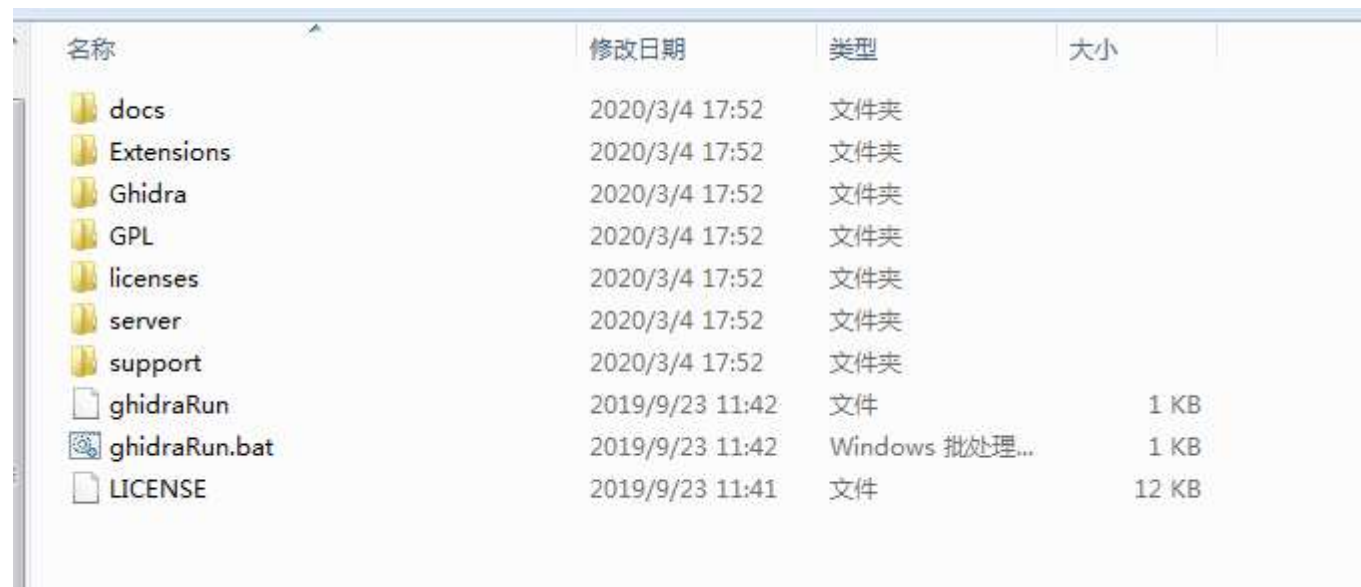


1 下载 Ghidra

从地址 <https://github.com/NationalSecurityAgency/ghidra/releases> 下载

目前我下载了 ghidra_9.1-BETA_DEV 版本，解压如下图所示

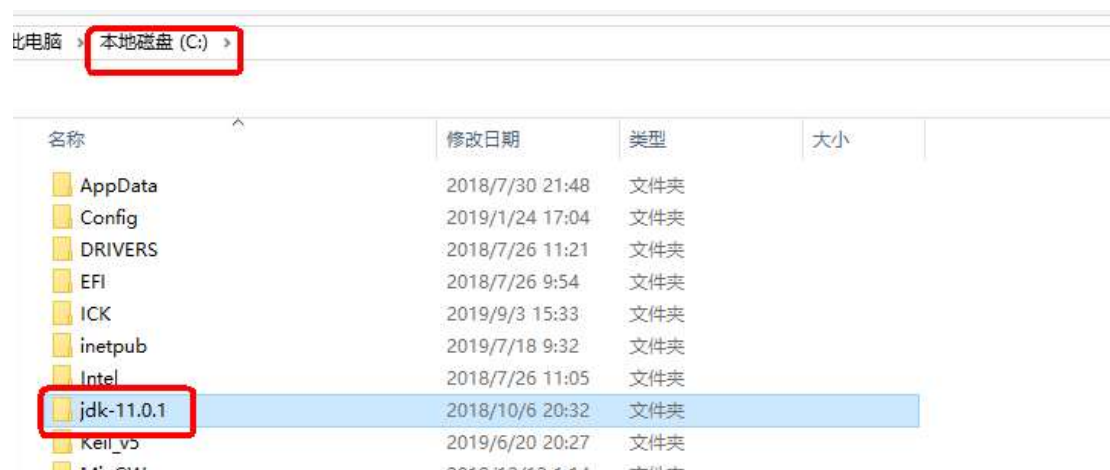


名称	修改日期	类型	大小
docs	2020/3/4 17:52	文件夹	
Extensions	2020/3/4 17:52	文件夹	
Ghidra	2020/3/4 17:52	文件夹	
GPL	2020/3/4 17:52	文件夹	
licenses	2020/3/4 17:52	文件夹	
server	2020/3/4 17:52	文件夹	
support	2020/3/4 17:52	文件夹	
ghidraRun	2019/9/23 11:42	文件	1 KB
ghidraRun.bat	2019/9/23 11:42	Windows 批处理...	1 KB
LICENSE	2019/9/23 11:41	文件	12 KB

2 安装 java 环境

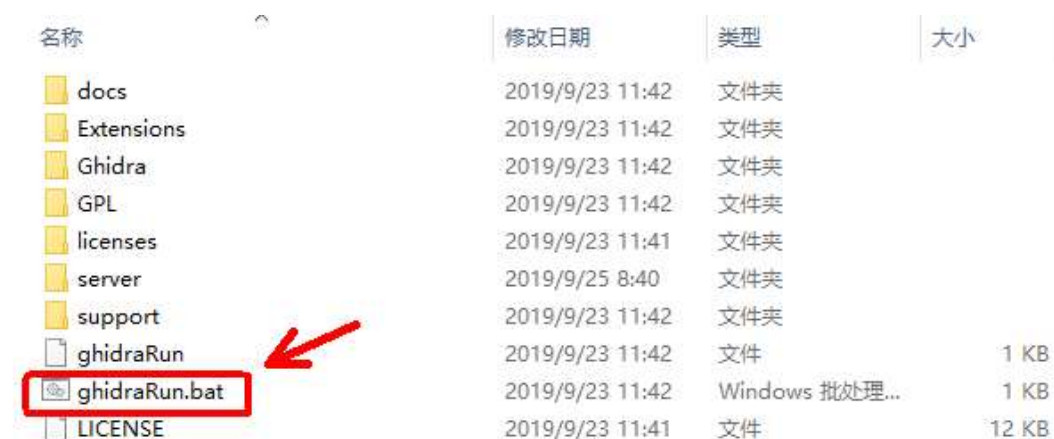
目前我下载了 jdk-11.0.1_windows-x64_bin.zip 这个版本，直接解压到 C 盘即

可，如下图所示

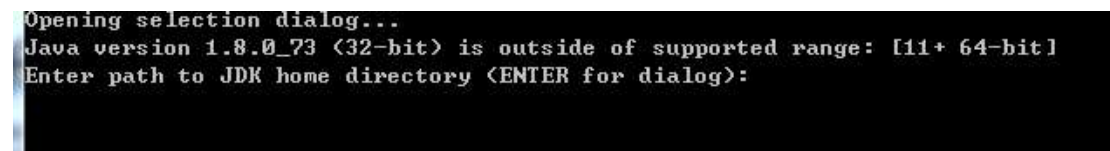


3 运行 Ghidra

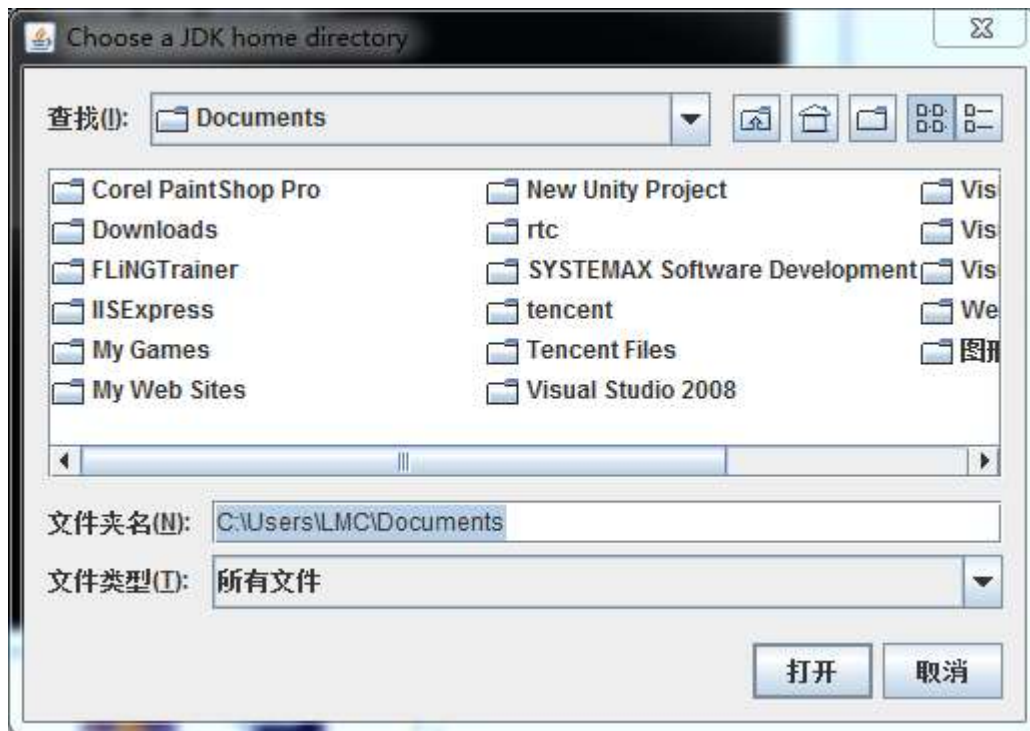
点击下图 ghidraRun.bat , 即可以运行



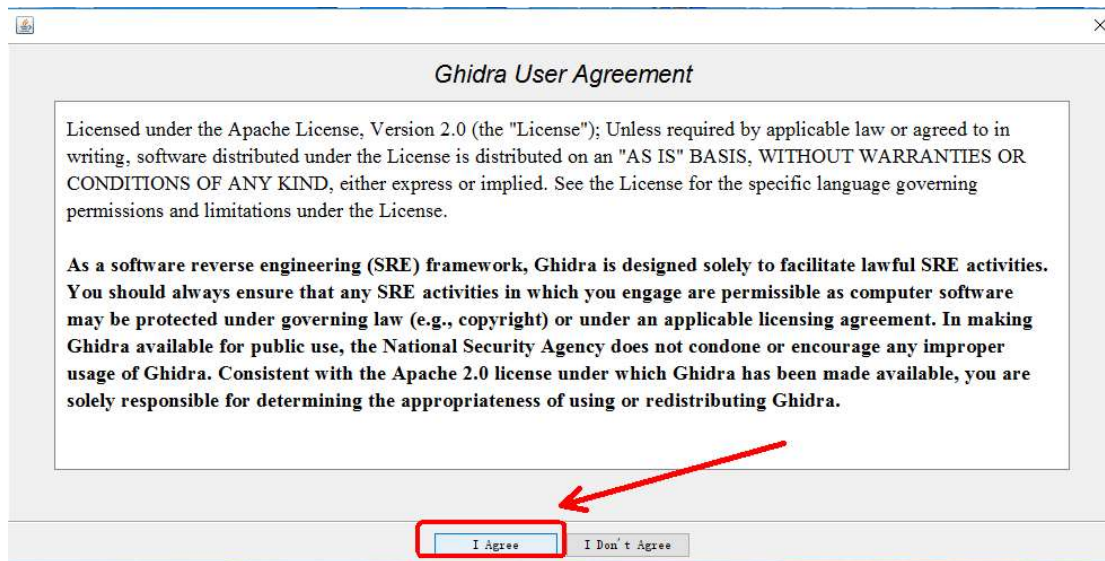
会弹出下图，提示输入回车键

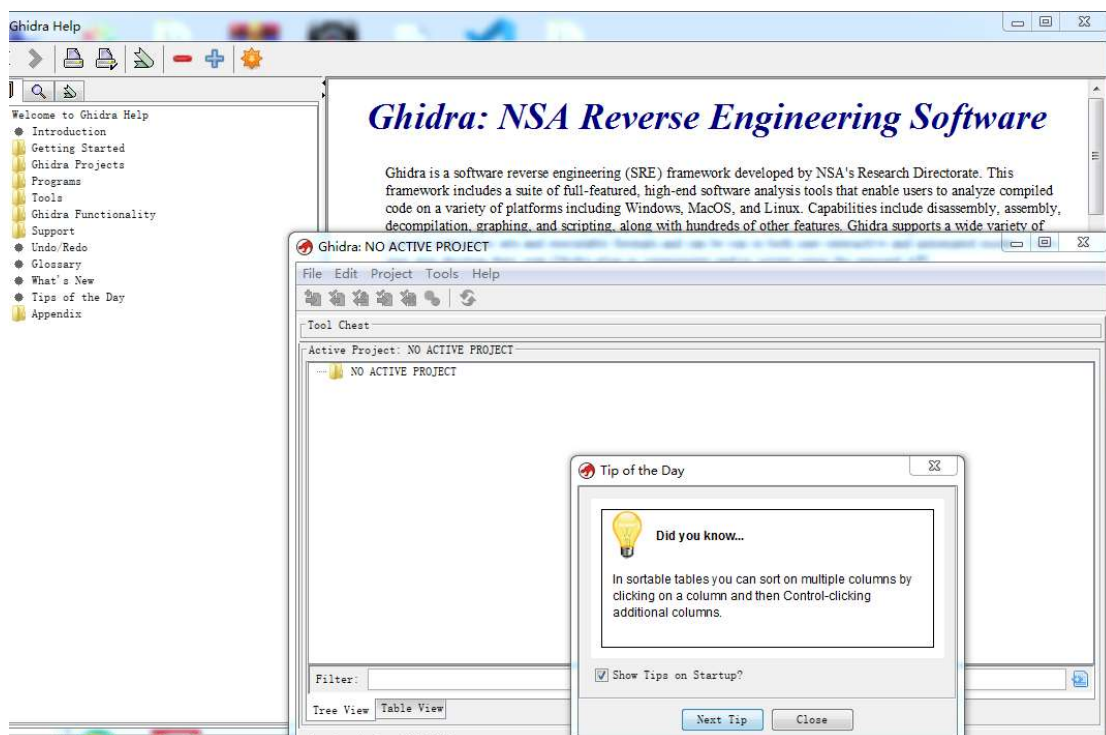


按了回车键后，会弹出下图所示，然后选择 java 的环境，即 C:\jdk-11.0.1，点击打开



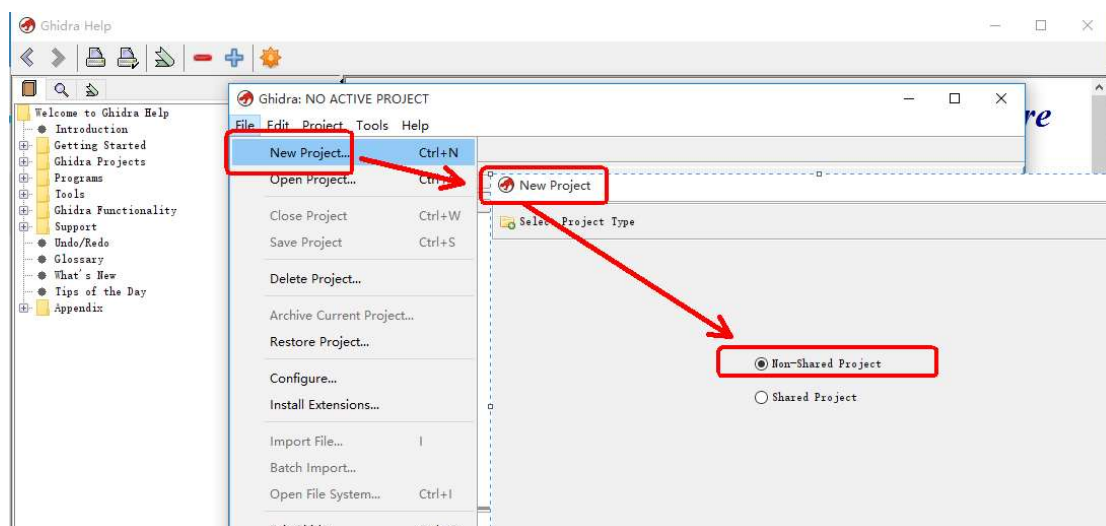
然后，点击“同意”



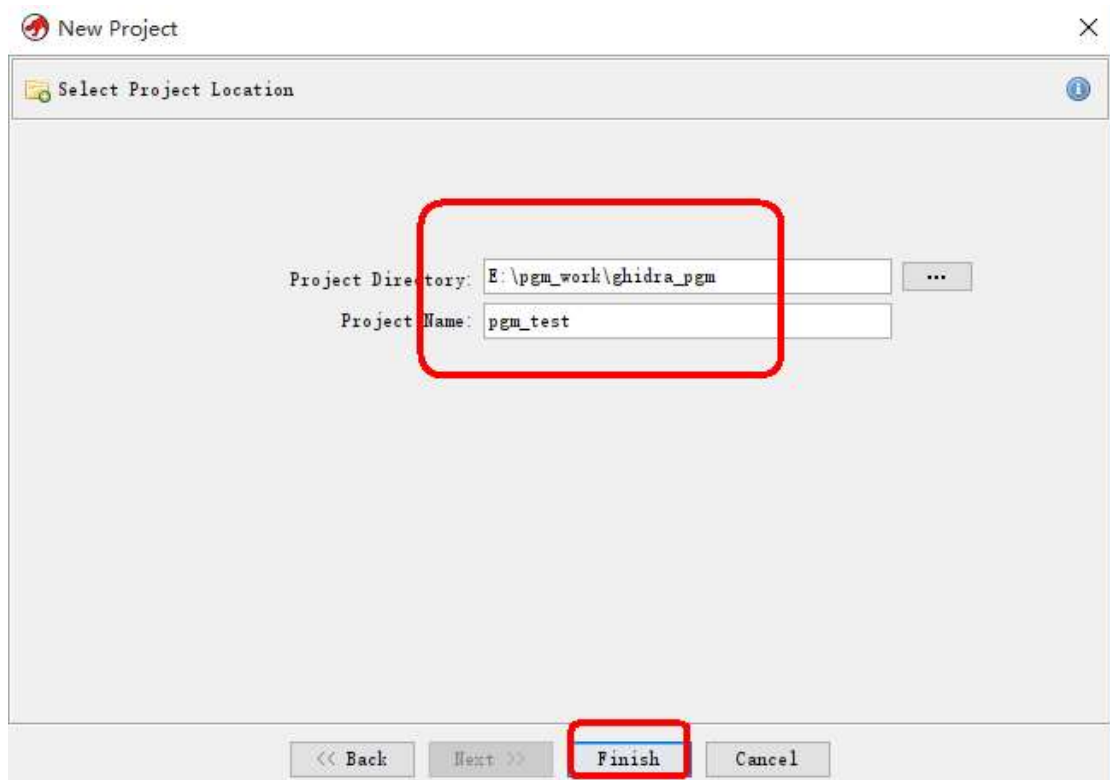


4 Ghidra 加载游戏 ROM

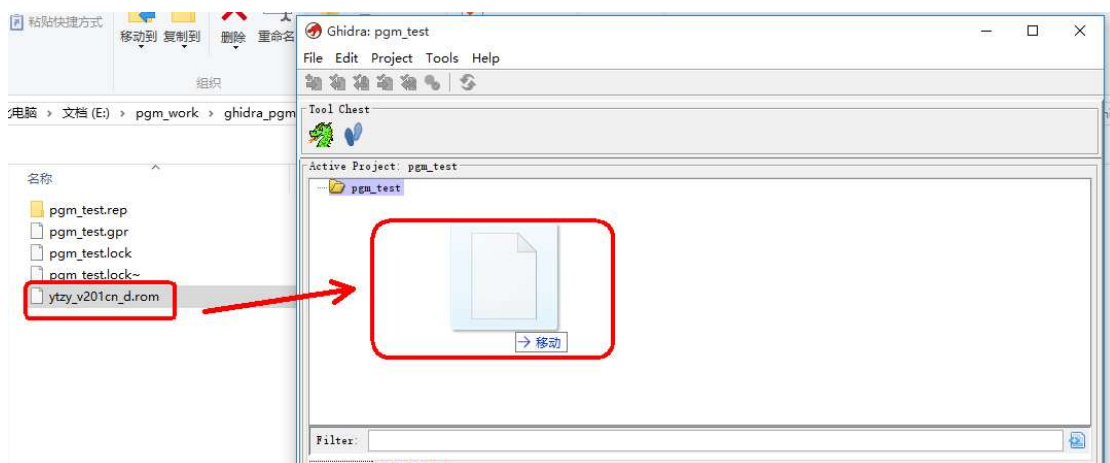
按照下图所示，新建工程



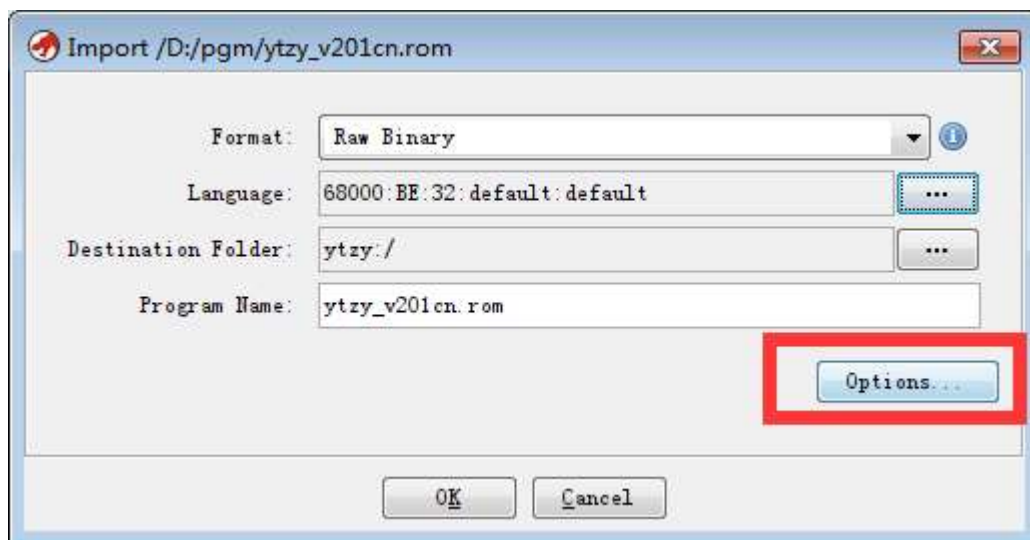
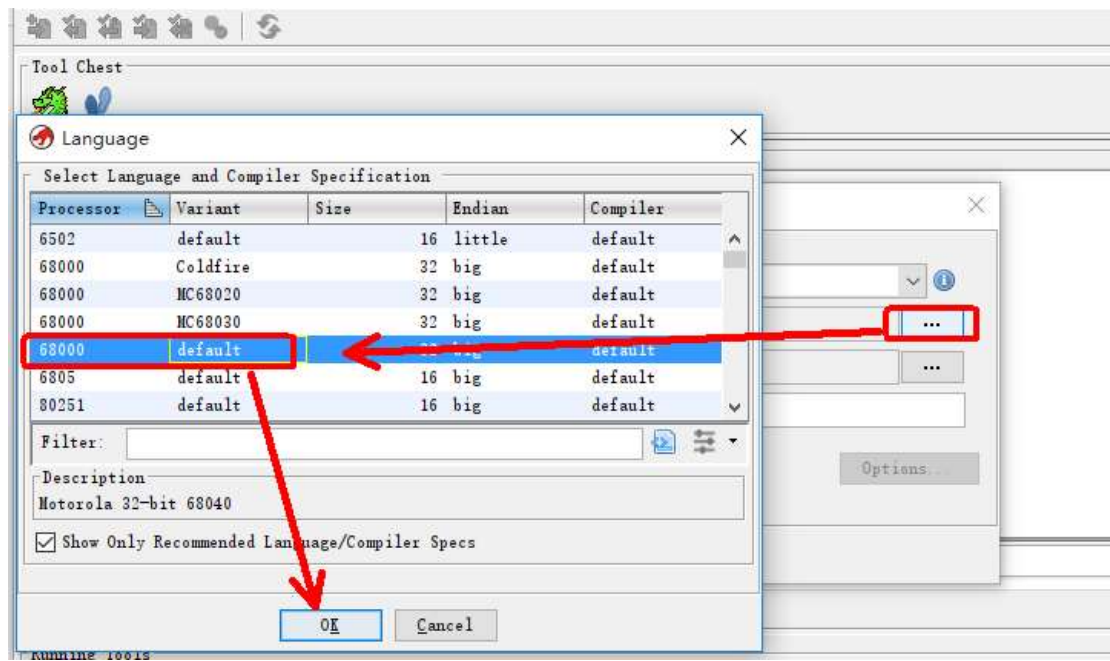
选择好工程目录（自己找一下目录）



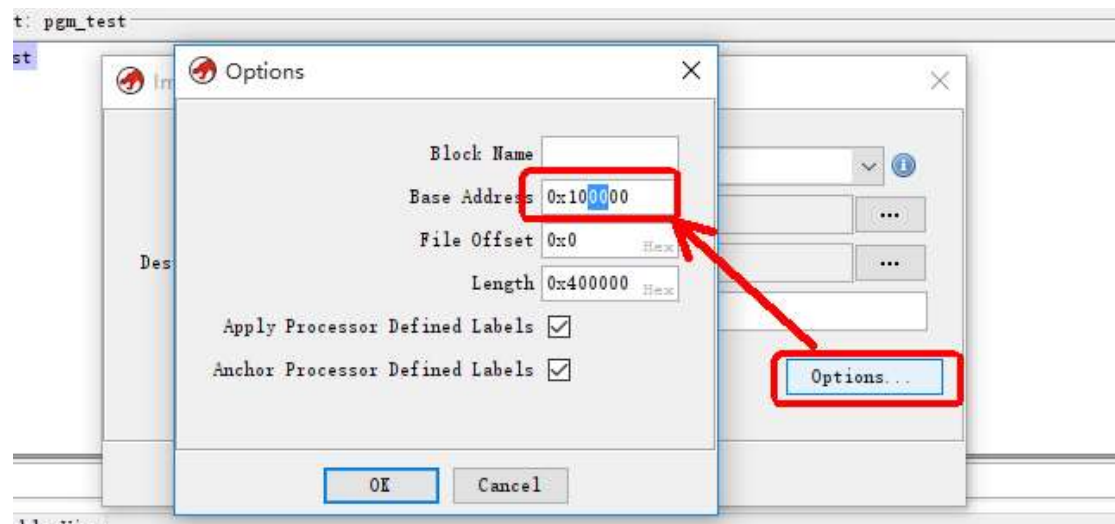
工程建好了，然后把游戏文件 `ytzy_v201cn_d.rom`，拖到工程里，如下图所示



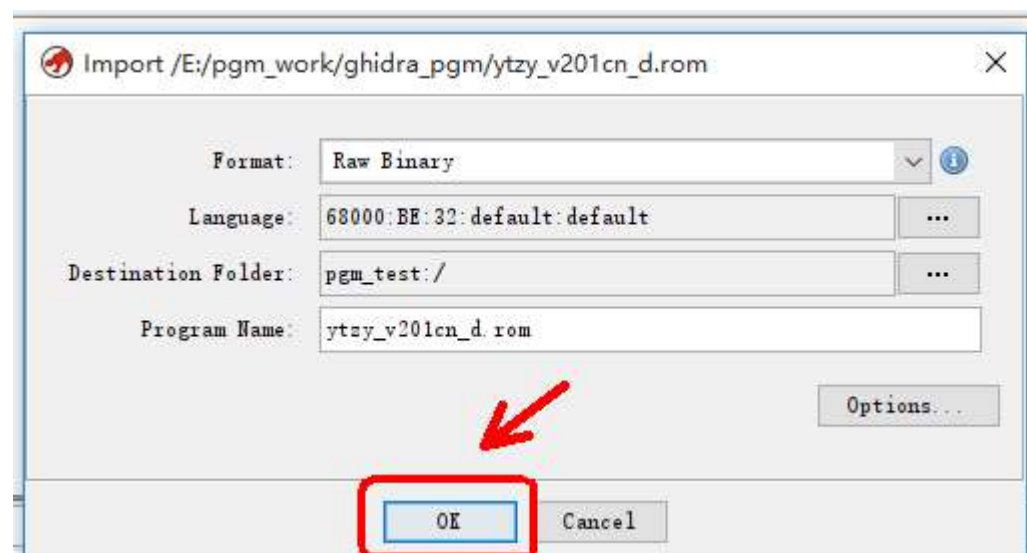
接着，选择 CPU 的型号，如下图所示



接着选择基地址 0x100000，如下图所示

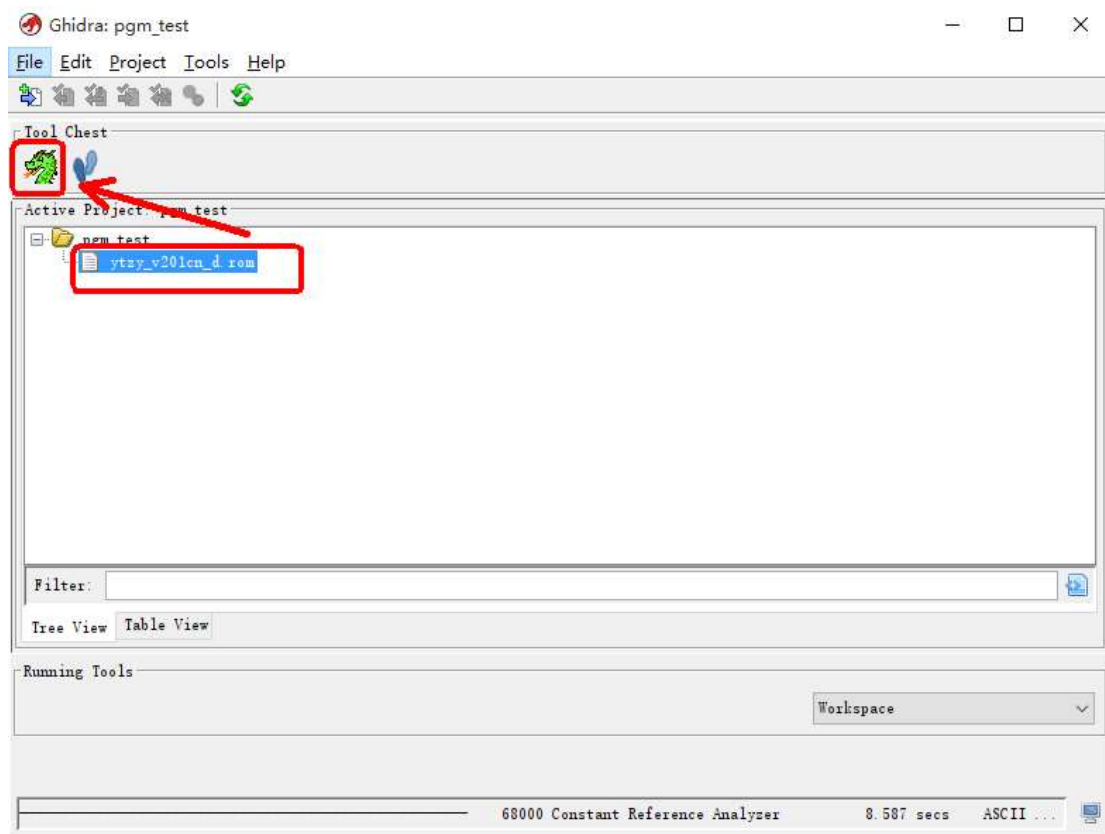


最后，点击 OK，即配置完成。

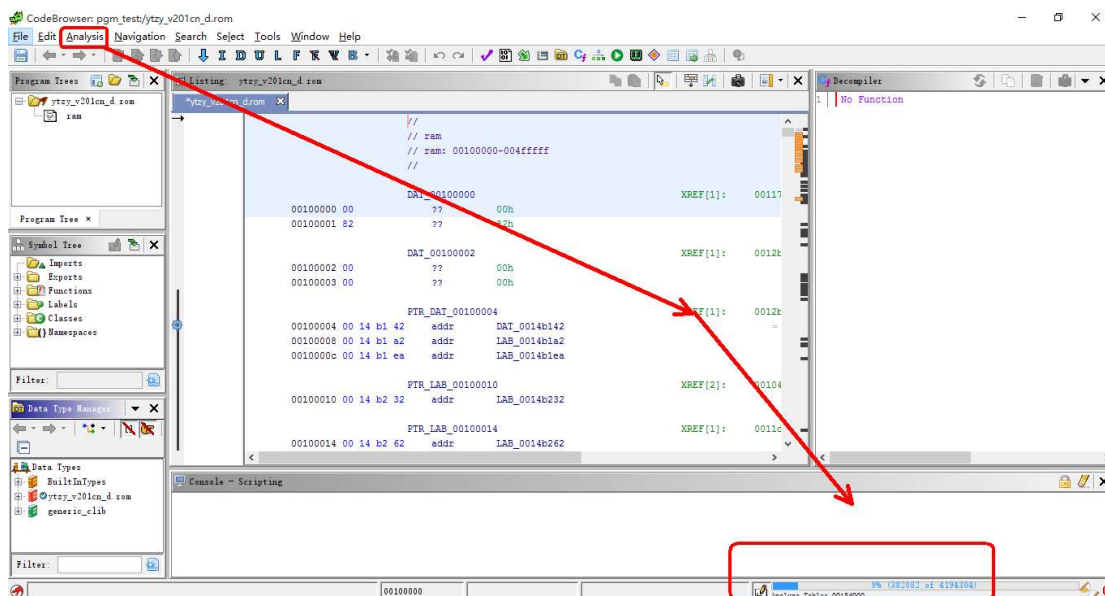


5 Ghidra 反汇编代码

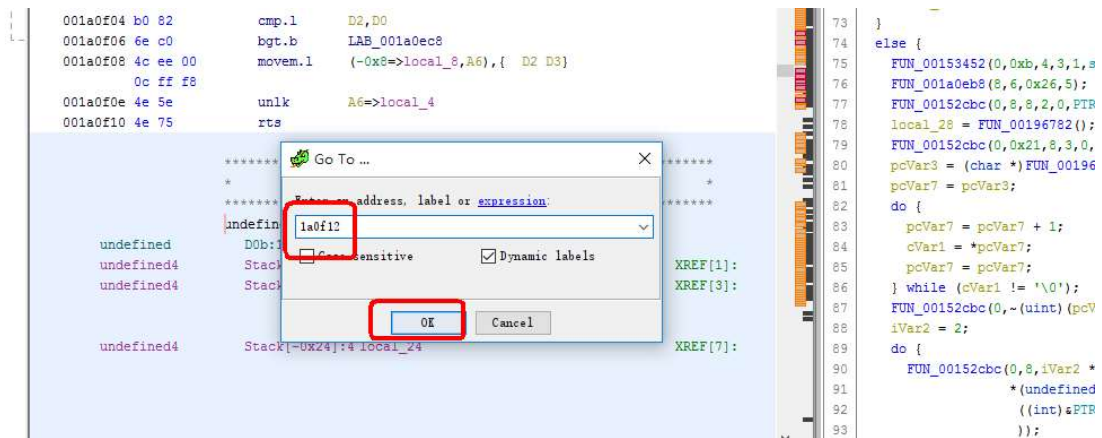
如下图所示，点击那个图片，就可以进入反汇编界面。



下图就是自动分析汇编，编译 C 代码。



按 G 键，跳到地址 0x1a0f12，去修改 warring 的字样。



心林, 2020-03-10