目录

iOS逆向分析：恢复符号表

- 最新版本： `v0.5`
- 更新时间： `20240507`

简介

介绍关于iOS逆向期间的，恢复符号表相关的各种内容。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

HonKit源码

- crifan/ios_re_restore_symbol: iOS逆向分析：恢复符号表

如何使用此HonKit源码去生成发布为电子书

详见：crifan/honkit_template: demo how to use crifan honkit template and demo

在线浏览

- iOS逆向分析：恢复符号表 book.crifan.org
- iOS逆向分析：恢复符号表 crifan.github.io

离线下载阅读

- iOS逆向分析：恢复符号表 PDF
- iOS逆向分析：恢复符号表 ePub
- iOS逆向分析：恢复符号表 Mobi

版权和用途说明

此电子书教程的全部内容，如无特别说明，均为本人原创。其中部分内容参考自网络，均已备注了出处。如发现有侵权，请通过邮箱联系我 `admin 艾特 crifan.com` ，我会尽快删除。谢谢合作。

各种技术类教程，仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途，均与本人无关。

鸣谢

感谢我的老婆**陈雪**的包容理解和悉心照料，才使得我 `crifan` 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

其他

作者的其他电子书

本人 `crifan` 还写了其他 `150+` 本电子书教程，感兴趣可移步至：

crifan/crifan_ebook_readme: Crifan的电子书的使用说明

关于作者

关于作者更多介绍，详见：

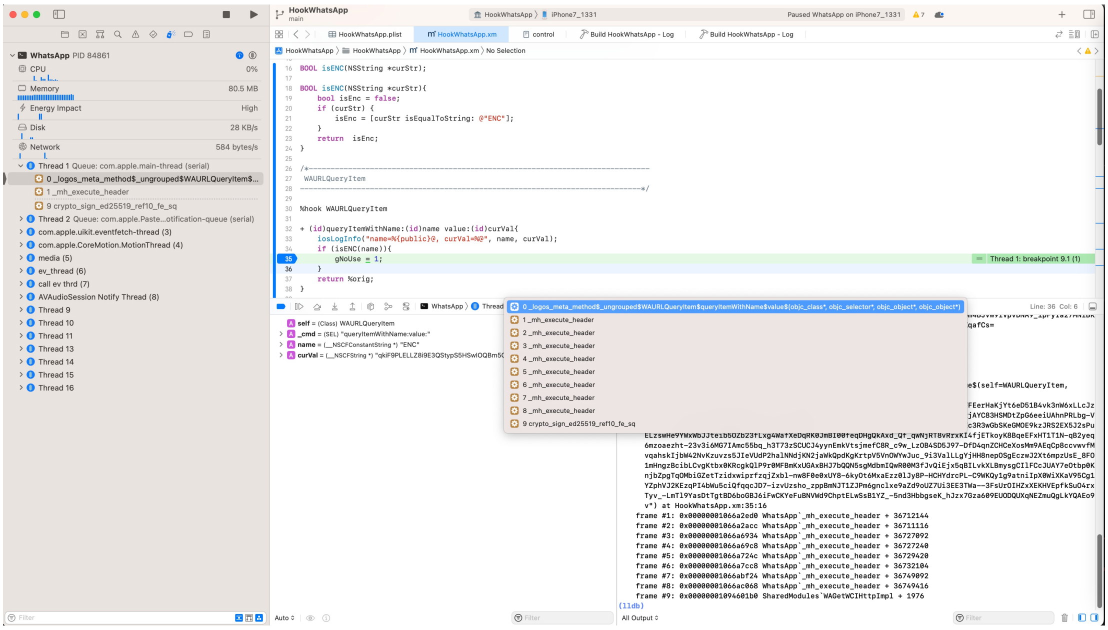
关于CrifanLi李茂 – 在路上

恢复符号表概述

什么是符号表

恢复符号表前后对比

恢复符号表之前

- 效果
  - Xcode调试iOS程序 -》 查看函数调用堆栈 -》只能看到无名函数或错误的函数名 -》 无法看到期望的（ObjC等）函数名
    - 

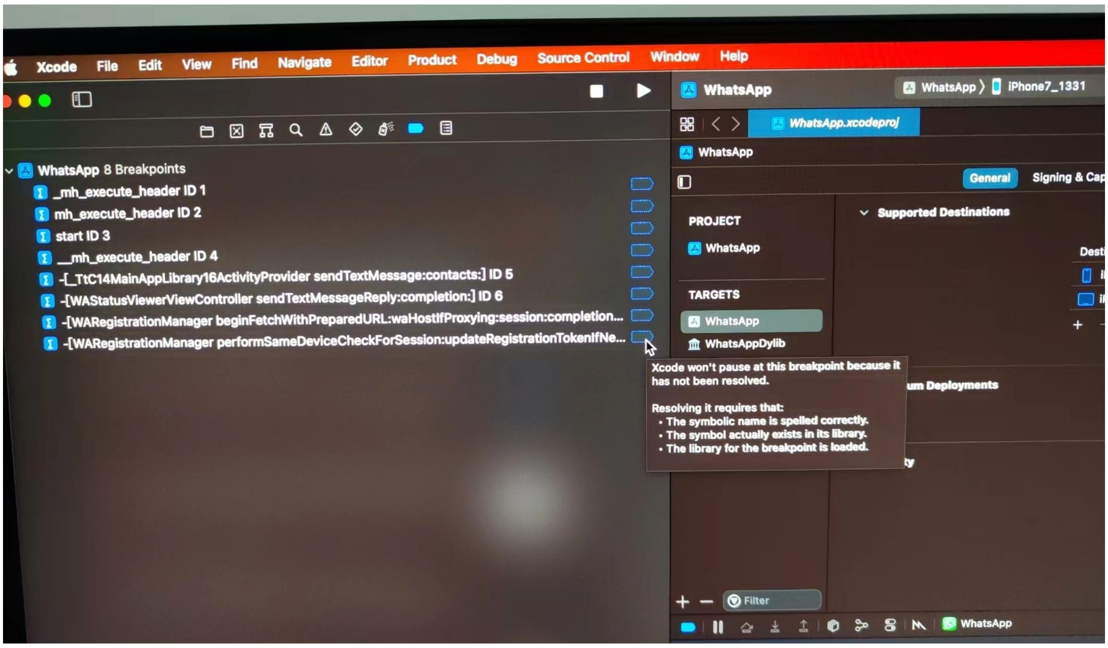
WhatsApp PID 84861
CPU 0%
Memory 80.5 MB
Energy Impact High
Disk 28 KB/s
Network 584 bytes/s
Thread 1 Queue: com.apple.main-thread (serial)
0 _logos_meta_method$_ungrouped$WAURLQueryItem$...
1 _mh_execute_header
9 crypto_sign_ed25519_ref10_fe_sq
Thread 2 Queue: com.apple.Paste...otification-queue (serial)
com.apple.uikit.eventfetch-thread (3)
com.apple.CoreMotion.MotionThread (4)
media (5)
ev_thread (6)
call ev thrd (7)
AVAudioSession Notify Thread (8)
Thread 9
Thread 10
Thread 11
Thread 13
Thread 14
Thread 15
Thread 16
HookWhatsApp
main
HookWhatsApp 〉 iPhone7_1331
Paused WhatsApp on iPhone7_1331
HookWhatsApp.plist
HookWhatsApp.xm
control
Build HookWhatsApp - Log
HookWhatsApp 〉 HookWhatsApp 〉 HookWhatsApp.xm 〉 No Selection
Thread 1: breakpoint 9.1 (1)
WhatsApp 〉 Thread
Line: 36 Col: 6
All Output
Filter

```
BOOL isENC(NSString *curStr);

BOOL isENC(NSString *curStr){
    bool isEnc = false;
    if (curStr) {
        isEnc = [curStr isEqualToString: @"ENC"];
    }
    return  isEnc;
}

/*----------------------------------------------------------------------
 WAURLQueryItem
----------------------------------------------------------------------*/

%hook WAURLQueryItem

+ (id)queryItemWithName:(id)name value:(id)curVal{
    iosLogInfo("name=%{public}@, curVal=%@", name, curVal);
    if (isENC(name)){
        gNoUse = 1;
    }
    return %orig;
}
```

```
self = (Class) WAURLQueryItem
_cmd = (SEL) "queryItemWithName:value:"
name = (__NSCFConstantString *) "ENC"
curVal = (__NSCFString *) "qkiF9PLELLZ8i9E3QStypS5HSwlOQBm5C
```

```
0 _logos_meta_method$_ungrouped$WAURLQueryItem$queryItemWithName$value$(objc_class*, objc_selector*, objc_object*, objc_object*)
1 _mh_execute_header
2 _mh_execute_header
3 _mh_execute_header
4 _mh_execute_header
5 _mh_execute_header
6 _mh_execute_header
7 _mh_execute_header
8 _mh_execute_header
9 crypto_sign_ed25519_ref10_fe_sq
```

```
qafCs=
e$(self=WAURLQueryItem,
FEerHaKjYt6eD51B4vk3nW6xLLcJz
jAYC83HSMDtZpG6eeiUAhnPRLbg-V
c3R3wGbSKeGMOE9kzJRS2EX5J2sPu
    ELzswHe9YWxWbJJteib5OZb23fLxg4WafXeDqRK0JmBI00feqDHgQkAxd_Qf_qwNjRT8vRrxKI4fjETkoyK8BqeEFxHT1T1N-qB2yeq
    6mzoaezht-23v3i6MG7IAmc55bq_h3T73zSCUCJ4yynEmkVtsjmefC8R_c9w_LzOB4SD5J97-DfD4qnZCHCeXosMm9AEqCp8ccvwvfM
    vqahskIjbW42NvKzuvzs5JIeVUdP2halNNdjKN2jaWkQpdKgKrtpV5VnOWYwJuc_9i3ValLLgYjHH8nepOSgEczwJ2Xt6mpzUsE_8FO
    1mHngzBcibLCvgKtbx0KRcgkQlP9r0MFBmKxUGAxBHJ7bQQN5sgMdbmIQwR00M3fJvQiEjx5qBILvkXLBmysgCIlFCcJUAY7eOtbp0K
    njbZpgTqOMbiGZetTzidxwiprfzqjZxbl-nw8F0e0xUY8-6kyOt6MxaEzz0lJy8P-HCHYdrcPL-C9WKQy1g9atniIpX0WiXKaV95Cg1
    YZphVJ2KEzqPI4bWu5ciQfqqcJD7-izvUzsho_zppBmNJT1ZJPm6gnclxe9aZd9oUZ7Ui3EE3TWa--3FsUrOIHZxXEKHVEpfkSuO4rx
    Tyv_-LmTl9YasDtTgtBD6boGBJ6iFwCKYeFuBNVWd9ChptELwSsB1YZ_-5nd3HbbgseK_hJzx7Gza609EUODQUXqNEZmuQgLkYQAEo9
    v") at HookWhatsApp.xm:35:16
  frame #1: 0x00000001066a2ed0 WhatsApp`_mh_execute_header + 36712144
  frame #2: 0x00000001066a2acc WhatsApp`_mh_execute_header + 36711116
  frame #3: 0x00000001066a6934 WhatsApp`_mh_execute_header + 36727092
  frame #4: 0x00000001066a69c8 WhatsApp`_mh_execute_header + 36727240
  frame #5: 0x00000001066a724c WhatsApp`_mh_execute_header + 36729420
  frame #6: 0x00000001066a7cc8 WhatsApp`_mh_execute_header + 36732104
  frame #7: 0x00000001066abf24 WhatsApp`_mh_execute_header + 36749092
  frame #8: 0x00000001066ac068 WhatsApp`_mh_execute_header + 36749416
  frame #9: 0x00000001094601b0 SharedModules`WAGetWCIHttpImpl + 1976
(lldb)
```

  - Xcode给iOS的ObjC函数加断点 -》 通过（ObjC的）函数名加断点，加不上
    - 

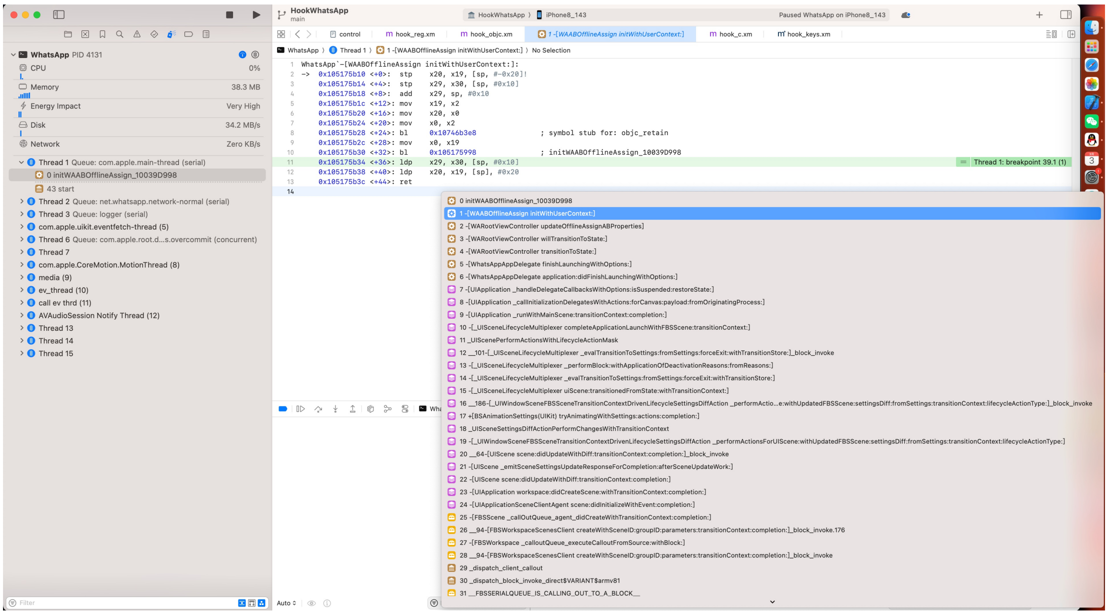
WhatsApp 8 Breakpoints
_mh_execute_header ID 1
mh_execute_header ID 2
start ID 3
__mh_execute_header ID 4
-[_TtC14MainAppLibrary16ActivityProvider sendTextMessage:contacts:] ID 5
-[WAStatusViewerViewController sendTextMessageReply:completion:] ID 6
-[WARegistrationManager beginFetchWithPreparedURL:waHostIfProxying:session:completion...
-[WARegistrationManager performSameDeviceCheckForSession:updateRegistrationTokenIfNe...

Xcode won't pause at this breakpoint because it has not been resolved.

Resolving it requires that:
• The symbolic name is spelled correctly.
• The symbol actually exists in its library.
• The library for the breakpoint is loaded.

恢复符号表之后

- 效果
  - Xcode调试iOS程序 -》 查看函数调用堆栈 -》就能看到函数名了

- 

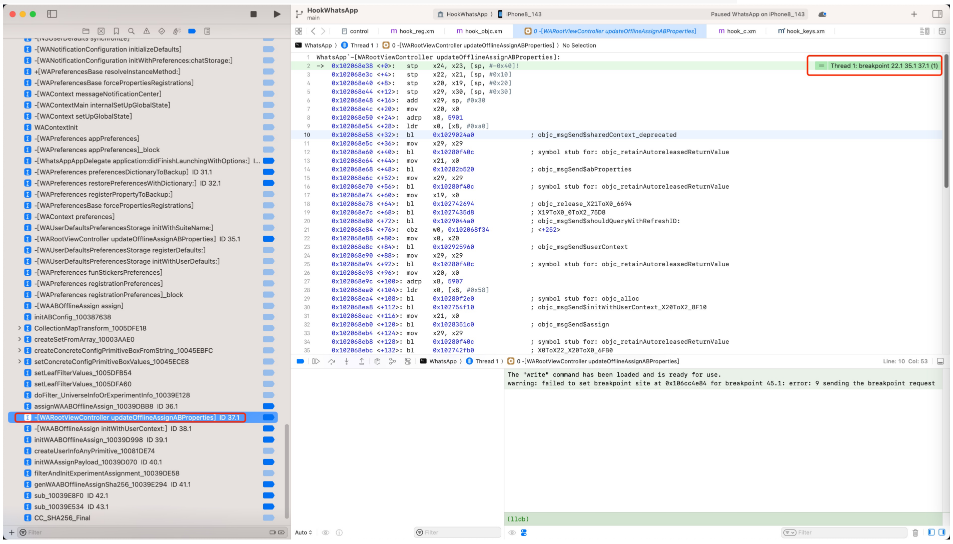
HookWhatsApp
main
HookWhatsApp 〉 iPhone8_143
Paused WhatsApp on iPhone8_143
control
hook_reg.xm
hook_objc.xm
1 -[WAABOfflineAssign initWithUserContext:]
hook_c.xm
hook_keys.xm
WhatsApp 〉 Thread 1 〉 1 -[WAABOfflineAssign initWithUserContext:] 〉 No Selection
Auto ◇
Filter

WhatsApp PID 4131
CPU 0%
Memory 38.3 MB
Energy Impact Very High
Disk 34.2 MB/s
Network Zero KB/s
Thread 1 Queue: com.apple.main-thread (serial)
0 initWAABOfflineAssign_10039D998
43 start
Thread 2 Queue: net.whatsapp.network-normal (serial)
Thread 3 Queue: logger (serial)
com.apple.uikit.eventfetch-thread (5)
Thread 6 Queue: com.apple.root.d...s.overcommit (concurrent)
Thread 7
com.apple.CoreMotion.MotionThread (8)
media (9)
ev_thread (10)
call ev thrd (11)
AVAudioSession Notify Thread (12)
Thread 13
Thread 14
Thread 15

```
WhatsApp`-[WAABOfflineAssign initWithUserContext:]:
->  0x105175b10 <+0>:  stp    x20, x19, [sp, #-0x20]!
    0x105175b14 <+4>:  stp    x29, x30, [sp, #0x10]
    0x105175b18 <+8>:  add    x29, sp, #0x10
    0x105175b1c <+12>: mov    x19, x2
    0x105175b20 <+16>: mov    x20, x0
    0x105175b24 <+20>: mov    x0, x2
    0x105175b28 <+24>: bl     0x10746b3e8               ; symbol stub for: objc_retain
    0x105175b2c <+28>: mov    x0, x19
    0x105175b30 <+32>: bl     0x105175998               ; initWAABOfflineAssign_10039D998
    0x105175b34 <+36>: ldp    x29, x30, [sp, #0x10]
    0x105175b38 <+40>: ldp    x20, x19, [sp], #0x20
    0x105175b3c <+44>: ret
```

Thread 1: breakpoint 39.1 (1)

0 initWAABOfflineAssign_10039D998
1 -[WAABOfflineAssign initWithUserContext:]
2 -[WARootViewController updateOfflineAssignABProperties]
3 -[WARootViewController willTransitionToState:]
4 -[WARootViewController transitionToState:]
5 -[WhatsAppAppDelegate finishLaunchingWithOptions:]
6 -[WhatsAppAppDelegate application:didFinishLaunchingWithOptions:]
7 -[UIApplication _handleDelegateCallbacksWithOptions:isSuspended:restoreState:]
8 -[UIApplication _callInitializationDelegatesWithActions:forCanvas:payload:fromOriginatingProcess:]
9 -[UIApplication _runWithMainScene:transitionContext:completion:]
10 -[_UISceneLifecycleMultiplexer completeApplicationLaunchWithFBSScene:transitionContext:]
11 _UIScenePerformActionsWithLifecycleActionMask
12 __101-[_UISceneLifecycleMultiplexer _evalTransitionToSettings:fromSettings:forceExit:withTransitionStore:]_block_invoke
13 -[_UISceneLifecycleMultiplexer _performBlock:withApplicationOfDeactivationReasons:fromReasons:]
14 -[_UISceneLifecycleMultiplexer _evalTransitionToSettings:fromSettings:forceExit:withTransitionStore:]
15 -[_UISceneLifecycleMultiplexer uiScene:transitionedFromState:withTransitionContext:]
16 __186-[_UIWindowSceneFBSSceneTransitionContextDrivenLifecycleSettingsDiffAction _performActio...e:withUpdatedFBSScene:settingsDiff:fromSettings:transitionContext:lifecycleActionType:]_block_invoke
17 +[BSAnimationSettings(UIKit) tryAnimatingWithSettings:actions:completion:]
18 _UISceneSettingsDiffActionPerformChangesWithTransitionContext
19 -[_UIWindowSceneFBSSceneTransitionContextDrivenLifecycleSettingsDiffAction _performActionsForUIScene:withUpdatedFBSScene:settingsDiff:fromSettings:transitionContext:lifecycleActionType:]
20 __64-[UIScene scene:didUpdateWithDiff:transitionContext:completion:]_block_invoke
21 -[UIScene _emitSceneSettingsUpdateResponseForCompletion:afterSceneUpdateWork:]
22 -[UIScene scene:didUpdateWithDiff:transitionContext:completion:]
23 -[UIApplication workspace:didCreateScene:withTransitionContext:completion:]
24 -[UIApplicationSceneClientAgent scene:didInitializeWithEvent:completion:]
25 -[FBSScene _callOutQueue_agent_didCreateWithTransitionContext:completion:]
26 __94-[FBSWorkspaceScenesClient createWithSceneID:groupID:parameters:transitionContext:completion:]_block_invoke.176
27 -[FBSWorkspace _calloutQueue_executeCalloutFromSource:withBlock:]
28 __94-[FBSWorkspaceScenesClient createWithSceneID:groupID:parameters:transitionContext:completion:]_block_invoke
29 _dispatch_client_callout
30 _dispatch_block_invoke_direct$VARIANT$armv81
31 __FBSSERIALQUEUE_IS_CALLING_OUT_TO_A_BLOCK__

- Xcode给iOS的ObjC函数加断点 -》 断点就能加上了
  - 举例
    - WhatsApp
      - `-[WARootViewController updateOfflineAssignABProperties]`
      - 

HookWhatsApp
main
HookWhatsApp 〉 iPhone8_143
Paused WhatsApp on iPhone8_143
control
hook_reg.xm
hook_objc.xm
0 -[WARootViewController updateOfflineAssignABProperties]
hook_c.xm
hook_keys.xm
WhatsApp 〉 Thread 1 〉 0 -[WARootViewController updateOfflineAssignABProperties] 〉 No Selection
Line: 10 Col: 53
Auto ◇
Filter

-[NSUserDefaults synchronize]
-[WANotificationConfiguration initializeDefaults]
-[WANotificationConfiguration initWithPreferences:chatStorage:]
+[WAPreferencesBase resolveInstanceMethod:]
-[WAPreferencesBase forcePropertiesRegistrations]
-[WAContext messageNotificationCenter]
-[WAContextMain internalSetUpGlobalState]
-[WAContext setUpGlobalState]
WAContextInit
-[WAPreferences appPreferences]
-[WAPreferences appPreferences]_block
-[WhatsAppAppDelegate application:didFinishLaunchingWithOptions:] I...
-[WAPreferences preferencesDictionaryToBackup] ID 31.1
-[WAPreferences restorePreferencesWithDictionary:] ID 32.1
-[WAPreferences registerPropertyToBackup:]
-[WAPreferencesBase forcePropertiesRegistrations]
-[WAContext preferences]
-[WAUserDefaultsPreferencesStorage initWithSuiteName:]
-[WARootViewController updateOfflineAssignABProperties] ID 35.1
-[WAUserDefaultsPreferencesStorage registerDefaults:]
-[WAUserDefaultsPreferencesStorage initWithUserDefaults:]
-[WAPreferences funStickersPreferences]
-[WAPreferences registrationPreferences]
-[WAPreferences registrationPreferences]_block
-[WAABOfflineAssign assign]
initABConfig_100387638
CollectionMapTransform_1005DFE18
createSetFromArray_10003AAE0
createConcreteConfigPrimitiveBoxFromString_10045EBFC
setConcreteConfigPrimitiveBoxValues_10045ECE8
setLeafFilterValues_1005DFB54
setLeafFilterValues_1005DFA60
doFilter_UniverseInfoOrExperimentInfo_10039E128
assignWAABOfflineAssign_10039DBB8 ID 36.1
-[WARootViewController updateOfflineAssignABProperties] ID 37.1
-[WAABOfflineAssign initWithUserContext:] ID 38.1
initWAABOfflineAssign_10039D998 ID 39.1
createUserInfoAnyPrimitive_10081DE74
initWAAssignPayload_10039D070 ID 40.1
filterAndInitExperimentAssignment_10039DE58
genWAABOfflineAssignSha256_10039E294 ID 41.1
sub_10039E8F0 ID 42.1
sub_10039E534 ID 43.1
CC_SHA256_Final

```
WhatsApp`-[WARootViewController updateOfflineAssignABProperties]:
->  0x102068e38 <+0>:   stp    x24, x23, [sp, #-0x40]!
    0x102068e3c <+4>:   stp    x22, x21, [sp, #0x10]
    0x102068e40 <+8>:   stp    x20, x19, [sp, #0x20]
    0x102068e44 <+12>:  stp    x29, x30, [sp, #0x30]
    0x102068e48 <+16>:  add    x29, sp, #0x30
    0x102068e4c <+20>:  mov    x20, x0
    0x102068e50 <+24>:  adrp   x8, 5901
    0x102068e54 <+28>:  ldr    x0, [x8, #0xa0]
    0x102068e58 <+32>:  bl     0x1029024a0               ; objc_msgSend$sharedContext_deprecated
    0x102068e5c <+36>:  mov    x29, x29
    0x102068e60 <+40>:  bl     0x10280f40c               ; symbol stub for: objc_retainAutoreleasedReturnValue
    0x102068e64 <+44>:  mov    x21, x0
    0x102068e68 <+48>:  bl     0x10282b520               ; objc_msgSend$abProperties
    0x102068e6c <+52>:  mov    x29, x29
    0x102068e70 <+56>:  bl     0x10280f40c               ; symbol stub for: objc_retainAutoreleasedReturnValue
    0x102068e74 <+60>:  mov    x19, x0
    0x102068e78 <+64>:  bl     0x102742694               ; objc_release_X21ToX0_6694
    0x102068e7c <+68>:  bl     0x1027435d8               ; X19ToX0_0ToX2_75D8
    0x102068e80 <+72>:  bl     0x1029044a0               ; objc_msgSend$shouldQueryWithRefreshID:
    0x102068e84 <+76>:  cbz    w0, 0x102068f34           ; <+252>
    0x102068e88 <+80>:  mov    x0, x20
    0x102068e8c <+84>:  bl     0x102925960               ; objc_msgSend$userContext
    0x102068e90 <+88>:  mov    x29, x29
    0x102068e94 <+92>:  bl     0x10280f40c               ; symbol stub for: objc_retainAutoreleasedReturnValue
    0x102068e98 <+96>:  mov    x20, x0
    0x102068e9c <+100>: adrp   x8, 5907
    0x102068ea0 <+104>: ldr    x0, [x8, #0x58]
    0x102068ea4 <+108>: bl     0x10280f2e0               ; symbol stub for: objc_alloc
    0x102068ea8 <+112>: bl     0x102754f10               ; objc_msgSend$initWithUserContext_X20ToX2_8F10
    0x102068eac <+116>: mov    x21, x0
    0x102068eb0 <+120>: bl     0x1028351c0               ; objc_msgSend$assign
    0x102068eb4 <+124>: mov    x29, x29
    0x102068eb8 <+128>: bl     0x10280f40c               ; symbol stub for: objc_retainAutoreleasedReturnValue
    0x102068ebc <+132>: bl     0x102742fb0               ; X0ToX22_X20ToX0_6FB0
```

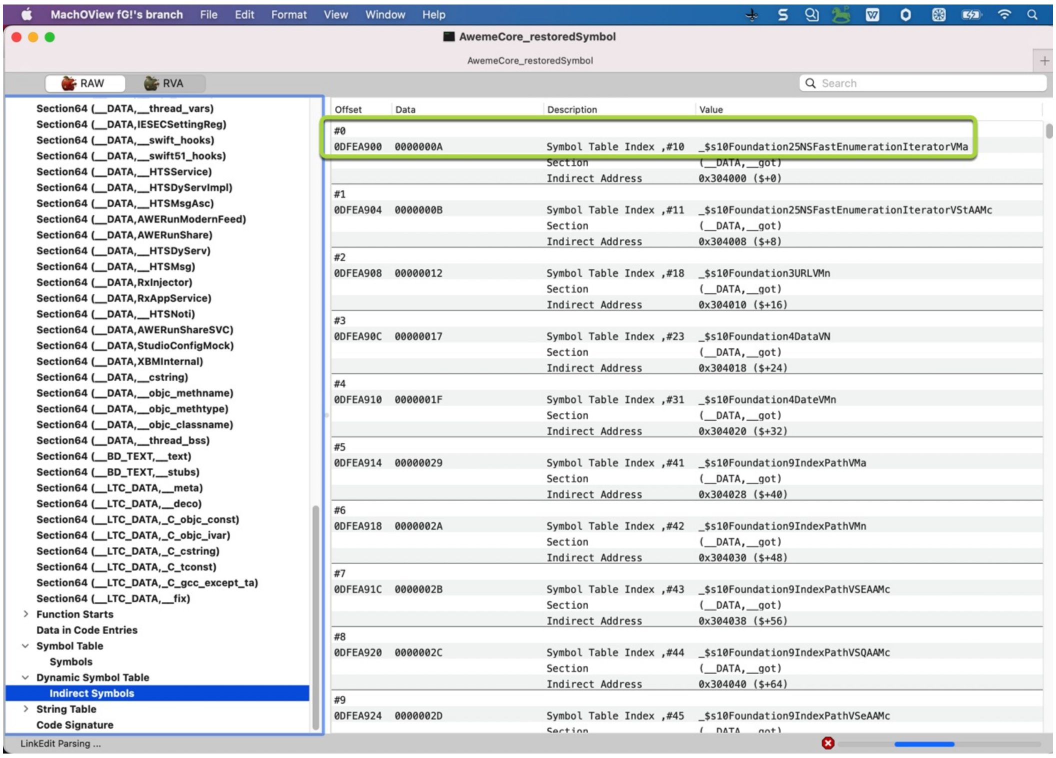
Thread 1: breakpoint 22.1 35.1 37.1 (1)

```
The "write" command has been loaded and is ready for use.
warning: failed to set breakpoint site at 0x106cc4e84 for breakpoint 45.1: error: 9 sending the breakpoint request
(lldb)
```

用工具辅助验证

且可以用其他工具辅助验证：的确加上了函数名=符号表了：

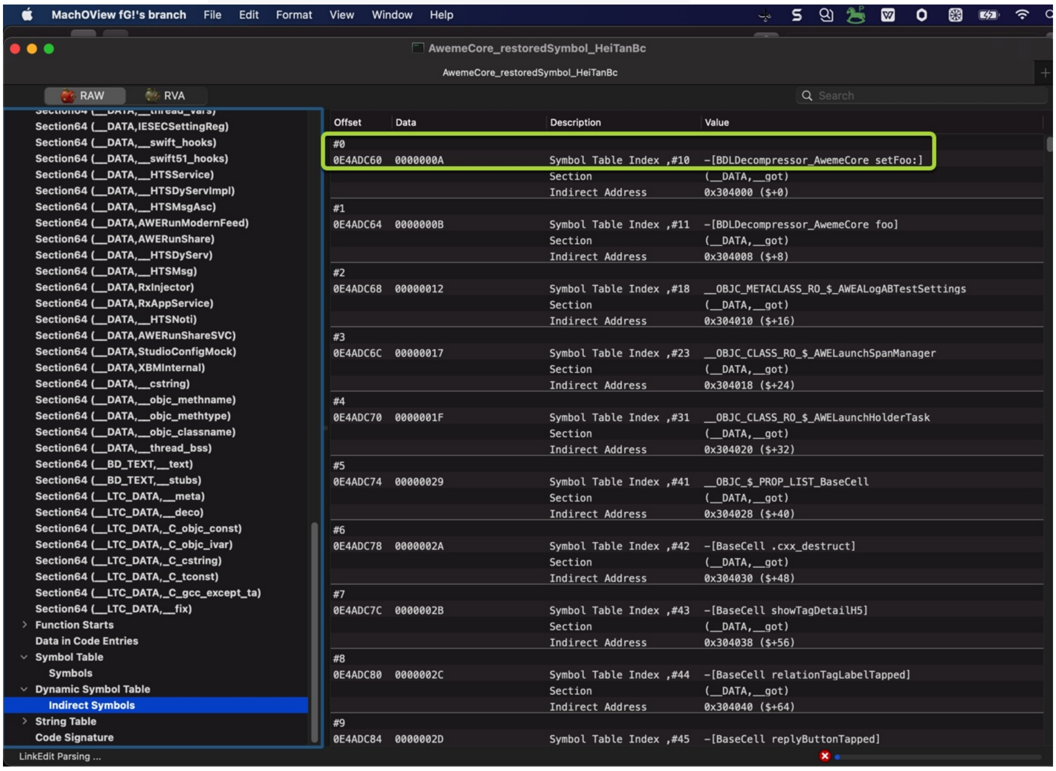
- MachOView
  - `Dynamic Symbol Table` -> `Indirect Symbols`
    - 之前=没有恢复符号表：`AwemeCore_noSymbol` 、 `AwemeCore_restoredSymbol`

- 

MachOView fG!'s branch
File
Edit
Format
View
Window
Help
AwemeCore_restoredSymbol
AwemeCore_restoredSymbol
RAW
RVA
Search
Section64 (__DATA,__thread_vars)
Section64 (__DATA,IESECSettingReg)
Section64 (__DATA,__swift_hooks)
Section64 (__DATA,__swift51_hooks)
Section64 (__DATA,__HTSService)
Section64 (__DATA,__HTSDyServImpl)
Section64 (__DATA,__HTSMsgAsc)
Section64 (__DATA,AWERunModernFeed)
Section64 (__DATA,AWERunShare)
Section64 (__DATA,__HTSDyServ)
Section64 (__DATA,__HTSMsg)
Section64 (__DATA,RxInjector)
Section64 (__DATA,RxAppService)
Section64 (__DATA,__HTSNoti)
Section64 (__DATA,AWERunShareSVC)
Section64 (__DATA,StudioConfigMock)
Section64 (__DATA,XBMInternal)
Section64 (__DATA,__cstring)
Section64 (__DATA,__objc_methname)
Section64 (__DATA,__objc_methtype)
Section64 (__DATA,__objc_classname)
Section64 (__DATA,__thread_bss)
Section64 (__BD_TEXT,__text)
Section64 (__BD_TEXT,__stubs)
Section64 (__LTC_DATA,__meta)
Section64 (__LTC_DATA,__deco)
Section64 (__LTC_DATA,_C_objc_const)
Section64 (__LTC_DATA,_C_objc_ivar)
Section64 (__LTC_DATA,_C_cstring)
Section64 (__LTC_DATA,_C_tconst)
Section64 (__LTC_DATA,_C_gcc_except_ta)
Section64 (__LTC_DATA,__fix)
Function Starts
Data in Code Entries
Symbol Table
Symbols
Dynamic Symbol Table
Indirect Symbols
String Table
Code Signature
LinkEdit Parsing ...

```
Offset    Data        Description              Value
#0
0DFEA900  0000000A    Symbol Table Index ,#10  _$s10Foundation25NSFastEnumerationIteratorVMa
                      Section                  (__DATA,__got)
                      Indirect Address         0x304000 ($+0)
#1
0DFEA904  0000000B    Symbol Table Index ,#11  _$s10Foundation25NSFastEnumerationIteratorVStAAMc
                      Section                  (__DATA,__got)
                      Indirect Address         0x304008 ($+8)
#2
0DFEA908  00000012    Symbol Table Index ,#18  _$s10Foundation3URLVMn
                      Section                  (__DATA,__got)
                      Indirect Address         0x304010 ($+16)
#3
0DFEA90C  00000017    Symbol Table Index ,#23  _$s10Foundation4DataVN
                      Section                  (__DATA,__got)
                      Indirect Address         0x304018 ($+24)
#4
0DFEA910  0000001F    Symbol Table Index ,#31  _$s10Foundation4DateVMn
                      Section                  (__DATA,__got)
                      Indirect Address         0x304020 ($+32)
#5
0DFEA914  00000029    Symbol Table Index ,#41  _$s10Foundation9IndexPathVMa
                      Section                  (__DATA,__got)
                      Indirect Address         0x304028 ($+40)
#6
0DFEA918  0000002A    Symbol Table Index ,#42  _$s10Foundation9IndexPathVMn
                      Section                  (__DATA,__got)
                      Indirect Address         0x304030 ($+48)
#7
0DFEA91C  0000002B    Symbol Table Index ,#43  _$s10Foundation9IndexPathVSEAAMc
                      Section                  (__DATA,__got)
                      Indirect Address         0x304038 ($+56)
#8
0DFEA920  0000002C    Symbol Table Index ,#44  _$s10Foundation9IndexPathVSQAAMc
                      Section                  (__DATA,__got)
                      Indirect Address         0x304040 ($+64)
#9
0DFEA924  0000002D    Symbol Table Index ,#45  _$s10Foundation9IndexPathVSeAAMc
                      Section                  (__DATA,__got)
```

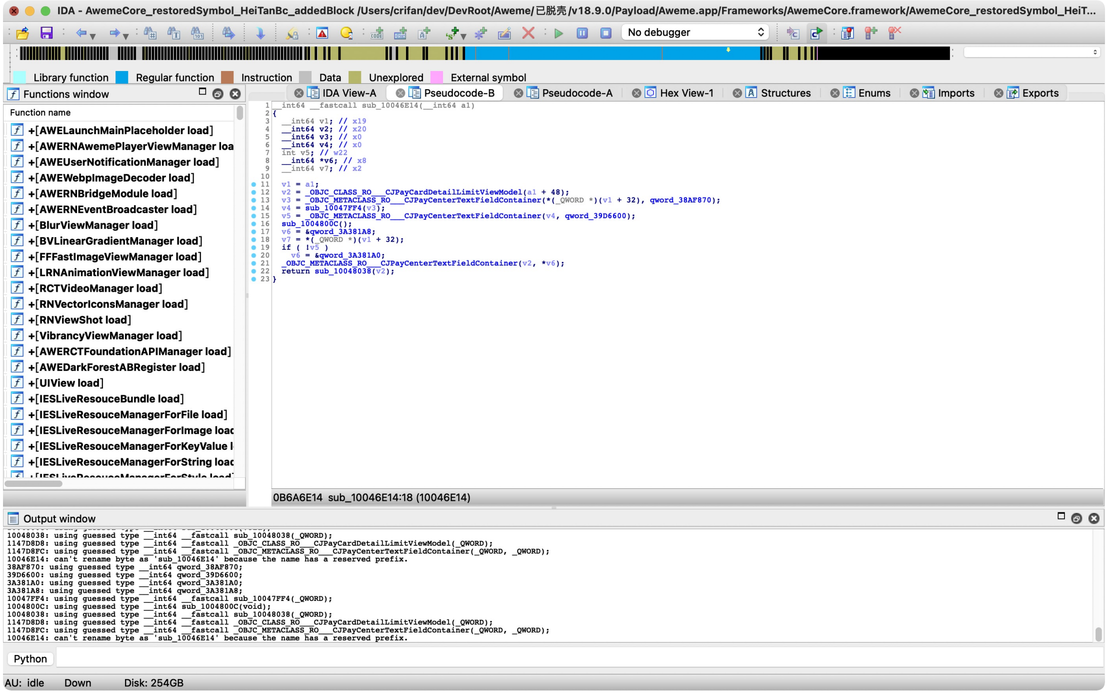
- 之后=已恢复符号表： `AwemeCore_restoredSymbol_HeiTanBc`

- 

MachOView fG!'s branch
File
Edit
Format
View
Window
Help
AwemeCore_restoredSymbol_HeiTanBc
AwemeCore_restoredSymbol_HeiTanBc
RAW
RVA
Search
Section64 (__DATA,__thread_vars)
Section64 (__DATA,IESECSettingReg)
Section64 (__DATA,__swift_hooks)
Section64 (__DATA,__swift51_hooks)
Section64 (__DATA,__HTSService)
Section64 (__DATA,__HTSDyServImpl)
Section64 (__DATA,__HTSMsgAsc)
Section64 (__DATA,AWERunModernFeed)
Section64 (__DATA,AWERunShare)
Section64 (__DATA,__HTSDyServ)
Section64 (__DATA,__HTSMsg)
Section64 (__DATA,RxInjector)
Section64 (__DATA,RxAppService)
Section64 (__DATA,__HTSNoti)
Section64 (__DATA,AWERunShareSVC)
Section64 (__DATA,StudioConfigMock)
Section64 (__DATA,XBMInternal)
Section64 (__DATA,__cstring)
Section64 (__DATA,__objc_methname)
Section64 (__DATA,__objc_methtype)
Section64 (__DATA,__objc_classname)
Section64 (__DATA,__thread_bss)
Section64 (__BD_TEXT,__text)
Section64 (__BD_TEXT,__stubs)
Section64 (__LTC_DATA,__meta)
Section64 (__LTC_DATA,__deco)
Section64 (__LTC_DATA,_C_objc_const)
Section64 (__LTC_DATA,_C_objc_ivar)
Section64 (__LTC_DATA,_C_cstring)
Section64 (__LTC_DATA,_C_tconst)
Section64 (__LTC_DATA,_C_gcc_except_ta)
Section64 (__LTC_DATA,__fix)
Function Starts
Data in Code Entries
Symbol Table
Symbols
Dynamic Symbol Table
Indirect Symbols
String Table
Code Signature
LinkEdit Parsing ...

```
Offset    Data        Description              Value
#0
0E4ADC60  0000000A    Symbol Table Index ,#10  -[BDLDecompressor_AwemeCore setFoo:]
                      Section                  (__DATA,__got)
                      Indirect Address         0x304000 ($+0)
#1
0E4ADC64  0000000B    Symbol Table Index ,#11  -[BDLDecompressor_AwemeCore foo]
                      Section                  (__DATA,__got)
                      Indirect Address         0x304008 ($+8)
#2
0E4ADC68  00000012    Symbol Table Index ,#18  __OBJC_METACLASS_RO_$_AWEALogABTestSettings
                      Section                  (__DATA,__got)
                      Indirect Address         0x304010 ($+16)
#3
0E4ADC6C  00000017    Symbol Table Index ,#23  __OBJC_CLASS_RO_$_AWELaunchSpanManager
                      Section                  (__DATA,__got)
                      Indirect Address         0x304018 ($+24)
#4
0E4ADC70  0000001F    Symbol Table Index ,#31  __OBJC_CLASS_RO_$_AWELaunchHolderTask
                      Section                  (__DATA,__got)
                      Indirect Address         0x304020 ($+32)
#5
0E4ADC74  00000029    Symbol Table Index ,#41  __OBJC_$_PROP_LIST_BaseCell
                      Section                  (__DATA,__got)
                      Indirect Address         0x304028 ($+40)
#6
0E4ADC78  0000002A    Symbol Table Index ,#42  -[BaseCell .cxx_destruct]
                      Section                  (__DATA,__got)
                      Indirect Address         0x304030 ($+48)
#7
0E4ADC7C  0000002B    Symbol Table Index ,#43  -[BaseCell showTagDetailH5]
                      Section                  (__DATA,__got)
                      Indirect Address         0x304038 ($+56)
#8
0E4ADC80  0000002C    Symbol Table Index ,#44  -[BaseCell relationTagLabelTapped]
                      Section                  (__DATA,__got)
                      Indirect Address         0x304040 ($+64)
#9
0E4ADC84  0000002D    Symbol Table Index ,#45  -[BaseCell replyButtonTapped]
```

- IDA
  - 之后=已恢复符号表： `AwemeCore_restoredSymbol_HeiTanBc`



+[AWELaunchMainPlaceholder load]
+[AWERNAwemePlayerViewManager loa
+[AWEUserNotificationManager load]
+[AWEWebpImageDecoder load]
+[AWERNBridgeModule load]
+[AWERNEventBroadcaster load]
+[BlurViewManager load]
+[BVLinearGradientManager load]
+[FFFastImageViewManager load]
+[LRNAnimationViewManager load]
+[RCTVideoManager load]
+[RNVectorIconsManager load]
+[RNViewShot load]
+[VibrancyViewManager load]
+[AWERCTFoundationAPIManager load]
+[AWEDarkForestABRegister load]
+[UIView load]
+[IESLiveResouceBundle load]
+[IESLiveResouceManagerForFile load]
+[IESLiveResouceManagerForImage loac
+[IESLiveResouceManagerForKeyValue l
+[IESLiveResouceManagerForString loac

```
__int64 __fastcall sub_10046E14(__int64 a1)
{
  __int64 v1; // x19
  __int64 v2; // x20
  __int64 v3; // x0
  __int64 v4; // x0
  int v5; // w22
  __int64 *v6; // x8
  __int64 v7; // x2

  v1 = a1;
  v2 = _OBJC_CLASS_RO___CJPayCardDetailLimitViewModel(a1 + 48);
  v3 = _OBJC_METACLASS_RO___CJPayCenterTextFieldContainer(*(_QWORD *)(v1 + 32), qword_38AF870);
  v4 = sub_10047FF4(v3);
  v5 = _OBJC_METACLASS_RO___CJPayCenterTextFieldContainer(v4, qword_39D6600);
  sub_1004800C();
  v6 = &qword_3A381A8;
  v7 = *(_QWORD *)(v1 + 32);
  if ( !v5 )
    v6 = &qword_3A381A0;
  _OBJC_METACLASS_RO___CJPayCenterTextFieldContainer(v2, *v6);
  return sub_10048038(v2);
}
```

0B6A6E14 sub_10046E14:18 (10046E14)

```
10048038: using guessed type __int64 __fastcall sub_10048038(_QWORD);
1147D8D8: using guessed type __int64 __fastcall _OBJC_CLASS_RO___CJPayCardDetailLimitViewModel(_QWORD);
1147D8FC: using guessed type __int64 __fastcall _OBJC_METACLASS_RO___CJPayCenterTextFieldContainer(_QWORD, _QWORD);
10046E14: can't rename byte as 'sub_10046E14' because the name has a reserved prefix.
38AF870: using guessed type __int64 qword_38AF870;
39D6600: using guessed type __int64 qword_39D6600;
3A381A0: using guessed type __int64 qword_3A381A0;
3A381A8: using guessed type __int64 qword_3A381A8;
10047FF4: using guessed type __int64 __fastcall sub_10047FF4(_QWORD);
1004800C: using guessed type __int64 sub_1004800C(void);
10048038: using guessed type __int64 __fastcall sub_10048038(_QWORD);
1147D8D8: using guessed type __int64 __fastcall _OBJC_CLASS_RO___CJPayCardDetailLimitViewModel(_QWORD);
1147D8FC: using guessed type __int64 __fastcall _OBJC_METACLASS_RO___CJPayCenterTextFieldContainer(_QWORD, _QWORD);
10046E14: can't rename byte as 'sub_10046E14' because the name has a reserved prefix.
```

- (Xcode中)lldb

  ○

如何恢复符号表

原版restore-symbol

此处所说的原始版本的 `restore-symbol`，是相对于我自己修改的版本来说的。

而演示版本的 `restore-symbol`，又分几个版本：

- 最原始版本： `tobefuturer 的 restore-symbol`
  - https://github.com/tobefuturer/restore-symbol
- 改进版本： `HeiTanBc 的 restore-symbol`
  - https://github.com/HeiTanBc/restore-symbol

但是总体用法是一样的，下面以 `HeiTanBc` 版本的 `restore-symbol` 为例，来说明如何使用：

准备

下载、编译、确认：

```
git clone --recursive https://github.com/HeiTanBc/restore-symbol.git
cd restore-symbol
make
./restore-symbol
```

用restore-symbol恢复ObjC符号表

下面举例说明：

AwemeCore

```
➜  AwemeCore.framework /Users/crifan/dev/DevSrc/iOS/restore-symbol/HeiTanBc/restore-symbol/restore-symbol AwemeCore_noSymbol -o AwemeCore_restoredSymbol_HeiTanBc
=========== Start =============
Scan OC method in mach-o-file.
Scan OC method finish.
restore 329610 symbols
=========== Finish ============
```

Aweme

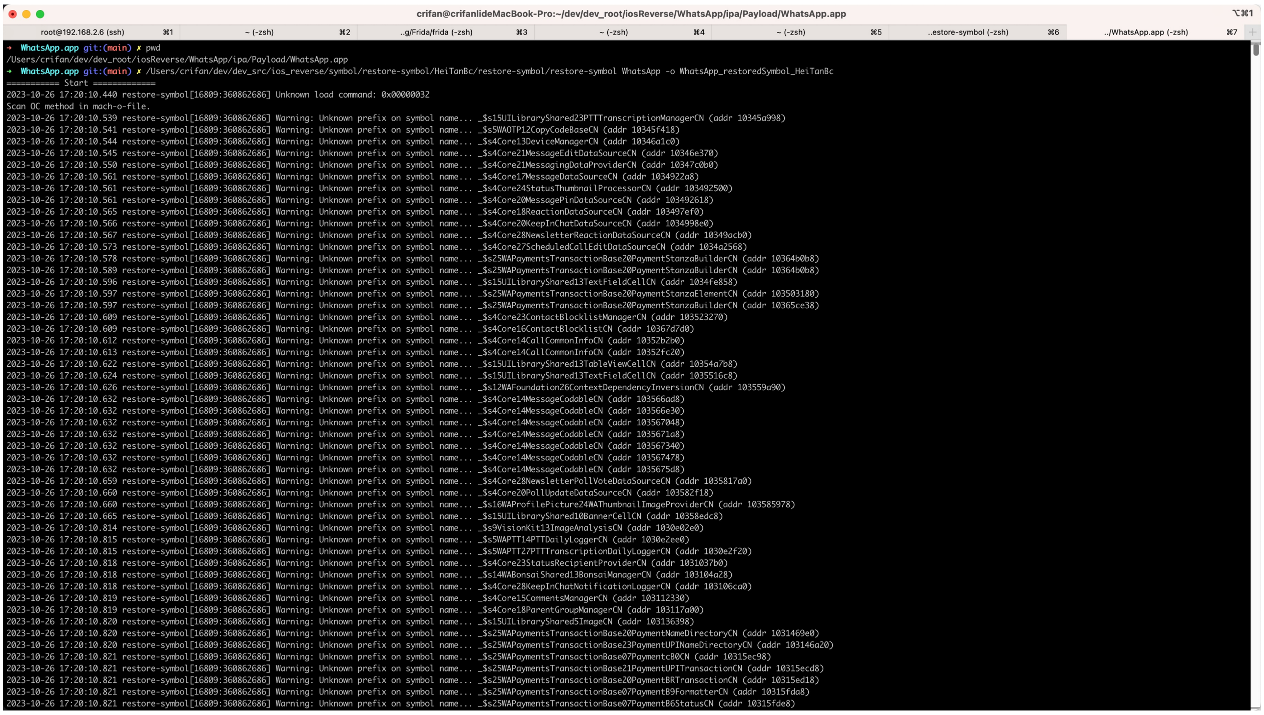
```
➜  Aweme.app /Users/crifan/dev/DevSrc/iOS/restore-symbol/HeiTanBc/restore-symbol/restore-symbol Aweme_noSymbol -o Aweme_restoredSymbol_HeiTanBc
=========== Start =============
Scan OC method in mach-o-file.
Scan OC method finish.
restore 0 symbols
=========== Finish ============
```

注：此处0个symbol，说明：没有可用符号。

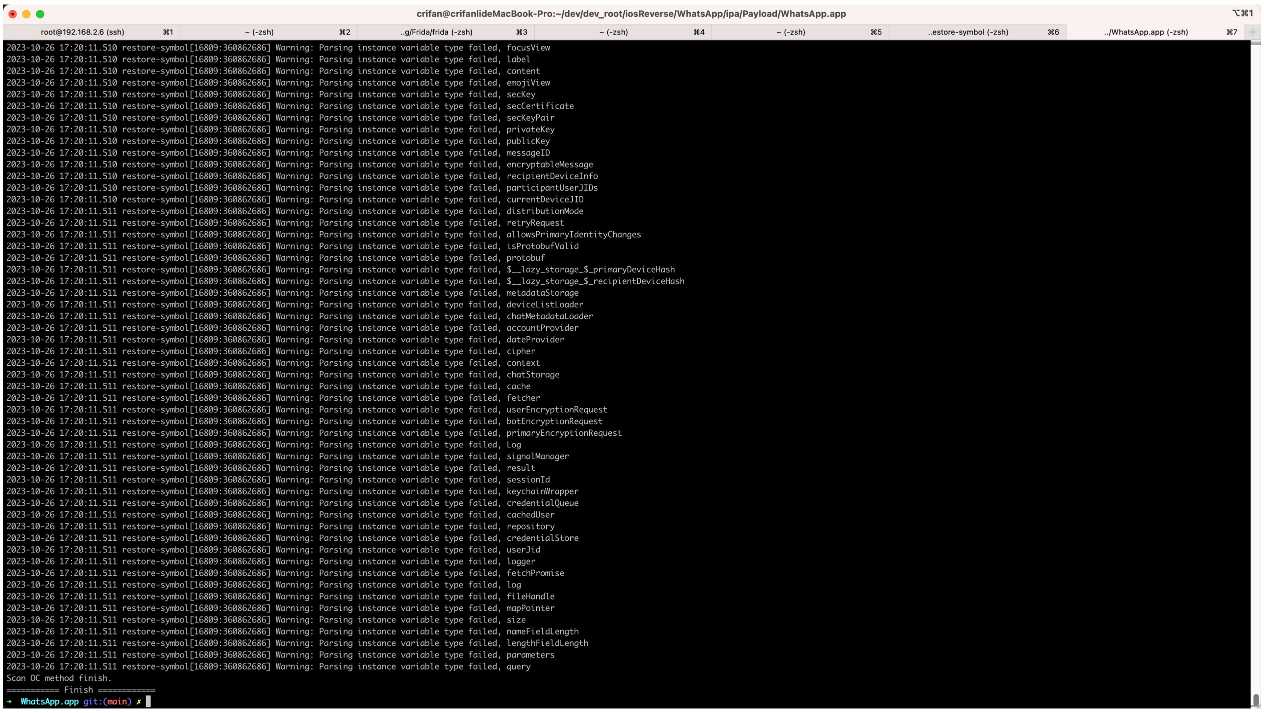
WhatsApp

```
➜  WhatsApp.app git:(main) ✗ /Users/crifan/dev/dev_src/ios_reverse/symbol/restore-symbo
l/HeiTanBc/restore-symbol/restore-symbol WhatsApp -o WhatsApp_restoredSymbol_HeiTanBc
=========== Start =============
2023-10-26 17:20:10.440 restore-symbol[16809:360862686] Unknown load command: 0x0000003
2
Scan OC method in mach-o-file.
2023-10-26 17:20:10.539 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s15UILibraryShared23PTTTranscriptionManagerCN (addr 10345a998)
2023-10-26 17:20:10.541 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s5WAOTP12CopyCodeBaseCN (addr 10345f418)
2023-10-26 17:20:10.544 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core13DeviceManagerCN (addr 10346a1c0)
2023-10-26 17:20:10.545 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core21MessageEditDataSourceCN (addr 10346e370)
2023-10-26 17:20:10.550 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core21MessagingDataProviderCN (addr 10347c0b0)
2023-10-26 17:20:10.561 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core17MessageDataSourceCN (addr 1034922a8)
2023-10-26 17:20:10.561 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core24StatusThumbnailProcessorCN (addr 103492500)
2023-10-26 17:20:10.561 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core20MessagePinDataSourceCN (addr 103492618)
2023-10-26 17:20:10.565 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core18ReactionDataSourceCN (addr 103497ef0)
2023-10-26 17:20:10.566 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core20KeepInChatDataSourceCN (addr 1034998e0)
2023-10-26 17:20:10.567 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core28NewsletterReactionDataSourceCN (addr 10349acb0)
2023-10-26 17:20:10.573 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s4Core27ScheduledCallEditDataSourceCN (addr 1034a2568)
2023-10-26 17:20:10.578 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s25WAPaymentsTransactionBase20PaymentStanzaBuilderCN (addr 10364b0b8)
2023-10-26 17:20:10.589 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s25WAPaymentsTransactionBase20PaymentStanzaBuilderCN (addr 10364b0b8)
2023-10-26 17:20:10.596 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s15UILibraryShared13TextFieldCellCN (addr 1034fe858)
2023-10-26 17:20:10.597 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s25WAPaymentsTransactionBase20PaymentStanzaElementCN (addr 103503180)
2023-10-26 17:20:10.597 restore-symbol[16809:360862686] Warning: Unknown prefix on symb
ol name... _$s25WAPaymentsTransactionBase20PaymentStanzaBuilderCN (addr 10365ce38)
...
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, botEncryptionRequest
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, primaryEncryptionRequest
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, Log
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, signalManager
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
```

```
ble type failed, result
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, sessionId
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, keychainWrapper
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, credentialQueue
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, cachedUser
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, repository
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, credentialStore
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, userJid
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, logger
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, fetchPromise
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, log
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, fileHandle
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, mapPointer
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, size
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, nameFieldLength
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, lengthFieldLength
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, parameters
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance varia
ble type failed, query
Scan OC method finish.
=========== Finish ============
➜  WhatsApp.app git:(main) ✗
```


crifan@crifanlideMacBook-Pro:~/dev/dev_root/iosReverse/WhatsApp/ipa/Payload/WhatsApp.app
⌥⌘1
root@192.168.2.6 (ssh) ⌘1
~ (-zsh) ⌘2
..g/Frida/frida (-zsh) ⌘3
~ (-zsh) ⌘4
~ (-zsh) ⌘5
..estore-symbol (-zsh) ⌘6
../WhatsApp.app (-zsh) ⌘7

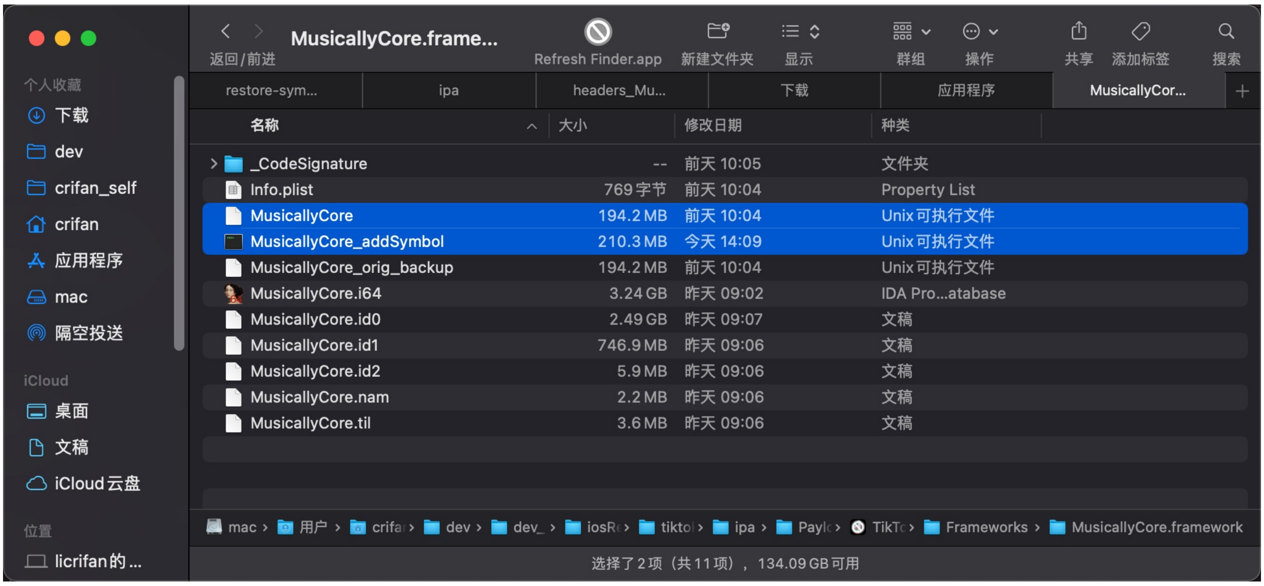
```
➜  WhatsApp.app git:(main) ✗ pwd
/Users/crifan/dev/dev_root/iosReverse/WhatsApp/ipa/Payload/WhatsApp.app
➜  WhatsApp.app git:(main) ✗ /Users/crifan/dev/dev_src/ios_reverse/symbol/restore-symbol/HeiTanBc/restore-symbol/restore-symbol WhatsApp -o WhatsApp_restoredSymbol_HeiTanBc
=========== Start =============
2023-10-26 17:20:10.440 restore-symbol[16809:360862686] Unknown load command: 0x00000032
Scan OC method in mach-o-file.
2023-10-26 17:20:10.539 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s15UILibraryShared23PTTTranscriptionManagerCN (addr 10345a998)
2023-10-26 17:20:10.541 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s5WAOTP12CopyCodeBaseCN (addr 10345f418)
2023-10-26 17:20:10.544 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core13DeviceManagerCN (addr 10346a1c0)
2023-10-26 17:20:10.545 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core21MessageEditDataSourceCN (addr 10346e370)
2023-10-26 17:20:10.550 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core21MessagingDataProviderCN (addr 10347c0b0)
2023-10-26 17:20:10.561 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core17MessageDataSourceCN (addr 1034922a8)
2023-10-26 17:20:10.561 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core24StatusThumbnailProcessorCN (addr 103492500)
2023-10-26 17:20:10.561 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core20MessagePinDataSourceCN (addr 103492618)
2023-10-26 17:20:10.565 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core18ReactionDataSourceCN (addr 103497ef0)
2023-10-26 17:20:10.566 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core20KeepInChatDataSourceCN (addr 1034998e0)
2023-10-26 17:20:10.567 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core28NewsletterReactionDataSourceCN (addr 10349acb0)
2023-10-26 17:20:10.573 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core27ScheduledCallEditDataSourceCN (addr 1034a2568)
2023-10-26 17:20:10.578 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase20PaymentStanzaBuilderCN (addr 10364b0b8)
2023-10-26 17:20:10.589 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase20PaymentStanzaBuilderCN (addr 10364b0b8)
2023-10-26 17:20:10.596 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s15UILibraryShared13TextFieldCellCN (addr 1034fe858)
2023-10-26 17:20:10.597 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase20PaymentStanzaElementCN (addr 103503180)
2023-10-26 17:20:10.597 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase20PaymentStanzaBuilderCN (addr 10365ce38)
2023-10-26 17:20:10.609 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core23ContactBlocklistManagerCN (addr 103523270)
2023-10-26 17:20:10.609 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core16ContactBlocklistCN (addr 10367d7d0)
2023-10-26 17:20:10.612 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14CallCommonInfoCN (addr 10352b2b0)
2023-10-26 17:20:10.613 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14CallCommonInfoCN (addr 10352fc20)
2023-10-26 17:20:10.622 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s15UILibraryShared13TableViewCellCN (addr 10354a7b8)
2023-10-26 17:20:10.624 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s15UILibraryShared13TextFieldCellCN (addr 1035516c8)
2023-10-26 17:20:10.626 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s12WAFoundation26ContextDependencyInversionCN (addr 103559a90)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 103566ad8)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 103566e30)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 103567048)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 1035671a8)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 103567340)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 103567478)
2023-10-26 17:20:10.632 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core14MessageCodableCN (addr 1035675d8)
2023-10-26 17:20:10.659 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core28NewsletterPollVoteDataSourceCN (addr 1035817a0)
2023-10-26 17:20:10.660 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core20PollUpdateDataSourceCN (addr 103582f18)
2023-10-26 17:20:10.660 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s16WAProfilePicture24WAThumbnailImageProviderCN (addr 103585978)
2023-10-26 17:20:10.665 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s15UILibraryShared10BannerCellCN (addr 10358edc8)
2023-10-26 17:20:10.814 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s9VisionKit13ImageAnalysisCN (addr 1030e02e0)
2023-10-26 17:20:10.815 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s5WAPTT14PTTDailyLoggerCN (addr 1030e2ee0)
2023-10-26 17:20:10.815 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s5WAPTT27PTTTranscriptionDailyLoggerCN (addr 1030e2f20)
2023-10-26 17:20:10.818 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core23StatusRecipientProviderCN (addr 1031037b0)
2023-10-26 17:20:10.818 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s14WABonsaiShared13BonsaiManagerCN (addr 103104a28)
2023-10-26 17:20:10.818 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core28KeepInChatNotificationLoggerCN (addr 103106ca0)
2023-10-26 17:20:10.819 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core15CommentsManagerCN (addr 103112330)
2023-10-26 17:20:10.819 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s4Core18ParentGroupManagerCN (addr 103117a00)
2023-10-26 17:20:10.820 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s15UILibraryShared5ImageCN (addr 103136398)
2023-10-26 17:20:10.820 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase20PaymentNameDirectoryCN (addr 1031469e0)
2023-10-26 17:20:10.820 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase23PaymentUPINameDirectoryCN (addr 103146a20)
2023-10-26 17:20:10.821 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase07PaymentcB0CN (addr 10315ec98)
2023-10-26 17:20:10.821 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase21PaymentUPITransactionCN (addr 10315ecd8)
2023-10-26 17:20:10.821 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase20PaymentBRTransactionCN (addr 10315ed18)
2023-10-26 17:20:10.821 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase07PaymentB9FormatterCN (addr 10315fda8)
2023-10-26 17:20:10.821 restore-symbol[16809:360862686] Warning: Unknown prefix on symbol name... _$s25WAPaymentsTransactionBase07PaymentB6StatusCN (addr 10315fde8)
```


crifan@crifanlideMacBook-Pro:~/dev/dev_root/iosReverse/WhatsApp/ipa/Payload/WhatsApp.app
⌥⌘1
root@192.168.2.6 (ssh) ⌘1
~ (-zsh) ⌘2
..g/Frida/frida (-zsh) ⌘3
~ (-zsh) ⌘4
~ (-zsh) ⌘5
..estore-symbol (-zsh) ⌘6
../WhatsApp.app (-zsh) ⌘7

```
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, focusView
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, label
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, content
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, emojiView
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, secKey
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, secCertificate
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, secKeyPair
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, privateKey
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, publicKey
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, messageID
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, encryptableMessage
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, recipientDeviceInfo
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, participantUserJIDs
2023-10-26 17:20:11.510 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, currentDeviceJID
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, distributionMode
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, retryRequest
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, allowsPrimaryIdentityChanges
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, isProtobufValid
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, protobuf
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, $__lazy_storage_$_primaryDeviceHash
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, $__lazy_storage_$_recipientDeviceHash
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, metadataStorage
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, deviceListLoader
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, chatMetadataLoader
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, accountProvider
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, dateProvider
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, cipher
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, context
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, chatStorage
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, cache
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, fetcher
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, userEncryptionRequest
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, botEncryptionRequest
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, primaryEncryptionRequest
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, Log
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, signalManager
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, result
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, sessionId
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, keychainWrapper
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, credentialQueue
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, cachedUser
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, repository
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, credentialStore
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, userJid
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, logger
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, fetchPromise
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, log
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, fileHandle
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, mapPointer
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, size
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, nameFieldLength
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, lengthFieldLength
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, parameters
2023-10-26 17:20:11.511 restore-symbol[16809:360862686] Warning: Parsing instance variable type failed, query
Scan OC method finish.
=========== Finish ============
➜  WhatsApp.app git:(main) ✗ 
```

MusicallyCore

```
crifan@licrifandeMacBook-Pro⌜ ~/dev/dev_src/ios_reverse/symbol/restore-symbol/HeiTanBc/restore-symbol⌜ ＼ master⌜ ./restore-symbol /Users/crifan/dev/dev_root/iosReverse/tiktok/ipa/Payload/TikTok.app/Frameworks/MusicallyCore.framework/MusicallyCore -o /Users/crifan/dev/dev_root/iosReverse/tiktok/ipa/Payload/TikTok.app/Frameworks/MusicallyCore.framework/MusicallyCore_addSymbol
============ Start =============
Scan OC method in mach-o-file.
Scan OC method finish.
restore 261142 symbols
============ Finish ============
```



名称	大小	修改日期	种类
_CodeSignature	--	前天 10:05	文件夹
Info.plist	769字节	前天 10:04	Property List
MusicallyCore	194.2 MB	前天 10:04	Unix可执行文件
MusicallyCore_addSymbol	210.3 MB	今天 14:09	Unix可执行文件
MusicallyCore_orig_backup	194.2 MB	前天 10:04	Unix可执行文件
MusicallyCore.i64	3.24 GB	昨天 09:02	IDA Pro...atabase
MusicallyCore.id0	2.49 GB	昨天 09:07	文稿
MusicallyCore.id1	746.9 MB	昨天 09:06	文稿
MusicallyCore.id2	5.9 MB	昨天 09:06	文稿
MusicallyCore.nam	2.2 MB	昨天 09:06	文稿
MusicallyCore.til	3.6 MB	昨天 09:06	文稿

选择了2项（共11项），134.09 GB可用

RzGame

```
✘ crifan@licrifandeMacBook-Pro ⌜ ~/dev/dev_src/ios_reverse/symbol/restore-symbol/HeiTanBc/restore-symbol ⌜ ╲ master ●⌜ ./restore-symbol /Users/crifan/dev/dev_root/iosReverse/undecember/ipa/Payload/RzGame.app/RzGame -o /Users/crifan/dev/dev_root/iosReverse/undecember/ipa/Payload/RzGame.app/RzGame_addSymbol
=========== Start =============
Scan OC method in mach-o-file.
Scan OC method finish.
restore 28136 symbols
=========== Finish ============
```

导出Block符号表

用restore-symbol去恢复=导出，ObjC的符号表后，对于更加完整的用法，则还可以继续去导出block符号表

需要借用相关的工具：`ida_search_block.py` 的IDA插件

ida_search_block.py的版本

而关于 `ida_search_block.py` 的文件，此处代码仓库中是有的：

- https://github.com/HeiTanBc/restore-symbol/blob/master/search_oc_block/ida_search_block.py

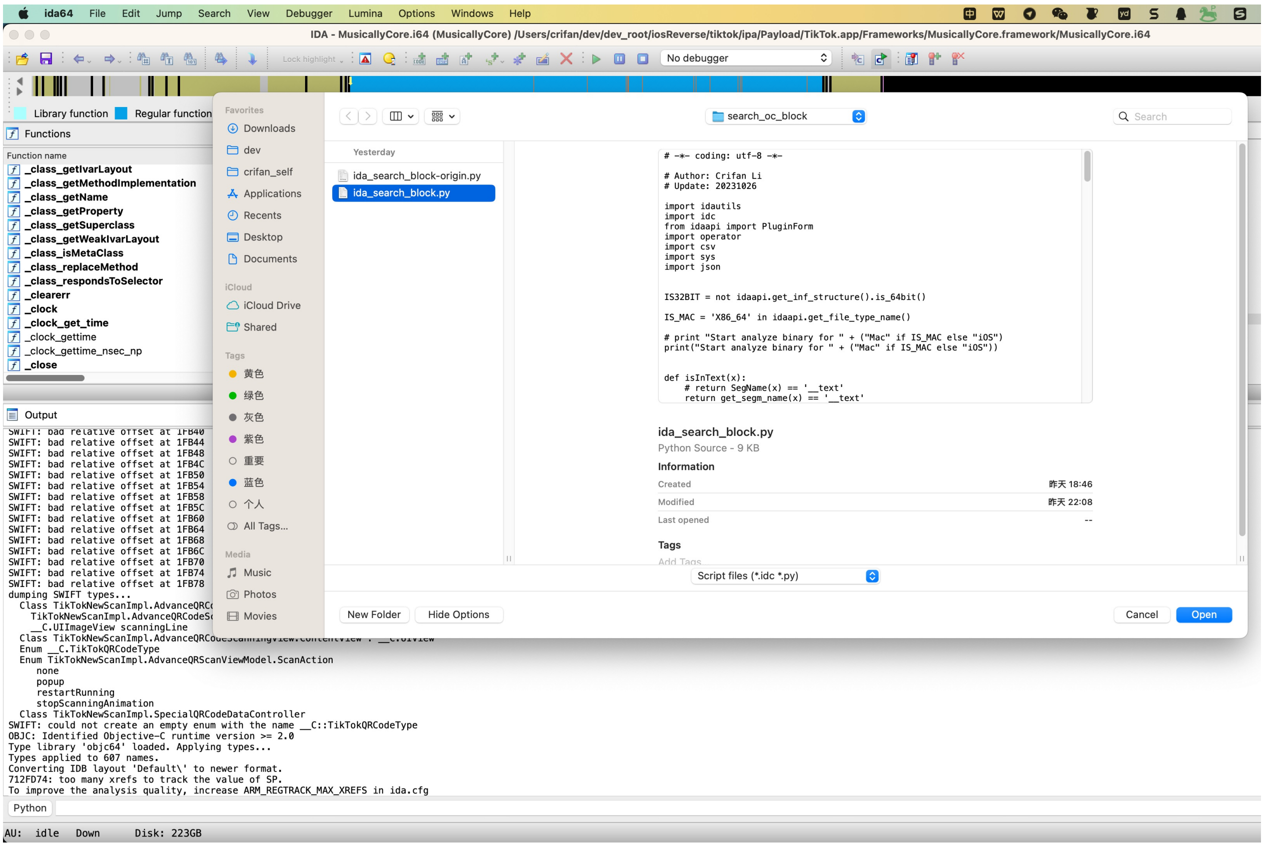
但该版本有些bug，而我Crifan修改后的：修复该bug+额外优化后的最新版本是：

- https://github.com/crifan/restore-symbol/blob/master/tools/IDAScripts/search_oc_block/ida_search_block.py

举例

此处举例说明如何使用：

MusicallyCore



IDA - MusicallyCore.i64 (MusicallyCore) /Users/crifan/dev/dev_root/iosReverse/tiktok/ipa/Payload/TikTok.app/Frameworks/MusicallyCore.framework/MusicallyCore.i64

```python
# -*- coding: utf-8 -*-

# Author: Crifan Li
# Update: 20231026

import idautils
import idc
from idaapi import PluginForm
import operator
import csv
import sys
import json


IS32BIT = not idaapi.get_inf_structure().is_64bit()

IS_MAC = 'X86_64' in idaapi.get_file_type_name()

# print "Start analyze binary for " + ("Mac" if IS_MAC else "iOS")
print("Start analyze binary for " + ("Mac" if IS_MAC else "iOS"))


def isInText(x):
    # return SegName(x) == '__text'
    return get_segm_name(x) == '__text'
```

ida_search_block.py

Python Source - 9 KB

Information

Created 昨天 18:46

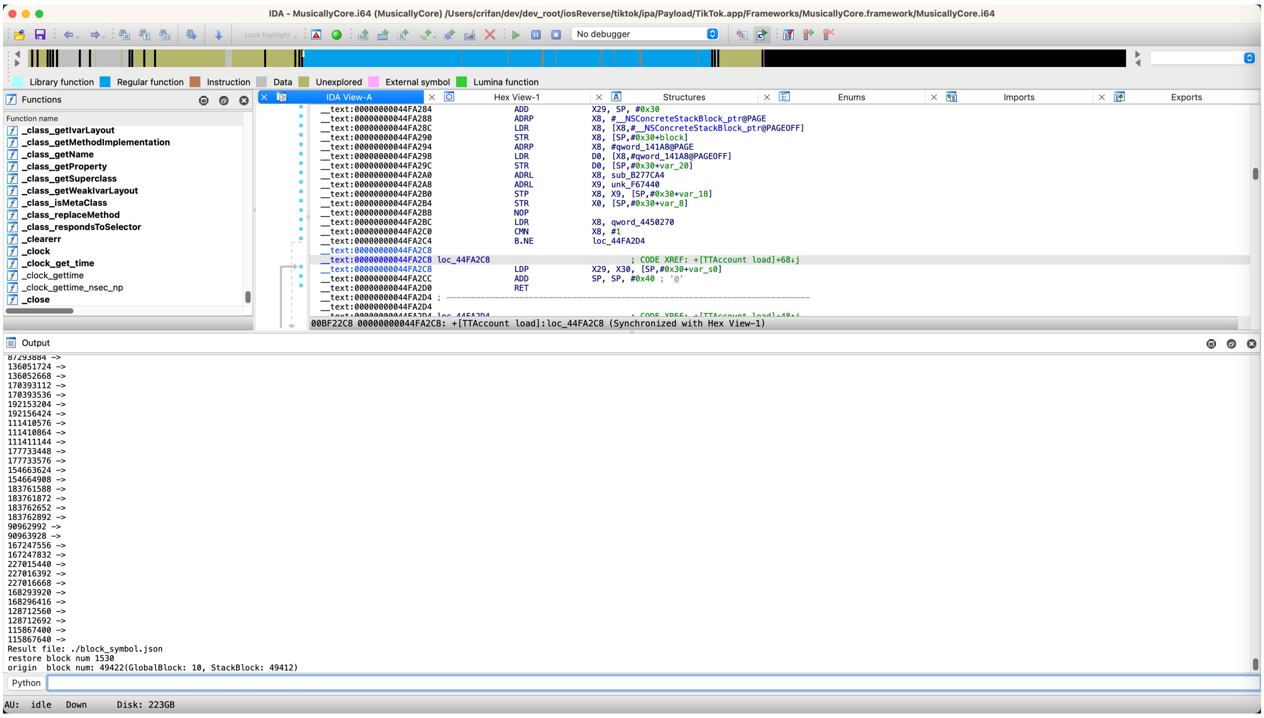
Modified 昨天 22:08

Last opened --

```
SWIFT: bad relative offset at 1FB40
SWIFT: bad relative offset at 1FB44
SWIFT: bad relative offset at 1FB48
SWIFT: bad relative offset at 1FB4C
SWIFT: bad relative offset at 1FB50
SWIFT: bad relative offset at 1FB54
SWIFT: bad relative offset at 1FB58
SWIFT: bad relative offset at 1FB5C
SWIFT: bad relative offset at 1FB60
SWIFT: bad relative offset at 1FB64
SWIFT: bad relative offset at 1FB68
SWIFT: bad relative offset at 1FB6C
SWIFT: bad relative offset at 1FB70
SWIFT: bad relative offset at 1FB74
SWIFT: bad relative offset at 1FB78
dumping SWIFT types...
  Class TikTokNewScanImpl.AdvanceQRC
    TikTokNewScanImpl.AdvanceQRCodeS
    __C.UIImageView scanningLine
  Class TikTokNewScanImpl.AdvanceQRCo
  Enum __C.TikTokQRCodeType
  Enum TikTokNewScanImpl.AdvanceQRScanViewModel.ScanAction
     none
     popup
     restartRunning
     stopScanningAnimation
  Class TikTokNewScanImpl.SpecialQRCodeDataController
SWIFT: could not create an empty enum with the name __C::TikTokQRCodeType
OBJC: Identified Objective-C runtime version >= 2.0
Type library 'objc64' loaded. Applying types...
Types applied to 607 names.
Converting IDB layout 'Default\' to newer format.
712FD74: too many xrefs to track the value of SP.
To improve the analysis quality, increase ARM_REGTRACK_MAX_XREFS in ida.cfg
```

最后会输出：

```
'''
Result file: ./block_symbol.json
restore block num 1530
origin  block num: 49422(GlobalBlock: 10, StackBlock: 49412)
```



IDA - MusicallyCore.i64 (MusicallyCore) /Users/crifan/dev/dev_root/iosReverse/tiktok/ipa/Payload/TikTok.app/Frameworks/MusicallyCore.framework/MusicallyCore.i64

```
__text:00000000044FA284                 ADD             X29, SP, #0x30
__text:00000000044FA288                 ADRP            X8, #__NSConcreteStackBlock_ptr@PAGE
__text:00000000044FA28C                 LDR             X8, [X8,#__NSConcreteStackBlock_ptr@PAGEOFF]
__text:00000000044FA290                 STR             X8, [SP,#0x30+block]
__text:00000000044FA294                 ADRP            X8, #qword_141A8@PAGE
__text:00000000044FA298                 LDR             D0, [X8,#qword_141A8@PAGEOFF]
__text:00000000044FA29C                 STR             D0, [SP,#0x30+var_20]
__text:00000000044FA2A0                 ADRL            X8, sub_B277CA4
__text:00000000044FA2A8                 ADRL            X9, unk_F67440
__text:00000000044FA2B0                 STP             X8, X9, [SP,#0x30+var_18]
__text:00000000044FA2B4                 STR             X0, [SP,#0x30+var_8]
__text:00000000044FA2B8                 NOP
__text:00000000044FA2BC                 LDR             X8, qword_4450270
__text:00000000044FA2C0                 CMN             X8, #1
__text:00000000044FA2C4                 B.NE            loc_44FA2D4
__text:00000000044FA2C8
__text:00000000044FA2C8 loc_44FA2C8                             ; CODE XREF: +[TTAccount load]+68↓j
__text:00000000044FA2C8                 LDP             X29, X30, [SP,#0x30+var_s0]
__text:00000000044FA2CC                 ADD             SP, SP, #0x40 ; '@'
__text:00000000044FA2D0                 RET
__text:00000000044FA2D4 ; ---------------------------------------------------------------------------
__text:00000000044FA2D4
__text:00000000044FA2D4 loc_44FA2D4                             ; CODE XREF: +[TTAccount load]+48↓j
00BF22C8 00000000044FA2C8: +[TTAccount load]:loc_44FA2C8 (Synchronized with Hex View-1)
```

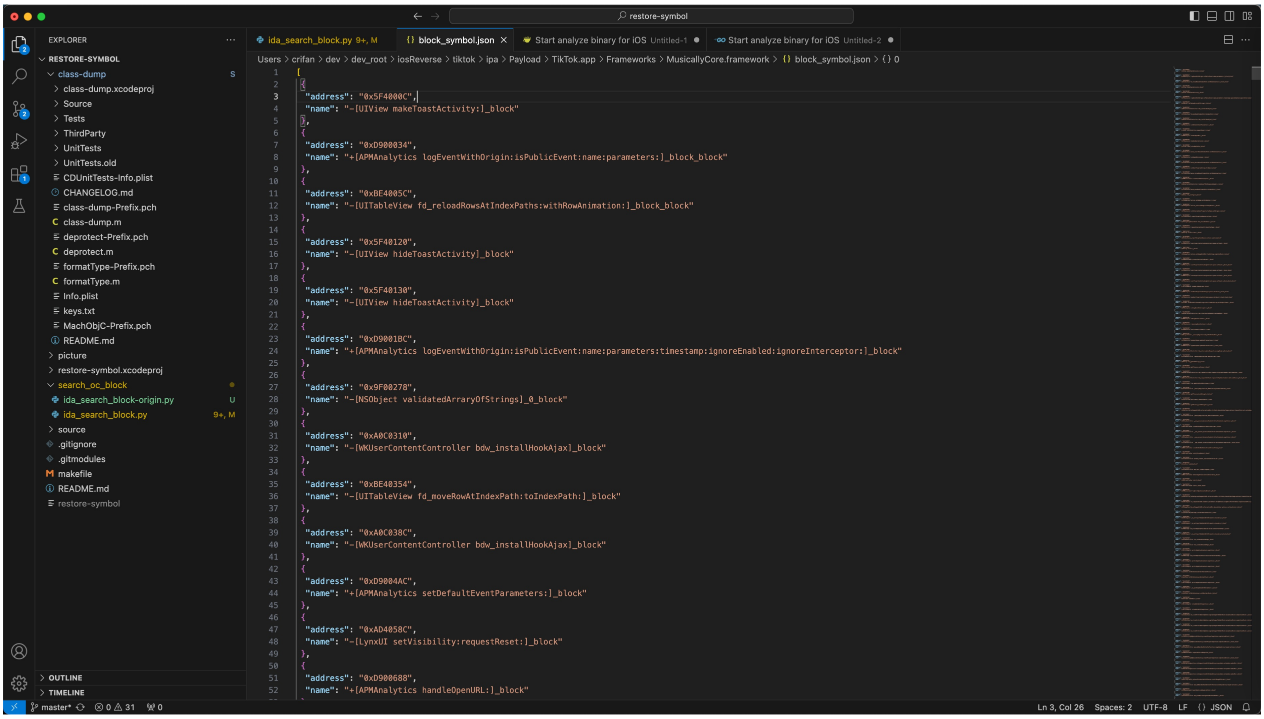
```
87293884 ->
136051724 ->
136052668 ->
170393112 ->
170393536 ->
192153204 ->
192156424 ->
111410576 ->
111410864 ->
111411144 ->
177733448 ->
177733576 ->
154663624 ->
154664908 ->
183761588 ->
183761872 ->
183762652 ->
183762892 ->
90962992 ->
90963928 ->
167247556 ->
167247832 ->
227015440 ->
227016392 ->
227016668 ->
168293920 ->
168296416 ->
128712560 ->
128712692 ->
115867400 ->
115867640 ->
Result file: ./block_symbol.json
restore block num 1530
origin  block num: 49422(GlobalBlock: 10, StackBlock: 49412)
```

对应的输出文件：

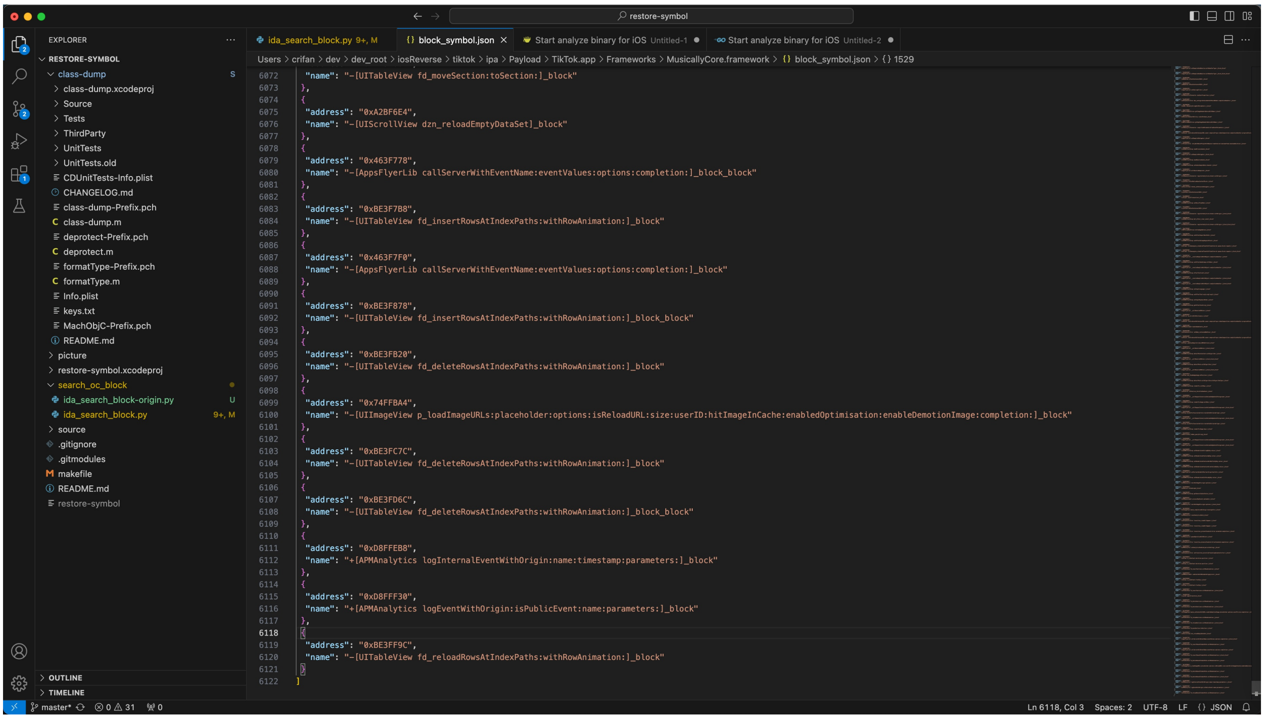
- `/Users/crifan/dev/dev_root/iosReverse/tiktok/ipa/Payload/TikTok.app/Frameworks/MusicallyCore.framework/block_symbol.json`
    -

```
[
 {
  "address": "0x5F4000C",
  "name": "-[UIView makeToastActivity:]_block"
 },
 {
  "address": "0xD900034",
  "name": "+[APMAnalytics logEventWithOrigin:isPublicEvent:name:parameters:]_block_block"
 },
 {
  "address": "0xBE4005C",
  "name": "-[UITableView fd_reloadRowsAtIndexPaths:withRowAnimation:]_block_block"
 },
 {
  "address": "0x5F40120",
  "name": "-[UIView hideToastActivity]_block"
 },
 {
  "address": "0x5F40130",
  "name": "-[UIView hideToastActivity]_block"
 },
 {
  "address": "0xD9001BC",
  "name": "+[APMAnalytics logEventWithOrigin:isPublicEvent:name:parameters:timestamp:ignoreEnabled:ignoreInterceptor:]_block"
 },
 {
  "address": "0x9F00278",
  "name": "-[NSObject validatedArrayOfStrings]_0_block"
 },
...
```

```
 {
  "address": "0xA2BF6E4",
  "name": "-[UIScrollView dzn_reloadEmptyDataSet]_block"
 },
 {
  "address": "0x463F778",
  "name": "-[AppsFlyerLib callServerWithEventName:eventValues:options:completion:]_block_block"
 },
 {
  "address": "0xBE3F7B8",
  "name": "-[UITableView fd_insertRowsAtIndexPaths:withRowAnimation:]_block"
 },
 {
  "address": "0x463F7F0",
  "name": "-[AppsFlyerLib callServerWithEventName:eventValues:options:completion:]_block"
 },
 {
  "address": "0xBE3F878",
  "name": "-[UITableView fd_insertRowsAtIndexPaths:withRowAnimation:]_block_block"
 },
 {
  "address": "0xBE3FB20",
  "name": "-[UITableView fd_deleteRowsAtIndexPaths:withRowAnimation:]_block"
 },
 {
  "address": "0x74FFBA4",
  "name": "-[UIImageView p_loadImageURLs:placeholder:options:isReloadURL:size:userID:hitImageInCache:enabledOptimisation:enableDemotionImage:completion:]_block"
 },
 {
  "address": "0xBE3FC7C",
  "name": "-[UITableView fd_deleteRowsAtIndexPaths:withRowAnimation:]_block"
 },
 {
  "address": "0xBE3FD6C",
  "name": "-[UITableView fd_deleteRowsAtIndexPaths:withRowAnimation:]_block_block"
 },
 {
  "address": "0xD8FFEB8",
  "name": "+[APMAnalytics logInternalEventWithOrigin:name:timestamp:parameters:]_block"
 },
 {
  "address": "0xD8FFF30",
  "name": "+[APMAnalytics logEventWithOrigin:isPublicEvent:name:parameters:]_block"
 },
 {
  "address": "0xBE3FF9C",
  "name": "-[UITableView fd_reloadRowsAtIndexPaths:withRowAnimation:]_block"
 }
]
```



```json
[
  {
    "address": "0x5F4000C",
    "name": "-[UIView makeToastActivity:]_block"
  },
  {
    "address": "0xD900034",
    "name": "+[APMAnalytics logEventWithOrigin:isPublicEvent:name:parameters:]_block_block"
  },
  {
    "address": "0xBE4005C",
    "name": "-[UITableView fd_reloadRowsAtIndexPaths:withRowAnimation:]_block_block"
  },
  {
    "address": "0x5F40120",
    "name": "-[UIView hideToastActivity]_block"
  },
  {
    "address": "0x5F40130",
    "name": "-[UIView hideToastActivity]_block"
  },
  {
    "address": "0xD9001BC",
    "name": "+[APMAnalytics logEventWithOrigin:isPublicEvent:name:parameters:timestamp:ignoreEnabled:ignoreInterceptor:]_block"
  },
  {
    "address": "0x9F00278",
    "name": "-[NSObject validatedArraryOfStrings]_0_block"
  },
  {
    "address": "0xA0C0310",
    "name": "-[WKUserContentController bdw_installHookAjax]_block"
  },
  {
    "address": "0xBE40354",
    "name": "-[UITableView fd_moveRowAtIndexPath:toIndexPath:]_block"
  },
  {
    "address": "0xA0C038C",
    "name": "-[WKUserContentController bdw_installHookAjax]_block"
  },
  {
    "address": "0xD9004AC",
    "name": "+[APMAnalytics setDefaultEventParameters:]_block"
  },
  {
    "address": "0xAD4058C",
    "name": "-[LynxUI setVisibility:requestReset:]_block"
  },
  {
    "address": "0xD900688",
    "name": "+[APMAnalytics handleOpenURL:]_block"
```


restore-symbol
EXPLORER
RESTORE-SYMBOL
OUTLINE
TIMELINE
ida_search_block.py 9+, M
block_symbol.json
Start analyze binary for iOS Untitled-1
Start analyze binary for iOS Untitled-2
Users > crifan > dev > dev_root > iosReverse > tiktok > ipa > Payload > TikTok.app > Frameworks > MusicallyCore.framework > block_symbol.json > { } 1529
master* ⊗ 0 ⚠ 31 ⚐ 0
Ln 6118, Col 3 Spaces: 2 UTF-8 LF { } JSON

```json
    "name": "-[UITableView fd_moveSection:toSection:]_block"
  },
  {
    "address": "0xA2BF6E4",
    "name": "-[UIScrollView dzn_reloadEmptyDataSet]_block"
  },
  {
    "address": "0x463F778",
    "name": "-[AppsFlyerLib callServerWithEventName:eventValues:options:completion:]_block_block"
  },
  {
    "address": "0xBE3F7B8",
    "name": "-[UITableView fd_insertRowsAtIndexPaths:withRowAnimation:]_block"
  },
  {
    "address": "0x463F7F0",
    "name": "-[AppsFlyerLib callServerWithEventName:eventValues:options:completion:]_block"
  },
  {
    "address": "0xBE3F878",
    "name": "-[UITableView fd_insertRowsAtIndexPaths:withRowAnimation:]_block_block"
  },
  {
    "address": "0xBE3FB20",
    "name": "-[UITableView fd_deleteRowsAtIndexPaths:withRowAnimation:]_block"
  },
  {
    "address": "0x74FFBA4",
    "name": "-[UIImageView p_loadImageURLs:placeholder:options:isReloadURL:size:userID:hitImageInCache:enabledOptimisation:enableDemotionImage:completion:]_block"
  },
  {
    "address": "0xBE3FC7C",
    "name": "-[UITableView fd_deleteRowsAtIndexPaths:withRowAnimation:]_block"
  },
  {
    "address": "0xBE3FD6C",
    "name": "-[UITableView fd_deleteRowsAtIndexPaths:withRowAnimation:]_block_block"
  },
  {
    "address": "0xD8FFEB8",
    "name": "+[APMAnalytics logInternalEventWithOrigin:name:timestamp:parameters:]_block"
  },
  {
    "address": "0xD8FFF30",
    "name": "+[APMAnalytics logEventWithOrigin:isPublicEvent:name:parameters:]_block"
  },
  {
    "address": "0xBE3FF9C",
    "name": "-[UITableView fd_reloadRowsAtIndexPaths:withRowAnimation:]_block"
  }
]
```

用restore-symbol恢复ObjC+block符号表

此处，想要一次性恢复ObjC和Block的符号表，则用 `-j` 参数即可

举例说明：

YouTube

```
/Users/crifan/dev/DevSrc/iOS/symbol/restore-symbol/HeiTanBc/restore-symbol/restore-symbol YouTube -o YouTube_objcBlockSymbol -j
 block_symbol.json
```

Module_Framework

```
/Users/crifan/dev/DevSrc/iOS/symbol/restore-symbol/HeiTanBc/restore-symbol/restore-symb
ol Module_Framework -o Module_Framework_objcBlockSymbol -j block_symbol.json
```

RzGame

```
cd ~/dev/dev_root/iosReverse/undecember/ipa/Payload/RzGame.app

✘ crifan@licrifandeMacBook-Pro⌜ ~/dev/dev_root/iosReverse/undecember/ipa/Payload/RzGame
.app⌜ /Users/crifan/dev/dev_src/ios_reverse/symbol/restore-symbol/HeiTanBc/restore-symb
ol/restore-symbol RzGame_addSymbol -o RzGame_addedAllSymbol -j block_symbol.json
=========== Start =============
Scan OC method in mach-o-file.
Scan OC method finish.
restore 28136 symbols
Parse symbols in json file.
Parse finish.
=========== Finish ============
```

crifan版restore-symbol

用crifan版restore-symbol恢复符号表：

- 核心步骤
    - 用IDA脚本（exportIDASymbol.py）从IDA中导出符号表
        - 导出之前
            - 优化变量名=符号名称
                - 自动
                    - 用crifan的IDA脚本AutoRename，自动优化函数名=符号名
                - 手动
                    - 经过（静态或动态）分析代码逻辑后，给函数名等重新命名，优化函数名=符号名称
    - 用crifan版restore-symbol去恢复符号表（导入符号表）

常见问题

Address not found in the image

- 现象

去用：

```
/Users/crifan/dev/DevSrc/iOS/symbol/restore-symbol/HeiTanBc/restore-symbol/restore-symbol YouTube -o YouTube_objcBlockSymbol -j
 block_symbol.json
```

去恢复Block符号表，但报错：

```
2022-04-20 20:35:09.565 restore-symbol[17780:328585] Address(100eaf5a8) not found in the image
```

- 原因

block的符号表的输入文件中，包含无效的地址的条目

```
{
  "name": "-[YTYouTubeUserDefaultsKeysProvider userSpecificSettingKeys]_block",
  "address": "0x100EAF5A8"
 },
```

其中的： `0x100EAF5A8` 无法识别

解决办法：

删除这个条目，另存为新的json文件，（比如 `block_symbol_removedInvalid.json` ）再重新执行

```
/Users/crifan/dev/DevSrc/iOS/symbol/restore-symbol/HeiTanBc/restore-symbol/restore-symbol YouTube -o YouTube_objcBlockSymbol -j block_symbol_removedInvalid.json
```

附录

下面列出相关参考资料。

参考资料

- 【未解决】iOS逆向WhatsApp：+[WAURLQueryItem queryItemWithName:value:]
- 【未解决】iOS逆向WhatsApp：SharedModules中的函数加不上如何加上断点且确保能触发
- 【整理】抖音AwemeCore恢复符号表的效果举例
- 【记录】用MachOView对比AwemeCore恢复符号表前后的Symbol变化
- 【记录】用IDA分析加了符号表的抖音AwemeCore二进制
- 【整理】抖音AwemeCore恢复符号表的效果举例
- 【已解决】抖音AwemeCore恢复符号表后导致部分函数显示错乱
- 【已解决】Xcode的lldb调试恢复符号表后的抖音AwemeCore
- 【已解决】restore-symbol给抖音AwemeCore恢复符号表无效
- 【已解决】restore-symbol恢复YouTube的Block符号表报错：Address not found in the image
- 【已解决】用HeiTanBc的restore-symbol去给抖音AwemeCore恢复符号表
- 【已解决】新旧版本HeiTanBc/restore-symbol有何区别和不同
- 【记录】完全用官网版本的HeiTanBc/restore-symbol去给WhatsApp恢复符号表
- 【已解决】iOS逆向WhatsApp：给WhatsApp的普通ObjC函数去恢复符号表
- 【未解决】用restore-symbol给TikTok恢复符号表
- 【未解决】给Tiktok的Block去恢复符号表
- 【已解决】给YouTube恢复符号表方便Xcode调试
- 【未解决】iOS逆向Apple账号：给iOS 15.1的CFNetwork恢复符号表
- 【未解决】iOS逆向AppleStore：恢复符号表
- 【已解决】iOS逆向游戏Undecember：恢复符号表
-