1. **Section 段处理**

   鉴于 shdr 没有被 linker 用于加载，故可以对 Section 段写入无用数据，可以阻碍静态分析软件的分析。

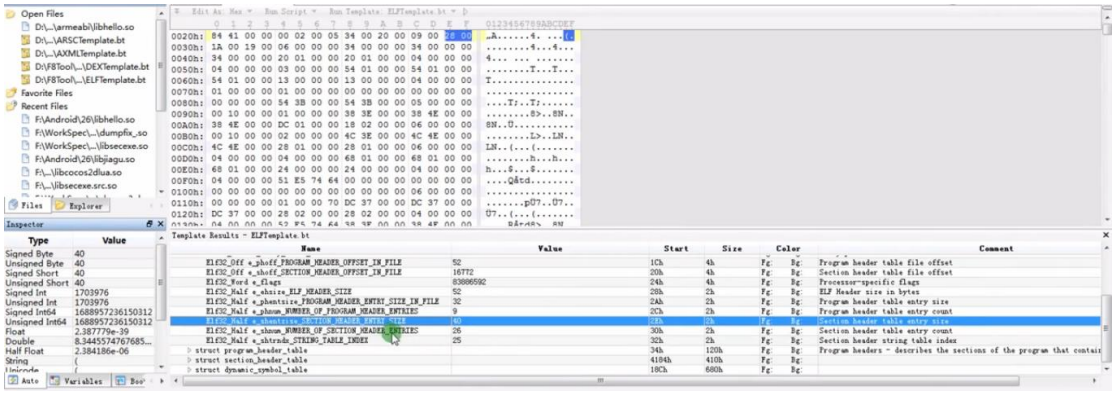
2. **Program 段处理**

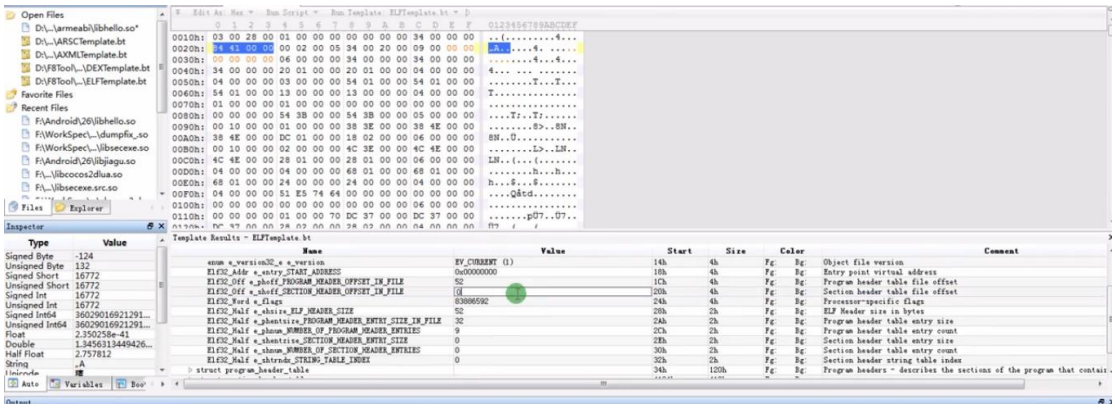
   Program 段中可以对 dynamic 区段进行混淆，添加重复和无效的数据。

3. **Demo 演示**

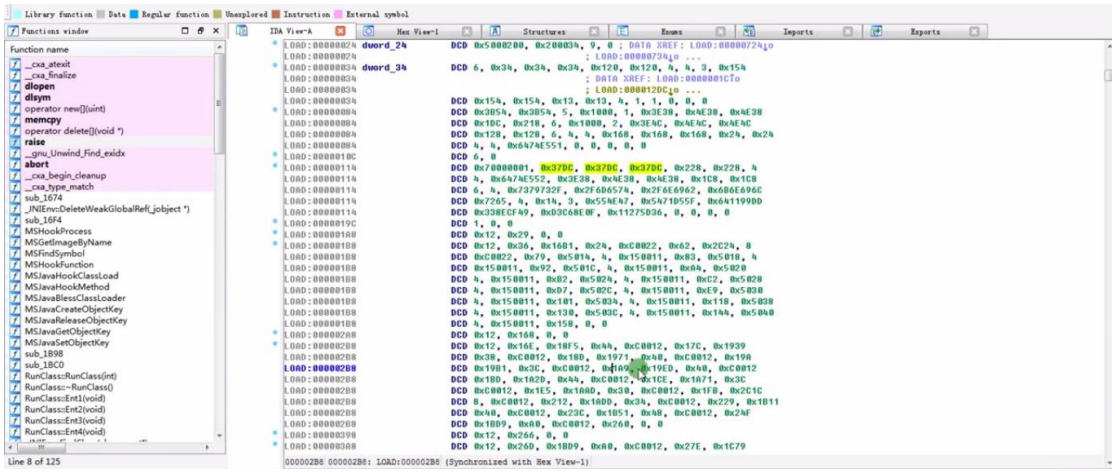
   混淆方法一：

   将 elf header 中的 section 相关参数置 0



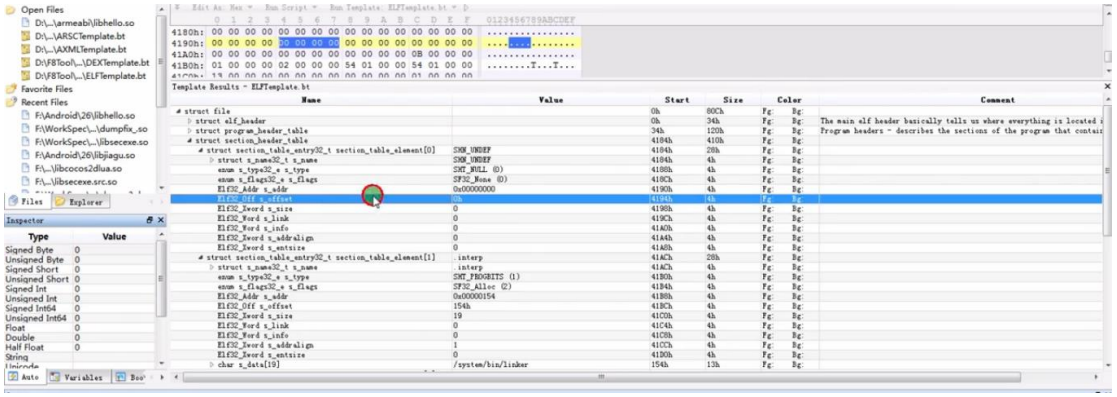


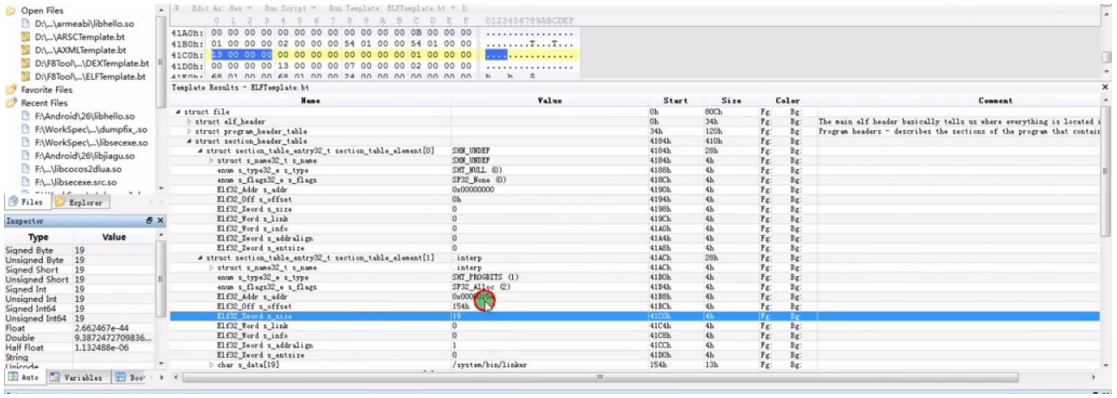
修改后 ida 的识别情况：一些函数无法正常识别

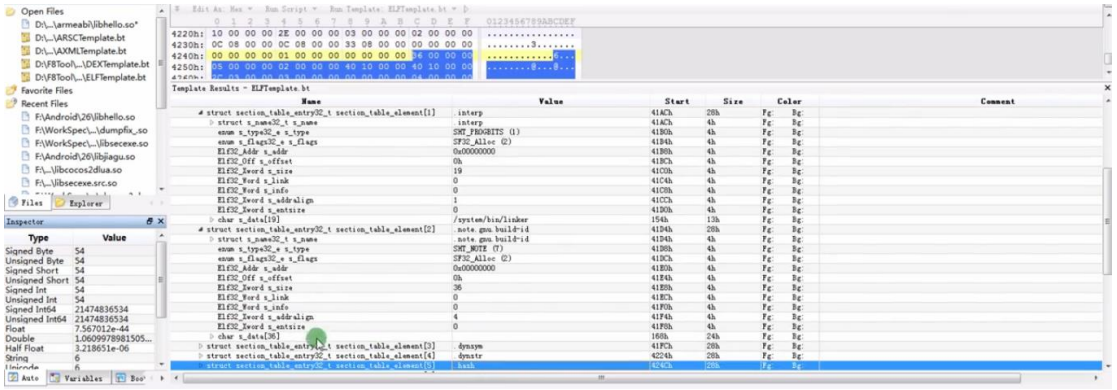


   混淆方法二：

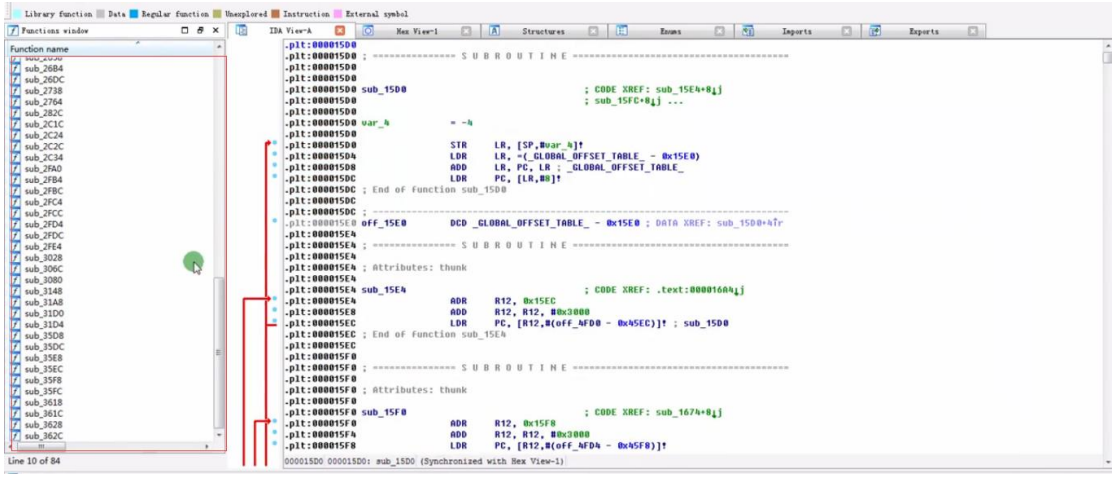
   将 section_header_table 中的 offset 和 addr 置 0



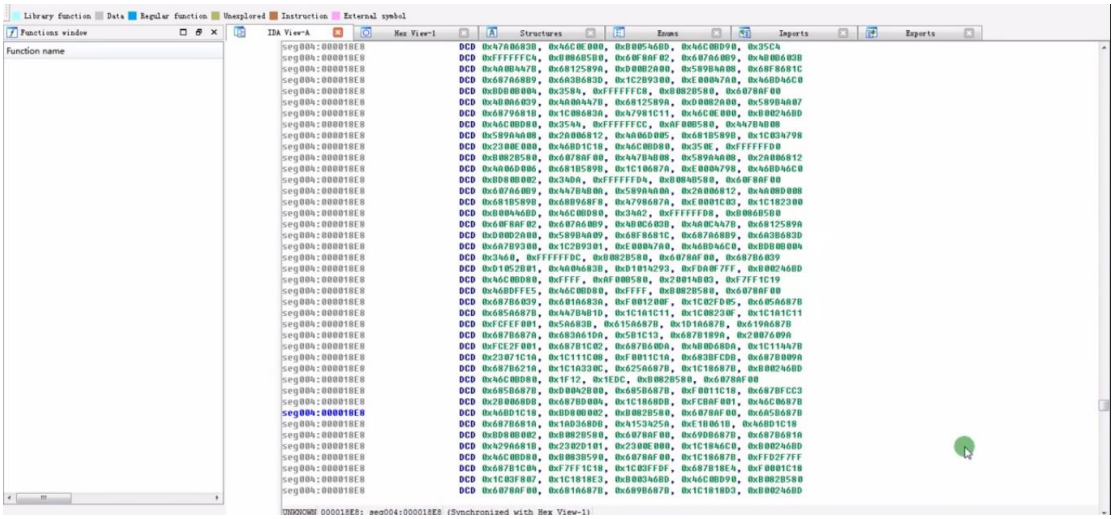




左侧函数列表很多函数没有被正常识别

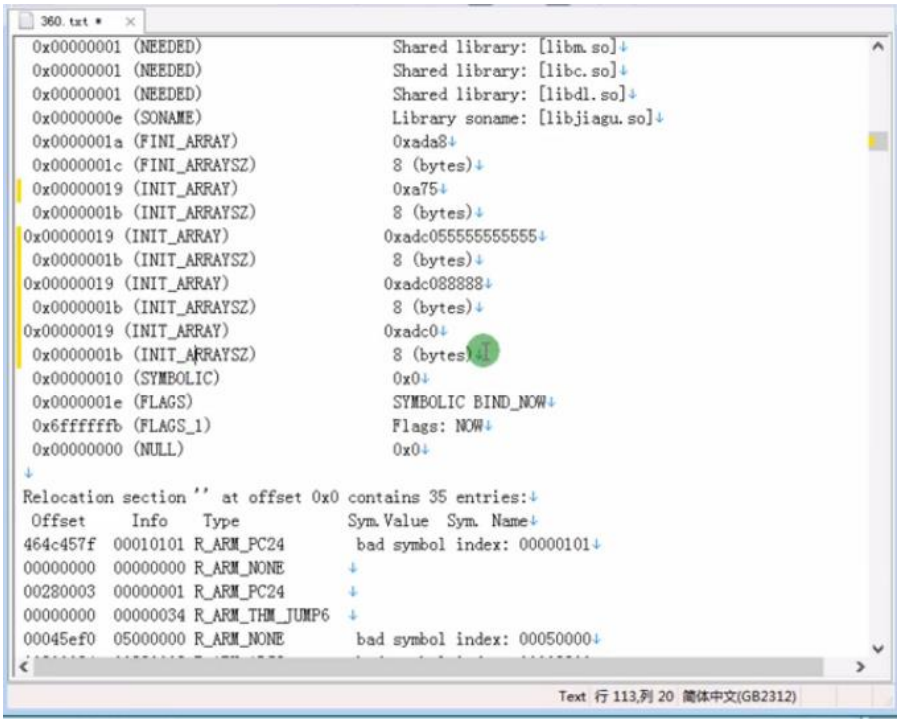


如果将所有的 addr 和 offset 都清空掉，那么左侧没有函数被识别



混淆方法三：

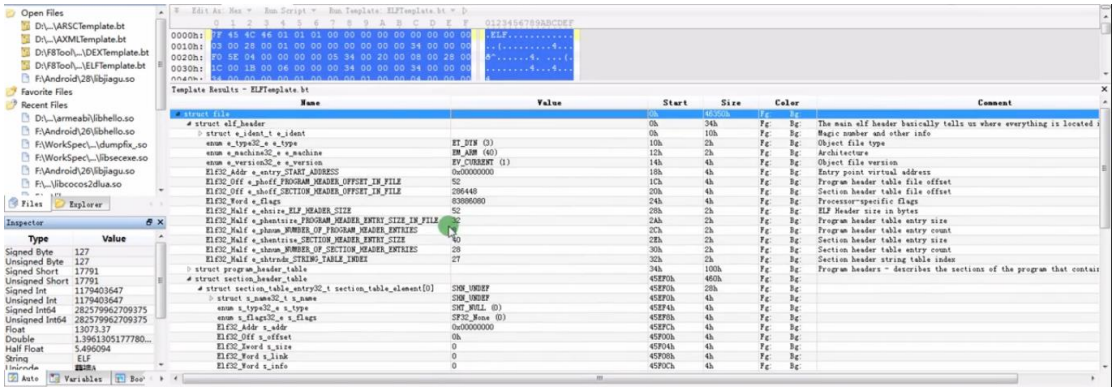
dynamic 段添加重复和无用数据，如果要还原的话只需要关注最后一段数据，删除掉之前重名的数据，因为后面的数据会覆盖掉前面的数据。

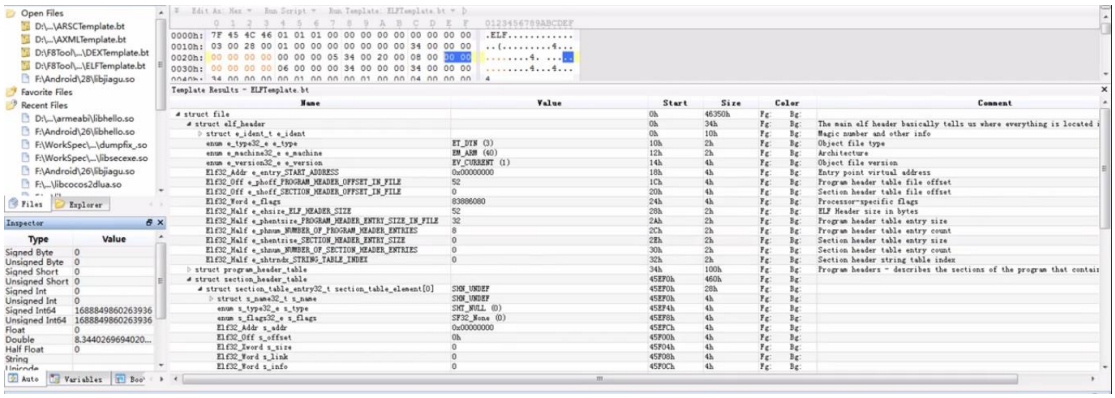


混淆还原：

方法一：手动将 start 和 end 地址重新赋值

方法二：将 section 段信息清空为 0（最简单，而且具有普适性）


Open Files
Favorite Files
Recent Files
Inspector
Type
Value
Template Results - ELFTemplate.bt
Name
Value
Start
Size
Color
Comment


Open Files
Favorite Files
Recent Files
Inspector
Type
Value
Template Results - ELFTemplate.bt
Name
Value
Start
Size
Color
Comment