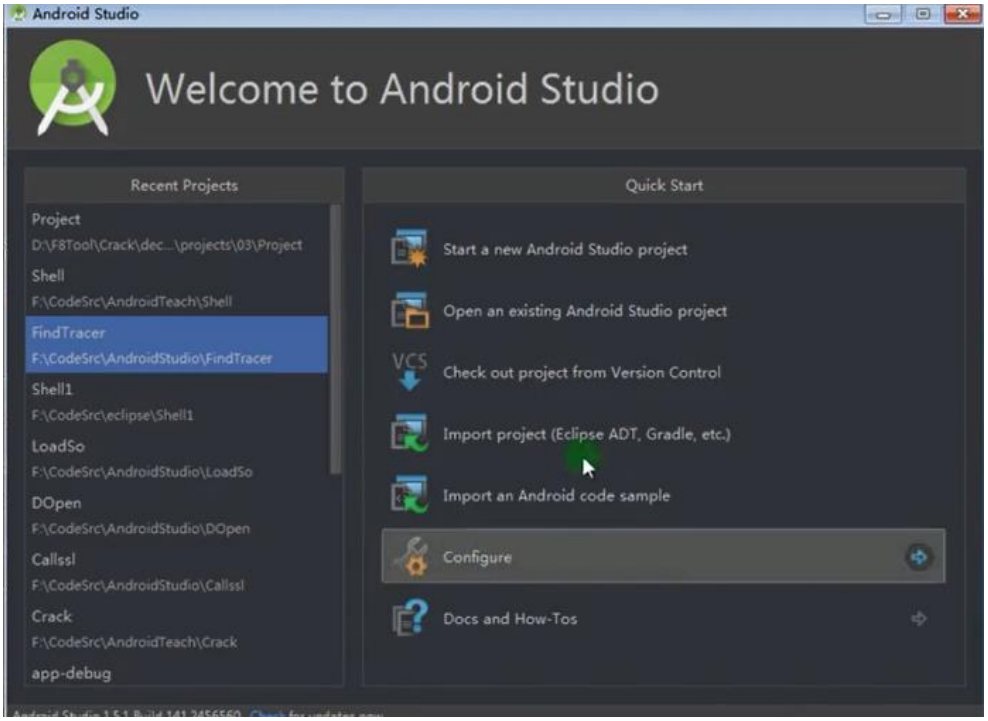
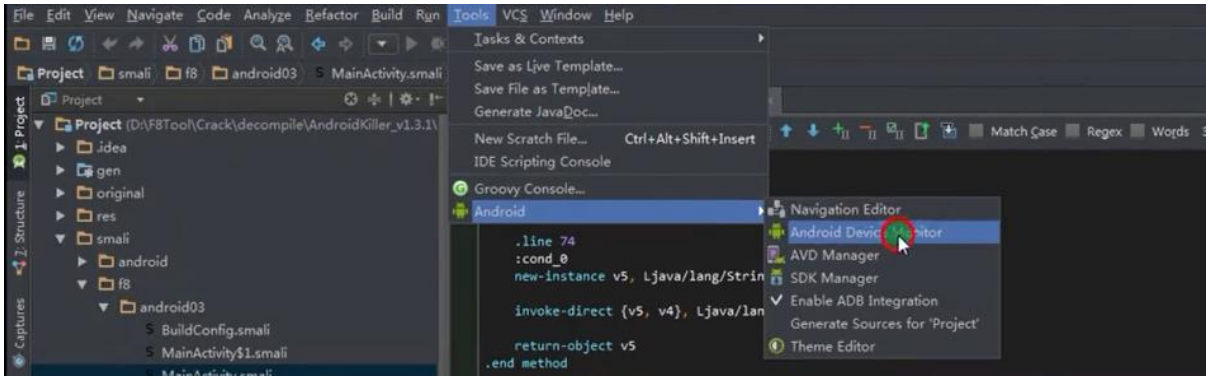
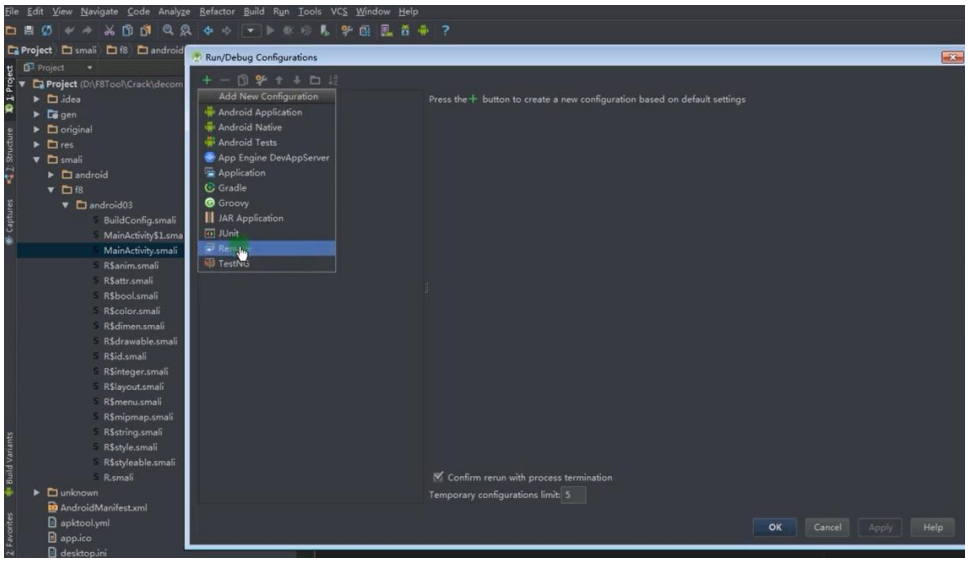
1. ShakaApktool 工具：比 Apktool 更加强大
   d -> 反编译
   b -> 回编译
   -df -> 使用默认框架
   -o -> 输出目录和文件名
2. 新调试方法：AndroidStudio/idea + smaliIdea 插件
   (1)反编译 apk 文件
   (2)AS/Idea 中导入源码, File -> open Or Import project



   (3)安装好对应的 app 并打开 Android Device Monitor

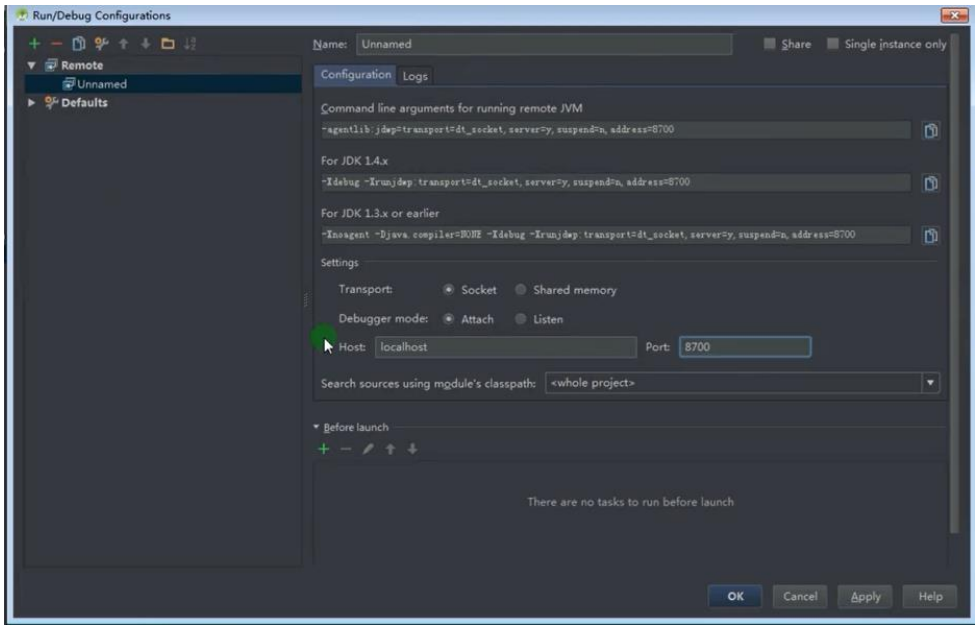


   设置远程调试选项
   Run -> Debug Configurations -> Remote Java Application



Host 填写为 localhost

端口为 Debug 开放的端口 8700



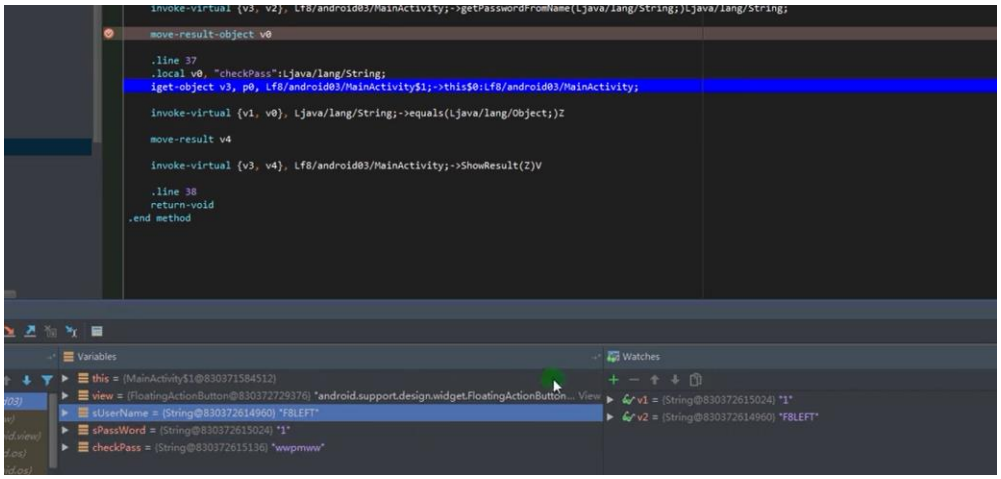
(4)使用 adb 以 debug 方式启动 apk

Adb shell am start -D -n packageName/ActivityName

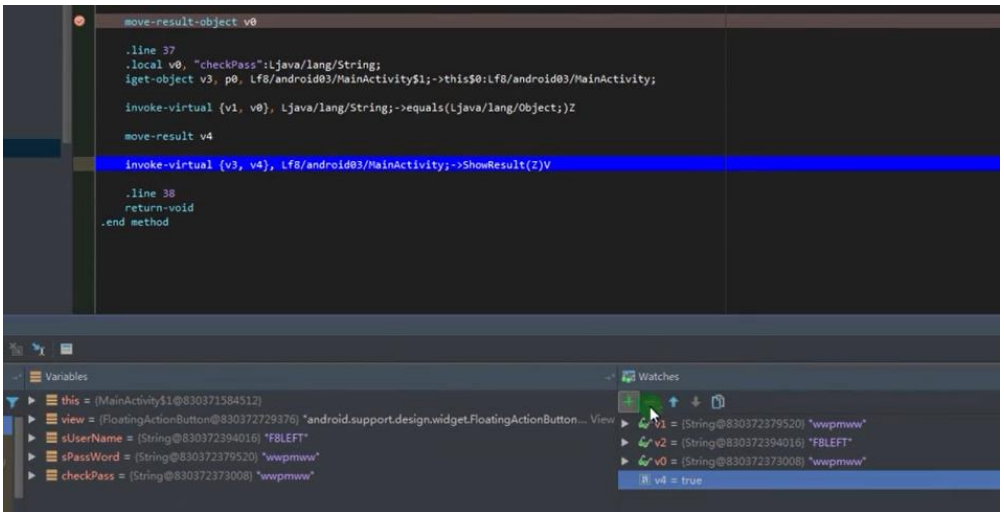
(5)下定断点，开始 Debug 操作

(6)对关注的寄存器添加 watch

Ps:需要在 monitor 中打开 8700 端口



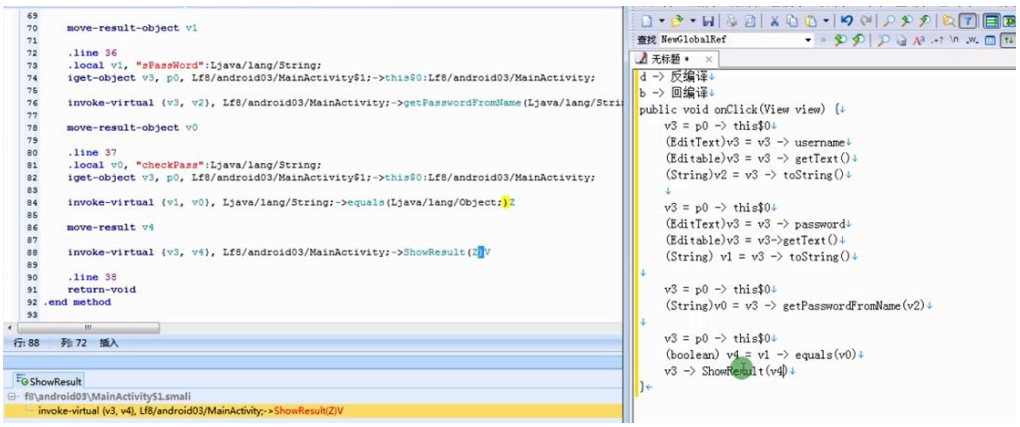
动态调试得到注册码信息



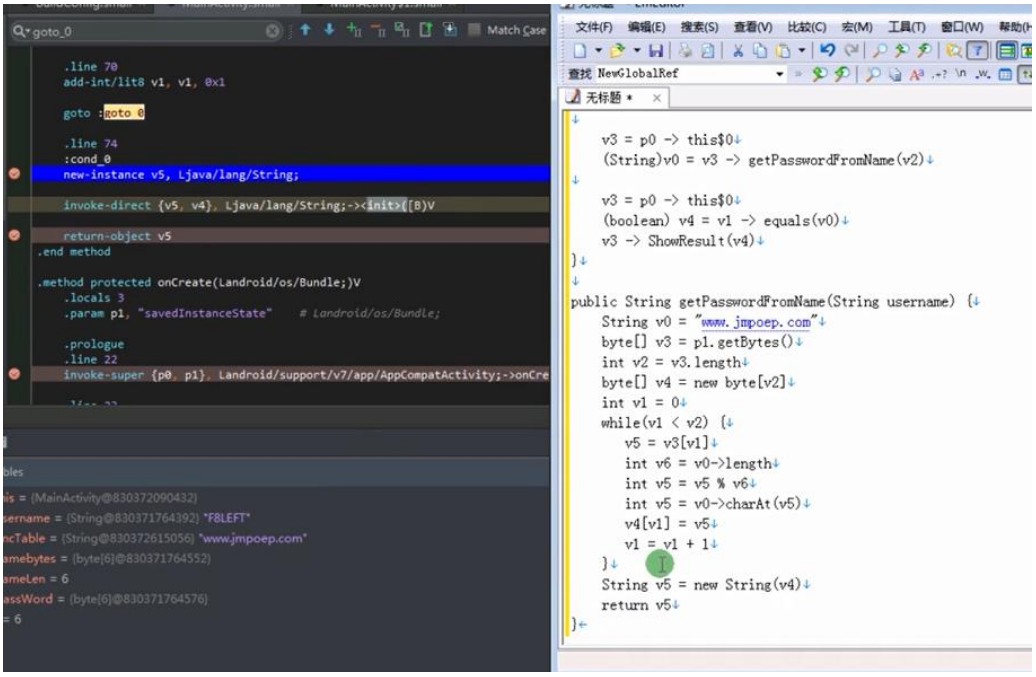
动态调试验证注册码，check 信息为 true

Java type	Type descriptor
boolean	Z
char	C
byte	B
short	S
int	I
float	F
long	J
double	D
Object	Ljava/lang/Object;
int[]	[I
Object[][]	[[Ljava/lang/Object;

Smali 代码与 Java 代码格式对照



静态分析 onClick 函数中的操作



静态分析出 getPasswordFromName 函数

3. Smali 函数以及调用

   使用 p-v 寄存器

   .method 访问修饰符 函数名 函数签名

   .locals n　#使用 n 个寄存器，即 v0~v(n-1)

   .param p1, “savedInstanceState” #Landroid/os/Bundle; #注释

   …　#函数实现

   Return-xxx　#返回

   .end method

   调用

   Invoke {参数}, 方法名

   参数都是通过寄存器传递的(Pn, Vn)

4. Smali 文件修改

   (1)跳转修改；(2)添加 log；(3)手动调用类中的方法