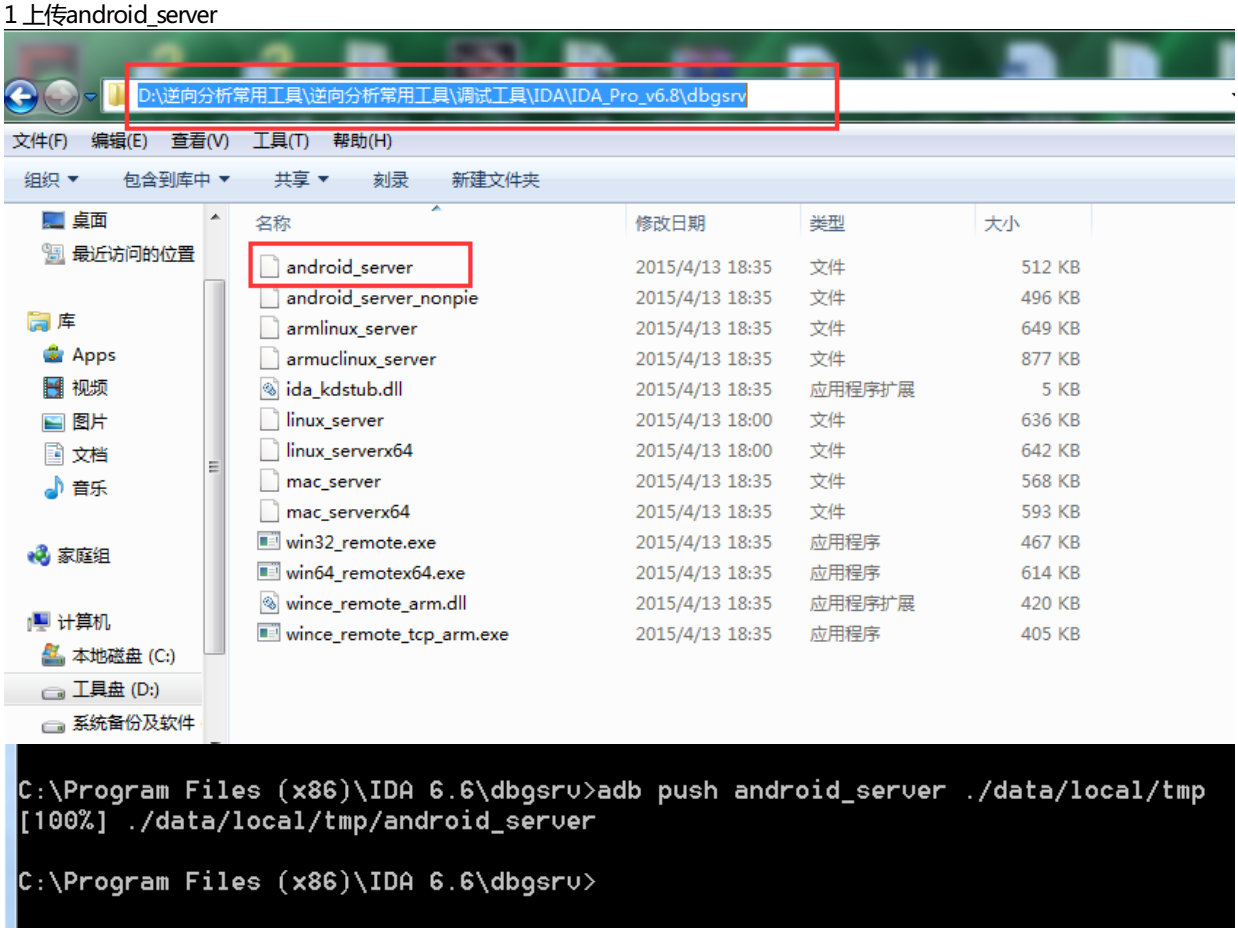
建立IDA调试so文件：一般性步骤

1 上传android_server



//shell进去，su 提下权限，到你上传android_server的地方，更改执行权限，可执行

```
root@ja3g:/data/local/tmp # chmod 777 and
android.support.graphics.drawable
android.support.graphics.drawable-build-id.txt
android_server
root@ja3g:/data/local/tmp # chmod 777 android_server
root@ja3g:/data/local/tmp # ls -l
-rw-r--r-- shell    shell        3166 2016-06-29 09:53 android.support.graphics
-rw-r--r-- shell    shell           0 2016-06-29 09:53 android.support.graphics
-rwxrwxrwx shell    shell      570904 2014-06-04 20:43 android_server
-rw-r--r-- shell    shell     1254463 2016-06-29 14:40 com.example.laiwenjie.he
-rw-r--r-- shell    shell           0 2016-06-29 14:40 com.example.laiwenjie.he
-rw-r--r-- shell    shell     1515048 2016-06-06 16:26 com.example.laiwenjie.my
drwxrwxrwx shell    shell             2016-06-17 15:24 dalvik-cache
-rw-r--r-- shell    shell    15296508 2016-06-28 22:50 lldb-server
-rw-r--r-- shell    shell        1428 2016-06-28 22:50 start_lldb_server.sh
-rw------- shell    shell       13193 2016-06-17 15:24 uidump.xml
```

//运行下android_server //之后就别管这个，千万别关了，另外打开终端

```
sh: android_server: not found
127|root@ja3g:/data/local/tmp # ./android_server
IDA Android 32-bit remote debug server(ST) v1.17. Hex-Rays (c) 2004-2014
Listening on port #23946...
```

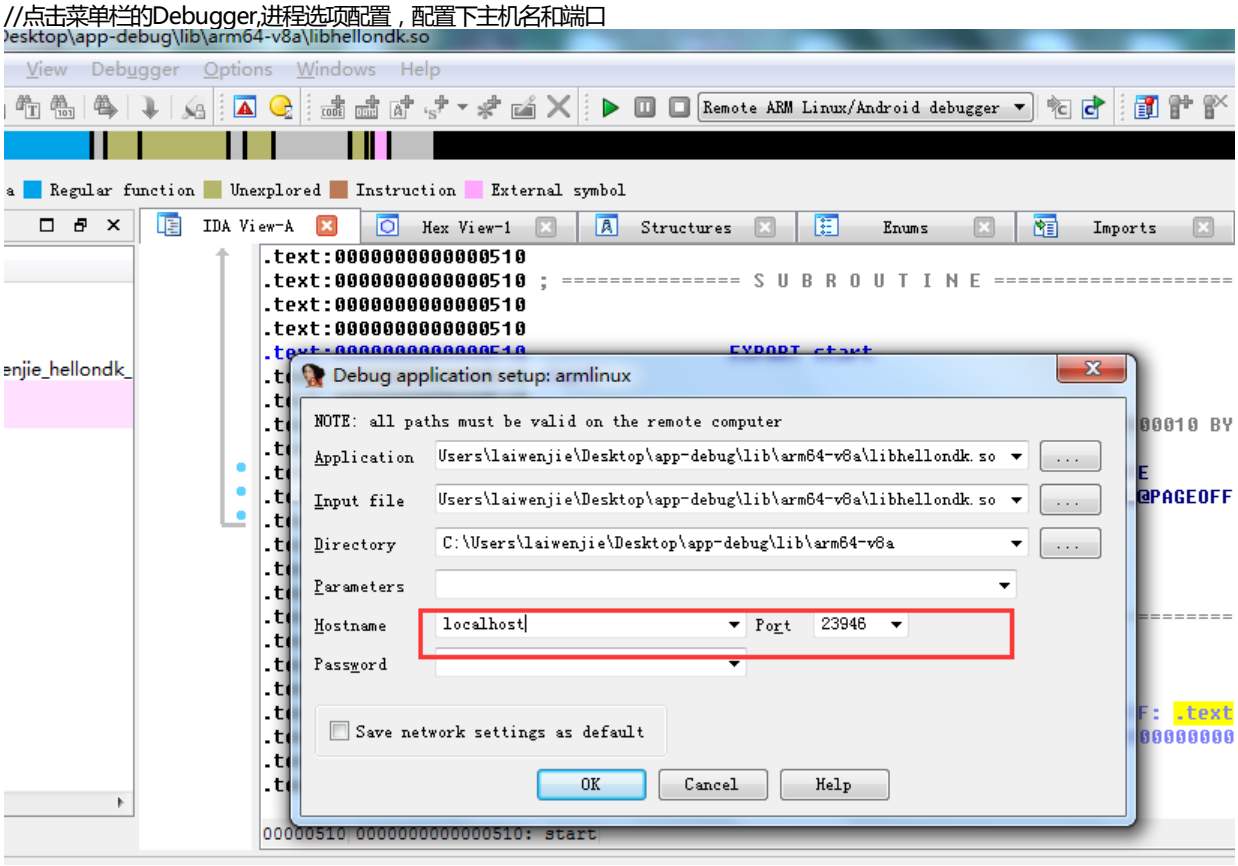
//转发下PC，这里配置的意思就是PC上的消息通过它转发给android

```
icrosoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

:\Users\laiwenjie\Desktop\app-debug\lib\arm64-v8a>adb forward tcp:23946 tcp:23946

:\Users\laiwenjie\Desktop\app-debug\lib\arm64-v8a>
```

//将你的so文件用IDA打开
//选择调试引擎，Remote ARM Linux/Android debugger
//点击菜单栏的Debugger,进程选项配置，配置下主机名和端口

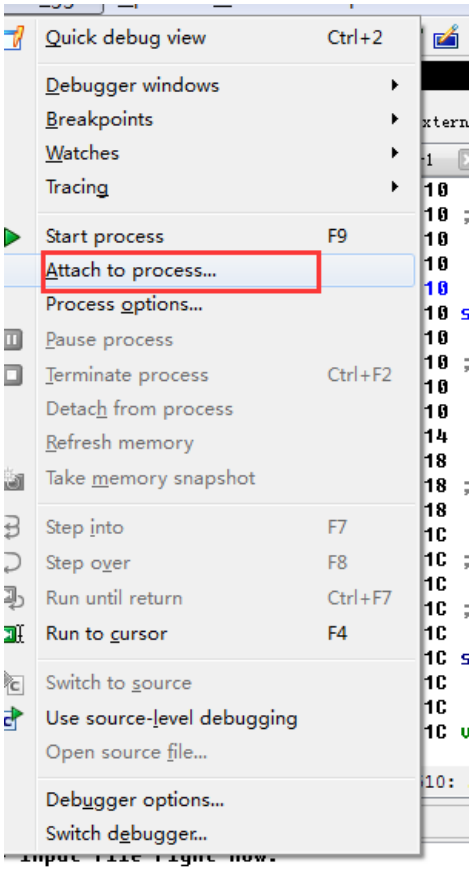


//以调试方式打开apk

```
C:\Users\laiwenjie\Desktop\app-debug\lib\arm64-v8a>adb shell am start -D -n com.example.laiwenjie.hellondk/com.example.la
llondk.MainActivity
Starting: Intent { cmp=com.example.laiwenjie.hellondk/.MainActivity }

C:\Users\laiwenjie\Desktop\app-debug\lib\arm64-v8a>_
```

//附加进程//选择你的进程



//在这之前，先下个断点（F2）
//启动下应用层jdb（看图）