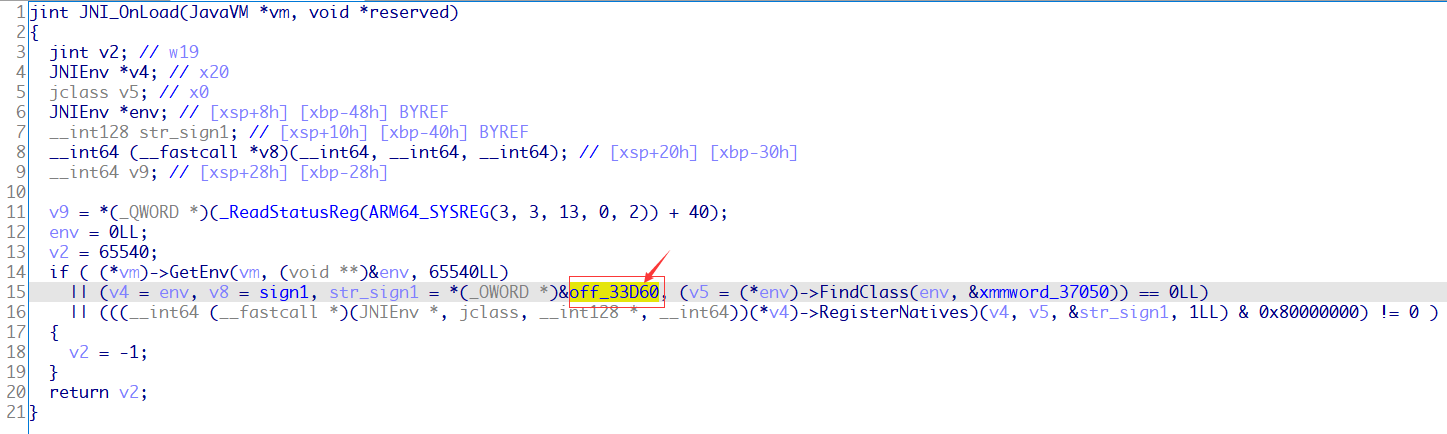
# 0X00 字符串加密

加密.data端中的数据

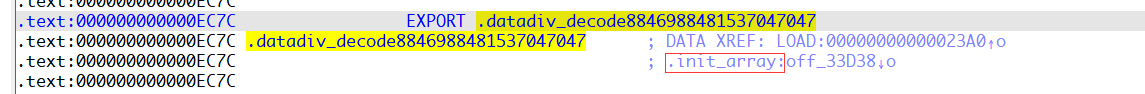
## 0x0001 JNI\_Onload

加密JNI\_Onload中的字符串



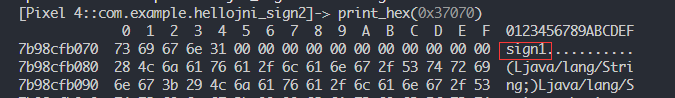
进入相应的data段，发现被.init\_array段中的函数调用





应对方法：

直接加载后用frida去hexdump相应的地址



或者像要得到jni函数的函数名，签名和相对地址可以直接hook RegisterNatives函数。

## 0x0002 data段

其实准确的来说是加密data端的数据，jni\_onload只是一起被加密了而已