目录

可执行文件格式：Mach-O

- 最新版本： `v1.0.1`
- 更新时间： `20240325`

简介

介绍Mac和iOS等Apple苹果系统的常见可执行文件格式：Mach-O；先是Mach-O概览；包括背景知识的XNU、PIC等；然后介绍Mach-O格式，包括结构概述和结构图，以及结构详情，包括Header、Load Commands和Segment的data；其中Header包括magic、cputype和cpusubtype、filetype、flags；Load Commands包括LC_UUID、LC_SEGMENT、LC_SEGMENT_64、LC_SYMTAB、LC_DYLD_CHAINED_FIXUPS、LC_DYLD_EXPORTS_TRIE等；Segment包括**TEXT**、DATA、**IMPORT**、LINKEDIT、__OBJC；以及各个Segment的section，比如symbol、strings等；然后是Mach-O格式的子项，包括FAT、codesign、虚拟地址、大小限制等；然后整理Mach-O的各种工具，包括MachOView、rabin2、jtool2、otool、pagestuff，以及每个工具的用法、举例、help语法等；

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/exec_file_format_macho: 可执行文件格式：Mach-O

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

- 可执行文件格式：Mach-O book.crifan.org
- 可执行文件格式：Mach-O crifan.github.io

离线下载阅读

- 可执行文件格式：Mach-O PDF
- 可执行文件格式：Mach-O ePub
- 可执行文件格式：Mach-O Mobi

版权和用途说明

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

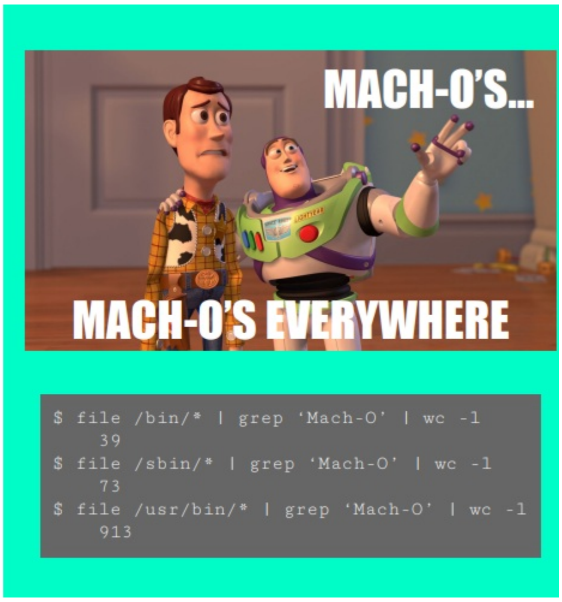
关于作者

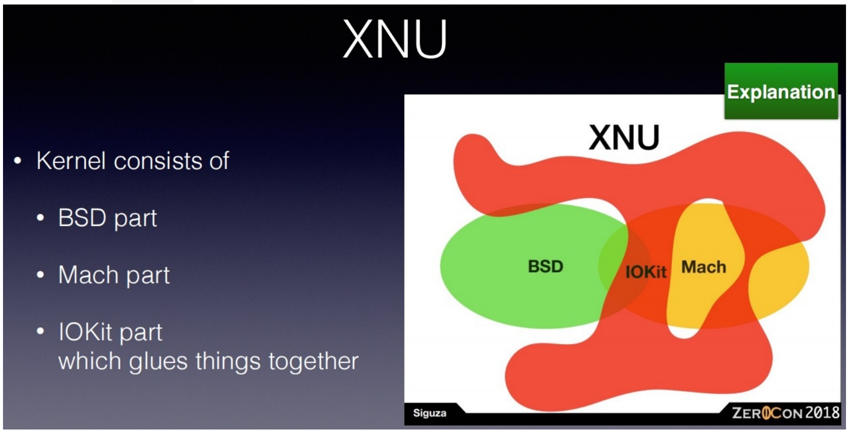
关于作者更多介绍，详见：

关于CrifanLi李茂 – 在路上

Mach-O概览

- `Mach-O`
  - `Mach-O = Mach Object = Mach Object file format`
  - 是什么： `Mac` 和 `iOS` 等 `Apple` 平台中的可执行文件格式
    - 



  - 名词解释
    - `Mach-O` = `Mach` + `O`
      - `Mach`
        - iOS的内核是 `XNU`
          - `XNU` 由多个部分组成
            - 其中一部分是 `Mach` 微内核microkernel
              - 

      - `O = Object` =对象
  - 用到 `Mach-O` 的系统
    - `Mach kernel`
    - `NeXTSTEP`
    - `macOS`
    - `iOS`

Mach-O背景知识

XNU

- `XUN`
    - 名称
        - `XNU` = **X** is **N**ot **U**nix
    - 概述
        - 英文
            - XNU kernel is part of the Darwin operating system for use in macOS and iOS operating systems.
        - 中文
            - XNU是：iOS（和tvOS、watchOS）的（操作系统）内核
            - XNU也是Darwin的一部分
                - Darwin是MacOS的操作系统内核
    - 特点
        - XNU is a hybrid kernel combining the Mach kernel developed at Carnegie Mellon University with components from FreeBSD and a C++ API for writing drivers called IOKit. XNU runs on x86_64 for both single processor and multi-processor configurations.
    - （开源代码）源码
        - opensource.apple.com
            - Source Browser (apple.com)
        - Github
            - https://github.com/apple/darwin-xnu
                - apple/darwin-xnu: The Darwin Kernel (mirror)
    - XNU组成
        - 2个主要部分
            - Mach：微内核=microkernel
                - 实现了操作系统的核心部分
            - BSD：内核=kernel
                - BSD在Mach的基础上，实现了更高层的各种功能
    - 代码组成=代码树
        - `config` - configurations for exported apis for supported architecture and platform
        - `SETUP` - Basic set of tools used for configuring the kernel, versioning and kextsymbol management.
        - `EXTERNAL_HEADERS` - Headers sourced from other projects to avoid dependency cycles when building. These headers should be regularly synced when source is updated.
        - `libkern` - C++ IOKit library code for handling of drivers and kexts.
        - `libsa` - kernel bootstrap code for startup
        - `libsyscall` - syscall library interface for userspace programs
        - `libkdd` - source for user library for parsing kernel data like kernel chunked data.
        - `makedefs` - top level rules and defines for kernel build.
        - `osfmk` - Mach kernel based subsystems
        - `pexpert` - Platform specific code like interrupt handling, atomics etc.
        - `security` - Mandatory Access Check policy interfaces and related implementation.
        - `bsd` - BSD subsystems code

- `tools` - A set of utilities for testing, debugging and profiling kernel.

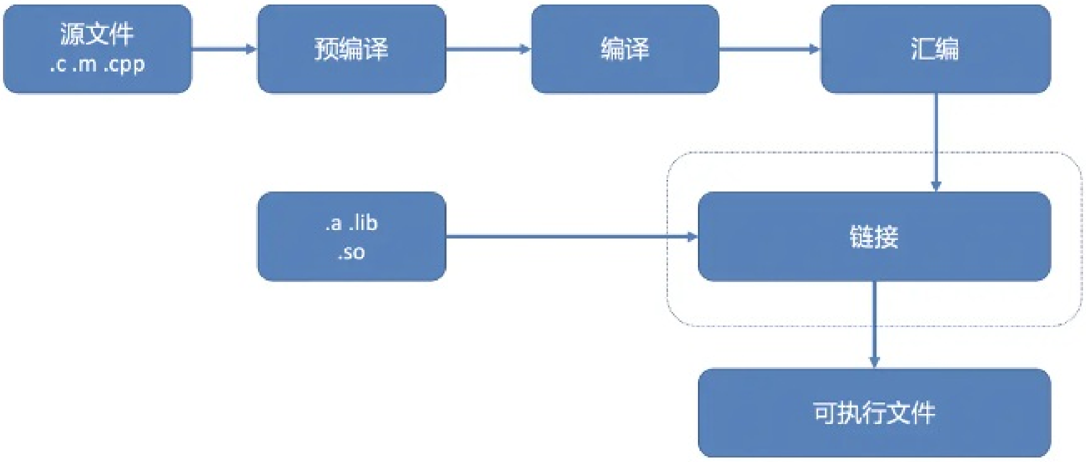
查看系统信息中会有XNU的版本等信息

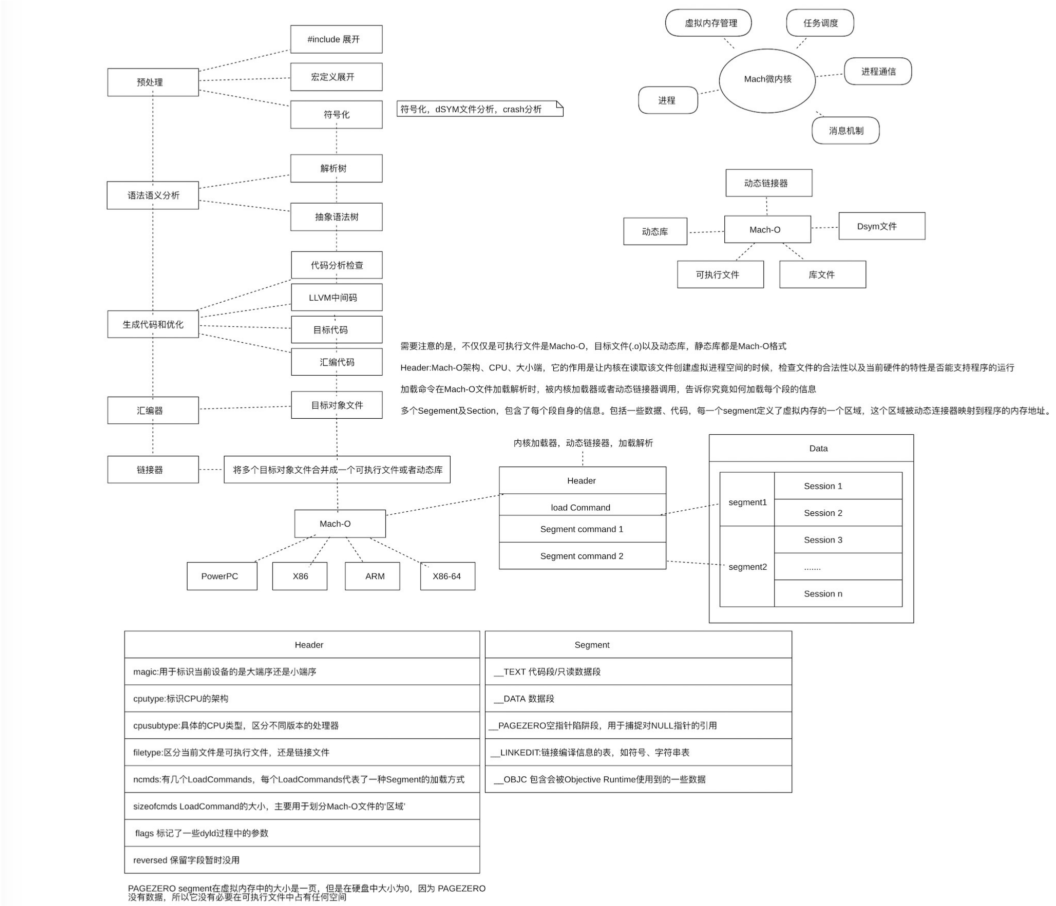
- iOS 15.1，iPhone8的信息

```
iPhone8-150:~ root# uname -a
Darwin iPhone8-150 21.0.0 Darwin Kernel Version 21.0.0: Sun Aug 15 20:55:55 PDT 2021
; root:xnu-8019.12.5~1/RELEASE_ARM64_T8015 iPhone10,1 arm Darwin
```

  - `xnu-8019.12.5~1/RELEASE_ARM64_T8015`
    - xnu是：iOS的内核
      - 版本是：8019.12.5

编译链接加载过程

- 编译链接加载过程
  - 概述
    - 

  - 详解
    - 

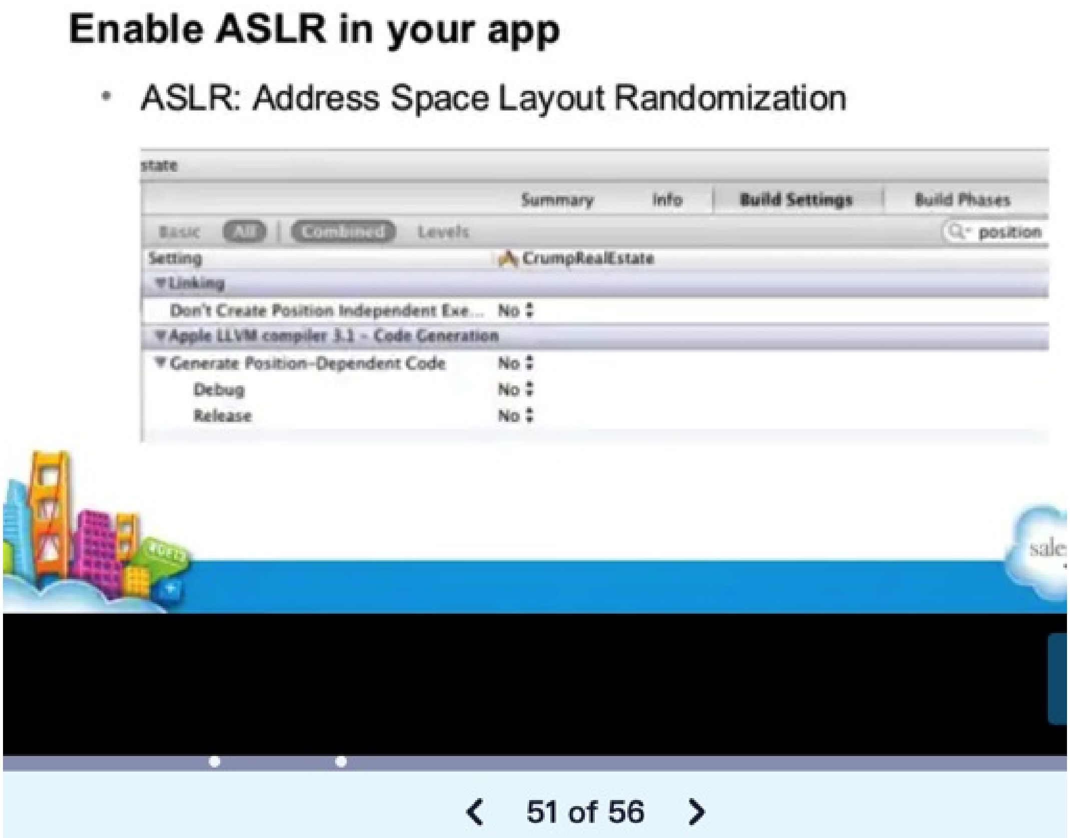
PIC

- `PIC` = `Position-Independent Code` = `位置无关代码`
  - 详解
    - 位置无关代码（PIC）是 PowerPC 环境中使用的代码生成技术的名称，该技术允许动态链接器在非固定虚拟内存地址加载代码区域。如果没有某种形式的与位置无关的代码生成，操作系统将需要将您想要共享的所有代码放置在虚拟内存中的固定地址，这将使操作系统的维护变得非常困难。例如，支持共享库和框架几乎是不可能的，因为每个库和框架都需要预先分配一个永远不会改变的地址。
    - `Mach-O` 与位置无关的代码设计基于这样的观察：`__DATA` 段始终位于距 `__TEXT` 段恒定的偏移处。也就是说，动态加载器在加载任何 `Mach-O` 文件时，绝不会相对于其 `__DATA` 段移动文件的 `__TEXT` 段。因此，函数可以使用自己的当前地址加上固定偏移量来确定它希望访问的数据的位置。`Mach-O` 文件的所有段（不仅是 `__TEXT` 和 `__DATA` 段）相对于其他段的偏移量是固定的。
  - 官网文档
    - Position-Independent Code
  - 对比
    - `Mach-O` 的 `PIC` ~= ELF的 `GOT`
      - 区别：Mach-O 代码使用直接偏移引用数据，而 ELF 通过全局偏移表间接访问所有数据。
  - `PIC`
    - ~= `PIE` = `Position-Independent Executable`
      - 对应的Mach-O中有个flag是：`MH_PIE`
    - ~= `ASLR`

ASLR

- `ASLR` = `Address Space Layout Randomization` = `地址空间布局随机化`

参考：



去尝试给iOS的app去开启ASLR：

- Linking->Generate Position-Dependent Executable
    -
- Apple Clang - Code Generation->Generate Position-Dependent Code

-

结果：

编译都会报错：

```
ld: -no_pie and -bitcode_bundle (Xcode setting ENABLE_BITCODE=YES) cannot be used toget
her

Showing All Messages
-no_pie and -bitcode_bundle (Xcode setting ENABLE_BITCODE=YES) cannot be used together
```

看起来是和BITCODE的 `ENABLE_BITCODE=YES` 相冲突了。

所以暂时放弃深究。

后记：

上述的：

`Position-Dependent Executable` 和 `Generate Position-Dependent Code`

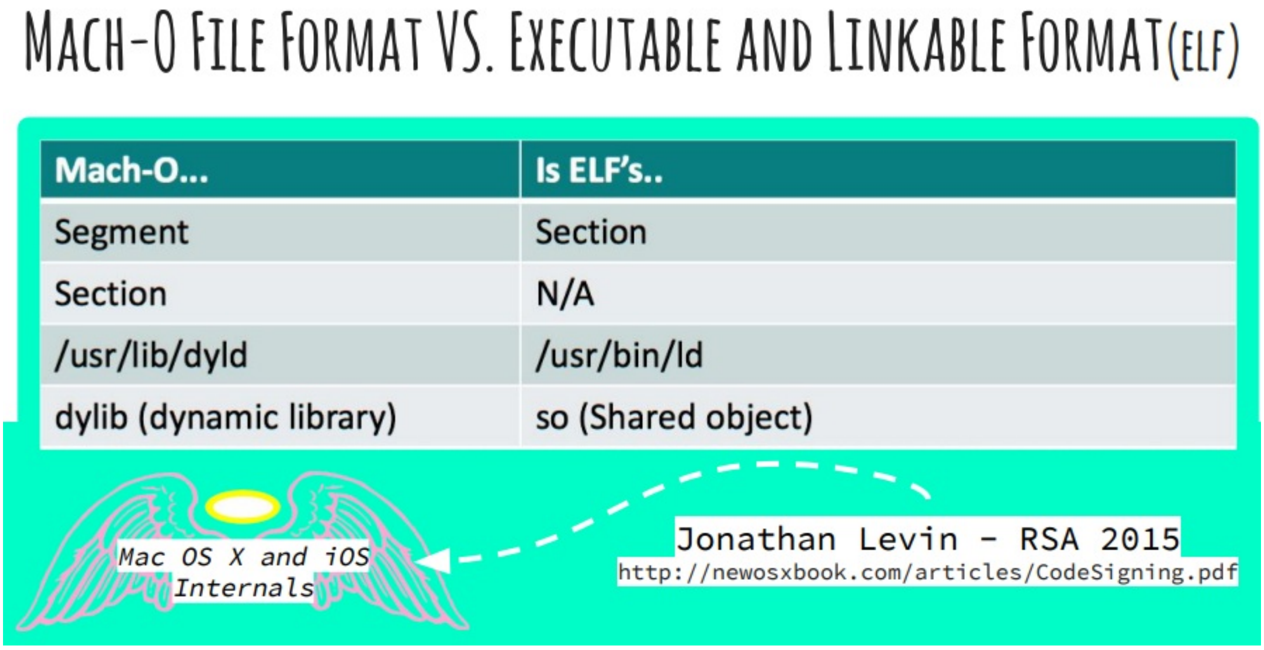
很明显是：要关闭 `ASLR` = `PIC` = `PIE` 的意思啊

所以感觉是：

- `ASLR` = `PIC` = `PIE` ：默认已开启
  - 如果想要去**关闭**ALSR，才需要去更改设置，改为
    - Linking->Generate Position-Dependent Executable = `YES`
    - Apple Clang - Code Generation->Generate Position-Dependent Code = `YES`

Mach-O格式

Mach-O vs ELF

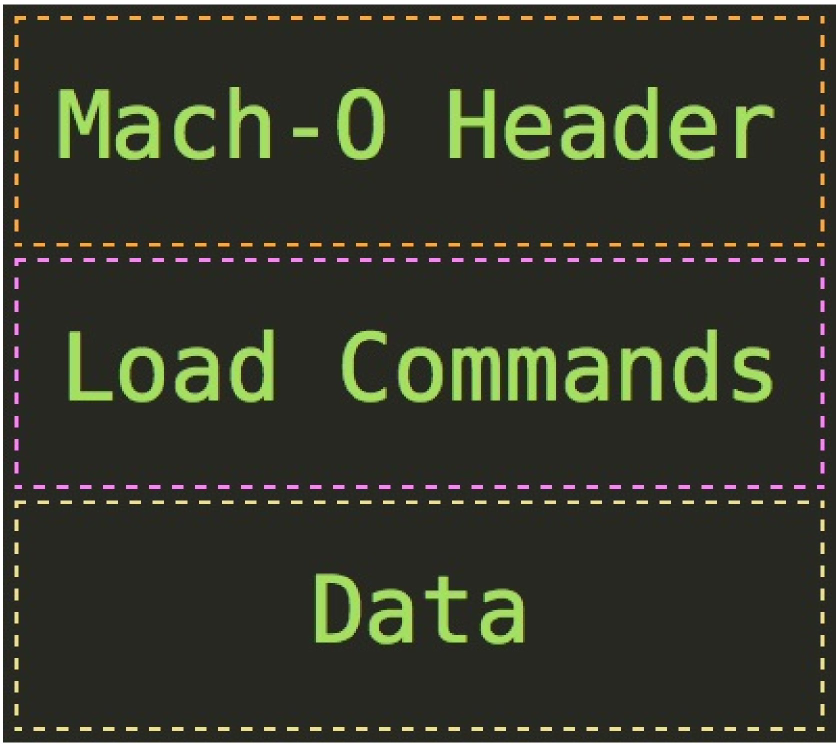


Mach-O结构概述

- Mach-O基本结构
  - `Header` ：文件类型、目标架构类型等
  - `Load Commands` ：描述文件在虚拟内存中的逻辑结构、布局
  - (Raw segment) `data` ：在Load commands中定义的Segment的原始数据
    - 一个或多个segment=段
      - 每个segment包含 一个或多个 section=节
        - 每个section包含 （某种类型的）代码 或 数据

Mach-O结构图

概览

- 

普通单架构 vs FAT多架构

- 普通：单架构 = Mach-O文件

    -

- 特殊：多架构= `FAT` =Universal通用文件

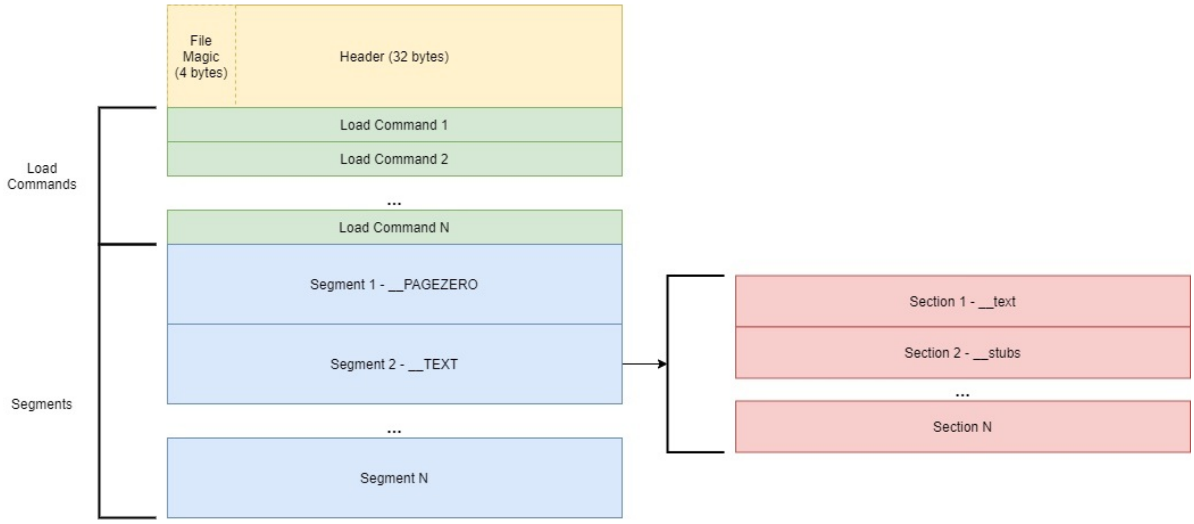
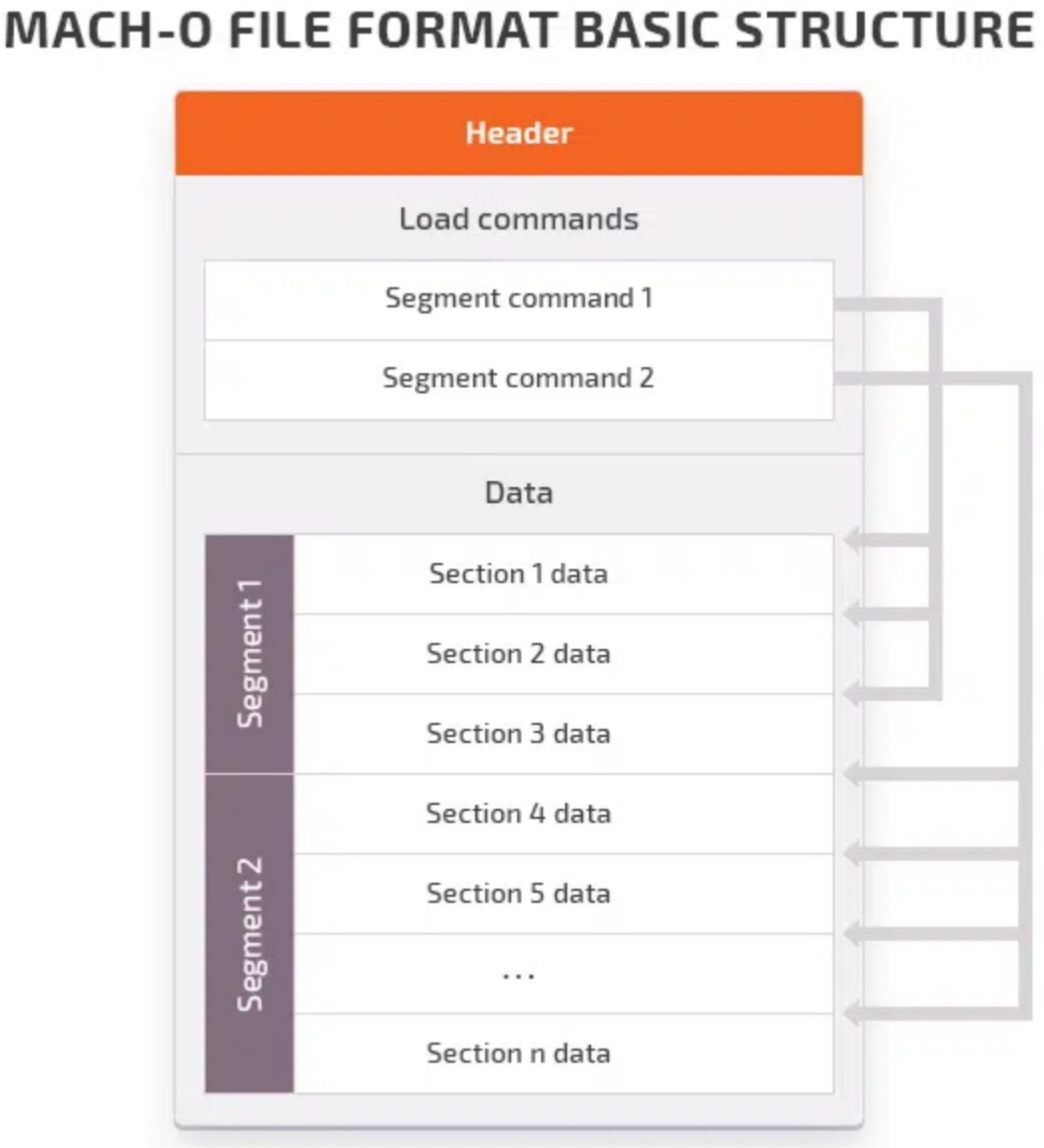
-
- 文字版

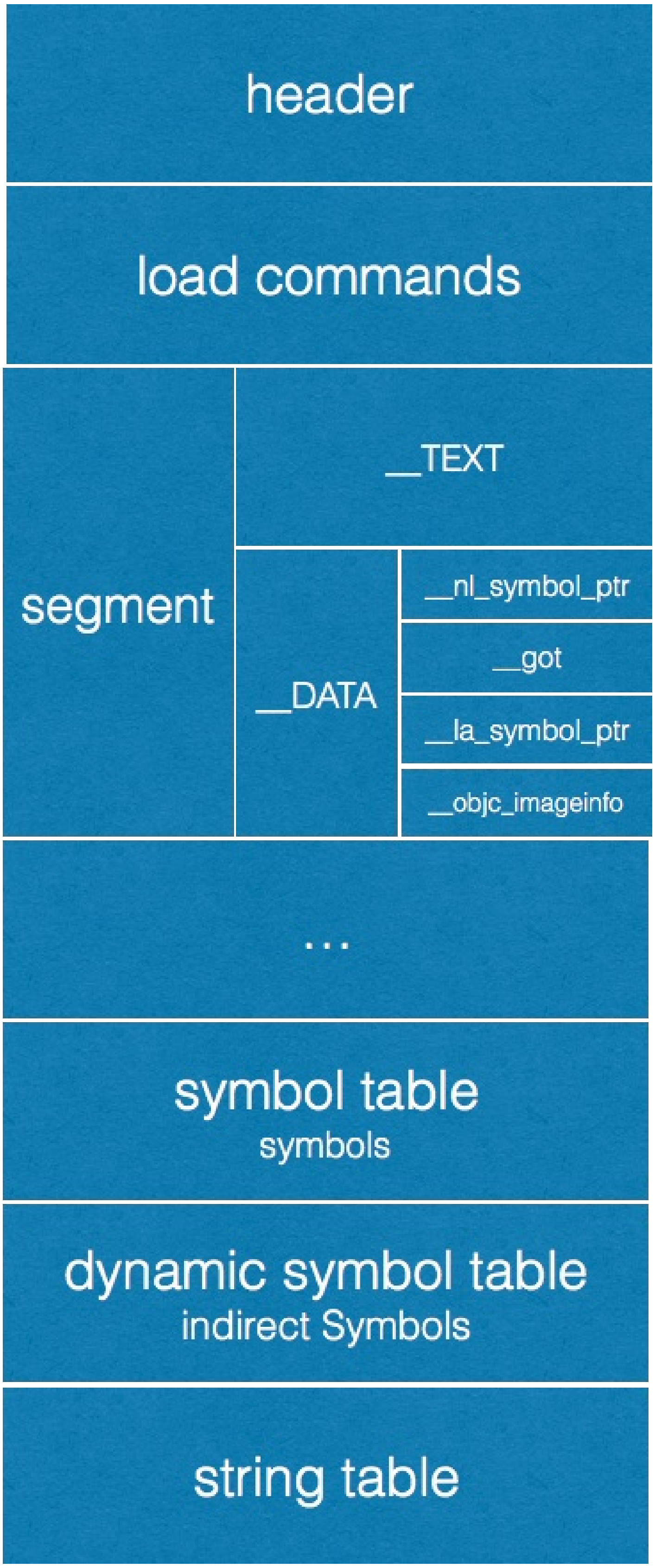
```
+---------------------+       /* header (fat_header: 0x8) */
|                     |
|     FAT HEADER      |
|                     |
```

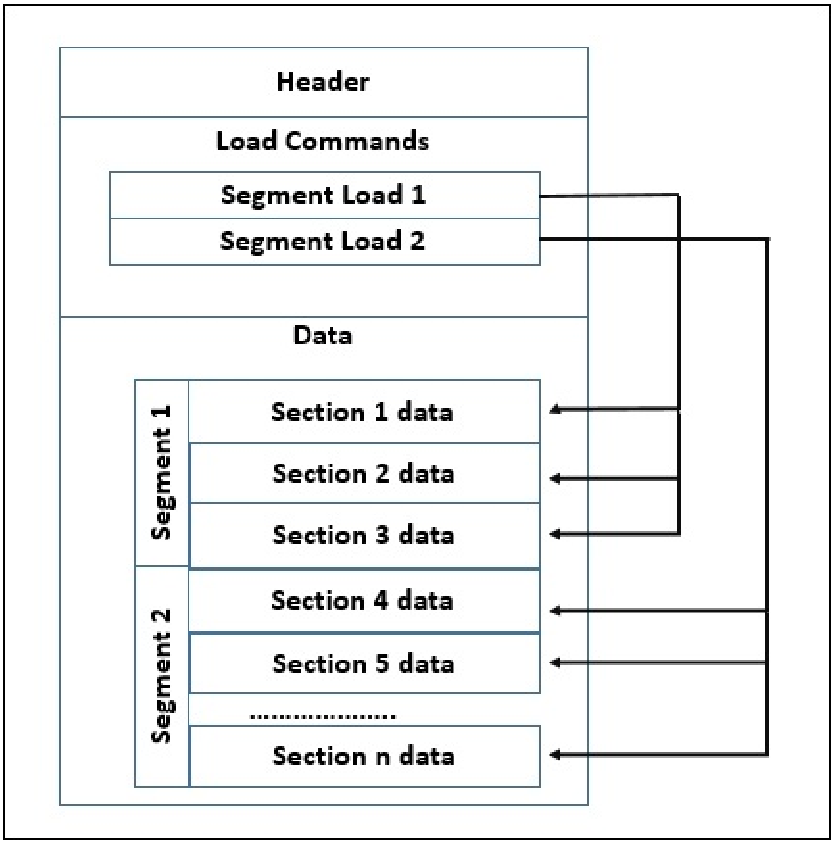
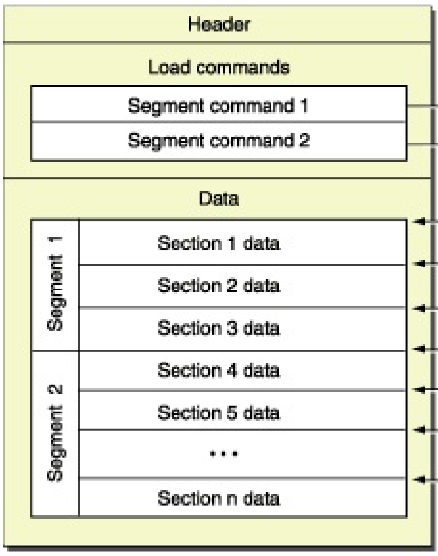
```
+--------------------+       /* archs (fat_arch: 0x14) */
|     FAT ARCH #1    |
+--------------------+
|     FAT ARCH #2    |
+--------------------+
|        ...         |       /* other eventual fat archs... */
+--------------------+       /* Mach-Os section (variable size) */
|                    |
|                    |
|                    |
|                    |
|      MACH-O #1     |
|                    |
|                    |
|                    |
|                    |
|                    |
+--------------------+
|                    |
|                    |
|                    |
|                    |
|                    |
|      MACH-O #2     |
|                    |
|                    |
|                    |
|                    |
+--------------------+
|        ...         |       /* other eventual Mach-Os... */
+--------------------+
```

详解

- 带字段的Mach-O结构图
    -

- 
File
Magic
(4 bytes)
Header (32 bytes)
Load Commands
Load Command 1
Load Command 2
...
Load Command N
Segments
Segment 1 - __PAGEZERO
Segment 2 - __TEXT
...
Segment N
Section 1 - __text
Section 2 - __stubs
...
Section N
- 
MACH-O FILE FORMAT BASIC STRUCTURE
Header
Load commands
Segment command 1
Segment command 2
Data
Segment 1
Segment 2
Section 1 data
Section 2 data
Section 3 data
Section 4 data
Section 5 data
...
Section n data

- 
header
load commands
segment
__TEXT
__DATA
__nl_symbol_ptr
__got
__la_symbol_ptr
__objc_imageinfo
...
symbol table
symbols
dynamic symbol table
indirect Symbols
string table

- 
Header
Load Commands
Segment Load 1
Segment Load 2
Data
Segment 1
Section 1 data
Section 2 data
Section 3 data
Segment 2
Section 4 data
Section 5 data
Section n data
- 
Header
Load commands
Segment command 1
Segment command 2
Data
Segment 1
Section 1 data
Section 2 data
Section 3 data
Segment 2
Section 4 data
Section 5 data
...
Section n data

Mach-O结构详情

Mach-O详细定义

相关源码

- Mach-O详细定义
  - 相关源码
    - xnu源码
      - https://opensource.apple.com/tarballs/xnu/
        - `EXTERNAL_HEADERS/mach-o/fat.h`
        - `EXTERNAL_HEADERS/mach-o/loader.h`
          - 举例
            - https://opensource.apple.com/source/xnu/xnu-2050.18.24/EXTERNAL_HEADERS/mach-o/loader.h

Mach-O的Header

Mach-O的Header结构图

- Header的详细定义
    -
- MachOView显示Mach-O的Header举例
    -
        - 说明
            - 该文件是可执行文件
            - 文件的构架是x86_64
            - number of Load commands表示有74个load commond
            - MH_TWOLEVEL二级名字空间
            - `MH_PIE` 随机地址空间
- Mach-O Core Dump File Structure

-
    -
- 内存映射 = 结构体偏移 = 结构体字段

mach_header定义

- 精简定义

```
struct mach_header {
  uint32_t        magic;
  cpu_type_t      cputype;
  cpu_subtype_t cpusubtype;
  uint32_t        filetype;
  uint32_t        ncmds;
  uint32_t        sizeofcmds;
  uint32_t        flags;
};
```

- 详细定义

源码定义：

```
/*
 * The 32-bit mach header appears at the very beginning of the object file for
 * 32-bit architectures.
 */
struct mach_header {
    uint32_t    magic;        /* mach magic number identifier */
    cpu_type_t    cputype;    /* cpu specifier */
    cpu_subtype_t    cpusubtype;    /* machine specifier */
    uint32_t    filetype;    /* type of file */
    uint32_t    ncmds;        /* number of load commands */
    uint32_t    sizeofcmds;    /* the size of all the load commands */
    uint32_t    flags;        /* flags */
};

/* Constant for the magic field of the mach_header (32-bit architectures) */
#define    MH_MAGIC    0xfeedface    /* the mach magic number */
#define MH_CIGAM    0xcefaedfe    /* NXSwapInt(MH_MAGIC) */

/*
 * The 64-bit mach header appears at the very beginning of object files for
 * 64-bit architectures.
 */
struct mach_header_64 {
    uint32_t    magic;        /* mach magic number identifier */
    cpu_type_t    cputype;    /* cpu specifier */
    cpu_subtype_t    cpusubtype;    /* machine specifier */
    uint32_t    filetype;    /* type of file */
    uint32_t    ncmds;        /* number of load commands */
    uint32_t    sizeofcmds;    /* the size of all the load commands */
    uint32_t    flags;        /* flags */
    uint32_t    reserved;    /* reserved */
};

/* Constant for the magic field of the mach_header_64 (64-bit architectures) */
#define MH_MAGIC_64 0xfeedfacf /* the 64-bit mach magic number */
#define MH_CIGAM_64 0xcffaedfe /* NXSwapInt(MH_MAGIC_64) */
```

Mach-O的Header的magic

- `magic` = `魔数`

源码定义：

```
/* Constant for the magic field of the mach_header (32-bit architectures) */
#define MH_MAGIC        0xfeedface      /* the mach magic number */
#define MH_CIGAM        0xcefaedfe      /* NXSwapInt(MH_MAGIC) */

/* Constant for the magic field of the mach_header_64 (64-bit architectures) */
#define MH_MAGIC_64 0xfeedfacf /* the 64-bit mach magic number */
#define MH_CIGAM_64 0xcffaedfe /* NXSwapInt(MH_MAGIC_64) */
```

->

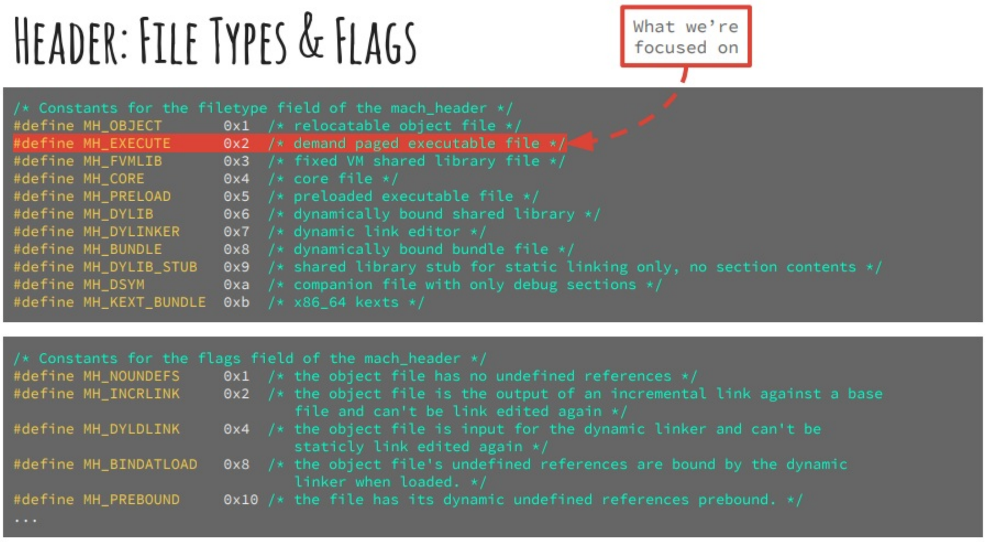
- magic
  - 通用格式： `0xcafebabe`
  - （ `armv7` 等）32bit： `0xfeedface`
  - （ `arm64` 等）64bit： `0xfeedfacf`

cputype和cpusubtype

- CPU架构
    - `armv7` 等32bit
        - cputype = 12, cpusubtype=9
    - `arm64` 等64bit
        - cputype = 1677228, cpusubtype = 0

Mach-O的Header的filetype

常见文件类型filetype

- Mach-O的filetype
    - 文件类型概述：Executables, bundles, dylibs, kexts, cores等等
    - 常见文件类型
        - `MH_EXECUTE` =可执行文件= `executable` =应用
            - 文件： `.app/xxx`
            - 

        - `MH_OBJECT`
            - 目标文件
                - 文件： `.o`
            - 静态库文件=静态链接库= `static library` ：N个 `.o` 合并在一起
                - 文件： `.a`
        - `MH_DYLIB` =动态链接库= `dylib library` ：类似于Win中的 `DLL`
            - 文件： `.dylib` 、 `.framework/xxx`
        - `MH_DYLINKER` ：动态链接编辑器
            - 文件： `/usr/lib/dyld`
        - `MH_DSYM` ：存储着二进制文件符号信息的文件
            - 文件： `.dSYM/Contents/Resources/DWARF/xxx`
                - 常用于分析APP的崩溃信息
                    - 调试信息保存在：dSYM文件

全部文件类型解释

- 全部文件类型解释
    - `MH_OBJECT`
        - The MH_OBJECT file type is the format used for intermediate object files. It is a very compact format containing all its sections in one segment. The compiler and assembler usually create one MH_OBJECT file for each source code file. By convention, the file name

extension for this format is .o.

- `MH_EXECUTE`
  - The MH_EXECUTE file type is the format used by standard executable programs.
- `MH_BUNDLE`
  - The MH_BUNDLE file type is the type typically used by code that you load at runtime (typically called bundles or plug-ins). By convention, the file name extension for this format is .bundle.
- `MH_DYLIB`
  - The MH_DYLIB file type is for dynamic shared libraries. It contains some additional tables to support multiple modules. By convention, the file name extension for this format is .dylib, except for the main shared library of a framework, which does not usually have a file name extension.
- `MH_PRELOAD`
  - The MH_PRELOAD file type is an executable format used for special-purpose programs that are not loaded by the OS X kernel, such as programs burned into programmable ROM chips. Do not confuse this file type with the MH_PREBOUND flag, which is a flag that the static linker sets in the header structure to mark a prebound image.
- `MH_CORE`
  - The MH_CORE file type is used to store core files, which are traditionally created when a program crashes. Core files store the entire address space of a process at the time it crashed. You can later run gdb on the core file to figure out why the crash occurred.
- `MH_DYLINKER`
  - The MH_DYLINKER file type is the type of a dynamic linker shared library. This is the type of the dyld file.
- `MH_DSYM`
  - The MH_DSYM file type designates files that store symbol information for a corresponding binary file.

filetype的定义

-
```
#define MH_OBJECT   0x1     /* relocatable object file */
#define MH_EXECUTE  0x2     /* demand paged executable file */
#define MH_FVMLIB   0x3     /* fixed VM shared library file */
#define MH_CORE     0x4     /* core file */
#define MH_PRELOAD  0x5     /* preloaded executable file */
#define MH_DYLIB    0x6     /* dynamically bound shared library */
#define MH_DYLINKER 0x7     /* dynamic link editor */
#define MH_BUNDLE   0x8     /* dynamically bound bundle file */
#define MH_DYLIB_STUB   0x9     /* shared library stub for static */
                    /*  linking only, no section contents */
#define MH_DSYM     0xa     /* companion file with only debug */
                    /*  sections */
#define MH_KEXT_BUNDLE  0xb     /* x86_64 kexts */
```

源码定义：

```
/*
 * The layout of the file depends on the filetype.  For all but the MH_OBJECT
```

```
 * file type the segments are padded out and aligned on a segment alignment
 * boundary for efficient demand pageing.  The MH_EXECUTE, MH_FVMLIB, MH_DYLIB,
 * MH_DYLINKER and MH_BUNDLE file types also have the headers included as part
 * of their first segment.
 *
 * The file type MH_OBJECT is a compact format intended as output of the
 * assembler and input (and possibly output) of the link editor (the .o
 * format).  All sections are in one unnamed segment with no segment padding.
 * This format is used as an executable format when the file is so small the
 * segment padding greatly increases its size.
 *
 * The file type MH_PRELOAD is an executable format intended for things that
 * are not executed under the kernel (proms, stand alones, kernels, etc).  The
 * format can be executed under the kernel but may demand paged it and not
 * preload it before execution.
 *
 * A core file is in MH_CORE format and can be any in an arbritray legal
 * Mach-O file.
 *
 * Constants for the filetype field of the mach_header
 */
#define    MH_OBJECT    0x1        /* relocatable object file */
#define    MH_EXECUTE    0x2        /* demand paged executable file */
#define    MH_FVMLIB    0x3        /* fixed VM shared library file */
#define    MH_CORE        0x4        /* core file */
#define    MH_PRELOAD    0x5        /* preloaded executable file */
#define    MH_DYLIB    0x6        /* dynamically bound shared library */
#define    MH_DYLINKER    0x7        /* dynamic link editor */
#define    MH_BUNDLE    0x8        /* dynamically bound bundle file */
#define    MH_DYLIB_STUB    0x9        /* shared library stub for static */
                    /*  linking only, no section contents */
#define    MH_DSYM        0xa        /* companion file with only debug */
                    /*  sections */
#define    MH_KEXT_BUNDLE    0xb        /* x86_64 kexts */
```

Mach-O的Header的flags

flags含义解释

- `MH_NOUNDEFS`
    - The object file contained no undefined references when it was built.
- `MH_INCRLINK`
    - The object file is the output of an incremental link against a base file and cannot be linked again.
- `MH_DYLDLINK`
    - The file is input for the dynamic linker and cannot be statically linked again.
- `MH_TWOLEVEL`
    - The image is using two-level namespace bindings.
- `MH_BINDATLOAD`
    - The dynamic linker should bind the undefined references when the file is loaded.
- `MH_PREBOUND`
    - The file's undefined references are prebound.
- `MH_PREBINDABLE`
    - This file is not prebound but can have its prebinding redone. Used only when MH_PREBEOUND is not set.
- `MH_NOFIXPREBINDING`
    - The dynamic linker doesn't notify the prebinding agent about this executable.
- `MH_ALLMODSBOUND`
    - Indicates that this binary binds to all two-level namespace modules of its dependent libraries. Used only when MH_PREBINDABLE and MH_TWOLEVEL are set.
- `MH_CANONICAL`
    - This file has been canonicalized by unprebinding—clearing prebinding information from the file. See the redo_prebinding man page for details.
- `MH_SPLIT_SEGS`
    - The file has its read-only and read-write segments split.
- `MH_FORCE_FLAT`
    - The executable is forcing all images to use flat namespace bindings.
- `MH_SUBSECTIONS_VIA_SYMBOLS`
    - The sections of the object file can be divided into individual blocks. These blocks are dead-stripped if they are not used by other code. See Linking for details.
- `MH_NOMULTIDEFS`
    - This umbrella guarantees there are no multiple definitions of symbols in its subimages. As a result, the two-level namespace hints can always be used.

flags定义

- 

源码定义:

```
/* Constants for the flags field of the mach_header */
#define     MH_NOUNDEFS     0x1         /* the object file has no undefined
                        references */
#define     MH_INCRLINK     0x2         /* the object file is the output of an
                        incremental link against a base file
                        and can't be link edited again */
#define MH_DYLDLINK     0x4         /* the object file is input for the
                        dynamic linker and can't be staticly
                        link edited again */
#define MH_BINDATLOAD     0x8         /* the object file's undefined
                        references are bound by the dynamic
                        linker when loaded. */
#define MH_PREBOUND     0x10         /* the file has its dynamic undefined
                        references prebound. */
#define MH_SPLIT_SEGS     0x20         /* the file has its read-only and
                        read-write segments split */
#define MH_LAZY_INIT     0x40         /* the shared library init routine is
                        to be run lazily via catching memory
                        faults to its writeable segments
                        (obsolete) */
#define MH_TWOLEVEL     0x80         /* the image is using two-level name
                        space bindings */
#define MH_FORCE_FLAT     0x100         /* the executable is forcing all images
                        to use flat name space bindings */
#define MH_NOMULTIDEFS     0x200         /* this umbrella guarantees no multiple
                        defintions of symbols in its
                        sub-images so the two-level namespace
                        hints can always be used. */
#define MH_NOFIXPREBINDING 0x400     /* do not have dyld notify the
                        prebinding agent about this
                        executable */
#define MH_PREBINDABLE  0x800           /* the binary is not prebound but can
                        have its prebinding redone. only used
```

```
                                        when MH_PREBOUND is not set. */
#define MH_ALLMODSBOUND 0x1000          /* indicates that this binary binds to
                                        all two-level namespace modules of
                        its dependent libraries. only used
                        when MH_PREBINDABLE and MH_TWOLEVEL
                        are both set. */
#define MH_SUBSECTIONS_VIA_SYMBOLS 0x2000/* safe to divide up the sections into
                         sub-sections via symbols for dead
                         code stripping */
#define MH_CANONICAL     0x4000         /* the binary has been canonicalized
                        via the unprebind operation */
#define MH_WEAK_DEFINES     0x8000         /* the final linked image contains
                        external weak symbols */
#define MH_BINDS_TO_WEAK 0x10000     /* the final linked image uses
                        weak symbols */

#define MH_ALLOW_STACK_EXECUTION 0x20000/* When this bit is set, all stacks
                        in the task will be given stack
                        execution privilege.  Only used in
                        MH_EXECUTE filetypes. */
#define MH_ROOT_SAFE 0x40000           /* When this bit is set, the binary
                       declares it is safe for use in
                       processes with uid zero */

#define MH_SETUID_SAFE 0x80000         /* When this bit is set, the binary
                       declares it is safe for use in
                       processes when issetugid() is true */

#define MH_NO_REEXPORTED_DYLIBS 0x100000 /* When this bit is set on a dylib,
                       the static linker does not need to
                       examine dependent dylibs to see
                       if any are re-exported */
#define    MH_PIE 0x200000            /* When this bit is set, the OS will
                        load the main executable at a
                        random address.  Only used in
                        MH_EXECUTE filetypes. */
#define    MH_DEAD_STRIPPABLE_DYLIB 0x400000 /* Only for use on dylibs.  When
                          linking against a dylib that
                          has this bit set, the static linker
                          will automatically not create a
                          LC_LOAD_DYLIB load command to the
                          dylib if no symbols are being
                          referenced from the dylib. */
#define MH_HAS_TLV_DESCRIPTORS 0x800000 /* Contains a section of type
                         S_THREAD_LOCAL_VARIABLES */

#define MH_NO_HEAP_EXECUTION 0x1000000    /* When this bit is set, the OS will
                        run the main executable with
                        a non-executable heap even on
                        platforms (e.g. i386) that don't
                        require it. Only used in MH_EXECUTE
                        filetypes. */
```

Load Commands

- 概述
    - 位置：Load commands紧跟在Mach-O的Header之后
    - 作用：Load commands指定了文件的布局结构和链接特征
        - 有很多很多种Load commands
        - 这些加载指令清晰地告诉加载器如何处理二进制数据，有些命令是由内核处理的，有些是由动态链接器处理的

Load Commands类型介绍

- 概述
    - `LC_SEGMENT` ：被映射到内存的段
    - `LC_SYMTAB` ：符号表
    - `LC_DYSYMTAB` ：动态符号表
    - `LC_LOAD_DYLIB` ：动态链接库
- 详解
    - `LC_REQ_DYLD` = 0x8000_0000
        - 含义：After MacOS X 10.1 when a new load command is added that is required to be understood by the dynamic linker for the image to execute properly the LC_REQ_DYLD bit will be or'ed into the load command constant. If the dynamic linker sees such a load command it it does not understand will issue a "unknown load command required for execution" error and refuse to use the image. Other load commands without this bit that are not understood will simply be ignored.
    - `LC_SEGMENT` = 0x1
        - 数据结构定义： `segment_command`
        - 含义：segment of this file to be mapped
            - Defines a segment of this file to be mapped into the address space of the process that loads this file. It also includes all the sections contained by the segment.
    - `LC_SYMTAB` = 0x2
        - 数据结构定义： `symtab_command`
        - 含义：link-edit stab symbol table info
            - Specifies the symbol table for this file. This information is used by both static and dynamic linkers when linking the file, and also by debuggers to map symbols to the original source code files from which the symbols were generated.
    - LC_SYMSEG = 0x3
        - link-edit gdb symbol table info (obsolete)
    - `LC_THREAD` = 0x4
        - 数据结构定义： `thread_command`
        - 含义：thread
            - For an executable file, the `LC_UNIXTHREAD` command defines the initial thread state of the main thread of the process. `LC_THREAD` is similar to `LC_UNIXTHREAD` but does not cause the kernel to allocate a stack.

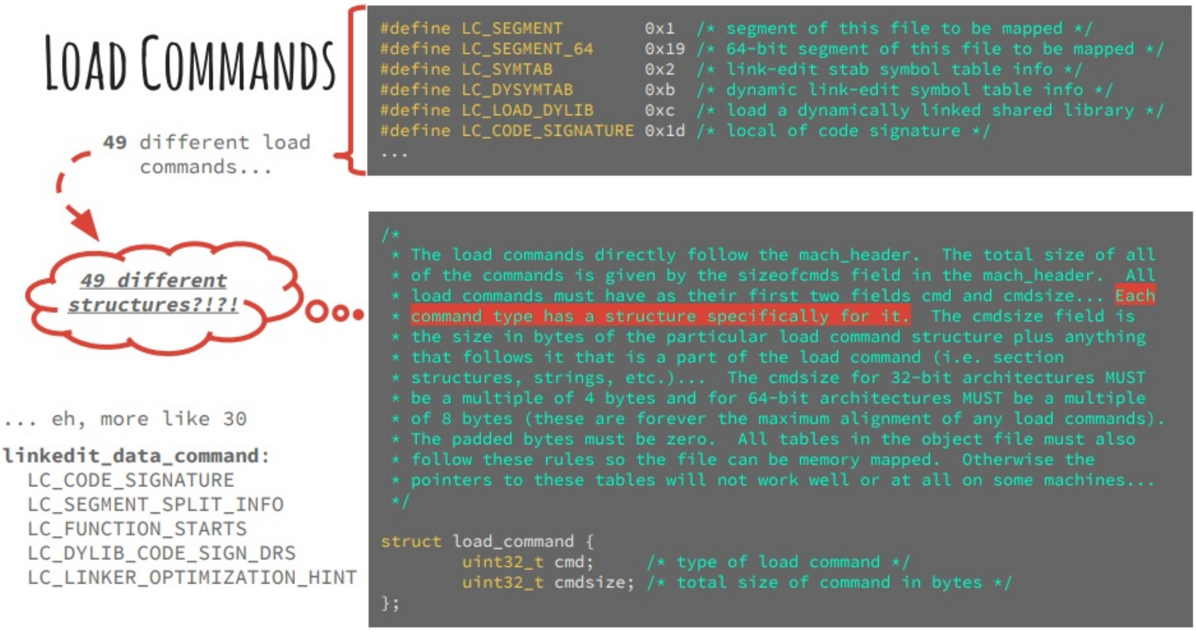
- `LC_UNIXTHREAD` = 0x5
  - 含义：unix thread (includes a stack)
- LC_LOADFVMLIB = 0x6
  - load a specified fixed VM shared library
- LC_IDFVMLIB = 0x7
  - object identification info (obsolete)
- LC_IDENT = 0x8
  - object identification info (obsolete)
- LC_FVMFILE = 0x9
  - fixed VM file inclusion (internal use)
- LC_PREPAGE = 0xa
  - prepage command (internal use)
- `LC_DYSYMTAB` = 0xb
  - 数据结构定义：`dysymtab_command`
  - 含义：dynamic link-edit symbol table info
    - Specifies additional symbol table information used by the dynamic linker.
- `LC_LOAD_DYLIB` = 0xc
  - 数据结构定义：`dylib_command`
  - 含义：load a dynamically linked shared library
    - Defines the name of a dynamic shared library that this file links against.
- `LC_ID_DYLIB` = 0xd
  - 数据结构定义：`dylib_command`
  - 含义：dynamically linked shared lib ident
    - Specifies the install name of a dynamic shared library.
- `LC_LOAD_DYLINKER` = 0xe
  - 数据结构定义：`dylinker_command`
  - 含义：load a dynamic linker
    - Specifies the dynamic linker that the kernel executes to load this file.
- `LC_ID_DYLINKER` = 0xf
  - 数据结构定义：`dylinker_command`
  - 含义：dynamic linker identification
    - Identifies this file as a dynamic linker.
- `LC_PREBOUND_DYLIB` = 0x10
  - 数据结构定义：`prebound_dylib_command`
  - 含义：modules prebound for a dynamically linked shared library
    - For a shared library that this executable is linked prebound against, specifies the modules in the shared library that are used.
- `LC_ROUTINES` = 0x11
  - 数据结构定义：`routines_command`
  - 含义：image routines
    - Contains the address of the shared library initialization routine (specified by the linker's `-init` option).
- `LC_SUB_FRAMEWORK` = 0x12
  - 数据结构定义：`sub_framework_command`
  - 含义：sub framework

        - Identifies this file as the implementation of a subframework of an umbrella framework. The name of the umbrella framework is stored in the string parameter.
  - `LC_SUB_UMBRELLA` = 0x13
    - 数据结构定义： `sub_umbrella_command`
    - 含义：sub umbrella
      - Specifies a file that is a subumbrella of this umbrella framework.
  - `LC_SUB_CLIENT` = 0x14
    - 数据结构定义： `sub_client_command`
    - 含义：sub client
      - A subframework can explicitly allow another framework or bundle to link against it by including an `LC_SUB_CLIENT` load command containing the name of the framework or a client name for a bundle.
  - `LC_SUB_LIBRARY` = 0x15
    - 数据结构定义： `sub_library_command`
    - 含义：sub library
      - Defines the attributes of the `LC_SUB_LIBRARY` load command. Identifies a sublibrary of this framework and marks this framework as an umbrella framework.
  - `LC_TWOLEVEL_HINTS` = 0x16
    - 数据结构定义： `twolevel_hints_command`
    - 含义：two-level namespace lookup hints
      - Contains the two-level namespace lookup hint table.
  - LC_PREBIND_CKSUM = 0x17
    - prebind checksum
  - LC_LOAD_WEAK_DYLIB = 0x18 | LC_REQ_DYLD = 0x80000018
    - load a dynamically linked shared library that is allowed to be missing (all symbols are weak imported)
  - `LC_SEGMENT_64` = 0x19
    - 数据结构定义： `segment_command_64`
    - 含义：64-bit segment of this file to be mapped
      - Defines a 64-bit segment of this file to be mapped into the address space of the process that loads this file. It also includes all the sections contained by the segment.
  - `LC_ROUTINES_64` = 0x1a
    - 数据结构定义： `routines_command_64`
    - 含义：64-bit image routines
      - Contains the address of the shared library 64-bit initialization routine (specified by the linker's `-init` option).
  - `LC_UUID` = 0x1b
    - 数据结构定义： `uuid_command`
    - 含义：the uuid
      - Specifies the 128-bit UUID for an image or its corresponding dSYM file
  - LC_RPATH = 0x1c | LC_REQ_DYLD = 0x8000001c
    - run path additions
  - LC_CODE_SIGNATURE = 0x1d
    - local of code signature
  - LC_SEGMENT_SPLIT_INFO = 0x1e

    - local of info to split segments
- LC_REEXPORT_DYLIB = 0x1f | LC_REQ_DYLD = 0x8000001f
    - load and re-export dylib
- LC_LAZY_LOAD_DYLIB = 0x20
    - delay load of dylib until first use
- LC_ENCRYPTION_INFO = 0x21
    - encrypted segment information
- LC_DYLD_INFO = 0x22
    - compressed dyld information
- LC_DYLD_INFO_ONLY = 0x22 | LC_REQ_DYLD = 0x80000022
    - compressed dyld information only
- LC_LOAD_UPWARD_DYLIB = 0x23 | LC_REQ_DYLD = 0x80000023
    - load upward dylib
- LC_VERSION_MIN_MACOSX = 0x24
    - build for MacOSX min OS version
- LC_VERSION_MIN_IPHONEOS = 0x25
    - build for iPhoneOS min OS version
- LC_FUNCTION_STARTS = 0x26
    - compressed table of function start addresses
- LC_DYLD_ENVIRONMENT = 0x27
    - string for dyld to treat like environment variable
- LC_MAIN = 0x28 | LC_REQ_DYLD = 0x80000028
    - replacement for LC_UNIXTHREAD
- LC_DATA_IN_CODE = 0x29
    - table of non-instructions in __text
- LC_SOURCE_VERSION = 0x2A
    - source version used to build binary
- LC_DYLIB_CODE_SIGN_DRS = 0x2B
    - Code signing DRs copied from linked dylibs
- LC_ENCRYPTION_INFO_64 = 0x2C
    - 64-bit encrypted segment information
- LC_LINKER_OPTION = 0x2D
    - linker options in MH_OBJECT files
- LC_LINKER_OPTIMIZATION_HINT = 0x2E
    - optimization hints in MH_OBJECT files
- LC_VERSION_MIN_TVOS = 0x2F
    - build for AppleTV min OS version
- LC_VERSION_MIN_WATCHOS = 0x30
    - build for Watch min OS version
- LC_NOTE = 0x31
    - arbitrary data included within a Mach-O file
- LC_BUILD_VERSION = 0x32
    - build for platform min OS version
- LC_DYLD_EXPORTS_TRIE = 0x33 | LC_REQ_DYLD = 0x80000033
    - used with `LinkeditDataCommand` , payload is trie
- LC_DYLD_CHAINED_FIXUPS = 0x34 | LC_REQ_DYLD = 0x80000034

        - used with `LinkeditDataCommand`
    - LC_FILESET_ENTRY = 0x35 | LC_REQ_DYLD = 0x80000035
        - used with `FilesetEntryCommand`

Load Commands定义



- 源码定义
    - loader.h
        - xnu-2050.18.24
            - loader.h
        - xnu-7195.81.3
            - loader.h html

```
/*
 * The load commands directly follow the mach_header.  The total size of all
 * of the commands is given by the sizeofcmds field in the mach_header.  All
 * load commands must have as their first two fields cmd and cmdsize.  The cmd
 * field is filled in with a constant for that command type.  Each command type
 * has a structure specifically for it.  The cmdsize field is the size in bytes
 * of the particular load command structure plus anything that follows it that
 * is a part of the load command (i.e. section structures, strings, etc.).  To
 * advance to the next load command the cmdsize can be added to the offset or
 * pointer of the current load command.  The cmdsize for 32-bit architectures
 * MUST be a multiple of 4 bytes and for 64-bit architectures MUST be a multiple
 * of 8 bytes (these are forever the maximum alignment of any load commands).
 * The padded bytes must be zero.  All tables in the object file must also
 * follow these rules so the file can be memory mapped.  Otherwise the pointers
 * to these tables will not work well or at all on some machines.  With all
 * padding zeroed like objects will compare byte for byte.
 */
struct load_command {
    uint32_t cmd;          /* type of load command */
```

```
    uint32_t cmdsize;    /* total size of command in bytes */
};

/*
 * After MacOS X 10.1 when a new load command is added that is required to be
 * understood by the dynamic linker for the image to execute properly the
 * LC_REQ_DYLD bit will be or'ed into the load command constant.  If the dynamic
 * linker sees such a load command it it does not understand will issue a
 * "unknown load command required for execution" error and refuse to use the
 * image.  Other load commands without this bit that are not understood will
 * simply be ignored.
 */
#define LC_REQ_DYLD 0x80000000

/* Constants for the cmd field of all load commands, the type */
#define    LC_SEGMENT    0x1    /* segment of this file to be mapped */
#define    LC_SYMTAB    0x2    /* link-edit stab symbol table info */
#define    LC_SYMSEG    0x3    /* link-edit gdb symbol table info (obsolete) */
#define    LC_THREAD    0x4    /* thread */
#define    LC_UNIXTHREAD    0x5    /* unix thread (includes a stack) */
#define    LC_LOADFVMLIB    0x6    /* load a specified fixed VM shared library */
#define    LC_IDFVMLIB    0x7    /* fixed VM shared library identification */
#define    LC_IDENT    0x8    /* object identification info (obsolete) */
#define LC_FVMFILE    0x9    /* fixed VM file inclusion (internal use) */
#define LC_PREPAGE      0xa     /* prepage command (internal use) */
#define    LC_DYSYMTAB    0xb    /* dynamic link-edit symbol table info */
#define    LC_LOAD_DYLIB    0xc    /* load a dynamically linked shared library */
#define    LC_ID_DYLIB    0xd    /* dynamically linked shared lib ident */
#define LC_LOAD_DYLINKER 0xe    /* load a dynamic linker */
#define LC_ID_DYLINKER    0xf    /* dynamic linker identification */
#define    LC_PREBOUND_DYLIB 0x10    /* modules prebound for a dynamically */
                /*  linked shared library */
#define    LC_ROUTINES    0x11    /* image routines */
#define    LC_SUB_FRAMEWORK 0x12    /* sub framework */
#define    LC_SUB_UMBRELLA 0x13    /* sub umbrella */
#define    LC_SUB_CLIENT    0x14    /* sub client */
#define    LC_SUB_LIBRARY  0x15    /* sub library */
#define    LC_TWOLEVEL_HINTS 0x16    /* two-level namespace lookup hints */
#define    LC_PREBIND_CKSUM  0x17    /* prebind checksum */

/*
 * load a dynamically linked shared library that is allowed to be missing
 * (all symbols are weak imported).
 */
#define    LC_LOAD_WEAK_DYLIB (0x18 | LC_REQ_DYLD)

#define    LC_SEGMENT_64    0x19    /* 64-bit segment of this file to be
                   mapped */
#define    LC_ROUTINES_64    0x1a    /* 64-bit image routines */
#define LC_UUID        0x1b    /* the uuid */
#define LC_RPATH       (0x1c | LC_REQ_DYLD)    /* runpath additions */
#define LC_CODE_SIGNATURE 0x1d    /* local of code signature */
#define LC_SEGMENT_SPLIT_INFO 0x1e /* local of info to split segments */
#define LC_REEXPORT_DYLIB (0x1f | LC_REQ_DYLD) /* load and re-export dylib */
#define    LC_LAZY_LOAD_DYLIB 0x20    /* delay load of dylib until first use */
#define    LC_ENCRYPTION_INFO 0x21    /* encrypted segment information */
```

```
#define     LC_DYLD_INFO      0x22    /* compressed dyld information */
#define     LC_DYLD_INFO_ONLY (0x22|LC_REQ_DYLD)    /* compressed dyld information only
*/
#define     LC_LOAD_UPWARD_DYLIB (0x23 | LC_REQ_DYLD) /* load upward dylib */
#define LC_VERSION_MIN_MACOSX 0x24   /* build for MacOSX min OS version */
#define LC_VERSION_MIN_IPHONEOS 0x25 /* build for iPhoneOS min OS version */
#define LC_FUNCTION_STARTS 0x26 /* compressed table of function start addresses */
#define LC_DYLD_ENVIRONMENT 0x27 /* string for dyld to treat
                  like environment variable */
#define LC_MAIN (0x28|LC_REQ_DYLD) /* replacement for LC_UNIXTHREAD */
#define LC_DATA_IN_CODE 0x29 /* table of non-instructions in __text */
#define LC_SOURCE_VERSION 0x2A /* source version used to build binary */
#define LC_DYLIB_CODE_SIGN_DRS 0x2B /* Code signing DRs copied from linked dylibs */
#define     LC_ENCRYPTION_INFO_64 0x2C /* 64-bit encrypted segment information */
#define LC_LINKER_OPTION 0x2D /* linker options in MH_OBJECT files */
#define LC_LINKER_OPTIMIZATION_HINT 0x2E /* optimization hints in MH_OBJECT files */
#define LC_VERSION_MIN_TVOS 0x2F /* build for AppleTV min OS version */
#define LC_VERSION_MIN_WATCHOS 0x30 /* build for Watch min OS version */
#define LC_NOTE 0x31 /* arbitrary data included within a Mach-O file */
#define LC_BUILD_VERSION 0x32 /* build for platform min OS version */
#define LC_DYLD_EXPORTS_TRIE (0x33 | LC_REQ_DYLD) /* used with linkedit_data_command, p
ayload is trie */
#define LC_DYLD_CHAINED_FIXUPS (0x34 | LC_REQ_DYLD) /* used with linkedit_data_command
*/
#define LC_FILESET_ENTRY      (0x35 | LC_REQ_DYLD) /* used with fileset_entry_command */
```

- 说明
  - `iOS 15.0` 后新增的Load Command
    - `LC_DYLD_CHAINED_FIXUPS`
    - `LC_DYLD_EXPORTS_TRIE`

LC_UUID

- `LC_UUID`
  - 是什么：Specifies the 128-bit UUID for an image or its corresponding dSYM file
  - 作用：用来标识唯一APP
    - 每个可执行程序都有一个uuid，这样根据不同的uuid能确定包。比如崩溃日志中就会包含uuid字段。表示是哪个包崩溃了
  - 数据结构定义：`uuid_command`

uuid_command定义

```
struct uuid_command {
    uint32_t     cmd;        /* LC_UUID */
    uint32_t     cmdsize;    /* sizeof(struct uuid_command) */
    uint8_t     uuid[16];    /* the 128-bit uuid */
};
```

举例

- MachOView查看到某 `LC_UUID`

  -

- jtool2解析AwemeCore中 `jtool2 -l xxx/AwemeCore` 输出的

  ```
  LC 09: LC_UUID                 UUID: F1FCF15A-6465-31F0-9300-5BA1B8F91017
  ```

LC_SEGMENT

- `LC_SEGMENT`
    - 含义：Defines a segment of this file to be mapped into the address space of the process that loads this file. It also includes all the sections contained by the segment.
    - 数据结构定义： `segment_command`

segment_command定义

- 精简定义

```
struct segment_command {
  uint32_t   cmd;
  uint32_t   cmdsize;
  char       segname[16];
  uint32_t   vmaddr;
  uint32_t   vmsize;
  uint32_t   fileoff;
  uint32_t   filesize;
  vm_prot_t  maxprot;
  vm_prot_t  initprot;
  uint32_t   nsects;
  uint32_t   flags;
};
```

- 完整定义

```
/*
 * The segment load command indicates that a part of this file is to be
 * mapped into the task's address space.  The size of this segment in memory,
 * vmsize, maybe equal to or larger than the amount to map from this file,
 * filesize.  The file is mapped starting at fileoff to the beginning of
 * the segment in memory, vmaddr.  The rest of the memory of the segment,
 * if any, is allocated zero fill on demand.  The segment's maximum virtual
 * memory protection and initial virtual memory protection are specified
 * by the maxprot and initprot fields.  If the segment has sections then the
 * section structures directly follow the segment command and their size is
 * reflected in cmdsize.
 */
struct segment_command { /* for 32-bit architectures */
    uint32_t    cmd;        /* LC_SEGMENT */
    uint32_t    cmdsize;    /* includes sizeof section structs */
    char        segname[16];    /* segment name */
    uint32_t    vmaddr;        /* memory address of this segment */
    uint32_t    vmsize;        /* memory size of this segment */
    uint32_t    fileoff;    /* file offset of this segment */
    uint32_t    filesize;    /* amount to map from the file */
    vm_prot_t    maxprot;    /* maximum VM protection */
    vm_prot_t    initprot;    /* initial VM protection */
    uint32_t    nsects;        /* number of sections in segment */
```

```
    uint32_t    flags;        /* flags */
};
```

LC_SEGMENT_64

- `LC_SEGMENT_64`
  - 数据结构定义： `segment_command_64`
    - 含义：Defines a 64-bit segment of this file to be mapped into the address space of the process that loads this file. It also includes all the sections contained by the segment.

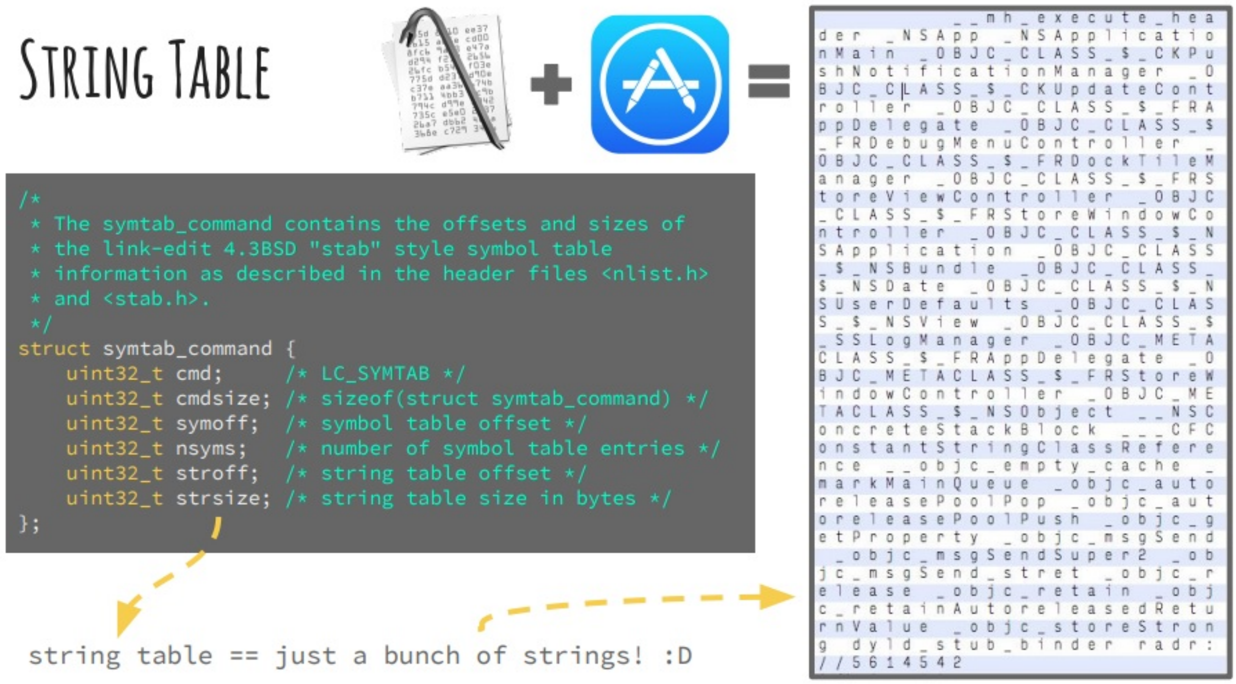
segment_command_64定义

```
/*
 * The 64-bit segment load command indicates that a part of this file is to be
 * mapped into a 64-bit task's address space.  If the 64-bit segment has
 * sections then section_64 structures directly follow the 64-bit segment
 * command and their size is reflected in cmdsize.
 */
struct segment_command_64 { /* for 64-bit architectures */
    uint32_t    cmd;        /* LC_SEGMENT_64 */
    uint32_t    cmdsize;    /* includes sizeof section_64 structs */
    char        segname[16];    /* segment name */
    uint64_t    vmaddr;        /* memory address of this segment */
    uint64_t    vmsize;        /* memory size of this segment */
    uint64_t    fileoff;    /* file offset of this segment */
    uint64_t    filesize;    /* amount to map from the file */
    vm_prot_t    maxprot;    /* maximum VM protection */
    vm_prot_t    initprot;    /* initial VM protection */
    uint32_t    nsects;        /* number of sections in segment */
    uint32_t    flags;        /* flags */
};
```

LC_SYMTAB

- `LC_SYMTAB`
  - 数据结构定义： `symtab_command`
  - 含义：Specifies the symbol table for this file. This information is used by both static and dynamic linkers when linking the file, and also by debuggers to map symbols to the original source code files from which the symbols were generated.

symtab_command定义



源码定义：

- 精简定义

```
struct symtab_command {
    uint32_t cmd;
    uint32_t cmdsize;
    uint32_t symoff;
    uint32_t nsyms;
    uint32_t stroff;
    uint32_t strsize;
};
```

- 详细定义

```
/*
 * The symtab_command contains the offsets and sizes of the link-edit 4.3BSD
 * "stab" style symbol table information as described in the header files
 * <nlist.h> and <stab.h>.
```

```
 * symtab_command 包含了符号表、字符串索引表 的偏移量和大小 。
 */
struct symtab_command {
    uint32_t    cmd;        /* LC_SYMTAB */
    uint32_t    cmdsize;    /* sizeof(struct symtab_command) */
    uint32_t    symoff;        /* symbol table offset */
    uint32_t    nsyms;        /* number of symbol table entries */
    uint32_t    stroff;        /* string table offset */
    uint32_t    strsize;    /* string table size in bytes */
};
```

举例

- MachOView查看到某 `LC_SYMTAB` 的效果
    -
        - 说明
            - 命令的大小是24 （十进制）
            - 符号表在物理文件的偏移量是 77360448
            - 符号表的大小 1069179
            - String表的物理文件偏移量是94479244
            - string表的大小是22093264

LC_DYLD_CHAINED_FIXUPS

- `LC_DYLD_CHAINED_FIXUPS`
  - 说明： `iOS 15.0+` 新出现的Load Command
  - 含义
    - Chained fixups is a new way to store information that will be used by `dyld`. Replacing `LC_DYLD_INFO` (_ONLY), the chained fixups can save binary size and reduce launch time.
    - Traditionally, `dyld`, at launch time, needs to slide the fixed addresses with a random number, known as `ASLR`. This operation is called `rebasing`. Also, `dyld` needs to connect symbols from current binary with its linked dynamic libraries. This is called `binding`. Under the new format, both `rebasing` and `binding` have a new name, **fixup**, because they need to be "fixed up" before main function.
    - Chained fixups is enabled by default if the binary is built for device and targeted at iOS 14+. We can also manually enable it by passing `-fixup_chains` to ld. To disable it, use `-no_fixup_chains`.

LC_DYLD_EXPORTS_TRIE

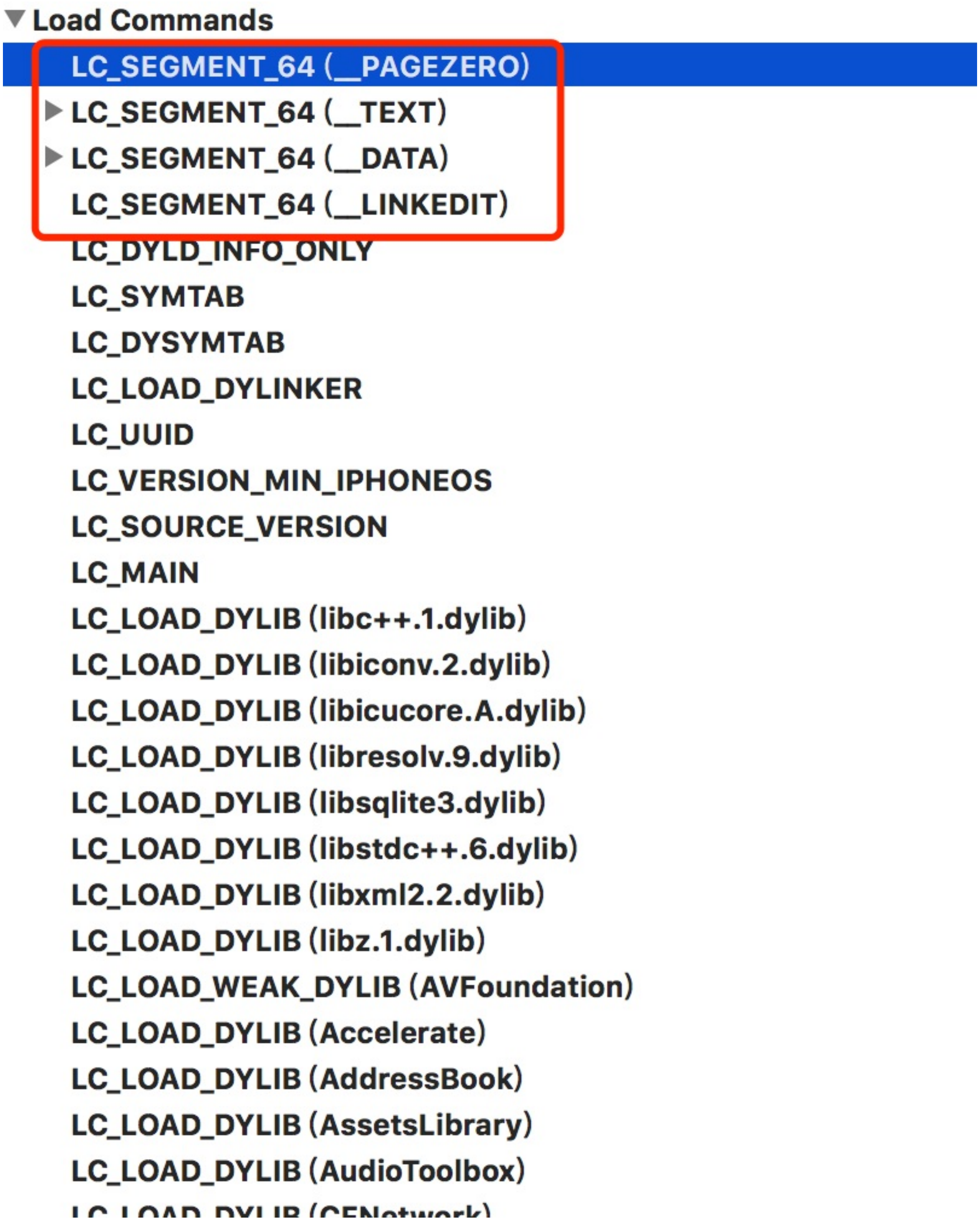
- `LC_DYLD_EXPORTS_TRIE`
    - 说明： `iOS 15.0+` 新出现的Load Command
    - 含义
        - If the binary is targeted at iOS 14+ or is linked with `-fixup_chains` linker flag, the same information is stored in `LC_DYLD_EXPORTS_TRIE` load command instead. The detail of this change is discussed at Chained Fixups.

segment

- Mach-O中包含1个或多个segment
  - 一个segment中包含0或多个section
- segment和sectoin的基本定义
  -

常见segment

- 概述
  - 最常用的segment：`__PAGEZERO`、`__TEXT`、`__DATA`、`__LINKEDIT`
    - 举例
      - MachOView查看某Mach-O的效果

- 

- 详解
  - `__PAGEZERO`
    - The static linker creates a `__PAGEZERO` segment as the first segment of an executable file. This segment is located at virtual memory location 0 and has no protection rights assigned, the combination of which causes accesses to NULL, a common C programming error, to immediately crash. The `__PAGEZERO` segment is the size of one full VM page for the current architecture (for Intel-based and PowerPC-based Macintosh computers, this is 4096 bytes or 0x1000 in hexadecimal). Because there is no data in the `__PAGEZERO` segment, it occupies no space in the file (the file size in the segment command is 0).
  - `__TEXT`
    - The `__TEXT` segment contains executable code and other read-only data. To allow the kernel to map it directly from the executable into sharable memory, the static linker sets this segment's virtual memory permissions to disallow writing. When the segment is mapped into memory, it can be shared among all processes interested in its contents. (This is primarily used with frameworks, bundles, and shared libraries, but it is possible to run multiple copies of the same executable in OS X, and this applies in that case as well.) The read-only

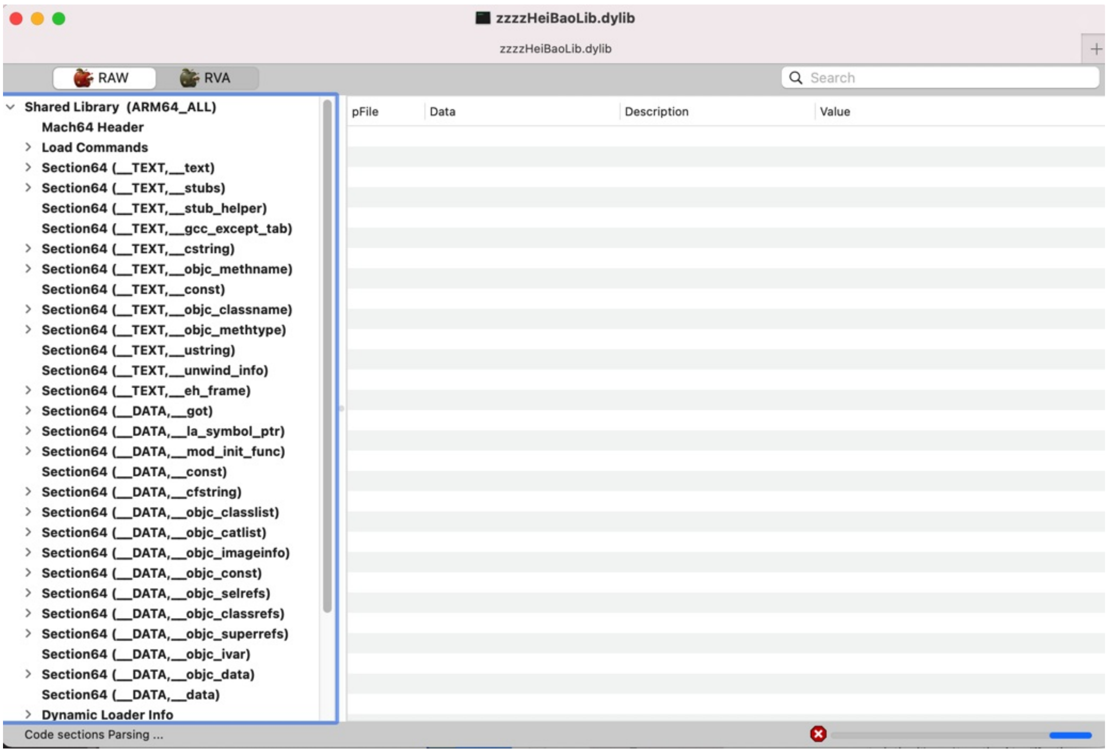
attribute also means that the pages that make up the `__TEXT` segment never need to be written back to disk. When the kernel needs to free up physical memory, it can simply discard one or more `__TEXT` pages and re-read them from disk when they are next needed.
    - `__DATA`
        - The `__DATA` segment contains writable data. The static linker sets the virtual memory permissions of this segment to allow both reading and writing. Because it is writable, the `__DATA` segment of a framework or other shared library is logically copied for each process linking with the library. When memory pages such as those making up the `__DATA` segment are readable and writable, the kernel marks them copy-on-write; therefore when a process writes to one of these pages, that process receives its own private copy of the page.
    - `__OBJC`
        - The __OBJC segment contains data used by the Objective-C language runtime support library.
    - `__IMPORT`
        - The __IMPORT segment contains symbol stubs and non-lazy pointers to symbols not defined in the executable. This segment is generated only for executables targeted for the IA-32 architecture.
    - `__LINKEDIT`
        - The __LINKEDIT segment contains raw data used by the dynamic linker, such as symbol, string, and relocation table entries.

主要segment的section

- segment段
    - `__TEXT` 段
        - Section节
            - `__text` : The compiled machine code for the executable
            - `__const` : The general constant data for the executable
            - `__cstring` : Literal string constants (quoted strings in source code)
            - `__picsymbol_stub` : Position-independent code stub routines used by the dynamic linker (dyld)
    - `__DATA` 段
        - Section节
            - `__data` : Initialized global variables (for example `int a = 1;` or `static int a = 1;`)
            - `__const` : Constant data needing relocation (for example, `char * const p = "foo";`)
            - `__bss` : Uninitialized static variables (for example, `static int a;`)
            - `__common` : Uninitialized external globals (for example, `int a;` outside function blocks)
            - `__dyld` : A placeholder section, used by the dynamic linker
            - `__la_symbol_ptr` : **Lazy** symbol pointers. Symbol pointers for each undefined function called by the executable

- `__nl_symbol_ptr` : **Non lazy** symbol pointers. Symbol pointers for each undefined data symbol referenced by the executable

举例

- 举例1
  -
- 举例2
  - MachOView查看zzzzHeiBaoLib.dylib
    - 

- 举例3

```
# Sections:
# Address     Size          Segment    Section
0x100001DC0    0x00A38B42    __TEXT    __text
0x100A3A902    0x00001C9E    __TEXT    __stubs
0x100A3C5A0    0x0000204A    __TEXT    __stub_helper
0x100A3E5EC    0x000231B0    __TEXT    __gcc_except_tab
0x100A617A0    0x000178D0    __TEXT    __const
0x100A79070    0x0008A5DA    __TEXT    __cstring
0x100B0364A    0x0005F462    __TEXT    __objc_methname
0x100B62AAC    0x00008794    __TEXT    __objc_classname
0x100B6B240    0x0003B4EB    __TEXT    __objc_methtype
0x100BA672C    0x00001742    __TEXT    __ustring
0x100BA7E6E    0x00000172    __TEXT    __entitlements
0x100BA7FE0    0x0000037B    __TEXT    __dof_RACSignal
0x100BA835B    0x000002E8    __TEXT    __dof_RACCompou
0x100BA8644    0x00012964    __TEXT    __unwind_info
0x100BBAFA8    0x00000058    __TEXT    __eh_frame
0x100BBB000    0x00000008    __DATA    __nl_symbol_ptr
0x100BBB008    0x00000BD8    __DATA    __got
0x100BBBBE0    0x00002628    __DATA    __la_symbol_ptr
0x100BBE208    0x00000070    __DATA    __mod_init_func
0x100BBE280    0x0001CEE0    __DATA    __const
0x100BDB160    0x00039CA0    __DATA    __cfstring
0x100C14E00    0x00002B00    __DATA    __objc_classlist
0x100C17900    0x000000A0    __DATA    __objc_nlclslist
0x100C179A0    0x00000680    __DATA    __objc_catlist
0x100C18020    0x000000D0    __DATA    __objc_nlcatlist
0x100C180F0    0x00000638    __DATA    __objc_protolist
0x100C18728    0x00000008    __DATA    __objc_imageinfo
0x100C18730    0x001252F8    __DATA    __objc_const
0x100D3DA28    0x000150B0    __DATA    __objc_selrefs
0x100D52AD8    0x00000150    __DATA    __objc_protorefs
0x100D52C28    0x00002A38    __DATA    __objc_classrefs
0x100D55660    0x000019F8    __DATA    __objc_superrefs
0x100D57058    0x000085E8    __DATA    __objc_ivar
0x100D5F640    0x0001AE00    __DATA    __objc_data
0x100D7A440    0x0000CC70    __DATA    __data
0x100D870B0    0x00004698    __DATA    __bss
0x100D8B750    0x00001298    __DATA    __common
```

__TEXT

`__TEXT` segment的section：

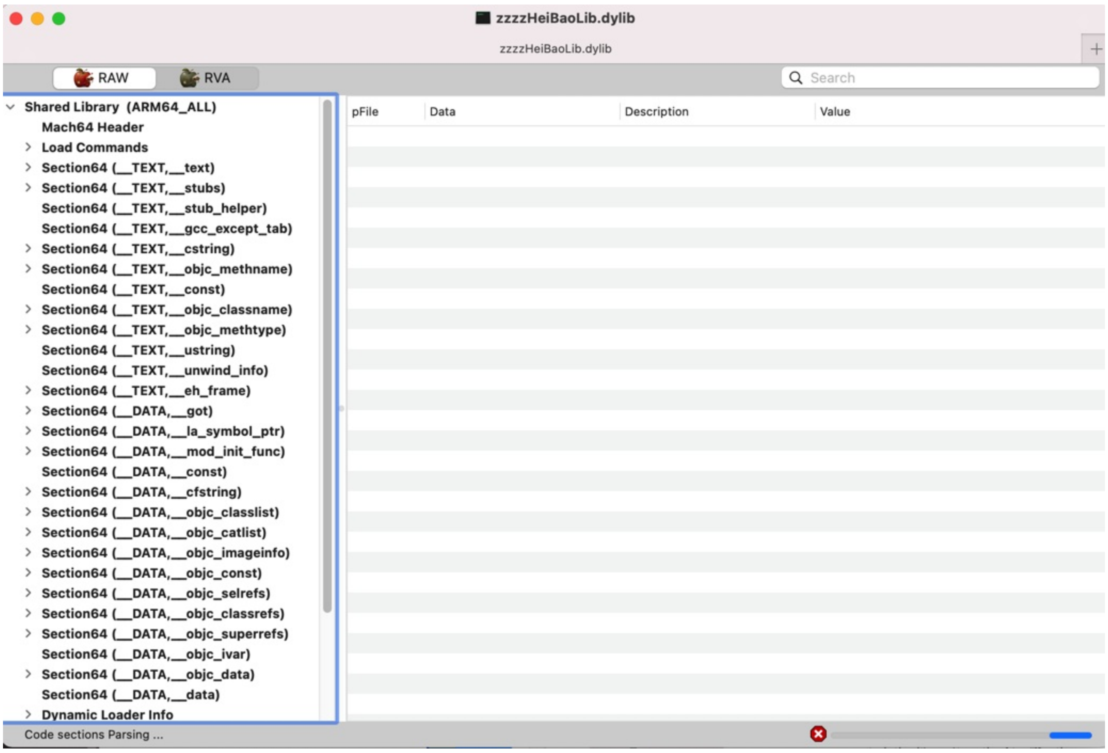
- 概述
  - 图
    - Table 1 Major sections in the __TEXT segment

Section	Description
`__text`	The compiled machine code for the executable
`__const`	The general constant data for the executable
`__cstring`	Literal string constants (quoted strings in source code)
`__picsymbol_stub`	Position-independent code stub routines used by the dynamic linker (`dyld`).
  - 文字
    - `__TEXT,__text` : The compiled machine code for the executable
    - `__TEXT,__const` : The general constant data for the executable
    - `__TEXT,__cstring` : Literal string constants (quoted strings in source code)
    - `__TEXT,__picsymbol_stub` : Position-independent code stub routines used by the dynamic linker (dyld).
- 详解
  - `__TEXT,__text`
    - Executable machine code
      - The compiler generally places only executable code in this section, no tables or data of any sort.
    - 代码节，存放机器编译后的代码
  - `__TEXT,__const`
    - Initialized constant variables
      - The compiler places all nonrelocatable data declared const in this section. (The compiler typically places uninitialized constant variables in a zero-filled section.)
    - 存储const修饰的常量
  - `__TEXT,__cstring`
    - Constant C strings
      - A C string is a sequence of non-null bytes that ends with a null byte (`'\0'`). The static linker coalesces constant C string values, removing duplicates, when building the final product.
    - 代码运行中包含的字符串常量
      - 比如
        - 代码中定义 `#define kGeTuiPushAESKey @"DWE2#@e2!"` ,那 `DWE2#@e2!` 会存在这个区里
  - `__TEXT,__objc_classname`
    - objc类名
  - `__TEXT,__objc_methname`
    - objc的方法名称

- `__TEXT,__objc_methtype`
    - objc方法类型
- `__TEXT,__picsymbol_stub`
    - Position-independent indirect symbol stubs
        - See in Mach-O Programming Topics for more information.
- `__TEXT,__stubs`
    - 用于辅助做动态链接代码（dyld）
- `__TEXT,__stub_helper`
    - 用于辅助做动态链接（dyld）
- `__TEXT,__symbol_stub`
    - Indirect symbol stubs
        - 详见：PIC
- `__TEXT,__literal4`
    - 4-byte literal values
        - The compiler places single-precision floating point constants in this section. The static linker coalesces these values, removing duplicates, when building the final product. With some architectures, it’s more efficient for the compiler to use immediate load instructions rather than adding to this section.
- `__TEXT,__literal8`
    - 8-byte literal values
        - The compiler places double-precision floating point constants in this section. The static linker coalesces these values, removing duplicates, when building the final product. With some architectures, it’s more efficient for the compiler to use immediate load instructions rather than adding to this section.
- `__TEXT,__gcc_except_tab`
- `__TEXT,__dof_RACSignal`
- `__TEXT,__dof_RACCompou`
- `__TEXT,__unwind_info`
- `__TEXT,__ustring`

举例

- MachOView查看
    - zzzzHeiBaoLib.dylib

- 
zzzzHeiBaoLib.dylib
zzzzHeiBaoLib.dylib
RAW
RVA
Search
Shared Library (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__gcc_except_tab)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__objc_methname)
Section64 (__TEXT,__const)
Section64 (__TEXT,__objc_classname)
Section64 (__TEXT,__objc_methtype)
Section64 (__TEXT,__ustring)
Section64 (__TEXT,__unwind_info)
Section64 (__TEXT,__eh_frame)
Section64 (__DATA,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__mod_init_func)
Section64 (__DATA,__const)
Section64 (__DATA,__cfstring)
Section64 (__DATA,__objc_classlist)
Section64 (__DATA,__objc_catlist)
Section64 (__DATA,__objc_imageinfo)
Section64 (__DATA,__objc_const)
Section64 (__DATA,__objc_selrefs)
Section64 (__DATA,__objc_classrefs)
Section64 (__DATA,__objc_superrefs)
Section64 (__DATA,__objc_ivar)
Section64 (__DATA,__objc_data)
Section64 (__DATA,__data)
Dynamic Loader Info
pFile
Data
Description
Value
Code sections Parsing ...

TEXT,text

* section: `__TEXT,__text`
  * 含义
    * Executable machine code
      * The compiler generally places only executable code in this section, no tables or data of any sort.
    * 代码节，存放机器编译后的代码

举例

arm64的akd中的 `__TEXT,__text`

jtool2

```
jtool2 --pages ./akd
0x0-0xf4000 __TEXT     (999424 bytes)
    0x43d0-0xbbf24 __TEXT.__text     (752468 bytes)
...
```

->

* 整个TEXT代码段范围： `0x0-0xf4000 __TEXT (999424 bytes)` = 976KB
  * 代码段内代码的二进制数据opcode的范围： `0x43d0-0xbbf24 __TEXT.__text (752468 bytes)` = 0xB7B54 = 约734.8KB

rabin2

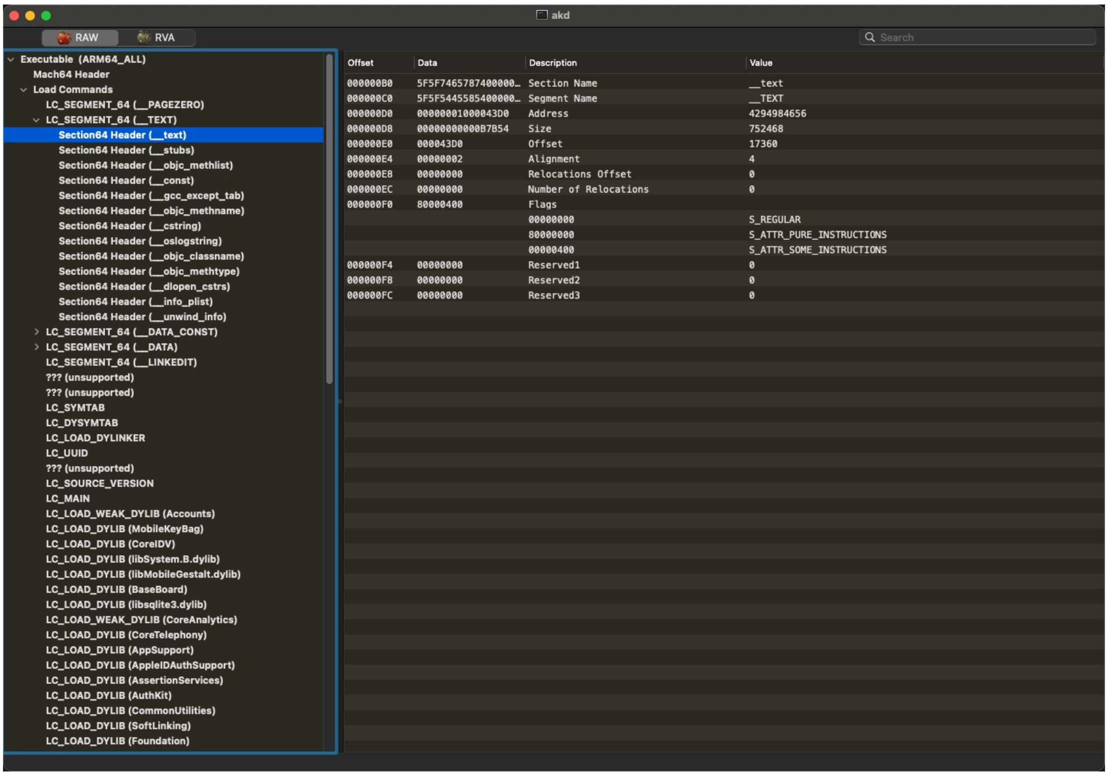
```
rabin2 -S ./akd
...
0   0x000043d0  0xb7b54 0x1000043d0  0xb7b54 -r-x 0.__TEXT.__text
```

->

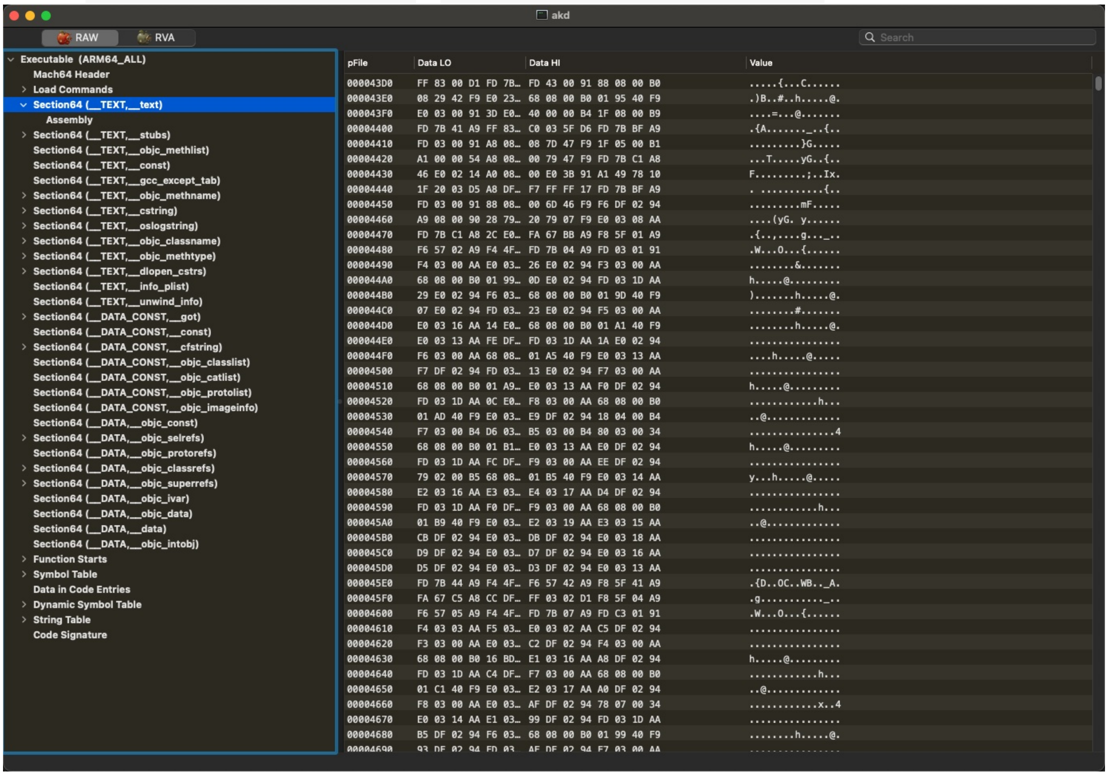
* text代码段的
  * 起始地址：0x000043d0
    * `vaddr` =虚拟地址：0x1000043d0
  * 大小：0xb7b54
    * = 0xB7B54 = 752468

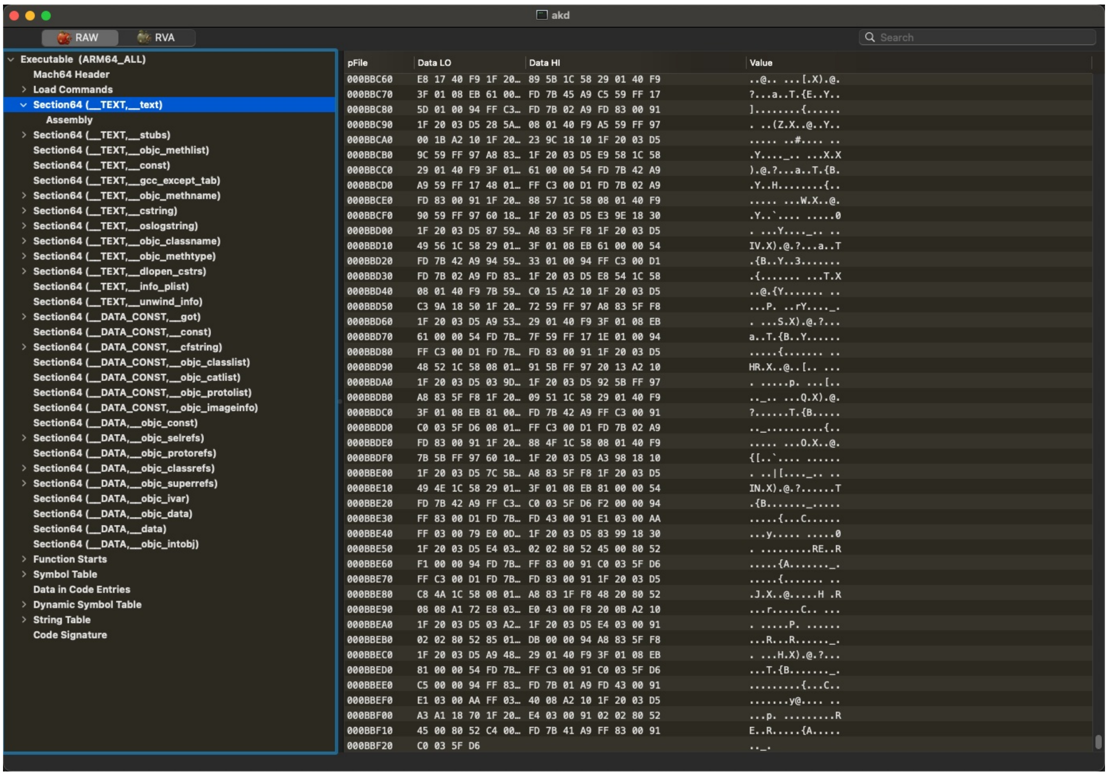
MachOView

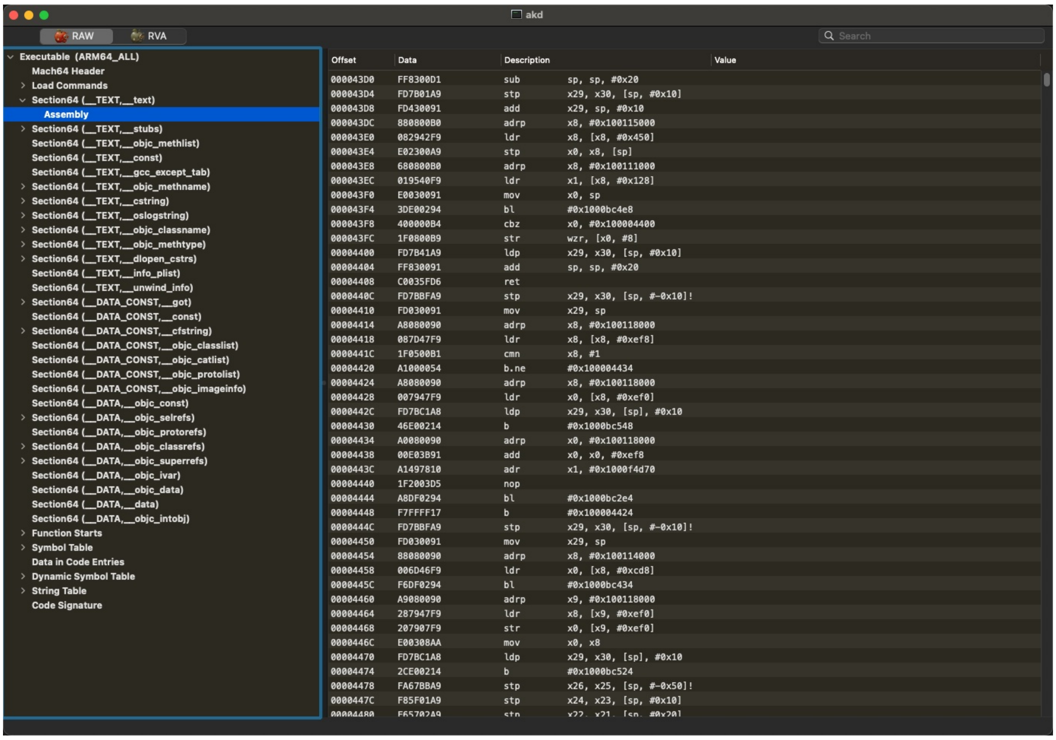
* 代码段的代码信息
  * 概述： `Executable (ARM64_ALL)` -> `Load Commands` -> `LC_SEGMENT_64 (__TEXT)` -> `Section64 Header (__text)`

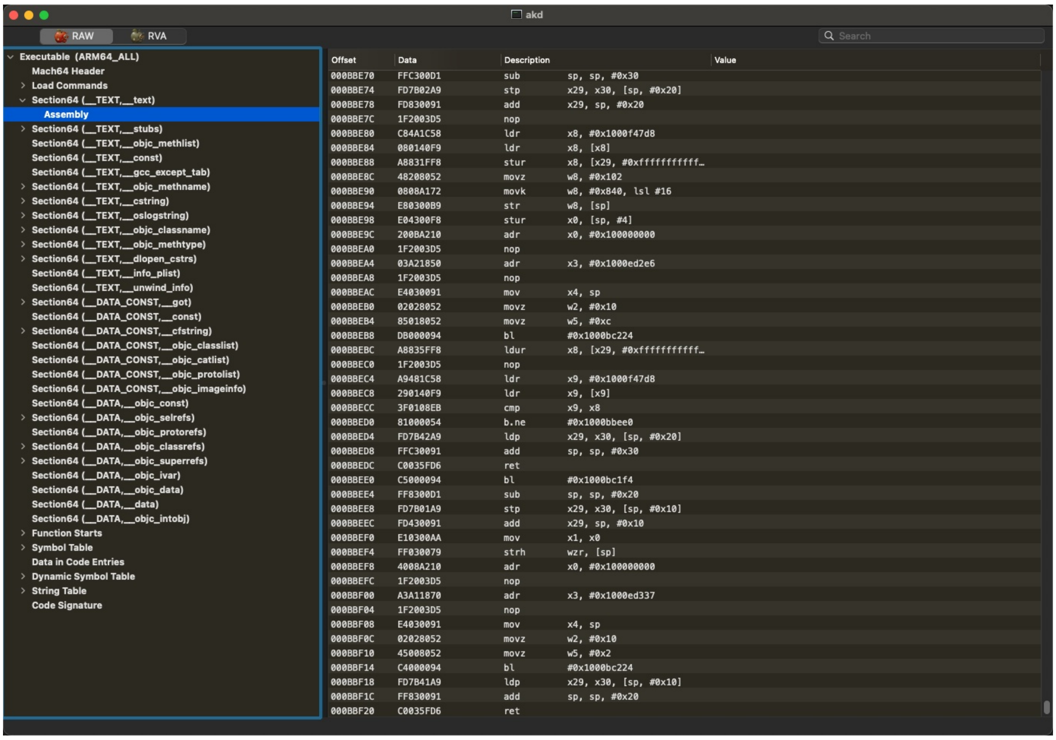
- 

- 真正数据： `Executable (ARM64_ALL)` -> `Section64 (__TEXT, __text)`

- 

- 

- 另外： `Executable (ARM64_ALL)` -> `Section64 (__TEXT, __text)` -> `Assembly`
    - MachOView还提供了，该二进制数据对应的反汇编结果Assembly（仅供参考）
    - 

- 
akd
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Assembly
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__objc_methlist)
Section64 (__TEXT,__const)
Section64 (__TEXT,__gcc_except_tab)
Section64 (__TEXT,__objc_methname)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__oslogstring)
Section64 (__TEXT,__objc_classname)
Section64 (__TEXT,__objc_methtype)
Section64 (__TEXT,__dlopen_cstrs)
Section64 (__TEXT,__info_plist)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA_CONST,__const)
Section64 (__DATA_CONST,__cfstring)
Section64 (__DATA_CONST,__objc_classlist)
Section64 (__DATA_CONST,__objc_catlist)
Section64 (__DATA_CONST,__objc_protolist)
Section64 (__DATA_CONST,__objc_imageinfo)
Section64 (__DATA,__objc_const)
Section64 (__DATA,__objc_selrefs)
Section64 (__DATA,__objc_protorefs)
Section64 (__DATA,__objc_classrefs)
Section64 (__DATA,__objc_superrefs)
Section64 (__DATA,__objc_ivar)
Section64 (__DATA,__objc_data)
Section64 (__DATA,__data)
Section64 (__DATA,__objc_intobj)
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
000BBE70 FFC300D1 sub sp, sp, #0x30
000BBE74 FD7B02A9 stp x29, x30, [sp, #0x20]
000BBE78 FD830091 add x29, sp, #0x20
000BBE7C 1F2003D5 nop
000BBE80 C84A1C58 ldr x8, #0x1000f47d8
000BBE84 080140F9 ldr x8, [x8]
000BBE88 A8831FF8 stur x8, [x29, #0xffffffffff…
000BBE8C 48208052 movz w8, #0x102
000BBE90 0808A172 movk w8, #0x840, lsl #16
000BBE94 E80300B9 str w8, [sp]
000BBE98 E04300F8 stur x0, [sp, #4]
000BBE9C 200BA210 adr x0, #0x100000000
000BBEA0 1F2003D5 nop
000BBEA4 03A21850 adr x3, #0x1000ed2e6
000BBEA8 1F2003D5 nop
000BBEAC E4030091 mov x4, sp
000BBEB0 02028052 movz w2, #0x10
000BBEB4 85018052 movz w5, #0xc
000BBEB8 DB000094 bl #0x1000bc224
000BBEBC A8835FF8 ldur x8, [x29, #0xffffffffff…
000BBEC0 1F2003D5 nop
000BBEC4 A9481C58 ldr x9, #0x1000f47d8
000BBEC8 290140F9 ldr x9, [x9]
000BBECC 3F0108EB cmp x9, x8
000BBED0 81000054 b.ne #0x1000bbee0
000BBED4 FD7B42A9 ldp x29, x30, [sp, #0x20]
000BBED8 FFC30091 add sp, sp, #0x30
000BBEDC C0035FD6 ret
000BBEE0 C5000094 bl #0x1000bc1f4
000BBEE4 FF8300D1 sub sp, sp, #0x20
000BBEE8 FD7B01A9 stp x29, x30, [sp, #0x10]
000BBEEC FD430091 add x29, sp, #0x10
000BBEF0 E10300AA mov x1, x0
000BBEF4 FF030079 strh wzr, [sp]
000BBEF8 4008A210 adr x0, #0x100000000
000BBEFC 1F2003D5 nop
000BBF00 A3A11870 adr x3, #0x1000ed337
000BBF04 1F2003D5 nop
000BBF08 E4030091 mov x4, sp
000BBF0C 02028052 movz w2, #0x10
000BBF10 45008052 movz w5, #0x2
000BBF14 C4000094 bl #0x1000bc224
000BBF18 FD7B41A9 ldp x29, x30, [sp, #0x10]
000BBF1C FF830091 add sp, sp, #0x20
000BBF20 C0035FD6 ret

__DATA

`__DATA` segment的section：

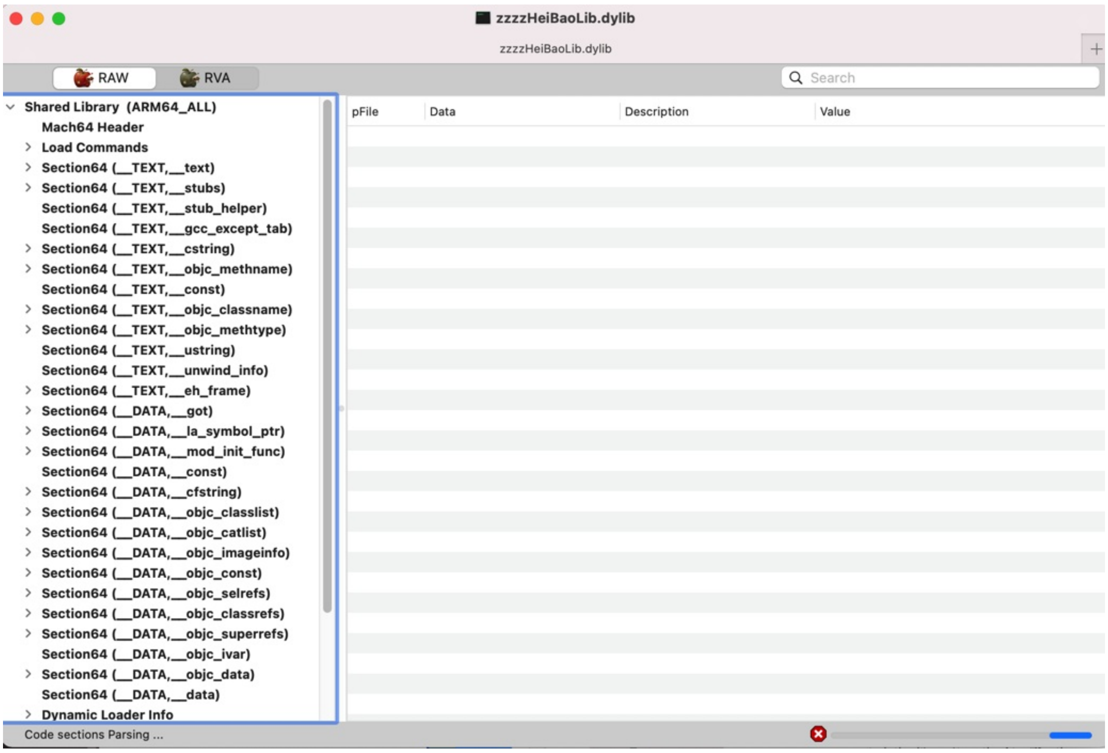
- 概述
  - 图
    - Table 2 Major sections of the __DATA segment

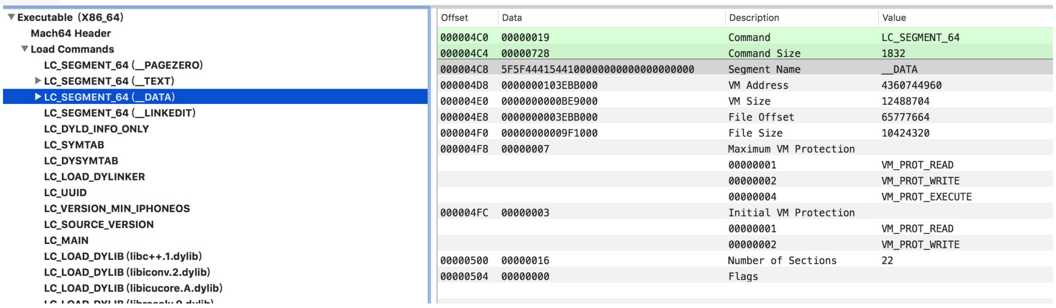
Section	Description
__data	Initialized global variables (for example `int a = 1;` or `static int a = 1;`).
__const	Constant data needing relocation (for example, `char * const p = "foo";`).
__bss	Uninitialized static variables (for example, `static int a;`).
__common	Uninitialized external globals (for example, `int a;` outside function blocks).
__dyld	A placeholder section, used by the dynamic linker.
__la_symbol_ptr	"Lazy" symbol pointers. Symbol pointers for each undefined function called by the executable.
__nl_symbol_ptr	"Non lazy" symbol pointers. Symbol pointers for each undefined data symbol referenced by the executable.
  - 文字
    - `__DATA,__data` : Initialized global variables (for example `int a = 1;` or `static int a = 1;`).
    - `__DATA,__const` : Constant data needing relocation (for example, `char * const p = "foo";`).
    - `__DATA,__bss` : Uninitialized static variables (for example, `static int a;`).
    - `__DATA,__common` : Uninitialized external globals (for example, `int a;` outside function blocks).
    - `__DATA,__dyld` : A placeholder section, used by the dynamic linker.
    - `__DATA,__la_symbol_ptr` : **Lazy** symbol pointers. Symbol pointers for each undefined function called by the executable.
    - `__DATA,__nl_symbol_ptr` : **Non lazy** symbol pointers. Symbol pointers for each undefined data symbol referenced by the executable.
- 详解
  - `__DATA,__bss`
    - Data for uninitialized static variables (for example, `static int i;`).
    - 存储未初始化的静态量。比如： `static NSThread *_networkRequestThread = nil;`
      - 其中这里面的size表示应用运行占用的内存，不是实际的占用空间。所以计算大小的时候应该去掉这部分数据。
  - `__DATA,__common`
    - Uninitialized imported symbol definitions (for example, `int i;`) located in the global scope (outside of a function declaration).
    - 存储导出的全局的数据。类似于 `static` ，但是没有用 `static` 修饰
      - 比如
        - KSCrash里面 `NSDictionary* g_registerOrders;` ， `g_registerOrders` 就存储在 `__common` 里面
  - `__DATA,__data`
    - Initialized mutable variables, such as writable C strings and data arrays.

- 放了协议和一些固定了地址（已经初始化）的静态量
- `__DATA,__la_symbol_ptr`
    - Lazy symbol pointers, which are indirect references to functions imported from a different file
        - 详见：PIC
    - 懒加载的函数指针地址。和 `__stubs` 和 `__stub_helper` 配合使用
- `__DATA,__nl_symbol_ptr`
    - Non-lazy symbol pointers, which are indirect references to data items imported from a different file
        - 详见：PIC
- `__DATA,__dyld`
    - Placeholder section used by the dynamic linker.
- `__DATA,__cfstring`
    - 使用Core Foundation字符串
- `__DATA,__const`
    - Initialized relocatable constant variables.
    - 存储constant常量的数据。比如使用extern导出的const修饰的常量
- `__DATA,__mod_init_func`
    - Module initialization functions. The C++ compiler places static constructors here.
    - 模块初始化的方法
- `__DATA,__mod_term_func`
    - Module termination functions.
- `__DATA,__objc_classlist`
    - objc类列表,保存类信息，映射了 `__objc_data` 的地址
- `__DATA,__objc_data`
    - objc的数据。用于保存类需要的数据。最主要的内容是映射 `__objc_const` 地址，用于找到类的相关数据
- `__DATA,__objc_nlclslist`
    - `Objective-C` 的 `+load` 函数列表，比 `__mod_init_func` 更早执行
- `__DATA,__objc_catlist`
    - categories
- `__DATA,__objc_nlcatlist`
    - `Objective-C` 的categories的 `+load` 函数列表
- `__DATA,__objc_protolist`
    - objc协议列表
- `__DATA,__objc_imageinfo`
    - objc镜像信息
- `__DATA,__got`
    - 存储引用符号的实际地址，类似于动态符号表
- `__DATA,__objc_const`
    - objc常量。保存 `objc_classdata` 结构体数据。用于映射类相关数据的地址，比如类名，方法名等
- `__DATA,__objc_selrefs`
    - 引用到的objc方法
- `__DATA,__objc_protorefs`
    - 引用到的objc协议

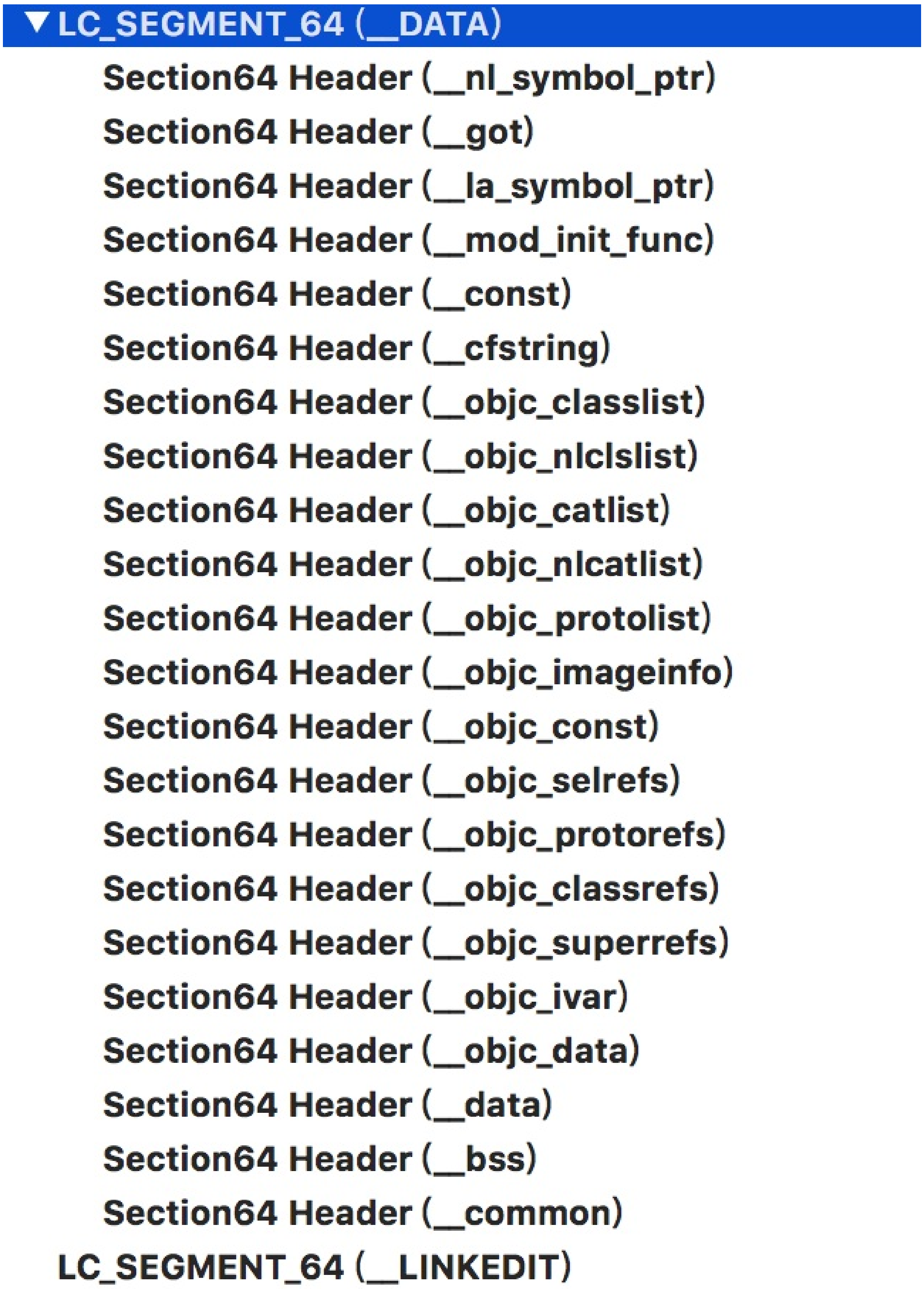
- `__DATA,__objc_classrefs`
  - 引用到的objc类
- `__DATA,__objc_superrefs`
  - objc超类引用
- `__DATA,__objc_ivar`
  - objc的 `ivar` 指针,存储属性

举例

- MachOView查看
  - zzzzHeiBaoLib.dylib
    - 

  - 某app
    - `__DATA` 的segment commond
      - 

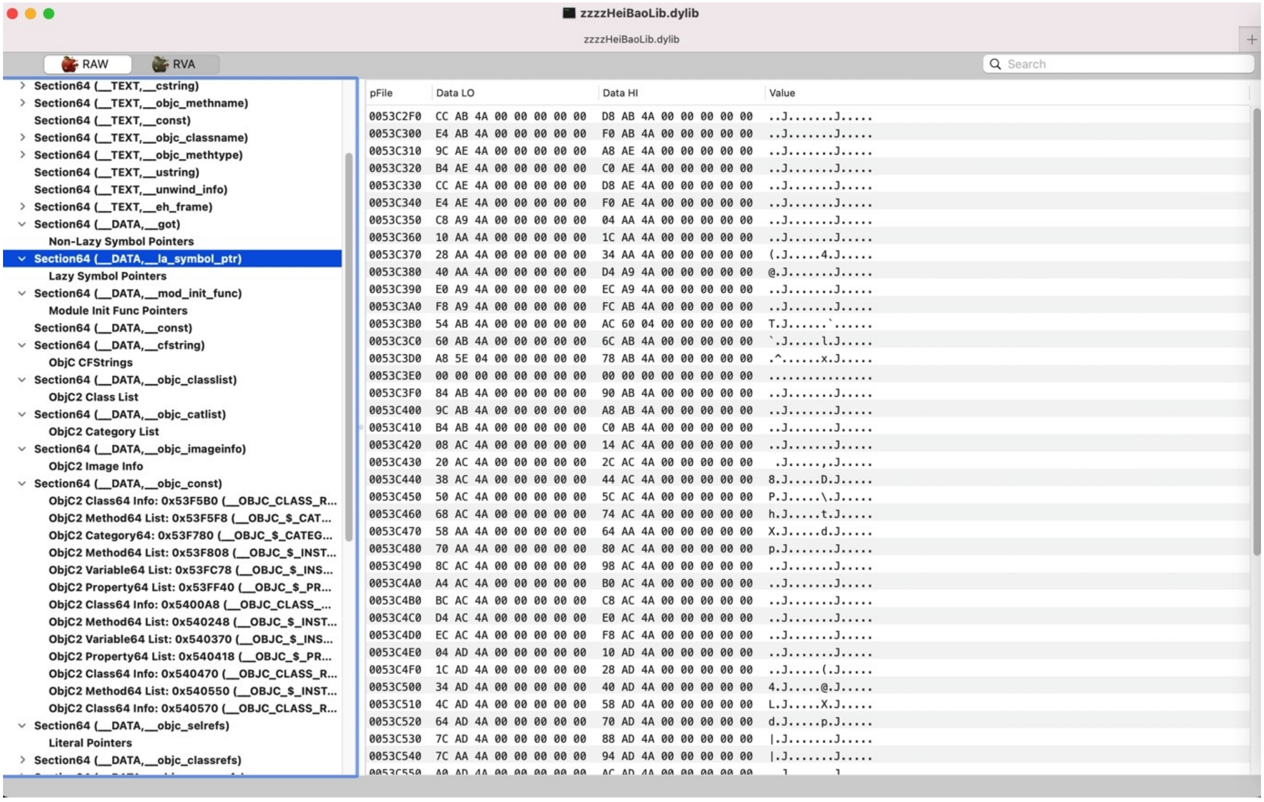
        - 说明
          - 命令类型是LC_SEGMENT_64
          - 命令的大小1832
          - segment 命令的名称是__DATA
          - 映射的内存地址是4360744960（十进制）
          - 内存的大小12488704
          - 文件的偏移量是65777664

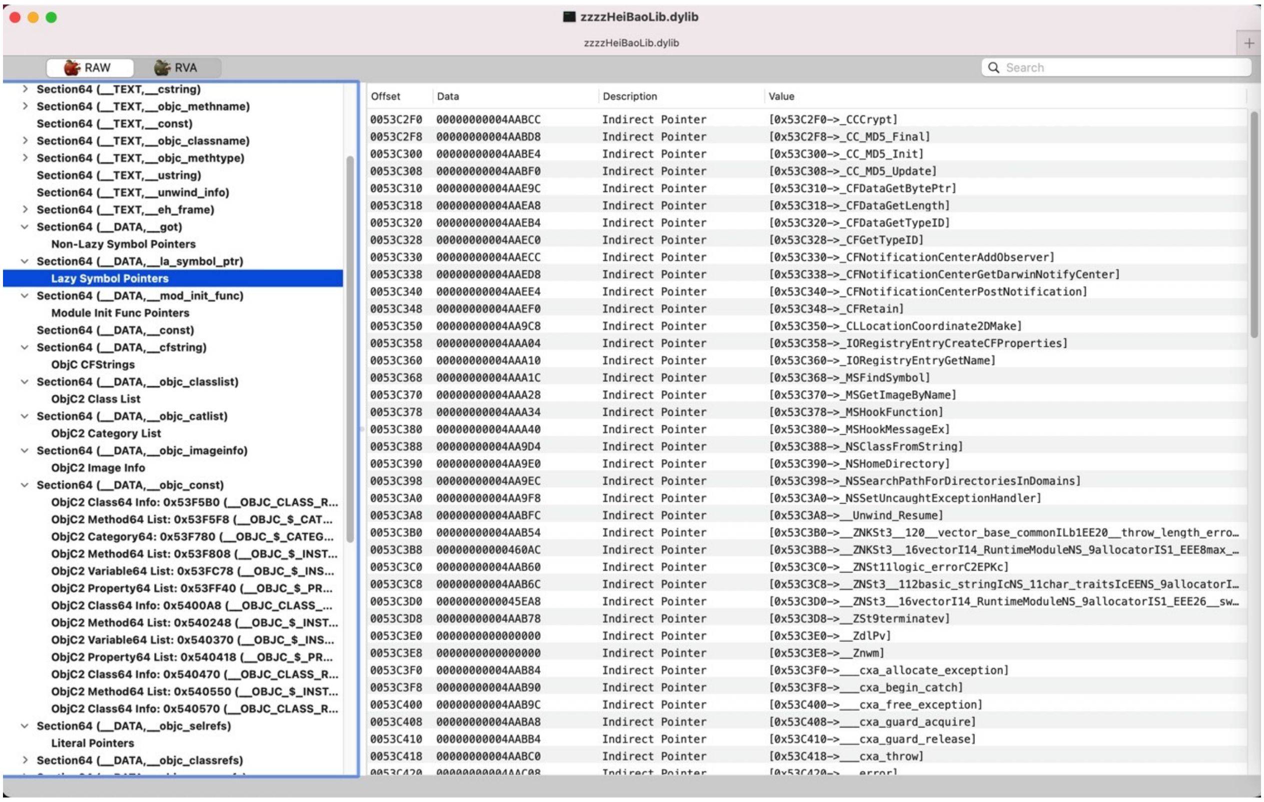
    - 需要映射的文件的大小10424320
    - 最大内存保护权限：读写执行
    - 初始内存权限：读写
    - 这个端附属了22个 section，也就是说1832大小的segment_command包括了22个section命令的大小。
    - 看的方法：offset代表文件的便宜量、Data表示内存地址中存储的值、description表示这段内存地址的名称的描述、value表示存储的值的可视描述。
- 后续的22个section
    - 

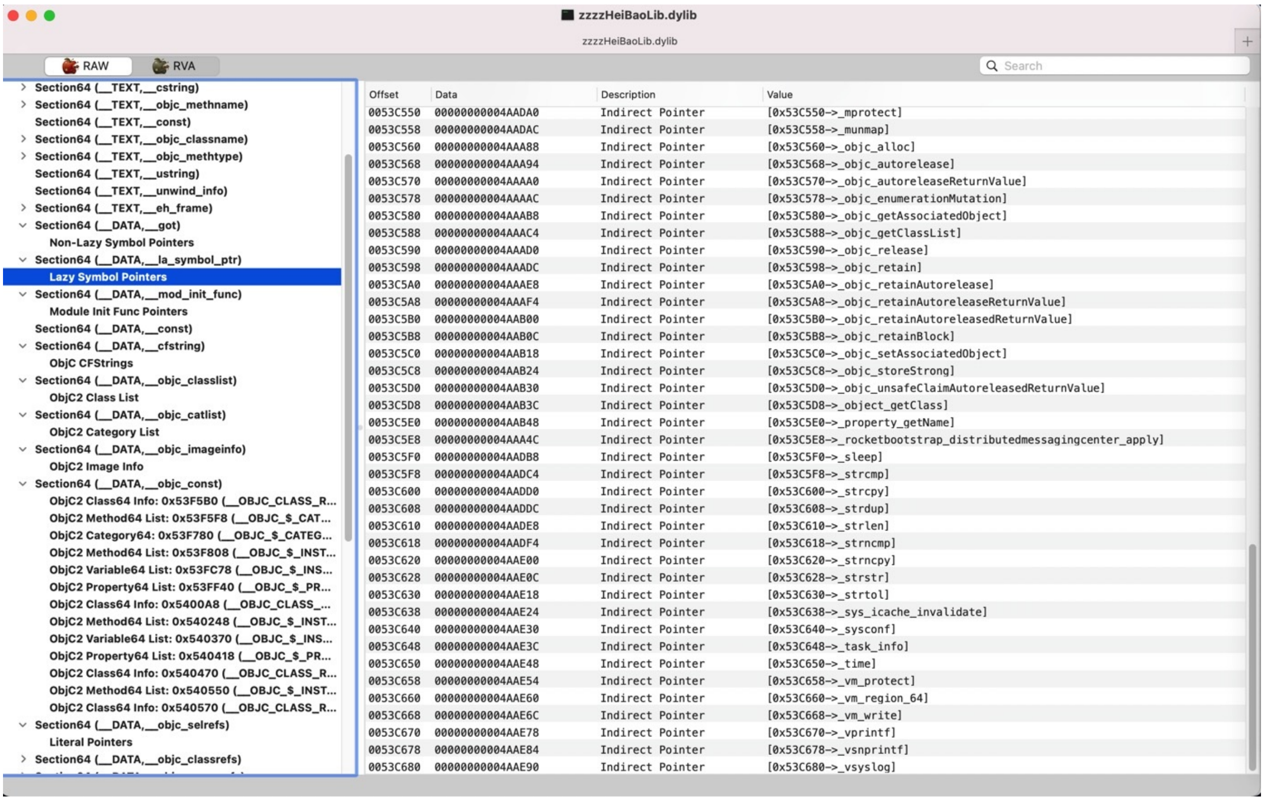
DATA,la_symbol_ptr

举例

MachOView查看zzzzHeiBaoLib.dylib

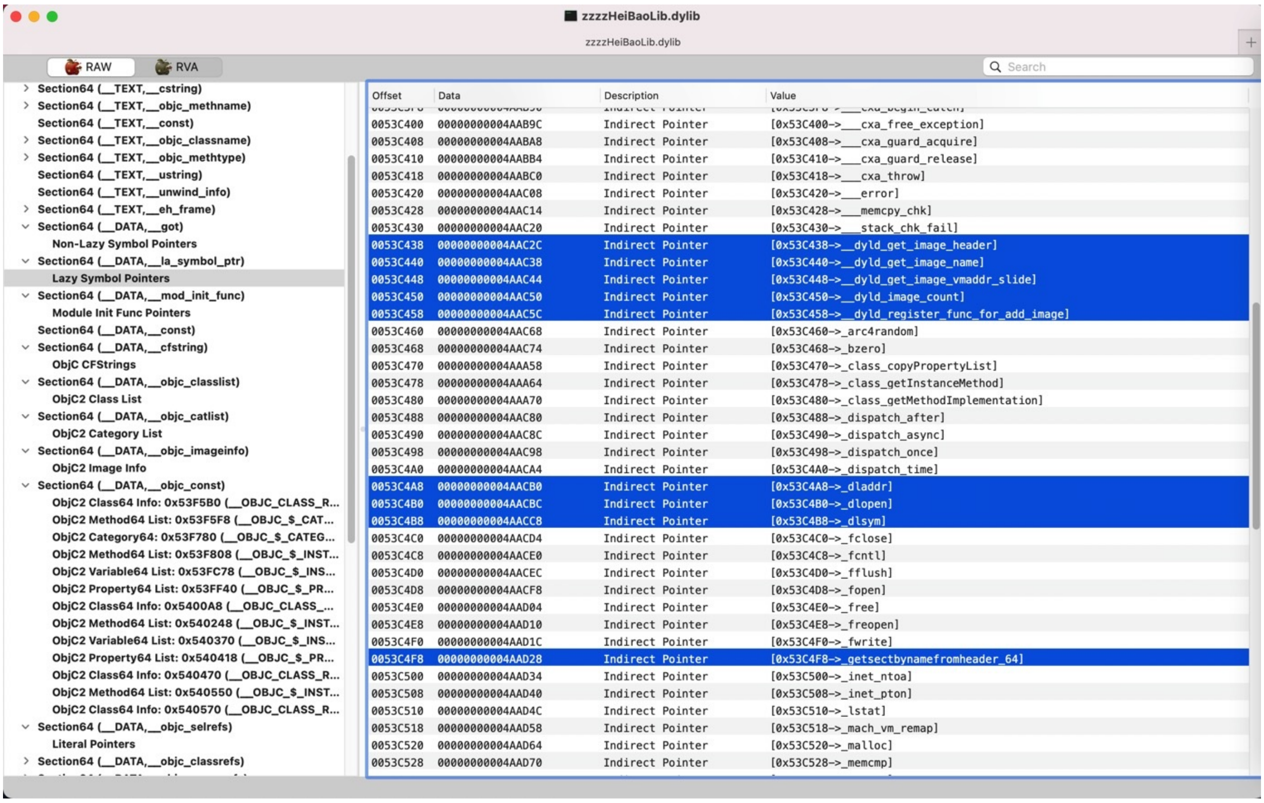






分析：

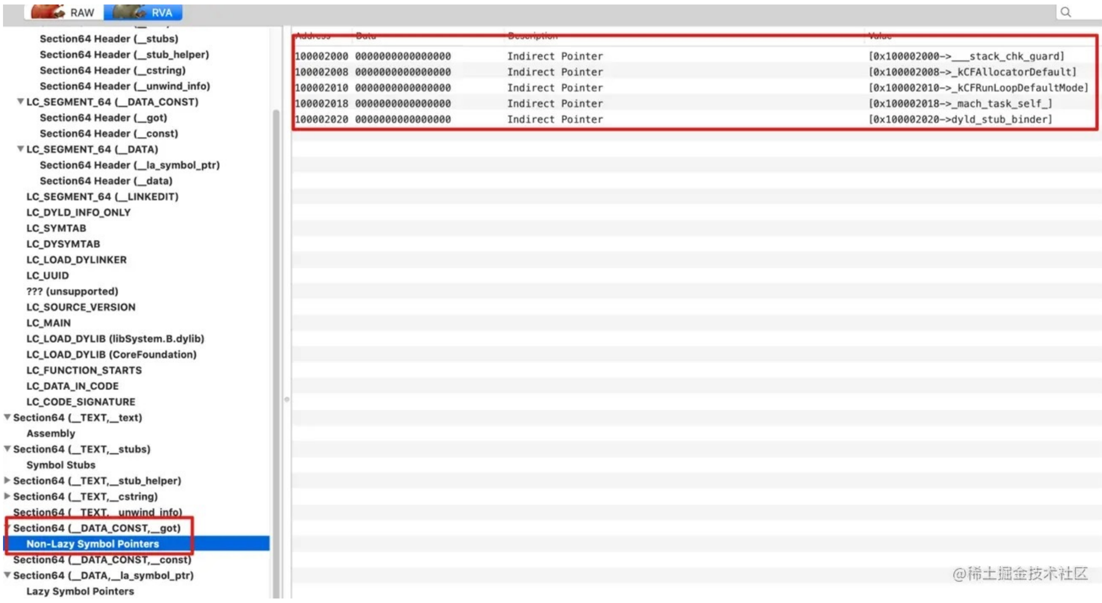
其中很多函数，就是IDA中Imports的函数：



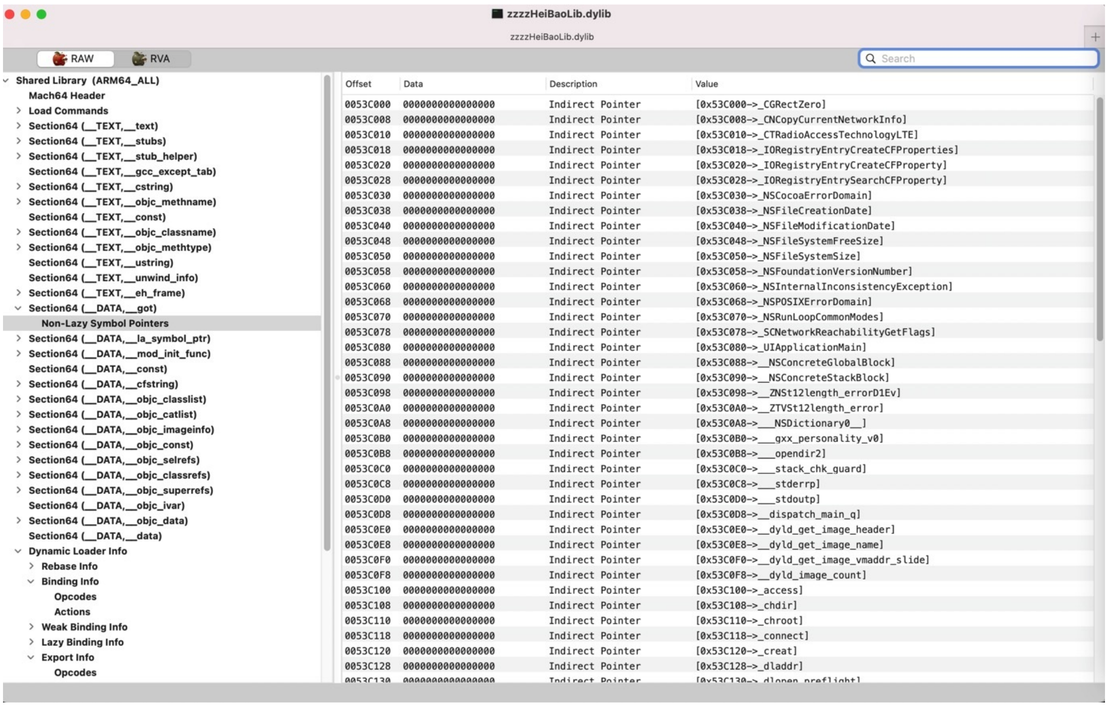
DATA,got

- `GOT = Global Offset Table = 全局符号偏移表`
    - 解释
        - iOS 开发中，动态库是个绕不开的话题，系统库基本上是动态库。它的一大优势是节约内存，可让多个程序映射同一份的动态库，实现代码共享。动态库本身也是一个 Mach-O 文件，也有数据段、代码段等。其中代码段可读可执行，数据段可读可写。
        - 动态库共享的只是代码段部分，为了达到代码段共享的目的，其符号地址在生成时就不能写死，因为它映射到每个程序中虚拟内存空间中的位置可能不一样。对于数据段部分，由于各个程序会对其进行修改，因此每个程序会单独映射一份。
        - 那么如何解决代码段共享的问题呢？聪明的人们，想出一种精妙的解决方式。通过添加一个中间层，到另一个表中去查找符号的地址。这个表就叫 `got = global offset table = 全局符号偏移表` ，然后在运行时绑定地址信息，将地址填入到 `got` 中。这样代码段中的符号就与具体地址无关，只和 got 中的数据有关。这种方式就叫 `PIC = Program Independent Code = 地址无关代码`

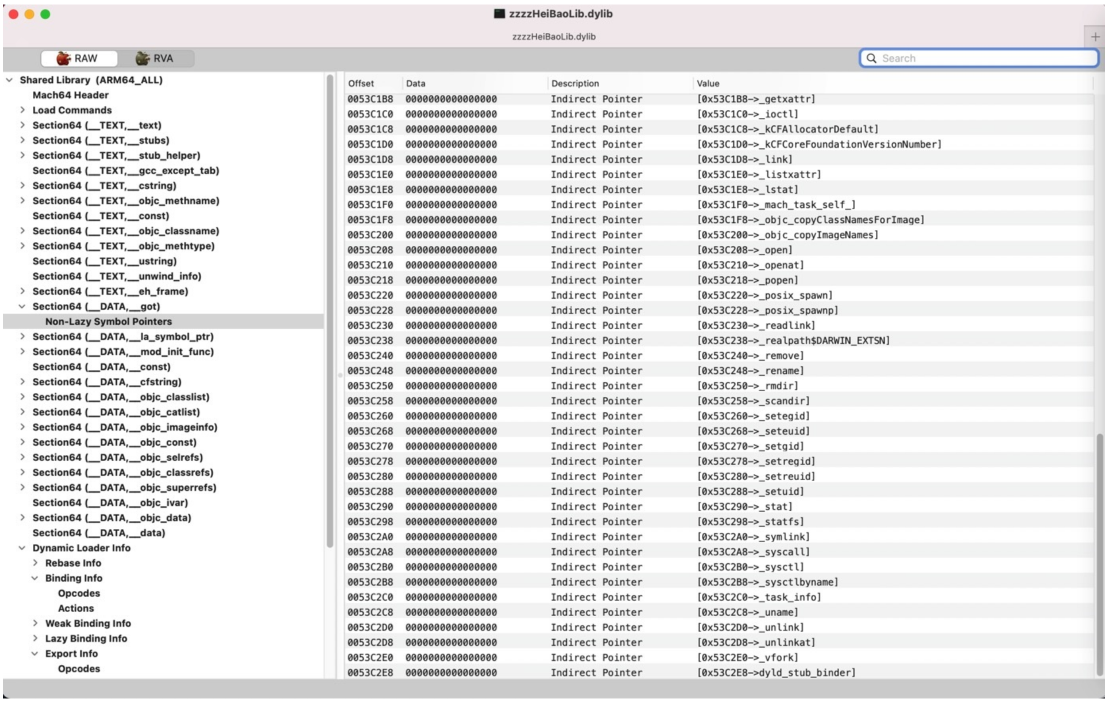
举例

- MachOView查看
    - 某程序
        - 

    - zzzzHeiBaoLib.dylib

- 

zzzzHeiBaoLib.dylib
zzzzHeiBaoLib.dylib
RAW
RVA
Search
Shared Library (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__gcc_except_tab)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__objc_methname)
Section64 (__TEXT,__const)
Section64 (__TEXT,__objc_classname)
Section64 (__TEXT,__objc_methtype)
Section64 (__TEXT,__ustring)
Section64 (__TEXT,__unwind_info)
Section64 (__TEXT,__eh_frame)
Section64 (__DATA,__got)
Non-Lazy Symbol Pointers
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__mod_init_func)
Section64 (__DATA,__const)
Section64 (__DATA,__cfstring)
Section64 (__DATA,__objc_classlist)
Section64 (__DATA,__objc_catlist)
Section64 (__DATA,__objc_imageinfo)
Section64 (__DATA,__objc_const)
Section64 (__DATA,__objc_selrefs)
Section64 (__DATA,__objc_classrefs)
Section64 (__DATA,__objc_superrefs)
Section64 (__DATA,__objc_ivar)
Section64 (__DATA,__objc_data)
Section64 (__DATA,__data)
Dynamic Loader Info
Rebase Info
Binding Info
Opcodes
Actions
Weak Binding Info
Lazy Binding Info
Export Info
Opcodes
Offset Data Description Value
0053C000 0000000000000000 Indirect Pointer [0x53C000->_CGRectZero]
0053C008 0000000000000000 Indirect Pointer [0x53C008->_CNCopyCurrentNetworkInfo]
0053C010 0000000000000000 Indirect Pointer [0x53C010->_CTRadioAccessTechnologyLTE]
0053C018 0000000000000000 Indirect Pointer [0x53C018->_IORegistryEntryCreateCFProperties]
0053C020 0000000000000000 Indirect Pointer [0x53C020->_IORegistryEntryCreateCFProperty]
0053C028 0000000000000000 Indirect Pointer [0x53C028->_IORegistryEntrySearchCFProperty]
0053C030 0000000000000000 Indirect Pointer [0x53C030->_NSCocoaErrorDomain]
0053C038 0000000000000000 Indirect Pointer [0x53C038->_NSFileCreationDate]
0053C040 0000000000000000 Indirect Pointer [0x53C040->_NSFileModificationDate]
0053C048 0000000000000000 Indirect Pointer [0x53C048->_NSFileSystemFreeSize]
0053C050 0000000000000000 Indirect Pointer [0x53C050->_NSFileSystemSize]
0053C058 0000000000000000 Indirect Pointer [0x53C058->_NSFoundationVersionNumber]
0053C060 0000000000000000 Indirect Pointer [0x53C060->_NSInternalInconsistencyException]
0053C068 0000000000000000 Indirect Pointer [0x53C068->_NSPOSIXErrorDomain]
0053C070 0000000000000000 Indirect Pointer [0x53C070->_NSRunLoopCommonModes]
0053C078 0000000000000000 Indirect Pointer [0x53C078->_SCNetworkReachabilityGetFlags]
0053C080 0000000000000000 Indirect Pointer [0x53C080->_UIApplicationMain]
0053C088 0000000000000000 Indirect Pointer [0x53C088->__NSConcreteGlobalBlock]
0053C090 0000000000000000 Indirect Pointer [0x53C090->__NSConcreteStackBlock]
0053C098 0000000000000000 Indirect Pointer [0x53C098->__ZNSt12length_errorD1Ev]
0053C0A0 0000000000000000 Indirect Pointer [0x53C0A0->__ZTVSt12length_error]
0053C0A8 0000000000000000 Indirect Pointer [0x53C0A8->___NSDictionary0__]
0053C0B0 0000000000000000 Indirect Pointer [0x53C0B0->___gxx_personality_v0]
0053C0B8 0000000000000000 Indirect Pointer [0x53C0B8->___opendir2]
0053C0C0 0000000000000000 Indirect Pointer [0x53C0C0->___stack_chk_guard]
0053C0C8 0000000000000000 Indirect Pointer [0x53C0C8->___stderrp]
0053C0D0 0000000000000000 Indirect Pointer [0x53C0D0->___stdoutp]
0053C0D8 0000000000000000 Indirect Pointer [0x53C0D8->__dispatch_main_q]
0053C0E0 0000000000000000 Indirect Pointer [0x53C0E0->__dyld_get_image_header]
0053C0E8 0000000000000000 Indirect Pointer [0x53C0E8->__dyld_get_image_name]
0053C0F0 0000000000000000 Indirect Pointer [0x53C0F0->__dyld_get_image_vmaddr_slide]
0053C0F8 0000000000000000 Indirect Pointer [0x53C0F8->__dyld_image_count]
0053C100 0000000000000000 Indirect Pointer [0x53C100->_access]
0053C108 0000000000000000 Indirect Pointer [0x53C108->_chdir]
0053C110 0000000000000000 Indirect Pointer [0x53C110->_chroot]
0053C118 0000000000000000 Indirect Pointer [0x53C118->_connect]
0053C120 0000000000000000 Indirect Pointer [0x53C120->_creat]
0053C128 0000000000000000 Indirect Pointer [0x53C128->_dladdr]

- 

zzzzHeiBaoLib.dylib
zzzzHeiBaoLib.dylib
RAW
RVA
Search
Shared Library (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__gcc_except_tab)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__objc_methname)
Section64 (__TEXT,__const)
Section64 (__TEXT,__objc_classname)
Section64 (__TEXT,__objc_methtype)
Section64 (__TEXT,__ustring)
Section64 (__TEXT,__unwind_info)
Section64 (__TEXT,__eh_frame)
Section64 (__DATA,__got)
Non-Lazy Symbol Pointers
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__mod_init_func)
Section64 (__DATA,__const)
Section64 (__DATA,__cfstring)
Section64 (__DATA,__objc_classlist)
Section64 (__DATA,__objc_catlist)
Section64 (__DATA,__objc_imageinfo)
Section64 (__DATA,__objc_const)
Section64 (__DATA,__objc_selrefs)
Section64 (__DATA,__objc_classrefs)
Section64 (__DATA,__objc_superrefs)
Section64 (__DATA,__objc_ivar)
Section64 (__DATA,__objc_data)
Section64 (__DATA,__data)
Dynamic Loader Info
Rebase Info
Binding Info
Opcodes
Actions
Weak Binding Info
Lazy Binding Info
Export Info
Opcodes
Offset Data Description Value
0053C1B8 0000000000000000 Indirect Pointer [0x53C1B8->_getxattr]
0053C1C0 0000000000000000 Indirect Pointer [0x53C1C0->_ioctl]
0053C1C8 0000000000000000 Indirect Pointer [0x53C1C8->_kCFAllocatorDefault]
0053C1D0 0000000000000000 Indirect Pointer [0x53C1D0->_kCFCoreFoundationVersionNumber]
0053C1D8 0000000000000000 Indirect Pointer [0x53C1D8->_link]
0053C1E0 0000000000000000 Indirect Pointer [0x53C1E0->_listxattr]
0053C1E8 0000000000000000 Indirect Pointer [0x53C1E8->_lstat]
0053C1F0 0000000000000000 Indirect Pointer [0x53C1F0->_mach_task_self_]
0053C1F8 0000000000000000 Indirect Pointer [0x53C1F8->_objc_copyClassNamesForImage]
0053C200 0000000000000000 Indirect Pointer [0x53C200->_objc_copyImageNames]
0053C208 0000000000000000 Indirect Pointer [0x53C208->_open]
0053C210 0000000000000000 Indirect Pointer [0x53C210->_openat]
0053C218 0000000000000000 Indirect Pointer [0x53C218->_popen]
0053C220 0000000000000000 Indirect Pointer [0x53C220->_posix_spawn]
0053C228 0000000000000000 Indirect Pointer [0x53C228->_posix_spawnp]
0053C230 0000000000000000 Indirect Pointer [0x53C230->_readlink]
0053C238 0000000000000000 Indirect Pointer [0x53C238->_realpath$DARWIN_EXTSN]
0053C240 0000000000000000 Indirect Pointer [0x53C240->_remove]
0053C248 0000000000000000 Indirect Pointer [0x53C248->_rename]
0053C250 0000000000000000 Indirect Pointer [0x53C250->_rmdir]
0053C258 0000000000000000 Indirect Pointer [0x53C258->_scandir]
0053C260 0000000000000000 Indirect Pointer [0x53C260->_setegid]
0053C268 0000000000000000 Indirect Pointer [0x53C268->_seteuid]
0053C270 0000000000000000 Indirect Pointer [0x53C270->_setgid]
0053C278 0000000000000000 Indirect Pointer [0x53C278->_setregid]
0053C280 0000000000000000 Indirect Pointer [0x53C280->_setreuid]
0053C288 0000000000000000 Indirect Pointer [0x53C288->_setuid]
0053C290 0000000000000000 Indirect Pointer [0x53C290->_stat]
0053C298 0000000000000000 Indirect Pointer [0x53C298->_statfs]
0053C2A0 0000000000000000 Indirect Pointer [0x53C2A0->_symlink]
0053C2A8 0000000000000000 Indirect Pointer [0x53C2A8->_syscall]
0053C2B0 0000000000000000 Indirect Pointer [0x53C2B0->_sysctl]
0053C2B8 0000000000000000 Indirect Pointer [0x53C2B8->_sysctlbyname]
0053C2C0 0000000000000000 Indirect Pointer [0x53C2C0->_task_info]
0053C2C8 0000000000000000 Indirect Pointer [0x53C2C8->_uname]
0053C2D0 0000000000000000 Indirect Pointer [0x53C2D0->_unlink]
0053C2D8 0000000000000000 Indirect Pointer [0x53C2D8->_unlinkat]
0053C2E0 0000000000000000 Indirect Pointer [0x53C2E0->_vfork]
0053C2E8 0000000000000000 Indirect Pointer [0x53C2E8->dyld_stub_binder]

__IMPORT

`__IMPORT` segment的section：

- `__IMPORT,__jump_table`
  - Stubs for calls to functions in a dynamic library.
- `__IMPORT,__pointers`
  - Non-lazy symbol pointers, which are direct references to functions imported from a different file.

__LINKEDIT

- 用户层的完全链接后的Mach-O文件，最后一个segment是 `link edit`
  - 包含 `link edit` 信息
    - `Symbol Table` = `符号表`
    - `String Table` = `字符串表`
    - 等等
  - 用于：动态加载器 `dynamic loader` 去链接所依赖的库

__OBJC

- segment: `__OBJC`
    - 相关解释
        - Objective-C是一种Reflection反射型语言，可以在运行时获取和修改自身状态，其中的实现存在于 `libobjc.A.dylib` 库中，这些“运行时”能力源于objective-c类结构组织较为灵活，并提供了操作自身结构的接口，同时在生成的可执行文件(`Mach-O`)中存在 `__OBJC` 段，这些节中提供了足够的类构成信息，而Mac端gdb可以解析这些结构，而正由于objc提供了如此多的信息，因此也比c++在同等情况下逆向难度低一些。

section节

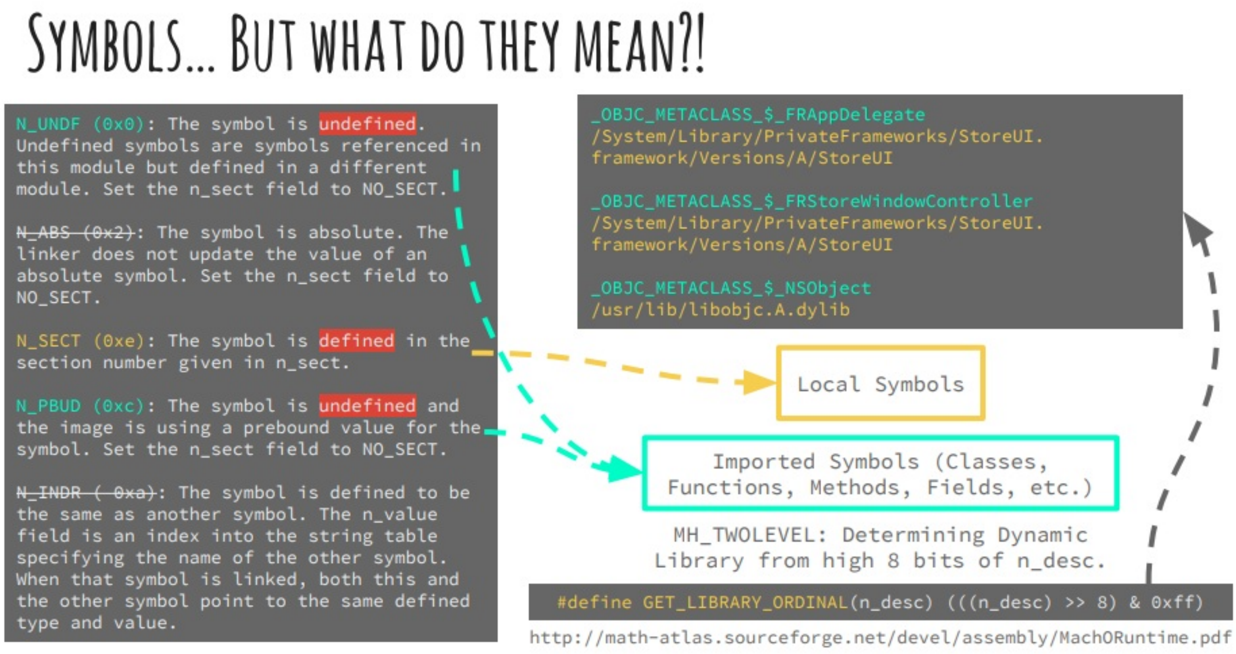
section定义

源码定义:

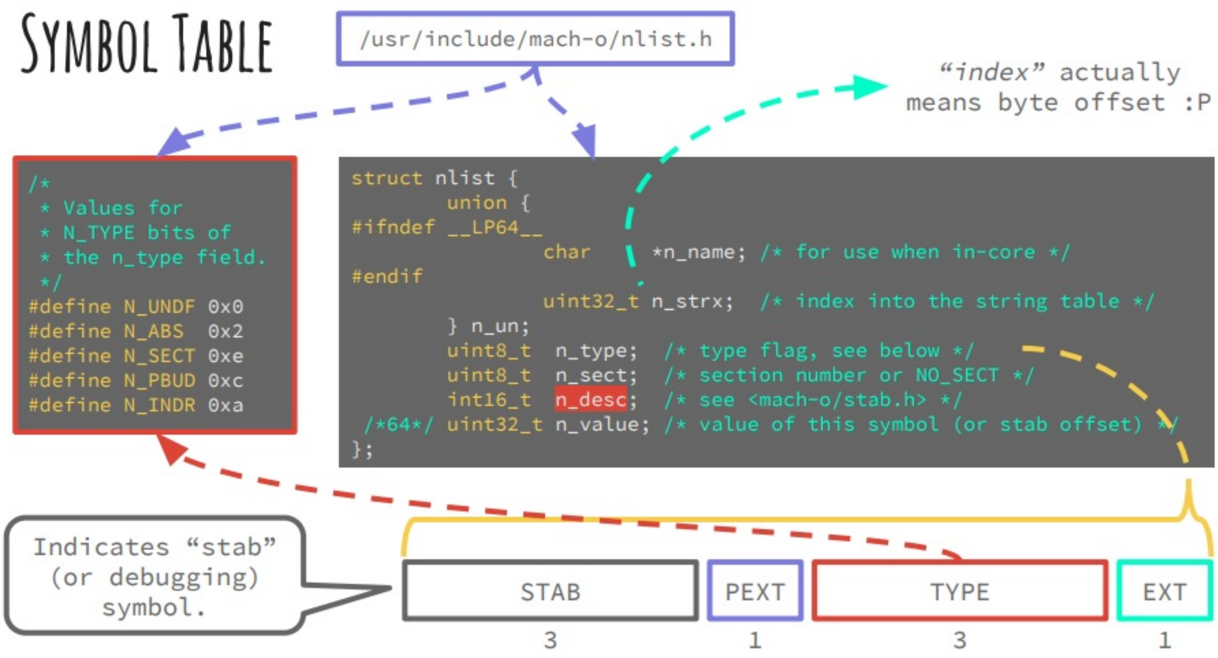
```
/*
 * A segment is made up of zero or more sections.  Non-MH_OBJECT files have
 * all of their segments with the proper sections in each, and padded to the
 * specified segment alignment when produced by the link editor.  The first
 * segment of a MH_EXECUTE and MH_FVMLIB format file contains the mach_header
 * and load commands of the object file before its first section.  The zero
 * fill sections are always last in their segment (in all formats).  This
 * allows the zeroed segment padding to be mapped into memory where zero fill
 * sections might be. The gigabyte zero fill sections, those with the section
 * type S_GB_ZEROFILL, can only be in a segment with sections of this type.
 * These segments are then placed after all other segments.
 *
 * The MH_OBJECT format has all of its sections in one segment for
 * compactness.  There is no padding to a specified segment boundary and the
 * mach_header and load commands are not part of the segment.
 *
 * Sections with the same section name, sectname, going into the same segment,
 * segname, are combined by the link editor.  The resulting section is aligned
 * to the maximum alignment of the combined sections and is the new section's
 * alignment.  The combined sections are aligned to their original alignment in
 * the combined section.  Any padded bytes to get the specified alignment are
 * zeroed.
 *
 * The format of the relocation entries referenced by the reloff and nreloc
 * fields of the section structure for mach object files is described in the
 * header file <reloc.h>.
 */
struct section { /* for 32-bit architectures */
    char        sectname[16];    /* name of this section */
    char        segname[16];    /* segment this section goes in */
    uint32_t    addr;        /* memory address of this section */
    uint32_t    size;        /* size in bytes of this section */
    uint32_t    offset;        /* file offset of this section */
    uint32_t    align;        /* section alignment (power of 2) */
    uint32_t    reloff;        /* file offset of relocation entries */
    uint32_t    nreloc;        /* number of relocation entries */
    uint32_t    flags;        /* flags (section type and attributes)*/
    uint32_t    reserved1;    /* reserved (for offset or index) */
    uint32_t    reserved2;    /* reserved (for count or sizeof) */
};

struct section_64 { /* for 64-bit architectures */
    char        sectname[16];    /* name of this section */
    char        segname[16];    /* segment this section goes in */
    uint64_t    addr;        /* memory address of this section */
    uint64_t    size;        /* size in bytes of this section */
```

```
    uint32_t    offset;        /* file offset of this section */
    uint32_t    align;        /* section alignment (power of 2) */
    uint32_t    reloff;        /* file offset of relocation entries */
    uint32_t    nreloc;        /* number of relocation entries */
    uint32_t    flags;        /* flags (section type and attributes)*/
    uint32_t    reserved1;    /* reserved (for offset or index) */
    uint32_t    reserved2;    /* reserved (for count or sizeof) */
    uint32_t    reserved3;    /* reserved */
};
```

symbol



nlist定义



nlist_64定义

```
struct nlist_64 {
    union {
        uint32_t  n_strx; /* index into the string table */
    } n_un;
    uint8_t n_type;        /* type flag, see below */
```

```
    uint8_t n_sect;        /* section number or NO_SECT */
    uint16_t n_desc;       /* see <mach-o/stab.h> */
    uint64_t n_value;      /* value of this symbol (or stab offset) */
};
/*
 * Symbols with a index into the string table of zero (n_un.n_strx == 0) are
 * defined to have a null, "", name.  Therefore all string indexes to non null
 * names must not have a zero string index.  This is bit historical information
 * that has never been well documented.
 */

/*
 * The n_type field really contains four fields:
 *    unsigned char N_STAB:3,
 *              N_PEXT:1,
 *              N_TYPE:3,
 *              N_EXT:1;
 * which are used via the following masks.
 */
#define    N_STAB    0xe0  /* if any of these bits set, a symbolic debugging entry */
#define    N_PEXT    0x10  /* private external symbol bit */
#define    N_TYPE    0x0e  /* mask for the type bits */
#define    N_EXT    0x01  /* external symbol bit, set for external symbols */
```

举例

- MachOView查看到的 `Symbol Table`
    -
        - 说明
            - String表的偏移量是 `0xbbff8` ，翻译后是 `[GMRYouHaoHuoReq getRequestURL]`
            - 地址是 `0x100003300`

string

- String Table
    - String表顺序列出了二进制mach-O文件的中的所有可见字符串。串之间通过0x00分隔。可以通过相对String表起始位置的偏移量随机访问String表中的字符串。符号表结构中的n_strx指定的就是String表中的偏移量。通过这个偏移量可以访问到符号对应的具体字符串

举例

- MachOView查看到的某 `String Table`
    -
        - 说明
            - String表的 `0xbbf8` 处是不是 `[GMRYouHaoHuoReq getRequestURL]` ，string表的地址是 `0x049C6D40` 加上偏移量 `0x000BBFB1` ，等于 `0x54d633d`
            - 可以看出string表的 `0x54d633d` 地址出就是： `[GMRYouHaoHuoReq getRequestURL]`

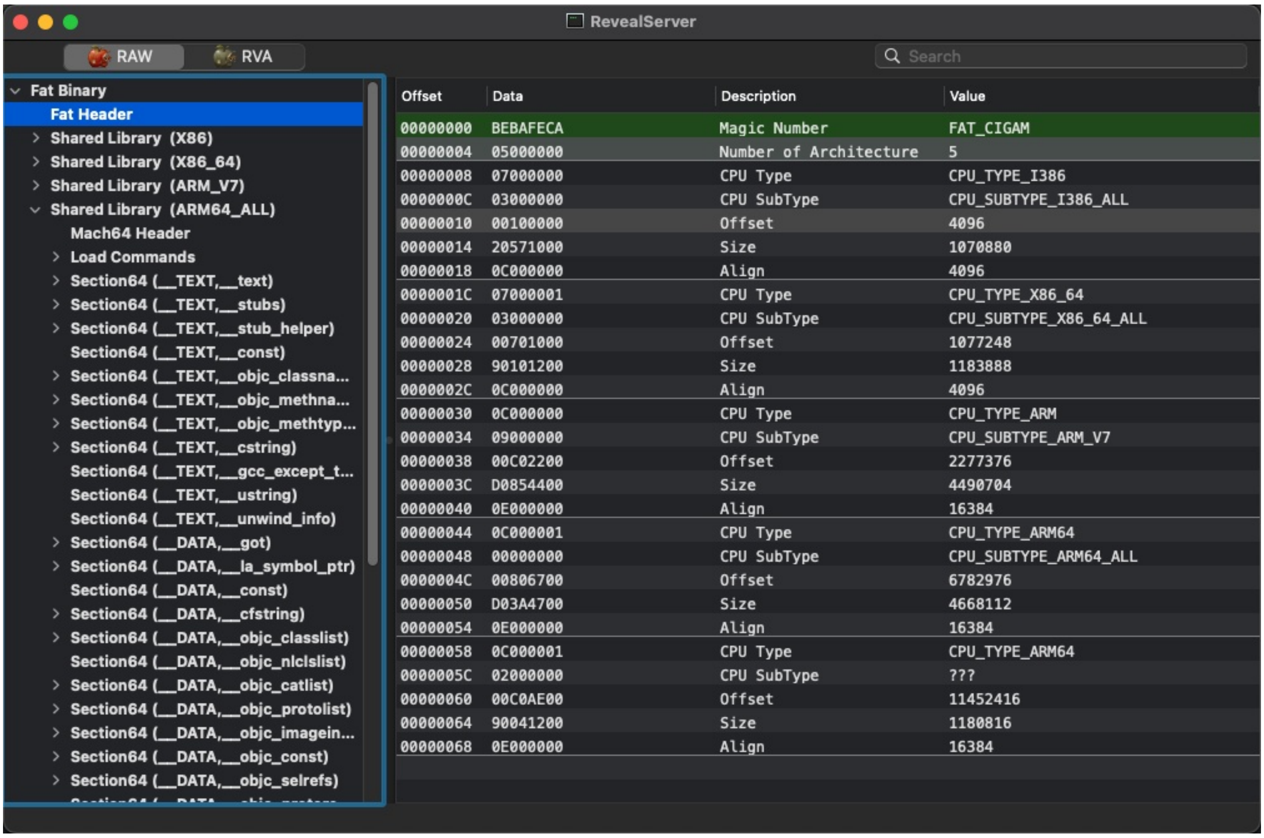
FAT

- `FAT`
  - 名称
    - `Fat Binary` = 胖二进制
      - = `Fat File` = 胖二进制文件
      - = `Universal Binary` = 通用二进制
  - 含义：把多个架构的二进制（比如 `armv7` 、 `arm64` 等）合并在一起，成了个胖子，所以叫 `Fat Binary`
    - 一个由**不同的编译架构**后的 `Mach-O` 产物所合成的集合体
    - 一个架构的 `Mach-O` 只能在相同架构的机器或者模拟器上用
    - 为了支持不同架构需要一个集合体
  - 文件大小
    - 一般比单一架构的文件要大
    - 但是由于多架构会共用一部分资源，所以往往比多个（常常是2个）的总大小要小

FAT举例

用MachOView查看

RevealServer



用file查看

可以用 `file` ：查看Mach-O的文件类型

- 语法： `file inputMacOFile`

RevealServer

```
crifan@licrifandeMacBook-Pro  ~/dev/dev_tool/reverse_security/iOS/Tweak/Reveal2Loader/lemon4ex  file Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealServer
Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealServer: Mach-O universal binary with 5 architectures: [i386:Mach-O dynamically linked shared library i386] [x86_64] [arm_v7] [arm64] [arm64e]
Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealServer (for architecture i386):    Mach-O dynamically linked shared library i386
Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealServer (for architecture x86_64):    Mach-O 64-bit dynamically linked shared library x86_64
```

```
Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealSer
ver (for architecture armv7):    Mach-O dynamically linked shared library arm_v7
Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealSer
ver (for architecture arm64):    Mach-O 64-bit dynamically linked shared library arm64
Reveal2Loader/Reveal2Loader/Package/Library/Frameworks/RevealServer.framework/RevealSer
ver (for architecture arm64e):    Mach-O 64-bit dynamically linked shared library arm64
e
```

rsync

```
➜  ~ which rsync
/usr/bin/rsync
➜  ~ file /usr/bin/rsync
/usr/bin/rsync: Mach-O universal binary with 2 architectures: [x86_64:Mach-O 64-bit exe
cutable x86_64] [arm64e:Mach-O 64-bit executable arm64e]
/usr/bin/rsync (for architecture x86_64):    Mach-O 64-bit executable x86_64
/usr/bin/rsync (for architecture arm64e):    Mach-O 64-bit executable arm64e
```

adb

```
➜  platform-tools pwd
/Users/crifan/dev/dev_tool/android/AndroidSDK/platform-tools
➜  platform-tools ll
total 49520
...
-rwxr-xr-x@ 1 crifan  staff    13M  7 24 15:26 adb
...
➜  platform-tools file adb
adb: Mach-O universal binary with 2 architectures: [x86_64:Mach-O 64-bit executable x86
_64] [arm64]
adb (for architecture x86_64):    Mach-O 64-bit executable x86_64
adb (for architecture arm64):    Mach-O 64-bit executable arm64
```

lldb

```
➜  ~ file /usr/bin/lldb
/usr/bin/lldb: Mach-O universal binary with 2 architectures: [x86_64:Mach-O 64-bit exec
utable x86_64] [arm64e:Mach-O 64-bit executable arm64e]
/usr/bin/lldb (for architecture x86_64):    Mach-O 64-bit executable x86_64
/usr/bin/lldb (for architecture arm64e):    Mach-O 64-bit executable arm64e
```

debugserver

```
crifan@licrifandeMacBook-Pro ~/dev/dev_root/iosReverse/AppleStore/fromiPhone8/Develope
r/usr/bin ll
total 5240
-rw-r--r--  1 crifan  staff   832B  3  3 11:48 debugable_entitlement.xml
-rwxrwxr-x  1 crifan  staff   1.3M  8  8  2021 debugserver
-rwxr-xr-x  1 crifan  staff   1.3M  3  3 11:49 debugserver_debugable
```

```
 crifan@licrifandeMacBook-Pro ~/dev/dev_root/iosReverse/AppleStore/fromiPhone8/Develop
er/usr/bin file debugserver
debugserver: Mach-O universal binary with 2 architectures: [arm64:Mach-O 64-bit executa
ble arm64] [arm64e:Mach-O 64-bit executable arm64e]
debugserver (for architecture arm64):    Mach-O 64-bit executable arm64
debugserver (for architecture arm64e):    Mach-O 64-bit executable arm64e
```

FAT常见问题

Select an architecture setting the ARCH= environment variable

用jtool2导出Mask的dylib信息期间就遇到了 `FAT Binary` ：

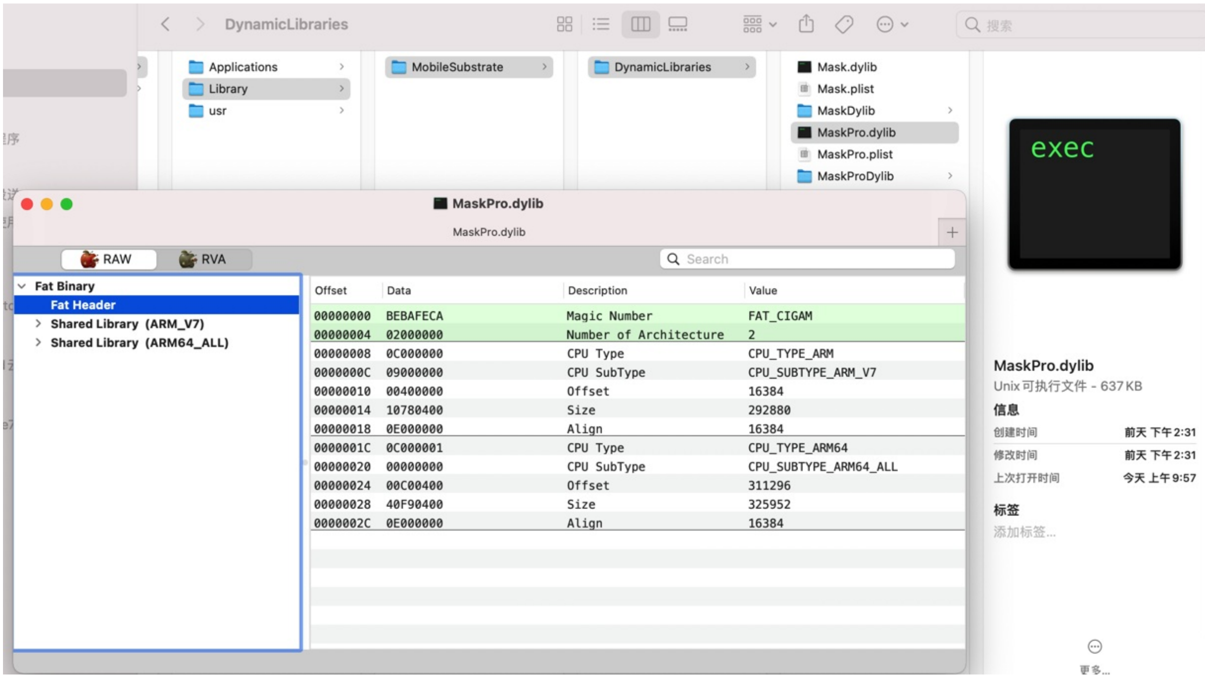
```
➜ DynamicLibraries jtool2 -h MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_h_header
.txt
Fat binary, little-endian, 2 architectures: armv7, arm64
Select an architecture setting the ARCH= environment variable
```

即，一个Dylib中，包含了多种架构，此处是 `armv7` 和 `arm64`

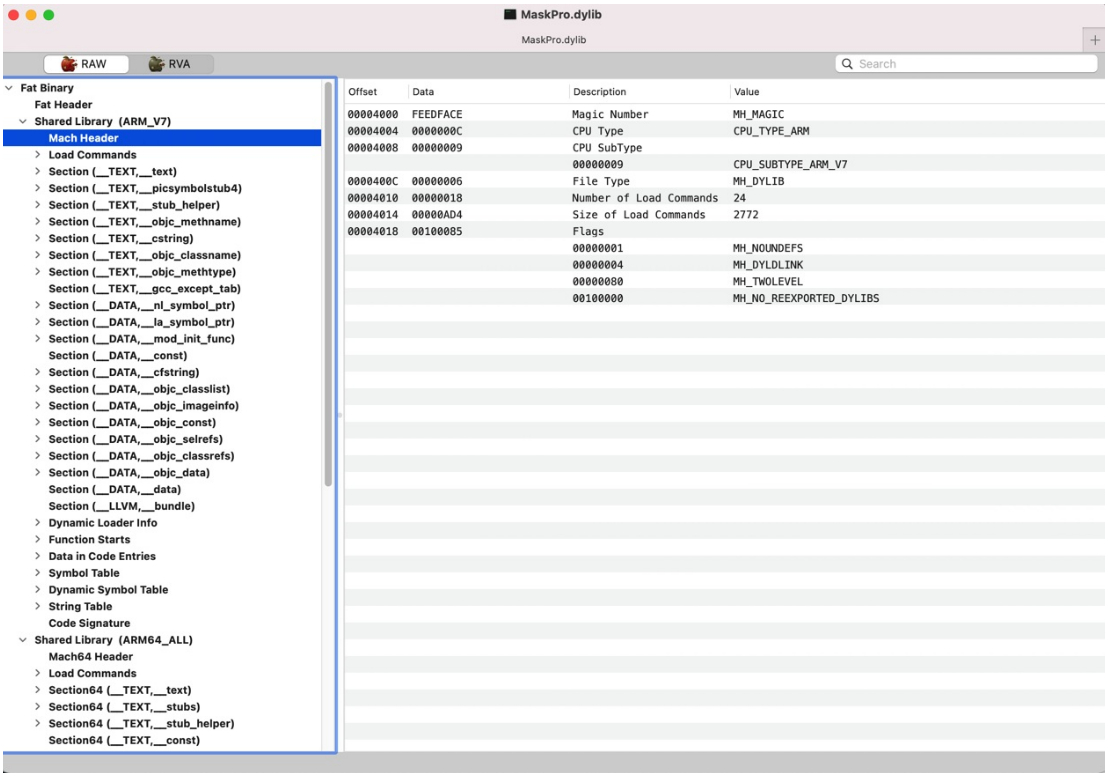
此处要指定具体架构，才能继续用 `jtool2` 查看信息：

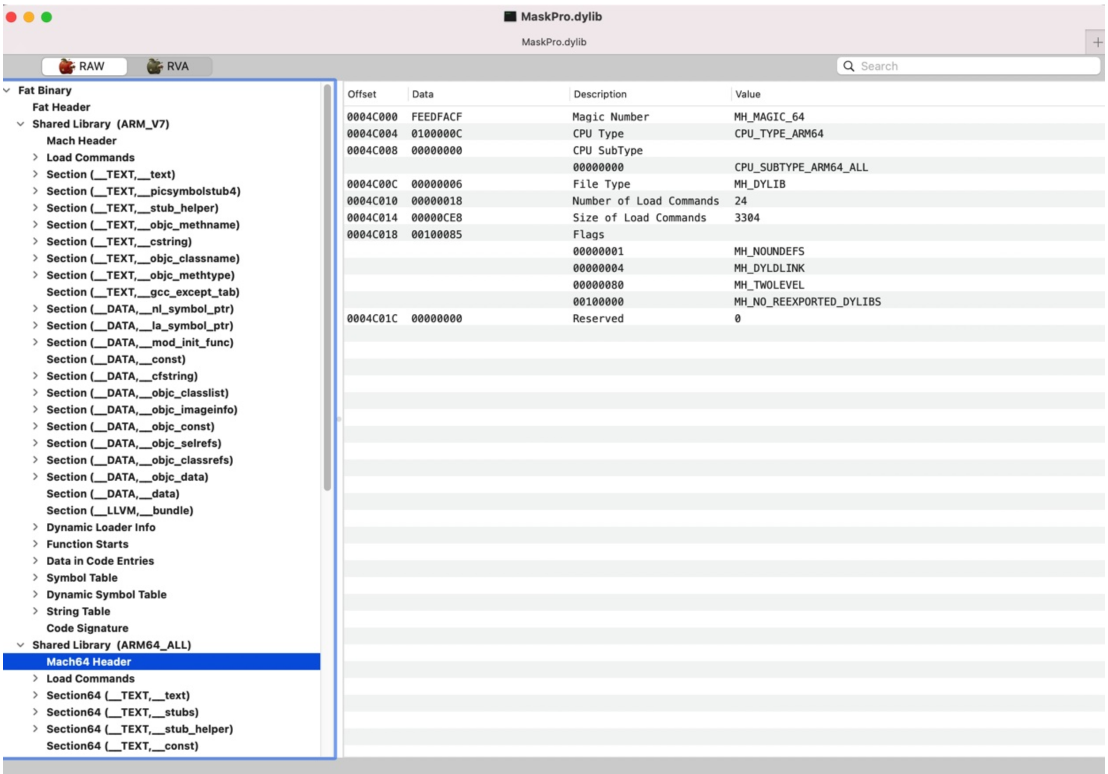
```
➜ DynamicLibraries export ARCH=arm64
➜ DynamicLibraries jtool2 -h MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_h_header
.txt
```

类似的，后续去用 `MachOView` 查看信息，也能看到是： `FAT Binary`

- 

    - ARMV7

- 
MaskPro.dylib
MaskPro.dylib
RAW
RVA
Search
Fat Binary
Fat Header
Shared Library (ARM_V7)
Mach Header
Load Commands
Section (__TEXT,__text)
Section (__TEXT,__picsymbolstub4)
Section (__TEXT,__stub_helper)
Section (__TEXT,__objc_methname)
Section (__TEXT,__cstring)
Section (__TEXT,__objc_classname)
Section (__TEXT,__objc_methtype)
Section (__TEXT,__gcc_except_tab)
Section (__DATA,__nl_symbol_ptr)
Section (__DATA,__la_symbol_ptr)
Section (__DATA,__mod_init_func)
Section (__DATA,__const)
Section (__DATA,__cfstring)
Section (__DATA,__objc_classlist)
Section (__DATA,__objc_imageinfo)
Section (__DATA,__objc_const)
Section (__DATA,__objc_selrefs)
Section (__DATA,__objc_classrefs)
Section (__DATA,__objc_data)
Section (__DATA,__data)
Section (__LLVM,__bundle)
Dynamic Loader Info
Function Starts
Data in Code Entries
Symbol Table
Dynamic Symbol Table
String Table
Code Signature
Shared Library (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__const)
Offset Data Description Value
00004000 FEEDFACE Magic Number MH_MAGIC
00004004 0000000C CPU Type CPU_TYPE_ARM
00004008 00000009 CPU SubType
00000009 CPU_SUBTYPE_ARM_V7
0000400C 00000006 File Type MH_DYLIB
00004010 00000018 Number of Load Commands 24
00004014 00000AD4 Size of Load Commands 2772
00004018 00100085 Flags
00000001 MH_NOUNDEFS
00000004 MH_DYLDLINK
00000080 MH_TWOLEVEL
00100000 MH_NO_REEXPORTED_DYLIBS

  - ARM64
    - 
MaskPro.dylib
MaskPro.dylib
RAW
RVA
Search
Fat Binary
Fat Header
Shared Library (ARM_V7)
Mach Header
Load Commands
Section (__TEXT,__text)
Section (__TEXT,__picsymbolstub4)
Section (__TEXT,__stub_helper)
Section (__TEXT,__objc_methname)
Section (__TEXT,__cstring)
Section (__TEXT,__objc_classname)
Section (__TEXT,__objc_methtype)
Section (__TEXT,__gcc_except_tab)
Section (__DATA,__nl_symbol_ptr)
Section (__DATA,__la_symbol_ptr)
Section (__DATA,__mod_init_func)
Section (__DATA,__const)
Section (__DATA,__cfstring)
Section (__DATA,__objc_classlist)
Section (__DATA,__objc_imageinfo)
Section (__DATA,__objc_const)
Section (__DATA,__objc_selrefs)
Section (__DATA,__objc_classrefs)
Section (__DATA,__objc_data)
Section (__DATA,__data)
Section (__LLVM,__bundle)
Dynamic Loader Info
Function Starts
Data in Code Entries
Symbol Table
Dynamic Symbol Table
String Table
Code Signature
Shared Library (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__const)
Offset Data Description Value
0004C000 FEEDFACF Magic Number MH_MAGIC_64
0004C004 0100000C CPU Type CPU_TYPE_ARM64
0004C008 00000000 CPU SubType
00000000 CPU_SUBTYPE_ARM64_ALL
0004C00C 00000006 File Type MH_DYLIB
0004C010 00000018 Number of Load Commands 24
0004C014 00000CE8 Size of Load Commands 3304
0004C018 00100085 Flags
00000001 MH_NOUNDEFS
00000004 MH_DYLDLINK
00000080 MH_TWOLEVEL
00100000 MH_NO_REEXPORTED_DYLIBS
0004C01C 00000000 Reserved 0

FAT工具

lipo

- `lipo` ：常用于多架构Mach-O文件的处理
    - 查看架构信息

        ```
        lipo -info inputMacOFile
        ```

    - 导出某种特定架构

        ```
        lipo inputMachOFile -thin ArchType -output OutputFile
        ```

    - 合并多种架构

        ```
        lipo inputMachOFile1 inputMachOFile2 -output OutputFile
        ```

举例

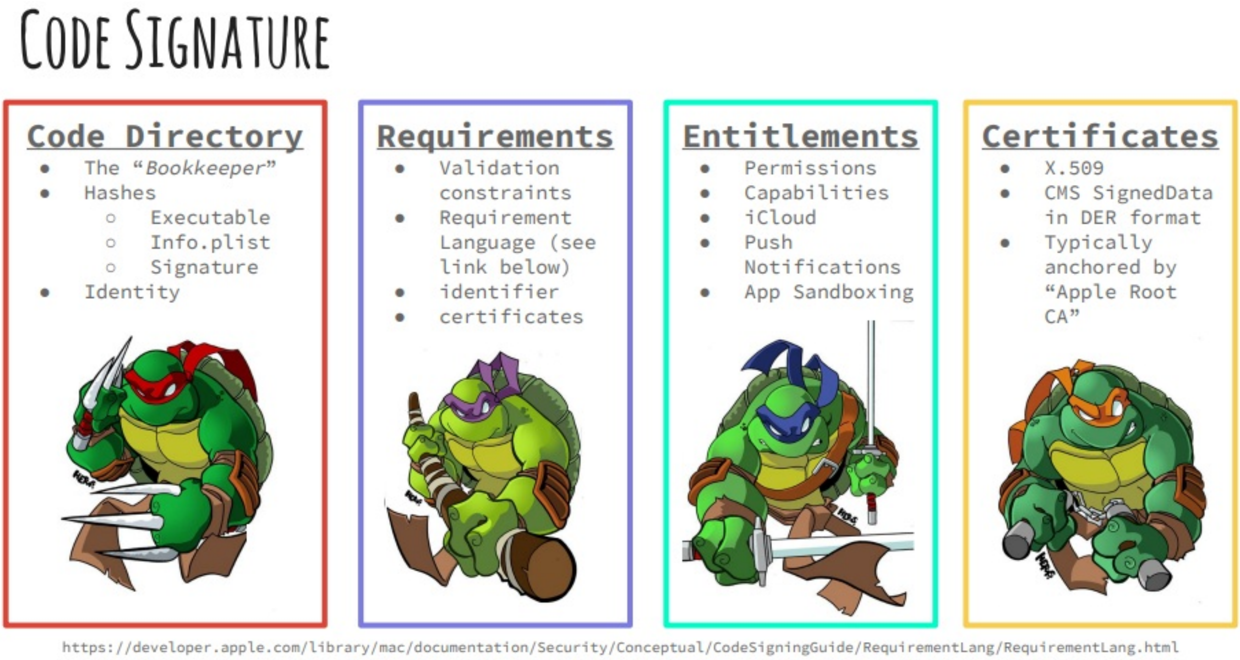
- 瘦身=导出单个架构
    - 导出arm64架构

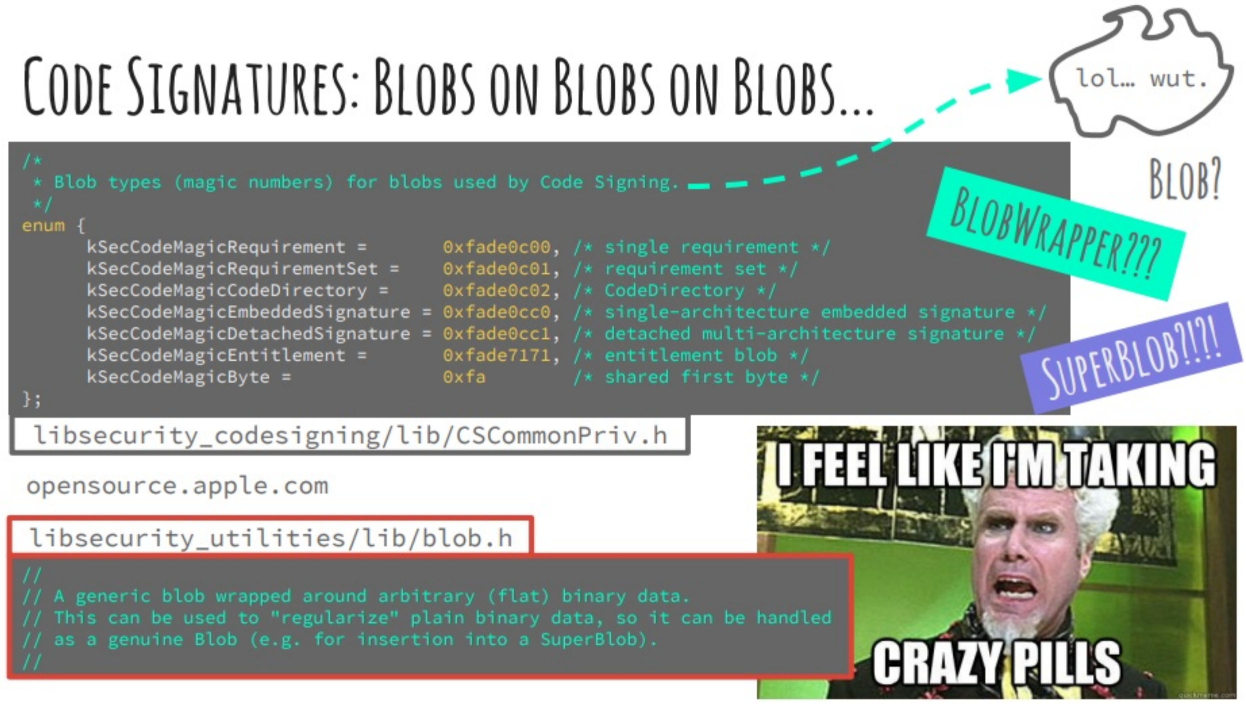
        ```
        lipo -thin arm64 debugserver_orig -output debugserver_arm64
        ```

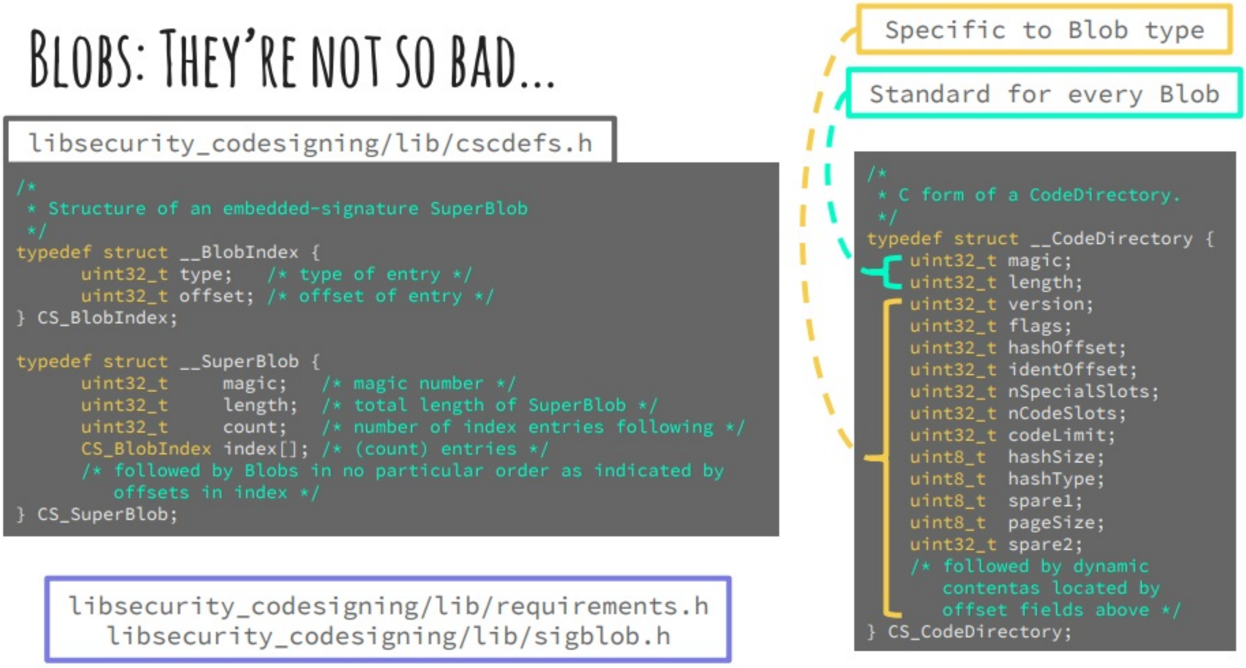
其中， `arm64` 是从 `file` 中查看到包含的多个架构中的其中一个：

```
crifan@licrifandeMacBook-Pro ~/dev/dev_root/iosReverse/AppleStore/dynamicDebug/debugserver_lldb file fromiPhone11/debugserver_orig
fromiPhone11/debugserver_orig: Mach-O universal binary with 2 architectures: [arm64:Mach-O 64-bit executable arm64] [arm64e:Mach-O 64-bit executable arm64e]
fromiPhone11/debugserver_orig (for architecture arm64):    Mach-O 64-bit executable arm64
fromiPhone11/debugserver_orig (for architecture arm64e):    Mach-O 64-bit executable arm64e
```

codesign


CODE SIGNATURE
Code Directory
• The "Bookkeeper"
• Hashes
○ Executable
○ Info.plist
○ Signature
• Identity
Requirements
• Validation constraints
• Requirement Language (see link below)
• identifier
• certificates
Entitlements
• Permissions
• Capabilities
• iCloud
• Push Notifications
• App Sandboxing
Certificates
• X.509
• CMS SignedData in DER format
• Typically anchored by "Apple Root CA"
https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/RequirementLang/RequirementLang.html

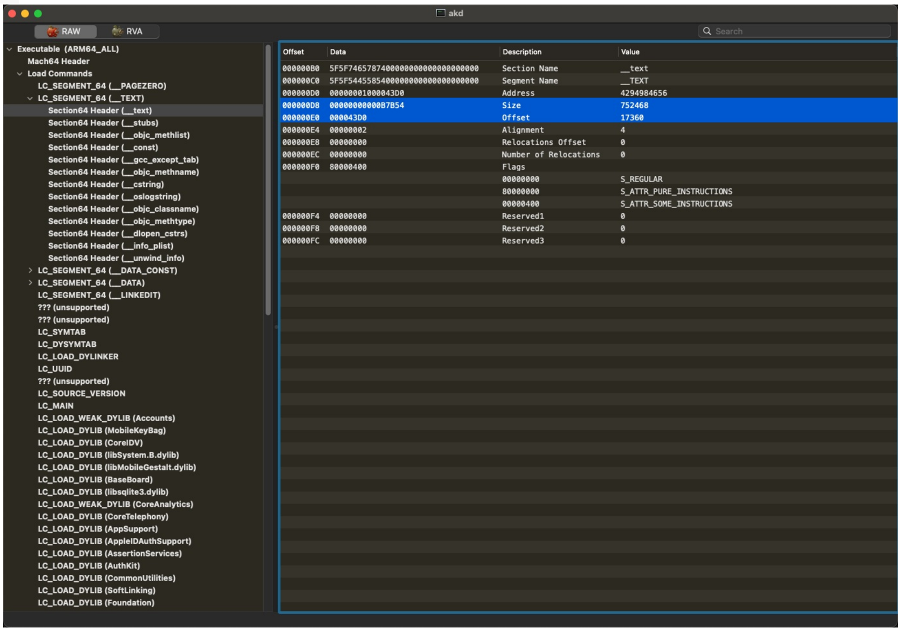
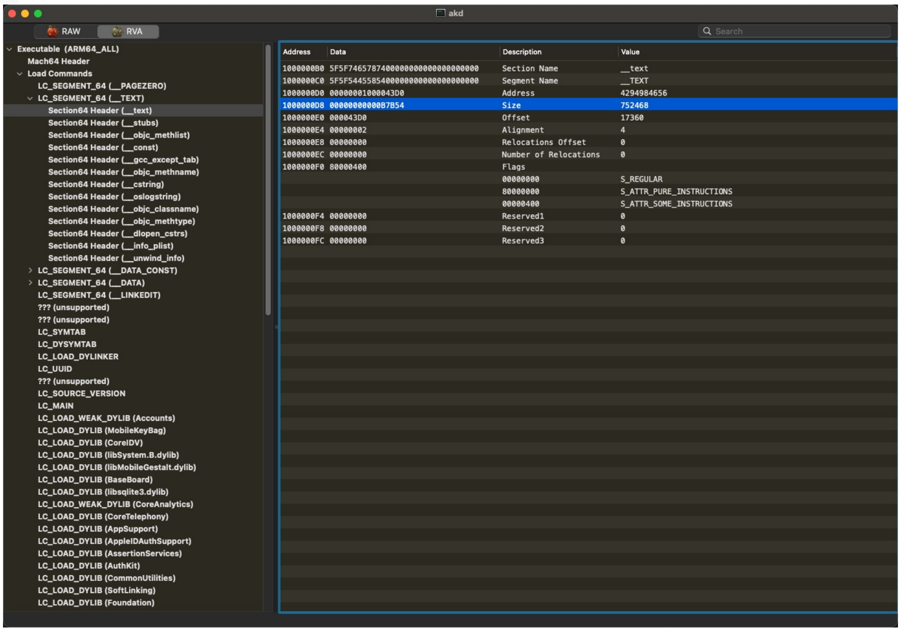

CODE SIGNATURES: BLOBS ON BLOBS ON BLOBS...
lol… wut.
BLOB?
BLOBWRAPPER???
SUPERBLOB?!?!
/*
 * Blob types (magic numbers) for blobs used by Code Signing.
 */
enum {
kSecCodeMagicRequirement = 0xfade0c00, /* single requirement */
kSecCodeMagicRequirementSet = 0xfade0c01, /* requirement set */
kSecCodeMagicCodeDirectory = 0xfade0c02, /* CodeDirectory */
kSecCodeMagicEmbeddedSignature = 0xfade0cc0, /* single-architecture embedded signature */
kSecCodeMagicDetachedSignature = 0xfade0cc1, /* detached multi-architecture signature */
kSecCodeMagicEntitlement = 0xfade7171, /* entitlement blob */
kSecCodeMagicByte = 0xfa /* shared first byte */
};
libsecurity_codesigning/lib/CSCommonPriv.h
opensource.apple.com
libsecurity_utilities/lib/blob.h
//
// A generic blob wrapped around arbitrary (flat) binary data.
// This can be used to "regularize" plain binary data, so it can be handled
// as a genuine Blob (e.g. for insertion into a SuperBlob).
//
I FEEL LIKE I'M TAKING
CRAZY PILLS

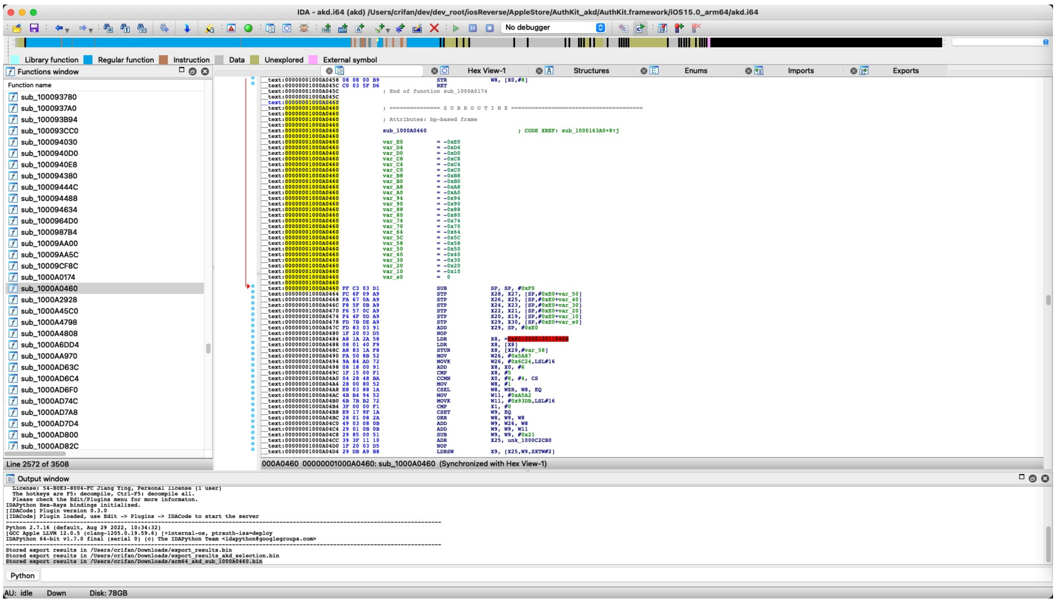


Blobs: They're not so bad...
Specific to Blob type
Standard for every Blob
libsecurity_codesigning/lib/cscdefs.h
/*
 * Structure of an embedded-signature SuperBlob
 */
typedef struct __BlobIndex {
uint32_t type; /* type of entry */
uint32_t offset; /* offset of entry */
} CS_BlobIndex;
typedef struct __SuperBlob {
uint32_t magic; /* magic number */
uint32_t length; /* total length of SuperBlob */
uint32_t count; /* number of index entries following */
CS_BlobIndex index[]; /* (count) entries */
/* followed by Blobs in no particular order as indicated by offsets in index */
} CS_SuperBlob;
libsecurity_codesigning/lib/requirements.h
libsecurity_codesigning/lib/sigblob.h
/*
 * C form of a CodeDirectory.
 */
typedef struct __CodeDirectory {
uint32_t magic;
uint32_t length;
uint32_t version;
uint32_t flags;
uint32_t hashOffset;
uint32_t identOffset;
uint32_t nSpecialSlots;
uint32_t nCodeSlots;
uint32_t codeLimit;
uint8_t hashSize;
uint8_t hashType;
uint8_t spare1;
uint8_t pageSize;
uint32_t spare2;
/* followed by dynamic contentas located by offset fields above */
} CS_CodeDirectory;

虚拟地址

- 关于虚拟地址
    - Mach-O中相关定义： `segment段 和 section节` 中的部分定义
        - `segment_command_64` 中有对应字段
            - `vmaddr`
                - `VM Address = 虚拟内存地址`
                    - 当程序被加载到内存中后，对应的（虚拟）内存地址
                        - 注：现代CPU都支持（映射后的）虚拟内存
            - `vmsize`
                - 虚拟内存中的程序大小
                    - 目前所见过的所有情况中，此值都是和文件大小一样
        - `section_64`
            - `addr`
                - 虚拟内存地址
                    - 不是我们从硬盘中读取的偏移量地址
            - `size`
                - 大小，单位是字节
                    - 适用于虚拟内存地址和文件偏移量
            - `offset`
                - （磁盘中的）文件内的偏移量
- 一般来说：
    - 有2个偏移量=地址
        - `虚拟内存 = vm`
        - `文件 = file`
    - 对应分别常被简称为
        - `vmoff`
        - `fileoff`
    - 举例
        - 最开始的起始地址
            - `fileoff` = 0x0
            - `vmoff` = 0x100000000
                - 程序常被映射到虚拟内存地址0x100000000
- 进一步说：
    - 其实有3个常见地址相关名词
        - `VA = Virtual Address = 虚拟地址`
            - `== VM Address = 虚拟内存地址`
        - `RVA = Relative Virtual Address = 相对的虚拟地址`
            - 相对于谁： `ImageBase = 二进制镜像文件的基地址`
        - `File Offset = 文件内偏移量`
            - `file_off` = (`address` - `seg.address`) + `seg.offset`
    - 举例

- `Virtual Address = 0x00401000`
  - `ImageBase = 0x00400000`
    - `RVA = 0x00001000`
- MachOView中能看到：
  - 2种显示模式
    - `RAW` =原始地址=虚拟地址
    - `RVA` =相对虚拟地址 = 类似于 `VA` 的概念
      - 比如： `baseAddress` = `基地址` = `VM Address` = `虚拟内存基地址` ： `0x100000000`
        - `File Offset` 地址： `0xA0460` -> 变成了 `RVA` 地址： `0x1000A0460`
  - 举例
    - `akd`
      - `RAW`
        - 
      - `RVA`
        - 
- IDA中的地址是：加了基地址后的 `RVA` 地址

- 
IDA - akd.i64 (akd) /Users/crifan/dev/dev_root/iosReverse/AppleStore/AuthKit_akd/AuthKit.framework/iOS15.0_arm64/akd.i64
No debugger
Library function
Regular function
Instruction
Data
Unexplored
External symbol
Functions window
Hex View-1
Structures
Enums
Imports
Exports
Function name
Line 2572 of 3508
Output window
Python
AU: idle
Down
Disk: 78GB

Mach-O大小限制

Apple会对iOS的app的大小做一定的限制，防止太大，影响用户下载（的体验）。

iOS的app的大小限制历史

若下载大小超过限制，将无法使用蜂窝网络下载App（ `iOS 13` 之前），会收到文件容量太大的提示，需通过 Wi-Fi 网络下载。如下，为苹果历年来对 App 下载大小限制的变化情况：

- 2008 年 7 月，搭载了 App Store 的 iPhone 3G 正式发售，下载限制仅为 10 MB
- 2010 年 2 月，苹果将 iPhone 3G 的下载限制从 10 MB 提升到 20 MB
- 2012 年 3 月，iOS 5.1 正式版后，下载限制从 20 MB 提升到 50 MB
- 2013 年 9 月，iOS 7 正式版后，下载限制从 50 MB 提升至 100 MB
- 2017 年 9 月，iOS 11 正式版后，下载限制从 100 MB 提升至 150 MB
- 2019 年 5 月，下载限制从 150 MB 提升至 200 MB
- 2019 年 9 月，iOS 13 正式版后，若下载大小超过 200 MB，用户可选择是否使用蜂窝网络下载

如今，App 下载大小超出 200 MB 时，会出现两种情况：

- iOS 13 以下的用户，无法通过蜂窝数据下载 App
- iOS 13 及以上的用户，需要手动设置才可以使用蜂窝网络下载 App

◦

Mach-O可执行文件大小限制

苹果对可执行文件大小亦有明确限制，超过该限制会导致 App 审核被拒：

> ERROR: ERROR ITMS-90122: "Invalid ExecutaBe Size. The size of your app's executaBe file 'News.app/News' is 68534272 bytes for architecture 'arm64', which exceeds the maximum allowed size of 60 MB."

具体限制如下：

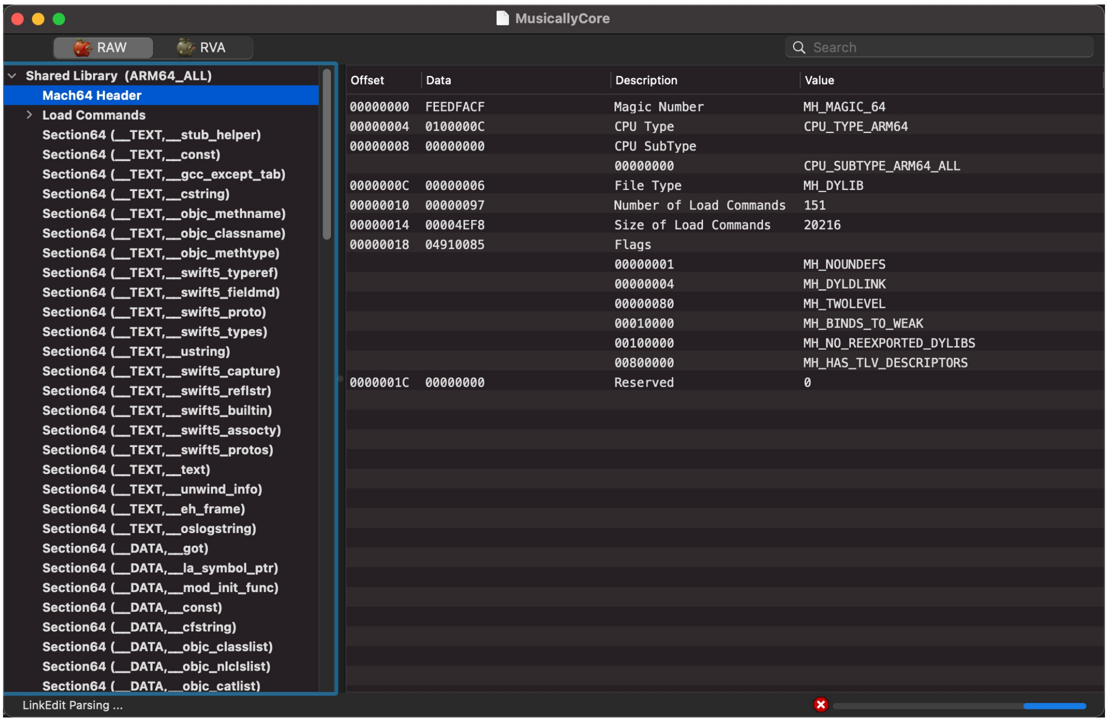
- `iOS <7.0` ：二进制文件中所有的 `__TEXT` 段总和不得超过**80 MB**
- `iOS 7.x` ~ `iOS 8.x` ：二进制文件中，每个特定架构中的 `__TEXT` 段不得超过**60 MB**
- `iOS >9.0` ：二进制文件中所有的 `__TEXT` 段总和不得超过**500 MB**

Mach-O工具

此处整理查看解析Mach-O文件信息的常用工具。

- `MachOView`
- `rabin2`
- `jtool2`
- `otool`
- `pagestuff`
- 其他
    - `optool`
        - 介绍：optool is a tool which interfaces with MachO binaries in order to insert/remove load commands, strip code signatures, resign, and remove aslr
        - 主页
            - https://github.com/alexzielenski/optool

MachOView

- `MachOView`
    - 是什么：查看和编辑 `x86` / `ARM` 的 `Mach-O` 二进制文件的工具
        - Visual Mach-O file browser that allows exploring and in-place editing Intel and ARM binaries.
    - 用途：常用来查看iOS的app的二进制文件的信息
    - 截图
        - 

    - 资料
        - 最早好像是在sourceforge
            - MachOView download | SourceForge.net
                - https://sourceforge.net/projects/machoview/
        - 后来有人fork到GitHub
            - gdbinit/MachOView: MachOView fork
                - https://github.com/gdbinit/MachOView
        - 现在有国人fork后继续维护
            - fangshufeng/MachOView: 分析Macho必备工具
                - https://github.com/fangshufeng/MachOView

下载和安装MachOView

- 下载

从fangshufeng/MachOView: 分析Macho必备工具，进入此时最新版Release 2.6.1去下载

MachOView-2.6.1.dmg

- 安装

下载后，双击 `dmg` ，打开窗口，把其中的 `MachOView.app` 拷贝到 `应用程序` 即可：

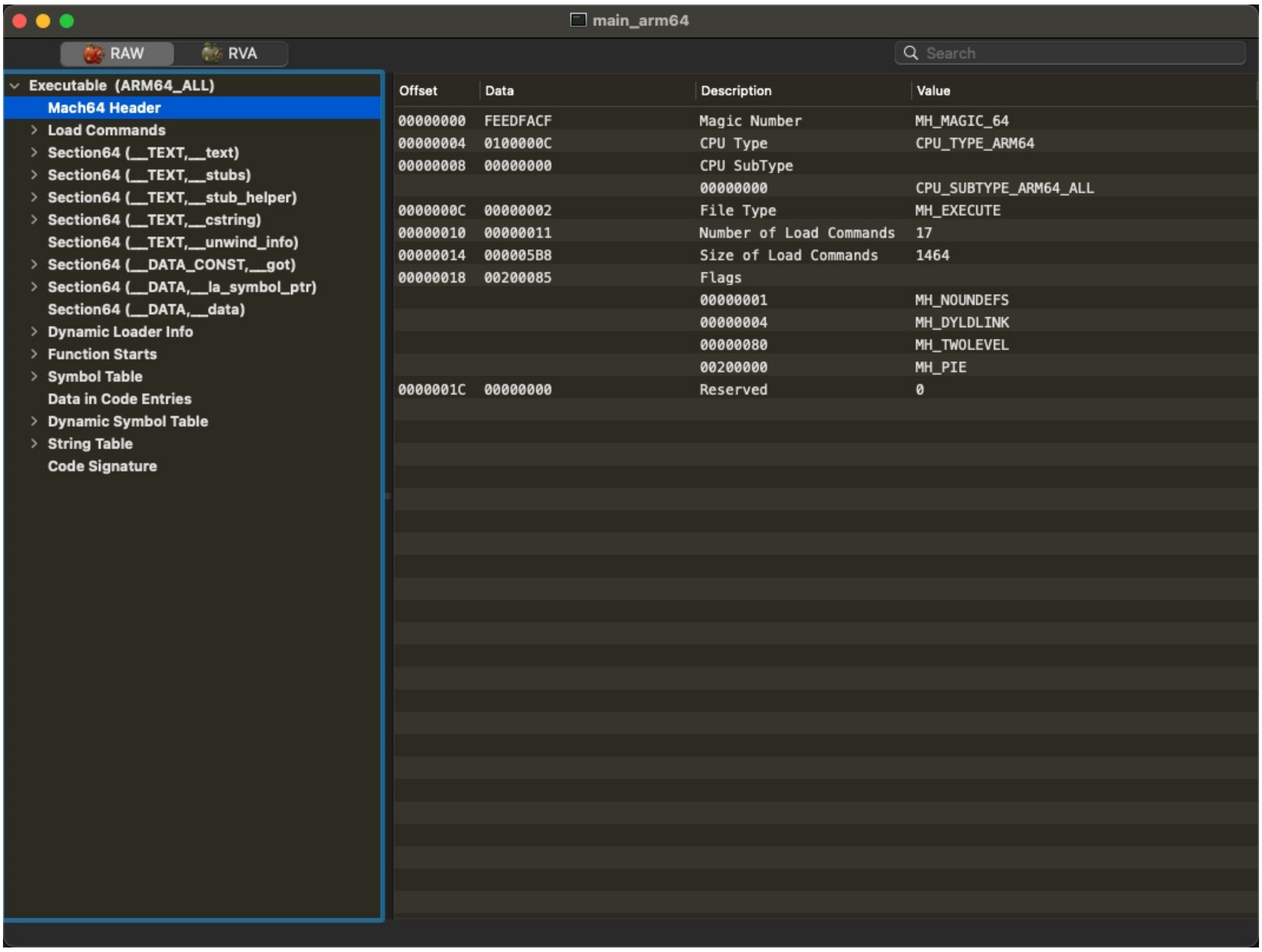

应用程序
返回/前进
个人收藏
下载
dev
crifan_self
crifan
应用程序
今天
MachOView.app

MachOView用法举例

main_arm64

用MachOView去查看这个 `main_arm64: Mach-O 64-bit executable arm64`

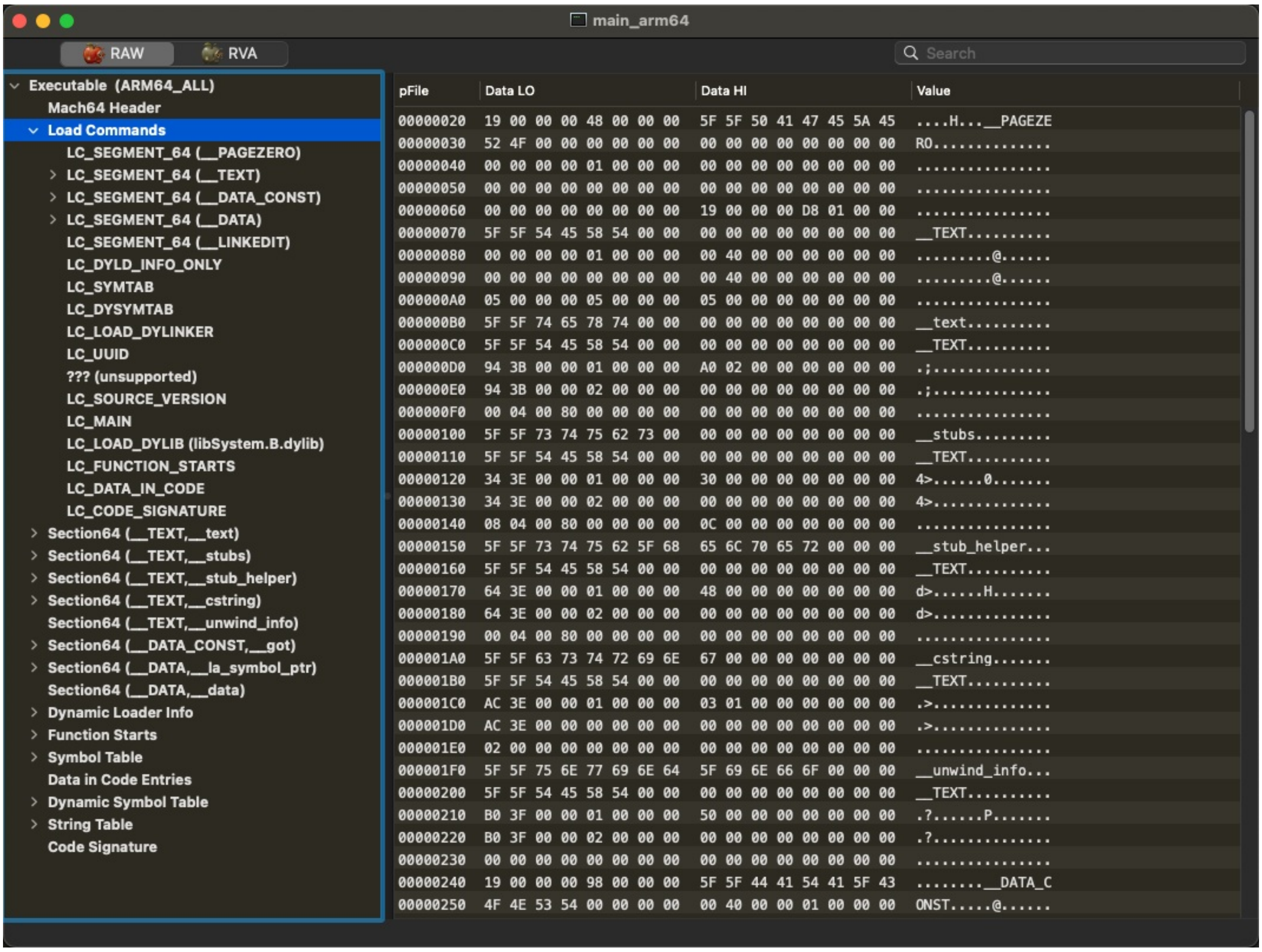
Mach64 Header



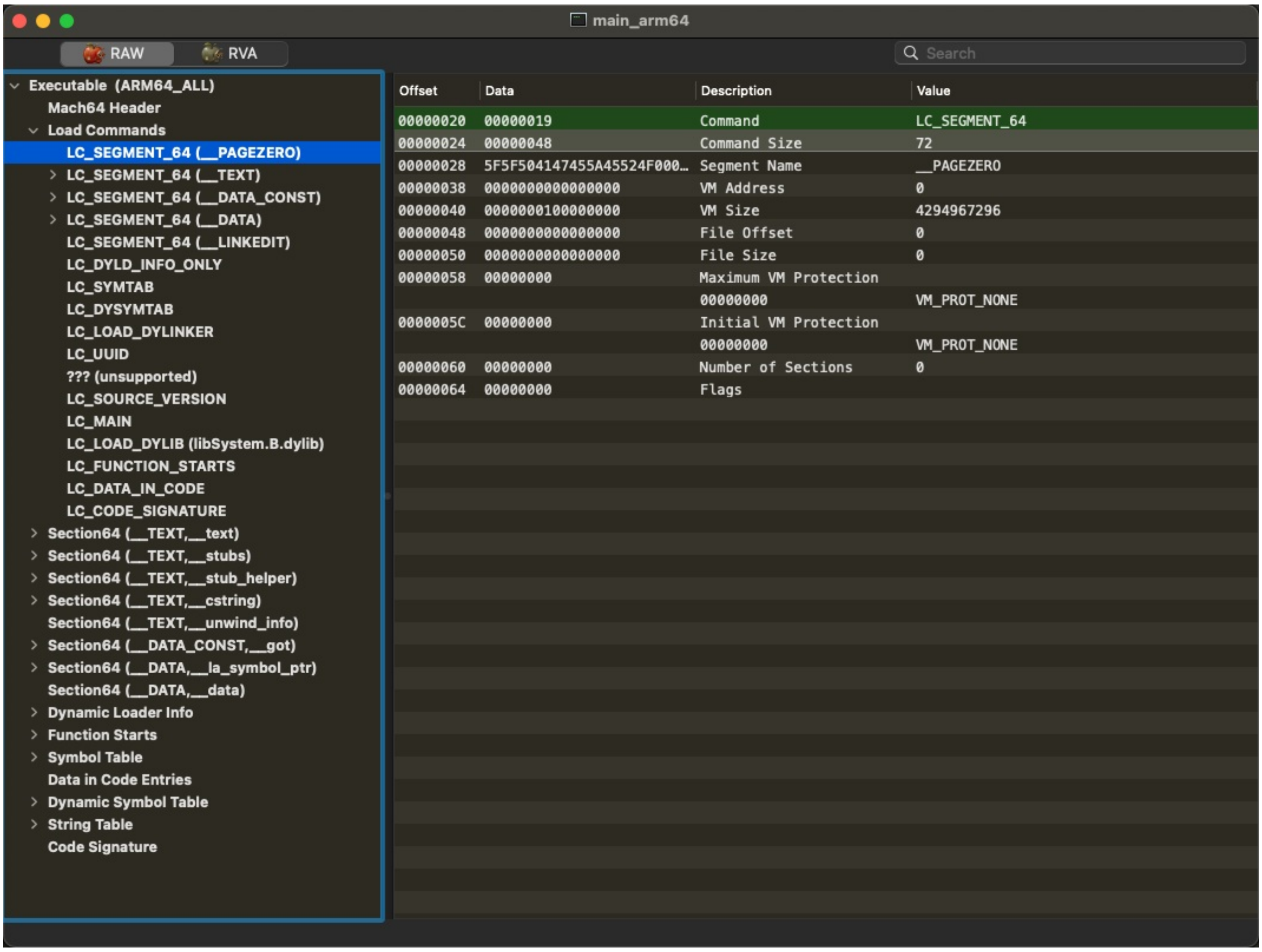
内容：

- Mach64 Header
  - `MH_MAGIC_64`
  - `CPU_TYPE_ARM64`
  - `CPU_SUBTYPE_ARM64_ALL`
  - `MH_EXECUTE`
  - Number for Load Commands: `17`
  - Flags
    - `MH_NOUNDEFS`
    - `MH_DYLDLINK`
    - `MH_TWOLEVEL`
    - `MH_PIC`
  - Reserved: 0

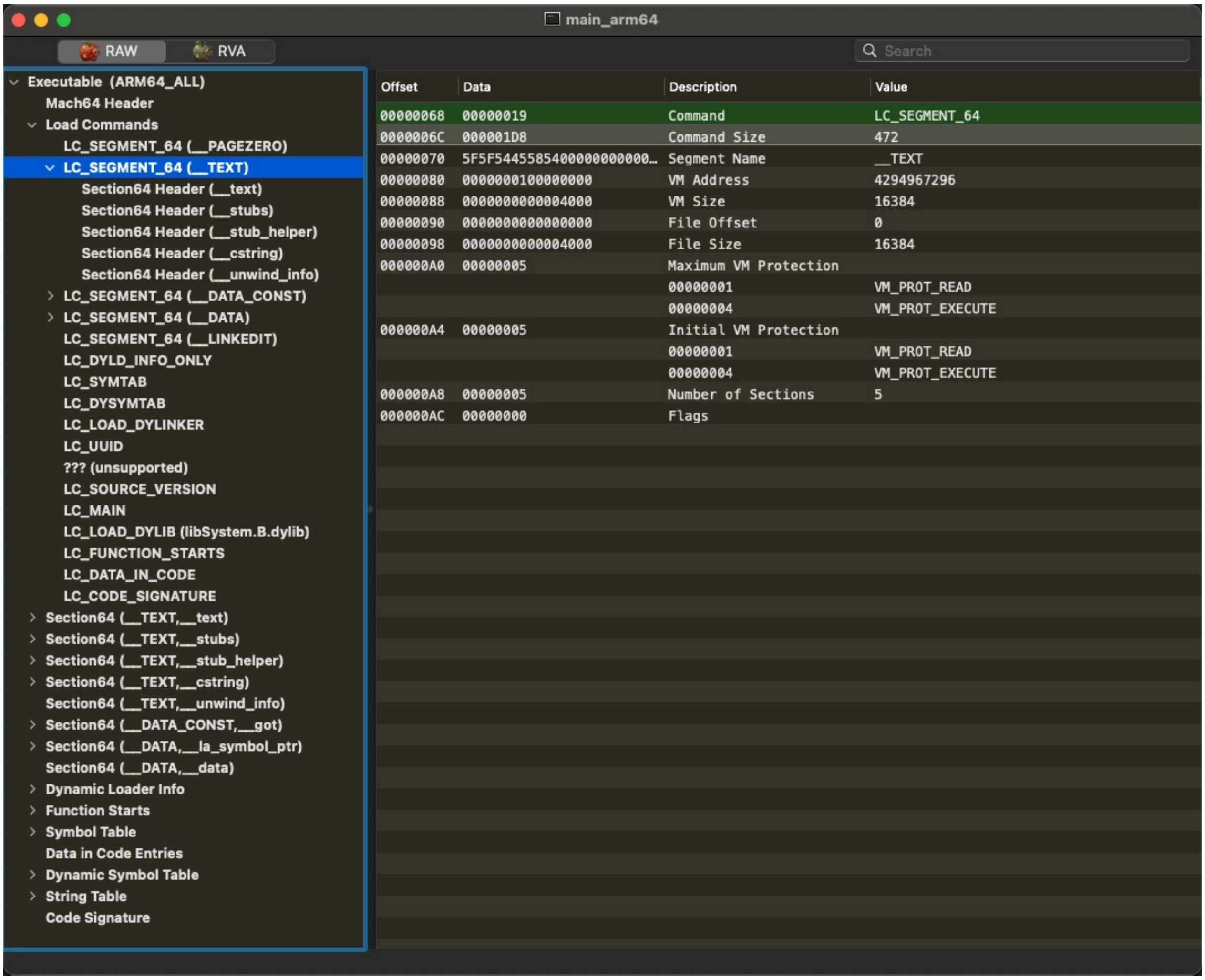
Load Commands



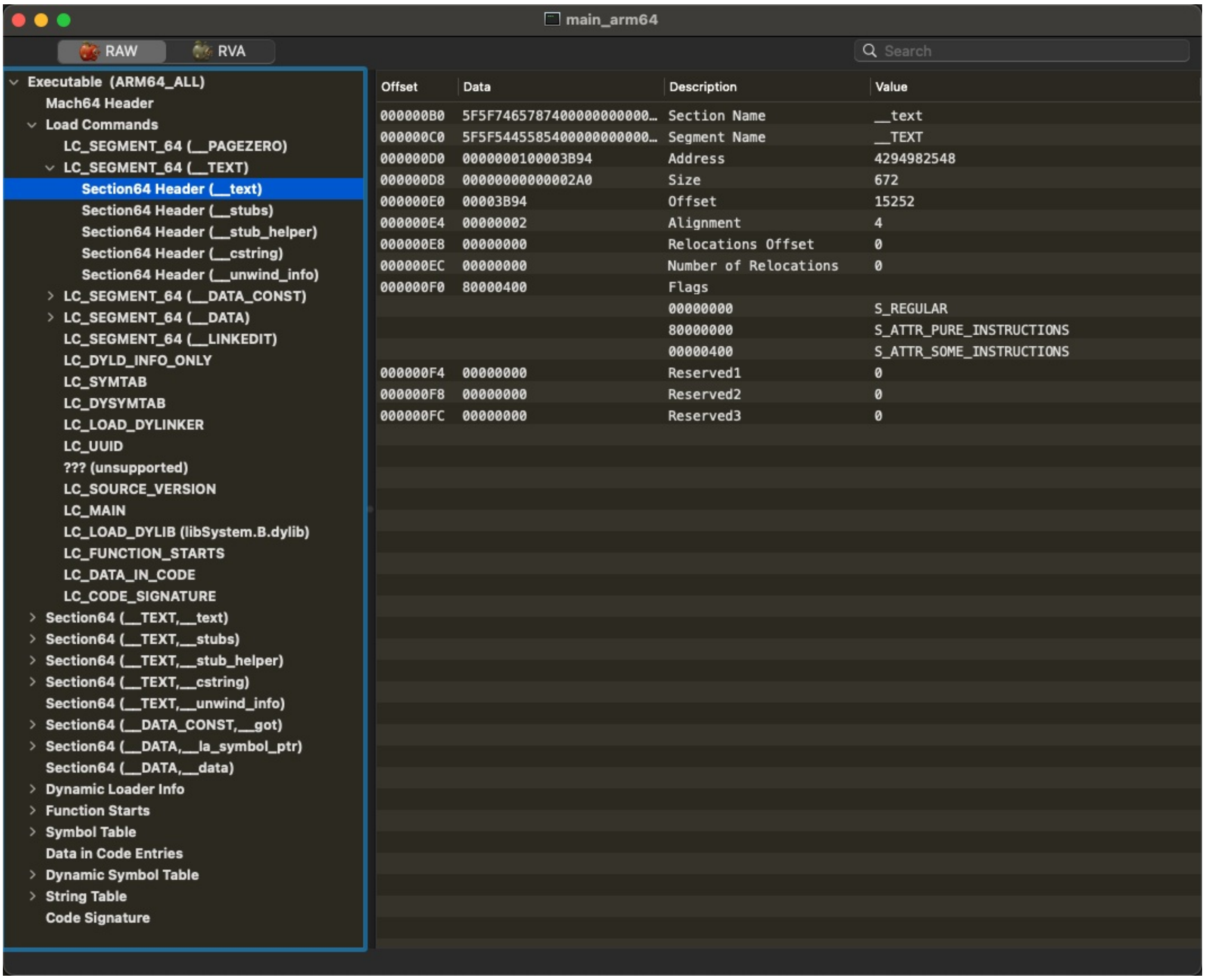
LC_SEGMENT_64 (`__PAGEZERO`)



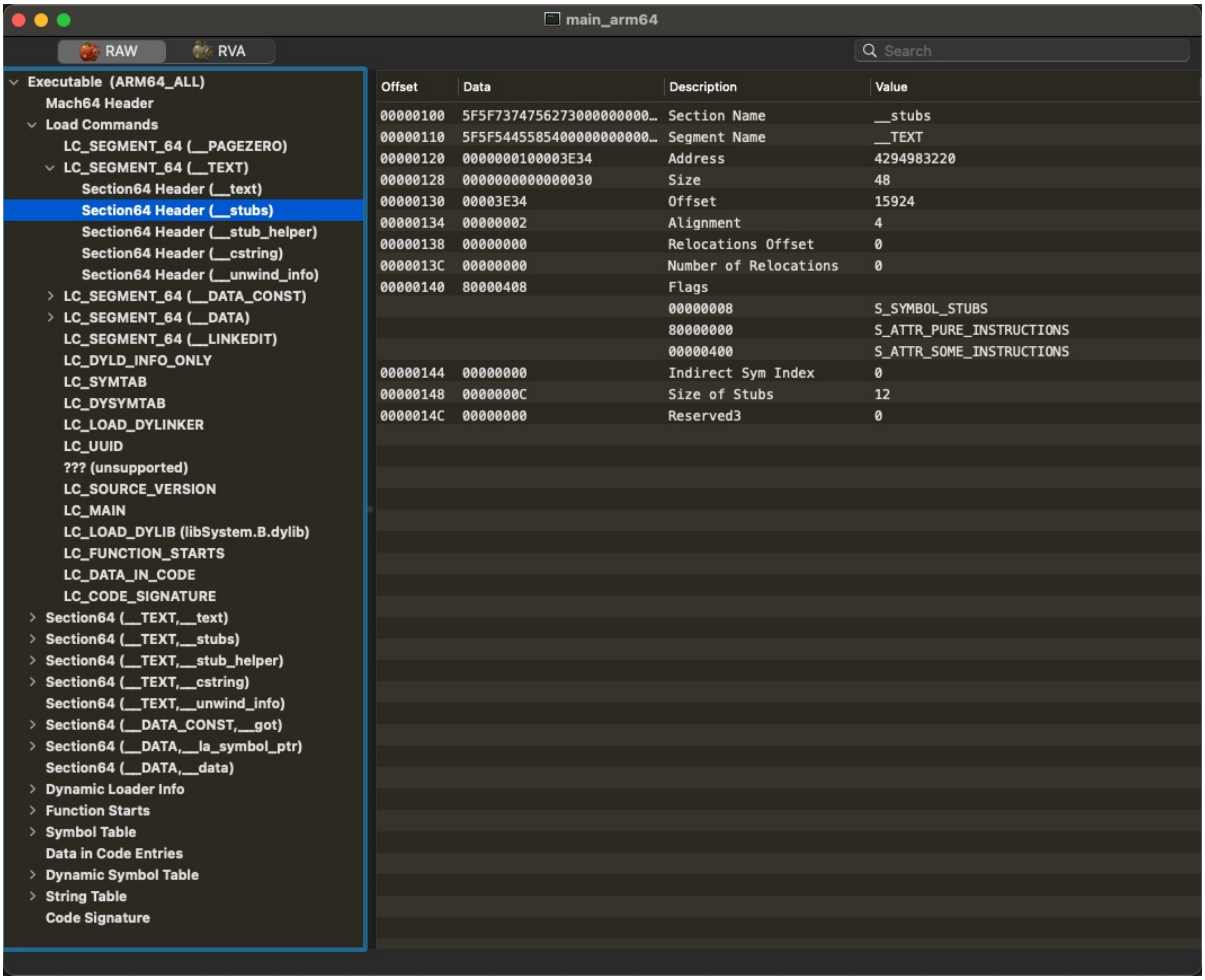
LC_SEGMENT_64 (__TEXT)


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
Section64 Header (__text)
Section64 Header (__stubs)
Section64 Header (__stub_helper)
Section64 Header (__cstring)
Section64 Header (__unwind_info)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
00000068 00000019 Command LC_SEGMENT_64
0000006C 000001D8 Command Size 472
00000070 5F5F544558540000000000... Segment Name __TEXT
00000080 0000000100000000 VM Address 4294967296
00000088 0000000000004000 VM Size 16384
00000090 0000000000000000 File Offset 0
00000098 0000000000004000 File Size 16384
000000A0 00000005 Maximum VM Protection
00000001 VM_PROT_READ
00000004 VM_PROT_EXECUTE
000000A4 00000005 Initial VM Protection
00000001 VM_PROT_READ
00000004 VM_PROT_EXECUTE
000000A8 00000005 Number of Sections 5
000000AC 00000000 Flags

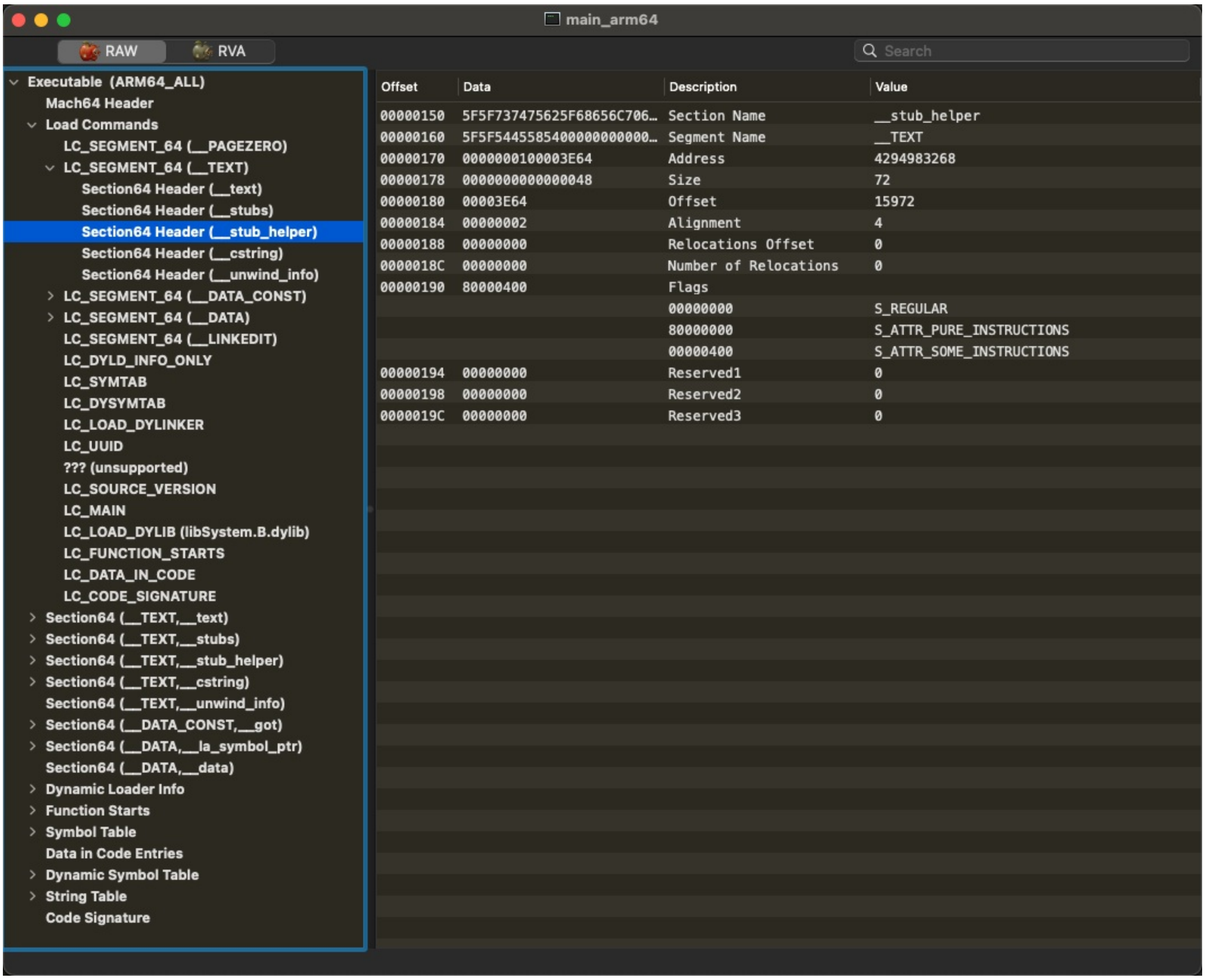
`__TEXT,__text`


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
Section64 Header (__text)
Section64 Header (__stubs)
Section64 Header (__stub_helper)
Section64 Header (__cstring)
Section64 Header (__unwind_info)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
000000B0 5F5F7465787400000000… Section Name __text
000000C0 5F5F5445585400000000… Segment Name __TEXT
000000D0 0000000100003B94 Address 4294982548
000000D8 00000000000002A0 Size 672
000000E0 00003B94 Offset 15252
000000E4 00000002 Alignment 4
000000E8 00000000 Relocations Offset 0
000000EC 00000000 Number of Relocations 0
000000F0 80000400 Flags
00000000 S_REGULAR
80000000 S_ATTR_PURE_INSTRUCTIONS
00000400 S_ATTR_SOME_INSTRUCTIONS
000000F4 00000000 Reserved1 0
000000F8 00000000 Reserved2 0
000000FC 00000000 Reserved3 0

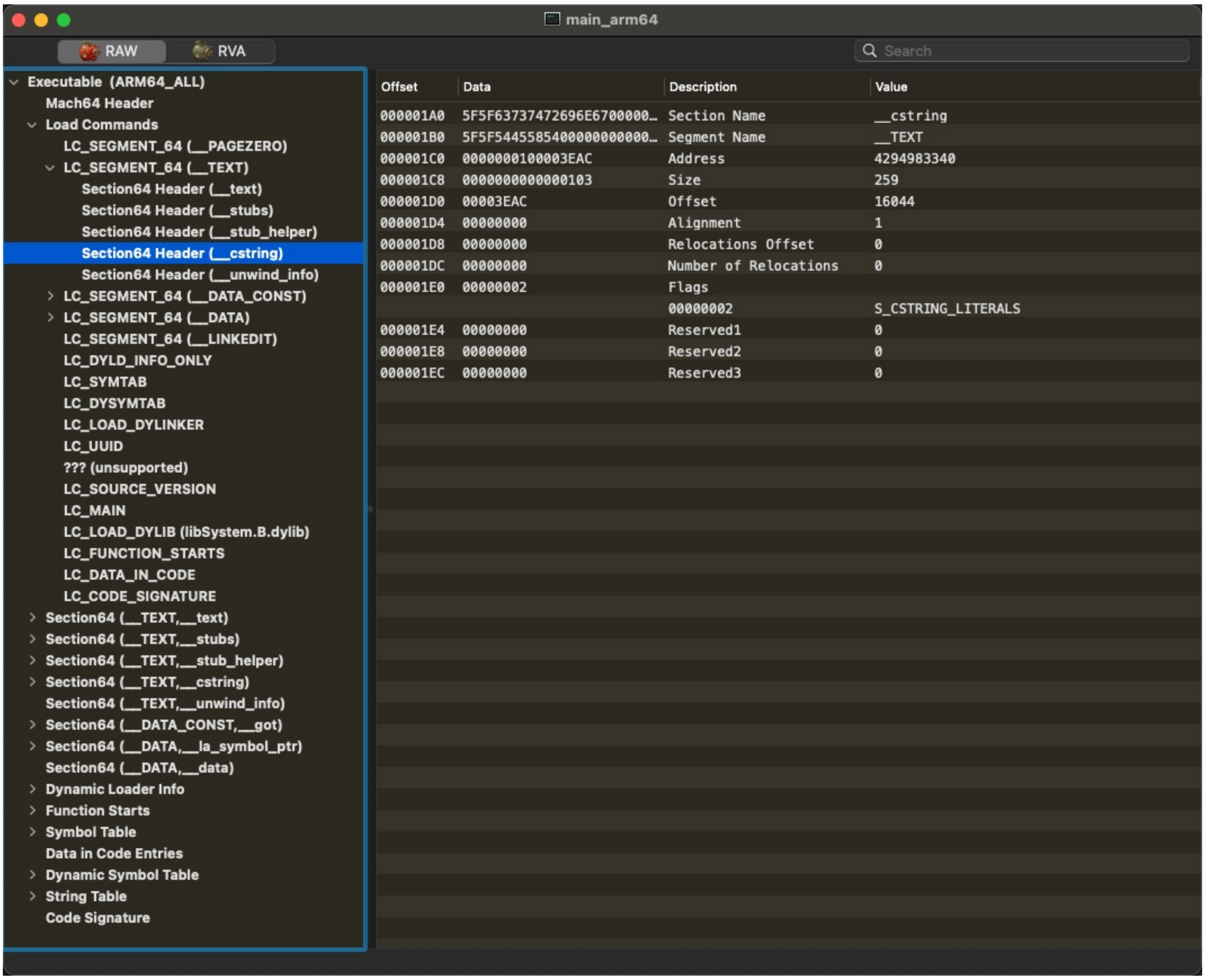
`__TEXT,__stubs`



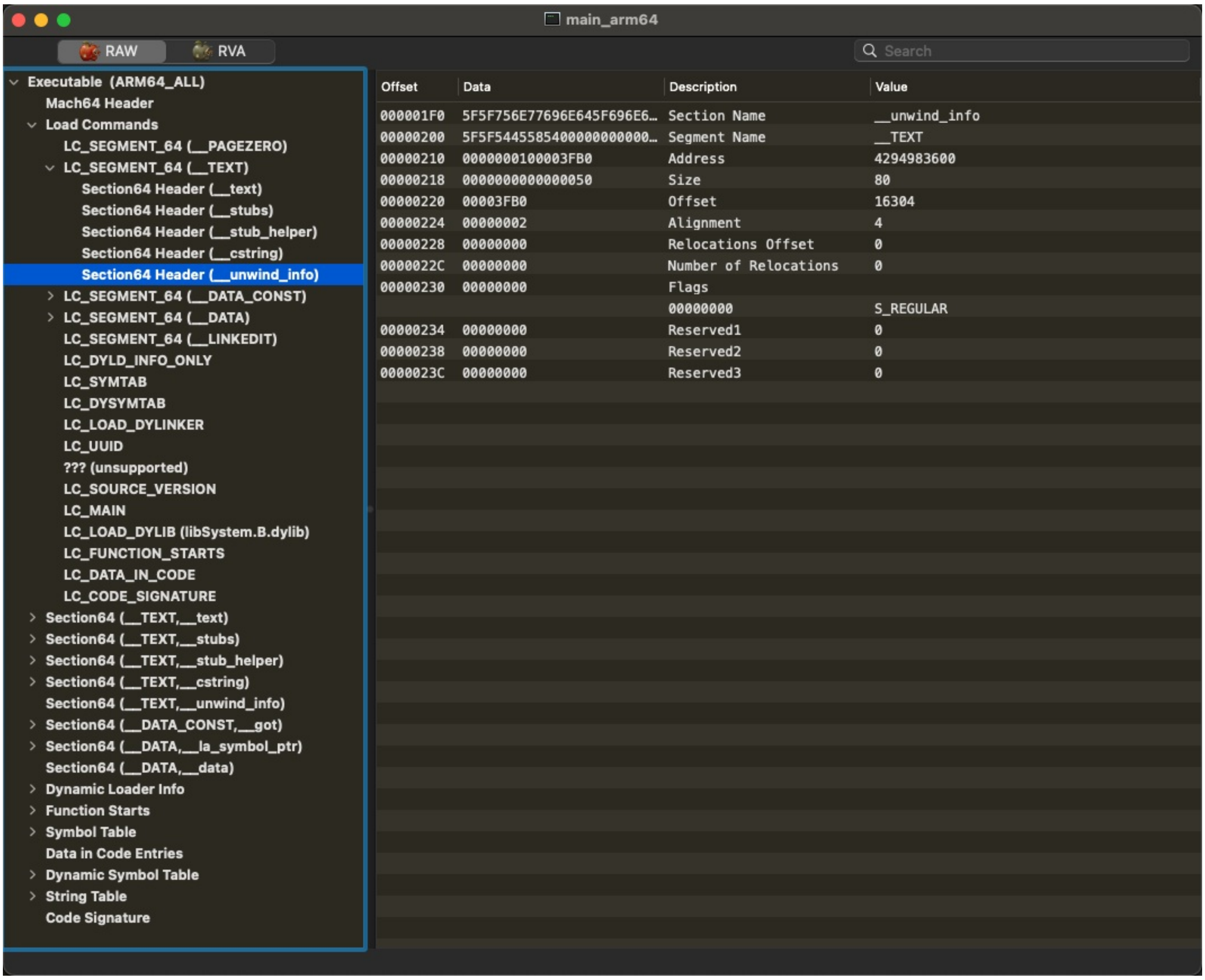
`__TEXT,__stub_helper`



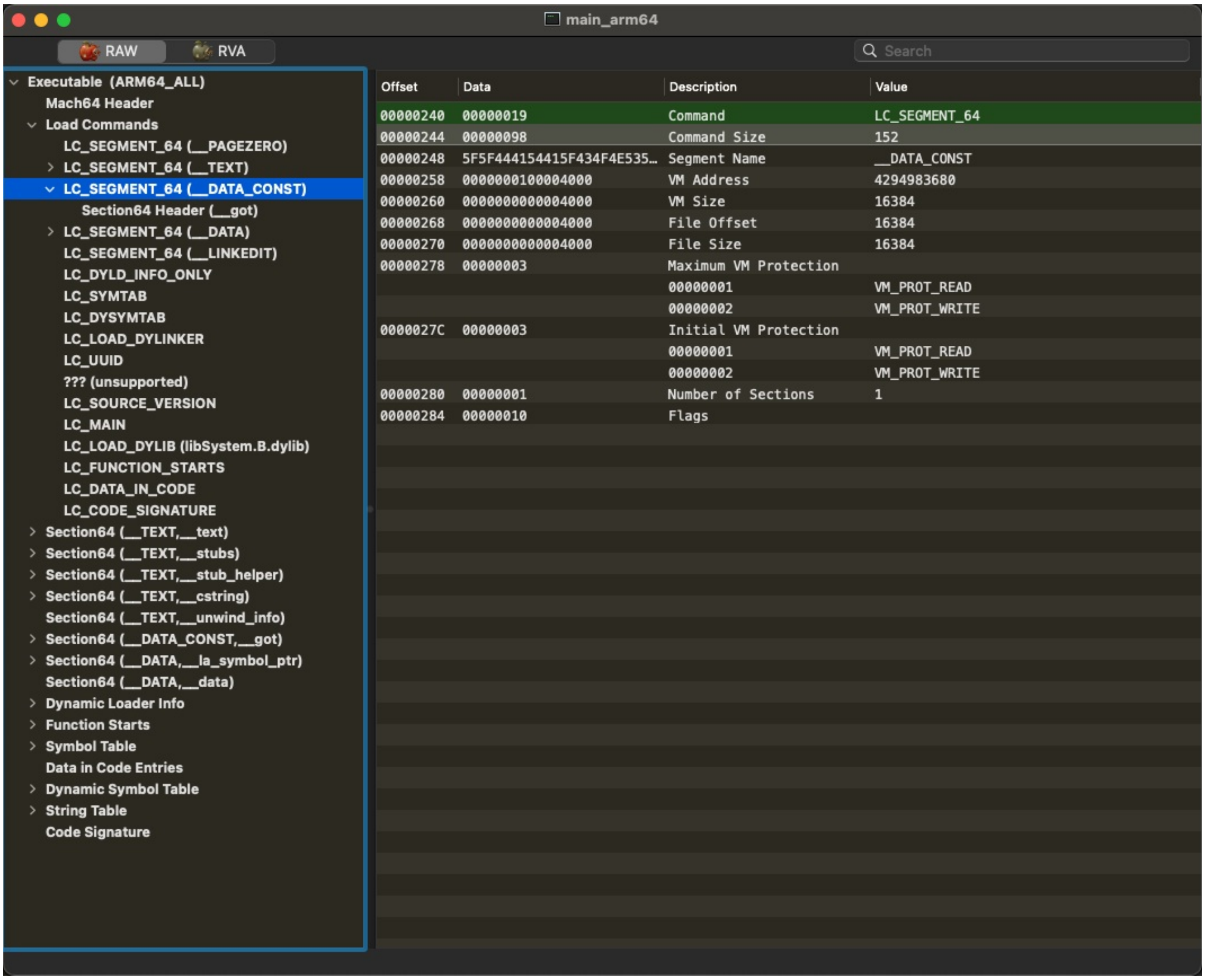
`__TEXT,__cstring`



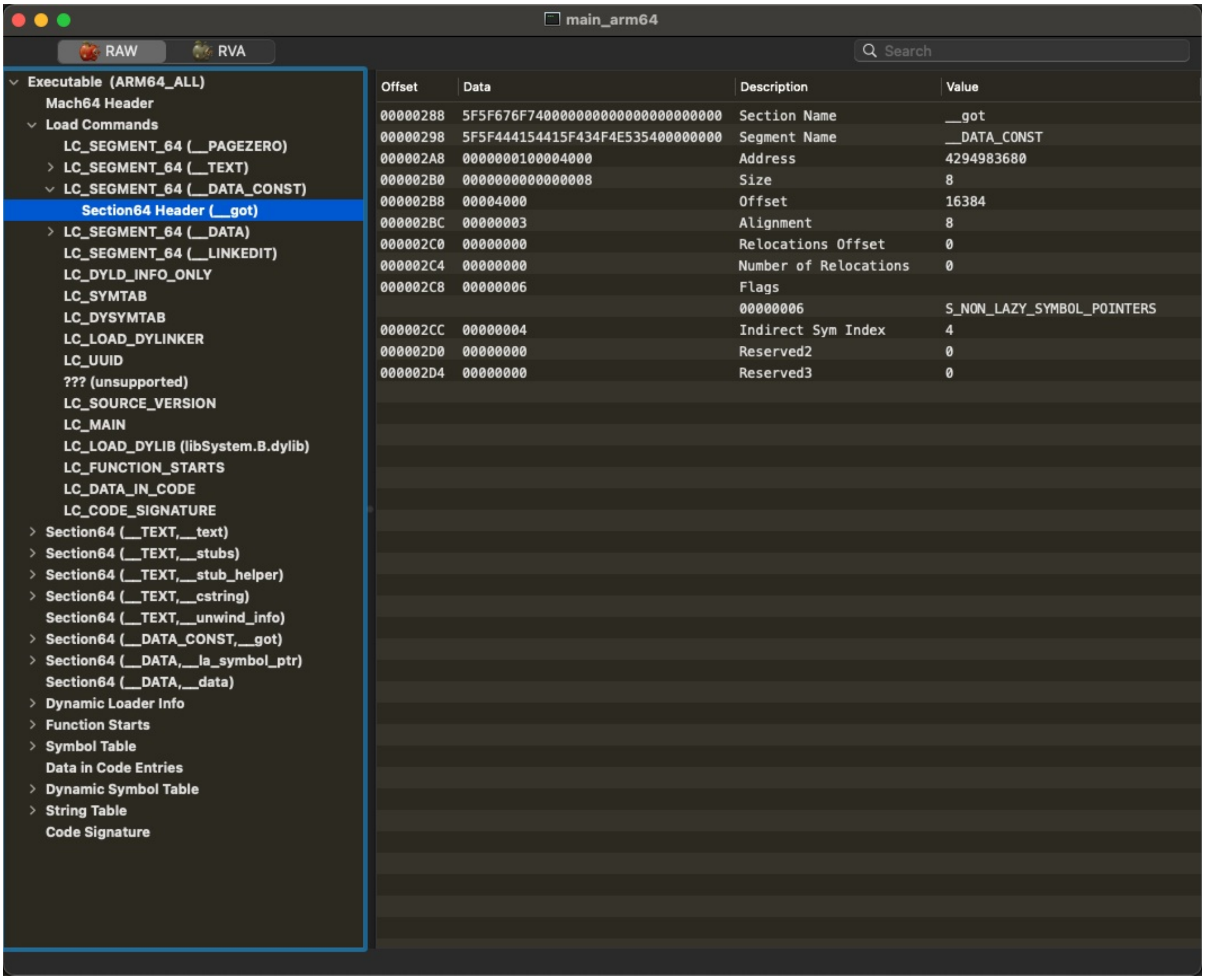
`__TEXT,__unwind_info`



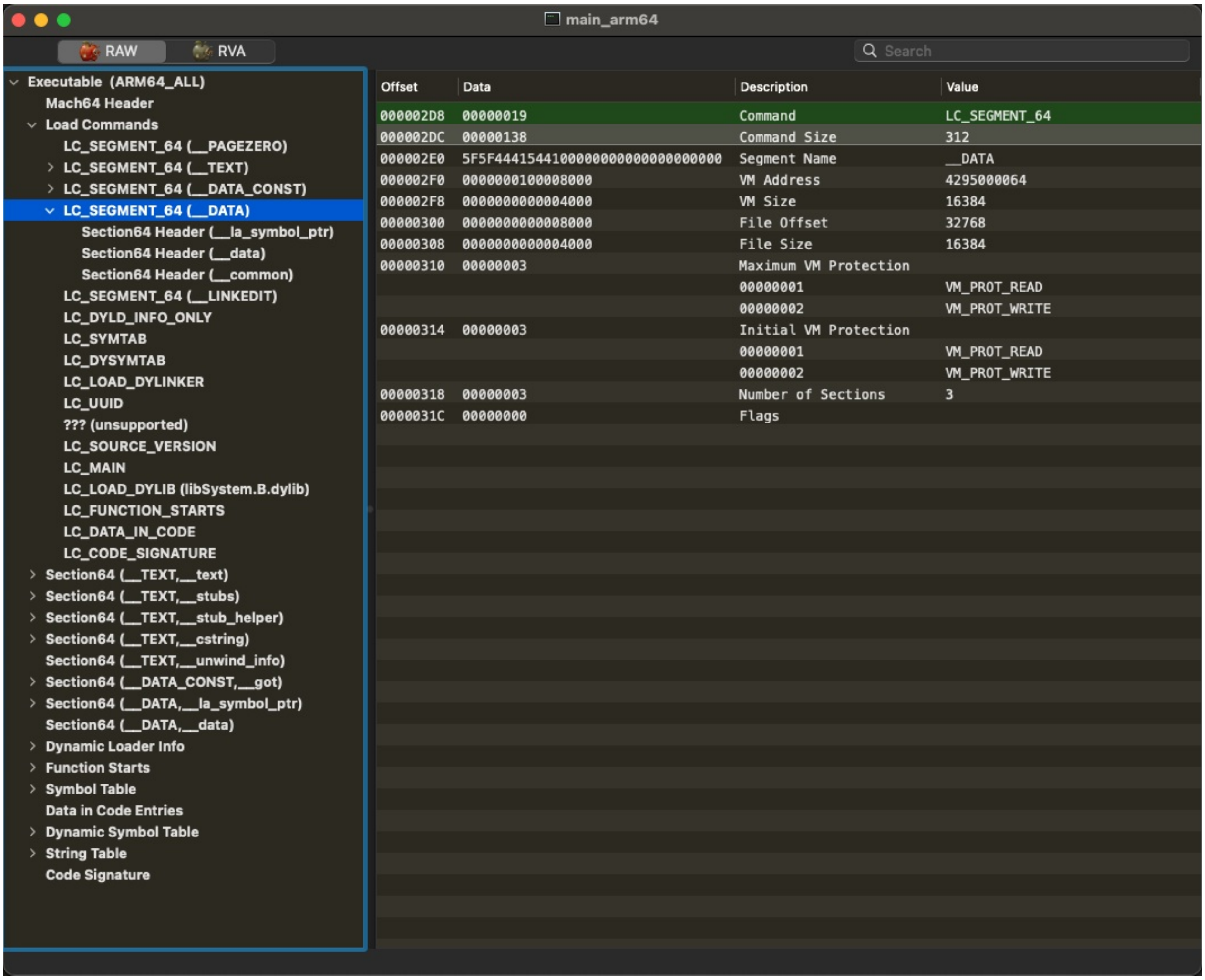
LC_SEGMENT_64 (`__DATA_CONST`)



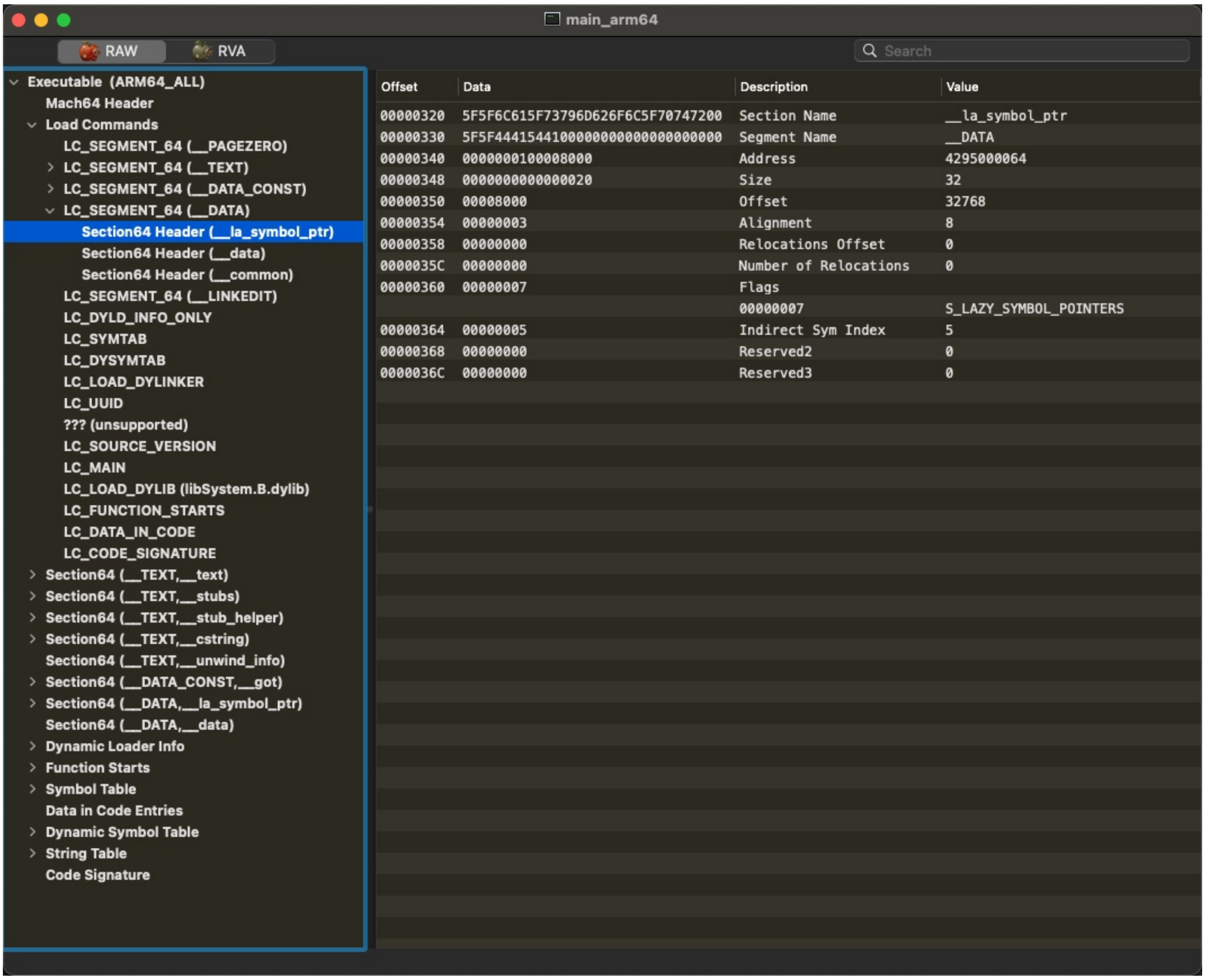
`__DATA_CONST,__got`



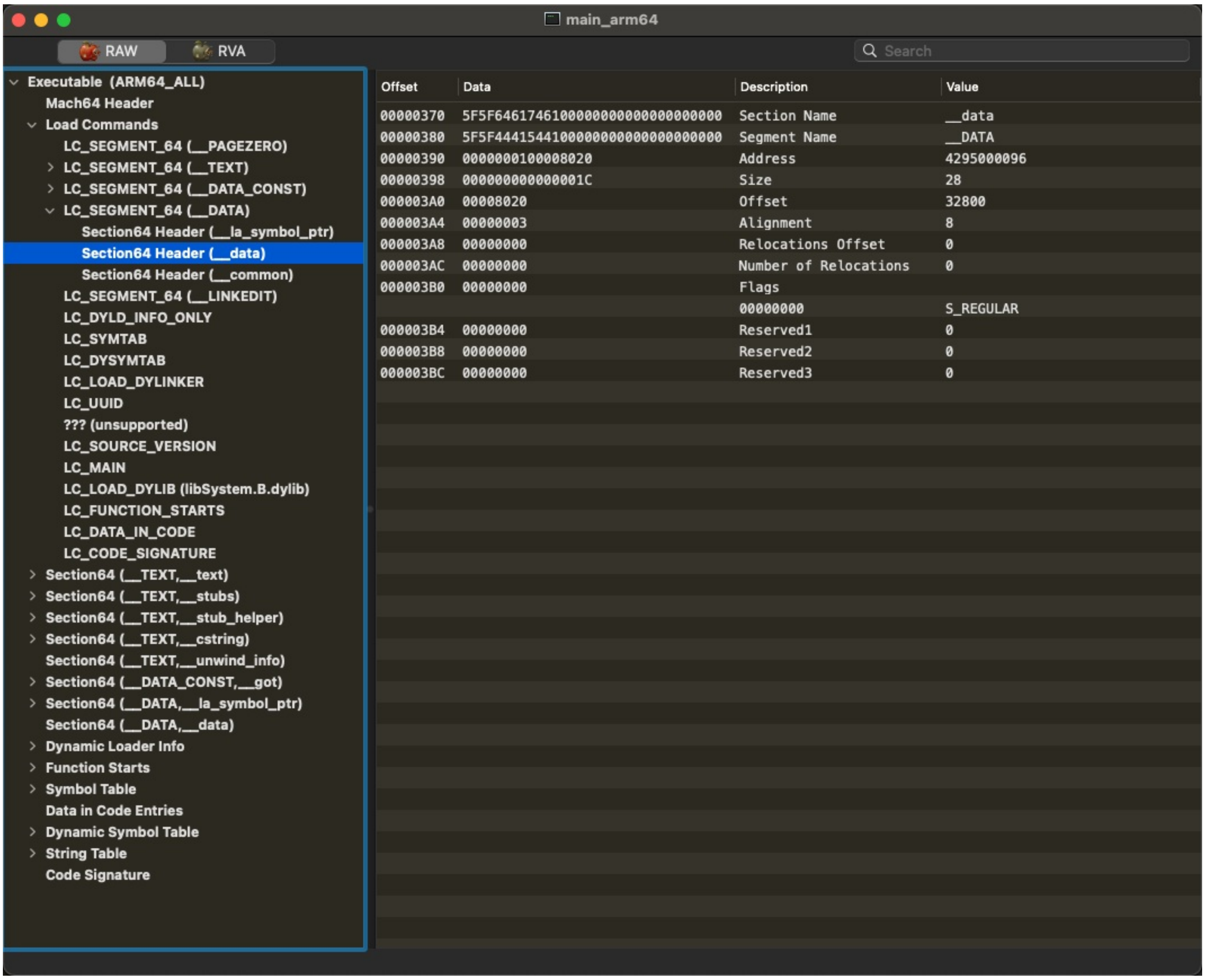
LC_SEGMENT_64 (`__DATA`)



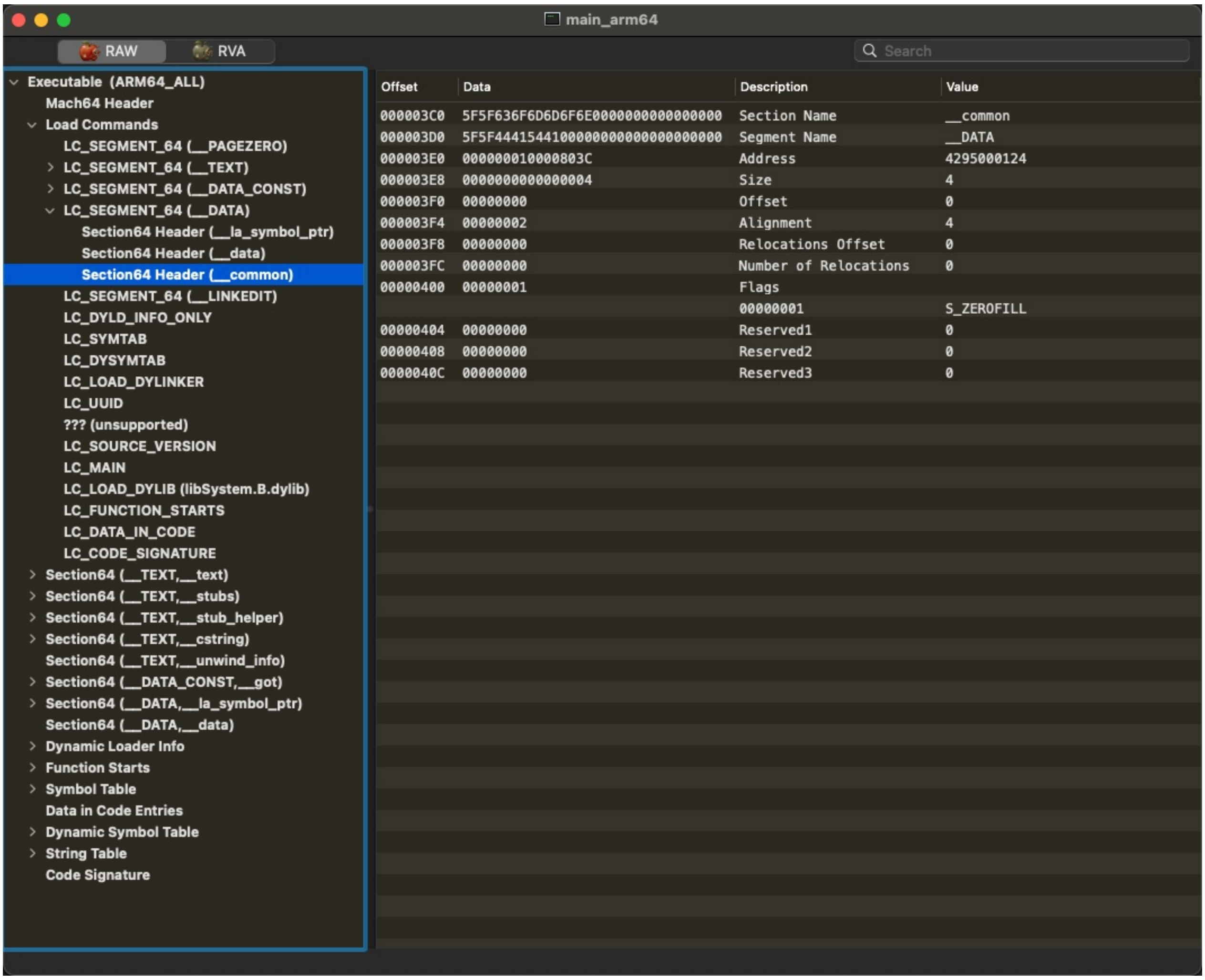
`__DATA,__la_symbol_ptr`


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
Section64 Header (__la_symbol_ptr)
Section64 Header (__data)
Section64 Header (__common)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
00000320 5F5F6C615F73796D626F6C5F70747200 Section Name __la_symbol_ptr
00000330 5F5F444154410000000000000000000000 Segment Name __DATA
00000340 0000000100008000 Address 4295000064
00000348 0000000000000020 Size 32
00000350 00008000 Offset 32768
00000354 00000003 Alignment 8
00000358 00000000 Relocations Offset 0
0000035C 00000000 Number of Relocations 0
00000360 00000007 Flags
00000007 S_LAZY_SYMBOL_POINTERS
00000364 00000005 Indirect Sym Index 5
00000368 00000000 Reserved2 0
0000036C 00000000 Reserved3 0

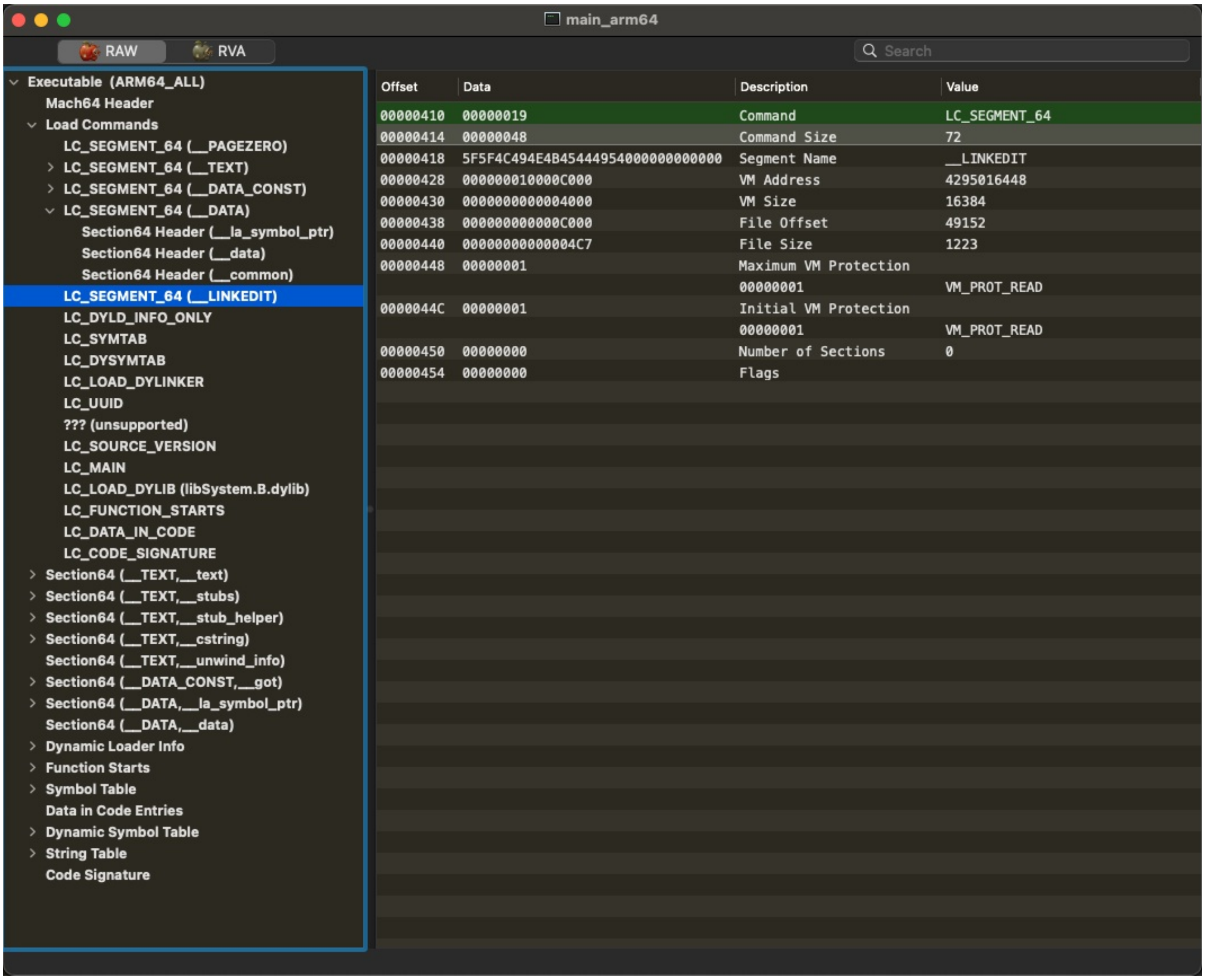
`__DATA,__data`


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
Section64 Header (__la_symbol_ptr)
Section64 Header (__data)
Section64 Header (__common)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
00000370 5F5F646174610000000000000000000000 Section Name __data
00000380 5F5F444154410000000000000000000000 Segment Name __DATA
00000390 0000000100008020 Address 4295000096
00000398 000000000000001C Size 28
000003A0 00008020 Offset 32800
000003A4 00000003 Alignment 8
000003A8 00000000 Relocations Offset 0
000003AC 00000000 Number of Relocations 0
000003B0 00000000 Flags
00000000 S_REGULAR
000003B4 00000000 Reserved1 0
000003B8 00000000 Reserved2 0
000003BC 00000000 Reserved3 0

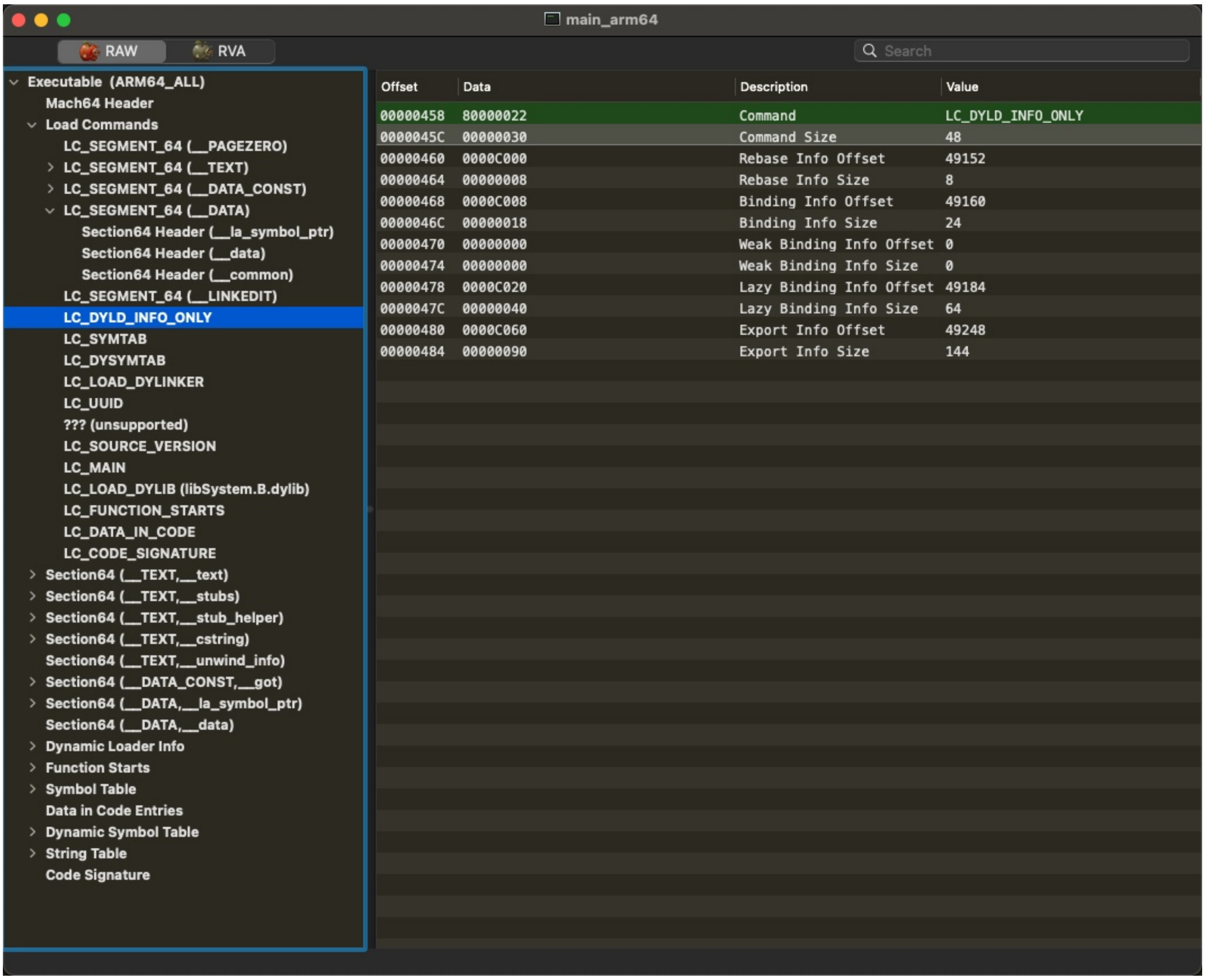
`__DATA,__common`



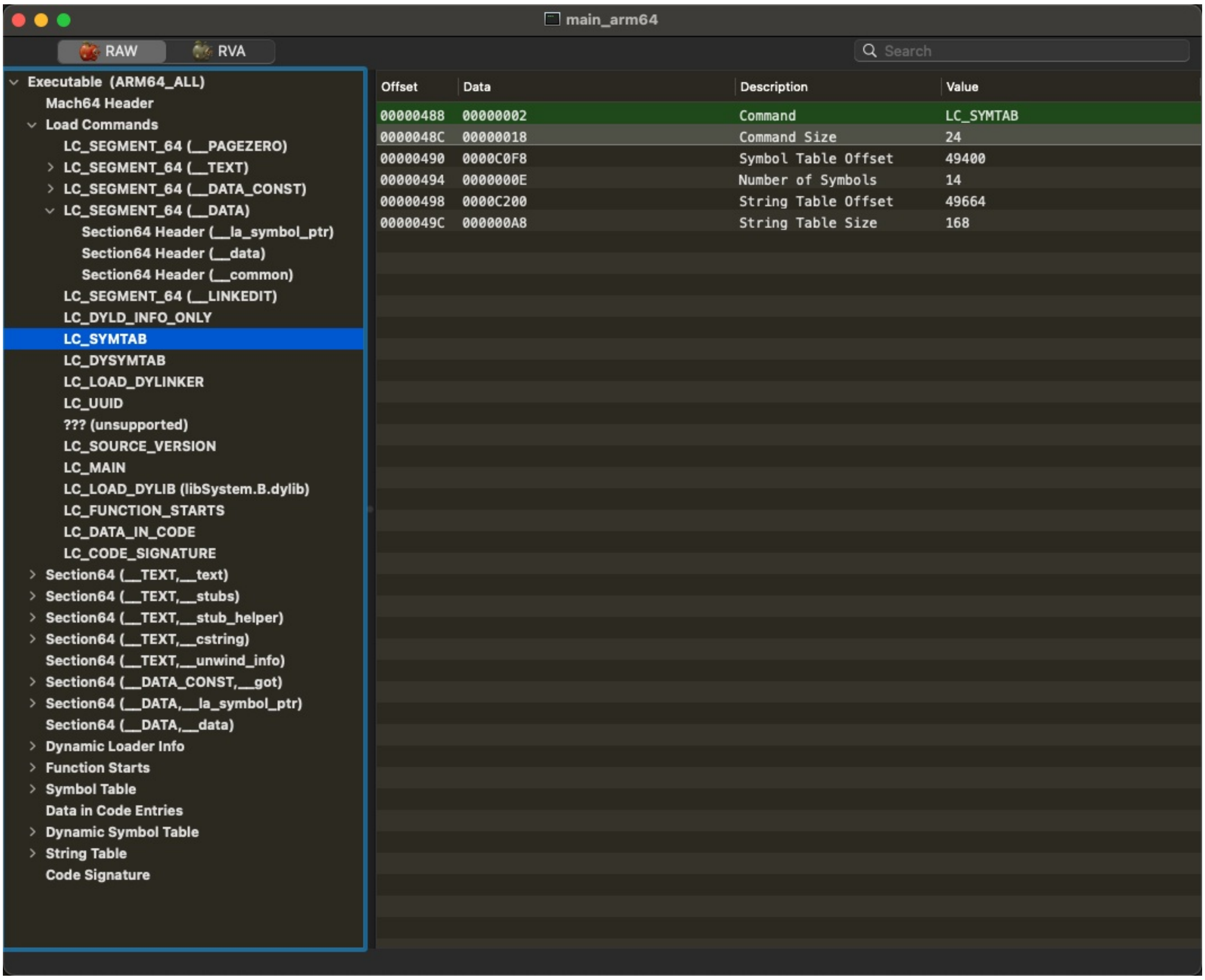
LC_SEGMENT_64 (`__LINKEDIT`)



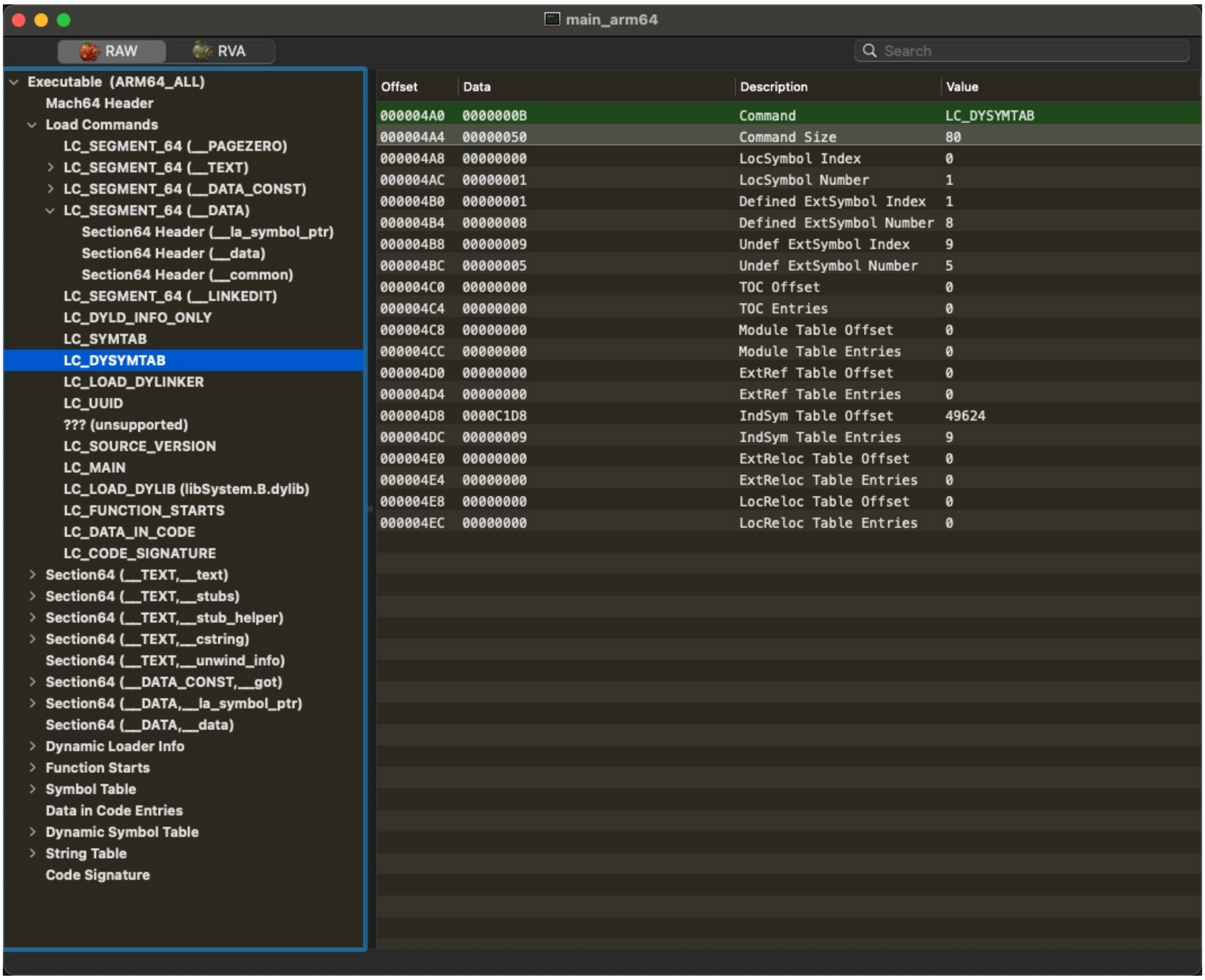
LC_DYLD_INFO_ONLY


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
Section64 Header (__la_symbol_ptr)
Section64 Header (__data)
Section64 Header (__common)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
00000458 80000022 Command LC_DYLD_INFO_ONLY
0000045C 00000030 Command Size 48
00000460 0000C000 Rebase Info Offset 49152
00000464 00000008 Rebase Info Size 8
00000468 0000C008 Binding Info Offset 49160
0000046C 00000018 Binding Info Size 24
00000470 00000000 Weak Binding Info Offset 0
00000474 00000000 Weak Binding Info Size 0
00000478 0000C020 Lazy Binding Info Offset 49184
0000047C 00000040 Lazy Binding Info Size 64
00000480 0000C060 Export Info Offset 49248
00000484 00000090 Export Info Size 144

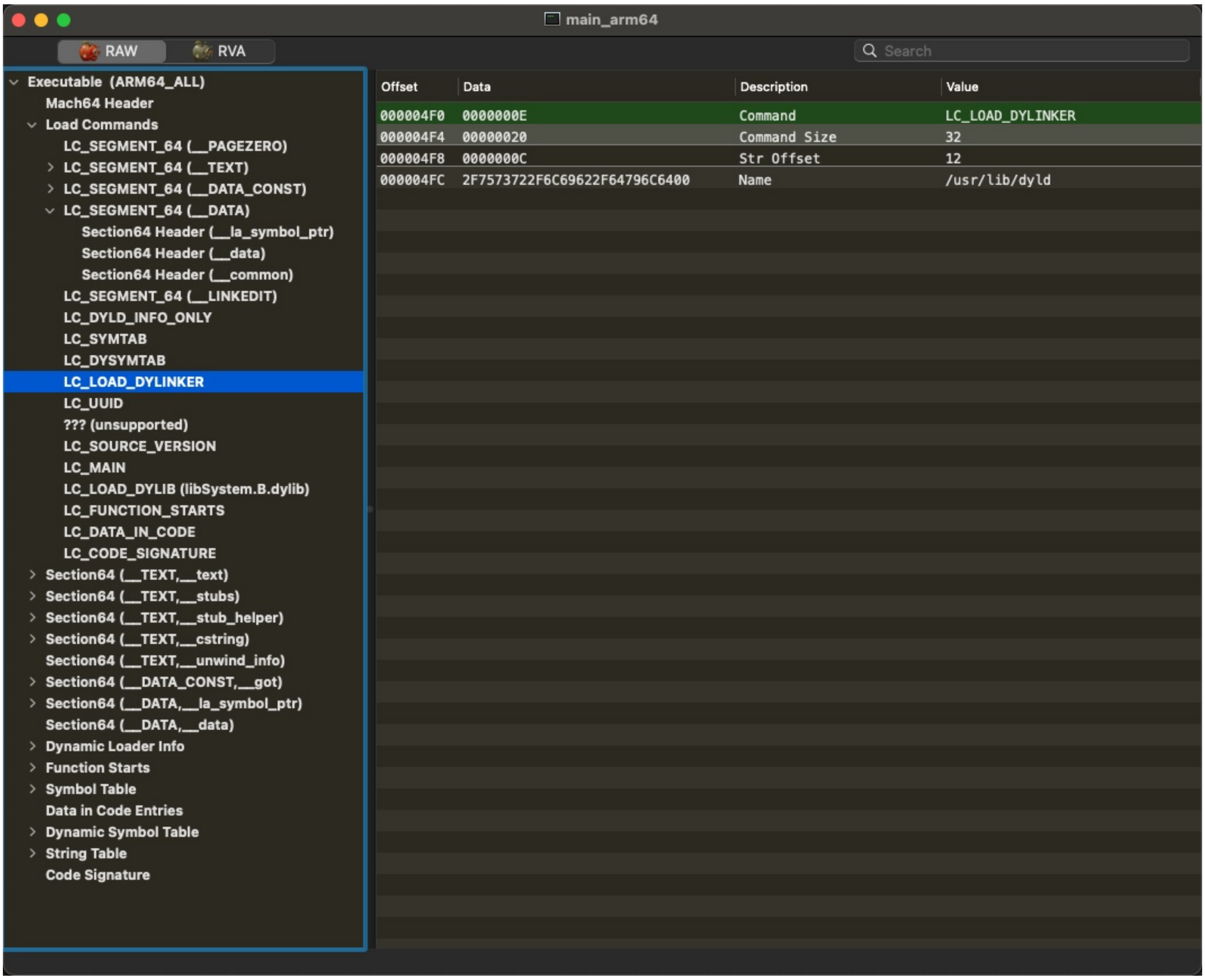
LC_SYMTAB


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
Section64 Header (__la_symbol_ptr)
Section64 Header (__data)
Section64 Header (__common)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
00000488 00000002 Command LC_SYMTAB
0000048C 00000018 Command Size 24
00000490 0000C0F8 Symbol Table Offset 49400
00000494 0000000E Number of Symbols 14
00000498 0000C200 String Table Offset 49664
0000049C 000000A8 String Table Size 168

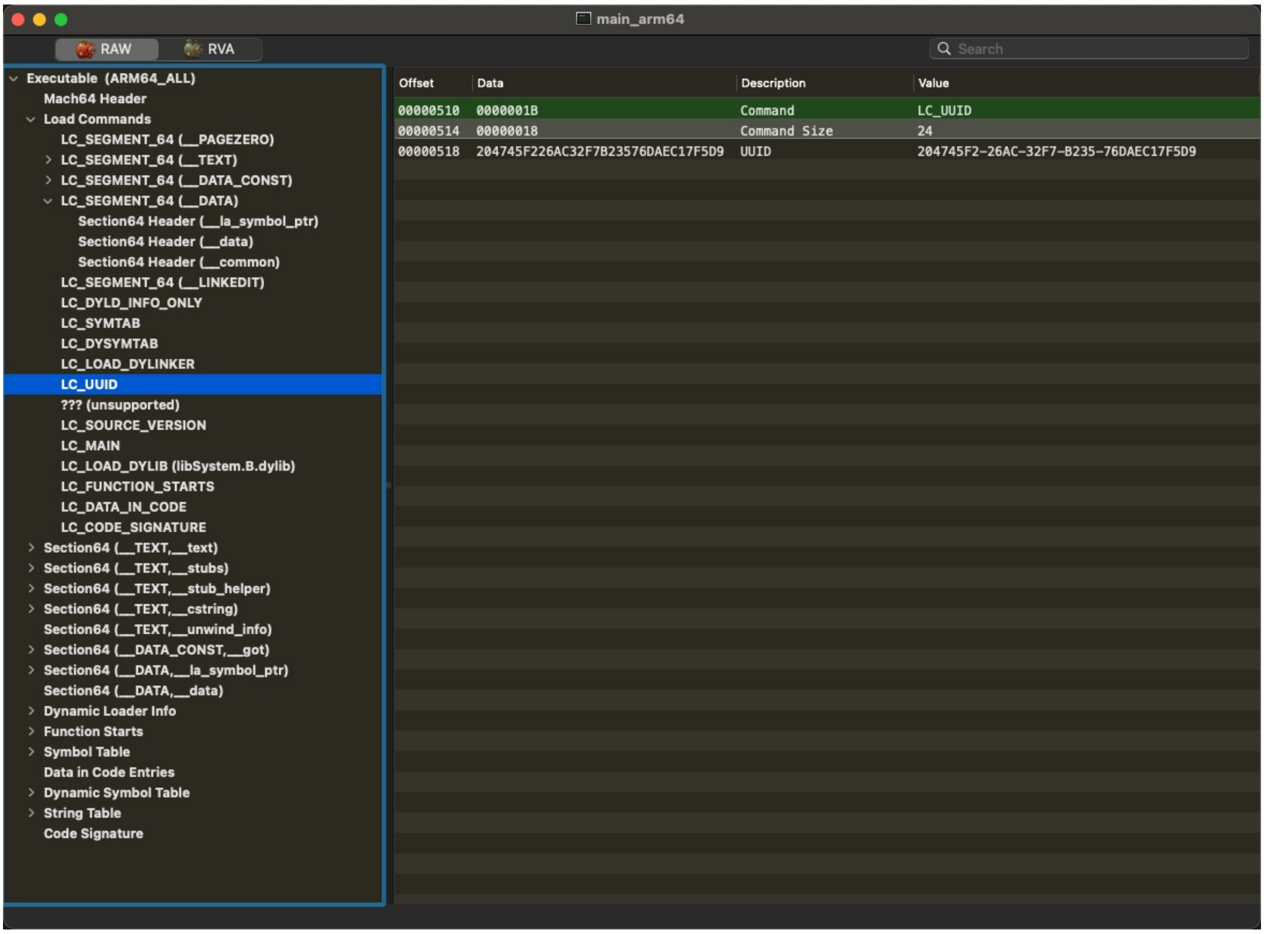
LC_DYSYMTAB



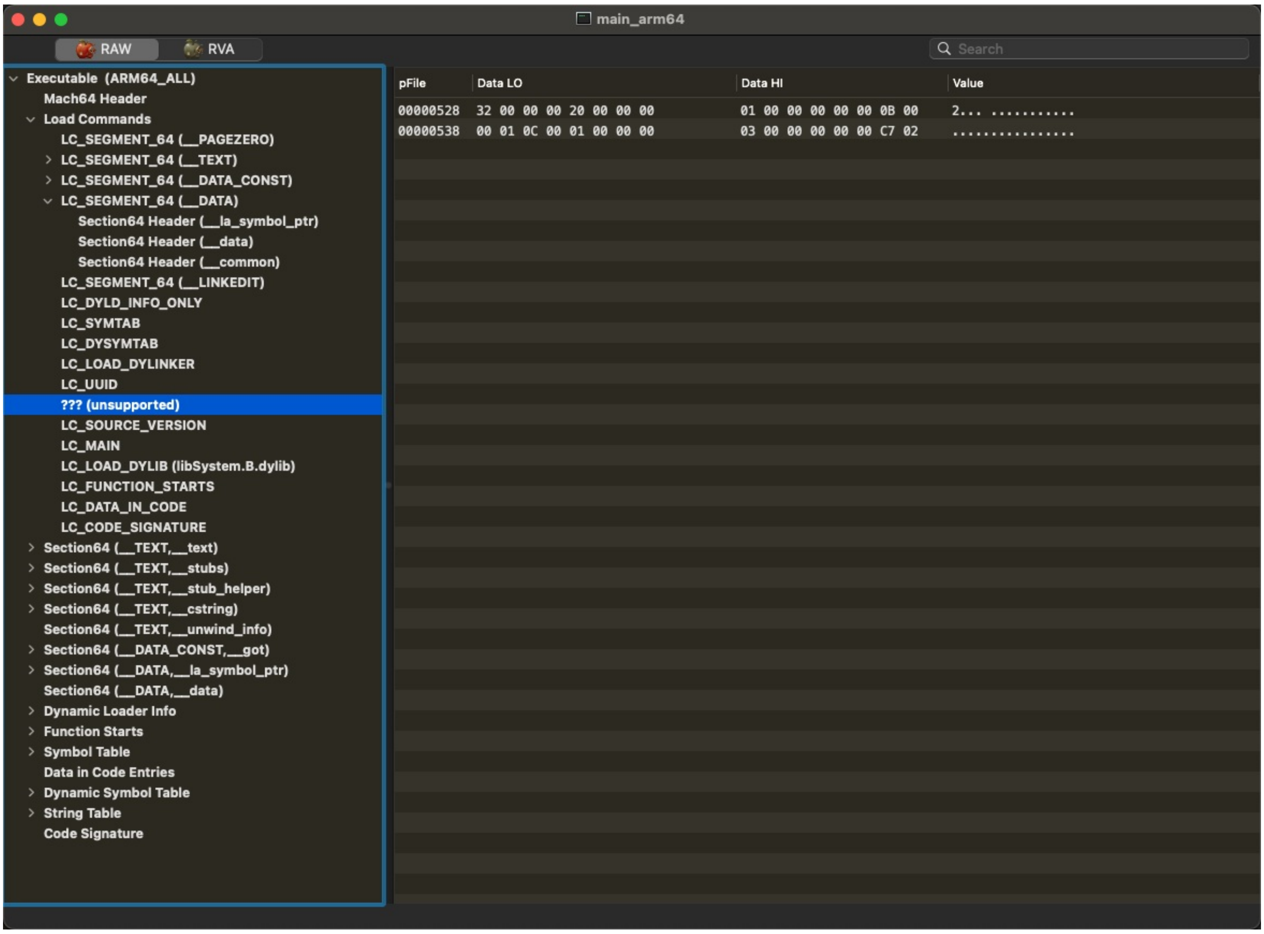
LC_LOAD_DYLINKER


main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
Section64 Header (__la_symbol_ptr)
Section64 Header (__data)
Section64 Header (__common)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset | Data | Description | Value
000004F0 0000000E Command LC_LOAD_DYLINKER
000004F4 00000020 Command Size 32
000004F8 0000000C Str Offset 12
000004FC 2F7573722F6C69622F64796C6400 Name /usr/lib/dyld

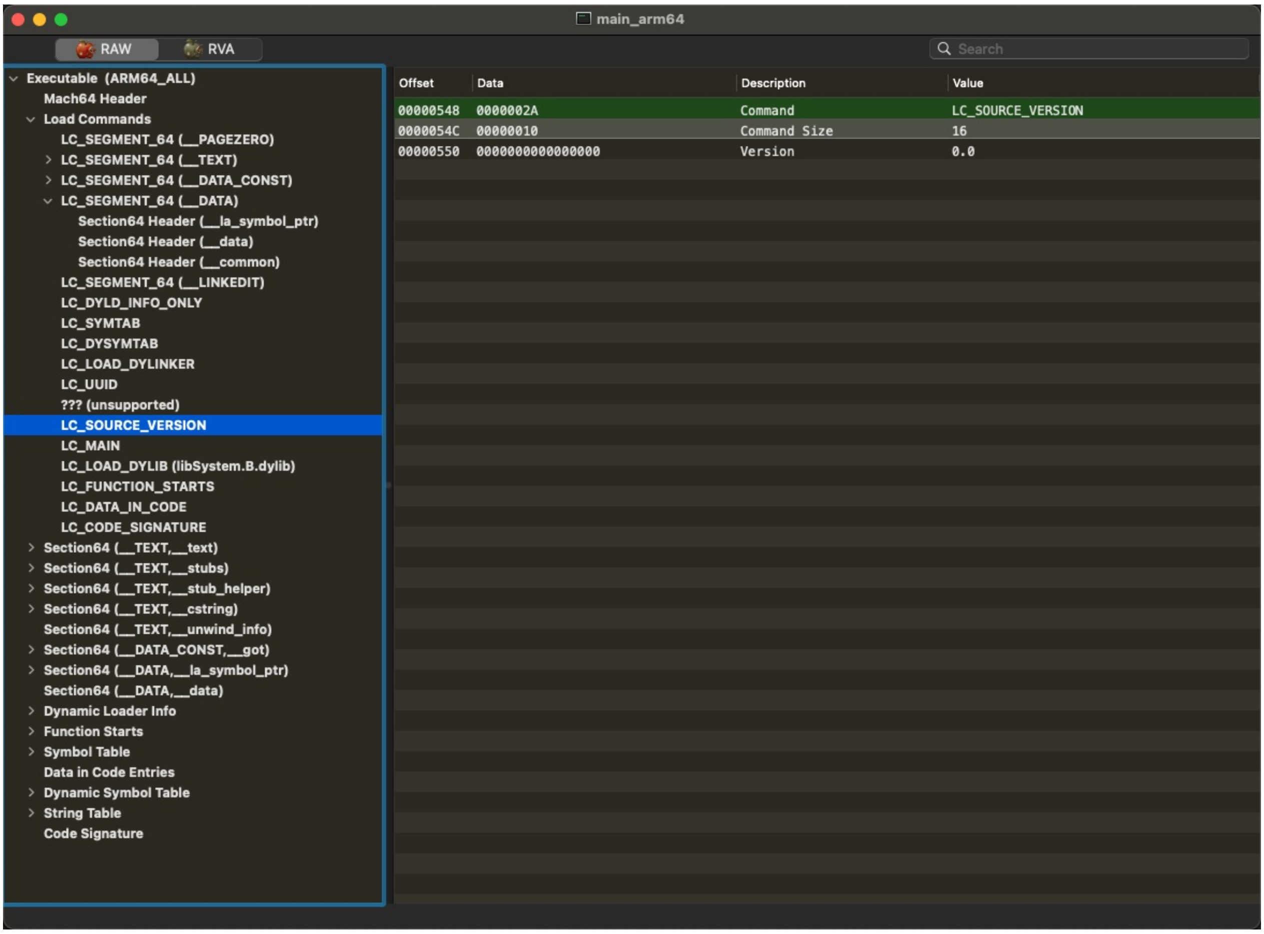
LC_UUID



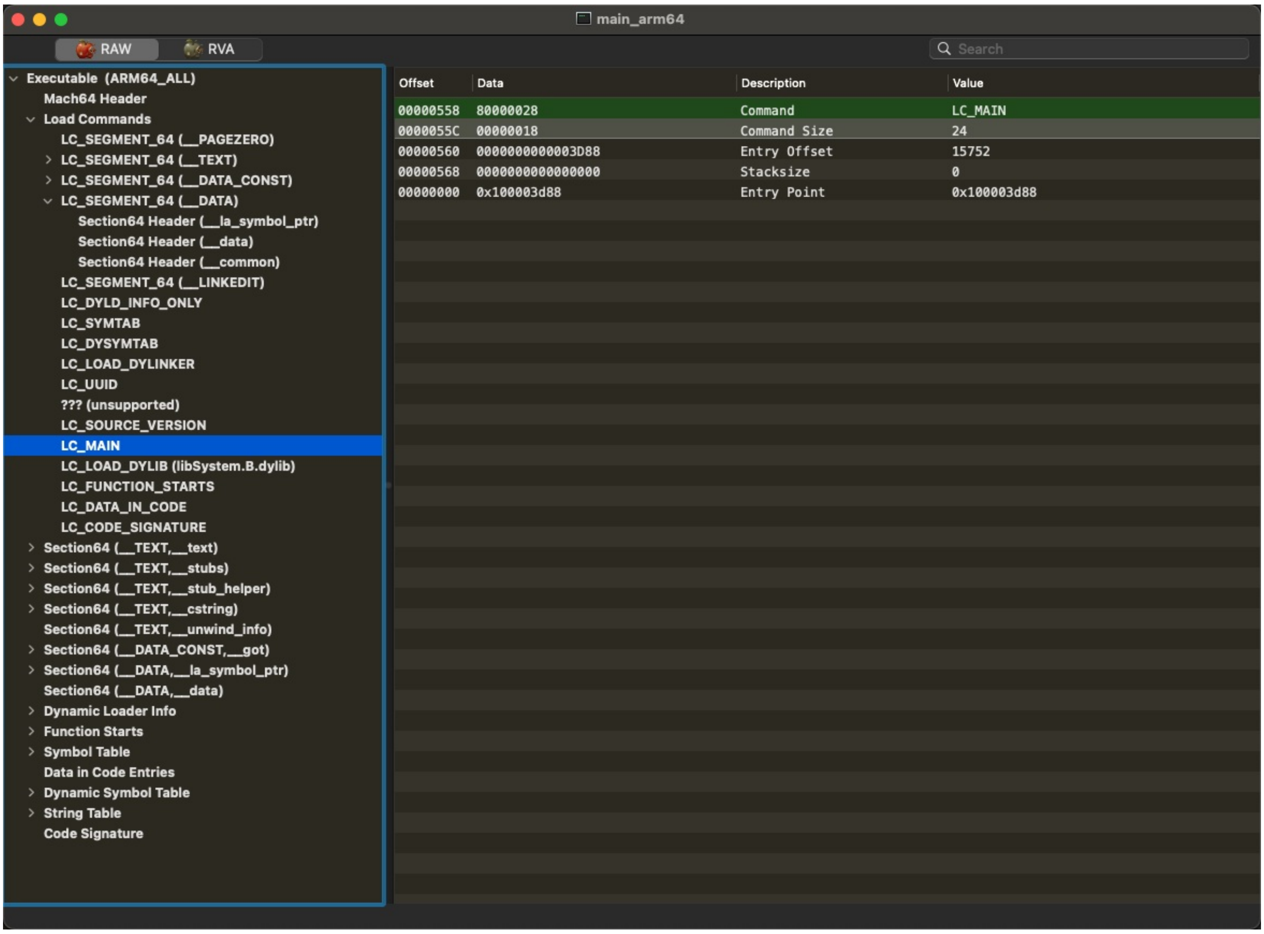
??? (unsupported)



LC_SOURCE_VERSION

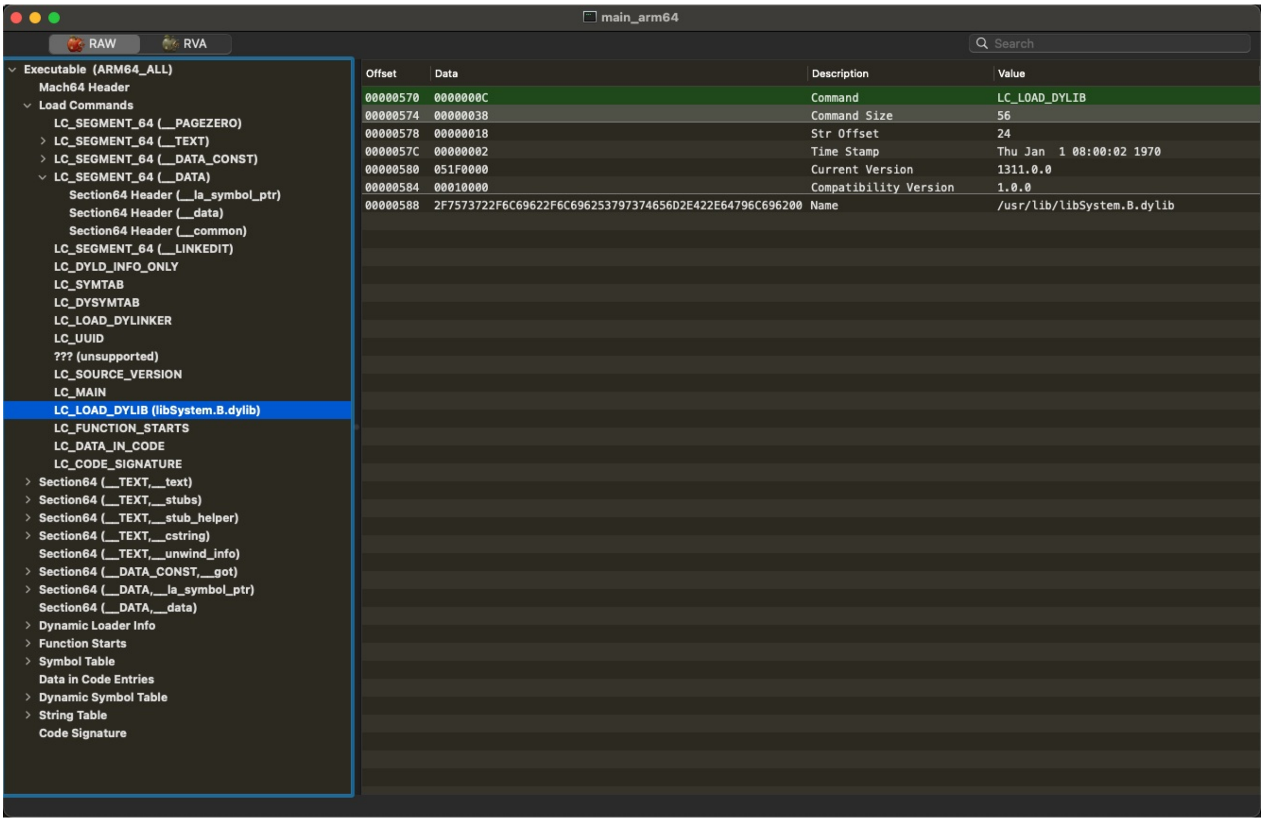

main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
LC_SEGMENT_64 (__PAGEZERO)
LC_SEGMENT_64 (__TEXT)
LC_SEGMENT_64 (__DATA_CONST)
LC_SEGMENT_64 (__DATA)
Section64 Header (__la_symbol_ptr)
Section64 Header (__data)
Section64 Header (__common)
LC_SEGMENT_64 (__LINKEDIT)
LC_DYLD_INFO_ONLY
LC_SYMTAB
LC_DYSYMTAB
LC_LOAD_DYLINKER
LC_UUID
??? (unsupported)
LC_SOURCE_VERSION
LC_MAIN
LC_LOAD_DYLIB (libSystem.B.dylib)
LC_FUNCTION_STARTS
LC_DATA_IN_CODE
LC_CODE_SIGNATURE
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
00000548 0000002A Command LC_SOURCE_VERSION
0000054C 00000010 Command Size 16
00000550 0000000000000000 Version 0.0

LC_MAIN

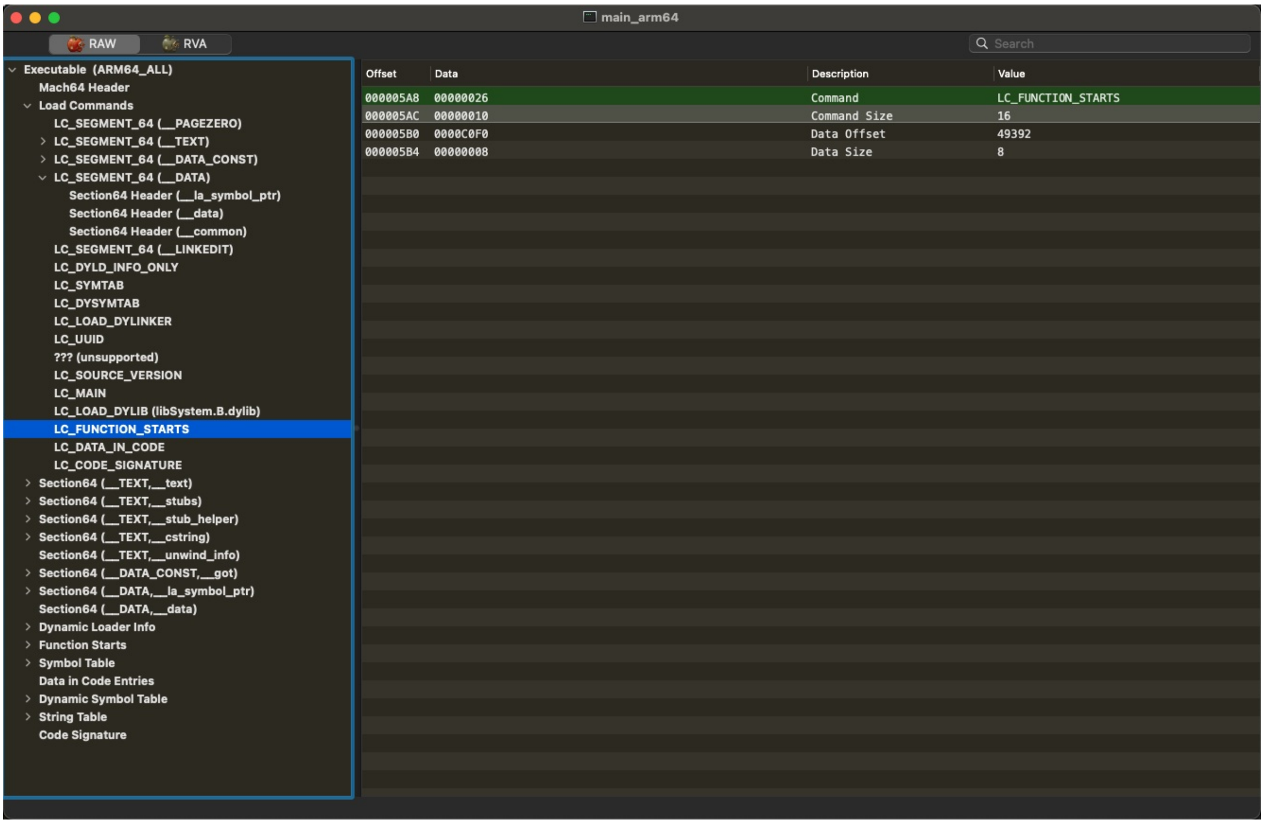


估计就是 入口函数 入口地址 = 一般叫做 main函数的 地方了

LC_LOAD_DYLIB (libSystem.B.dylib)

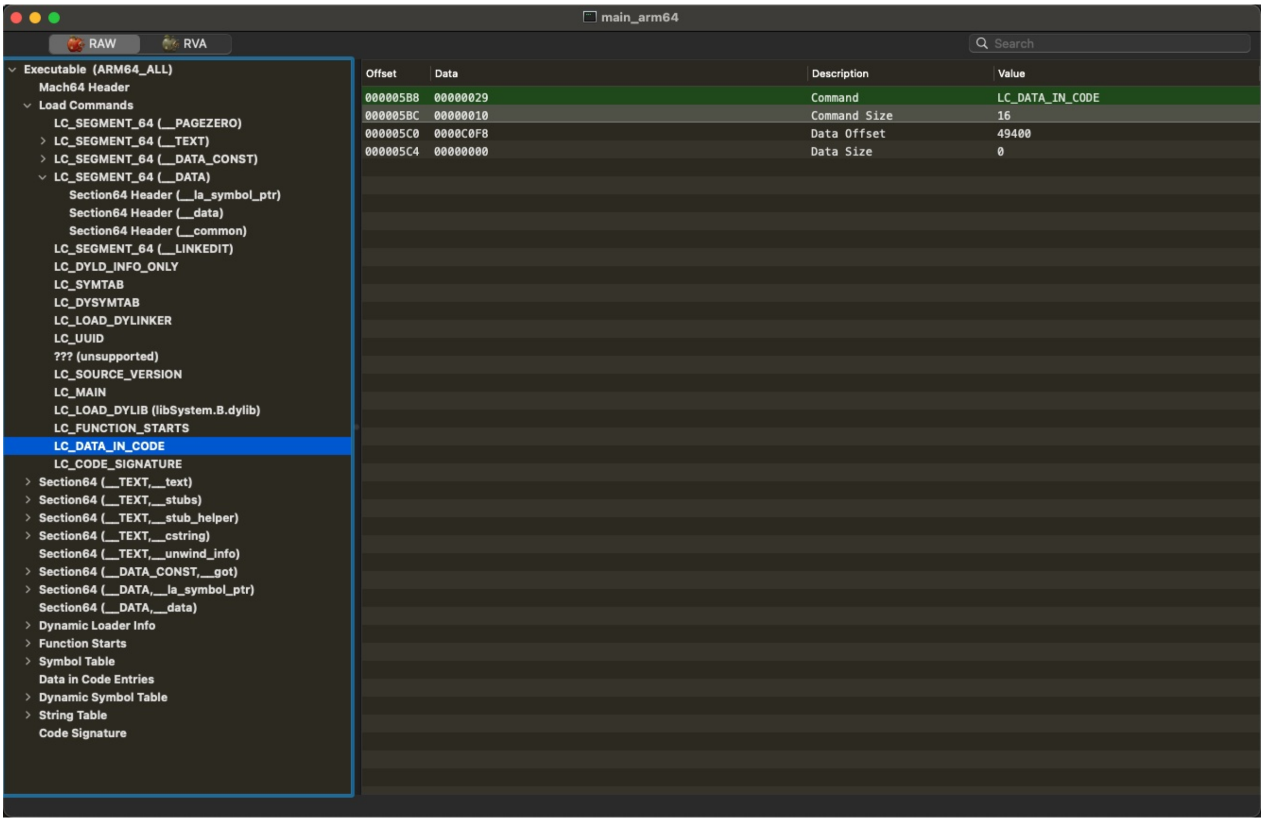


LC_FUNCTION_STARTS

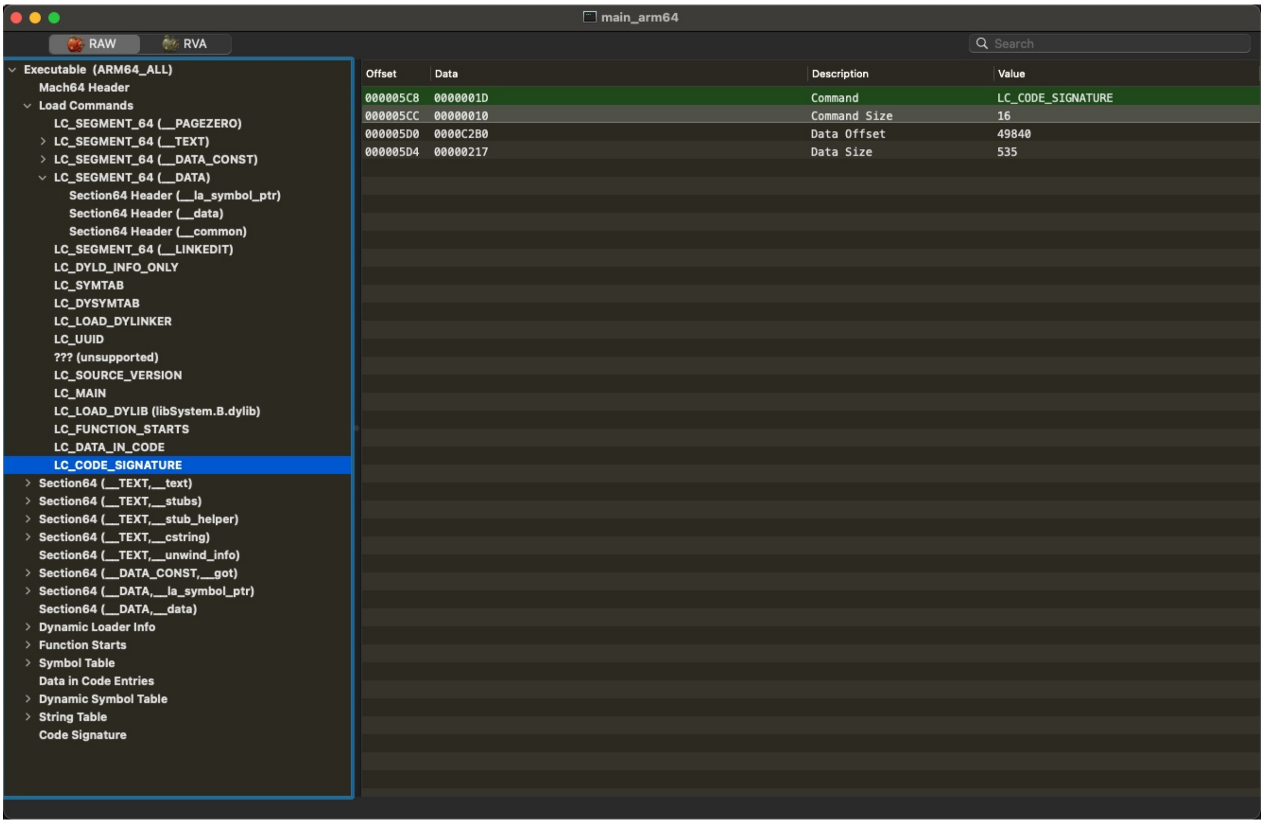


好像是：需要启动运行的函数的列表？

LC_DATA_IN_CODE

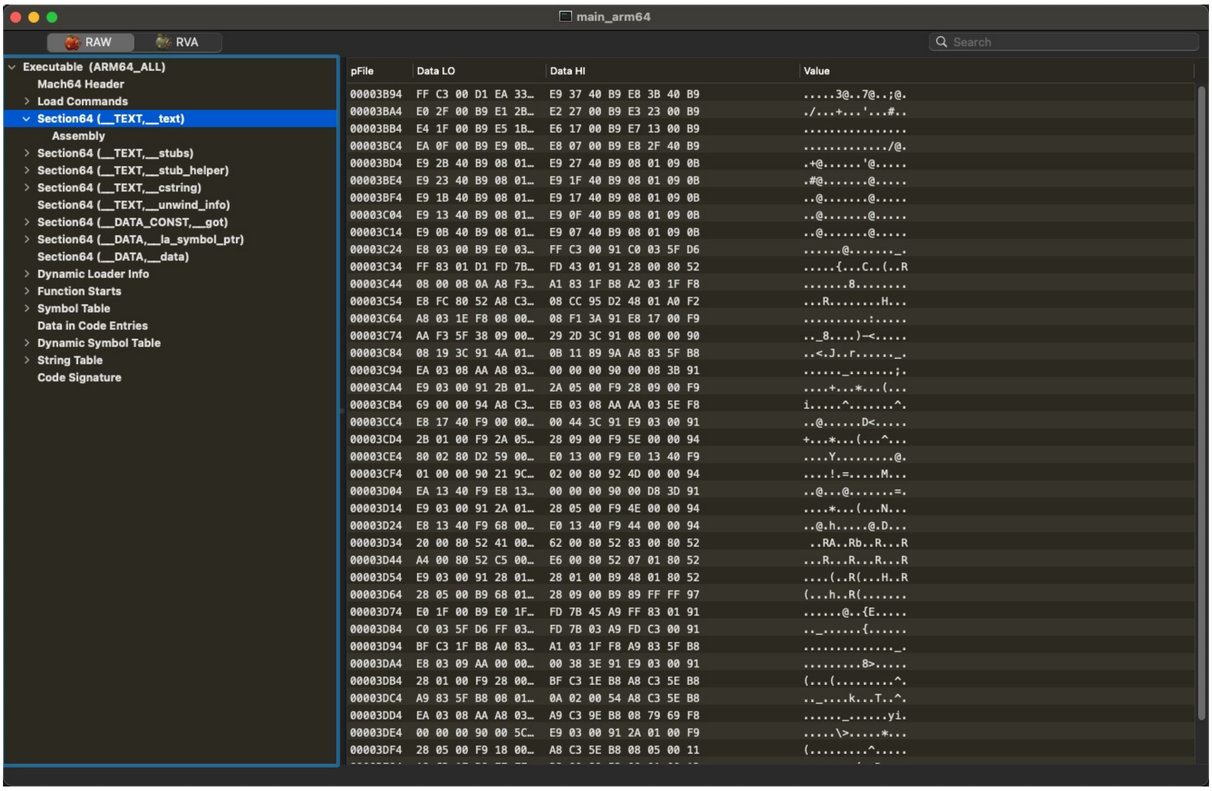


LC_CODE_SIGNATURE

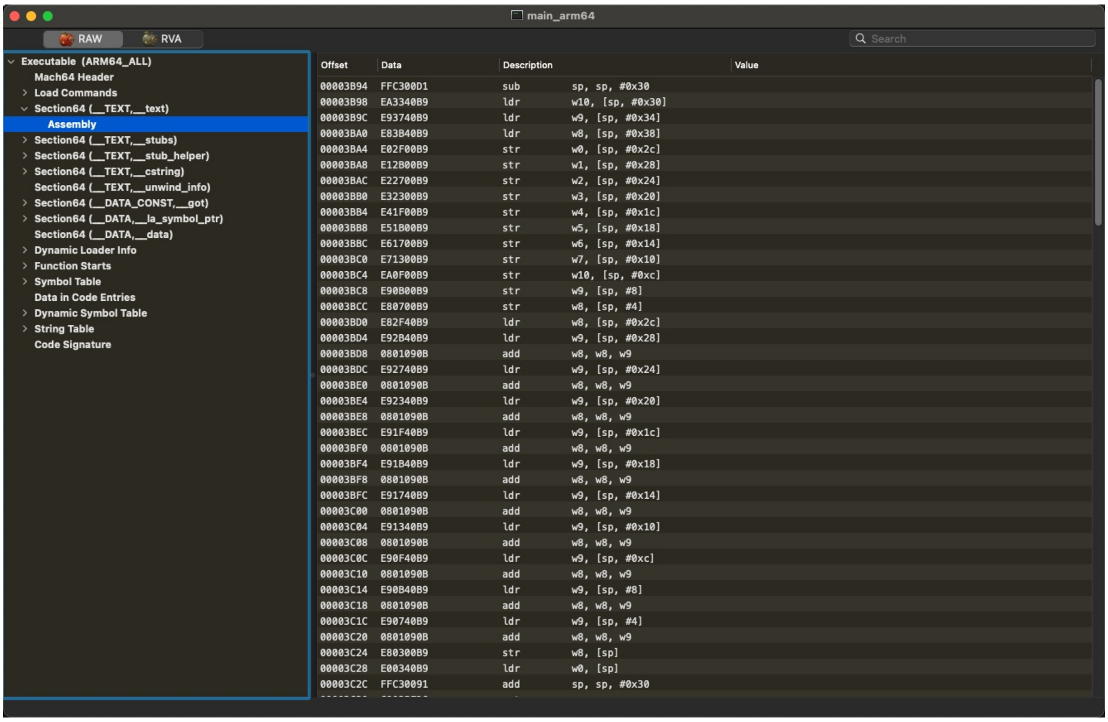


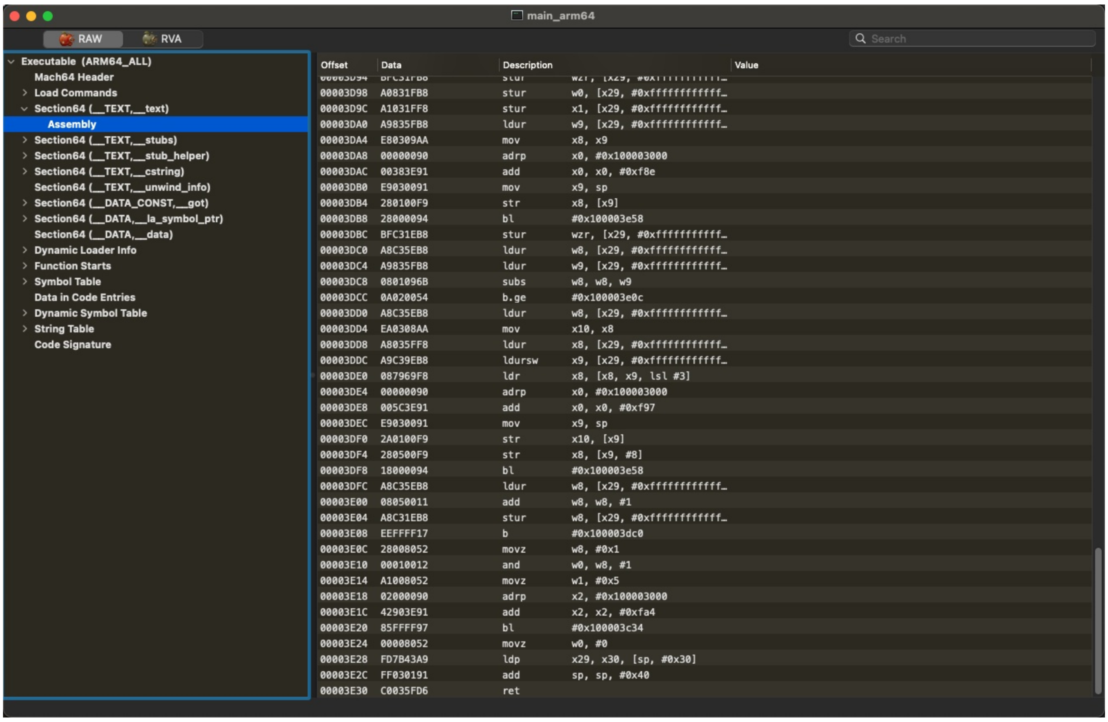
Sections

Section64 (`__TEXT,__text`)

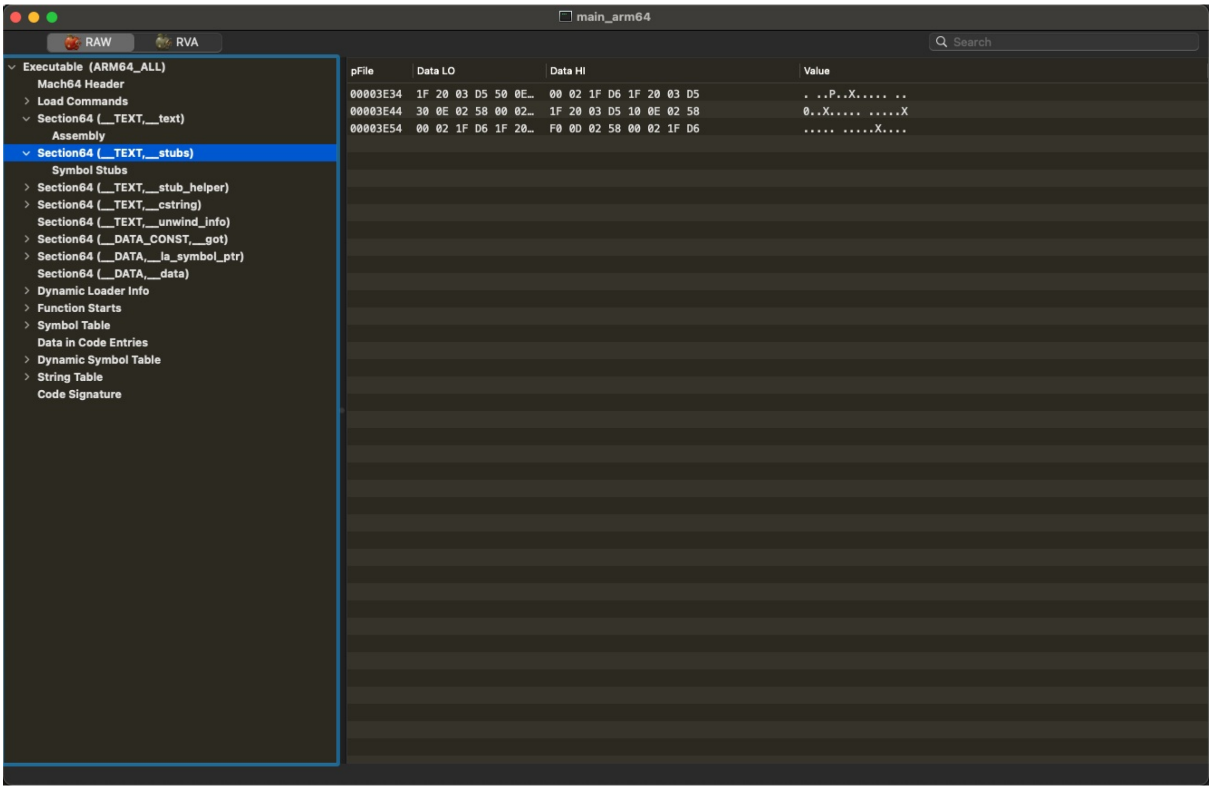
- 

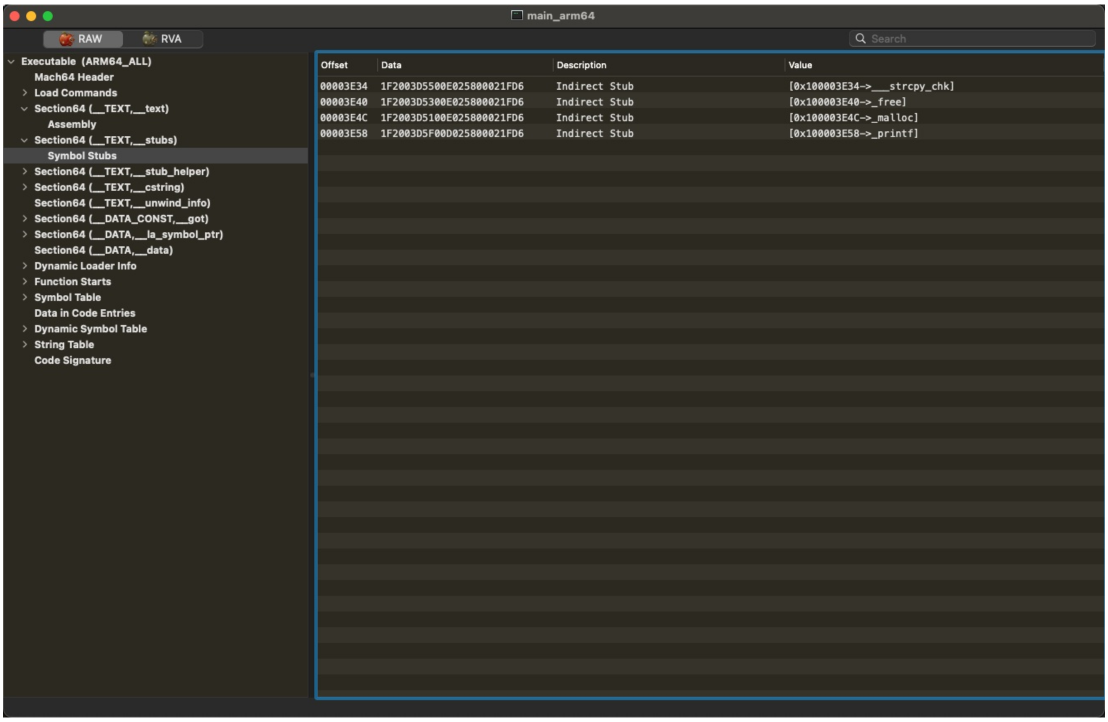
  - Assembly

- 

- 

Section64 (`__TEXT,__stubs`)

- 

    - Symbol Stubs
        - 

好像是：

stub=表示 桩， 地基

表示，代码运行前，要打地基 = 做好准备

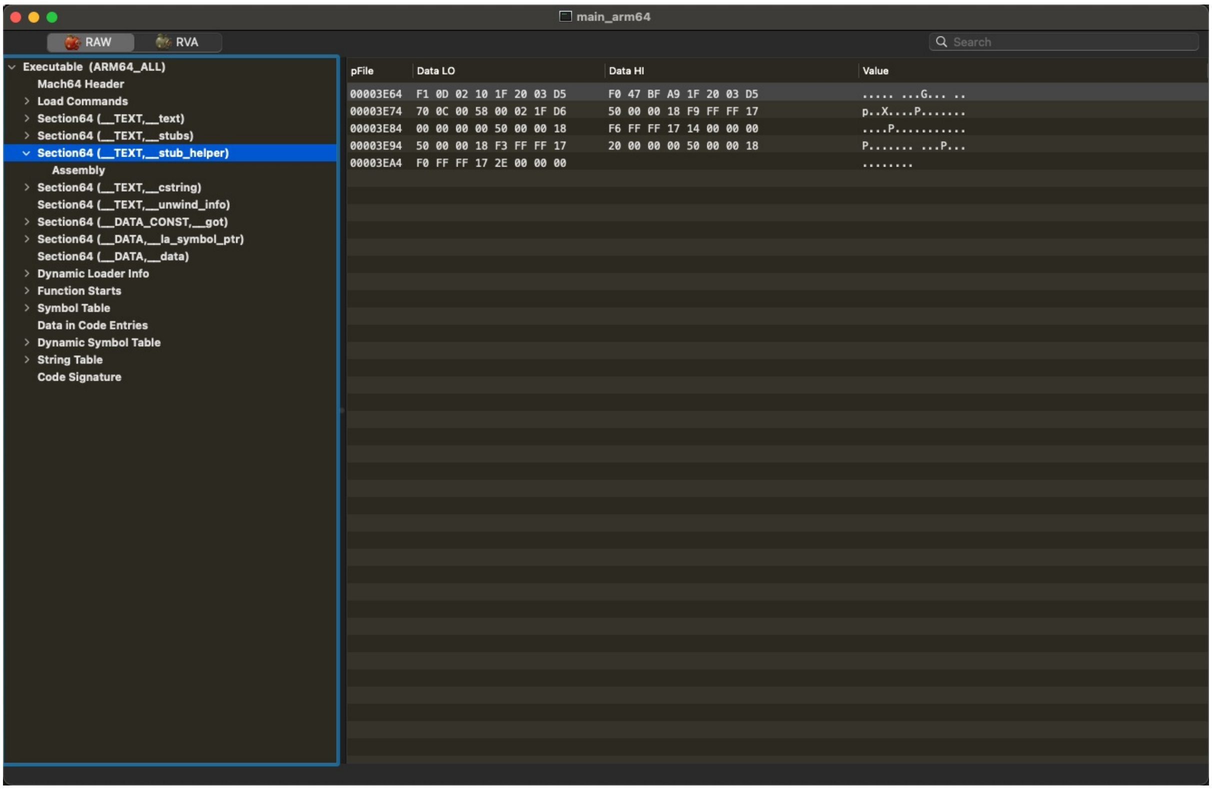
所以此处表示：所引用的外部的函数

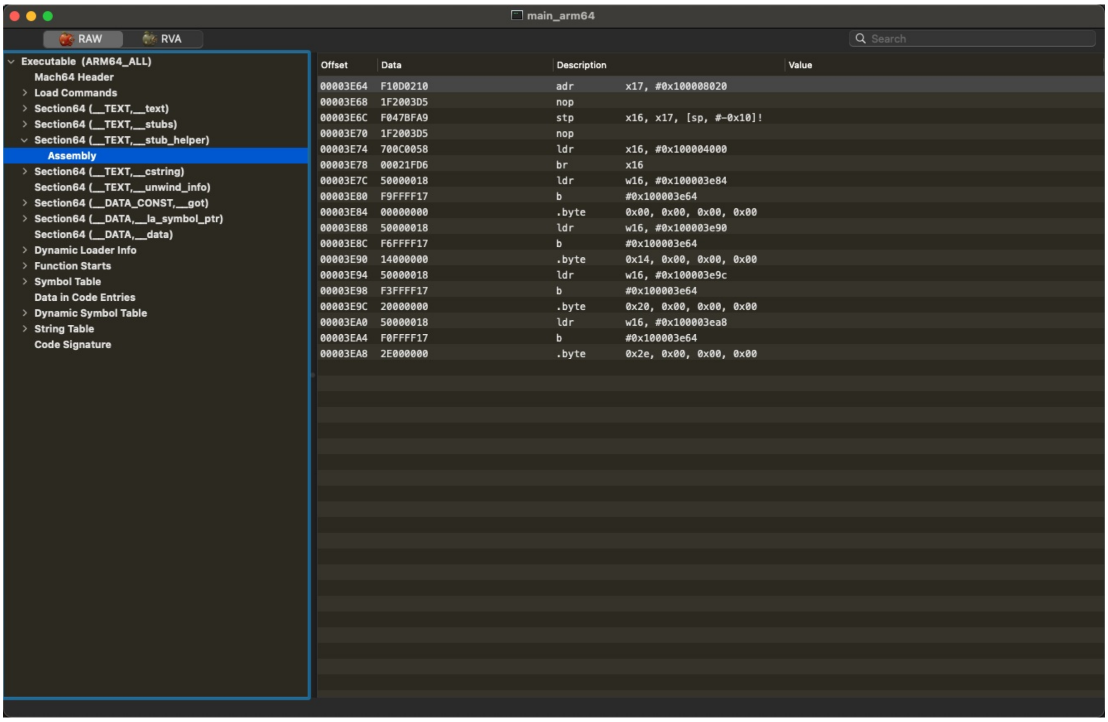
此处分别是：

- `___strcpy_chk`

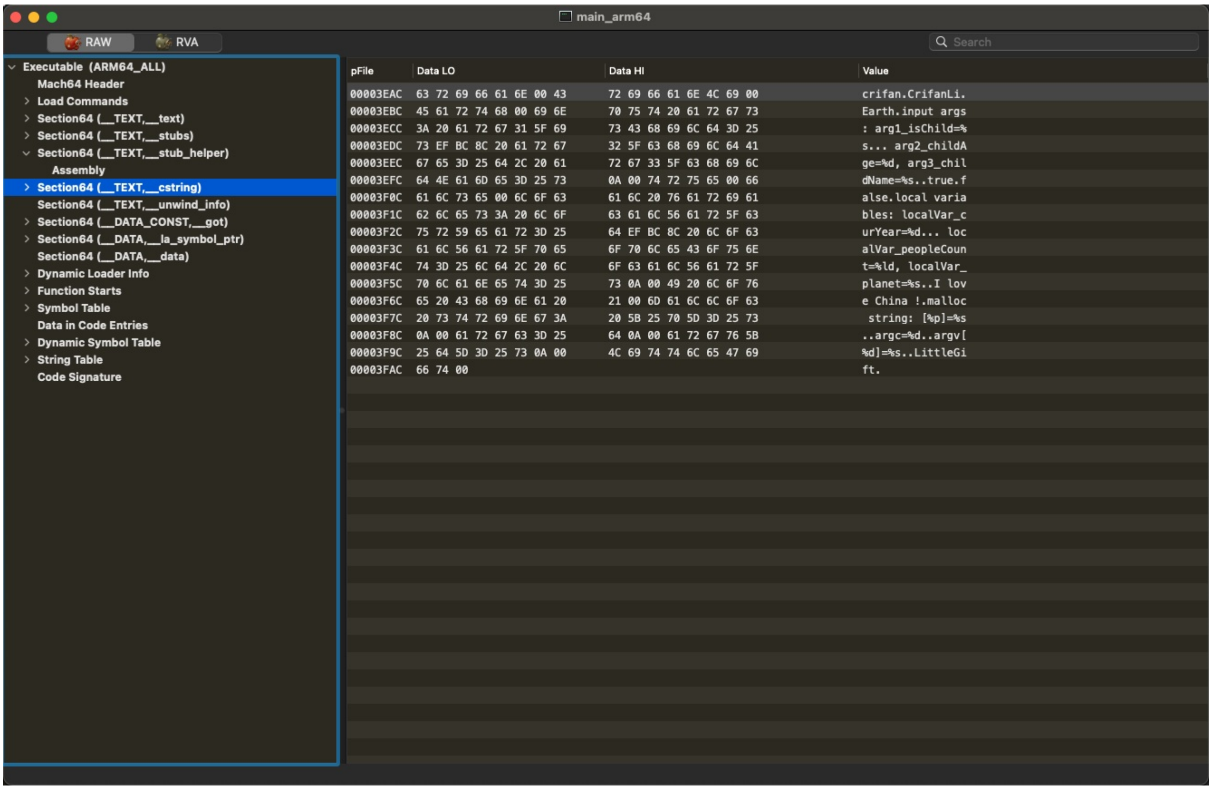
- `_free`
- `_malloc`
- `_printf`

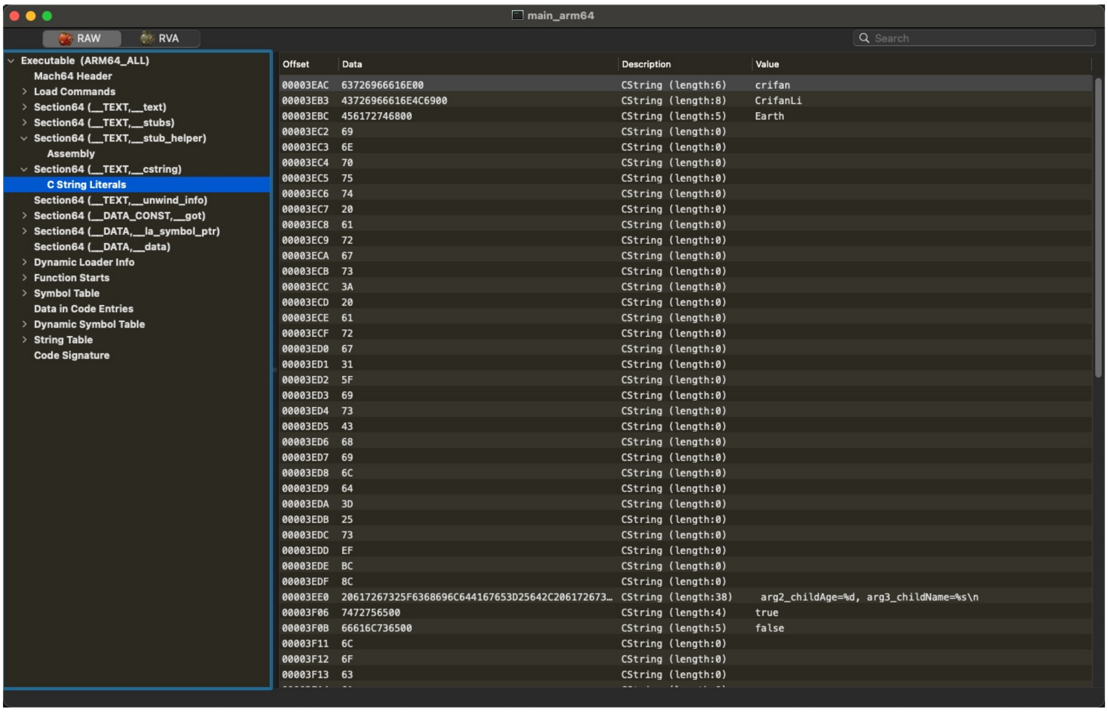
Section64 (`__TEXT,__stub_helper`)

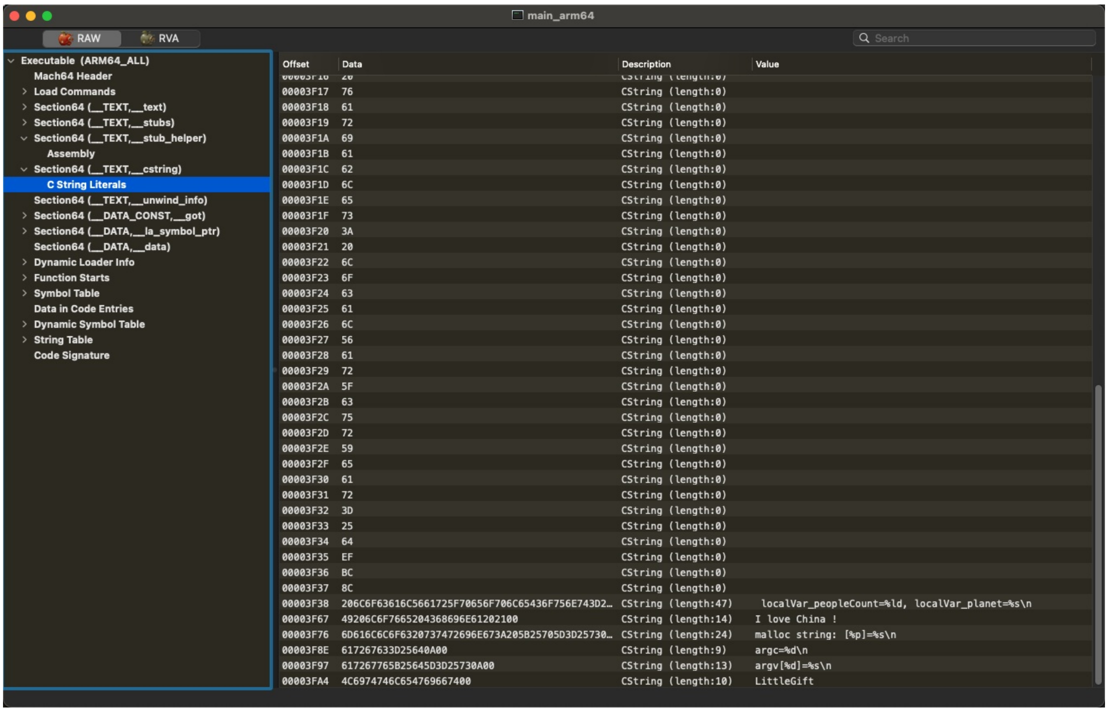
- 

  - Assembly
    - 

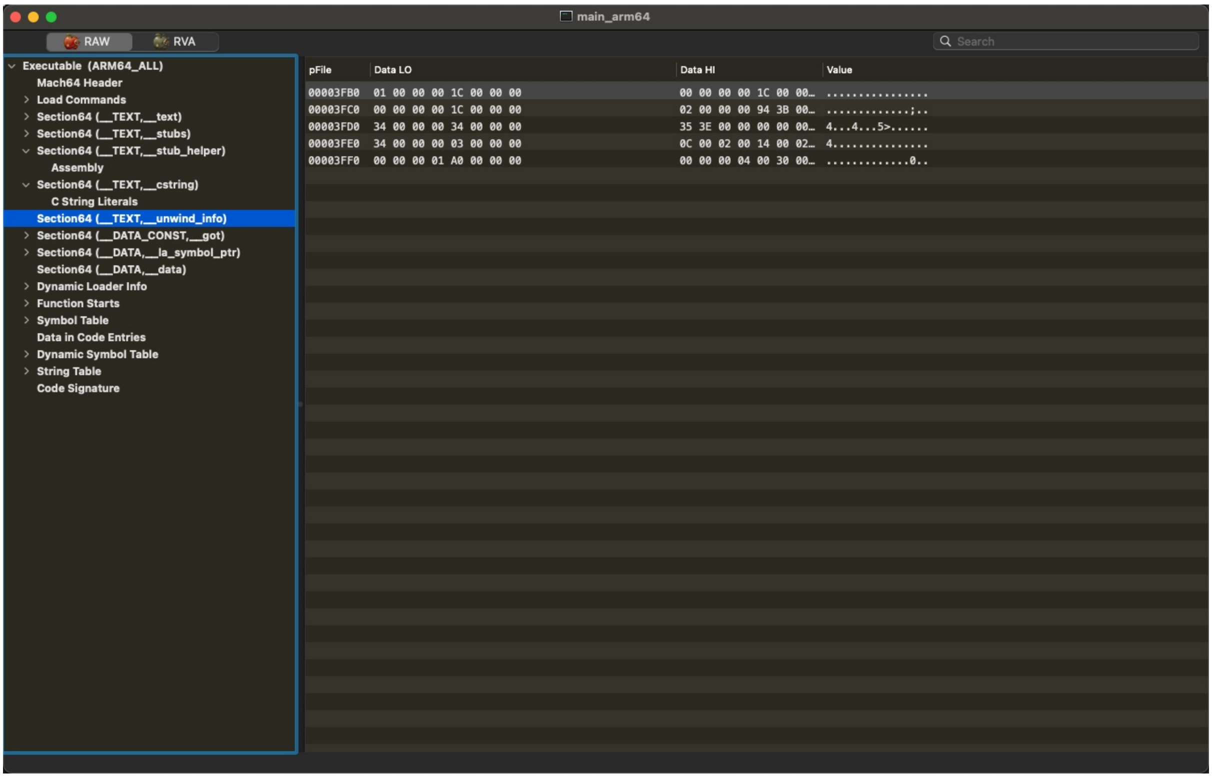
Section64 (`__TEXT,__cstring`)

- 

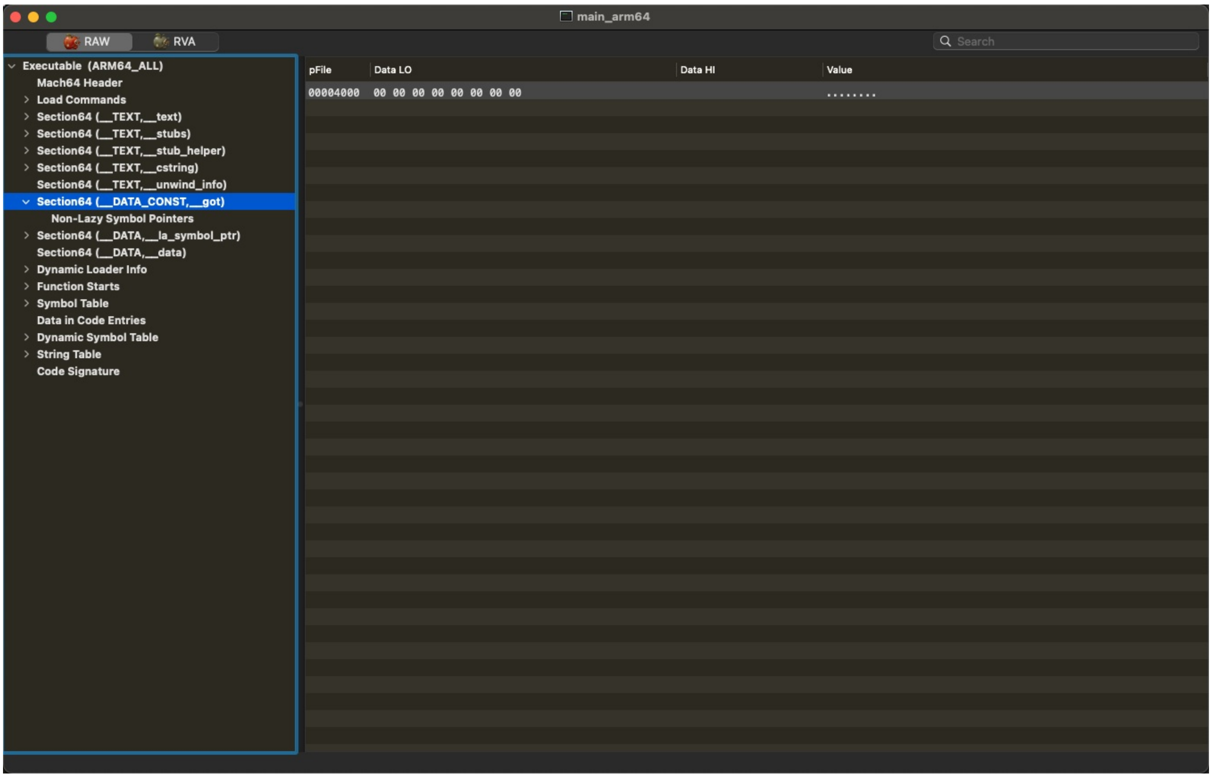
    - C String Literals
        - 

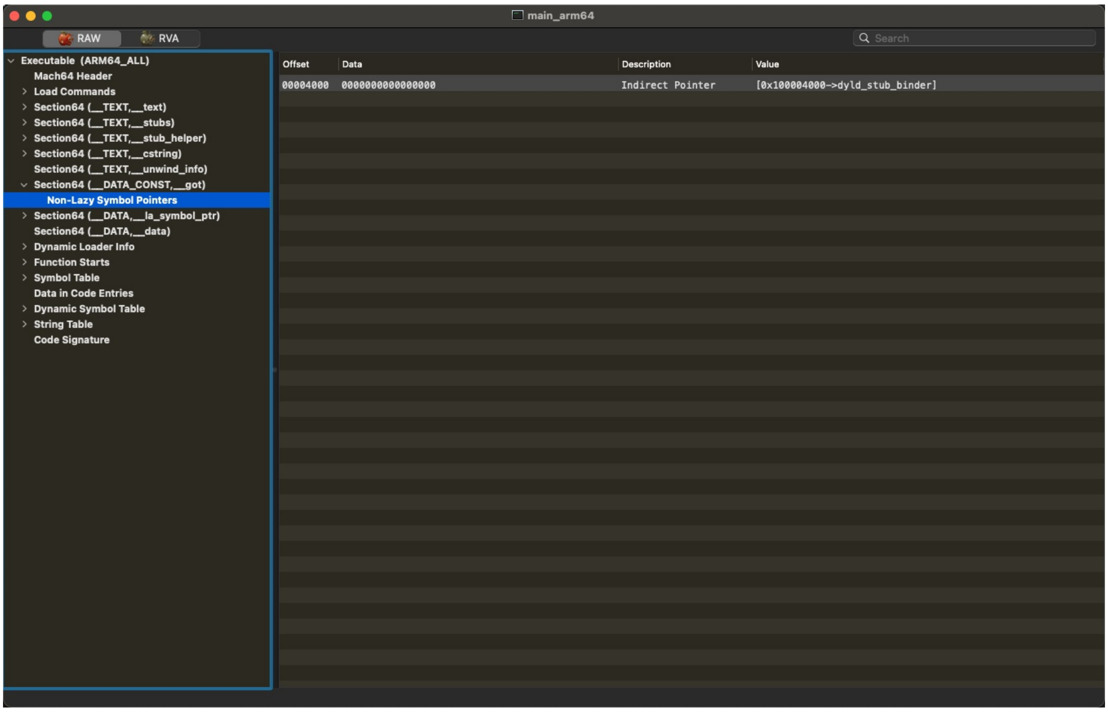
- 

Section64 (`__TEXT,__unwind_info`)

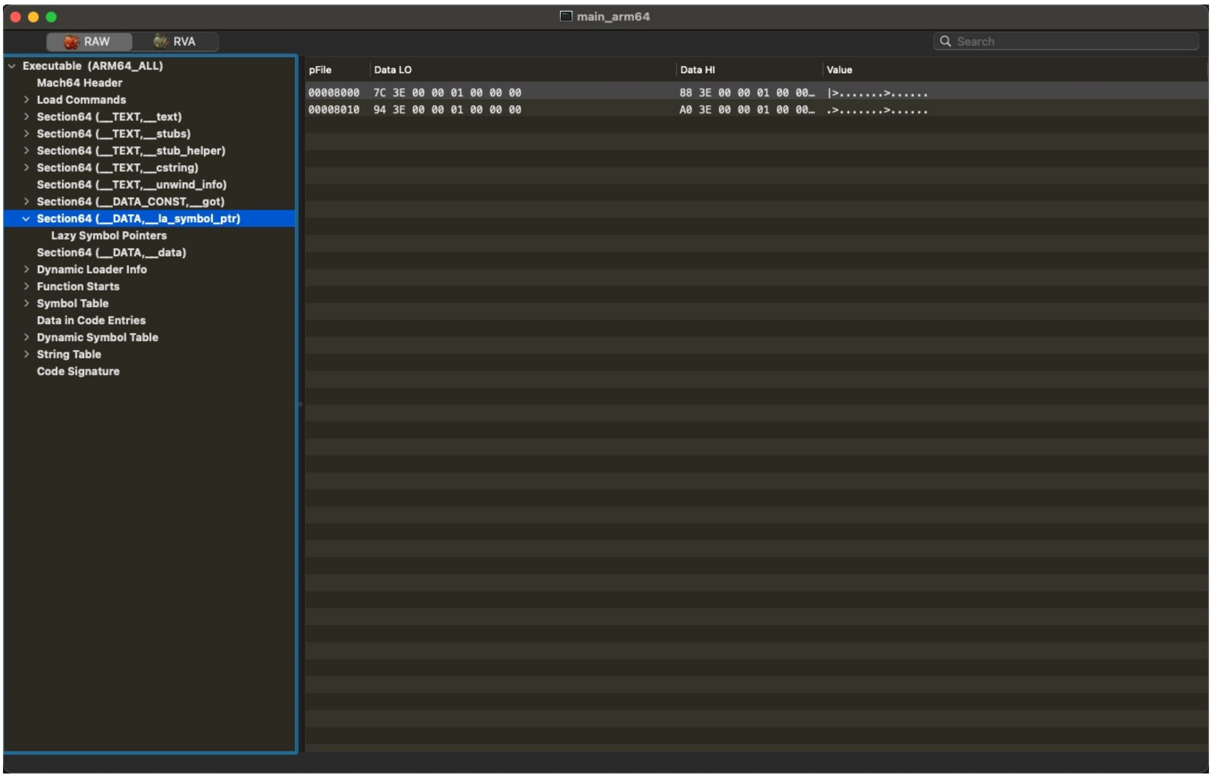
- 

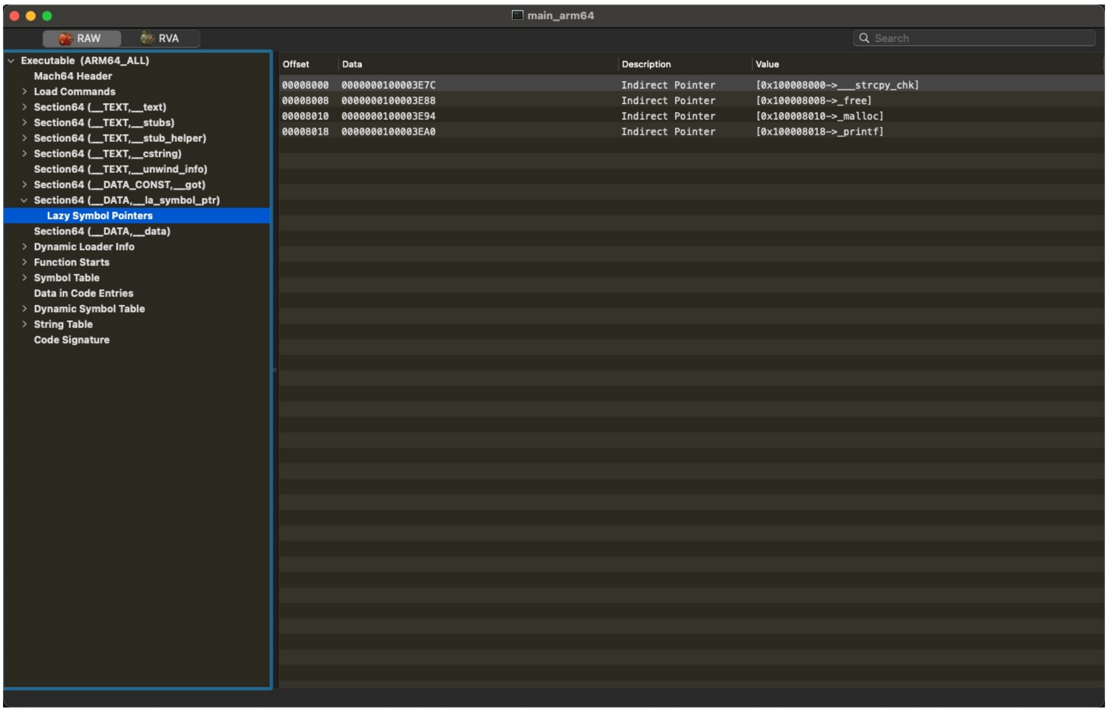
Section64 (`__DATA_CONST,__got`)

- 

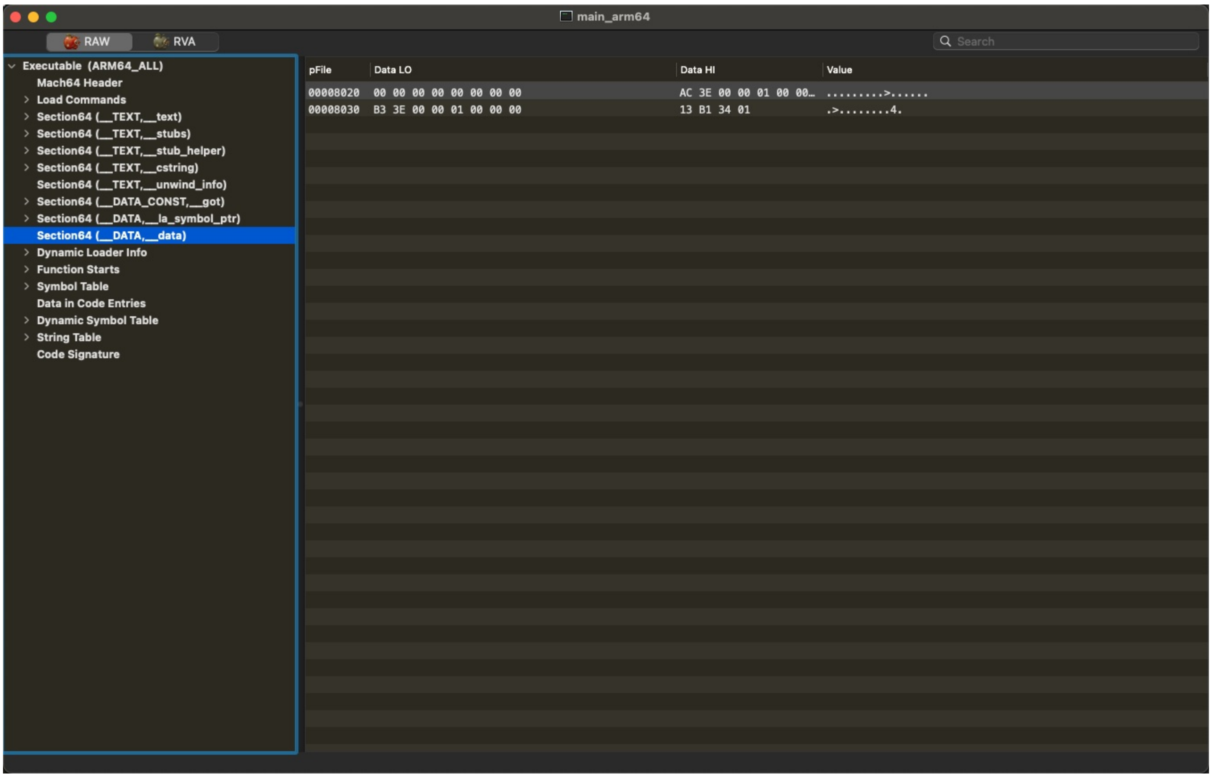
    - Non-Lazy Symbol Pointers
        - 

Section64 (`__DATA,__la_symbol_ptr`)

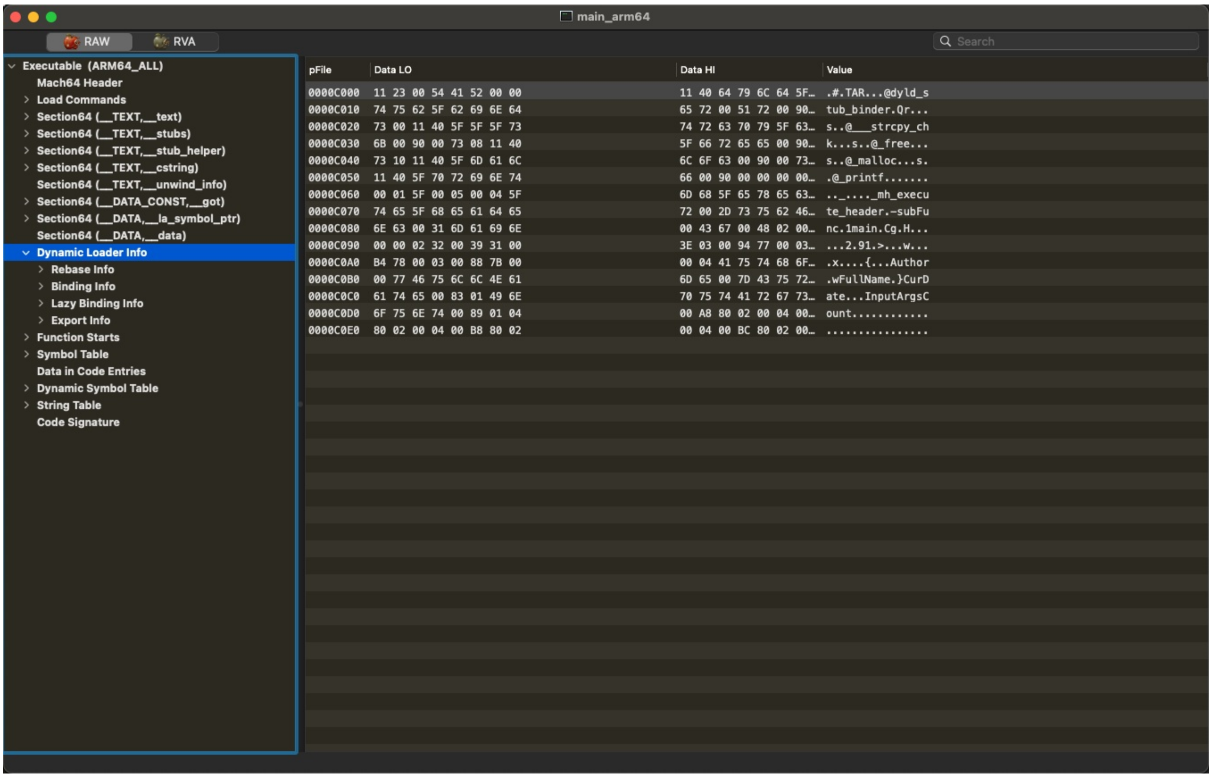
- 

    - Lazy Symbol Pointers
        - 

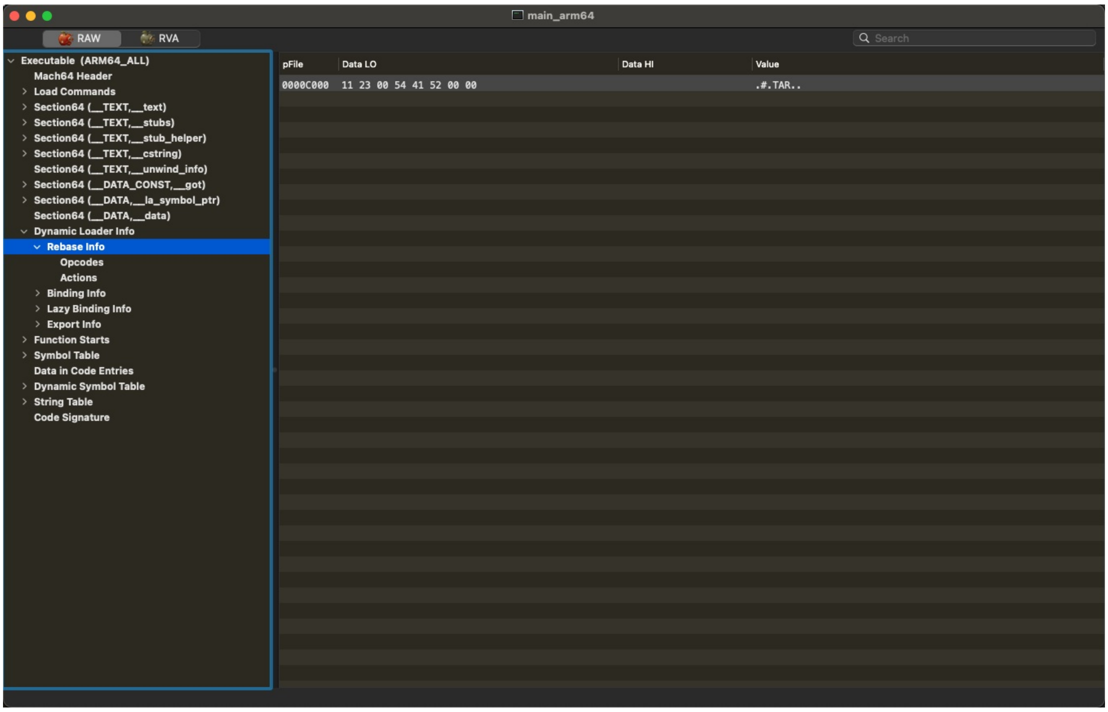
Section64 (`__DATA,__data`)

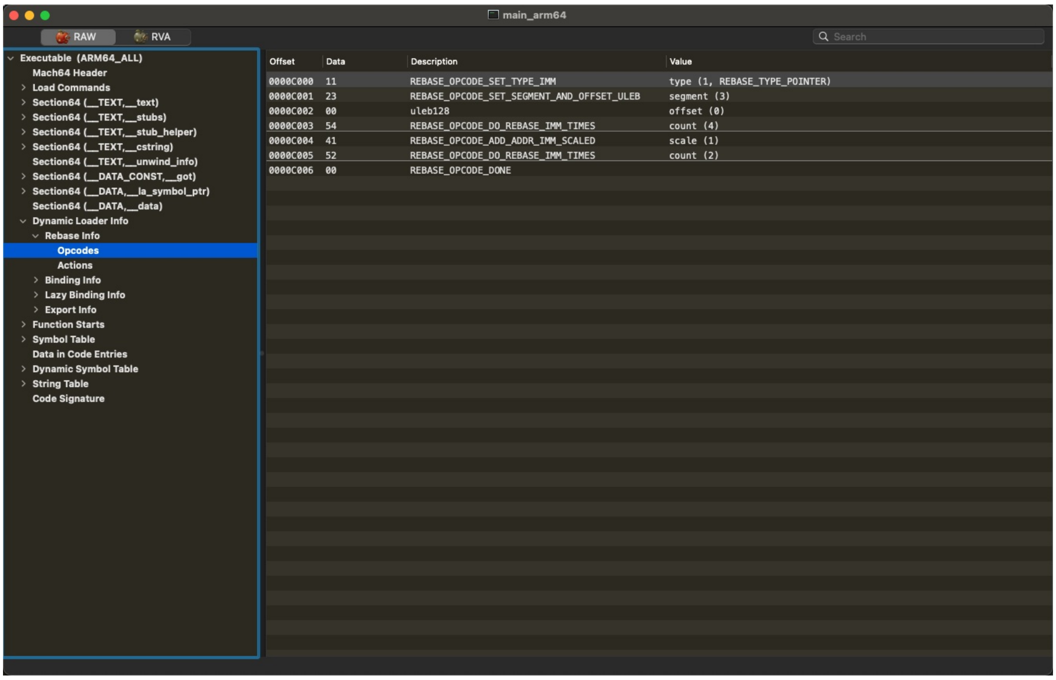
- 

Dynamic Loader Info

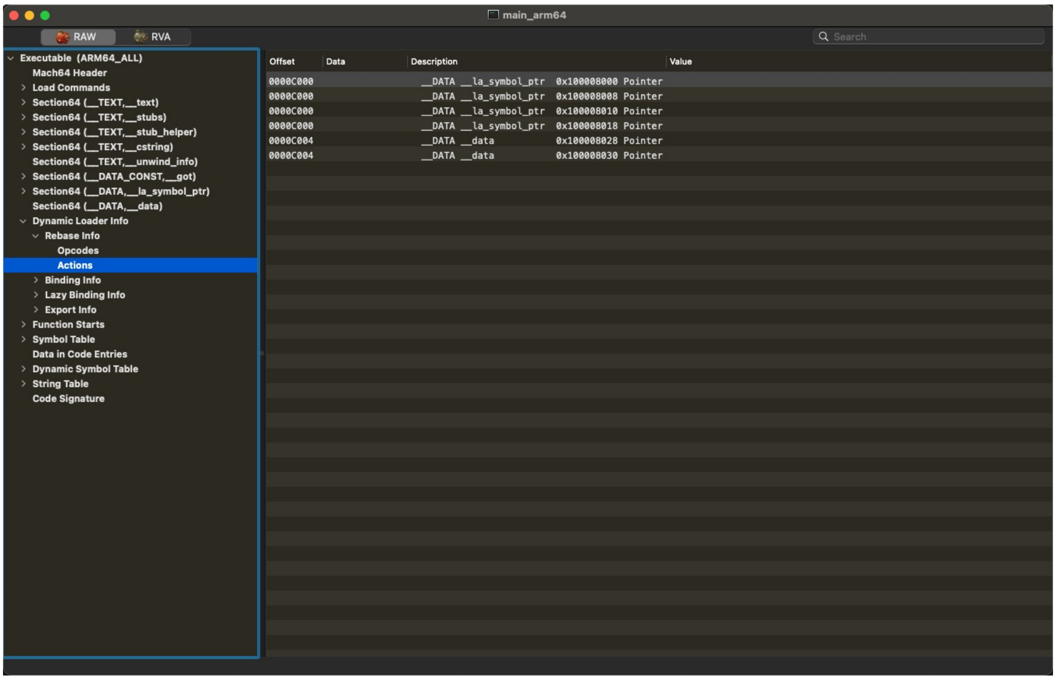
- 

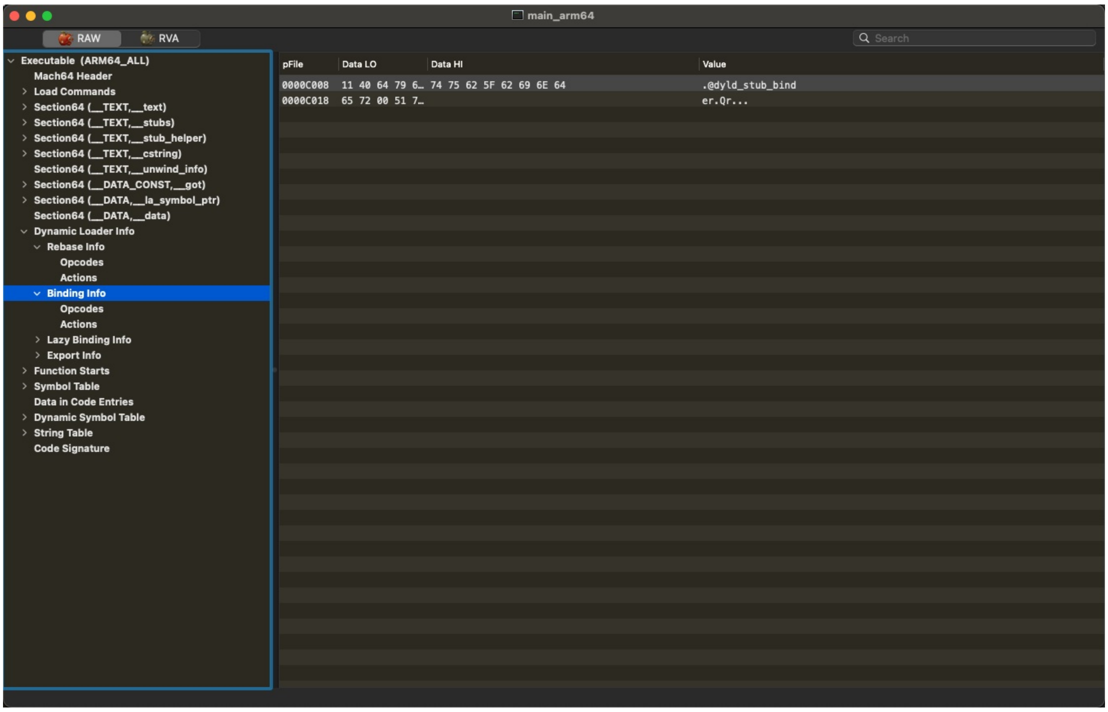
    - Rebase Info

- 

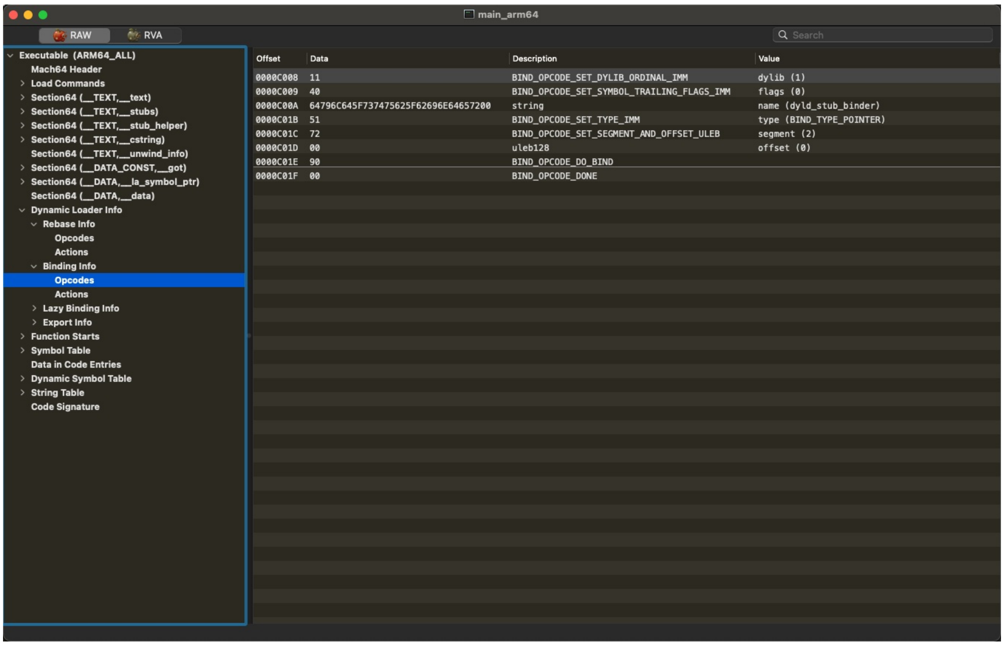
- Opcodes
  - 

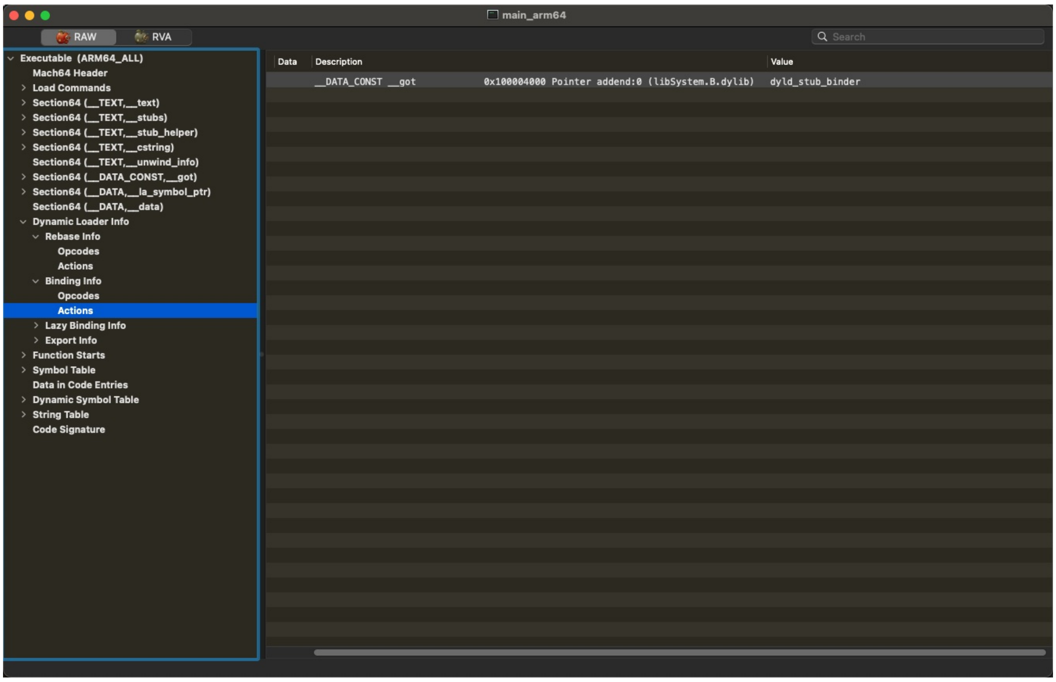
- Actions

- 

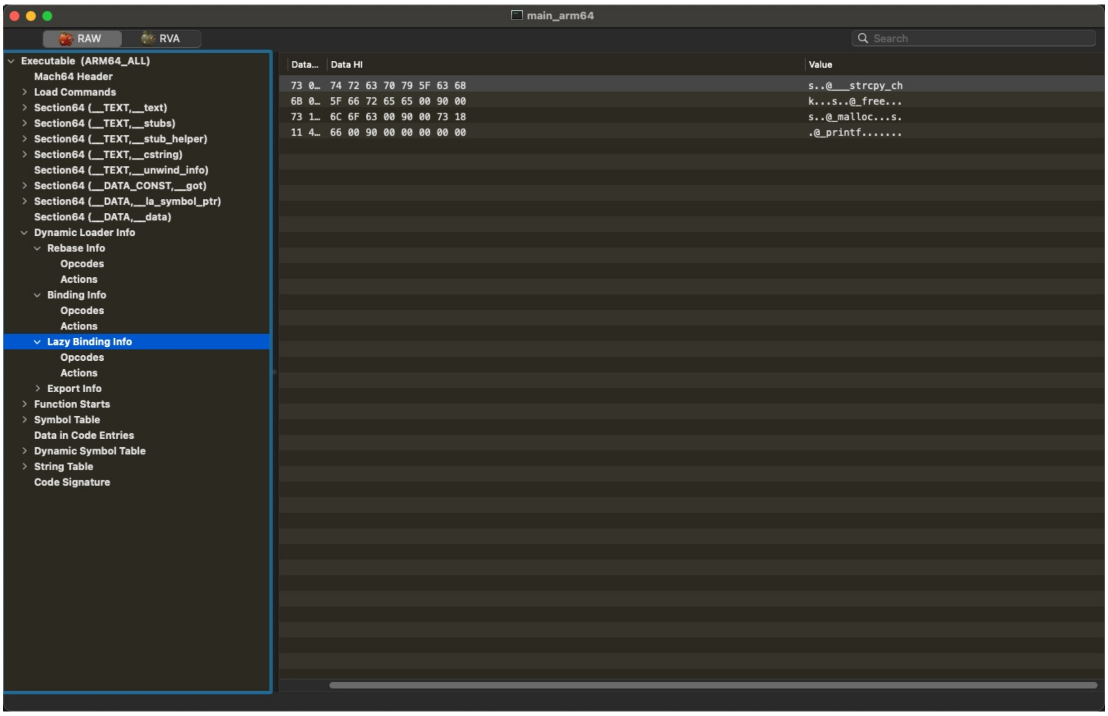
- Binding Info
    - 

        - Opcodes

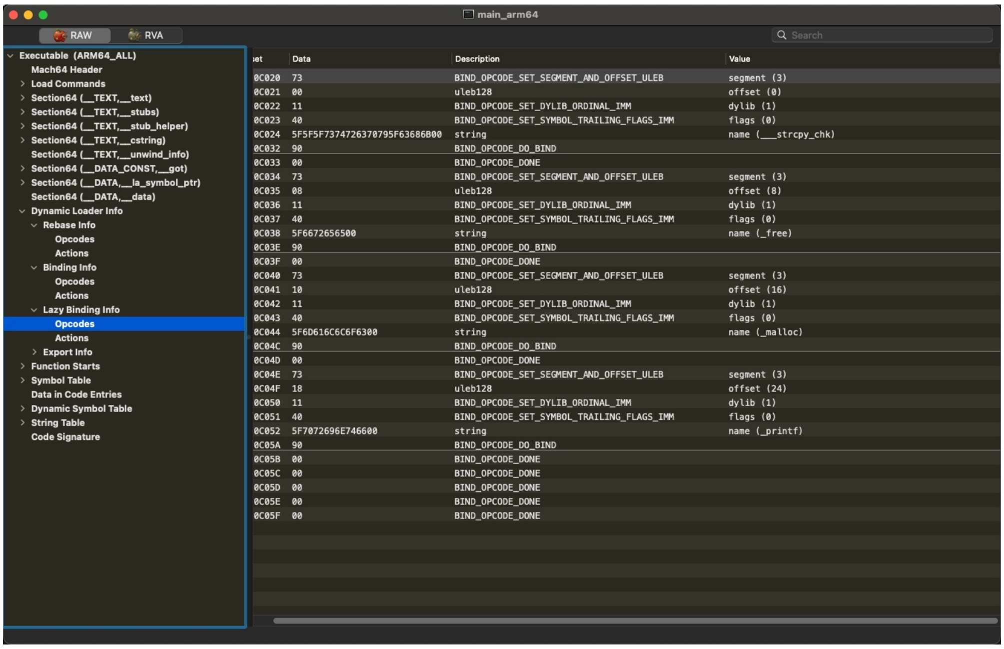
- 

- Actions
  - 

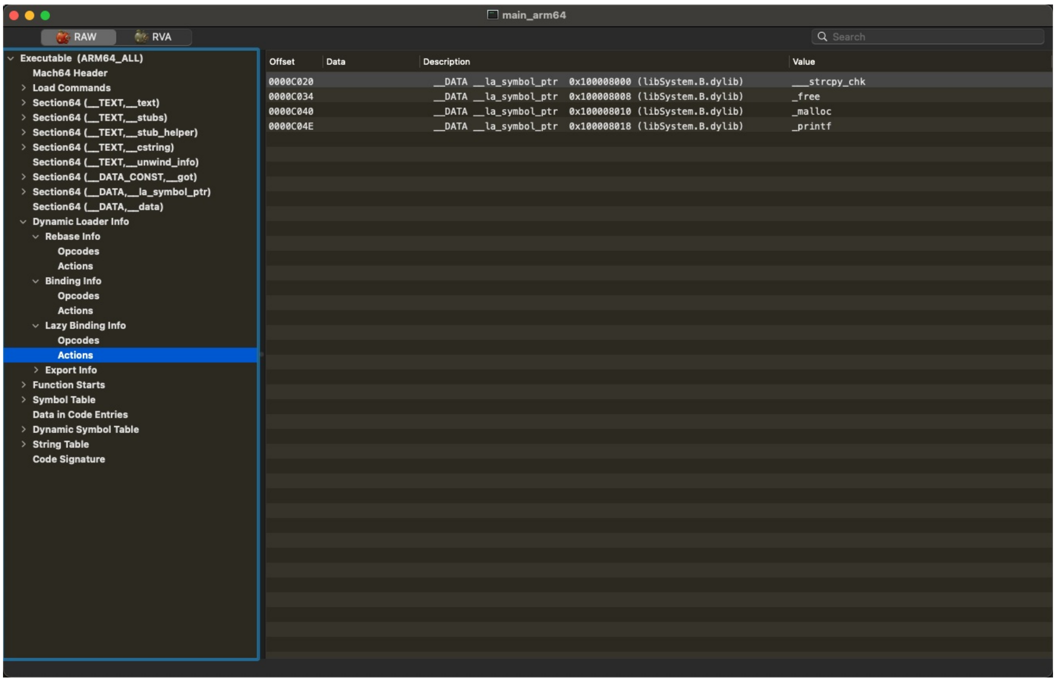
- Lazy Binding Info

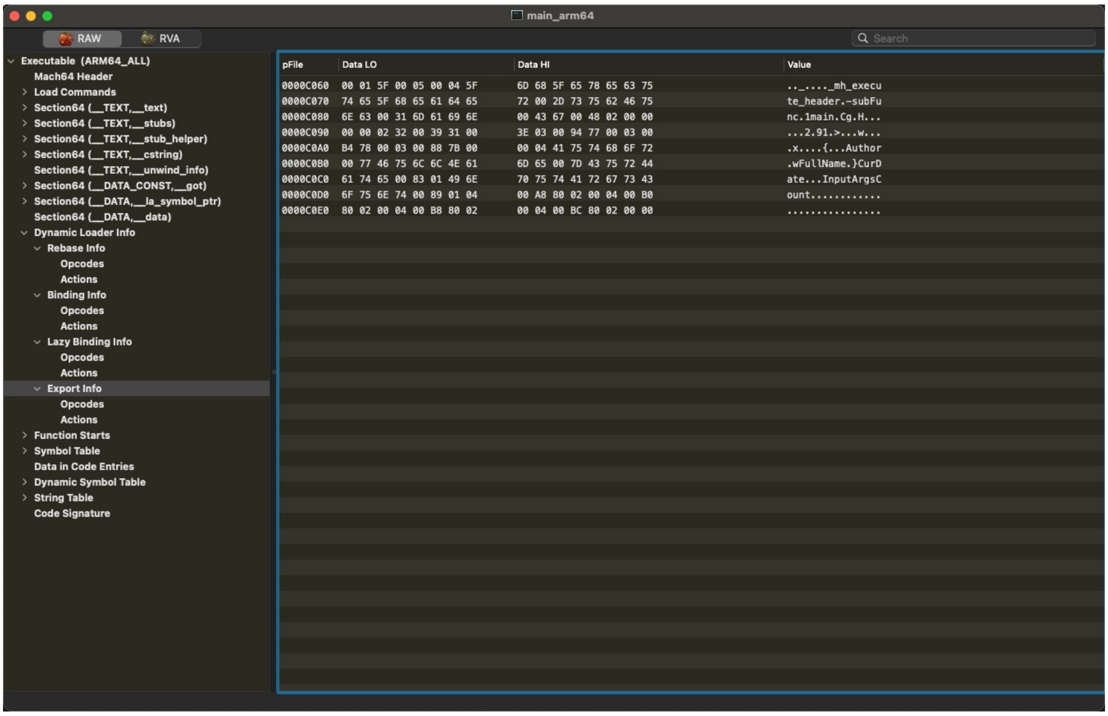
- 

    - Opcodes

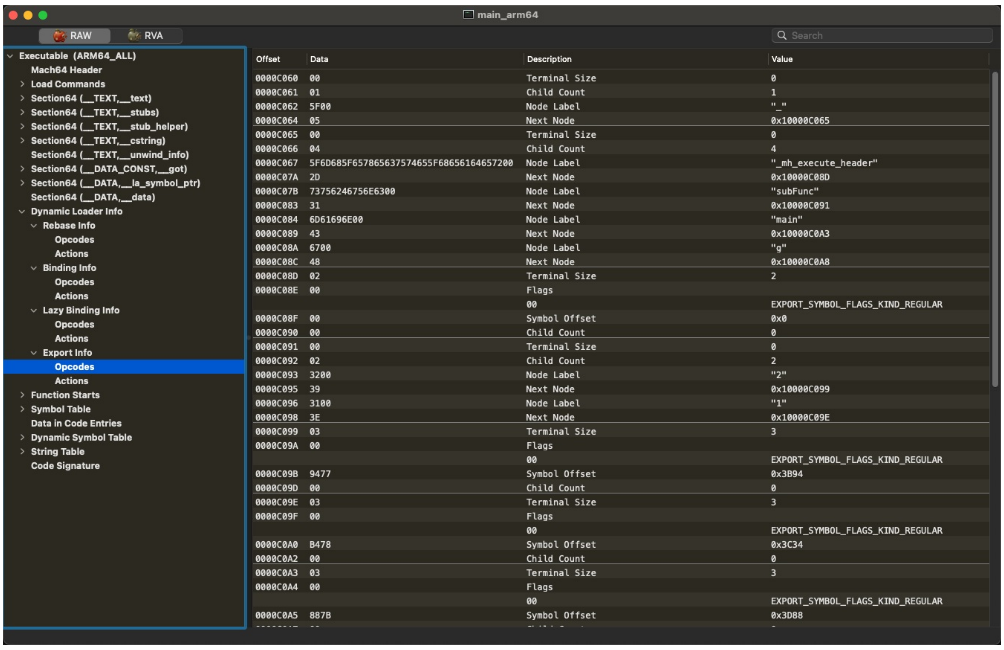
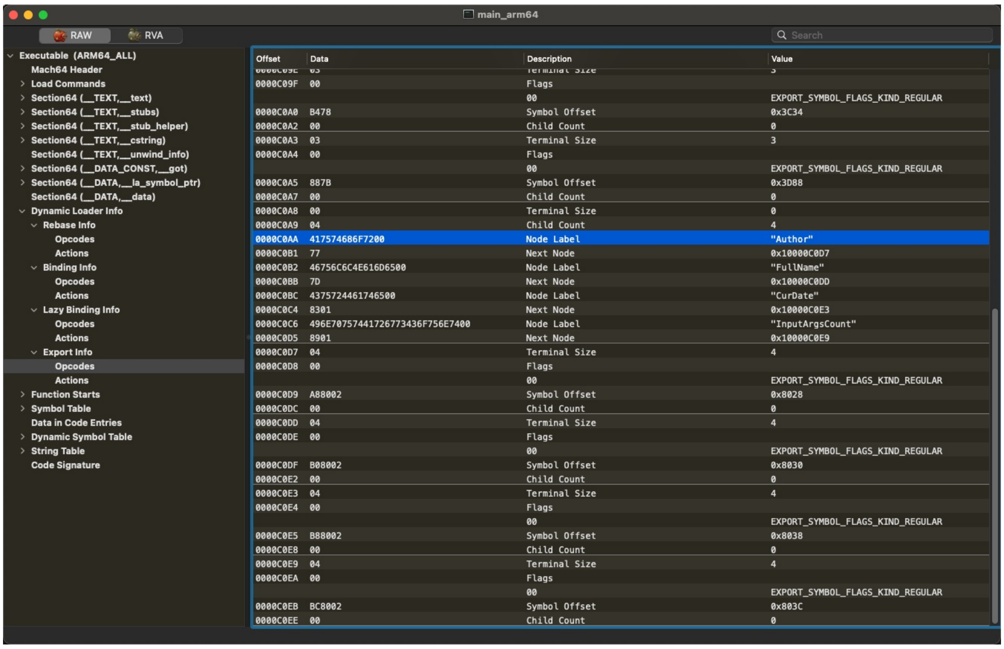
        - 

- Actions

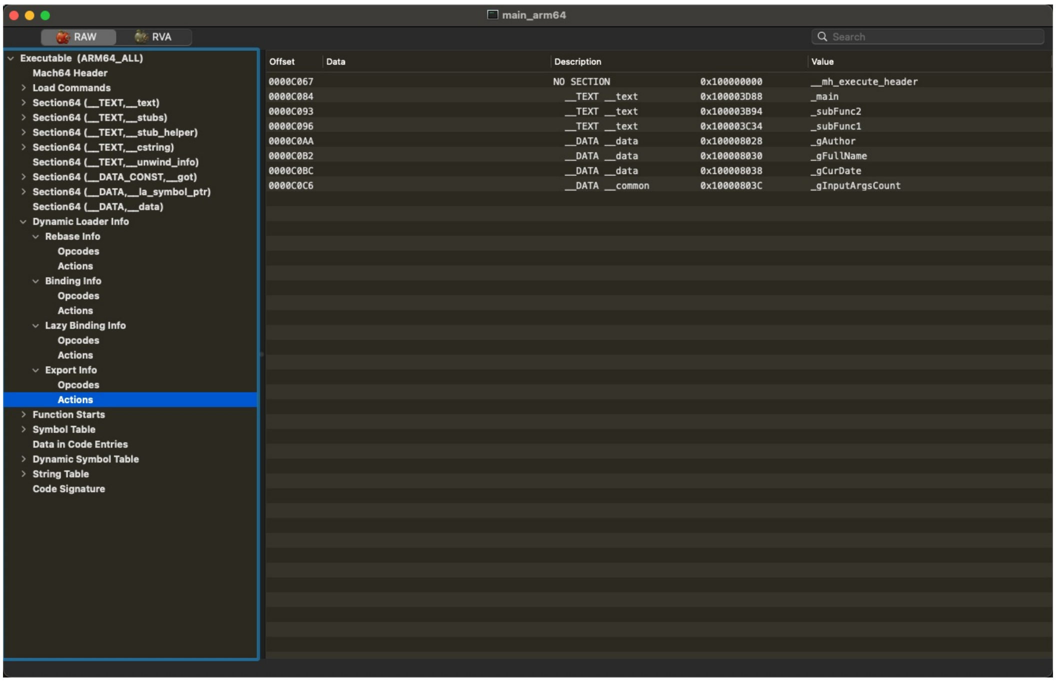
- 

- Export Info
  - 

  - Opcodes

- 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Rebase Info
Opcodes
Actions
Binding Info
Opcodes
Actions
Lazy Binding Info
Opcodes
Actions
Export Info
Opcodes
Actions
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
0000C060 00 Terminal Size 0
0000C061 01 Child Count 1
0000C062 5F00 Node Label "_"
0000C064 05 Next Node 0x10000C065
0000C065 00 Terminal Size 0
0000C066 04 Child Count 4
0000C067 5F6D685F657865637574655F68656164657200 Node Label "_mh_execute_header"
0000C07A 2D Next Node 0x10000C08D
0000C07B 73756246756E6300 Node Label "subFunc"
0000C083 31 Next Node 0x10000C091
0000C084 6D61696E00 Node Label "main"
0000C089 43 Next Node 0x10000C0A3
0000C08A 6700 Node Label "g"
0000C08C 48 Next Node 0x10000C0A8
0000C08D 02 Terminal Size 2
0000C08E 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C08F 00 Symbol Offset 0x0
0000C090 00 Child Count 0
0000C091 00 Terminal Size 0
0000C092 02 Child Count 2
0000C093 3200 Node Label "2"
0000C095 39 Next Node 0x10000C099
0000C096 3100 Node Label "1"
0000C098 3E Next Node 0x10000C09E
0000C099 03 Terminal Size 3
0000C09A 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C09B 9477 Symbol Offset 0x3B94
0000C09D 00 Child Count 0
0000C09E 03 Terminal Size 3
0000C09F 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0A0 B478 Symbol Offset 0x3C34
0000C0A2 00 Child Count 0
0000C0A3 03 Terminal Size 3
0000C0A4 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0A5 887B Symbol Offset 0x3D88
- 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Rebase Info
Opcodes
Actions
Binding Info
Opcodes
Actions
Lazy Binding Info
Opcodes
Actions
Export Info
Opcodes
Actions
Function Starts
Symbol Table
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
0000C09F 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0A0 B478 Symbol Offset 0x3C34
0000C0A2 00 Child Count 0
0000C0A3 03 Terminal Size 3
0000C0A4 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0A5 887B Symbol Offset 0x3D88
0000C0A7 00 Child Count 0
0000C0A8 00 Terminal Size 0
0000C0A9 04 Child Count 4
0000C0AA 417574686F7200 Node Label "Author"
0000C0B1 77 Next Node 0x10000C0D7
0000C0B2 46756C6C4E616D6500 Node Label "FullName"
0000C0BB 7D Next Node 0x10000C0DD
0000C0BC 437572446174650 0 Node Label "CurDate"
0000C0C4 8301 Next Node 0x10000C0E3
0000C0C6 496E707574417267734 36F756E7400 Node Label "InputArgsCount"
0000C0D5 8901 Next Node 0x10000C0E9
0000C0D7 04 Terminal Size 4
0000C0D8 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0D9 A88002 Symbol Offset 0x8028
0000C0DC 00 Child Count 0
0000C0DD 04 Terminal Size 4
0000C0DE 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0DF B08002 Symbol Offset 0x8030
0000C0E2 00 Child Count 0
0000C0E3 04 Terminal Size 4
0000C0E4 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0E5 B88002 Symbol Offset 0x8038
0000C0E8 00 Child Count 0
0000C0E9 04 Terminal Size 4
0000C0EA 00 Flags
00 EXPORT_SYMBOL_FLAGS_KIND_REGULAR
0000C0EB BC8002 Symbol Offset 0x803C
0000C0EE 00 Child Count 0

- Actions

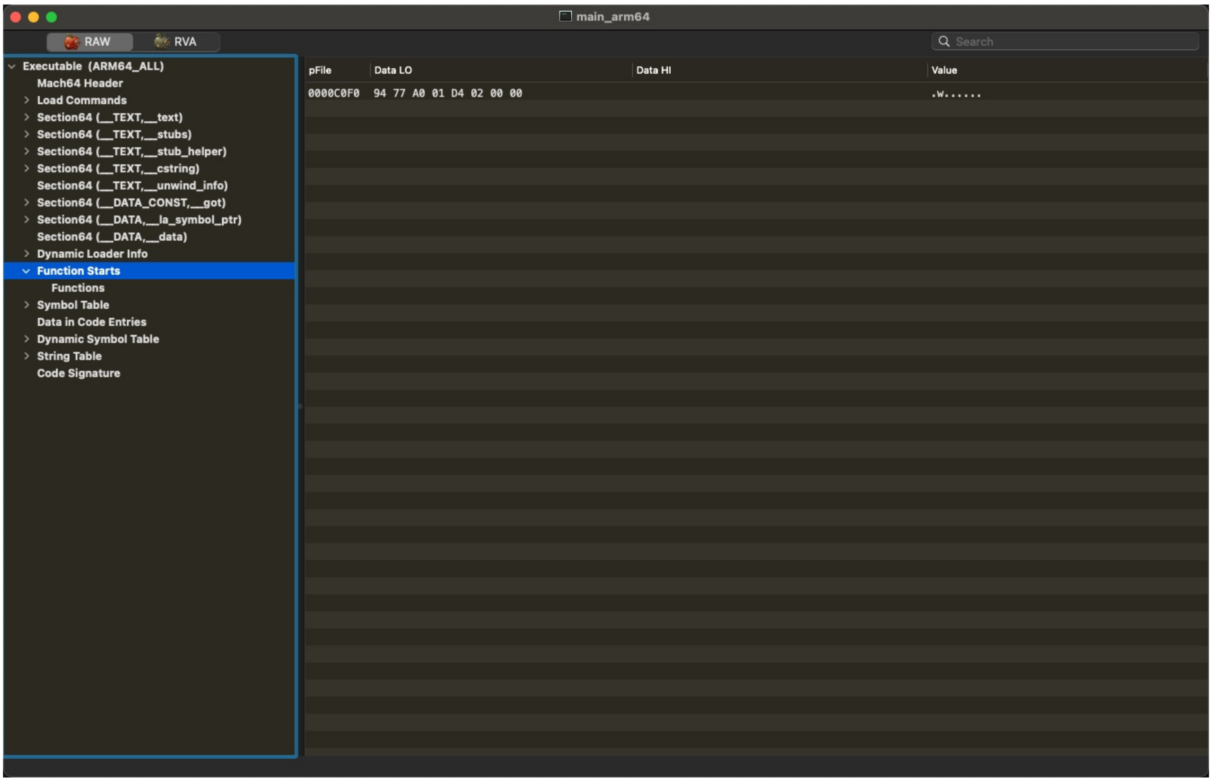
- 

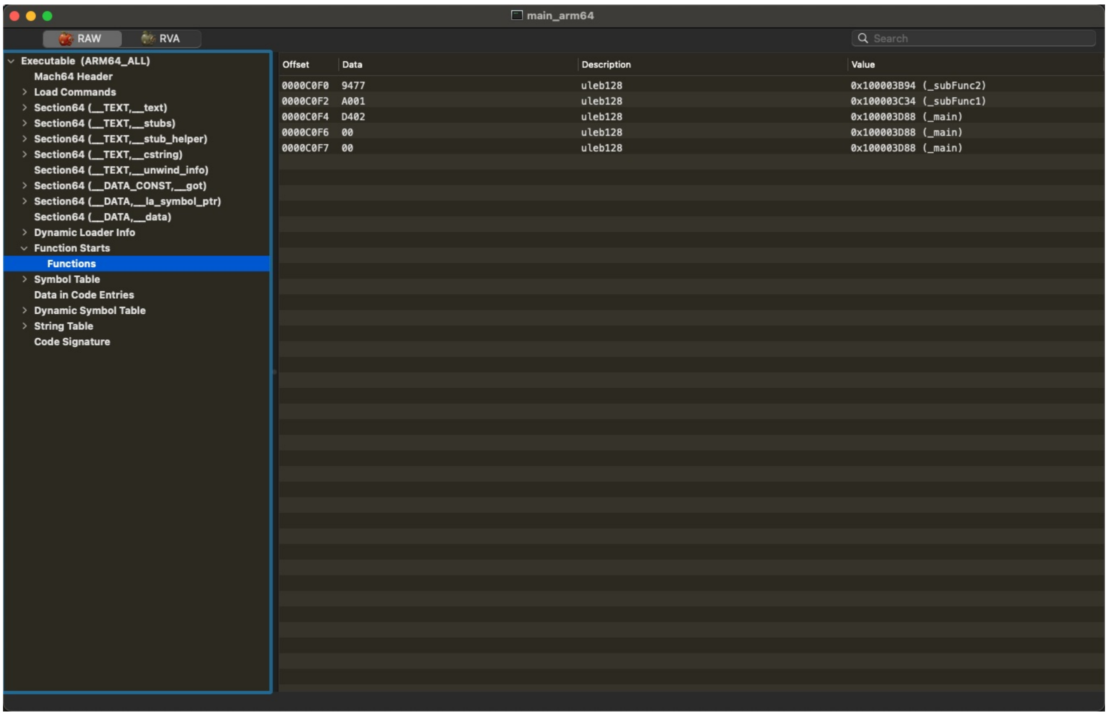
对应原先代码中的，全局变量：

```
// demo Data segment
const char* gAuthor = "crifan"; // demo const string, place where?
char* gFullName = "CrifanLi"; // demo non-const string, place where?
int gInputArgsCount; // demo uninitialized data
int gCurDate = 20230419;  // demo initialized data
```

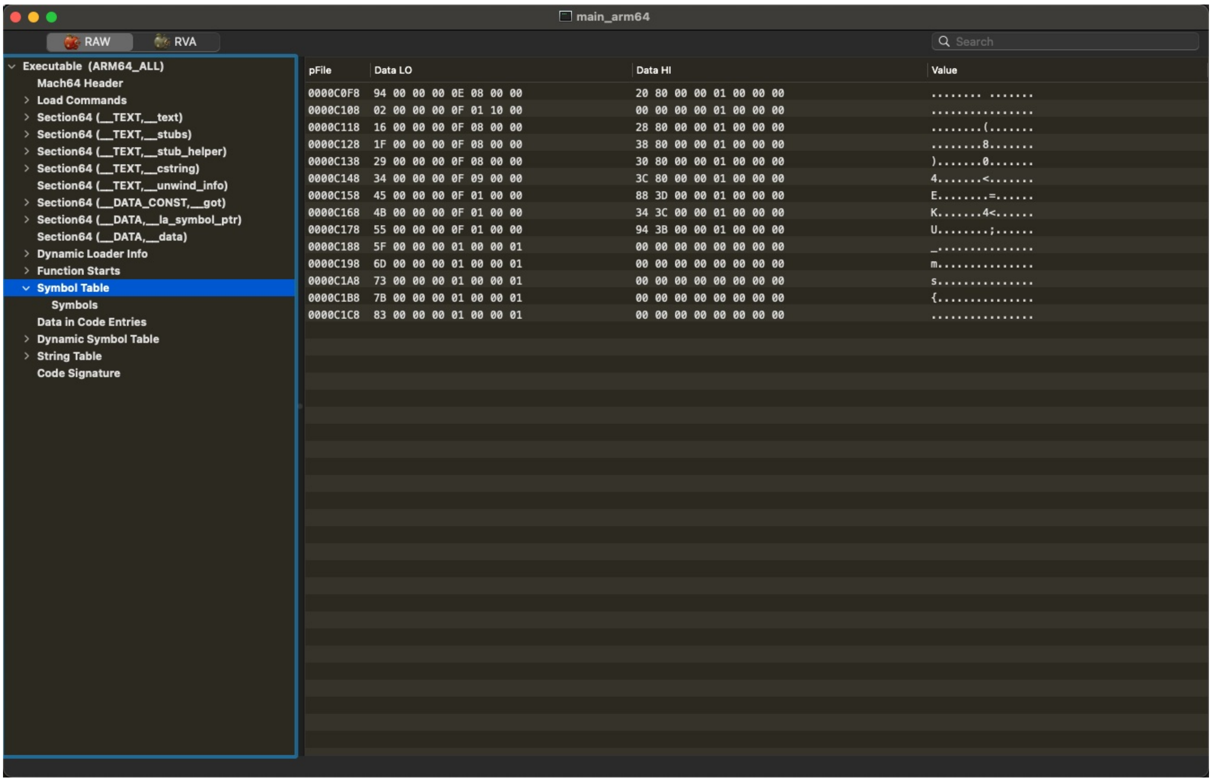
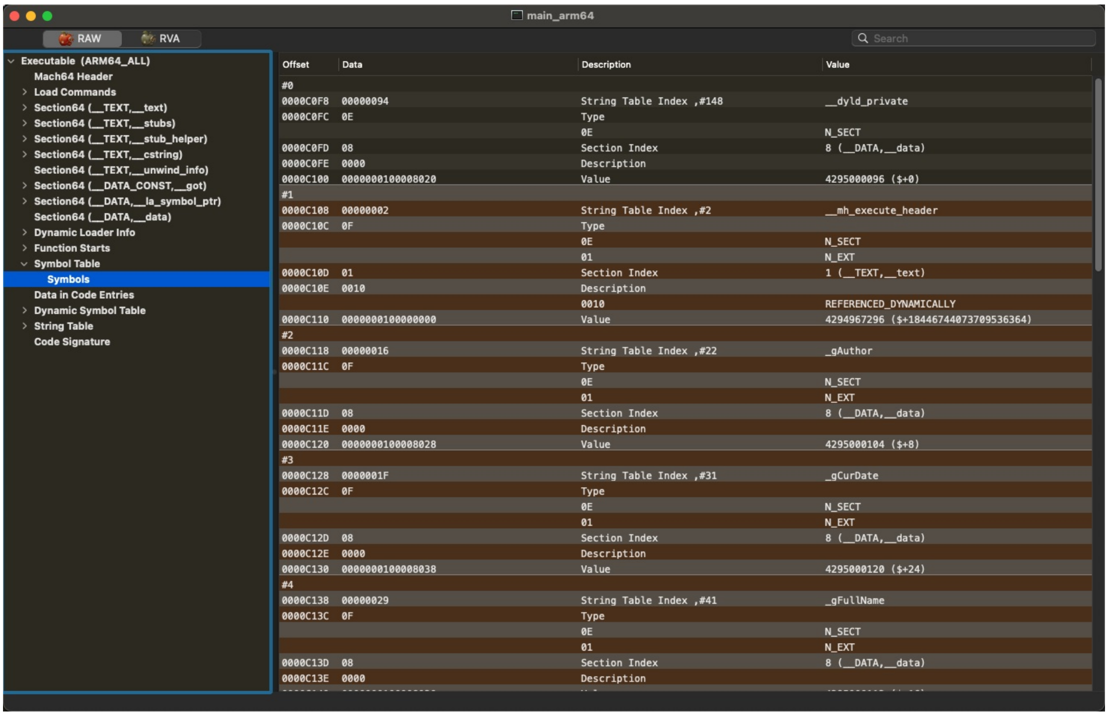
好像还额外去导出了这些全局变量？

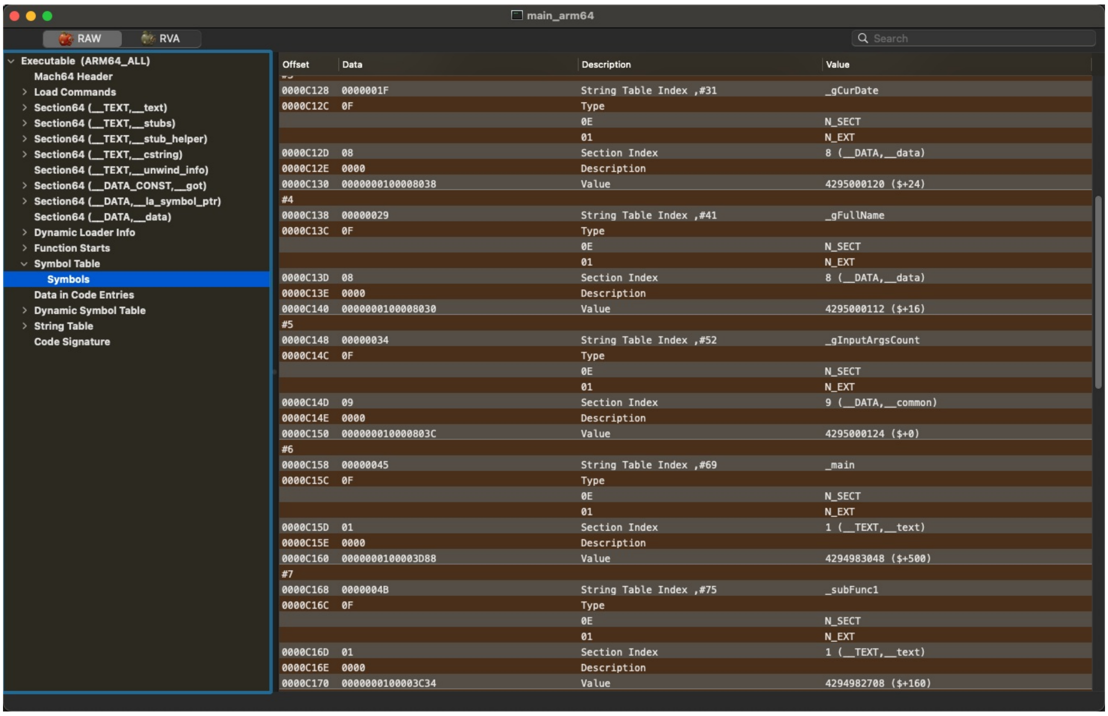
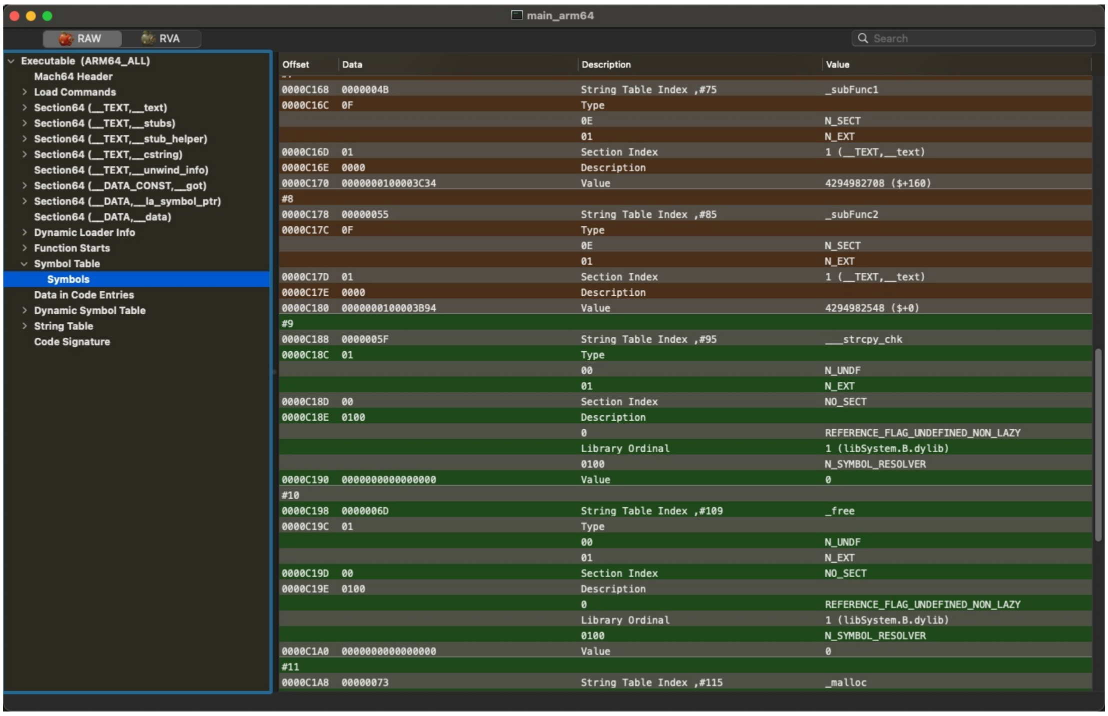
Function Starts

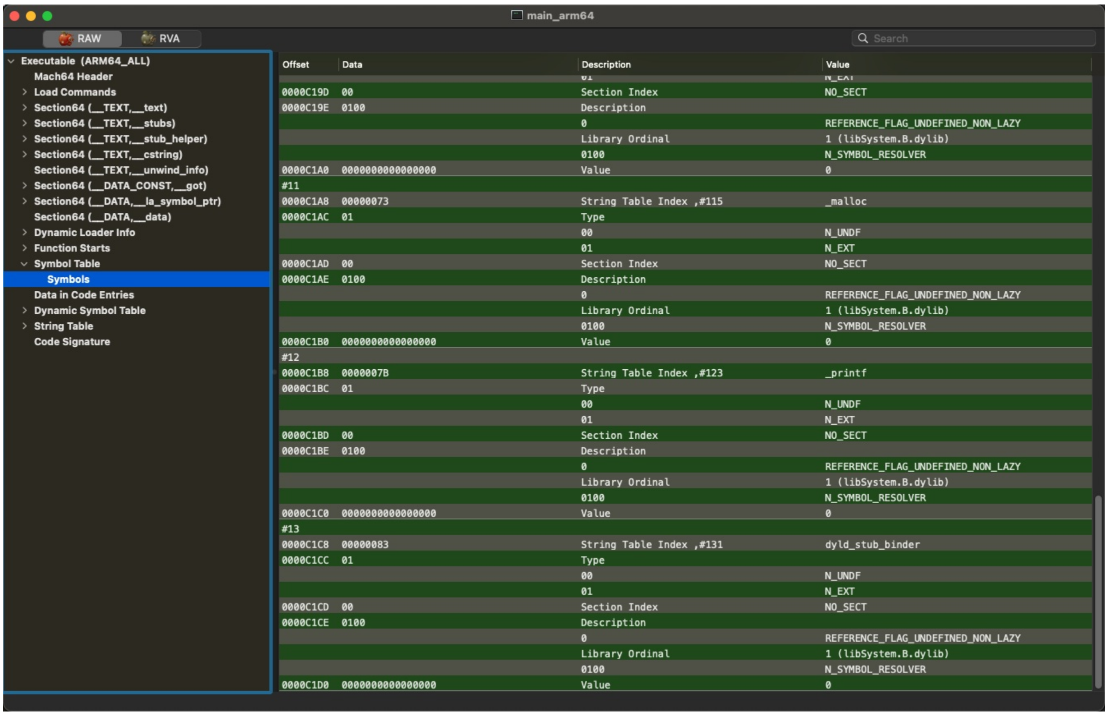
- 

    - Functions
        - 

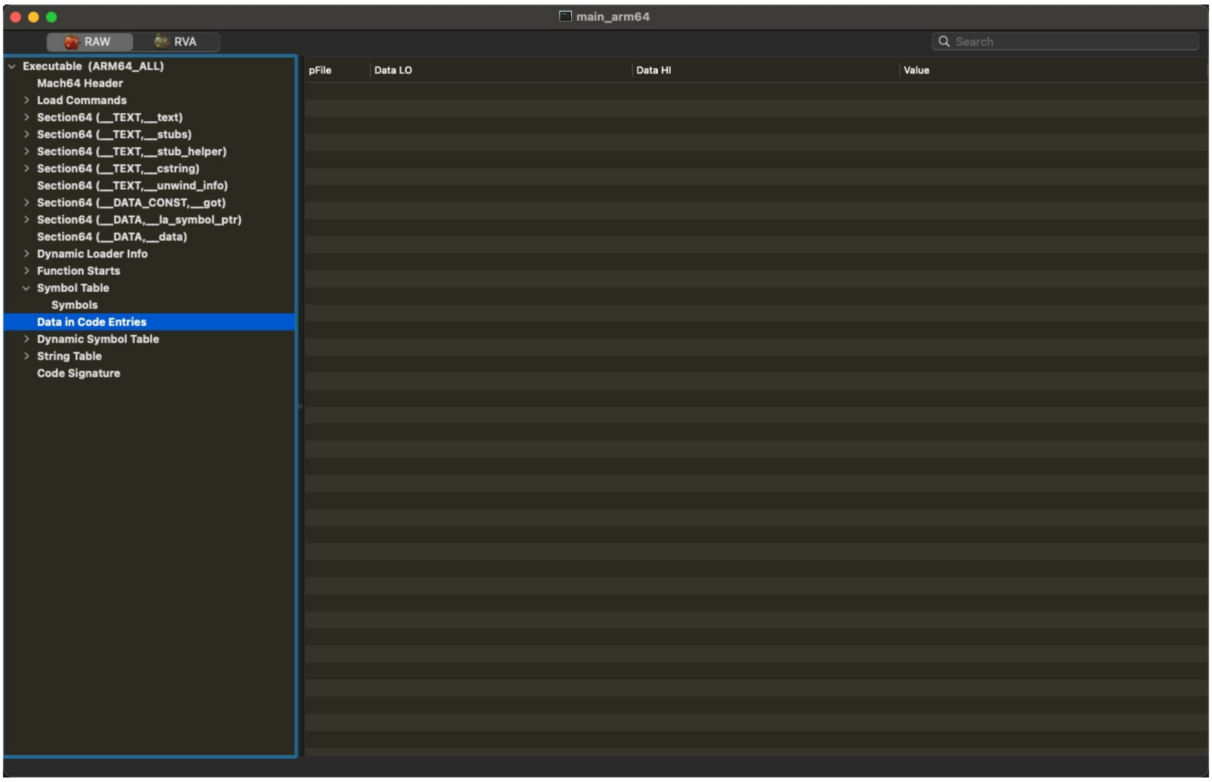
Symbol Table

- 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Symbols
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
pFile
Data LO
Data HI
Value
0000C0F8 94 00 00 00 0E 08 00 00 20 80 00 00 01 00 00 00
0000C108 02 00 00 00 0F 01 10 00 00 00 00 00 01 00 00 00
0000C118 16 00 00 00 0F 08 00 00 28 80 00 00 01 00 00 00
0000C128 1F 00 00 00 0F 08 00 00 38 80 00 00 01 00 00 00
0000C138 29 00 00 00 0F 08 00 00 30 80 00 00 01 00 00 00
0000C148 34 00 00 00 0F 09 00 00 3C 80 00 00 01 00 00 00
0000C158 45 00 00 00 0F 01 00 00 88 3D 00 00 01 00 00 00
0000C168 4B 00 00 00 0F 01 00 00 34 3C 00 00 01 00 00 00
0000C178 55 00 00 00 0F 01 00 00 94 3B 00 00 01 00 00 00
0000C188 5F 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00
0000C198 6D 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00
0000C1A8 73 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00
0000C1B8 7B 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00
0000C1C8 83 00 00 00 01 00 00 01 00 00 00 00 00 00 00 00
  - Symbols
    - 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Symbols
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset
Data
Description
Value
#0
0000C0F8 00000094 String Table Index ,#148 _dyld_private
0000C0FC 0E Type
0E N_SECT
0000C0FD 08 Section Index 8 (__DATA,__data)
0000C0FE 0000 Description
0000C100 0000000100008020 Value 4295000096 ($+0)
#1
0000C108 00000002 String Table Index ,#2 __mh_execute_header
0000C10C 0F Type
0E N_SECT
01 N_EXT
0000C10D 01 Section Index 1 (__TEXT,__text)
0000C10E 0010 Description
0010 REFERENCED_DYNAMICALLY
0000C110 0000000100000000 Value 4294967296 ($+18446744073709536364)
#2
0000C118 00000016 String Table Index ,#22 _gAuthor
0000C11C 0F Type
0E N_SECT
01 N_EXT
0000C11D 08 Section Index 8 (__DATA,__data)
0000C11E 0000 Description
0000C120 0000000100008028 Value 4295000104 ($+8)
#3
0000C128 0000001F String Table Index ,#31 _gCurDate
0000C12C 0F Type
0E N_SECT
01 N_EXT
0000C12D 08 Section Index 8 (__DATA,__data)
0000C12E 0000 Description
0000C130 0000000100008038 Value 4295000120 ($+24)
#4
0000C138 00000029 String Table Index ,#41 _gFullName
0000C13C 0F Type
0E N_SECT
01 N_EXT
0000C13D 08 Section Index 8 (__DATA,__data)
0000C13E 0000 Description

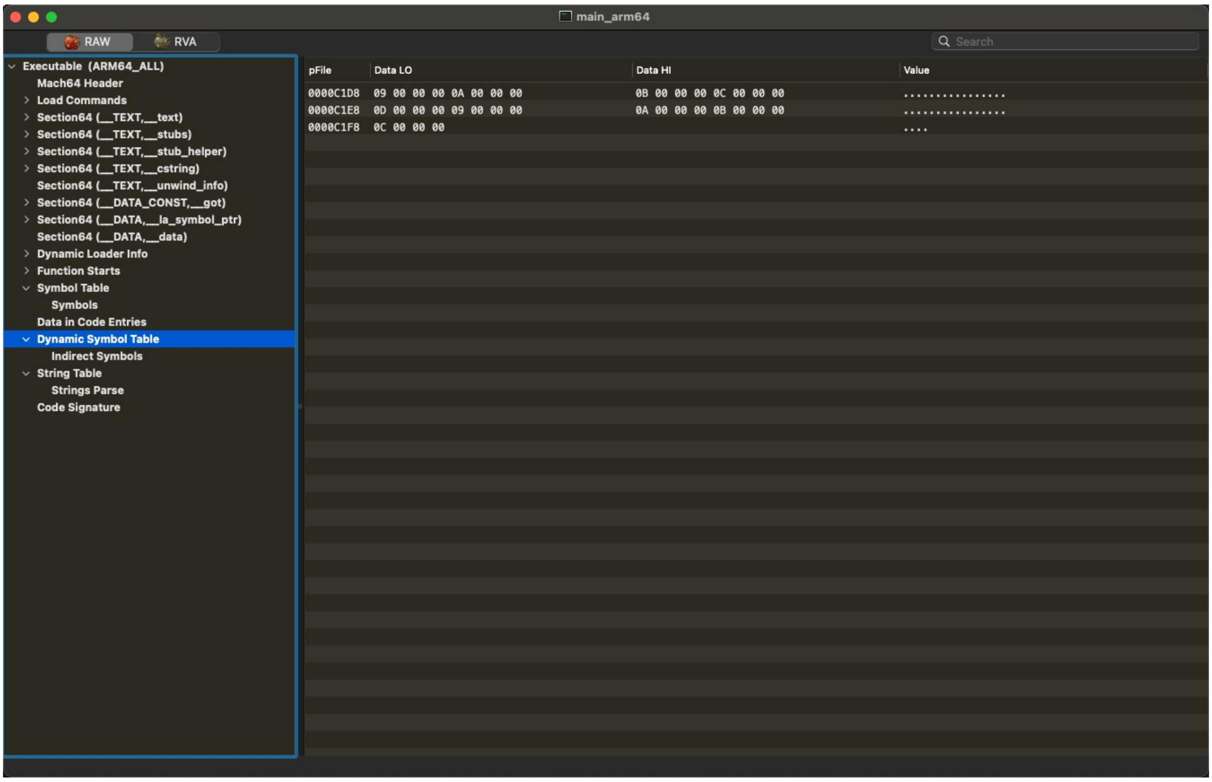
- 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Symbols
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
0000C128 0000001F String Table Index ,#31 _gCurDate
0000C12C 0F Type
0E N_SECT
01 N_EXT
0000C12D 08 Section Index 8 (__DATA,__data)
0000C12E 0000 Description
0000C130 0000000100008038 Value 4295000120 ($+24)
#4
0000C138 00000029 String Table Index ,#41 _gFullName
0000C13C 0F Type
0E N_SECT
01 N_EXT
0000C13D 08 Section Index 8 (__DATA,__data)
0000C13E 0000 Description
0000C140 0000000100008030 Value 4295000112 ($+16)
#5
0000C148 00000034 String Table Index ,#52 _gInputArgsCount
0000C14C 0F Type
0E N_SECT
01 N_EXT
0000C14D 09 Section Index 9 (__DATA,__common)
0000C14E 0000 Description
0000C150 000000010000803C Value 4295000124 ($+0)
#6
0000C158 00000045 String Table Index ,#69 _main
0000C15C 0F Type
0E N_SECT
01 N_EXT
0000C15D 01 Section Index 1 (__TEXT,__text)
0000C15E 0000 Description
0000C160 0000000100003D88 Value 4294983048 ($+500)
#7
0000C168 0000004B String Table Index ,#75 _subFunc1
0000C16C 0F Type
0E N_SECT
01 N_EXT
0000C16D 01 Section Index 1 (__TEXT,__text)
0000C16E 0000 Description
0000C170 0000000100003C34 Value 4294982708 ($+160)
- 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Symbols
Data in Code Entries
Dynamic Symbol Table
String Table
Code Signature
Offset Data Description Value
0000C168 0000004B String Table Index ,#75 _subFunc1
0000C16C 0F Type
0E N_SECT
01 N_EXT
0000C16D 01 Section Index 1 (__TEXT,__text)
0000C16E 0000 Description
0000C170 0000000100003C34 Value 4294982708 ($+160)
#8
0000C178 00000055 String Table Index ,#85 _subFunc2
0000C17C 0F Type
0E N_SECT
01 N_EXT
0000C17D 01 Section Index 1 (__TEXT,__text)
0000C17E 0000 Description
0000C180 0000000100003B94 Value 4294982548 ($+0)
#9
0000C188 0000005F String Table Index ,#95 ___strcpy_chk
0000C18C 01 Type
00 N_UNDF
01 N_EXT
0000C18D 00 Section Index NO_SECT
0000C18E 0100 Description
0 REFERENCE_FLAG_UNDEFINED_NON_LAZY
Library Ordinal 1 (libSystem.B.dylib)
0100 N_SYMBOL_RESOLVER
0000C190 0000000000000000 Value 0
#10
0000C198 0000006D String Table Index ,#109 _free
0000C19C 01 Type
00 N_UNDF
01 N_EXT
0000C19D 00 Section Index NO_SECT
0000C19E 0100 Description
0 REFERENCE_FLAG_UNDEFINED_NON_LAZY
Library Ordinal 1 (libSystem.B.dylib)
0100 N_SYMBOL_RESOLVER
0000C1A0 0000000000000000 Value 0
#11
0000C1A8 00000073 String Table Index ,#115 _malloc

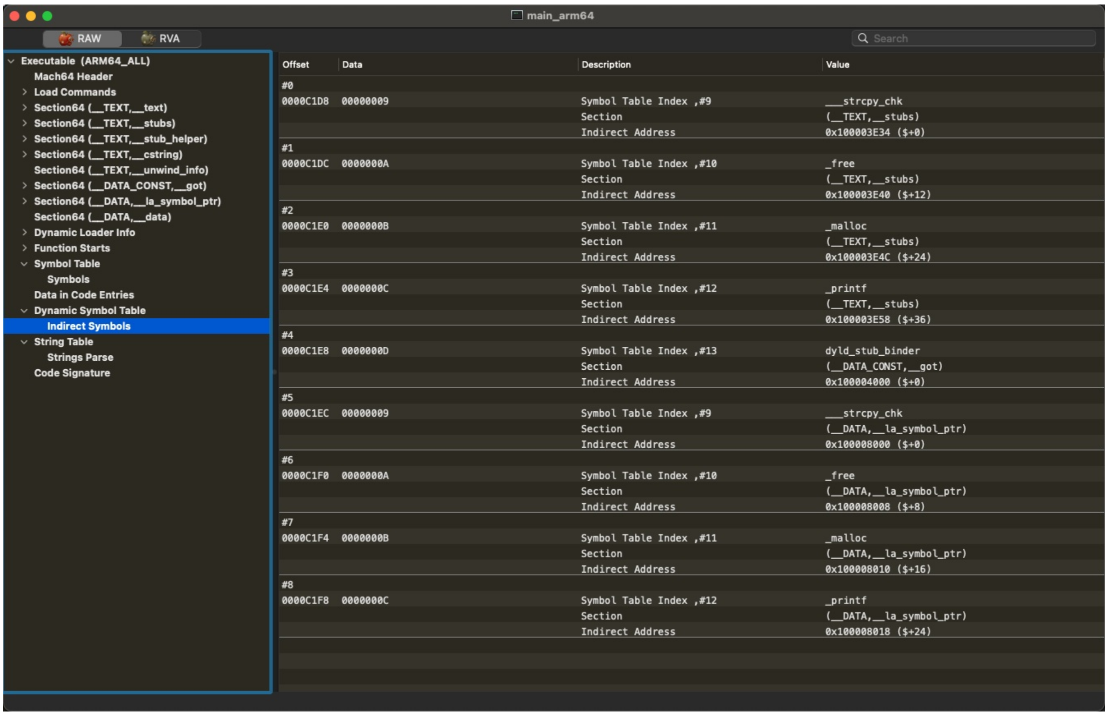
- 

Data in Code Entries

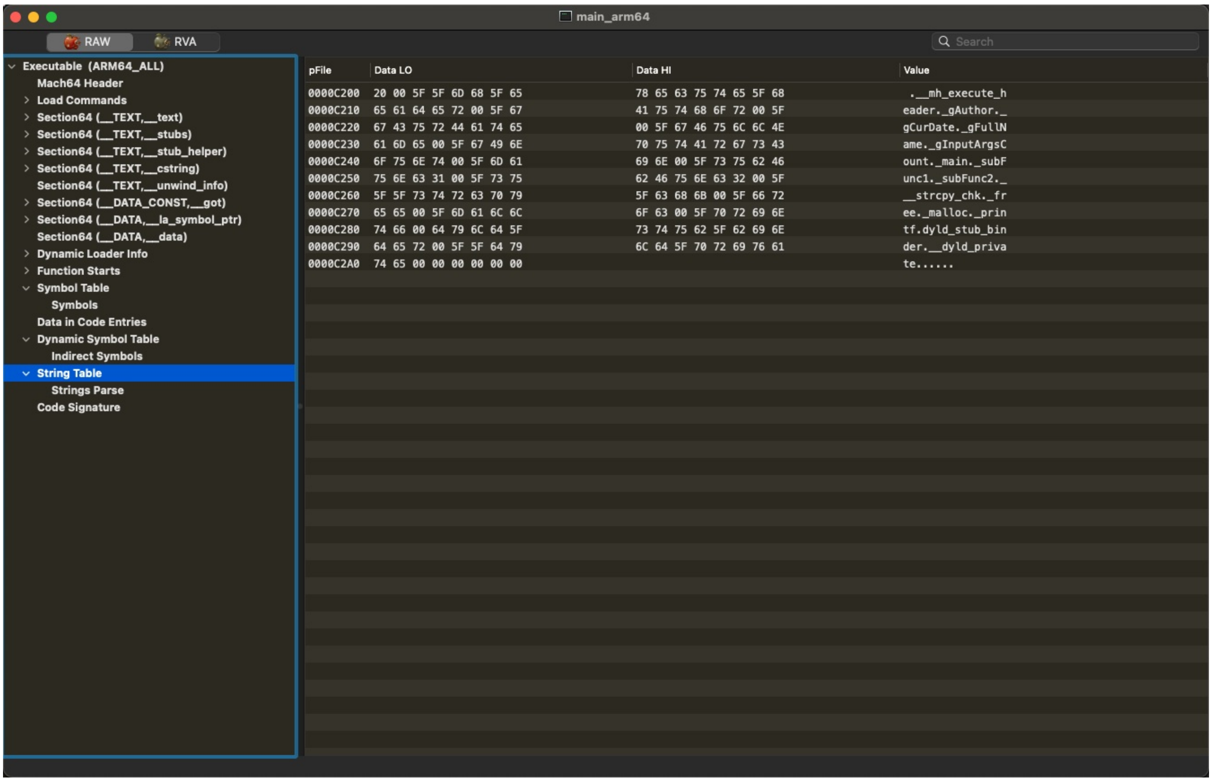
- 

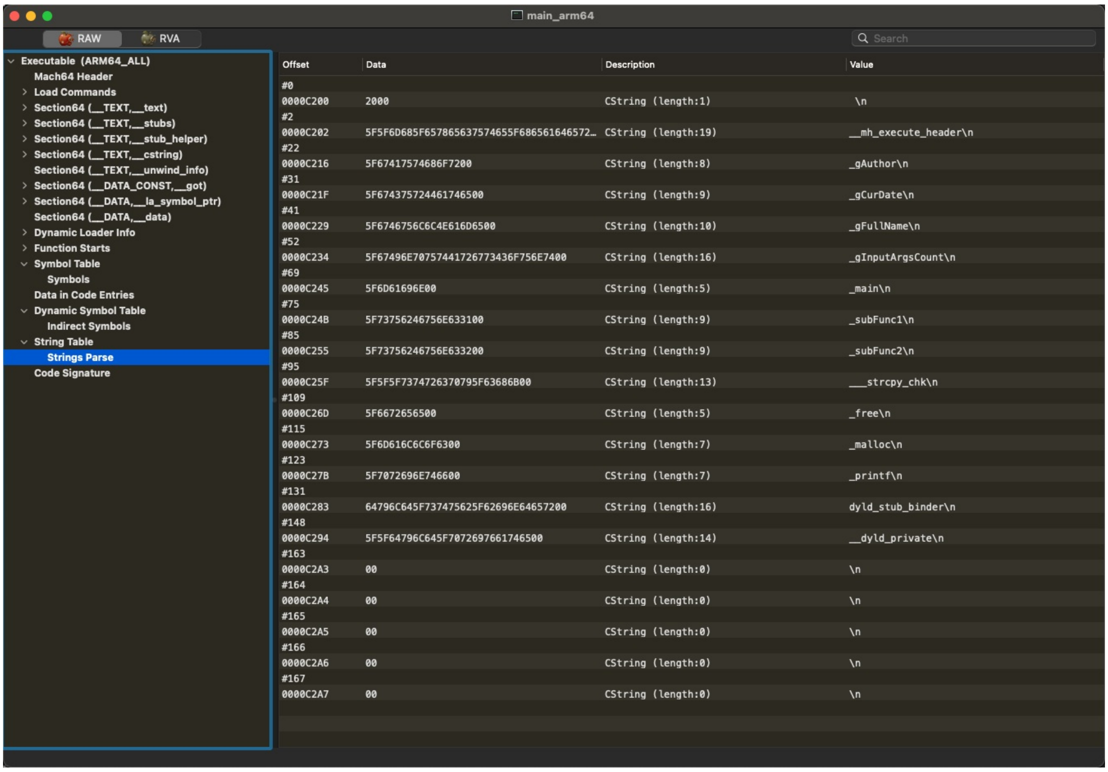
Dynamic Symbol Table

- 

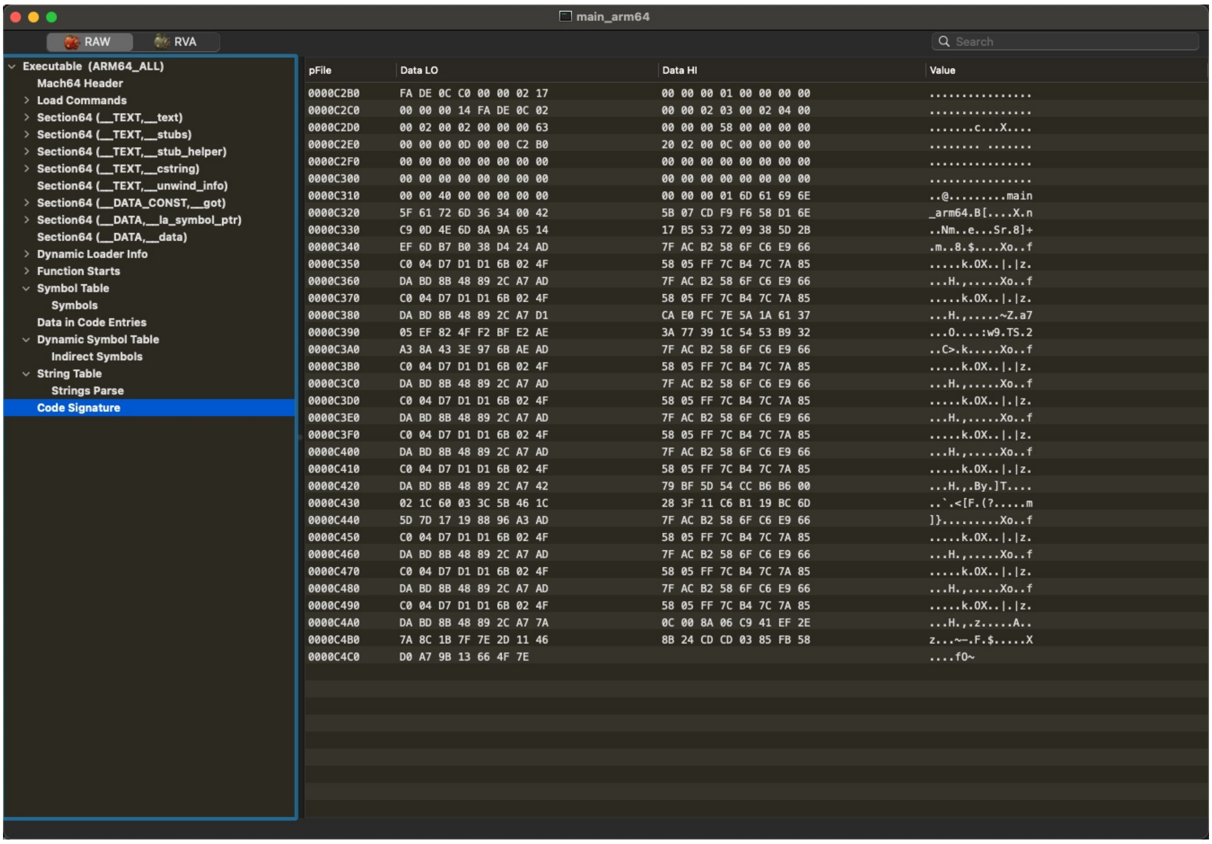
    - Indirect Symbols
        - 

String Table

- 

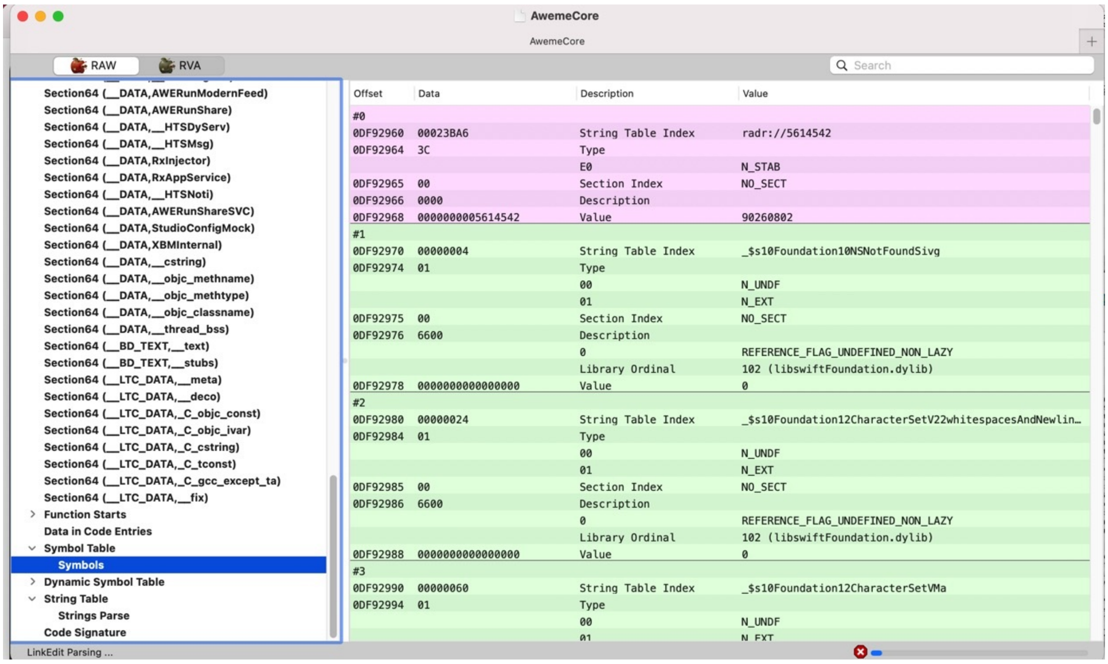
  - Strings Parse
    - 

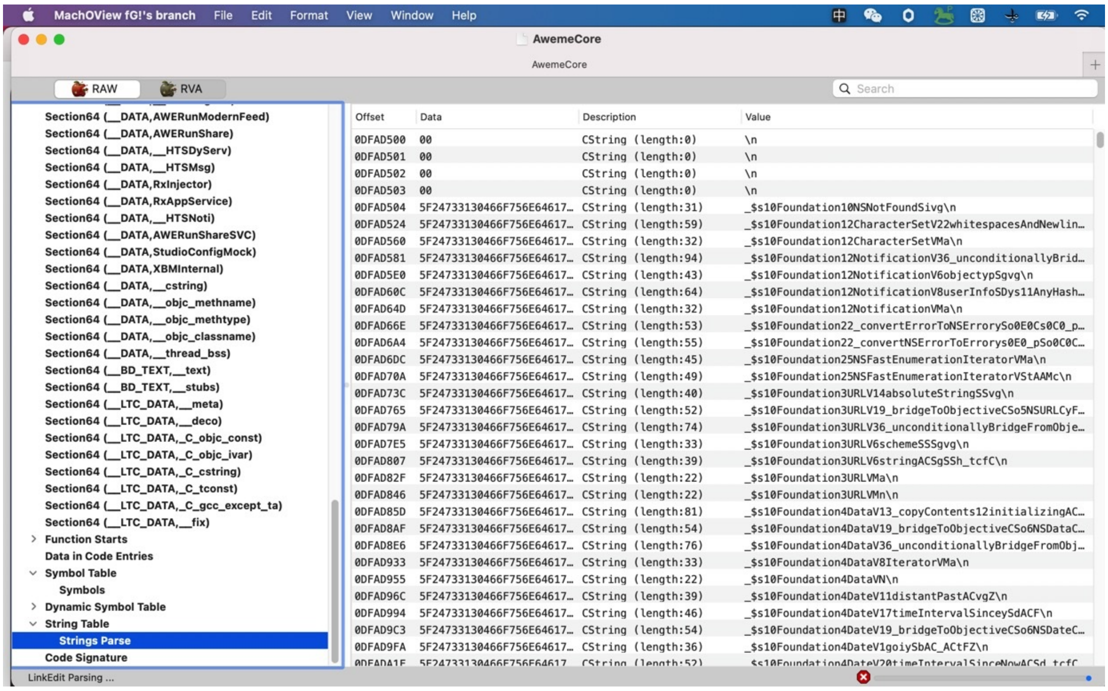
Code Signature

- 
main_arm64
RAW
RVA
Search
Executable (ARM64_ALL)
Mach64 Header
Load Commands
Section64 (__TEXT,__text)
Section64 (__TEXT,__stubs)
Section64 (__TEXT,__stub_helper)
Section64 (__TEXT,__cstring)
Section64 (__TEXT,__unwind_info)
Section64 (__DATA_CONST,__got)
Section64 (__DATA,__la_symbol_ptr)
Section64 (__DATA,__data)
Dynamic Loader Info
Function Starts
Symbol Table
Symbols
Data in Code Entries
Dynamic Symbol Table
Indirect Symbols
String Table
Strings Parse
Code Signature
pFile
Data LO
Data HI
Value
0000C2B0 FA DE 0C C0 00 00 02 17 00 00 00 01 00 00 00 00
0000C2C0 00 00 00 14 FA DE 0C 02 00 00 02 03 00 02 04 00
0000C2D0 00 02 00 02 00 00 00 63 00 00 00 58 00 00 00 00
0000C2E0 00 00 00 0D 00 00 C2 B0 20 02 00 0C 00 00 00 00
0000C2F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000C300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000C310 00 00 40 00 00 00 00 00 00 00 00 01 6D 61 69 6E ..@.........main
0000C320 5F 61 72 6D 36 34 00 42 5B 07 CD F9 F6 58 D1 6E _arm64.B[....X.n
0000C330 C9 0D 4E 6D 8A 9A 65 14 17 B5 53 72 09 38 5D 2B ..Nm..e...Sr.8]+
0000C340 EF 6D B7 B0 38 D4 24 AD 7F AC B2 58 6F C6 E9 66 .m..8.$....Xo..f
0000C350 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C360 DA BD 8B 48 89 2C A7 AD 7F AC B2 58 6F C6 E9 66 ...H.,.....Xo..f
0000C370 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C380 DA BD 8B 48 89 2C A7 D1 CA E0 FC 7E 5A 1A 61 37 ...H.,.....~Z.a7
0000C390 05 EF 82 4F F2 BF E2 AE 3A 77 39 1C 54 53 B9 32 ...O....:w9.TS.2
0000C3A0 A3 8A 43 3E 97 6B AE AD 7F AC B2 58 6F C6 E9 66 ..C>.k.....Xo..f
0000C3B0 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C3C0 DA BD 8B 48 89 2C A7 AD 7F AC B2 58 6F C6 E9 66 ...H.,.....Xo..f
0000C3D0 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C3E0 DA BD 8B 48 89 2C A7 AD 7F AC B2 58 6F C6 E9 66 ...H.,.....Xo..f
0000C3F0 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C400 DA BD 8B 48 89 2C A7 AD 7F AC B2 58 6F C6 E9 66 ...H.,.....Xo..f
0000C410 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C420 DA BD 8B 48 89 2C A7 42 79 BF 5D 54 CC B6 B6 00 ...H.,.By.]T....
0000C430 02 1C 60 03 3C 5B 46 1C 28 3F 11 C6 B1 19 BC 6D ..`.<[F.(?.....m
0000C440 5D 7D 17 19 88 96 A3 AD 7F AC B2 58 6F C6 E9 66]}.........Xo..f
0000C450 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C460 DA BD 8B 48 89 2C A7 AD 7F AC B2 58 6F C6 E9 66 ...H.,.....Xo..f
0000C470 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C480 DA BD 8B 48 89 2C A7 AD 7F AC B2 58 6F C6 E9 66 ...H.,.....Xo..f
0000C490 C0 04 D7 D1 D1 6B 02 4F 58 05 FF 7C B4 7C 7A 85 .....k.OX..|.|z.
0000C4A0 DA BD 8B 48 89 2C A7 7A 0C 00 8A 06 C9 41 EF 2E ...H.,.z.....A..
0000C4B0 7A 8C 1B 7F 7E 2D 11 46 8B 24 CD CD 03 85 FB 58 z...~-.F.$.....X
0000C4C0 D0 A7 9B 13 66 4F 7E ....fO~

MachOView用法举例：AwemeCore

- Mach64 Header
    -
- Symbol Table
    -
    - Symbols

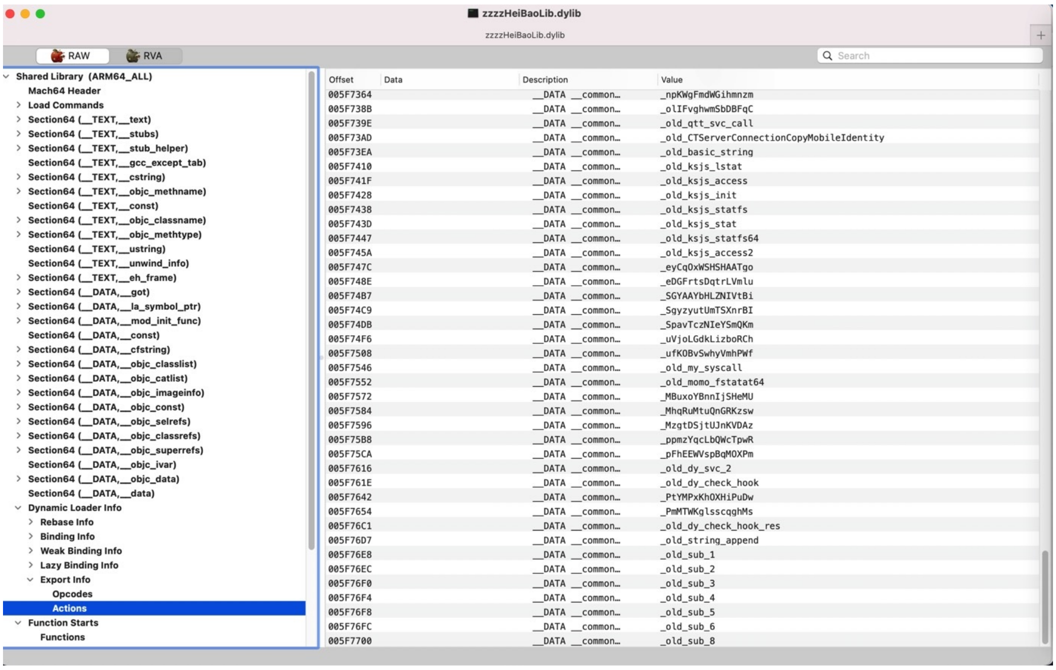
- 

- String Table
  - Strings Parse
    - 

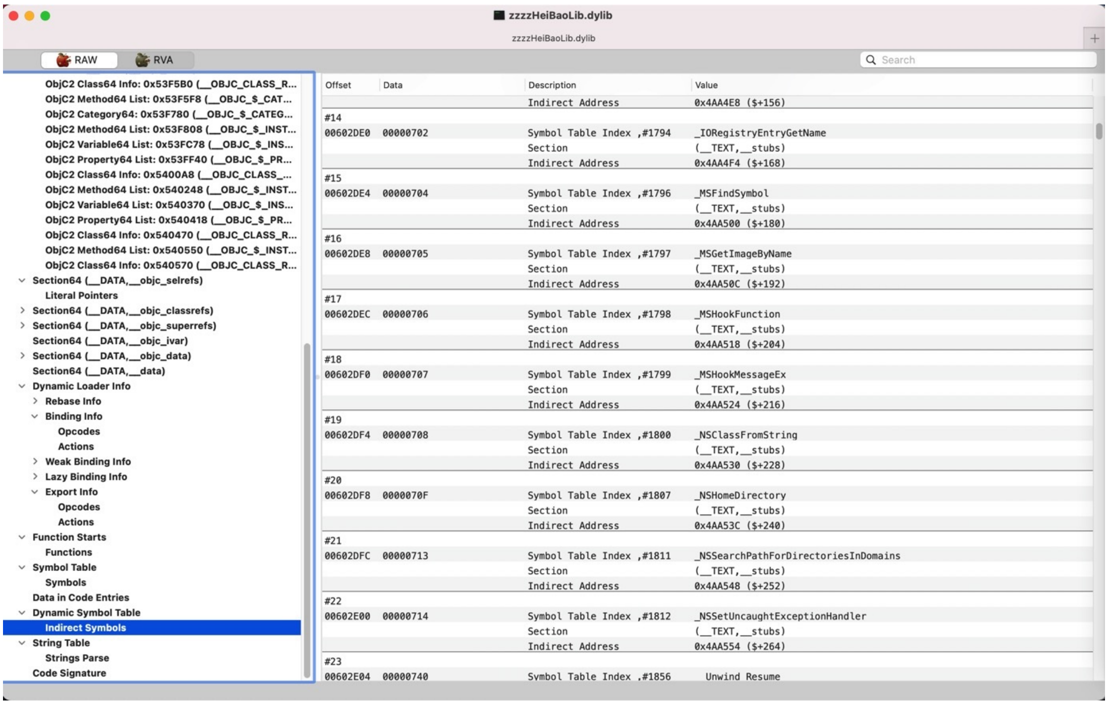
MachOView用法举例：zzzzHeiBaoLib.dylib

- 正在分析
    -
- `__DATA,__mode_init_func`
    -
- `__TEXT,__stubs`

- `__TEXT,__objc_methname`
- Dynamic Loader Info
  - Export Info
    - Actions



- Dynamic Symbol Table
  - Indirect Symbols



MachOView使用心得

一些心得：

- 如果二进制太大，或者本身防护做的比较好，则：MachOView完全加载出来二进制信息
    - 往往耗时很久
    - 也往往会直接崩溃，无法继续使用
        - 比如抖音的二进制加载到最后，就被崩溃。
            - 只能在崩溃之前，及时查看（大）部分已解析出的信息

自己编译

- 需求：想要自己编译gdbinit的MachOView
- 步骤

下载代码：

```
git clone https://github.com/gdbinit/MachOView.git
```

双击 `machoview.xcodeproj` 用XCode打开

即可自己编译

常见报错

unable to find sdk ‘macosx10.9'

- 解决办法
  - `TARGETS` -> `Build Settings` -> `Architecture` -> `Base SDK` ，从 `macosx 10.9(SDK not found)` 改为： `macOS`

MachOView/FatLayout.mm:9:10: 'string' file not found

- 解决办法
  - `TARGETS` -> `Build Settings` -> `Deployment` -> `macOS Deployment Target` ，从 `macOS10.7` 改为和你当前macOS版本一致或最接近的版本
    - 此处系统是 `macOS 11.6` ，但此处选项 `macOS 11.6` ，所以选了最接近的 `macOS 11.5`

rabin2

下载和安装

从官网radare，找到下载地址来源，比如

Releases · radareorg/radare2

下载对应的版本，比如我此处的：

- Mac
  - Intel Chip
    - radare2-x64-5.7.8.pkg

然后去安装pkg包，安装后，即可有 `/usr/local/bin/rabin2`

之前某次安装后的版本：

```
➜ ~ rabin2 --version
rabin2: illegal option -- -
rabin2 4.3.1 134 @ darwin-x86-64 git.4.3.1
commit: 815529f204bede6a232fce8b3ac88a905c6943c6 build: 2020-03-06__16:31:10
```

资料

- `Radare2` 官网资料
  - Introduction - The Official Radare2 Book
    - Rabin2 - The Official Radare2 Book

rabin2用法

- `-I` : File **I**dentification

  ```
  rabin2 -I binaryFile
  ```

- `-e` : **E**ntrypoint

  ```
  rabin2 -e binaryFile
  ```

- `-i` : **I**mports

  ```
  rabin2 -i binaryFile
  ```

- `-E` : **E**xports

  ```
  rabin2 -E binaryFile
  ```

- `-s` : **S**ymbols

  ```
  rabin2 -s binaryFile
  ```

- `-l` : **L**ibraries

  ```
  rabin2 -l binaryFile
  ```

- `-z` : Strings

  ```
  rabin2 -z binaryFile
  ```

- `S` : Program **S**ections

  ```
  rabin2 -S binaryFile
  ```

心得

很多的参数，都可以加上r，表示（输出内容是一致的，但是格式不同）以radare格式输出

举例：

```
rabin2 -I
rabin2 -Ir

rabin2 -s
rabin2 -sr

rabin2 -z
rabin2 -zr
```

```
rabin2 -S
rabin2 -Sr
```

rabin2用法举例

rabin2用法举例：AwemeCore

用rabin2查看抖音AwemeCore二进制的信息：

概述：

```
(1) File Identification
rabin2 -I AwemeCore

(2) Entrypoint
rabin2 -e AwemeCore

(3) Imports
rabin2 -i AwemeCore

(4) Exports
rabin2 -E AwemeCore > AwemeCore_rabin2_E.txt

(5) Symbols
rabin2 -s AwemeCore > AwemeCore_rabin2_s.txt
rabin2 -sr AwemeCore > AwemeCore_rabin2_sr.txt

(6) Libraries
rabin2 -l AwemeCore > AwemeCore_rabin2_l.txt

(7) Strings
rabin2 -z AwemeCore > AwemeCore_rabin2_z.txt
rabin2 -zr AwemeCore > AwemeCore_rabin2_zr.txt

(8) Program Sections
rabin2 -S AwemeCore > AwemeCore_rabin2_S_section.txt
rabin2 -Sr AwemeCore > AwemeCore_rabin2_Sr_section.txt
```

详解：

`-I` : File Identification

```
➜  AwemeCore rabin2 -I ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore
arch     arm
baddr    0x0
binsz    240666608
bintype  mach0
bits     64
canary   true
class    MACH064
crypto   false
endian   little
havecode true
laddr    0x0
lang     swift
```

```
linenum  false
lsyms    false
machine  all
maxopsz  16
minopsz  1
nx       false
os       ios
pcalign  0
pic      false
relocs   false
sanitiz  false
static   false
stripped true
subsys   darwin
va       true
```

`-Ir`

```
➜  AwemeCore rabin2 -Ir ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCor
e.framework/AwemeCore
e cfg.bigendian=false
e asm.bits=64
e asm.dwarf=true
e bin.lang=swift
e file.type=mach0
e asm.os=ios
e asm.arch=arm
e asm.pcalign=0
```

`-e` ： Entrypoint

```
➜  AwemeCore rabin2 -e ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore
[Entrypoints]
vaddr=0x00023448 paddr=0x00023448 haddr=-1 type=program

1 entrypoints
```

`-er`

```
➜  AwemeCore rabin2 -er ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCor
e.framework/AwemeCore
fs symbols
"f entry0 1 0x00023448"
"f entry0_haddr 1 0xffffffffffffffff"
"s entry0"
```

`-i` : Imports

```
➜  AwemeCore rabin2 -i ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore > AwemeCore_rabin2_i.txt
```

输出内容：

```
[Imports]
nth  vaddr      bind type           lib name
―――――――――――――――――――――――――――――――――――――――――――――
0     0x11476a38 NONE FUNC              sym.imp.Foundation.NSNotFound.getter : Swift.Int
1     0x11476a44 NONE FUNC              sym.imp.static Foundation.CharacterSet.whitespacesAndNewlines.getter : Foundation.CharacterSet
2     0x11476a50 NONE FUNC              sym.imp.type metadata accessor for Foundation.CharacterSet
3     0x11476a5c NONE FUNC              sym.imp.static Foundation.Notification._unconditionallyBridgeFromObjectiveC(Swift.Optional<__C.NSNotification>) -> Foundation.Notification
4     0x11476a68 NONE FUNC              sym.imp.Foundation.Notification.object.getter : Swift.Optional<Any>
5     0x11476a74 NONE FUNC              sym.imp.Foundation.Notification.userInfo.getter : Swift.Optional<Swift.Dictionary<Swift.AnyHashable, Any>>
6     0x11476a80 NONE FUNC              sym.imp.type metadata accessor for Foundation.Notification
7     0x11476a8c NONE FUNC              sym.imp.Foundation._convertErrorToNSError(Swift.Error) -> __C.NSError
8     0x11476a98 NONE FUNC              sym.imp.Foundation._convertNSErrorToError(Swift.Optional<__C.NSError>) -> Swift.Error
9     0x11476aa4 NONE FUNC              sym.imp.type metadata accessor for Foundation.NSFastEnumerationIterator
10    0x00000000 NONE FUNC              sym.imp.protocol conformance descriptor for Foundation.NSFastEnumerationIterator : Swift.IteratorProtocol in Foundation
11    0x11476ab0 NONE FUNC              sym.imp.Foundation.URL.absoluteString.getter : Swift.String
12    0x11476abc NONE FUNC              sym.imp.Foundation.URL._bridgeToObjectiveC() -> __C.NSURL
13    0x11476ac8 NONE FUNC              sym.imp.static Foundation.URL._unconditionallyBridgeFromObjectiveC(Swift.Optional<__C.NSURL>) -> Foundation.URL
14    0x11476ad4 NONE FUNC              sym.imp.Foundation.URL.scheme.getter : Swift.Optional<Swift.String>
15    0x11476ae0 NONE FUNC              sym.imp.Foundation.URL.init(string: __shared Swift.String) -> Swift.Optional<Foundation.URL>
16    0x11476aec NONE FUNC              sym.imp.type metadata accessor for Foundation.URL
17    0x00000000 NONE FUNC              sym.imp.nominal type descriptor for Foundation.URL
18    0x11476af8 NONE FUNC              sym.imp.Foundation.Data._copyContents(initializing: Swift.UnsafeMutableBufferPointer<Swift.UInt8>) -> (Foundation.Data.Iterator, Swift.Int)
19    0x11476b04 NONE FUNC              sym.imp.Foundation.Data._bridgeToObjectiveC() -> __C.NSData
20    0x11476b10 NONE FUNC              sym.imp.static Foundation.Data._unconditionallyBridgeFromObjectiveC(Swift.Optional<__C.NSData>) -> Foundation.Data
21    0x11476b1c NONE FUNC              sym.imp.type metadata accessor for Foundation.Data.Iterator
22    0x00000000 NONE FUNC              sym.imp.type metadata for Foundation.Data
```

```
23   0x11476b28 NONE FUNC              sym.imp.static Foundation.Date.distantPast.getter : Foundation.Date
24   0x11476b34 NONE FUNC              sym.imp.Foundation.Date.timeIntervalSince(Foundation.Date) -> Swift.Double
25   0x11476b40 NONE FUNC              sym.imp.Foundation.Date._bridgeToObjectiveC() -> __C.NSDate
26   0x11476b4c NONE FUNC              sym.imp.static Foundation.Date.< infix(Foundation.Date, Foundation.Date) -> Swift.Bool
27   0x11476b58 NONE FUNC              sym.imp.Foundation.Date.init(timeIntervalSinceNow: Swift.Double) -> Foundation.Date
28   0x11476b64 NONE FUNC              sym.imp.Foundation.Date.init() -> Foundation.Date
29   0x11476b70 NONE FUNC              sym.imp.type metadata accessor for Foundation.Date
30   0x00000000 NONE FUNC              sym.imp.nominal type descriptor for Foundation.Date
31   0x11476b7c NONE FUNC              sym.imp.Foundation.UUID.uuidString.getter : Swift.String
32   0x11476b88 NONE FUNC              sym.imp.type metadata accessor for Foundation.UUID
33   0x11476b94 NONE FUNC              sym.imp.Foundation.IndexPath._bridgeToObjectiveC() -> __C.NSIndexPath
34   0x11476ba0 NONE FUNC              sym.imp.static Foundation.IndexPath._unconditionallyBridgeFromObjectiveC(Swift.Optional<__C.NSIndexPath>) -> Foundation.IndexPath
35   0x11476bac NONE FUNC              sym.imp.(extension in UIKit):Foundation.IndexPath.init(row: Swift.Int, section: Swift.Int) -> Foundation.IndexPath
36   0x11476bb8 NONE FUNC              sym.imp.(extension in UIKit):Foundation.IndexPath.row.getter : Swift.Int
37   0x11476bc4 NONE FUNC              sym.imp.(extension in UIKit):Foundation.IndexPath.init(item: Swift.Int, section: Swift.Int) -> Foundation.IndexPath
38   0x11476bd0 NONE FUNC              sym.imp.(extension in UIKit):Foundation.IndexPath.item.getter : Swift.Int
39   0x11476bdc NONE FUNC              sym.imp.(extension in UIKit):Foundation.IndexPath.section.getter : Swift.Int
40   0x11476be8 NONE FUNC              sym.imp.type metadata accessor for Foundation.IndexPath
41   0x00000000 NONE FUNC              sym.imp.nominal type descriptor for Foundation.IndexPath
...
4922 0x1147ea84 NONE FUNC              vImageConverter_CreateWithCGImageFormat
4923 0x1147ea90 NONE FUNC              vImageConverter_Release
4924 0x1147ea9c NONE FUNC              vImageCreateCGImageFromBuffer
4925 0x1147eaa8 NONE FUNC              vImageHorizontalReflect_ARGB8888
4926 0x1147eab4 NONE FUNC              vImageMatrixMultiply_ARGB8888
4927 0x1147eac0 NONE FUNC              vImageMatrixMultiply_ARGB8888ToPlanar8
4928 0x1147eacc NONE FUNC              vImagePermuteChannels_ARGB8888
4929 0x1147ead8 NONE FUNC              vImagePremultiplyData_RGBA8888
4930 0x1147eae4 NONE FUNC              vImageRotate90_ARGB8888
4931 0x1147eaf0 NONE FUNC              vImageRotate90_Planar16U
4932 0x1147eafc NONE FUNC              vImageRotate90_Planar8
4933 0x1147eb08 NONE FUNC              vImageScale_ARGB8888
4934 0x1147eb14 NONE FUNC              vImageScale_Planar16U
4935 0x1147eb20 NONE FUNC              vImageScale_Planar8
4936 0x1147eb2c NONE FUNC              vImageTentConvolve_ARGB8888
4937 0x1147eb38 NONE FUNC              vImageUnpremultiplyData_ARGB8888
4938 0x1147eb44 NONE FUNC              vImageUnpremultiplyData_RGBA8888
```

```
4939 0x1147eb50 NONE FUNC                              vImageVerticalReflect_ARGB8888
4940 0x1147eb5c NONE FUNC                              vasprintf
4941 0x1147eb68 NONE FUNC                              vfprintf
4942 0x1147eb74 NONE FUNC                              vm_allocate
4943 0x1147eb80 NONE FUNC                              vm_deallocate
4944 0x00000000 NONE FUNC                              vm_kernel_page_size
4945 0x1147eb8c NONE FUNC                              vm_map_page_query
4946 0x00000000 NONE FUNC                              vm_page_mask
4947 0x00000000 NONE FUNC                              vm_page_size
4948 0x1147eb98 NONE FUNC                              vm_protect
4949 0x1147eba4 NONE FUNC                              vm_read
4950 0x1147ebb0 NONE FUNC                              vm_read_overwrite
4951 0x1147ebbc NONE FUNC                              vm_region_64
4952 0x1147ebc8 NONE FUNC                              vm_region_recurse_64
4953 0x1147ebd4 NONE FUNC                              vm_remap
4954 0x1147ebe0 NONE FUNC                              vprintf
4955 0x1147ebec NONE FUNC                              vsnprintf
4956 0x1147ebf8 NONE FUNC                              vsprintf
4957 0x1147ec04 NONE FUNC                              vvexpf
4958 0x1147ec10 NONE FUNC                              vvsqrt
4959 0x00000000 NONE FUNC                              wait
4960 0x1147ec1c NONE FUNC                              wcscat
4961 0x1147ec28 NONE FUNC                              wcschr
4962 0x1147ec34 NONE FUNC                              wcscmp
4963 0x1147ec40 NONE FUNC                              wcscpy
4964 0x1147ec4c NONE FUNC                              wcsftime
4965 0x1147ec58 NONE FUNC                              wcslen
4966 0x1147ec64 NONE FUNC                              wcsncat
4967 0x1147ec70 NONE FUNC                              wcsncpy
4968 0x1147ec7c NONE FUNC                              wcstok
4969 0x1147ec88 NONE FUNC                              wcstombs
4970 0x1147ec94 NONE FUNC                              wmemcmp
4971 0x1147eca0 NONE FUNC                              wmemcpy
4972 0x1147ecac NONE FUNC                              write
4973 0x1147ecb8 NONE FUNC                              writev
4974 0x1147ecc4 NONE FUNC                              xmlAddChild
4975 0x1147ecd0 NONE FUNC                              xmlBufferContent
4976 0x1147ecdc NONE FUNC                              xmlBufferCreate
4977 0x1147ece8 NONE FUNC                              xmlBufferFree
4978 0x1147ecf4 NONE FUNC                              xmlBufferLength
4979 0x1147ed00 NONE FUNC                              xmlCheckVersion
4980 0x1147ed0c NONE FUNC                              xmlCleanupParser
4981 0x1147ed18 NONE FUNC                              xmlCopyNode
4982 0x1147ed24 NONE FUNC                              xmlCreatePushParserCtxt
4983 0x1147ed30 NONE FUNC                              xmlDocDumpMemory
4984 0x1147ed3c NONE FUNC                              xmlDocGetRootElement
4985 0x1147ed48 NONE FUNC                              xmlDocSetRootElement
4986 0x1147ed54 NONE FUNC                              xmlFirstElementChild
4987 0x00000000 NONE FUNC                              xmlFree
4988 0x1147ed60 NONE FUNC                              xmlFreeDoc
4989 0x1147ed6c NONE FUNC                              xmlFreeNode
4990 0x1147ed78 NONE FUNC                              xmlFreeNs
4991 0x1147ed84 NONE FUNC                              xmlFreeNsList
4992 0x1147ed90 NONE FUNC                              xmlFreeParserCtxt
4993 0x1147ed9c NONE FUNC                              xmlGetProp
4994 0x1147eda8 NONE FUNC                              xmlHasNsProp
```

```
4995 0x1147edb4 NONE FUNC               xmlHasProp
4996 0x1147edc0 NONE FUNC               xmlInitParser
4997 0x1147edcc NONE FUNC               xmlNewDoc
4998 0x1147edd8 NONE FUNC               xmlNewNode
4999 0x1147ede4 NONE FUNC               xmlNewNs
5000 0x1147edf0 NONE FUNC               xmlNewNsProp
5001 0x1147edfc NONE FUNC               xmlNewProp
5002 0x1147ee08 NONE FUNC               xmlNewText
5003 0x1147ee14 NONE FUNC               xmlNextElementSibling
5004 0x1147ee20 NONE FUNC               xmlNodeDump
5005 0x1147ee2c NONE FUNC               xmlNodeGetContent
5006 0x1147ee38 NONE FUNC               xmlNodeListGetString
5007 0x1147ee44 NONE FUNC               xmlNodeSetContent
5008 0x1147ee50 NONE FUNC               xmlNodeSetName
5009 0x1147ee5c NONE FUNC               xmlParseChunk
5010 0x1147ee68 NONE FUNC               xmlReadMemory
5011 0x1147ee74 NONE FUNC               xmlSearchNs
5012 0x1147ee80 NONE FUNC               xmlSearchNsByHref
5013 0x1147ee8c NONE FUNC               xmlSetNs
5014 0x1147ee98 NONE FUNC               xmlSetTreeDoc
5015 0x1147eea4 NONE FUNC               xmlStrEqual
5016 0x1147eeb0 NONE FUNC               xmlStrcmp
5017 0x1147eebc NONE FUNC               xmlStrdup
5018 0x1147eec8 NONE FUNC               xmlStrlen
5019 0x1147eed4 NONE FUNC               xmlStrsub
5020 0x1147eee0 NONE FUNC               xmlUnlinkNode
5021 0x1147eeec NONE FUNC               xmlXPathEval
5022 0x1147eef8 NONE FUNC               xmlXPathFreeContext
5023 0x1147ef04 NONE FUNC               xmlXPathFreeObject
5024 0x1147ef10 NONE FUNC               xmlXPathNewContext
5025 0x1147ef1c NONE FUNC               xmlXPathRegisterNs
5026 0x1147ef28 NONE FUNC               zlibCompileFlags
5027 0x1147ef34 NONE FUNC               zlibVersion
5028 0x00000000 NONE FUNC               dyld_stub_binder
```

结果分析

- 对比1：内容很像是nm输出的结果
  - `rabin2 -i`

    ```
    5024 0x1147ef10 NONE FUNC               xmlXPathNewContext
    5025 0x1147ef1c NONE FUNC               xmlXPathRegisterNs
    5026 0x1147ef28 NONE FUNC               zlibCompileFlags
    5027 0x1147ef34 NONE FUNC               zlibVersion
    5028 0x00000000 NONE FUNC               dyld_stub_binder
    ```

  - `nm`

    ```
    U _xmlXPathNewContext
    U _xmlXPathRegisterNs
    U _zlibCompileFlags
    U _zlibVersion
    U dyld_stub_binder
    ```

- 对比2：rabin2比nm的更加易懂
  - `rabin2 -i`

```
0    0x11476a38 NONE FUNC              sym.imp.Foundation.NSNotFound.getter :
Swift.Int
1    0x11476a44 NONE FUNC              sym.imp.static Foundation.CharacterSet.
whitespacesAndNewlines.getter : Foundation.CharacterSet
2    0x11476a50 NONE FUNC              sym.imp.type metadata accessor for Foun
dation.CharacterSet
3    0x11476a5c NONE FUNC              sym.imp.static Foundation.Notification.
_unconditionallyBridgeFromObjectiveC(Swift.Optional<__C.NSNotification>) -> Fou
ndation.Notification
4    0x11476a68 NONE FUNC              sym.imp.Foundation.Notification.object.
getter : Swift.Optional<Any>
5    0x11476a74 NONE FUNC              sym.imp.Foundation.Notification.userInf
o.getter : Swift.Optional<Swift.Dictionary<Swift.AnyHashable, Any>>
6    0x11476a80 NONE FUNC              sym.imp.type metadata accessor for Foun
dation.Notification
7    0x11476a8c NONE FUNC              sym.imp.Foundation._convertErrorToNSErr
or(Swift.Error) -> __C.NSError
8    0x11476a98 NONE FUNC              sym.imp.Foundation._convertNSErrorToErr
or(Swift.Optional<__C.NSError>) -> Swift.Error
9    0x11476aa4 NONE FUNC              sym.imp.type metadata accessor for Foun
dation.NSFastEnumerationIterator
```

  - `nm`

```
U _$s10Foundation10NSNotFoundSivg
U _$s10Foundation12CharacterSetV22whitespacesAndNewlinesACvgZ
U _$s10Foundation12CharacterSetVMa
U _$s10Foundation12NotificationV36_unconditionallyBridgeFromObjectiveCyACSo14NS
NotificationCSgFZ
U _$s10Foundation12NotificationV6objectypSgvg
U _$s10Foundation12NotificationV8userInfoSDys11AnyHashableVypGSgvg
U _$s10Foundation12NotificationVMa
U _$s10Foundation22_convertErrorToNSErrorySo0E0Cs0C0_pF
U _$s10Foundation22_convertNSErrorToErrorys0E0_pSo0C0CSgF
U _$s10Foundation25NSFastEnumerationIteratorVMa
```

`-E` : Exports

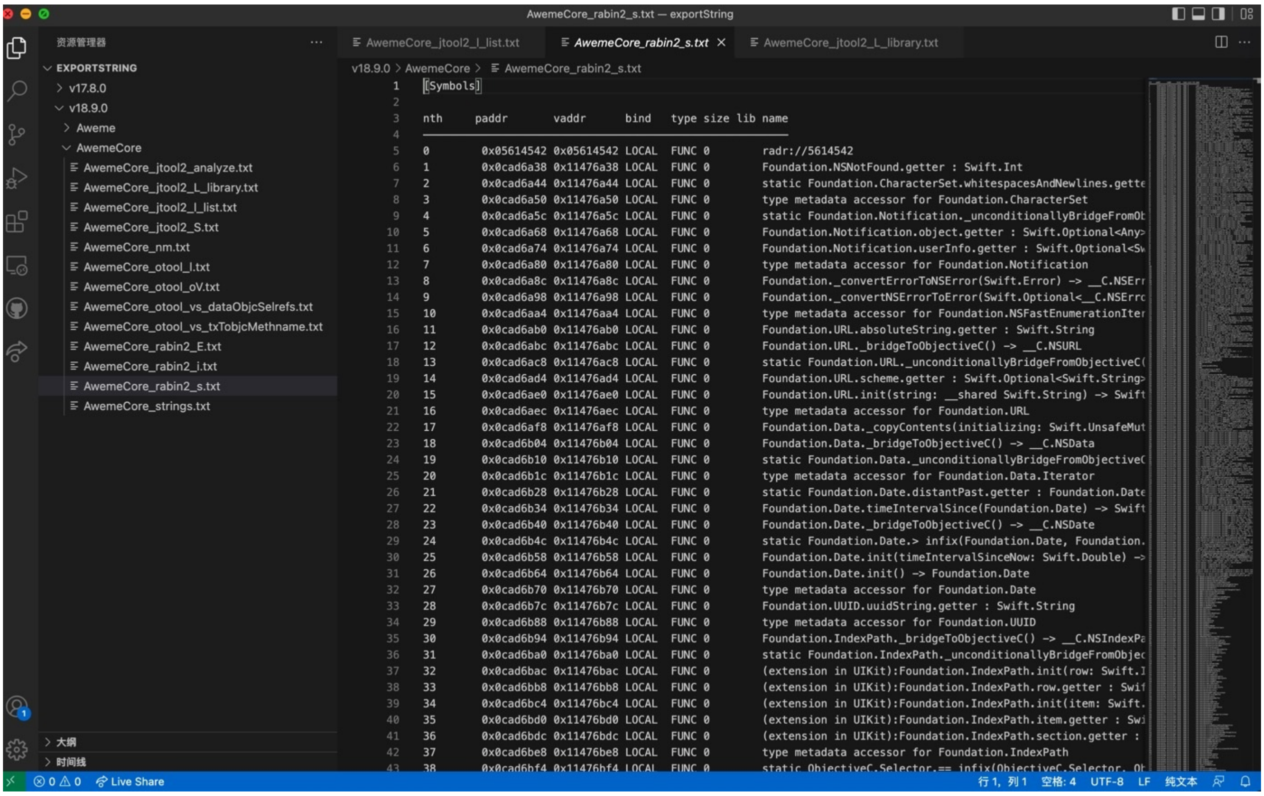
```
➜  AwemeCore rabin2 -E ../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore > AwemeCore_rabin2_E.txt

[Exports]

nth  paddr      vaddr      bind   type size lib name
―――――――――――――――――――――――――――――――――――――――――――――――――――――
2840  0x00b8e0b8 0x00b8e0b8 GLOBAL FUNC 0        _OBJC_METACLASS_$_AWEFriendsActivityWi
dgetConfigurationIntentResponse
2841  0x00b8e0e0 0x00b8e0e0 GLOBAL FUNC 0        _OBJC_METACLASS_$_AWEFriendsActivityWi
dgetLandingPageResolutionResult
2842  0x00b8e130 0x00b8e130 GLOBAL FUNC 0        _OBJC_METACLASS_$_AWEFriendsWidgetsCol
```

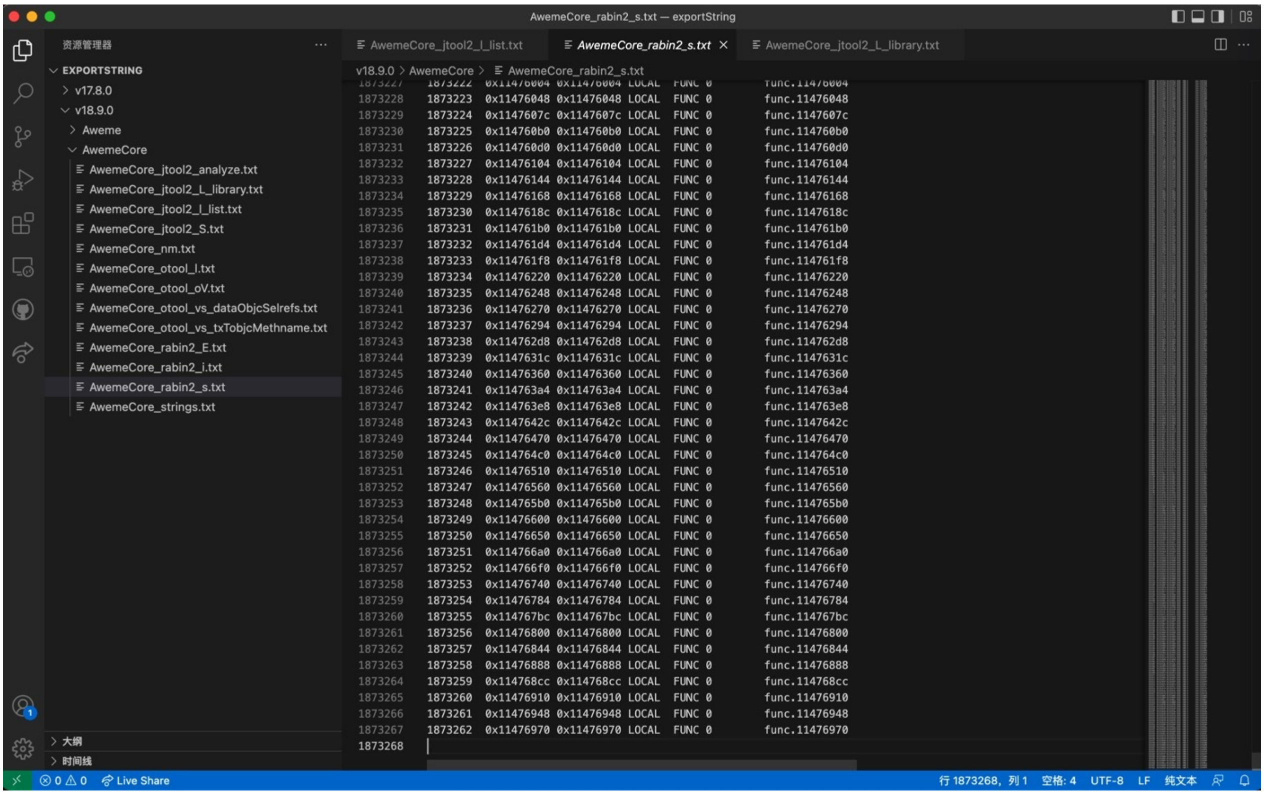
```
orSchemeResolutionResult
2843  0x00b8e068 0x00b8e068 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsActivityWidget
ConfigurationIntent
2844  0x00b8e090 0x00b8e090 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsActivityWidget
ConfigurationIntentResponse
2845  0x00b8e108 0x00b8e108 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsActivityWidget
LandingPageResolutionResult
2846  0x00b8e158 0x00b8e158 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsWidgetsColorSc
hemeResolutionResult
2847  0x0c46ffcc 0x10e0ffcc GLOBAL FUNC 0        _awemeMain
```

`-s` : Symbols

```
➜  AwemeCore rabin2 -s ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore > AwemeCore_rabin2_s.txt

[Symbols]

nth      paddr       vaddr      bind   type size lib name
―――――――――――――――――――――――――――――――――――――――――――――――――――――――――
0        0x05614542 0x05614542 LOCAL  FUNC 0        radr://5614542
1        0x0cad6a38 0x11476a38 LOCAL  FUNC 0        Foundation.NSNotFound.getter : Swif
t.Int
2        0x0cad6a44 0x11476a44 LOCAL  FUNC 0        static Foundation.CharacterSet.whit
espacesAndNewlines.getter : Foundation.CharacterSet
3        0x0cad6a50 0x11476a50 LOCAL  FUNC 0        type metadata accessor for Foundati
on.CharacterSet
...
2836     0x0cadef1c 0x1147ef1c LOCAL  FUNC 0        imp.xmlXPathRegisterNs
2837     0x0cadef28 0x1147ef28 LOCAL  FUNC 0        imp.zlibCompileFlags
2838     0x0cadef34 0x1147ef34 LOCAL  FUNC 0        imp.zlibVersion
2839     0x00b8e040 0x00b8e040 GLOBAL FUNC 0        imp._OBJC_METACLASS_$_AWEFriendsAct
ivityWidgetConfigurationIntent
2840     0x00b8e0b8 0x00b8e0b8 GLOBAL FUNC 0        _OBJC_METACLASS_$_AWEFriendsActivit
yWidgetConfigurationIntentResponse
2841     0x00b8e0e0 0x00b8e0e0 GLOBAL FUNC 0        _OBJC_METACLASS_$_AWEFriendsActivit
yWidgetLandingPageResolutionResult
2842     0x00b8e130 0x00b8e130 GLOBAL FUNC 0        _OBJC_METACLASS_$_AWEFriendsWidgets
ColorSchemeResolutionResult
2843     0x00b8e068 0x00b8e068 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsActivityWid
getConfigurationIntent
2844     0x00b8e090 0x00b8e090 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsActivityWid
getConfigurationIntentResponse
2845     0x00b8e108 0x00b8e108 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsActivityWid
getLandingPageResolutionResult
2846     0x00b8e158 0x00b8e158 GLOBAL FUNC 0        _OBJC_CLASS_$_AWEFriendsWidgetsColo
rSchemeResolutionResult
2847     0x0c46ffcc 0x10e0ffcc GLOBAL FUNC 0        _awemeMain
2848     0x05924000 0x05924000 LOCAL  FUNC 0        func.05924000
2849     0x05924290 0x05924290 LOCAL  FUNC 0        func.05924290
...
1873257  0x11476844 0x11476844 LOCAL  FUNC 0        func.11476844
1873258  0x11476888 0x11476888 LOCAL  FUNC 0        func.11476888
1873259  0x114768cc 0x114768cc LOCAL  FUNC 0        func.114768cc
```

```
1873260  0x11476910 0x11476910 LOCAL  FUNC 0       func.11476910
1873261  0x11476948 0x11476948 LOCAL  FUNC 0       func.11476948
1873262  0x11476970 0x11476970 LOCAL  FUNC 0       func.11476970
```





-sr

```
➜ AwemeCore rabin2 -sr ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCor
```

```
e.framework/AwemeCore > AwemeCore_rabin2_sr.txt

fs symbols
"f sym.radr:__5614542 0 0x05614542"
fs imports
"f sym.Foundation.NSNotFound.getter_:_Swift.Int 0 0x11476a38"
"f sym.static_Foundation.CharacterSet.whitespacesAndNewlines.getter_:_Foundation.Charac
terSet 0 0x11476a44"
"f sym.type_metadata_accessor_for_Foundation.CharacterSet 0 0x11476a50"
"f sym.static_Foundation.Notification._unconditionallyBridgeFromObjectiveC_Swift.Option
al___C.NSNotification______Foundation.Notific 0 0x11476a5c"
"f sym.Foundation.Notification.object.getter_:_Swift.Optional_Any 0 0x11476a68"
"f sym.Foundation.Notification.userInfo.getter_:_Swift.Optional_Swift.Dictionary_Swift.
AnyHashable__Any 0 0x11476a74"
"f sym.type_metadata_accessor_for_Foundation.Notification 0 0x11476a80"
"f sym.Foundation._convertErrorToNSError_Swift.Error_______C.NSError 0 0x11476a8c"
"f sym.Foundation._convertNSErrorToError_Swift.Optional___C.NSError______Swift.Error 0
0x11476a98"
...
"f sym.func.11476888 0 0x11476888"
"f sym.func.114768cc 0 0x114768cc"
"f sym.func.11476910 0 0x11476910"
"f sym.func.11476948 0 0x11476948"
"f sym.func.11476970 0 0x11476970"
```

`-l` : Libraries

```
➜  AwemeCore rabin2 -l ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore > AwemeCore_rabin2_l.txt

[Linked libraries]
/usr/lib/libcompression.dylib
@rpath/BDLRepairer.framework/BDLRepairer
/usr/lib/libc++.1.dylib
/System/Library/Frameworks/AdServices.framework/AdServices
/System/Library/Frameworks/AppTrackingTransparency.framework/AppTrackingTransparency
/System/Library/Frameworks/AuthenticationServices.framework/AuthenticationServices
/System/Library/Frameworks/CoreHaptics.framework/CoreHaptics
/System/Library/Frameworks/CoreTelephony.framework/CoreTelephony
/System/Library/Frameworks/MetalKit.framework/MetalKit
/System/Library/Frameworks/MetalPerformanceShaders.framework/MetalPerformanceShaders
/System/Library/Frameworks/MetricKit.framework/MetricKit
/System/Library/Frameworks/StoreKit.framework/StoreKit
@rpath/VolcEngineRTC.framework/VolcEngineRTC
@rpath/byteaudio.framework/byteaudio
/usr/lib/libbz2.1.0.dylib
/usr/lib/libc++abi.dylib
/usr/lib/libiconv.2.dylib
/usr/lib/libicucore.A.dylib
/usr/lib/liblzma.5.dylib
/usr/lib/libSystem.B.dylib
/usr/lib/libresolv.9.dylib
/usr/lib/libsqlite3.dylib
/usr/lib/libxml2.2.dylib
```

```
/usr/lib/libz.1.dylib
/System/Library/Frameworks/ARKit.framework/ARKit
/System/Library/Frameworks/AVFoundation.framework/AVFoundation
/System/Library/Frameworks/AVKit.framework/AVKit
/System/Library/Frameworks/Accelerate.framework/Accelerate
/System/Library/Frameworks/AdSupport.framework/AdSupport
/System/Library/Frameworks/AddressBook.framework/AddressBook
/System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary
/System/Library/Frameworks/AudioToolbox.framework/AudioToolbox
/System/Library/Frameworks/CFNetwork.framework/CFNetwork
/System/Library/Frameworks/Contacts.framework/Contacts
/System/Library/Frameworks/ContactsUI.framework/ContactsUI
/System/Library/Frameworks/CoreAudio.framework/CoreAudio
/System/Library/Frameworks/CoreAudioKit.framework/CoreAudioKit
/System/Library/Frameworks/CoreFoundation.framework/CoreFoundation
/System/Library/Frameworks/CoreGraphics.framework/CoreGraphics
/System/Library/Frameworks/CoreImage.framework/CoreImage
/System/Library/Frameworks/CoreLocation.framework/CoreLocation
/System/Library/Frameworks/CoreML.framework/CoreML
/System/Library/Frameworks/CoreMedia.framework/CoreMedia
/System/Library/Frameworks/CoreMotion.framework/CoreMotion
/System/Library/Frameworks/MobileCoreServices.framework/MobileCoreServices
/System/Library/Frameworks/CoreSpotlight.framework/CoreSpotlight
/System/Library/Frameworks/CoreText.framework/CoreText
/System/Library/Frameworks/CoreVideo.framework/CoreVideo
/System/Library/Frameworks/EventKit.framework/EventKit
/System/Library/Frameworks/Foundation.framework/Foundation
/System/Library/Frameworks/GLKit.framework/GLKit
/System/Library/Frameworks/GameplayKit.framework/GameplayKit
/System/Library/Frameworks/IOKit.framework/Versions/A/IOKit
/System/Library/Frameworks/ImageIO.framework/ImageIO
/System/Library/Frameworks/Intents.framework/Intents
/System/Library/Frameworks/JavaScriptCore.framework/JavaScriptCore
/System/Library/Frameworks/LocalAuthentication.framework/LocalAuthentication
/System/Library/Frameworks/MapKit.framework/MapKit
/System/Library/Frameworks/MediaAccessibility.framework/MediaAccessibility
/System/Library/Frameworks/MediaPlayer.framework/MediaPlayer
/System/Library/Frameworks/MediaToolbox.framework/MediaToolbox
/System/Library/Frameworks/MessageUI.framework/MessageUI
/System/Library/Frameworks/Metal.framework/Metal
/System/Library/Frameworks/NetworkExtension.framework/NetworkExtension
/System/Library/Frameworks/OpenAL.framework/OpenAL
/System/Library/Frameworks/OpenGLES.framework/OpenGLES
/System/Library/Frameworks/Photos.framework/Photos
/System/Library/Frameworks/PhotosUI.framework/PhotosUI
/System/Library/Frameworks/QuartzCore.framework/QuartzCore
/System/Library/Frameworks/ReplayKit.framework/ReplayKit
/System/Library/Frameworks/SafariServices.framework/SafariServices
/System/Library/Frameworks/Security.framework/Security
/System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration
/System/Library/Frameworks/UIKit.framework/UIKit
/System/Library/Frameworks/VideoToolbox.framework/VideoToolbox
/System/Library/Frameworks/WebKit.framework/WebKit
/System/Library/Frameworks/iAd.framework/iAd
/System/Library/Frameworks/QuickLook.framework/QuickLook
/usr/lib/libobjc.A.dylib
```

```
/System/Library/Frameworks/Combine.framework/Combine
/System/Library/Frameworks/GroupActivities.framework/GroupActivities
/System/Library/Frameworks/IOSurface.framework/IOSurface
/System/Library/Frameworks/UserNotifications.framework/UserNotifications
/System/Library/Frameworks/WidgetKit.framework/WidgetKit
/usr/lib/swift/libswiftCoreMIDI.dylib
/usr/lib/swift/libswiftDataDetection.dylib
/usr/lib/swift/libswiftFileProvider.dylib
/usr/lib/swift/libswiftUniformTypeIdentifiers.dylib
/usr/lib/swift/libswiftWebKit.dylib
/usr/lib/swift/libswift_Concurrency.dylib
@rpath/libswiftAVFoundation.dylib
@rpath/libswiftCore.dylib
@rpath/libswiftCoreAudio.dylib
@rpath/libswiftCoreData.dylib
@rpath/libswiftCoreFoundation.dylib
@rpath/libswiftCoreGraphics.dylib
@rpath/libswiftCoreImage.dylib
@rpath/libswiftCoreLocation.dylib
@rpath/libswiftCoreMedia.dylib
@rpath/libswiftDarwin.dylib
@rpath/libswiftDispatch.dylib
@rpath/libswiftFoundation.dylib
@rpath/libswiftIntents.dylib
@rpath/libswiftMapKit.dylib
@rpath/libswiftMetal.dylib
@rpath/libswiftNetwork.dylib
@rpath/libswiftObjectiveC.dylib
@rpath/libswiftPhotos.dylib
@rpath/libswiftQuartzCore.dylib
@rpath/libswiftUIKit.dylib
@rpath/libswiftos.dylib
@rpath/libswiftsimd.dylib

112 libraries
```

`-z` : Strings

- `-z` 参数含义
  - The -z option is used to list readable strings found in the .rodata section of ELF binaries, or the .text section of PE files.

```
➜  AwemeCore rabin2 -z ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore > AwemeCore_rabin2_z.txt

[Strings]
nth     paddr      vaddr      len  size section               type    string
―――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――
0       0x00013e7f 0x00013e7f 5    6    1.__TEXT.__const      ascii   7\rW?<
1       0x00013e89 0x00013e89 4    5    1.__TEXT.__const      ascii   \a)FA
2       0x00013eb0 0x00013eb0 19   20   1.__TEXT.__const      ascii   AWECommentS
wiftImpl
3       0x00013ed0 0x00013ed0 24   25   1.__TEXT.__const      ascii   ActionViewL
```

```
ayoutDelegate
4       0x00013f20 0x00013f20 10   11   1.__TEXT.__const             ascii    ActionView
5       0x00013f48 0x00013f48 4    20   1.__TEXT.__const             utf32le D:\v\n
6       0x000140f0 0x000140f0 19   20   1.__TEXT.__const             ascii    AWECommentC
olorMode
7       0x00014124 0x00014124 13   14   1.__TEXT.__const             ascii    AWECommentT
ab
8       0x00014160 0x00014160 24   25   1.__TEXT.__const             ascii    AWEModernFe
edEventSource
9       0x000141a0 0x000141a0 24   25   1.__TEXT.__const             ascii    AWEAwemeMod
elCommentType
10      0x000141e0 0x000141e0 21   22   1.__TEXT.__const             ascii    AWEUserFoll
owerStatus
11      0x00014220 0x00014220 19   20   1.__TEXT.__const             ascii    AWEUserFoll
owStatus
12      0x00014260 0x00014260 23   24   1.__TEXT.__const             ascii    AWECommentC
ellSceneType
13      0x000142a0 0x000142a0 20   21   1.__TEXT.__const             ascii    AWECommentR
eplyStyle
14      0x000142e0 0x000142e0 19   20   1.__TEXT.__const             ascii    AWECommentP
ostState
15      0x00014320 0x00014320 17   18   1.__TEXT.__const             ascii    AWECommentT
agType
16      0x00014354 0x00014354 11   12   1.__TEXT.__const             ascii    ActionStyle
17      0x0001437c 0x0001437c 10   11   1.__TEXT.__const             ascii    ActionType
18      0x000143b0 0x000143b0 27   28   1.__TEXT.__const             ascii    AWECommentB
aseListViewModel
19      0x00014430 0x00014430 4    5    1.__TEXT.__const             ascii    Weak
20      0x000144e2 0x000144e2 11   12   1.__TEXT.__const             ascii    stIndexPath
21      0x00014510 0x00014510 19   20   1.__TEXT.__const             ascii    AWECommentS
wiftImpl
22      0x00014530 0x00014530 8    9    1.__TEXT.__const             ascii    BaseCell
23      0x00014560 0x00014560 4    20   1.__TEXT.__const             utf32le A\nKÎ blocks
=Basic Latin,Latin-1 Supplement
24      0x00014be0 0x00014be0 24   25   1.__TEXT.__const             ascii    BaseListSec
tionViewModel
25      0x00014c70 0x00014c70 11   12   1.__TEXT.__const             ascii    CommentCell
26      0x00014c80 0x00014c80 19   20   1.__TEXT.__const             ascii    AWECommentS
wiftImpl
27      0x00014cc0 0x00014cc0 5    24   1.__TEXT.__const             utf32le 2\fęĥ& bloc
ks=Basic Latin,Latin Extended-A
28      0x00014e20 0x00014e20 35   36   1.__TEXT.__const             ascii    CommentCont
ainerInnerViewController
29      0x00015030 0x00015030 31   32   1.__TEXT.__const             ascii    CommentCont
ainerInnerViewHolder
30      0x000150d0 0x000150d0 24   25   1.__TEXT.__const             ascii    CommentCont
ainerProtocol
31      0x00015120 0x00015120 19   20   1.__TEXT.__const             ascii    AWECommentS
wiftImpl
32      0x00015140 0x00015140 30   31   1.__TEXT.__const             ascii    CommentCont
ainerViewController
33      0x00015184 0x00015184 4    20   1.__TEXT.__const             utf32le 2\n<| blocks
=Basic Latin,Latin-1 Supplement
34      0x000156a0 0x000156a0 25   26   1.__TEXT.__const             ascii    CommentCont
ainerViewModel
...
```

```
39595  0x00f17294 0x00f17294 23   24   89.__DATA.__objc_classname   ascii   AWEVideoMergeTransParam
39596  0x00f172ac 0x00f172ac 35   36   89.__DATA.__objc_classname   ascii   AWEVideoNewPublishCircleTagItemCell
39597  0x00f172d0 0x00f172d0 38   39   89.__DATA.__objc_classname   ascii   AWEVideoNewPublishTagRecommendItemCell
39598  0x00f172f7 0x00f172f7 43   44   89.__DATA.__objc_classname   ascii   AWEVideoNewPublishTagRecommendTableViewCell
39599  0x00f17323 0x00f17323 12   13   89.__DATA.__objc_classname   ascii   LVAudioFrame
39600  0x00f17330 0x00f17330 11   12   89.__DATA.__objc_classname   ascii   Performance
39601  0x00f1733c 0x00f1733c 12   13   89.__DATA.__objc_classname   ascii   VoiceChanger
39602  0x00f17349 0x00f17349 32   33   89.__DATA.__objc_classname   ascii   AWEVideoNewPublishViewController
...
119537 0x0d7521ea 0x120f21ea 4    5    111.__LTC_DATA._C_cstring    ascii   \t\bC
119538 0x0d752209 0x120f2209 7    9    111.__LTC_DATA._C_cstring    utf8    ثITjpS4 blocks=Arabic,Basic Latin
119539 0x0d752246 0x120f2246 7    9    111.__LTC_DATA._C_cstring    utf8    ŋj~O{P\fc blocks=Latin Extended-B,Basic Latin
119540 0x0d752252 0x120f2252 5    7    111.__LTC_DATA._C_cstring    utf8    ȄFyr' blocks=Cyrillic,Basic Latin
119541 0x0d75226f 0x120f226f 5    6    111.__LTC_DATA._C_cstring    ascii   RS\rcJ
119542 0x0d752292 0x120f2292 4    5    111.__LTC_DATA._C_cstring    ascii   o3PR
119543 0x0d7522da 0x120f22da 4    4    111.__LTC_DATA._C_cstring    ascii   bvx$
```

-zr

```
➜  AwemeCore rabin2 -zr ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore > AwemeCore_rabin2_zr.txt

fs strings
f str.7__W 6 0x00013e7f
Cs 6 @ 0x00013e7f
f str.FA 5 0x00013e89
Cs 5 @ 0x00013e89
f str.AWECommentSwiftImpl 20 0x00013eb0
Cs 20 @ 0x00013eb0
f str.ActionViewLayoutDelegate 25 0x00013ed0
Cs 25 @ 0x00013ed0
f str.ActionView 11 0x00013f20
Cs 11 @ 0x00013f20
f str.D: 20 0x00013f48
Cs 20 @ 0x00013f48
f str.AWECommentColorMode 20 0x000140f0
Cs 20 @ 0x000140f0
f str.AWECommentTab 14 0x00014124
Cs 14 @ 0x00014124
f str.AWEModernFeedEventSource 25 0x00014160
Cs 25 @ 0x00014160
f str.AWEAwemeModelCommentType 25 0x000141a0
Cs 25 @ 0x000141a0
```

```
f str.AWEUserFollowerStatus 22 0x000141e0
Cs 22 @ 0x000141e0
f str.AWEUserFollowStatus 20 0x00014220
Cs 20 @ 0x00014220
f str.AWECommentCellSceneType 24 0x00014260
...
f str.ITjpS4 9 0x120f2209
Cs 9 @ 0x120f2209
f str.O_P__c 9 0x120f2246
Cs 9 @ 0x120f2246
f str.Fyr 7 0x120f2252
Cs 7 @ 0x120f2252
f str.RS__cJ 6 0x120f226f
Cs 6 @ 0x120f226f
f str.o3PR 5 0x120f2292
Cs 5 @ 0x120f2292
f str.bvx 4 0x120f22da
Cs 4 @ 0x120f22da
```

`-S` : Program Sections

```
➜  AwemeCore rabin2 -S ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore > AwemeCore_rabin2_S_section.txt

[Sections]

nth paddr            size vaddr           vsize perm name
―――――――――――――――――――――――――――――――――――――――――――――――――――――――――

0   0x0000b9b0     0x84c0 0x0000b9b0     0x84c0 -r-x 0.__TEXT.__stub_helper
1   0x00013e70     0x4020 0x00013e70     0x4020 -r-x 1.__TEXT.__const
2   0x00017e90     0x2ef8 0x00017e90     0x2ef8 -r-x 2.__TEXT.__swift5_typeref
3   0x0001ad88     0x2988 0x0001ad88     0x2988 -r-x 3.__TEXT.__swift5_fieldmd
4   0x0001d710      0x338 0x0001d710      0x338 -r-x 4.__TEXT.__swift5_proto
5   0x0001da48      0x28c 0x0001da48      0x28c -r-x 5.__TEXT.__swift5_types
6   0x0001dcd4        0x0 0x0001dcd4        0x0 -r-x 6.__TEXT.__cstring
7   0x0001dcd4        0x0 0x0001dcd4        0x0 -r-x 7.__TEXT.__objc_methname
8   0x0001dcd4        0x0 0x0001dcd4        0x0 -r-x 8.__TEXT.__objc_classname
9   0x0001dcd4        0x0 0x0001dcd4        0x0 -r-x 9.__TEXT.__objc_methtype
10  0x0001dcd4       0x68 0x0001dcd4       0x68 -r-x 10.__TEXT.__gcc_except_tab
11  0x0001dd40     0x362c 0x0001dd40     0x362c -r-x 11.__TEXT.__swift5_reflstr
12  0x0002136c      0x1b8 0x0002136c      0x1b8 -r-x 12.__TEXT.__swift5_builtin
13  0x00021524      0x2b8 0x00021524      0x2b8 -r-x 13.__TEXT.__swift5_assocty
14  0x000217dc     0x1c0c 0x000217dc     0x1c0c -r-x 14.__TEXT.__swift5_capture
15  0x000233e8       0x60 0x000233e8       0x60 -r-x 15.__TEXT.__swift5_protos
16  0x00023448        0x0 0x00023448        0x0 -r-x 16.__TEXT.__ustring
17  0x00023448        0x0 0x00023448        0x0 -r-x 17.__TEXT.__text
18  0x00023448   0x2a4b70 0x00023448   0x2a4b70 -r-x 18.__TEXT.__unwind_info
19  0x002c7fb8    0x38040 0x002c7fb8    0x38040 -r-x 19.__TEXT.__eh_frame
20  0x00300000       0x1b 0x00300000       0x1b -r-x 20.__TEXT.__oslogstring
21  0x00304000     0x3120 0x00304000     0x3120 -rw- 21.__DATA.__got
22  0x00307120     0x58b0 0x00307120     0x58b0 -rw- 22.__DATA.__la_symbol_ptr
23  0x0030c9d0     0x3d28 0x0030c9d0     0x3d28 -rw- 23.__DATA.__mod_init_func
24  0x00310700    0x11068 0x00310700    0x11068 -rw- 24.__DATA.__const
25  0x00321768      0xa60 0x00321768      0xa60 -rw- 25.__DATA.__cfstring
```

```
26  0x003221c8    0x47a08 0x003221c8    0x47a08 -rw- 26.__DATA.__objc_classlist
27  0x00369bd0      0x678 0x00369bd0      0x678 -rw- 27.__DATA.__objc_nlclslist
28  0x0036a248     0x37f0 0x0036a248     0x37f0 -rw- 28.__DATA.__objc_catlist
29  0x0036da38      0x120 0x0036da38      0x120 -rw- 29.__DATA.__objc_nlcatlist
30  0x0036db58    0x11af8 0x0036db58    0x11af8 -rw- 30.__DATA.__objc_protolist
31  0x0037f650        0x8 0x0037f650        0x8 -rw- 31.__DATA.__objc_imageinfo
32  0x0037f658   0x5c2148 0x0037f658   0x5c2148 -rw- 32.__DATA.__objc_const
33  0x009417a0        0x8 0x009417a0        0x8 -rw- 33.__DATA.__objc_selrefs
34  0x009417a8     0x6700 0x009417a8     0x6700 -rw- 34.__DATA.__objc_protorefs
35  0x00947ea8    0x40350 0x00947ea8    0x40350 -rw- 35.__DATA.__objc_classrefs
36  0x009881f8    0x23548 0x009881f8    0x23548 -rw- 36.__DATA.__objc_superrefs
37  0x009ab740     0x1388 0x009ab740     0x1388 -rw- 37.__DATA.__objc_ivar
38  0x009acac8   0x3a9058 0x009acac8   0x3a9058 -rw- 38.__DATA.__objc_data
39  0x00d55b20     0x4f10 0x00d55b20     0x4f10 -rw- 39.__DATA.__data
40  0x00d5aa30       0xf8 0x00d5aa30       0xf8 -rw- 40.__DATA.__HTSLifeCycle
41  0x00d5ab28       0x18 0x00d5ab28       0x18 -rw- 41.__DATA.__objc_stublist
42  0x00d5ab40       0x18 0x00d5ab40       0x18 -rw- 42.__DATA.RewardedADJSB
43  0x00d5ab58      0x1c8 0x00d5ab58      0x1c8 -rw- 43.__DATA.HGTimorLaunch
44  0x00d5ad20       0x68 0x00d5ad20       0x68 -rw- 44.__DATA.HGTimorLoad
45  0x00d5ad88      0x2f8 0x00d5ad88      0x2f8 -rw- 45.__DATA.TimorLaunch
46  0x00d5b080       0xc0 0x00d5b080       0xc0 -rw- 46.__DATA.TimorLoad
47  0x00d5b140       0xf0 0x00d5b140       0xf0 -rw- 47.__DATA.RSDHCampaign
48  0x00d5b230      0x280 0x00d5b230      0x280 -rw- 48.__DATA.XBMExternal
49  0x00d5b4b0       0xc0 0x00d5b4b0       0xc0 -rw- 49.__DATA.LazyRegHeader
50  0x00d5b570       0x10 0x00d5b570       0x10 -rw- 50.__DATA.AWELynxBridge
51  0x00d5b580       0x30 0x00d5b580       0x30 -rw- 51.__DATA.PremainCode
52  0x00d5b5b0     0x4f60 0x00d5b5b0     0x4f60 -rw- 52.__DATA.LazyRegData
53  0x00d60510      0xe80 0x00d60510      0xe80 -rw- 53.__DATA.__GAIA__SECTION
54  0x00d61390      0x120 0x00d61390      0x120 -rw- 54.__DATA.XBMDefault
55  0x00d614b0       0xc8 0x00d614b0       0xc8 -rw- 55.__DATA.HMDModule
56  0x00d61578       0x18 0x00d61578       0x18 -rw- 56.__DATA.HMDLocalModule
57  0x00d61590      0x180 0x00d61590      0x180 -rw- 57.__DATA.IESLiveBridge
58  0x00d61710      0xa28 0x00d61710      0xa28 -rw- 58.__DATA.__bd_timsdk
59  0x00d62138       0xf0 0x00d62138       0xf0 -rw- 59.__DATA.IESLiveTemplate
60  0x00d62228       0xe0 0x00d62228       0xe0 -rw- 60.__DATA.__LIVESEI
61  0x00d62308      0x360 0x00d62308      0x360 -rw- 61.__DATA.__LIVESCHEMA
62  0x00d62668       0x60 0x00d62668       0x60 -rw- 62.__DATA.__LSCHEMEMODEL
63  0x00d626c8       0x10 0x00d626c8       0x10 -rw- 63.__DATA.__ENTERROOMSEC
64  0x00d626d8       0xd0 0x00d626d8       0xd0 -rw- 64.__DATA.__VSUSERCARD
65  0x00d627a8       0x50 0x00d627a8       0x50 -rw- 65.__DATA.__PUZZLEMETHOD
66  0x00d627f8       0x10 0x00d627f8       0x10 -rw- 66.__DATA.IESSLynxBridge
67  0x00d62808       0x50 0x00d62808       0x50 -rw- 67.__DATA.RxAnnotation
68  0x00d62858     0x4850 0x00d62858     0x4850 -rw- 68.__DATA.__objc_clsrefs
69  0x00d670a8      0x6c0 0x00d670a8      0x6c0 -rw- 69.__DATA.__thread_vars
70  0x00d67768      0x2c0 0x00d67768      0x2c0 -rw- 70.__DATA.IESECSettingReg
71  0x00d67a28       0xb8 0x00d67a28       0xb8 -rw- 71.__DATA.__swift_hooks
72  0x00d67ae0       0xb8 0x00d67ae0       0xb8 -rw- 72.__DATA.__swift51_hooks
73  0x00d67b98      0x670 0x00d67b98      0x670 -rw- 73.__DATA.__HTSService
74  0x00d68208       0xf0 0x00d68208       0xf0 -rw- 74.__DATA.__HTSDyServImpl
75  0x00d682f8      0x620 0x00d682f8      0x620 -rw- 75.__DATA.__HTSMsgAsc
76  0x00d68918      0x450 0x00d68918      0x450 -rw- 76.__DATA.AWERunModernFeed
77  0x00d68d68      0x230 0x00d68d68      0x230 -rw- 77.__DATA.AWERunShare
78  0x00d68f98       0x90 0x00d68f98       0x90 -rw- 78.__DATA.__HTSDyServ
79  0x00d69028       0x80 0x00d69028       0x80 -rw- 79.__DATA.__HTSMsg
80  0x00d690a8     0xc058 0x00d690a8     0xc058 -rw- 80.__DATA.RxInjector
81  0x00d75100      0x118 0x00d75100      0x118 -rw- 81.__DATA.RxAppService
```

```
82  0x00d75218        0x30 0x00d75218        0x30 -rw- 82.__DATA.__HTSNoti
83  0x00d75248        0x80 0x00d75248        0x80 -rw- 83.__DATA.AWERunShareSVC
84  0x00d752c8      0x19a0 0x00d752c8      0x19a0 -rw- 84.__DATA.StudioConfigMock
85  0x00d76c68        0xc0 0x00d76c68        0xc0 -rw- 85.__DATA.XBMInternal
86  0x00d76d30      0xd537 0x00d76d30      0xd537 -rw- 86.__DATA.__cstring
87  0x00d84267     0x6f09b 0x00d84267     0x6f09b -rw- 87.__DATA.__objc_methname
88  0x00df3302     0x1dd08 0x00df3302     0x1dd08 -rw- 88.__DATA.__objc_methtype
89  0x00e1100a    0x13affc 0x00e1100a    0x13affc -rw- 89.__DATA.__objc_classname
90  0x00f4c008     0x34840 0x00f4c008     0x34840 -rw- 90.__DATA.__thread_bss
91  0x00000000         0x0 0x00f80860    0x2d6fe0 -rw- 91.__DATA._D_tconst
92  0x00000000         0x0 0x01257840    0x3c3558 -rw- 92.__DATA._D_dconst
93  0x00000000         0x0 0x0161c000    0x1225fc -rw- 93.__DATA._D_ddata
94  0x00000000         0x0 0x0173e600    0x499b00 -rw- 94.__DATA._D_cfstring
95  0x00000000         0x0 0x01bd8100   0x1c10870 -rw- 95.__DATA._D_objc_const
96  0x00000000         0x0 0x037e8970     0xaaee4 -rw- 96.__DATA._D_objc_ivar
97  0x00000000         0x0 0x03893858    0x2054c8 -rw- 97.__DATA._D_objc_selrefs
98  0x00000000         0x0 0x03a98d20    0x4b5df0 -rw- 98.__DATA._D_gcc_except_ta
99  0x00000000         0x0 0x03f4eb10    0x896683 -rw- 99.__DATA._D_cstring
100 0x00000000         0x0 0x047e5194     0x7795a -rw- 100.__DATA._D_ustring
101 0x00000000         0x0 0x0485caee    0xae06ba -rw- 101.__DATA._D_objc_methname
102 0x00000000         0x0 0x0533d1a8    0x1ca962 -rw- 102.__DATA._D_objc_methtype
103 0x00000000         0x0 0x05507c00    0x17fc48 -rw- 103.__DATA.__common
104 0x00000000         0x0 0x05687900    0x29b0ec -rw- 104.__DATA.__bss
105 0x00f84000   0xbb52a38 0x05924000   0xbb52a38 -r-x 105.__BD_TEXT.__text
106 0x0cad6a38      0x8508 0x11476a38      0x8508 -r-x 106.__BD_TEXT.__stubs
107 0x0cae0000       0x208 0x11480000       0x208 -r-- 107.__LTC_DATA.__meta
108 0x0cae0208        0x10 0x11480208        0x10 -r-- 108.__LTC_DATA.__deco
109 0x0cae0218    0x6d4b3f 0x11480218    0x6d4b3f -r-- 109.__LTC_DATA._C_objc_const
110 0x0d1b4d57     0x19d88 0x11b54d57     0x19d88 -r-- 110.__LTC_DATA._C_objc_ivar
111 0x0d1ceadf    0x5837ff 0x11b6eadf    0x5837ff -r-- 111.__LTC_DATA._C_cstring
112 0x0d7522de    0x23c64f 0x120f22de    0x23c64f -r-- 112.__LTC_DATA._C_tconst
113 0x0d98e92d    0x24ca15 0x1232e92d    0x24ca15 -r-- 113.__LTC_DATA._C_gcc_except_ta
114 0x0dbdb342     0xe1298 0x1257b342     0xe1298 -r-- 114.__LTC_DATA.__fix
```

-Sr

```
➜  AwemeCore rabin2 -Sr ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCor
e.framework/AwemeCore > AwemeCore_rabin2_Sr_section.txt

fs sections
"f section.0.__TEXT.__stub_helper 1 0x0000b9b0"
"f section.1.__TEXT.__const 1 0x00013e70"
"f section.2.__TEXT.__swift5_typeref 1 0x00017e90"
"f section.3.__TEXT.__swift5_fieldmd 1 0x0001ad88"
"f section.4.__TEXT.__swift5_proto 1 0x0001d710"
"f section.5.__TEXT.__swift5_types 1 0x0001da48"
"f section.6.__TEXT.__cstring 1 0x0001dcd4"
"f section.7.__TEXT.__objc_methname 1 0x0001dcd4"
"f section.8.__TEXT.__objc_classname 1 0x0001dcd4"
"f section.9.__TEXT.__objc_methtype 1 0x0001dcd4"
"f section.10.__TEXT.__gcc_except_tab 1 0x0001dcd4"
"f section.11.__TEXT.__swift5_reflstr 1 0x0001dd40"
"f section.12.__TEXT.__swift5_builtin 1 0x0002136c"
"f section.13.__TEXT.__swift5_assocty 1 0x00021524"
```

```
"f section.14.__TEXT.__swift5_capture 1 0x000217dc"
"f section.15.__TEXT.__swift5_protos 1 0x000233e8"
"f section.16.__TEXT.__ustring 1 0x00023448"
"f section.17.__TEXT.__text 1 0x00023448"
"f section.18.__TEXT.__unwind_info 1 0x00023448"
"f section.19.__TEXT.__eh_frame 1 0x002c7fb8"
"f section.20.__TEXT.__oslogstring 1 0x00300000"
"f section.21.__DATA.__got 1 0x00304000"
"f section.22.__DATA.__la_symbol_ptr 1 0x00307120"
"f section.23.__DATA.__mod_init_func 1 0x0030c9d0"
"f section.24.__DATA.__const 1 0x00310700"
"f section.25.__DATA.__cfstring 1 0x00321768"
"f section.26.__DATA.__objc_classlist 1 0x003221c8"
"f section.27.__DATA.__objc_nlclslist 1 0x00369bd0"
"f section.28.__DATA.__objc_catlist 1 0x0036a248"
"f section.29.__DATA.__objc_nlcatlist 1 0x0036da38"
"f section.30.__DATA.__objc_protolist 1 0x0036db58"
"f section.31.__DATA.__objc_imageinfo 1 0x0037f650"
"f section.32.__DATA.__objc_const 1 0x0037f658"
"f section.33.__DATA.__objc_selrefs 1 0x009417a0"
"f section.34.__DATA.__objc_protorefs 1 0x009417a8"
"f section.35.__DATA.__objc_classrefs 1 0x00947ea8"
"f section.36.__DATA.__objc_superrefs 1 0x009881f8"
"f section.37.__DATA.__objc_ivar 1 0x009ab740"
"f section.38.__DATA.__objc_data 1 0x009acac8"
"f section.39.__DATA.__data 1 0x00d55b20"
"f section.40.__DATA.__HTSLifeCycle 1 0x00d5aa30"
"f section.41.__DATA.__objc_stublist 1 0x00d5ab28"
"f section.42.__DATA.RewardedADJSB 1 0x00d5ab40"
"f section.43.__DATA.HGTimorLaunch 1 0x00d5ab58"
"f section.44.__DATA.HGTimorLoad 1 0x00d5ad20"
"f section.45.__DATA.TimorLaunch 1 0x00d5ad88"
"f section.46.__DATA.TimorLoad 1 0x00d5b080"
"f section.47.__DATA.RSDHCampaign 1 0x00d5b140"
"f section.48.__DATA.XBMExternal 1 0x00d5b230"
"f section.49.__DATA.LazyRegHeader 1 0x00d5b4b0"
"f section.50.__DATA.AWELynxBridge 1 0x00d5b570"
"f section.51.__DATA.PremainCode 1 0x00d5b580"
"f section.52.__DATA.LazyRegData 1 0x00d5b5b0"
"f section.53.__DATA.__GAIA__SECTION 1 0x00d60510"
"f section.54.__DATA.XBMDefault 1 0x00d61390"
"f section.55.__DATA.HMDModule 1 0x00d614b0"
"f section.56.__DATA.HMDLocalModule 1 0x00d61578"
"f section.57.__DATA.IESLiveBridge 1 0x00d61590"
"f section.58.__DATA.__bd_timsdk 1 0x00d61710"
"f section.59.__DATA.IESLiveTemplate 1 0x00d62138"
"f section.60.__DATA.__LIVESEI 1 0x00d62228"
"f section.61.__DATA.__LIVESCHEMA 1 0x00d62308"
"f section.62.__DATA.__LSCHEMEMODEL 1 0x00d62668"
"f section.63.__DATA.__ENTERROOMSEC 1 0x00d626c8"
"f section.64.__DATA.__VSUSERCARD 1 0x00d626d8"
"f section.65.__DATA.__PUZZLEMETHOD 1 0x00d627a8"
"f section.66.__DATA.IESSLynxBridge 1 0x00d627f8"
"f section.67.__DATA.RxAnnotation 1 0x00d62808"
"f section.68.__DATA.__objc_clsrefs 1 0x00d62858"
"f section.69.__DATA.__thread_vars 1 0x00d670a8"
```

```
"f section.70.__DATA.IESECSettingReg 1 0x00d67768"
"f section.71.__DATA.__swift_hooks 1 0x00d67a28"
"f section.72.__DATA.__swift51_hooks 1 0x00d67ae0"
"f section.73.__DATA.__HTSService 1 0x00d67b98"
"f section.74.__DATA.__HTSDyServImpl 1 0x00d68208"
"f section.75.__DATA.__HTSMsgAsc 1 0x00d682f8"
"f section.76.__DATA.AWERunModernFeed 1 0x00d68918"
"f section.77.__DATA.AWERunShare 1 0x00d68d68"
"f section.78.__DATA.__HTSDyServ 1 0x00d68f98"
"f section.79.__DATA.__HTSMsg 1 0x00d69028"
"f section.80.__DATA.RxInjector 1 0x00d690a8"
"f section.81.__DATA.RxAppService 1 0x00d75100"
"f section.82.__DATA.__HTSNoti 1 0x00d75218"
"f section.83.__DATA.AWERunShareSVC 1 0x00d75248"
"f section.84.__DATA.StudioConfigMock 1 0x00d752c8"
"f section.85.__DATA.XBMInternal 1 0x00d76c68"
"f section.86.__DATA.__cstring 1 0x00d76d30"
"f section.87.__DATA.__objc_methname 1 0x00d84267"
"f section.88.__DATA.__objc_methtype 1 0x00df3302"
"f section.89.__DATA.__objc_classname 1 0x00e1100a"
"f section.90.__DATA.__thread_bss 1 0x00f4c008"
"f section.91.__DATA._D_tconst 1 0x00f80860"
"f section.92.__DATA._D_dconst 1 0x01257840"
"f section.93.__DATA._D_ddata 1 0x0161c000"
"f section.94.__DATA._D_cfstring 1 0x0173e600"
"f section.95.__DATA._D_objc_const 1 0x01bd8100"
"f section.96.__DATA._D_objc_ivar 1 0x037e8970"
"f section.97.__DATA._D_objc_selrefs 1 0x03893858"
"f section.98.__DATA._D_gcc_except_ta 1 0x03a98d20"
"f section.99.__DATA._D_cstring 1 0x03f4eb10"
"f section.100.__DATA._D_ustring 1 0x047e5194"
"f section.101.__DATA._D_objc_methname 1 0x0485caee"
"f section.102.__DATA._D_objc_methtype 1 0x0533d1a8"
"f section.103.__DATA.__common 1 0x05507c00"
"f section.104.__DATA.__bss 1 0x05687900"
"f section.105.__BD_TEXT.__text 1 0x05924000"
"f section.106.__BD_TEXT.__stubs 1 0x11476a38"
"f section.107.__LTC_DATA.__meta 1 0x11480000"
"f section.108.__LTC_DATA.__deco 1 0x11480208"
"f section.109.__LTC_DATA._C_objc_const 1 0x11480218"
"f section.110.__LTC_DATA._C_objc_ivar 1 0x11b54d57"
"f section.111.__LTC_DATA._C_cstring 1 0x11b6eadf"
"f section.112.__LTC_DATA._C_tconst 1 0x120f22de"
"f section.113.__LTC_DATA._C_gcc_except_ta 1 0x1232e92d"
"f section.114.__LTC_DATA.__fix 1 0x1257b342"
```

rabin2用法举例：MaskPro.dylib

-I

```
➜ DynamicLibraries rabin2 -I MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_I_identi
fication.txt
```

输出：

```
arch     arm
baddr    0x0
binsz    311296
bintype  mach0
bits     32
canary   true
class    MACH0
crypto   false
endian   little
havecode true
laddr    0x0
lang     objc with blocks
linenum  false
lsyms    false
machine  v7
maxopsz  4
minopsz  4
nx       false
os       ios
pcalign  4
pic      false
relocs   false
sanitiz  false
static   false
stripped true
subsys   darwin
va       true
```

-i

```
➜ DynamicLibraries rabin2 -i MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_i_import
s.txt
```

输出：

```
[Imports]
nth vaddr      bind type          lib name
―――――――――――――――――――――――――――――――――――――――――――
0   0x0003b124 NONE FUNC              CC_MD5
```

```
0x0003b134 NONE FUNC                MGCopyAnswer
0x0003b144 NONE FUNC                MSHookFunction
0x0003b154 NONE FUNC                MSHookMessageEx
0x0003b164 NONE FUNC                NSClassFromString
0x00000000 NONE FUNC                NSFileSystemFreeSize
0x0003b174 NONE FUNC                NSHomeDirectory
0x00000000 NONE OBJC_CLASS          ASIdentifierManager
0x00000000 NONE OBJC_CLASS          NSBundle
0x00000000 NONE OBJC_CLASS          NSData
0x00000000 NONE OBJC_CLASS          NSDate
0x00000000 NONE OBJC_CLASS          NSDateFormatter
0x00000000 NONE OBJC_CLASS          NSDictionary
0x00000000 NONE OBJC_CLASS          NSFileManager
0x00000000 NONE OBJC_CLASS          NSJSONSerialization
0x00000000 NONE OBJC_CLASS          NSMutableData
0x00000000 NONE OBJC_CLASS          NSMutableDictionary
0x00000000 NONE OBJC_CLASS          NSMutableString
0x00000000 NONE OBJC_CLASS          NSMutableURLRequest
0x00000000 NONE OBJC_CLASS          NSNumber
0x00000000 NONE OBJC_CLASS          NSObject
0x00000000 NONE OBJC_CLASS          NSString
0x00000000 NONE OBJC_CLASS          NSTimeZone
0x00000000 NONE OBJC_CLASS          NSURL
0x00000000 NONE OBJC_CLASS          NSURLConnection
0x00000000 NONE OBJC_CLASS          NSURLRequest
0x00000000 NONE OBJC_CLASS          NSURLSession
0x00000000 NONE OBJC_CLASS          NSURLSessionConfiguration
0x00000000 NONE OBJC_CLASS          UIDevice
0x00000000 NONE OBJC_METACLASS      NSObject
0x0003b184 NONE FUNC                _Block_object_assign
0x0003b194 NONE FUNC                _Block_object_dispose
0x00000000 NONE FUNC                _NSConcreteGlobalBlock
0x00000000 NONE FUNC                _NSConcreteStackBlock
0x0003b1a4 NONE FUNC                _Unwind_SjLj_Register
0x0003b1b4 NONE FUNC                _Unwind_SjLj_Resume
0x0003b1c4 NONE FUNC                _Unwind_SjLj_Unregister
0x00000000 NONE FUNC                __CFConstantStringClassReference
0x0003b1d4 NONE FUNC                __assert_rtn
0x00000000 NONE FUNC                __gxx_personality_sj0
0x00000000 NONE FUNC                __objc_personality_v0
0x0003b1e4 NONE FUNC                __stack_chk_fail
0x00000000 NONE FUNC                __stack_chk_guard
0x0003b1f4 NONE FUNC                _dyld_get_image_vmaddr_slide
0x00000000 NONE FUNC                _objc_empty_cache
0x0003b204 NONE FUNC                dispatch_async
0x0003b214 NONE FUNC                dispatch_get_global_queue
0x0003b224 NONE FUNC                dispatch_semaphore_create
0x0003b234 NONE FUNC                dispatch_semaphore_signal
0x0003b244 NONE FUNC                dispatch_semaphore_wait
0x0003b254 NONE FUNC                dispatch_time
0x0003b264 NONE FUNC                dlclose
0x0003b274 NONE FUNC                dlopen
0x0003b284 NONE FUNC                dlsym
0x0003b294 NONE FUNC                exit
0x0003b2a4 NONE FUNC                free
0x0003b2b4 NONE FUNC                getpid
```

```
57  0x0003b2c4 NONE FUNC              ioctl
58  0x0003b2d4 NONE FUNC              isatty
59  0x0003b2e4 NONE FUNC              malloc
60  0x0003b2f4 NONE FUNC              memset
61  0x0003b304 NONE FUNC              objc_autorelease
62  0x0003b314 NONE FUNC              objc_autoreleaseReturnValue
63  0x0003b324 NONE FUNC              objc_getClass
64  0x0003b334 NONE FUNC              objc_msgSend
65  0x0003b344 NONE FUNC              objc_release
66  0x0003b354 NONE FUNC              objc_retain
67  0x0003b364 NONE FUNC              objc_retainAutorelease
68  0x0003b374 NONE FUNC              objc_retainAutoreleasedReturnValue
69  0x0003b384 NONE FUNC              perror
70  0x0003b394 NONE FUNC              pthread_create
71  0x0003b3a4 NONE FUNC              sleep
72  0x0003b3b4 NONE FUNC              strstr
73  0x0003b3c4 NONE FUNC              syscall
74  0x0003b3d4 NONE FUNC              sysctl
75  0x0003b3e4 NONE FUNC              uname
76  0x00000000 NONE FUNC              dyld_stub_binder
```

-E

```
➜  DynamicLibraries rabin2 -E MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_E_exports.txt
```

输出:

```
[Exports]

nth paddr      vaddr      bind   type size lib name
―――――――――――――――――――――――――――――――――――――――――――――――――――――
0    0x0004089c 0x0003c89c GLOBAL FUNC 0        _OBJC_CLASS_$_NbGzxsksqtAxgN
1    0x0004084c 0x0003c84c GLOBAL FUNC 0        _OBJC_CLASS_$_NxNXRxsbBxexSx
2    0x00040874 0x0003c874 GLOBAL FUNC 0        _OBJC_CLASS_$_daAxbxbayGwxtxdcca
3    0x000408c4 0x0003c8c4 GLOBAL FUNC 0        _OBJC_CLASS_$_xrxleWZnuCXPEx
4    0x000408ec 0x0003c8ec GLOBAL FUNC 0        _OBJC_CLASS_$_xxWxKxrETCxJpx
5    0x00040888 0x0003c888 GLOBAL FUNC 0        _OBJC_METACLASS_$_NbGzxsksqtAxgN
6    0x00040838 0x0003c838 GLOBAL FUNC 0        _OBJC_METACLASS_$_NxNXRxsbBxexSx
7    0x00040860 0x0003c860 GLOBAL FUNC 0        _OBJC_METACLASS_$_daAxbxbayGwxtxdcca
8    0x000408b0 0x0003c8b0 GLOBAL FUNC 0        _OBJC_METACLASS_$_xrxleWZnuCXPEx
9    0x000408d8 0x0003c8d8 GLOBAL FUNC 0        _OBJC_METACLASS_$_xxWxKxrETCxJpx
10   0x00043420 0x0003f420 GLOBAL FUNC 0        _g_slide
11   0x00043564 0x0003f564 GLOBAL FUNC 0        _x
12   0x00043568 0x0003f568 GLOBAL FUNC 0        _x.146
13   0x0004356c 0x0003f56c GLOBAL FUNC 0        _x.148
...
119  0x00043444 0x0003f444 GLOBAL FUNC 0        _y.380
120  0x00043448 0x0003f448 GLOBAL FUNC 0        _y.382
```

-l

```
➜  DynamicLibraries rabin2 -l MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_l_librar
ies.txt
```

输出：

```
[Linked libraries]
/System/Library/Frameworks/AdSupport.framework/AdSupport
/usr/lib/libMobileGestalt.dylib
/System/Library/Frameworks/UIKit.framework/UIKit
/System/Library/Frameworks/Foundation.framework/Foundation
/Library/Frameworks/CydiaSubstrate.framework/CydiaSubstrate
/usr/lib/libobjc.A.dylib
/usr/lib/libc++.1.dylib
/usr/lib/libSystem.B.dylib
/System/Library/Frameworks/CoreFoundation.framework/CoreFoundation

9 libraries
```

`-z`

```
➜  DynamicLibraries rabin2 -z MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_z_string
s.txt
```

输出：

```
[Strings]
nth paddr      vaddr      len size section                 type  string
―――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――――

0   0x0003b634 0x0003b634 13  14   3.__TEXT.__objc_methname  ascii currentDevice
1   0x0003b642 0x0003b642 4   5    3.__TEXT.__objc_methname  ascii name
2   0x0003b647 0x0003b647 13  14   3.__TEXT.__objc_methname  ascii systemVersion
3   0x0003b655 0x0003b655 10  11   3.__TEXT.__objc_methname  ascii systemName
4   0x0003b660 0x0003b660 14  15   3.__TEXT.__objc_methname  ascii xJWlxsPxxExAux
5   0x0003b66f 0x0003b66f 19  20   3.__TEXT.__objc_methname  ascii identifierForVendor
6   0x0003b683 0x0003b683 10  11   3.__TEXT.__objc_methname  ascii UUIDString
7   0x0003b68e 0x0003b68e 13  14   3.__TEXT.__objc_methname  ascii sharedManager
8   0x0003b69c 0x0003b69c 21  22   3.__TEXT.__objc_methname  ascii advertisingIdentifie
r
9   0x0003b6b2 0x0003b6b2 29  30   3.__TEXT.__objc_methname  ascii dictionaryWithObject
sAndKeys:
10  0x0003b6d0 0x0003b6d0 14  15   3.__TEXT.__objc_methname  ascii URLWithString:
11  0x0003b6df 0x0003b6df 39  40   3.__TEXT.__objc_methname  ascii stringWithContentsOf
URL:encoding:error:
12  0x0003b707 0x0003b707 10  11   3.__TEXT.__objc_methname  ascii hasPrefix:
13  0x0003b712 0x0003b712 24  25   3.__TEXT.__objc_methname  ascii deleteCharactersInRa
nge:
14  0x0003b72b 0x0003b72b 6   7    3.__TEXT.__objc_methname  ascii length
15  0x0003b732 0x0003b732 17  18   3.__TEXT.__objc_methname  ascii substringToIndex:
16  0x0003b744 0x0003b744 18  19   3.__TEXT.__objc_methname  ascii dataUsingEncoding:
17  0x0003b757 0x0003b757 33  34   3.__TEXT.__objc_methname  ascii JSONObjectWithData:o
ptions:error:
```

```
18  0x0003b779 0x0003b779 24  25   3.__TEXT.__objc_methname  ascii objectForKeyedSubscr
ipt:
19  0x0003b792 0x0003b792 27  28   3.__TEXT.__objc_methname  ascii stringWithCString:en
coding:
20  0x0003b7ae 0x0003b7ae 16  17   3.__TEXT.__objc_methname  ascii isEqualToString:
21  0x0003b7bf 0x0003b7bf 14  15   3.__TEXT.__objc_methname  ascii eKGEGSRRxxxPxt
22  0x0003b7ce 0x0003b7ce 14  15   3.__TEXT.__objc_methname  ascii PHcNExxxUJIxxH
23  0x0003b7dd 0x0003b7dd 14  15   3.__TEXT.__objc_methname  ascii graGqxxPtxaoBY
24  0x0003b7ec 0x0003b7ec 14  15   3.__TEXT.__objc_methname  ascii xHvTCxxxxxXVxm
25  0x0003b7fb 0x0003b7fb 15  16   3.__TEXT.__objc_methname  ascii bundleWithPath:
26  0x0003b80b 0x0003b80b 4   5    3.__TEXT.__objc_methname  ascii load
27  0x0003b810 0x0003b810 18  19   3.__TEXT.__objc_methname  ascii numberWithInteger:
28  0x0003b823 0x0003b823 63  64   3.__TEXT.__objc_methname  ascii setAppWirelessDataOp
tion:forBundleIdentifier:completionHandler:
29  0x0003b863 0x0003b863 14  15   3.__TEXT.__objc_methname  ascii numberWithInt:
30  0x0003b872 0x0003b872 64  65   3.__TEXT.__objc_methname  ascii setAppCellularDataEn
abled:forBundleIdentifier:completionHandler:
31  0x0003b8b3 0x0003b8b3 14  15   3.__TEXT.__objc_methname  ascii sharedInstance
32  0x0003b8c2 0x0003b8c2 40  41   3.__TEXT.__objc_methname  ascii setUsagePoliciesForB
undle:cellular:wifi:
33  0x0003b8eb 0x0003b8eb 40  41   3.__TEXT.__objc_methname  ascii resolveNetworkProblm
eForAppWithBundleId:
34  0x0003b914 0x0003b914 4   5    3.__TEXT.__objc_methname  ascii date
35  0x0003b919 0x0003b919 5   6    3.__TEXT.__objc_methname  ascii alloc
36  0x0003b91f 0x0003b91f 4   5    3.__TEXT.__objc_methname  ascii init
37  0x0003b924 0x0003b924 17  18   3.__TEXT.__objc_methname  ascii timeZoneWithName:
38  0x0003b936 0x0003b936 12  13   3.__TEXT.__objc_methname  ascii setTimeZone:
39  0x0003b943 0x0003b943 14  15   3.__TEXT.__objc_methname  ascii setDateFormat:
40  0x0003b952 0x0003b952 15  16   3.__TEXT.__objc_methname  ascii stringFromDate:
41  0x0003b962 0x0003b962 14  15   3.__TEXT.__objc_methname  ascii defaultManager
42  0x0003b971 0x0003b971 36  37   3.__TEXT.__objc_methname  ascii attributesOfFileSyst
emForPath:error:
43  0x0003b996 0x0003b996 13  14   3.__TEXT.__objc_methname  ascii objectForKey:
44  0x0003b9a4 0x0003b9a4 11  12   3.__TEXT.__objc_methname  ascii stringValue
45  0x0003b9b0 0x0003b9b0 40  41   3.__TEXT.__objc_methname  ascii initWithURL:cachePol
icy:timeoutInterval:
46  0x0003b9d9 0x0003b9d9 47  48   3.__TEXT.__objc_methname  ascii sendSynchronousReque
st:returningResponse:error:
47  0x0003ba09 0x0003ba09 28  29   3.__TEXT.__objc_methname  ascii componentsSeparatedB
yString:
48  0x0003ba26 0x0003ba26 5   6    3.__TEXT.__objc_methname  ascii count
49  0x0003ba2c 0x0003ba2c 25  26   3.__TEXT.__objc_methname  ascii objectAtIndexedSubsc
ript:
50  0x0003ba46 0x0003ba46 12  13   3.__TEXT.__objc_methname  ascii integerValue
51  0x0003ba53 0x0003ba53 18  19   3.__TEXT.__objc_methname  ascii isValidJSONObject:
52  0x0003ba66 0x0003ba66 33  34   3.__TEXT.__objc_methname  ascii dataWithJSONObject:o
ptions:error:
53  0x0003ba88 0x0003ba88 22  23   3.__TEXT.__objc_methname  ascii initWithData:encodin
g:
54  0x0003ba9f 0x0003ba9f 7   8    3.__TEXT.__objc_methname  ascii setURL:
55  0x0003baa7 0x0003baa7 19  20   3.__TEXT.__objc_methname  ascii setTimeoutInterval:
56  0x0003babb 0x0003babb 14  15   3.__TEXT.__objc_methname  ascii setHTTPMethod:
57  0x0003baca 0x0003baca 28  29   3.__TEXT.__objc_methname  ascii setValue:forHTTPHead
erField:
58  0x0003bae7 0x0003bae7 17  18   3.__TEXT.__objc_methname  ascii fileExistsAtPath:
59  0x0003baf9 0x0003baf9 29  30   3.__TEXT.__objc_methname  ascii ephemeralSessionConf
```

```
iguration
60  0x0003bb17 0x0003bb17 36  37   3.__TEXT.__objc_methname  ascii dictionaryWithObject
s:forKeys:count:
61  0x0003bb3c 0x0003bb3c 29  30   3.__TEXT.__objc_methname  ascii setConnectionProxyDi
ctionary:
62  0x0003bb5a 0x0003bb5a 25  26   3.__TEXT.__objc_methname  ascii sessionWithConfigura
tion:
63  0x0003bb74 0x0003bb74 13  14   3.__TEXT.__objc_methname  ascii sharedSession
64  0x0003bb82 0x0003bb82 10  11   3.__TEXT.__objc_methname  ascii statusCode
65  0x0003bb8d 0x0003bb8d 38  39   3.__TEXT.__objc_methname  ascii dataTaskWithRequest:
completionHandler:
66  0x0003bbb4 0x0003bbb4 6   7    3.__TEXT.__objc_methname  ascii resume
67  0x0003bbbb 0x0003bbbb 17  18   3.__TEXT.__objc_methname  ascii stringWithFormat:
68  0x0003bbcd 0x0003bbcd 12  13   3.__TEXT.__objc_methname  ascii setHTTPBody:
69  0x0003bbda 0x0003bbda 29  30   3.__TEXT.__objc_methname  ascii fileExistsAtPath:isD
irectory:
70  0x0003bbf8 0x0003bbf8 23  24   3.__TEXT.__objc_methname  ascii dataWithContentsOfFi
le:
71  0x0003bc10 0x0003bc10 5   6    3.__TEXT.__objc_methname  ascii bytes
72  0x0003bc16 0x0003bc16 19  20   3.__TEXT.__objc_methname  ascii stringWithCapacity:
73  0x0003bc2a 0x0003bc2a 13  14   3.__TEXT.__objc_methname  ascii appendFormat:
74  0x0003bc38 0x0003bc38 14  15   3.__TEXT.__objc_methname  ascii exASdcLNKxJfAM
75  0x0003bc47 0x0003bc47 14  15   3.__TEXT.__objc_methname  ascii xKxcixmmxdxPxZ
76  0x0003bc56 0x0003bc56 15  16   3.__TEXT.__objc_methname  ascii xKxcixmmxdxPxZ:
77  0x0003bc66 0x0003bc66 15  16   3.__TEXT.__objc_methname  ascii MxJgqzxvqFtQxV:
78  0x0003bc76 0x0003bc76 37  38   3.__TEXT.__objc_methname  ascii dVxAxlNLgYxxYh:compa
reVersionNumberB:
79  0x0003bc9c 0x0003bc9c 15  16   3.__TEXT.__objc_methname  ascii xxfxuGtxxxtRxx:
80  0x0003bcac 0x0003bcac 15  16   3.__TEXT.__objc_methname  ascii OxxXdjxnoanKzL:
81  0x0003bcbc 0x0003bcbc 15  16   3.__TEXT.__objc_methname  ascii NZufxnxxcFkCxb:
82  0x0003bccc 0x0003bccc 16  17   3.__TEXT.__objc_methname  ascii fcVwxqxhwdnpxa::
83  0x0003bcdd 0x0003bcdd 18  19   3.__TEXT.__objc_methname  ascii emxqoxrXzxPUvx::::
84  0x0003bcf0 0x0003bcf0 15  16   3.__TEXT.__objc_methname  ascii xxxxtpHhXMwfjx:
85  0x0003bd00 0x0003bd00 49  50   3.__TEXT.__objc_methname  ascii initWithBytesNoCopy:
length:encoding:freeWhenDone:
86  0x0003bd32 0x0003bd32 17  18   3.__TEXT.__objc_methname  ascii characterAtIndex:
87  0x0003bd44 0x0003bd44 15  16   3.__TEXT.__objc_methname  ascii xMRExdxMxkhxxx:
88  0x0003bd54 0x0003bd54 19  20   3.__TEXT.__objc_methname  ascii appendBytes:length:
89  0x0003bd68 0x0003bd68 15  16   3.__TEXT.__objc_methname  ascii LUxxxfWDhvpGxJ:
90  0x0003bd78 0x0003bd78 15  16   3.__TEXT.__objc_methname  ascii fexkIvlCfxhxsy:
91  0x0003bd88 0x0003bd88 14  15   3.__TEXT.__objc_methname  ascii MjOhDBJSUcxxxu
92  0x0003bd97 0x0003bd97 14  15   3.__TEXT.__objc_methname  ascii gxcyxmxxxIxNux
93  0x0003bda6 0x0003bda6 14  15   3.__TEXT.__objc_methname  ascii OxlpxkxxFLzEnr
94  0x0003bdb5 0x0003bdb5 14  15   3.__TEXT.__objc_methname  ascii fDjCxxvxTjxWeL
95  0x0003bdc4 0x0003bdc4 14  15   3.__TEXT.__objc_methname  ascii xouxVIvlOloYFX
96  0x0003bdd3 0x0003bdd3 14  15   3.__TEXT.__objc_methname  ascii xtxNTxxxsxVGxk
97  0x0003bde2 0x0003bde2 10  11   3.__TEXT.__objc_methname  ascii floatValue
98  0x0003bded 0x0003bded 10  11   3.__TEXT.__objc_methname  ascii mainBundle
99  0x0003bdf8 0x0003bdf8 16  17   3.__TEXT.__objc_methname  ascii bundleIdentifier
100 0x0003be09 0x0003be09 15  16   3.__TEXT.__objc_methname  ascii jailBrokenMask:
101 0x0003be19 0x0003be19 8   9    3.__TEXT.__objc_methname  ascii loadView
102 0x0003be22 0x0003be22 12  13   3.__TEXT.__objc_methname  ascii currentTitle
103 0x0003be2f 0x0003be2f 21  22   3.__TEXT.__objc_methname  ascii dataWithBytes:length
:
104 0x0003be45 0x0003be45 10  11   3.__TEXT.__objc_methname  ascii UTF8String
105 0x0003be50 0x0003be50 43  44   3.__TEXT.__objc_methname  ascii requestWithURL:cache
```

```
Policy:timeoutInterval:
0   0x0003be7d 0x0003be7d 45  46   4.__TEXT.__cstring        ascii v16@?0@"NSData"4@"NS
URLResponse"8@"NSError"12
1   0x0003beab 0x0003beab 5   6    4.__TEXT.__cstring        ascii v4@?0
0   0x0003beb1 0x0003beb1 14  15   5.__TEXT.__objc_classname ascii NxNXRxsbBxexSx
1   0x0003bec0 0x0003bec0 18  19   5.__TEXT.__objc_classname ascii daAxbxbayGwxtxdcca
2   0x0003bed3 0x0003bed3 14  15   5.__TEXT.__objc_classname ascii NbGzxsksqtAxgN
3   0x0003bee2 0x0003bee2 14  15   5.__TEXT.__objc_classname ascii xrxleWZnuCXPEx
4   0x0003bef1 0x0003bef1 14  15   5.__TEXT.__objc_classname ascii xxWxKxrETCxJpx
0   0x0003bf00 0x0003bf00 6   7    6.__TEXT.__objc_methtype  ascii @8@0:4
1   0x0003bf07 0x0003bf07 9   10   6.__TEXT.__objc_methtype  ascii v12@0:4@8
2   0x0003bf11 0x0003bf11 15  16   6.__TEXT.__objc_methtype  ascii v20@0:4@8@12@16
3   0x0003bf21 0x0003bf21 15  16   6.__TEXT.__objc_methtype  ascii v20@0:4@8c12c16
4   0x0003bf31 0x0003bf31 9   10   6.__TEXT.__objc_methtype  ascii @12@0:4@8
5   0x0003bf3b 0x0003bf3b 12  13   6.__TEXT.__objc_methtype  ascii i16@0:4@8@12
6   0x0003bf48 0x0003bf48 13  14   6.__TEXT.__objc_methtype  ascii @16@0:4@8^i12
7   0x0003bf56 0x0003bf56 19  20   6.__TEXT.__objc_methtype  ascii @24@0:4@8@12^i16i20
8   0x0003bf6a 0x0003bf6a 9   10   6.__TEXT.__objc_methtype  ascii i12@0:4c8
```

`-s`

```
➜  DynamicLibraries rabin2 -s MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_s_symbol
s.txt
```

输出：

```
[Symbols]

nth paddr       vaddr      bind   type size lib name
――――――――――――――――――――――――――――――――――――――――――――――――――――
0    0x0004089c 0x0003c89c GLOBAL FUNC 0        _OBJC_CLASS_$_NbGzxsksqtAxgN
1    0x0004084c 0x0003c84c GLOBAL FUNC 0        _OBJC_CLASS_$_NxNXRxsbBxexSx
2    0x00040874 0x0003c874 GLOBAL FUNC 0        _OBJC_CLASS_$_daAxbxbayGwxtxdcca
3    0x000408c4 0x0003c8c4 GLOBAL FUNC 0        _OBJC_CLASS_$_xrxleWZnuCXPEx
4    0x000408ec 0x0003c8ec GLOBAL FUNC 0        _OBJC_CLASS_$_xxWxKxrETCxJpx
5    0x00040888 0x0003c888 GLOBAL FUNC 0        _OBJC_METACLASS_$_NbGzxsksqtAxgN
6    0x00040838 0x0003c838 GLOBAL FUNC 0        _OBJC_METACLASS_$_NxNXRxsbBxexSx
7    0x00040860 0x0003c860 GLOBAL FUNC 0        _OBJC_METACLASS_$_daAxbxbayGwxtxdcca
8    0x000408b0 0x0003c8b0 GLOBAL FUNC 0        _OBJC_METACLASS_$_xrxleWZnuCXPEx
9    0x000408d8 0x0003c8d8 GLOBAL FUNC 0        _OBJC_METACLASS_$_xxWxKxrETCxJpx
10   0x00043420 0x0003f420 GLOBAL FUNC 0        _g_slide
11   0x00043564 0x0003f564 GLOBAL FUNC 0        _x
12   0x00043568 0x0003f568 GLOBAL FUNC 0        _x.146
13   0x0004356c 0x0003f56c GLOBAL FUNC 0        _x.148
...
120  0x00043448 0x0003f448 GLOBAL FUNC 0        _y.382
121  0x00004000 0x05614542 LOCAL  FUNC 0        radr://5614542
122  0x0003f124 0x0003b124 LOCAL  FUNC 0        imp.CC_MD5
123  0x0003f134 0x0003b134 LOCAL  FUNC 0        imp.MGCopyAnswer
124  0x0003f144 0x0003b144 LOCAL  FUNC 0        imp.MSHookFunction
125  0x0003f154 0x0003b154 LOCAL  FUNC 0        imp.MSHookMessageEx
126  0x0003f164 0x0003b164 LOCAL  FUNC 0        imp.NSClassFromString
127  0x0003f174 0x0003b174 LOCAL  FUNC 0        imp.NSHomeDirectory
```

```
128  0x0003f184 0x0003b184 LOCAL  FUNC 0        imp._Block_object_assign
129  0x0003f194 0x0003b194 LOCAL  FUNC 0        imp._Block_object_dispose
130  0x0003f1a4 0x0003b1a4 LOCAL  FUNC 0        imp._Unwind_SjLj_Register
131  0x0003f1b4 0x0003b1b4 LOCAL  FUNC 0        imp._Unwind_SjLj_Resume
132  0x0003f1c4 0x0003b1c4 LOCAL  FUNC 0        imp._Unwind_SjLj_Unregister
133  0x0003f1d4 0x0003b1d4 LOCAL  FUNC 0        imp.__assert_rtn
134  0x0003f1e4 0x0003b1e4 LOCAL  FUNC 0        imp.__stack_chk_fail
135  0x0003f1f4 0x0003b1f4 LOCAL  FUNC 0        imp._dyld_get_image_vmaddr_slide
136  0x0003f204 0x0003b204 LOCAL  FUNC 0        imp.dispatch_async
137  0x0003f214 0x0003b214 LOCAL  FUNC 0        imp.dispatch_get_global_queue
138  0x0003f224 0x0003b224 LOCAL  FUNC 0        imp.dispatch_semaphore_create
139  0x0003f234 0x0003b234 LOCAL  FUNC 0        imp.dispatch_semaphore_signal
140  0x0003f244 0x0003b244 LOCAL  FUNC 0        imp.dispatch_semaphore_wait
141  0x0003f254 0x0003b254 LOCAL  FUNC 0        imp.dispatch_time
142  0x0003f264 0x0003b264 LOCAL  FUNC 0        imp.dlclose
143  0x0003f274 0x0003b274 LOCAL  FUNC 0        imp.dlopen
144  0x0003f284 0x0003b284 LOCAL  FUNC 0        imp.dlsym
145  0x0003f294 0x0003b294 LOCAL  FUNC 0        imp.exit
146  0x0003f2a4 0x0003b2a4 LOCAL  FUNC 0        imp.free
147  0x0003f2b4 0x0003b2b4 LOCAL  FUNC 0        imp.getpid
148  0x0003f2c4 0x0003b2c4 LOCAL  FUNC 0        imp.ioctl
149  0x0003f2d4 0x0003b2d4 LOCAL  FUNC 0        imp.isatty
150  0x0003f2e4 0x0003b2e4 LOCAL  FUNC 0        imp.malloc
151  0x0003f2f4 0x0003b2f4 LOCAL  FUNC 0        imp.memset
152  0x0003f304 0x0003b304 LOCAL  FUNC 0        imp.objc_autorelease
153  0x0003f314 0x0003b314 LOCAL  FUNC 0        imp.objc_autoreleaseReturnValue
154  0x0003f324 0x0003b324 LOCAL  FUNC 0        imp.objc_getClass
155  0x0003f334 0x0003b334 LOCAL  FUNC 0        imp.objc_msgSend
156  0x0003f344 0x0003b344 LOCAL  FUNC 0        imp.objc_release
157  0x0003f354 0x0003b354 LOCAL  FUNC 0        imp.objc_retain
158  0x0003f364 0x0003b364 LOCAL  FUNC 0        imp.objc_retainAutorelease
159  0x0003f374 0x0003b374 LOCAL  FUNC 0        imp.objc_retainAutoreleasedReturnValue
160  0x0003f384 0x0003b384 LOCAL  FUNC 0        imp.perror
161  0x0003f394 0x0003b394 LOCAL  FUNC 0        imp.pthread_create
162  0x0003f3a4 0x0003b3a4 LOCAL  FUNC 0        imp.sleep
163  0x0003f3b4 0x0003b3b4 LOCAL  FUNC 0        imp.strstr
164  0x0003f3c4 0x0003b3c4 LOCAL  FUNC 0        imp.syscall
165  0x0003f3d4 0x0003b3d4 LOCAL  FUNC 0        imp.sysctl
166  0x0003f3e4 0x0003b3e4 LOCAL  FUNC 0        imp.uname
167  0x00004160 0x00004160 LOCAL  FUNC 0        func.00004161
168  0x00005b10 0x00005b10 LOCAL  FUNC 0        func.00005b11
...
223  0x00039220 0x00039220 LOCAL  FUNC 0        func.00039221
224  0x0003939e 0x0003939e LOCAL  FUNC 0        func.0003939f
225  0x000394dc 0x000394dc LOCAL  FUNC 0        func.000394dd
```

-S

```
➜  DynamicLibraries rabin2 -S MaskPro.dylib > MaskProDylib/MaskProDylib_rabin2_S_sectio
ns.txt
```

输出：

```
[Sections]

nth paddr          size vaddr         vsize perm name
―――――――――――――――――――――――――――――――――――――――――――――――――――――
0   0x00004160  0x36fc4 0x00004160  0x36fc4 -r-x 0.__TEXT.__text
1   0x0003b124    0x2d0 0x0003b124    0x2d0 -r-x 1.__TEXT.__picsymbolstub4
2   0x0003b3f4    0x240 0x0003b3f4    0x240 -r-x 2.__TEXT.__stub_helper
3   0x0003b634    0x848 0x0003b634    0x848 -r-x 3.__TEXT.__objc_methname
4   0x0003be7c     0x35 0x0003be7c     0x35 -r-x 4.__TEXT.__cstring
5   0x0003beb1     0x4f 0x0003beb1     0x4f -r-x 5.__TEXT.__objc_classname
6   0x0003bf00     0x74 0x0003bf00     0x74 -r-x 6.__TEXT.__objc_methtype
7   0x0003bf74     0x8c 0x0003bf74     0x8c -r-x 7.__TEXT.__gcc_except_tab
8   0x0003c000    0x1d0 0x0003c000    0x1d0 -rw- 8.__DATA.__nl_symbol_ptr
9   0x0003c1d0     0xb4 0x0003c1d0     0xb4 -rw- 9.__DATA.__la_symbol_ptr
10  0x0003c284      0x4 0x0003c284      0x4 -rw- 10.__DATA.__mod_init_func
11  0x0003c288     0x84 0x0003c288     0x84 -rw- 11.__DATA.__const
12  0x0003c30c     0x10 0x0003c30c     0x10 -rw- 12.__DATA.__cfstring
13  0x0003c31c     0x14 0x0003c31c     0x14 -rw- 13.__DATA.__objc_classlist
14  0x0003c330      0x8 0x0003c330      0x8 -rw- 14.__DATA.__objc_imageinfo
15  0x0003c338    0x328 0x0003c338    0x328 -rw- 15.__DATA.__objc_const
16  0x0003c660    0x170 0x0003c660    0x170 -rw- 16.__DATA.__objc_selrefs
17  0x0003c7d0     0x68 0x0003c7d0     0x68 -rw- 17.__DATA.__objc_classrefs
18  0x0003c838     0xc8 0x0003c838     0xc8 -rw- 18.__DATA.__objc_data
19  0x0003c900   0x2a24 0x0003c900   0x2a24 -rw- 19.__DATA.__data
20  0x00000000      0x0 0x0003f324     0xfc -rw- 20.__DATA.__bss
21  0x00000000      0x0 0x0003f420    0x1bc -rw- 21.__DATA.__common
22  0x00040000      0x1 0x00040000      0x1 -rw- 22.__LLVM.__bundle
```

rabin2的help语法

```
➜  ~ rabin2 --help
rabin2: illegal option -- -
Usage: rabin2 [-AcdeEghHiIjlLMqrRsSUvVxzZ] [-@ at] [-a arch] [-b bits] [-B addr]
              [-C F:C:D] [-f str] [-m addr] [-n str] [-N m:M] [-P[-P] pdb]
              [-o str] [-O str] [-k query] [-D lang symname] file
 -@ [addr]       show section, symbol or import at addr
 -A              list sub-binaries and their arch-bits pairs
 -a [arch]       set arch (x86, arm, .. or <arch>_<bits>)
 -b [bits]       set bits (32, 64 ...)
 -B [addr]       override base address (pie bins)
 -c              list classes
 -cc             list classes in header format
 -C [fmt:C:D]    create [elf,mach0,pe] with Code and Data hexpairs (see -a)
 -d              show debug/dwarf information
 -D lang name    demangle symbol name (-D all for bin.demangle=true)
 -e              entrypoint
 -ee             constructor/destructor entrypoints
 -E              globally exportable symbols
 -f [str]        select sub-bin named str
 -F [binfmt]     force to use that bin plugin (ignore header check)
 -g              same as -SMZIHVResizcld -SS -SSS -ee (show all info)
 -G [addr]       load address . offset to header
 -h              this help message
 -H              header fields
 -i              imports (symbols imported from libraries)
 -I              binary info
 -j              output in json
 -k [sdb-query]  run sdb query. for example: '*'
 -K [algo]       calculate checksums (md5, sha1, ..)
 -l              linked libraries
 -L [plugin]     list supported bin plugins or plugin details
 -m [addr]       show source line at addr
 -M              main (show address of main symbol)
 -n [str]        show section, symbol or import named str
 -N [min:max]    force min:max number of chars per string (see -z and -zz)
 -o [str]        output file/folder for write operations (out by default)
 -O [str]        write/extract operations (-O help)
 -p              show physical addresses
 -P              show debug/pdb information
 -PP             download pdb file for binary
 -q              be quiet, just show fewer data
 -qq             show less info (no offset/size for -z for ex.)
 -Q              show load address used by dlopen (non-aslr libs)
 -r              radare output
 -R              relocations
 -s              symbols
 -S              sections
 -SS             segments
 -SSS            sections mapping to segments
 -t              display file hashes
 -T              display file signature
```

```
  -u                unfiltered (no rename duplicated symbols/sections)
  -U                resoUrces
  -v                display version and quit
  -V                Show binary version information
  -w                display try/catch blocks
  -x                extract bins contained in file
  -X [fmt] [f] ..   package in fat or zip the given files and bins contained in file
  -z                strings (from data section)
  -zz               strings (from raw bins [e bin.rawstr=1])
  -zzz              dump raw strings to stdout (for huge files)
  -Z                guess size of binary program
 Environment:
  RABIN2_LANG:      e bin.lang         # assume lang for demangling
  RABIN2_NOPLUGINS: # do not load shared plugins (speedup loading)
  RABIN2_DEMANGLE=0:e bin.demangle     # do not demangle symbols
  RABIN2_MAXSTRBUF: e bin.maxstrbuf    # specify maximum buffer size
  RABIN2_STRFILTER: e bin.str.filter   #  r2 -qc 'e bin.str.filter=??' -
  RABIN2_STRPURGE:  e bin.str.purge    # try to purge false positives
  RABIN2_DEBASE64:  e bin.debase64     # try to debase64 all strings
  RABIN2_DMNGLRCMD: e bin.demanglercmd # try to purge false positives
  RABIN2_PDBSERVER: e pdb.server       # use alternative PDB server
  RABIN2_SYMSTORE:  e pdb.symstore     # path to downstream symbol store
  RABIN2_PREFIX:    e bin.prefix       # prefix symbols/sections/relocs with a specific
 string
  R2_CONFIG:        # sdb config file
```

jtool2

- `jtool2`
  - 旧版叫：`jtool`
  - 类似于 `otool` 的，解析查看 `Mach-O` 文件格式信息
    - 区别：添加了许多 `Mach-O` 相关的命令
      - `jtool` / `jtool2` 比 `otool` 功能更完善
  - 支持多种运行平台
    - `OS X` = `Mac`
    - `iOS`
    - `Linux`
  - 功能
    - in-binary search functionality
    - symbol injection
    - built-in disassembler functionality with (limited but constantly improving) emulation capabilities, which already outdo fancy commercial GUI disassemblers.
    - Color terminal output, enabled by JCOLOR=1
  - 资料
    - 官网
      - JTool2 - Taking the O out of otool - squared
        - http://www.newosxbook.com/tools/jtool.html

安装jtool2

`Mac` 中安装 `jtool2` ：

- Intel的CPU的Mac = Intel Mac
  - 方式1：`brew`

    ```
    brew install --cask jtool2
    ```

  - 方式2：官网下载二进制
    - 从JTool2官网下载jtool2.tgz
    - 解压得到：`jtool2` （和 `disarm` ）
      - 提示：可以把路径加到启动脚本的 `PATH` 中（再source），使得命令行中可以使用
- （M1/M2等）M系列CPU的Mac = Apple Silicon Mac

  ```
  brew tap excitedplus1s/repo/jtool2
  brew install --no-quarantine excitedplus1s/repo/jtool2
  ```

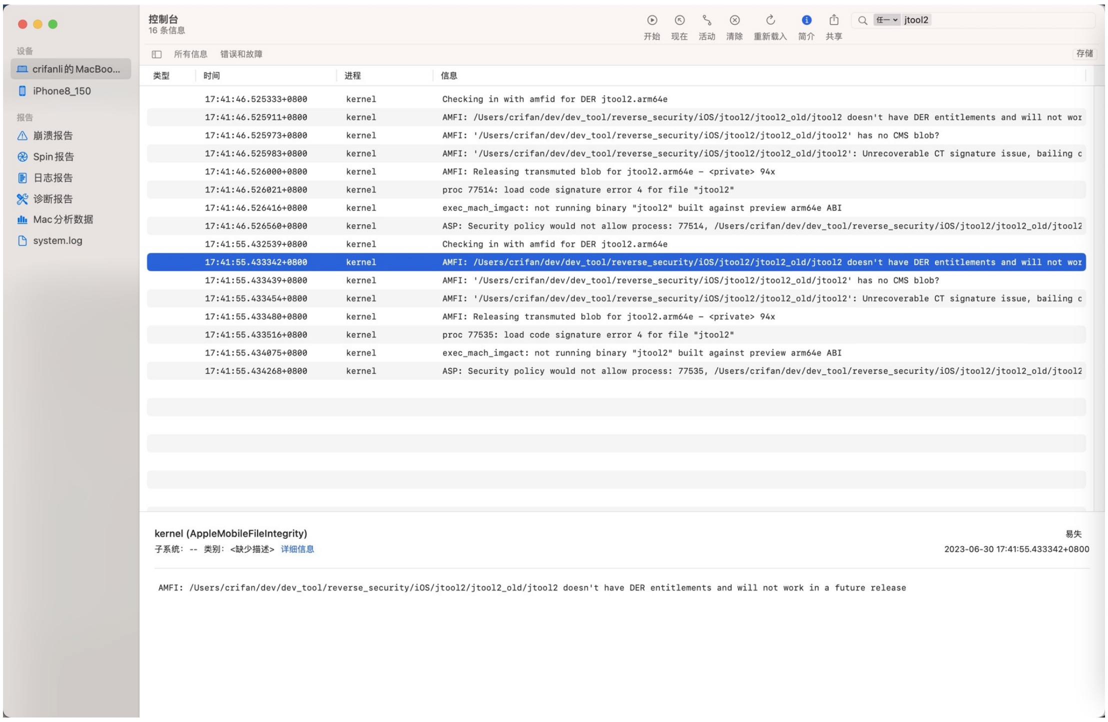
常见问题

killed

- 问题：`Mac M2 Max` + `macOS Ventura 13.2.1` 中，用brew安装的原始版本=官网版本的jtool2，运行

崩溃Killed

```
➜  ~ which jtool2
/usr/local/bin/jtool2
➜  ~ jtool2 --version
[1]    69975 killed     jtool2 --version
➜  ~ jtool2 --help
[1]    70025 killed     jtool2 --help
```

- 原因：签名问题
  - 找到崩溃日志，找到原因了
    - 


```
默认    17:41:55.432539+0800    kernel    Checking in with amfid for DER jtool2.arm64e
默认    17:41:55.433342+0800    kernel    AMFI: /Users/crifan/dev/dev_tool/reverse_security/iOS/jtool2/jtool2_old/jtool2 doesn't have DER entitlements and will not work in a future release
默认    17:41:55.433439+0800    kernel    AMFI: '/Users/crifan/dev/dev_tool/reverse_security/iOS/jtool2/jtool2_old/jtool2' has no CMS blob?
默认    17:41:55.433454+0800    kernel    AMFI: '/Users/crifan/dev/dev_tool/reverse_security/iOS/jtool2/jtool2_old/jtool2': Unrecoverable CT signature issue, bailing out.
默认    17:41:55.433480+0800    kernel    AMFI: Releasing transmuted blob for jtool2.arm64e - private 94x
默认    17:41:55.433516+0800    kernel    proc 77535: load code signature error 4 for file "jtool2"
默认    17:41:55.434075+0800    kernel    exec_mach_imgact: not running binary "jtool2" built against preview arm64e ABI
默认    17:41:55.434268+0800    kernel    ASP: Security policy would not allow process: 77535, /Users/crifan/dev/dev_tool/reverse_security/iOS/jtool2/jtool2_old/jtool2
```

- 解决办法：换装另外的版本：

- https://github.com/excitedplus1s/jtool2

  ```
  brew tap excitedplus1s/repo/jtool2
  brew install --no-quarantine excitedplus1s/repo/jtool2
  ```

- 即可正常使用jtool2

  ```
  ➜  jtool2 which jtool2
  /usr/local/bin/jtool2
  ➜  jtool2 jtool2 --version
  This is 2.1-The Resurgence compiled on Dec 21 2020 21:09:04
  ```

jtool2相关资料

- 官网
  - JTool2 - Taking the O out of otool - squared (newosxbook.com)

常见命令的常见用法举例

官网JTool2 - Taking the O out of otool - squared (newosxbook.com)中就有语法介绍：

```
* Otool Compatible options
* dyldinfo Compatible options
* Advanced options:
    * -pages (get layout)
    * -a (lookup address)
    * -S
* Code Singing options
    * --sig
    * --ent
    * --sign
* Objective-C
* Darn Cool Options
```

对应的别人的中文翻译：

【OSG】jtool - Taking the O out of otool(1)-iOS安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com

jtool2用法

- `-h` ：查看基本头文件header信息

  ```
  jtool2 -h yourBinary
  ```

- `-l` ：列出段

  ```
  jtool2 -l yourBinary
  ```

- `-L` ：查看使用了哪些共享库Library

  ```
  jtool2 -L yourBinary
  ```

- `-S` ：列出符号表Symbol == nm

  ```
  jtool2 -S yourBinary
  ```

- `--analyze` ：分析analyze -》 导出类和函数名等

  ```
  jtool2 --analyze yourBinary
  ```

- `--pages` ：显示layout

  ```
  jtool2 --pages yourBinary
  ```

jtool2用法举例

jtool2用法举例：AwemeCore

-h：查看header头信息

```
➜  AwemeCore jtool2 -h v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCo
re
Magic:    64-bit MachO (Little Endian)
Type:    dylib
CPU:    ARM64 (ARMv8)
Cmds:    133
Size:    18720
Flags:    0x910085
```

-l: list列出段

```
jtool2 -l v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore
```

输出内容：

```
➜  AwemeCore jtool2 -l ../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore
LC 00: LC_SEGMENT_64              Mem: 0x000000000-0x304000    __TEXT
    Mem: 0x00000b9b0-0x000013e70        __TEXT.__stub_helper    (Normal)
    Mem: 0x000013e70-0x000017e90        __TEXT.__const
    Mem: 0x000017e90-0x00001ad88        __TEXT.__swift5_typeref
    Mem: 0x00001ad88-0x00001d710        __TEXT.__swift5_fieldmd
    Mem: 0x00001d710-0x00001da48        __TEXT.__swift5_proto
    Mem: 0x00001da48-0x00001dcd4        __TEXT.__swift5_types
    Mem: 0x00001dcd4-0x00001dcd4        __TEXT.__cstring    (C-String Literals)
    Mem: 0x00001dcd4-0x00001dcd4        __TEXT.__objc_methname    (C-String Literals)
    Mem: 0x00001dcd4-0x00001dcd4        __TEXT.__objc_classname    (C-String Literals)
    Mem: 0x00001dcd4-0x00001dcd4        __TEXT.__objc_methtype    (C-String Literals)
    Mem: 0x00001dcd4-0x00001dd3c        __TEXT.__gcc_except_tab
    Mem: 0x00001dd40-0x00002136c        __TEXT.__swift5_reflstr
    Mem: 0x00002136c-0x000021524        __TEXT.__swift5_builtin
    Mem: 0x000021524-0x0000217dc        __TEXT.__swift5_assocty
    Mem: 0x0000217dc-0x0000233e8        __TEXT.__swift5_capture
    Mem: 0x0000233e8-0x000023448        __TEXT.__swift5_protos
    Mem: 0x000023448-0x000023448        __TEXT.__ustring
    Mem: 0x000023448-0x000023448        __TEXT.__text
    Mem: 0x000023448-0x0002c7fb8        __TEXT.__unwind_info
    Mem: 0x0002c7fb8-0x0002ffff8        __TEXT.__eh_frame
    Mem: 0x000300000-0x00030001b        __TEXT.__oslogstring    (C-String Literals)
LC 01: LC_SEGMENT_64              Mem: 0x000304000-0x5924000    __DATA
    Mem: 0x000304000-0x000307120        __DATA.__got    (Non-Lazy Symbol Ptrs)
    Mem: 0x000307120-0x00030c9d0        __DATA.__la_symbol_ptr    (Lazy Symbol Ptrs)
    Mem: 0x00030c9d0-0x0003106f8        __DATA.__mod_init_func    (Module Init Function
 Ptrs)
    Mem: 0x000310700-0x000321768        __DATA.__const
```

```
    Mem: 0x000321768-0x0003221c8        __DATA.__cfstring
    Mem: 0x0003221c8-0x000369bd0        __DATA.__objc_classlist     (Normal)
    Mem: 0x000369bd0-0x00036a248        __DATA.__objc_nlclslist     (Normal)
    Mem: 0x00036a248-0x00036da38        __DATA.__objc_catlist     (Normal)
    Mem: 0x00036da38-0x00036db58        __DATA.__objc_nlcatlist     (Normal)
    Mem: 0x00036db58-0x00037f650        __DATA.__objc_protolist
    Mem: 0x00037f650-0x00037f658        __DATA.__objc_imageinfo
    Mem: 0x00037f658-0x0009417a0        __DATA.__objc_const
    Mem: 0x0009417a0-0x0009417a8        __DATA.__objc_selrefs     (Literal Pointers)
    Mem: 0x0009417a8-0x000947ea8        __DATA.__objc_protorefs
    Mem: 0x000947ea8-0x0009881f8        __DATA.__objc_classrefs     (Normal)
    Mem: 0x0009881f8-0x0009ab740        __DATA.__objc_superrefs     (Normal)
    Mem: 0x0009ab740-0x0009acac8        __DATA.__objc_ivar
    Mem: 0x0009acac8-0x000d55b20        __DATA.__objc_data
    Mem: 0x000d55b20-0x000d5aa30        __DATA.__data
    Mem: 0x000d5aa30-0x000d5ab28        __DATA.__HTSLifeCycle
    Mem: 0x000d5ab28-0x000d5ab40        __DATA.__objc_stublist
    Mem: 0x000d5ab40-0x000d5ab58        __DATA.RewardedADJSB
    Mem: 0x000d5ab58-0x000d5ad20        __DATA.HGTimorLaunch
    Mem: 0x000d5ad20-0x000d5ad88        __DATA.HGTimorLoad
    Mem: 0x000d5ad88-0x000d5b080        __DATA.TimorLaunch
    Mem: 0x000d5b080-0x000d5b140        __DATA.TimorLoad
    Mem: 0x000d5b140-0x000d5b230        __DATA.RSDHCampaign
    Mem: 0x000d5b230-0x000d5b4b0        __DATA.XBMExternal
    Mem: 0x000d5b4b0-0x000d5b570        __DATA.LazyRegHeader
    Mem: 0x000d5b570-0x000d5b580        __DATA.AWELynxBridge
    Mem: 0x000d5b580-0x000d5b5b0        __DATA.PremainCode
    Mem: 0x000d5b5b0-0x000d60510        __DATA.LazyRegData
    Mem: 0x000d60510-0x000d61390        __DATA.__GAIA__SECTION
    Mem: 0x000d61390-0x000d614b0        __DATA.XBMDefault
    Mem: 0x000d614b0-0x000d61578        __DATA.HMDModule
    Mem: 0x000d61578-0x000d61590        __DATA.HMDLocalModule
    Mem: 0x000d61590-0x000d61710        __DATA.IESLiveBridge
    Mem: 0x000d61710-0x000d62138        __DATA.__bd_timsdk
    Mem: 0x000d62138-0x000d62228        __DATA.IESLiveTemplate
    Mem: 0x000d62228-0x000d62308        __DATA.__LIVESEI__
    Mem: 0x000d62308-0x000d62668        __DATA.__LIVESCHEMA__
    Mem: 0x000d62668-0x000d626c8        __DATA.__LSCHEMEMODEL__
    Mem: 0x000d626c8-0x000d626d8        __DATA.__ENTERROOMSEC__
    Mem: 0x000d626d8-0x000d627a8        __DATA.__VSUSERCARD__
    Mem: 0x000d627a8-0x000d627f8        __DATA.__PUZZLEMETHOD__
    Mem: 0x000d627f8-0x000d62808        __DATA.IESSLynxBridge
    Mem: 0x000d62808-0x000d62858        __DATA.RxAnnotation
    Mem: 0x000d62858-0x000d670a8        __DATA.__objc_clsrefs
    Mem: 0x000d670a8-0x000d67768        __DATA.__thread_vars     (TLV descriptors)
    Mem: 0x000d67768-0x000d67a28        __DATA.IESECSettingReg
    Mem: 0x000d67a28-0x000d67ae0        __DATA.__swift_hooks
    Mem: 0x000d67ae0-0x000d67b98        __DATA.__swift51_hooks
    Mem: 0x000d67b98-0x000d68208        __DATA.__HTSService
    Mem: 0x000d68208-0x000d682f8        __DATA.__HTSDyServImpl
    Mem: 0x000d682f8-0x000d68918        __DATA.__HTSMsgAsc
    Mem: 0x000d68918-0x000d68d68        __DATA.AWERunModernFeed
    Mem: 0x000d68d68-0x000d68f98        __DATA.AWERunShare
    Mem: 0x000d68f98-0x000d69028        __DATA.__HTSDyServ
    Mem: 0x000d69028-0x000d690a8        __DATA.__HTSMsg
    Mem: 0x000d690a8-0x000d75100        __DATA.RxInjector
```

```
    Mem: 0x000d75100-0x000d75218        __DATA.RxAppService
    Mem: 0x000d75218-0x000d75248        __DATA.__HTSNoti
    Mem: 0x000d75248-0x000d752c8        __DATA.AWERunShareSVC
    Mem: 0x000d752c8-0x000d76c68        __DATA.StudioConfigMock
    Mem: 0x000d76c68-0x000d76d28        __DATA.XBMInternal
    Mem: 0x000d76d30-0x000d84267        __DATA.__cstring    (C-String Literals)
    Mem: 0x000d84267-0x000df3302        __DATA.__objc_methname    (C-String Literals)
    Mem: 0x000df3302-0x000e1100a        __DATA.__objc_methtype    (C-String Literals)
    Mem: 0x000e1100a-0x000f4c006        __DATA.__objc_classname    (C-String Literals)
    Mem: 0x000f4c008-0x000f80848        __DATA.__thread_bss    (Thread local zerofill)
    Mem: 0x000f80860-0x001257840        __DATA._D_tconst    (Zero Fill)
    Mem: 0x001257840-0x00161ad98        __DATA._D_dconst    (Zero Fill)
    Mem: 0x00161c000-0x00173e5fc        __DATA._D_ddata    (Zero Fill)
    Mem: 0x00173e600-0x001bd8100        __DATA._D_cfstring    (Zero Fill)
    Mem: 0x001bd8100-0x0037e8970        __DATA._D_objc_const    (Zero Fill)
    Mem: 0x0037e8970-0x003893854        __DATA._D_objc_ivar    (Zero Fill)
    Mem: 0x003893858-0x003a98d20        __DATA._D_objc_selrefs    (Zero Fill)
    Mem: 0x003a98d20-0x003f4eb10        __DATA._D_gcc_except_ta    (Zero Fill)
    Mem: 0x003f4eb10-0x0047e5193        __DATA._D_cstring    (Zero Fill)
    Mem: 0x0047e5194-0x00485caee        __DATA._D_ustring    (Zero Fill)
    Mem: 0x00485caee-0x00533d1a8        __DATA._D_objc_methname    (Zero Fill)
    Mem: 0x00533d1a8-0x005507b0a        __DATA._D_objc_methtype    (Zero Fill)
    Mem: 0x005507c00-0x005687848        __DATA.__common    (Zero Fill)
    Mem: 0x005687900-0x0059229ec        __DATA.__bss    (Zero Fill)
LC 02: LC_SEGMENT_64              Mem: 0x005924000-0x11480000    __BD_TEXT
    Mem: 0x005924000-0x011476a38        __BD_TEXT.__text    (Normal)
    Mem: 0x011476a38-0x01147ef40        __BD_TEXT.__stubs    (Symbol Stubs)
LC 03: LC_SEGMENT_64              Mem: 0x011480000-0x12660000    __LTC_DATA
    Mem: 0x011480000-0x011480208        __LTC_DATA.__meta
    Mem: 0x011480208-0x011480218        __LTC_DATA.__deco
    Mem: 0x011480218-0x011b54d57        __LTC_DATA._C_objc_const
    Mem: 0x011b54d57-0x011b6eadf        __LTC_DATA._C_objc_ivar
    Mem: 0x011b6eadf-0x0120f22de        __LTC_DATA._C_cstring
    Mem: 0x0120f22de-0x01232e92d        __LTC_DATA._C_tconst
    Mem: 0x01232e92d-0x01257b342        __LTC_DATA._C_gcc_except_ta
    Mem: 0x01257b342-0x01265c5da        __LTC_DATA.__fix
LC 04: LC_SEGMENT_64              Mem: 0x012660000-0x12f28000    __LINKEDIT
LC 05: LC_ID_DYLIB               @rpath/AwemeCore.framework/AwemeCore
LC 06: LC_DYLD_INFO
       Rebase info: 350072 bytes at offset 231473152 (0xdcc0000-0xdd15778)
       Bind info:   292520 bytes at offset 231823224 (0xdd15778-0xdd5ce20)
       Weak info:   296    bytes at offset 0xdd5ce20
       Lazy info:   101024 bytes at offset 232116040 (0xdd5cf48-0xdd759e8)
       Export info: 384    bytes at offset 232217064 (0xdd759e8-0xdd75b68)
LC 07: LC_SYMTAB
LC 08: LC_DYSYMTAB
        1 local symbols at index     0
       No external symbols
      5029 undefined symbols at index 1
       No TOC
       No modtab
      7248 Indirect symbols at offset 0xdfa63c0
LC 09: LC_UUID                   UUID: F1FCF15A-6465-31F0-9300-5BA1B8F91017
LC 10: LC_VERSION_MIN_IPHONEOS    Minimum iOS version:    10.0.0
LC 11: LC_SOURCE_VERSION         Source Version:         0.0.0.0.0
LC 12: LC_ENCRYPTION_INFO_64     Encryption: 0 from offset 32768 spanning 3112960 bytes
```

```
LC 13: LC_LOAD_DYLIB             /usr/lib/libcompression.dylib
LC 14: LC_LOAD_DYLIB             @rpath/BDLRepairer.framework/BDLRepairer
LC 15: LC_LOAD_DYLIB             /usr/lib/libc++.1.dylib
LC 16: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/AdServices.framework/AdServ
ices
LC 17: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/AppTrackingTransparency.fra
mework/AppTrackingTransparency
LC 18: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/AuthenticationServices.fram
ework/AuthenticationServices
LC 19: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/CoreHaptics.framework/CoreH
aptics
LC 20: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/CoreTelephony.framework/Cor
eTelephony
LC 21: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/MetalKit.framework/MetalKit
LC 22: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/MetalPerformanceShaders.fra
mework/MetalPerformanceShaders
LC 23: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/MetricKit.framework/MetricK
it
LC 24: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/StoreKit.framework/StoreKit
LC 25: LC_LOAD_DYLIB             @rpath/VolcEngineRTC.framework/VolcEngineRTC
LC 26: LC_LOAD_DYLIB             @rpath/byteaudio.framework/byteaudio
LC 27: LC_LOAD_DYLIB             /usr/lib/libbz2.1.0.dylib
LC 28: LC_LOAD_DYLIB             /usr/lib/libc++abi.dylib
LC 29: LC_LOAD_DYLIB             /usr/lib/libiconv.2.dylib
LC 30: LC_LOAD_DYLIB             /usr/lib/libicucore.A.dylib
LC 31: LC_LOAD_DYLIB             /usr/lib/liblzma.5.dylib
LC 32: LC_LOAD_DYLIB             /usr/lib/libSystem.B.dylib
LC 33: LC_LOAD_DYLIB             /usr/lib/libresolv.9.dylib
LC 34: LC_LOAD_DYLIB             /usr/lib/libsqlite3.dylib
LC 35: LC_LOAD_DYLIB             /usr/lib/libxml2.2.dylib
LC 36: LC_LOAD_DYLIB             /usr/lib/libz.1.dylib
LC 37: LC_LOAD_WEAK_DYLIB        /System/Library/Frameworks/ARKit.framework/ARKit
LC 38: LC_LOAD_DYLIB             /System/Library/Frameworks/AVFoundation.framework/AVFo
undation
LC 39: LC_LOAD_DYLIB             /System/Library/Frameworks/AVKit.framework/AVKit
LC 40: LC_LOAD_DYLIB             /System/Library/Frameworks/Accelerate.framework/Accele
rate
LC 41: LC_LOAD_DYLIB             /System/Library/Frameworks/AdSupport.framework/AdSuppo
rt
LC 42: LC_LOAD_DYLIB             /System/Library/Frameworks/AddressBook.framework/Addre
ssBook
LC 43: LC_LOAD_DYLIB             /System/Library/Frameworks/AssetsLibrary.framework/Ass
etsLibrary
LC 44: LC_LOAD_DYLIB             /System/Library/Frameworks/AudioToolbox.framework/Audi
oToolbox
LC 45: LC_LOAD_DYLIB             /System/Library/Frameworks/CFNetwork.framework/CFNetwo
rk
LC 46: LC_LOAD_DYLIB             /System/Library/Frameworks/Contacts.framework/Contacts
LC 47: LC_LOAD_DYLIB             /System/Library/Frameworks/ContactsUI.framework/Contac
tsUI
LC 48: LC_LOAD_DYLIB             /System/Library/Frameworks/CoreAudio.framework/CoreAud
io
LC 49: LC_LOAD_DYLIB             /System/Library/Frameworks/CoreAudioKit.framework/Core
AudioKit
LC 50: LC_LOAD_DYLIB             /System/Library/Frameworks/CoreFoundation.framework/Co
reFoundation
```

```
LC 51: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreGraphics.framework/Core
Graphics
LC 52: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreImage.framework/CoreIma
ge
LC 53: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreLocation.framework/Core
Location
LC 54: LC_LOAD_WEAK_DYLIB           /System/Library/Frameworks/CoreML.framework/CoreML
LC 55: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreMedia.framework/CoreMed
ia
LC 56: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreMotion.framework/CoreMo
tion
LC 57: LC_LOAD_DYLIB                /System/Library/Frameworks/MobileCoreServices.framewor
k/MobileCoreServices
LC 58: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreSpotlight.framework/Cor
eSpotlight
LC 59: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreText.framework/CoreText
LC 60: LC_LOAD_DYLIB                /System/Library/Frameworks/CoreVideo.framework/CoreVid
eo
LC 61: LC_LOAD_DYLIB                /System/Library/Frameworks/EventKit.framework/EventKit
LC 62: LC_LOAD_DYLIB                /System/Library/Frameworks/Foundation.framework/Founda
tion
LC 63: LC_LOAD_DYLIB                /System/Library/Frameworks/GLKit.framework/GLKit
LC 64: LC_LOAD_DYLIB                /System/Library/Frameworks/GameplayKit.framework/Gamep
layKit
LC 65: LC_LOAD_DYLIB                /System/Library/Frameworks/IOKit.framework/Versions/A/
IOKit
LC 66: LC_LOAD_DYLIB                /System/Library/Frameworks/ImageIO.framework/ImageIO
LC 67: LC_LOAD_DYLIB                /System/Library/Frameworks/Intents.framework/Intents
LC 68: LC_LOAD_DYLIB                /System/Library/Frameworks/JavaScriptCore.framework/Ja
vaScriptCore
LC 69: LC_LOAD_DYLIB                /System/Library/Frameworks/LocalAuthentication.framewo
rk/LocalAuthentication
LC 70: LC_LOAD_DYLIB                /System/Library/Frameworks/MapKit.framework/MapKit
LC 71: LC_LOAD_DYLIB                /System/Library/Frameworks/MediaAccessibility.framewor
k/MediaAccessibility
LC 72: LC_LOAD_DYLIB                /System/Library/Frameworks/MediaPlayer.framework/Media
Player
LC 73: LC_LOAD_DYLIB                /System/Library/Frameworks/MediaToolbox.framework/Medi
aToolbox
LC 74: LC_LOAD_DYLIB                /System/Library/Frameworks/MessageUI.framework/Message
UI
LC 75: LC_LOAD_DYLIB                /System/Library/Frameworks/Metal.framework/Metal
LC 76: LC_LOAD_DYLIB                /System/Library/Frameworks/NetworkExtension.framework/
NetworkExtension
LC 77: LC_LOAD_DYLIB                /System/Library/Frameworks/OpenAL.framework/OpenAL
LC 78: LC_LOAD_DYLIB                /System/Library/Frameworks/OpenGLES.framework/OpenGLES
LC 79: LC_LOAD_DYLIB                /System/Library/Frameworks/Photos.framework/Photos
LC 80: LC_LOAD_WEAK_DYLIB           /System/Library/Frameworks/PhotosUI.framework/PhotosUI
LC 81: LC_LOAD_DYLIB                /System/Library/Frameworks/QuartzCore.framework/Quartz
Core
LC 82: LC_LOAD_DYLIB                /System/Library/Frameworks/ReplayKit.framework/ReplayK
it
LC 83: LC_LOAD_DYLIB                /System/Library/Frameworks/SafariServices.framework/Sa
fariServices
LC 84: LC_LOAD_DYLIB                /System/Library/Frameworks/Security.framework/Security
LC 85: LC_LOAD_DYLIB                /System/Library/Frameworks/SystemConfiguration.framewo
```

```
rk/SystemConfiguration
LC 86: LC_LOAD_DYLIB            /System/Library/Frameworks/UIKit.framework/UIKit
LC 87: LC_LOAD_DYLIB            /System/Library/Frameworks/VideoToolbox.framework/Vide
oToolbox
LC 88: LC_LOAD_DYLIB            /System/Library/Frameworks/WebKit.framework/WebKit
LC 89: LC_LOAD_DYLIB            /System/Library/Frameworks/iAd.framework/iAd
LC 90: LC_LOAD_WEAK_DYLIB       /System/Library/Frameworks/QuickLook.framework/QuickLo
ok
LC 91: LC_LOAD_DYLIB            /usr/lib/libobjc.A.dylib
LC 92: LC_LOAD_WEAK_DYLIB       /System/Library/Frameworks/Combine.framework/Combine
LC 93: LC_LOAD_WEAK_DYLIB       /System/Library/Frameworks/GroupActivities.framework/G
roupActivities
LC 94: LC_LOAD_WEAK_DYLIB       /System/Library/Frameworks/IOSurface.framework/IOSurfa
ce
LC 95: LC_LOAD_WEAK_DYLIB       /System/Library/Frameworks/UserNotifications.framework
/UserNotifications
LC 96: LC_LOAD_WEAK_DYLIB       /System/Library/Frameworks/WidgetKit.framework/WidgetK
it
LC 97: LC_LOAD_WEAK_DYLIB       /usr/lib/swift/libswiftCoreMIDI.dylib
LC 98: LC_LOAD_WEAK_DYLIB       /usr/lib/swift/libswiftDataDetection.dylib
LC 99: LC_LOAD_WEAK_DYLIB       /usr/lib/swift/libswiftFileProvider.dylib
LC 100: LC_LOAD_WEAK_DYLIB       /usr/lib/swift/libswiftUniformTypeIdentifiers.dylib
LC 101: LC_LOAD_WEAK_DYLIB       /usr/lib/swift/libswiftWebKit.dylib
LC 102: LC_LOAD_WEAK_DYLIB       /usr/lib/swift/libswift_Concurrency.dylib
LC 103: LC_LOAD_WEAK_DYLIB       @rpath/libswiftAVFoundation.dylib
LC 104: LC_LOAD_DYLIB            @rpath/libswiftCore.dylib
LC 105: LC_LOAD_WEAK_DYLIB       @rpath/libswiftCoreAudio.dylib
LC 106: LC_LOAD_WEAK_DYLIB       @rpath/libswiftCoreData.dylib
LC 107: LC_LOAD_WEAK_DYLIB       @rpath/libswiftCoreFoundation.dylib
LC 108: LC_LOAD_DYLIB            @rpath/libswiftCoreGraphics.dylib
LC 109: LC_LOAD_WEAK_DYLIB       @rpath/libswiftCoreImage.dylib
LC 110: LC_LOAD_WEAK_DYLIB       @rpath/libswiftCoreLocation.dylib
LC 111: LC_LOAD_WEAK_DYLIB       @rpath/libswiftCoreMedia.dylib
LC 112: LC_LOAD_WEAK_DYLIB       @rpath/libswiftDarwin.dylib
LC 113: LC_LOAD_DYLIB            @rpath/libswiftDispatch.dylib
LC 114: LC_LOAD_DYLIB            @rpath/libswiftFoundation.dylib
LC 115: LC_LOAD_WEAK_DYLIB       @rpath/libswiftIntents.dylib
LC 116: LC_LOAD_WEAK_DYLIB       @rpath/libswiftMapKit.dylib
LC 117: LC_LOAD_WEAK_DYLIB       @rpath/libswiftMetal.dylib
LC 118: LC_LOAD_WEAK_DYLIB       @rpath/libswiftNetwork.dylib
LC 119: LC_LOAD_DYLIB            @rpath/libswiftObjectiveC.dylib
LC 120: LC_LOAD_WEAK_DYLIB       @rpath/libswiftPhotos.dylib
LC 121: LC_LOAD_WEAK_DYLIB       @rpath/libswiftQuartzCore.dylib
LC 122: LC_LOAD_DYLIB            @rpath/libswiftUIKit.dylib
LC 123: LC_LOAD_WEAK_DYLIB       @rpath/libswiftos.dylib
LC 124: LC_LOAD_WEAK_DYLIB       @rpath/libswiftsimd.dylib
LC 125: LC_RPATH                 /usr/lib/swift
LC 126: LC_RPATH                 @executable_path/Frameworks
LC 127: LC_RPATH                 @loader_path/Frameworks
LC 128: LC_RPATH                 @executable_path/../../Frameworks
LC 129: LC_RPATH                 @executable_path/Frameworks
LC 130: LC_FUNCTION_STARTS       Offset: 232217448, Size: 2214096 (0xdd75b68-0xdf92438)

LC 131: LC_DATA_IN_CODE          Offset: 234431544, Size:   1320 (0xdf92438-0xdf92960)
LC 132: LC_CODE_SIGNATURE        Offset: 234688704, Size: 5977904 (0xdfd10c0-0xe5847f0)
```

-L：查看使用了哪些共享库Library

```
jtool2 -L v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore
```

输出内容：

```
➜  AwemeCore jtool2 -L ../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore
.framework/AwemeCore
Warning: Too many symbols: This can easily be fixed by J - tell him, please
../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore:
    /usr/lib/libcompression.dylib (compatibility version 1.0.0, current version 1.0.0)
    @rpath/BDLRepairer.framework/BDLRepairer (compatibility version 1.0.0, current vers
ion 1.0.0)
    /usr/lib/libc++.1.dylib (compatibility version 1.0.0, current version 1200.3.0)
    /System/Library/Frameworks/AdServices.framework/AdServices (compatibility version 1
.0.0, current version 1.0.0)
    /System/Library/Frameworks/AppTrackingTransparency.framework/AppTrackingTransparenc
y (compatibility version 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/AuthenticationServices.framework/AuthenticationServices (
compatibility version 1.0.0, current version 612.1.27)
    /System/Library/Frameworks/CoreHaptics.framework/CoreHaptics (compatibility version
1.0.0, current version 1.0.0)
    /System/Library/Frameworks/CoreTelephony.framework/CoreTelephony (compatibility ver
sion 1.0.0, current version 0.0.0)
    /System/Library/Frameworks/MetalKit.framework/MetalKit (compatibility version 1.0.0
, current version 153.0.0)
    /System/Library/Frameworks/MetalPerformanceShaders.framework/MetalPerformanceShader
s (compatibility version 1.0.0, current version 125.0.31)
    /System/Library/Frameworks/MetricKit.framework/MetricKit (compatibility version 1.0
.0, current version 1.0.0)
    /System/Library/Frameworks/StoreKit.framework/StoreKit (compatibility version 1.0.0
, current version 1.0.0)
    @rpath/VolcEngineRTC.framework/VolcEngineRTC (compatibility version 1.0.0, current
version 323.0.0)
    @rpath/byteaudio.framework/byteaudio (compatibility version 1.0.0, current version
1.0.1)
    /usr/lib/libbz2.1.0.dylib (compatibility version 1.0.0, current version 1.0.8)
    /usr/lib/libc++abi.dylib (compatibility version 1.0.0, current version 1200.3.0)
    /usr/lib/libiconv.2.dylib (compatibility version 7.0.0, current version 7.0.0)
    /usr/lib/libicucore.A.dylib (compatibility version 1.0.0, current version 68.2.0)
    /usr/lib/liblzma.5.dylib (compatibility version 6.0.0, current version 6.3.0)
    /usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1311.0.0)
    /usr/lib/libresolv.9.dylib (compatibility version 1.0.0, current version 1.0.0)
    /usr/lib/libsqlite3.dylib (compatibility version 9.0.0, current version 329.0.0)
    /usr/lib/libxml2.2.dylib (compatibility version 10.0.0, current version 10.9.0)
    /usr/lib/libz.1.dylib (compatibility version 1.0.0, current version 1.2.11)
    /System/Library/Frameworks/ARKit.framework/ARKit (compatibility version 1.0.0, curr
ent version 1.0.0)
    /System/Library/Frameworks/AVFoundation.framework/AVFoundation (compatibility versi
on 1.0.0, current version 2.0.0)
    /System/Library/Frameworks/AVKit.framework/AVKit (compatibility version 1.0.0, curr
```

```
ent version 1.0.0)
    /System/Library/Frameworks/Accelerate.framework/Accelerate (compatibility version 1
.0.0, current version 4.0.0)
    /System/Library/Frameworks/AdSupport.framework/AdSupport (compatibility version 1.0
.0, current version 1.0.0)
    /System/Library/Frameworks/AddressBook.framework/AddressBook (compatibility version
1.0.0, current version 1.0.0)
    /System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary (compatibility ver
sion 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/AudioToolbox.framework/AudioToolbox (compatibility versi
on 1.0.0, current version 1000.0.0)
    /System/Library/Frameworks/CFNetwork.framework/CFNetwork (compatibility version 1.0
.0, current version 1312.0.0)
    /System/Library/Frameworks/Contacts.framework/Contacts (compatibility version 0.0.0
, current version 3529.0.0)
    /System/Library/Frameworks/ContactsUI.framework/ContactsUI (compatibility version 1
.0.0, current version 1141.1.0)
    /System/Library/Frameworks/CoreAudio.framework/CoreAudio (compatibility version 1.0
.0, current version 1.0.0)
    /System/Library/Frameworks/CoreAudioKit.framework/CoreAudioKit (compatibility versi
on 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/CoreFoundation.framework/CoreFoundation (compatibility v
ersion 150.0.0, current version 1854.0.0)
    /System/Library/Frameworks/CoreGraphics.framework/CoreGraphics (compatibility versi
on 64.0.0, current version 1548.1.3)
    /System/Library/Frameworks/CoreImage.framework/CoreImage (compatibility version 1.0
.0, current version 5.0.0)
    /System/Library/Frameworks/CoreLocation.framework/CoreLocation (compatibility versi
on 1.0.0, current version 2663.0.3)
    /System/Library/Frameworks/CoreML.framework/CoreML (compatibility version 1.0.0, cu
rrent version 1.0.0)
    /System/Library/Frameworks/CoreMedia.framework/CoreMedia (compatibility version 1.0
.0, current version 1.0.0)
    /System/Library/Frameworks/CoreMotion.framework/CoreMotion (compatibility version 1
.0.0, current version 2663.0.3)
    /System/Library/Frameworks/MobileCoreServices.framework/MobileCoreServices (compati
bility version 1.0.0, current version 1141.1.0)
    /System/Library/Frameworks/CoreSpotlight.framework/CoreSpotlight (compatibility ver
sion 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/CoreText.framework/CoreText (compatibility version 1.0.0
, current version 1.0.0)
    /System/Library/Frameworks/CoreVideo.framework/CoreVideo (compatibility version 1.2
.0, current version 1.5.0)
    /System/Library/Frameworks/EventKit.framework/EventKit (compatibility version 1.0.0
, current version 1716.0.0)
    /System/Library/Frameworks/Foundation.framework/Foundation (compatibility version 3
00.0.0, current version 1854.0.0)
    /System/Library/Frameworks/GLKit.framework/GLKit (compatibility version 1.0.0, curr
ent version 126.0.0)
    /System/Library/Frameworks/GameplayKit.framework/GameplayKit (compatibility version
1.0.0, current version 96.1.0)
    /System/Library/Frameworks/IOKit.framework/Versions/A/IOKit (compatibility version
1.0.0, current version 275.0.0)
    /System/Library/Frameworks/ImageIO.framework/ImageIO (compatibility version 1.0.0,
current version 1.0.0)
    /System/Library/Frameworks/Intents.framework/Intents (compatibility version 1.0.0,
```

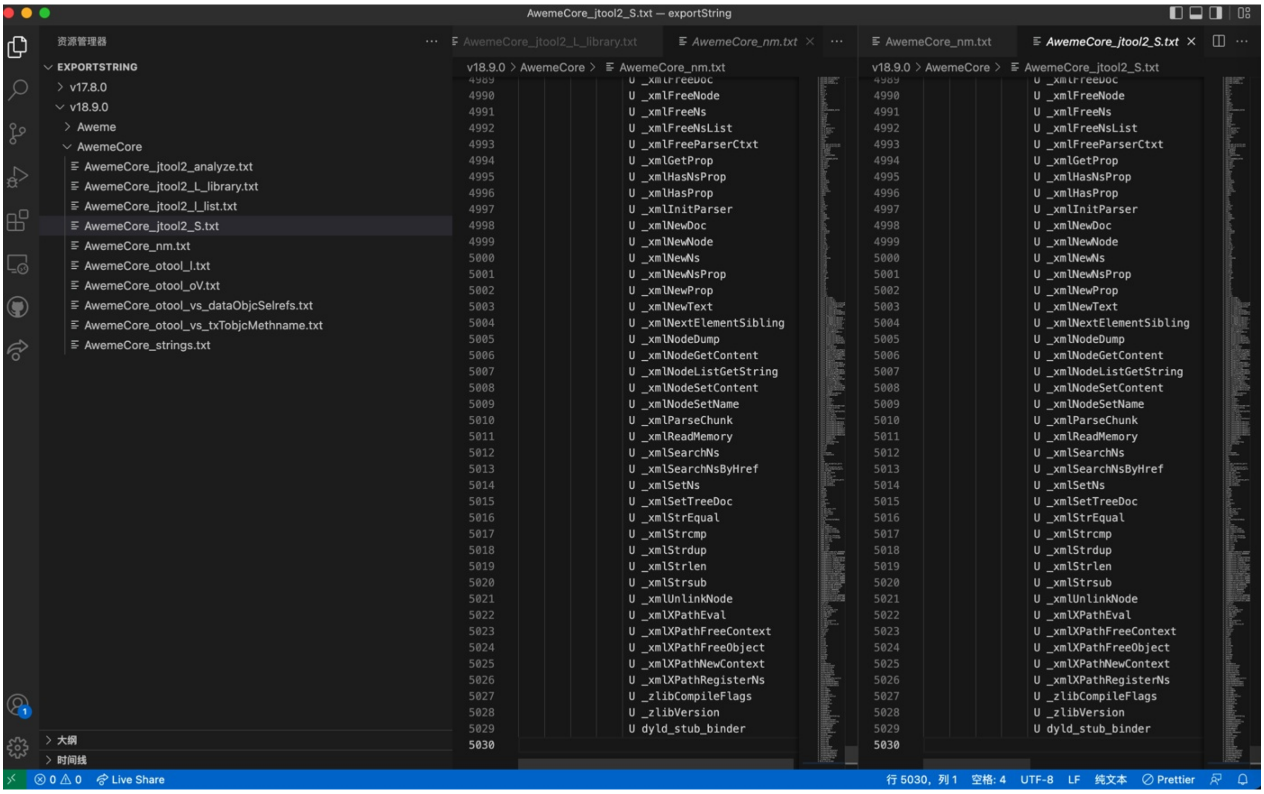
```
current version 1.0.0)
    /System/Library/Frameworks/JavaScriptCore.framework/JavaScriptCore (compatibility v
ersion 1.0.0, current version 612.1.27)
    /System/Library/Frameworks/LocalAuthentication.framework/LocalAuthentication (compa
tibility version 1.0.0, current version 984.10.2)
    /System/Library/Frameworks/MapKit.framework/MapKit (compatibility version 1.0.0, cu
rrent version 14.0.0)
    /System/Library/Frameworks/MediaAccessibility.framework/MediaAccessibility (compati
bility version 1.0.0, current version 62.0.0)
    /System/Library/Frameworks/MediaPlayer.framework/MediaPlayer (compatibility version
1.0.0, current version 1.0.0)
    /System/Library/Frameworks/MediaToolbox.framework/MediaToolbox (compatibility versi
on 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/MessageUI.framework/MessageUI (compatibility version 1.0
.0, current version 3693.0.2)
    /System/Library/Frameworks/Metal.framework/Metal (compatibility version 1.0.0, curr
ent version 257.25.0)
    /System/Library/Frameworks/NetworkExtension.framework/NetworkExtension (compatibili
ty version 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/OpenAL.framework/OpenAL (compatibility version 1.0.0, cu
rrent version 1.0.0)
    /System/Library/Frameworks/OpenGLES.framework/OpenGLES (compatibility version 1.0.0
, current version 1.0.0)
    /System/Library/Frameworks/Photos.framework/Photos (compatibility version 1.0.0, cu
rrent version 402.5.140)
    /System/Library/Frameworks/PhotosUI.framework/PhotosUI (compatibility version 1.0.0
, current version 402.5.140)
    /System/Library/Frameworks/QuartzCore.framework/QuartzCore (compatibility version 1
.2.0, current version 1.11.0)
    /System/Library/Frameworks/ReplayKit.framework/ReplayKit (compatibility version 1.0
.0, current version 1.0.0)
    /System/Library/Frameworks/SafariServices.framework/SafariServices (compatibility v
ersion 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/Security.framework/Security (compatibility version 1.0.0
, current version 60157.12.1)
    /System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration (compa
tibility version 1.0.0, current version 1163.10.2)
    /System/Library/Frameworks/UIKit.framework/UIKit (compatibility version 1.0.0, curr
ent version 5067.3.107)
    /System/Library/Frameworks/VideoToolbox.framework/VideoToolbox (compatibility versi
on 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/WebKit.framework/WebKit (compatibility version 1.0.0, cu
rrent version 612.1.27)
    /System/Library/Frameworks/iAd.framework/iAd (compatibility version 1.0.0, current
version 1.0.0)
    /System/Library/Frameworks/QuickLook.framework/QuickLook (compatibility version 1.0
.0, current version 846.1.0)
    /usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)
    /System/Library/Frameworks/Combine.framework/Combine (compatibility version 1.0.0,
current version 276.0.0)
    /System/Library/Frameworks/GroupActivities.framework/GroupActivities (compatibility
 version 1.0.0, current version 1.0.0)
    /System/Library/Frameworks/IOSurface.framework/IOSurface (compatibility version 1.0
.0, current version 1.0.0)
    /System/Library/Frameworks/UserNotifications.framework/UserNotifications (compatibi
lity version 1.0.0, current version 1.0.0)
```

```
    /System/Library/Frameworks/WidgetKit.framework/WidgetKit (compatibility version 1.0
.0, current version 181.0.0)
    /usr/lib/swift/libswiftCoreMIDI.dylib (compatibility version 1.0.0, current version
5.0.0)
    /usr/lib/swift/libswiftDataDetection.dylib (compatibility version 1.0.0, current ve
rsion 694.0.0)
    /usr/lib/swift/libswiftFileProvider.dylib (compatibility version 1.0.0, current ver
sion 374.1.2)
    /usr/lib/swift/libswiftUniformTypeIdentifiers.dylib (compatibility version 1.0.0, c
urrent version 718.0.0)
    /usr/lib/swift/libswiftWebKit.dylib (compatibility version 1.0.0, current version 6
12.1.27)
    /usr/lib/swift/libswift_Concurrency.dylib (compatibility version 1.0.0, current ver
sion 1300.0.29)
    @rpath/libswiftAVFoundation.dylib (compatibility version 1.0.0, current version 203
6.25.1)
    @rpath/libswiftCore.dylib (compatibility version 1.0.0, current version 1300.0.29)
    @rpath/libswiftCoreAudio.dylib (compatibility version 1.0.0, current version 1.1.0)
    @rpath/libswiftCoreData.dylib (compatibility version 1.0.0, current version 18.0.0)
    @rpath/libswiftCoreFoundation.dylib (compatibility version 1.0.0, current version 1
4.0.0)
    @rpath/libswiftCoreGraphics.dylib (compatibility version 1.0.0, current version 3.0
.0)
    @rpath/libswiftCoreImage.dylib (compatibility version 1.0.0, current version 2.0.0)
    @rpath/libswiftCoreLocation.dylib (compatibility version 1.0.0, current version 6.0
.0)
    @rpath/libswiftCoreMedia.dylib (compatibility version 1.0.0, current version 2896.25
.1)
    @rpath/libswiftDarwin.dylib (compatibility version 1.0.0, current version 0.0.0)
    @rpath/libswiftDispatch.dylib (compatibility version 1.0.0, current version 9.0.0)
    @rpath/libswiftFoundation.dylib (compatibility version 1.0.0, current version 69.0.0
)
    @rpath/libswiftIntents.dylib (compatibility version 1.0.0, current version 11.0.0)
    @rpath/libswiftMapKit.dylib (compatibility version 1.0.0, current version 3.0.0)
    @rpath/libswiftMetal.dylib (compatibility version 1.0.0, current version 257.25.1)
    @rpath/libswiftNetwork.dylib (compatibility version 1.0.0, current version 2736.12.1
)
    @rpath/libswiftObjectiveC.dylib (compatibility version 1.0.0, current version 2.0.0)

    @rpath/libswiftPhotos.dylib (compatibility version 1.0.0, current version 402.5.140)

    @rpath/libswiftQuartzCore.dylib (compatibility version 1.0.0, current version 3.0.0)

    @rpath/libswiftUIKit.dylib (compatibility version 1.0.0, current version 5038.0.0)
    @rpath/libswiftos.dylib (compatibility version 1.0.0, current version 1021.0.0)
    @rpath/libswiftsimd.dylib (compatibility version 1.0.0, current version 9.0.0)
```

-S: 列出符号表Symbol == nm

```
jtool2 -S v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore > AwemeCor
e_jtool2_S.txt
```

输出内容：



--analyze: 分析analyze -> 导出类和函数名等

```
jtool2 --analyze v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore
```

输出log：

```
➜  AwemeCore jtool2 --analyze ../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCore.framework/AwemeCore
Analyzing file...
Warning: Too many symbols. This can easily be fixed by J - tell him, please
Resolving stubs..
Processing __DATA..
opened companion file ./AwemeCore.ARM64.F1FCF15A-6465-31F0-9300-5BA1B8F91017
Dumping symbol cache to file
Symbolicated 144477 symbols and 355043 functions
```

输出内容：

```
0x8:_$s10Foundation25NSFastEnumerationIteratorVStAAMc:
0x10:_$s10Foundation3URLVMn:
0x18:_$s10Foundation4DataVN:
...
0x20:_$s10Foundation4DateVMn:
0x28:_$s10Foundation9IndexPathVMa:
0x30:_$s10Foundation9IndexPathVMn:
0x38:_$s10Foundation9IndexPathVSEAAMc:
0x40:_$s10Foundation9IndexPathVSQAAMc:
```

```
0x48 _$s10Foundation9IndexPathVSeAAMc
0x50 _$s10ObjectiveC8ObjCBoolVMn
0x58 _$s12CoreGraphics14CGPathFillRuleO7windingyA2CmFWC
0x60 _$s12CoreGraphics7CGFloatVMn
0x68 _$s12CoreGraphics7CGFloatVN
0xd8 _$s15GroupActivities0A13StateObserverCMn
0xe0 _$s15GroupActivities0A16ActivityMetadataVMa
0xe8 _$s15GroupActivities0A16ActivityMetadataVMn
0xf0 _$s15GroupActivities0A16ActivityMetadataVSEAAMc
0xf8 _$s15GroupActivities0A16ActivityMetadataVSeAAMc
0x100 _$s15GroupActivities0A16SessionMessengerC14MessageContextVMn
0x108 _$s15GroupActivities0A16SessionMessengerC4send_2toyx_AA12ParticipantsOtYaKSeRzSERzlFTu
0x110 _$s15GroupActivities0A16SessionMessengerC8MessagesV8IteratorVMa
0x118 _$s15GroupActivities0A16SessionMessengerC8MessagesV8IteratorVMn
0x120 _$s15GroupActivities0A16SessionMessengerC8MessagesV8IteratorVy_x_GScIAAMc
0x128 _$s15GroupActivities0A16SessionMessengerC8MessagesVMa
0x130 _$s15GroupActivities0A16SessionMessengerC8MessagesVMn
0x138 _$s15GroupActivities0A16SessionMessengerC8MessagesVy_xGSciAAMc
0x140 _$s15GroupActivities0A16SessionMessengerCMn
0x148 _$s15GroupActivities0A24ActivityActivationResultO18activationDisabledyA2CmFWC
0x150 _$s15GroupActivities0A24ActivityActivationResultO19activationPreferredyA2CmFWC
0x158 _$s15GroupActivities0A24ActivityActivationResultO9cancelledyA2CmFWC
0x160 _$s15GroupActivities0A7SessionC3endyyF
0x168 _$s15GroupActivities0A7SessionC5StateO11invalidatedyAEyx_Gs5Error_p_tcAGmAA0A8ActivityRzlFWC
0x170 _$s15GroupActivities0A7SessionC5leaveyyF
0x178 _$s15GroupActivities0A7SessionC8SessionsV8IteratorVyx__GScIAAMc
0x180 _$s15GroupActivities0A7SessionC8SessionsVyx_GSciAAMc
0x188 _$s15GroupActivities0A7SessionCMa
0x190 _$s15GroupActivities0A7SessionCMn
0x1a0 _$s15GroupActivities0A8ActivityPAAE20prepareForActivationAA0acF6ResultOyYaFTu
0x1a8 _$s15GroupActivities0A8ActivityPAAE8activateSbyYaKFTu
0x1b0 _$s15GroupActivities11ParticipantVMa
0x1b8 _$s15GroupActivities11ParticipantVMn
0x1c0 _$s15GroupActivities11ParticipantVSHAAMc
0x1c8 _$s15GroupActivities12ParticipantsO3allyA2CmFWC
0x348 _$s7Combine10PublishersO16RemoveDuplicatesVMn
0x350 _$s7Combine10PublishersO16RemoveDuplicatesVy_xGAA9PublisherAAMc
0x358 _$s7Combine10PublishersO3MapVMn
0x360 _$s7Combine10PublishersO3MapVy_xq_GAA9PublisherAAMc
0x368 _$s7Combine10PublishersO4DropVMn
0x370 _$s7Combine10PublishersO4DropVy_xGAA9PublisherAAMc
0x378 _$s7Combine10PublishersO9ReceiveOnVMn
0x380 _$s7Combine10PublishersO9ReceiveOnVy_xq_GAA9PublisherAAMc
0x388 _$s7Combine14AnyCancellableCMn
0x390 _$s7Combine9PublishedV9PublisherVMa
0x398 _$s7Combine9PublishedV9PublisherVMn
0x3a0 _$s7Combine9PublishedV9PublisherVyx_GAadAMc
0x3a8 _$s7Combine9PublishedVMa
0x3b0 _$s7Combine9PublishedVMn
0x3c8 _$s8Dispatch0A12TimeIntervalO12millisecondsyACSicACmFWC
0x3d0 _$s8Dispatch0A13WorkItemFlagsVMa
0x3d8 _$s8Dispatch0A13WorkItemFlagsVMn
0x3e0 _$s8Dispatch0A13WorkItemFlagsVs10SetAlgebraAAMc
0x3e8 _$s8Dispatch0A3QoSV0B6SClassO7defaultyA2EmFWC
```

```
0x400 _$sBbWV
0x410 _$sSDMn
...
0xc1ae6f8 -[APMobileIdentifier IMSI]
0xc1ae704 -[APMobileIdentifier IMEI]
0xc1ae710 -[APMobileIdentifier TID]
0xc1ae71c -[APMobileIdentifier deviceFingerprint]
0xc1ae728 -[APMobileIdentifier UTDID]
0xc1ae734 -[APMobileIdentifier setUTDID:]
0xc1ae73c -[APMobileIdentifier UUID]
0xc1ae748 -[APMobileIdentifier setUUID:]
0xc1ae750 -[APMobileIdentifier AWID]
0xc1ae75c -[APMobileIdentifier clientId]
0xc1ae768 -[APMobileIdentifier .cxx_destruct]
0xc5e5bc8 -[LynxView setAdInfoDict:]
0xc5e5bd8 -[LynxView adInfoDict]
0xc94fb00 -[LynxView model]
0xc94fb04 -[LynxView setModel:]
0xe20a878 -[LynxView awelynx_initWithBuilderBlock:]
0xea2140c -[CanvasAPI measureText:fontSize:]
0xea21570 -[CanvasAPI drawSync:actions:]
0xea21684 -[CanvasAPI release:]
0xea23408 -[CanvasViewManager view]
0xea23504 -[CanvasViewManager set_nativeID:forView:withDefaultView:]
0xea235e8 -[CanvasViewManager set_actions:forView:withDefaultView:]
0xea38bd4 -[AWERCTFoundationAPIManager init]
0xea38c54 -[AWERCTFoundationAPIManager showToast:]
0xea38c74 -[AWERCTFoundationAPIManager logCrash:]
0xea38d20 -[AWERCTFoundationAPIManager logEventV1:label:value:extraValue:extras:]
0xea38de0 -[AWERCTFoundationAPIManager logEventV3:parameters:]
0xea38e60 -[AWERCTFoundationAPIManager getUserInfo:]
0xea38e78 -[AWERCTFoundationAPIManager getRequestDomain:callback:]
0xea3904c -[AWERCTFoundationAPIManager getNetworkParams:]
0xea3918c -[AWERCTFoundationAPIManager getLocale:]
0xea39298 -[AWERCTFoundationAPIManager request:info:callback:]
0xea3a0dc -[AWERCTFoundationAPIManager openScene:sceneName:initProperties:callback:]
0xea3a274 -[AWERCTFoundationAPIManager openH5Page:URLString:controlFlags:callback:]
0xea3a41c -[AWERCTFoundationAPIManager openSchema:schemeURL:callback:]
0xea3a7fc -[AWERCTFoundationAPIManager pushViewController:withReactID:callback:]
0xea3a910 -[AWERCTFoundationAPIManager closeWithResult:result:callback:]
0xea3a92c -[AWERCTFoundationAPIManager close:callback:]
0xea3a938 -[AWERCTFoundationAPIManager closeReactID:callback:]
0xea3b048 -[AWERCTFoundationAPIManager darkMode:enable:]
0xea3b180 -[AWERCTFoundationAPIManager componentDidMount:]
0xea3b268 -[AWERCTFoundationAPIManager webVCWithRouterParams:]
0xea3b2c8 -[AWERCTFoundationAPIManager getUserInfoWithCallBack:]
0xea3b600 -[AWERCTFoundationAPIManager schemaHandler]
0xea3b608 -[AWERCTFoundationAPIManager setSchemaHandler:]
0xea3b614 -[AWERCTFoundationAPIManager .cxx_destruct]
0xf56fd94 -[WCTDatabase studio_recoverFromPath:withPageSize:backupCipher:databaseCipher
:error:]
0x105b540c -[LynxView lynxBridgeContext]
0x105b5418 -[LynxView setLynxBridgeContext:]
0x105e25a4 -[LynxView bdx_engineType]
0x105e25ec -[LynxView bdx_dealloc]
0x105f0d50 -[LynxView isBDXCreated]
```

```
0x105f0d94 -[LynxView setIsBDXCreated:]
0x11227850 -[LynxLayoutNode turboNativeLayoutNode]
0x11227974 -[LynxLayoutNode adoptNativeLayoutNode:]
0x112279e8 -[LynxLayoutNode setMeasureDelegate:]
0x11227a24 -[LynxLayoutNode updateLayoutWithFrame:]
0x11227a4c -[LynxLayoutNode setNeedsLayout]
0x11227a68 -[LynxLayoutNode needsLayout]
0x11227a7c -[LynxLayoutNode layoutDidStart]
0x11227a80 -[LynxLayoutNode layoutDidUpdate]
0x11227a84 -[LynxLayoutNode hasCustomLayout]
0x11227a8c -[LynxLayoutNode frame]
0x11227aa4 -[LynxLayoutNode padding]
0x11227abc -[LynxLayoutNode margin]
0x11227ad4 -[LynxLayoutNode border]
0x11227aec -[LynxLayoutNode style]
0x11227afc -[LynxLayoutNode measureDelegate]
0x11227b1c -[LynxLayoutNode .cxx_destruct]
0x112350a0 -[LynxUI drawParameter]
0x11235150 -[LynxUI enableAsyncDisplay]
0x11235210 -[LynxUI displayAsynchronously]
0x1123539c -[LynxUI displayComplexBackgroundAsynchronouslyWithDisplay:completion:]
0x1123559c -[LynxUI displayAsyncWithCompletionBlock:]
0x11239d48 -[LynxUIImage init]
0x11239dfc -[LynxUIImage createView]
0x11239e68 -[LynxUIImage onImageReady:]
0x1123a44c -[LynxUIImage updateLayerMaskOnFrameChangedInner:]
0x1123a934 -[LynxUIImage updateLayerMaskOnFrameChanged]
0x1123a9b0 -[LynxUIImage frameDidChange]
0x1123aa00 -[LynxUIImage propsDidUpdate]
0x1123aa50 -[LynxUIImage enableAsyncDisplay]
0x1123aa64 -[LynxUIImage requestImage]
0x1123aab4 -[LynxUIImage getEnableImageDownsampling]
0x1123ab48 -[LynxUIImage requestImage:]
0x1123b9ec -[LynxUIImage reportURLSrcError:type:source:]
0x1123bd38 -[LynxUIImage resetImage]
0x1123be74 -[LynxUIImage setSrc:requestReset:]
0x1123c0c4 -[LynxUIImage setPlaceholder:requestReset:]
0x1123c220 -[LynxUIImage setMode:requestReset:]
0x1123c378 -[LynxUIImage setCoverStart:requestReset:]
0x1123c420 -[LynxUIImage setBlurRadius:requestReset:]
0x1123c678 -[LynxUIImage setInnerCapInsets:requestReset:]
0x1123c92c -[LynxUIImage setCapInsets:requestReset:]
0x1123c9c0 -[LynxUIImage setCapInsetsScale:requestReset:]
0x1123ca8c -[LynxUIImage setLoopCount:requestReset:]
0x1123cb28 -[LynxUIImage setPreFetchWidth:requestReset:]
0x1123cc7c -[LynxUIImage setPreFetchHeight:requestReset:]
0x1123cdd0 -[LynxUIImage setDownsampling:requestReset:]
0x1123ce6c -[LynxUIImage setAutoSize:requestReset:]
0x1123ce80 -[LynxUIImage toCapInsetValue:]
0x1123d010 -[LynxUIImage frameSize]
0x1123d038 -[LynxUIImage drawParameter]
0x1123d758 -[LynxUIImage restartAnimation]
0x1123d7a8 -[LynxUIImage isAnimated]
0x1123d804 -[LynxUIImage enableAccessibilityByDefault]
0x1123d80c -[LynxUIImage startAnimating]
0x1123d84c -[LynxUIImage measureNode:withWidth:widthMode:height:heightMode:]
```

```
0x1123d9dc -[LynxUIImage accessibilityTraitsByDefault]
0x1123d9ec -[LynxUIImage resizeMode]
0x1123d9fc -[LynxUIImage setResizeMode:]
0x1123da0c -[LynxUIImage coverStart]
0x1123da1c -[LynxUIImage setCoverStart:]
0x1123da2c -[LynxUIImage src]
0x1123da3c -[LynxUIImage setSrc:]
0x1123da50 -[LynxUIImage placeholder]
0x1123da60 -[LynxUIImage setPlaceholder:]
0x1123da74 -[LynxUIImage blurRadius]
0x1123da84 -[LynxUIImage setBlurRadius:]
0x1123da94 -[LynxUIImage capInsets]
0x1123daac -[LynxUIImage setCapInsets:]
0x1123dac4 -[LynxUIImage capInsetsScale]
0x1123dad4 -[LynxUIImage setCapInsetsScale:]
0x1123dae4 -[LynxUIImage image]
0x1123daf4 -[LynxUIImage setImage:]
0x1123db08 -[LynxUIImage cancelBlocks]
0x1123db18 -[LynxUIImage setCancelBlocks:]
0x1123db2c -[LynxUIImage loopCount]
0x1123db3c -[LynxUIImage setLoopCount:]
0x1123db4c -[LynxUIImage preFetchWidth]
0x1123db5c -[LynxUIImage setPreFetchWidth:]
0x1123db6c -[LynxUIImage preFetchHeight]
0x1123db7c -[LynxUIImage setPreFetchHeight:]
0x1123db8c -[LynxUIImage downsampling]
0x1123db9c -[LynxUIImage setDownsampling:]
0x1123dbac -[LynxUIImage autoSize]
0x1123dbbc -[LynxUIImage setAutoSize:]
0x1123dbcc -[LynxUIImage .cxx_destruct]
0x1123fe18 -[LynxUIScroller init]
0x1123fe94 -[LynxUIScroller createView]
0x1123ff6c -[LynxUIScroller adjustContentOffsetForRTL]
0x11240148 -[LynxUIScroller layoutDidFinished]
0x112401a0 -[LynxUIScroller updateContentSize]
0x112405e4 -[LynxUIScroller contentOffset]
0x11240640 -[LynxUIScroller setScrollY:requestReset:]
0x1124065c -[LynxUIScroller setScrollX:requestReset:]
0x1124067c -[LynxUIScroller setScrollYReverse:requestReset:]
0x112407c8 -[LynxUIScroller setScrollXReverse:requestReset:]
0x11240918 -[LynxUIScroller setScrollLeft:requestReset:]
0x112409c8 -[LynxUIScroller setScrollTop:requestReset:]
0x11240a6c -[LynxUIScroller setScrollToIndex:requestReset:]
0x11240c34 -[LynxUIScroller setScrollBarEnable:requestReset:]
0x11240cbc -[LynxUIScroller setBounces:requestReset:]
0x11240d04 -[LynxUIScroller setEnableScroll:requestReset:]
0x11240d4c -[LynxUIScroller setUpperThreshold:requestReset:]
0x11240d64 -[LynxUIScroller setLowerThreshold:requestReset:]
0x11240d7c -[LynxUIScroller getHitTestPoint:]
0x11240eac -[LynxUIScroller eventDidSet]
0x1124106c -[LynxUIScroller onScrollSticky:withOffsetY:]
0x1124118c -[LynxUIScroller sendScrollEvent:]
0x1124149c -[LynxUIScroller scrollViewDidScroll:]
0x11241598 -[LynxUIScroller scrollViewDidEndDecelerating:]
0x11241680 -[LynxUIScroller scrollViewDidEndDragging:willDecelerate:]
0x1124176c -[LynxUIScroller scrollInto:isSmooth:blockType:inlineType:]
```

```
0x11241c64 -[LynxUIScroller sendScrollEvent:scrollTop:scollleft:scrollHeight:scrollWidt
h:deltaX:deltaY:]
0x11241f30 -[LynxUIScroller contentSizeDidChanged]
0x1124213c -[LynxUIScroller clampScrollToPosition:]
0x1124224c -[LynxUIScroller scrollTo:withResult:]
0x112424cc -[LynxUIScroller autoScroll:withResult:]
0x112425ac -[LynxUIScroller startAutoScrollWithRate:]
0x112426d4 -[LynxUIScroller stopAutoScroll]
0x11242734 -[LynxUIScroller dealloc]
0x112427b0 -[LynxUIScroller frameDidChange]
0x1124286c -[LynxUIScroller scrollLeftLimit]
0x11242900 -[LynxUIScroller scrollRightLimit]
0x112429fc -[LynxUIScroller scrollUpLimit]
0x11242a90 -[LynxUIScroller scrollDownLimit]
0x11242b8c -[LynxUIScroller canScroll:]
0x11242cb8 -[LynxUIScroller scroll:direction:]
0x11242e04 -[LynxUIScroller scrollByX:]
0x11242e14 -[LynxUIScroller scrollByY:]
0x11242e24 -[LynxUIScroller flick:direction:]
0x11243054 -[LynxUIScroller flickX:]
0x11243064 -[LynxUIScroller flickY:]
0x11243074 -[LynxUIScroller enableSticky]
0x11243084 -[LynxUIScroller setEnableSticky:]
0x11243094 -[LynxUIScroller enableScrollY]
0x112430a4 -[LynxUIScroller setEnableScrollY:]
0x112430b4 -[LynxUIScroller .cxx_destruct]
0x1124518c -[LynxView initWithCoder:]
0x11245224 -[LynxView onLongPress]
0x11245250 -[LynxView init]
0x11245260 -[LynxView initWithFrame:]
0x112452d8 -[LynxView initWithBuilderBlock:]
0x11245434 -[LynxView initWithoutRender]
0x11245524 -[LynxView getLifecycleDispatcher]
0x11245534 -[LynxView requestLayoutWhenSafepointEnable]
0x11245538 -[LynxView updateScreenMetricsWithWidth:height:]
0x11245550 -[LynxView updateFontScale:]
0x11245570 -[LynxView initLifecycleDispatcher]
0x11245644 -[LynxView loadTemplate:withURL:]
0x11245654 -[LynxView loadTemplateFromURL:]
0x11245664 -[LynxView loadTemplate:withURL:initData:]
0x112457a8 -[LynxView dispatchError:]
0x112458e0 -[LynxView loadTemplateFromURL:initData:]
0x112459f8 -[LynxView hotModuleReplace:withPaths:]
0x11245ad4 -[LynxView findUIByIndex:]
0x11245b08 -[LynxView setGlobalPropsWithDictionary:]
0x11245b7c -[LynxView setGlobalPropsWithTemplateData:]
0x11245bf0 -[LynxView updateDataWithString:]
0x11245c00 -[LynxView updateDataWithString:processorName:]
0x11245ca0 -[LynxView updateDataWithDictionary:]
0x11245cb0 -[LynxView updateDataWithDictionary:processorName:]
0x11245d50 -[LynxView updateDataWithTemplateData:]
0x11245dc4 -[LynxView resetDataWithTemplateData:]
0x11245e38 -[LynxView getCurrentData]
0x11245e6c -[LynxView onEnterForeground]
0x11245f24 -[LynxView onEnterBackground]
0x11245fd8 -[LynxView sendGlobalEvent:withParams:]
```

```
0x11246078 -[LynxView sendGlobalEventToLepus:withParams:]
0x11246118 -[LynxView setFrame:]
0x1124614c -[LynxView layoutSubviews]
0x112461bc -[LynxView invalidateIntrinsicContentSize]
0x11246208 -[LynxView triggerLayout]
0x11246234 -[LynxView setEnableRadonCompatible:]
0x11246244 -[LynxView setEnableTextNonContiguousLayout:]
0x11246254 -[LynxView enableTextNonContiguousLayout]
0x112462cc -[LynxView intrinsicContentSize]
0x112462e0 -[LynxView setIntrinsicContentSize:]
0x11246334 -[LynxView updateViewport]
0x11246360 -[LynxView updateViewportWithPreferredLayoutWidth:preferredLayoutHeight:]
0x11246370 -[LynxView updateViewportWithPreferredLayoutWidth:preferredLayoutHeight:need
Layout:]
0x112463f4 -[LynxView client]
0x11246428 -[LynxView setClient:]
0x112465d4 -[LynxView setImageFetcher:]
0x11246664 -[LynxView setResourceFetcher:]
0x112466f4 -[LynxView reset]
0x11246824 -[LynxView dispatchViewDidStartLoading]
0x112468c4 -[LynxView willMoveToWindow:]
0x1124696c -[LynxView didMoveToWindow]
0x112469dc -[LynxView tapOnUICalloutBarButton:withEvent:]
0x11246de0 -[LynxView hitTest:withEvent:]
0x112471cc -[LynxView clearForDestroy]
0x112474a8 -[LynxView dealloc]
0x1124759c -[LynxView viewWithName:]
0x11247618 -[LynxView findViewWithName:]
0x11247694 -[LynxView uiWithName:]
0x11247710 -[LynxView viewWithIdSelector:]
0x1124778c -[LynxView uiWithIdSelector:]
0x11247808 -[LynxView cardVersion]
0x1124783c -[LynxView lynxConfigInfo]
0x1124788c -[LynxView forceGetPerf]
0x11247894 -[LynxView getJSModule:]
0x11247910 -[LynxView getLynxRuntimeId]
0x11247944 -[LynxView pauseRootLayoutAnimation]
0x11247970 -[LynxView resumeRootLayoutAnimation]
0x1124799c -[LynxView addLifecycleClient:]
0x112479fc -[LynxView setTheme:]
0x11247a70 -[LynxView theme]
0x11247aa4 -[LynxView setEnableAsyncDisplay:]
0x11247ad0 -[LynxView enableAsyncDisplay]
0x11247af0 -[LynxView resetAnimation]
0x11247b1c -[LynxView restartAnimation]
0x11247b48 -[LynxView layoutHeightMode]
0x11247b6c -[LynxView setLayoutHeightMode:]
0x11247b98 -[LynxView layoutWidthMode]
0x11247bbc -[LynxView setLayoutWidthMode:]
0x11247be8 -[LynxView preferredMaxLayoutWidth]
0x11247c0c -[LynxView setPreferredMaxLayoutWidth:]
0x11247c38 -[LynxView preferredMaxLayoutHeight]
0x11247c5c -[LynxView setPreferredMaxLayoutHeight:]
0x11247c88 -[LynxView preferredLayoutWidth]
0x11247cac -[LynxView setPreferredLayoutWidth:]
0x11247cd8 -[LynxView preferredLayoutHeight]
```

```
0x11247cfc -[LynxView setPreferredLayoutHeight:]
0x11247d28 -[LynxView url]
0x11247d5c -[LynxView baseInspectorOwner]
0x11247e0c -[LynxView detachRender]
0x11247e24 -[LynxView attachTemplateRender:]
0x11247ec0 -[LynxView processLayout:withURL:initData:]
0x11247fa0 -[LynxView processRender]
0x11248144 -[LynxView isLayoutFinish]
0x1124815c -[LynxView resetViewAndLayer]
0x11248230 -[LynxView getAllJsSource]
0x11248264 -[LynxView rootWidth]
0x11248288 -[LynxView rootHeight]
0x112482ac -[LynxView isUIRunningMode]
0x112482bc -[LynxView imageFetcher]
0x112482dc -[LynxView resourceFetcher]
0x112482fc -[LynxView catchAllException]
0x1124830c -[LynxView setCatchAllException:]
0x1124831c -[LynxView attached]
0x1124832c -[LynxView setAttached:]
0x1124833c -[LynxView lifecycleDispatcher]
0x1124834c -[LynxView setLifecycleDispatcher:]
0x11248360 -[LynxView templateRender]
0x11248370 -[LynxView setTemplateRender:]
0x11248384 -[LynxView .cxx_destruct]
```

总体来说，还是有点用的。尤其是 `--analyze`

jtool2用法举例：MaskPro.dylib

-h

```
➜  DynamicLibraries export ARCH=arm64
➜  DynamicLibraries jtool2 -h MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_h_header.txt
```

输出：

```
Magic:    64-bit MachO (Little Endian)
Type:    dylib
CPU:    ARM64 (ARMv8)
Cmds:    24
Size:    3304
Flags:    0x100085
```

-l

```
➜  DynamicLibraries jtool2 -l MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_l_list.txt
```

输出：

```
LC 00: LC_SEGMENT_64              Mem: 0x000000000-0x40000    __TEXT
    Mem: 0x0000078e4-0x00003e3e0       __TEXT.__text    (Normal)
    Mem: 0x00003e3e0-0x00003e5e4       __TEXT.__stubs    (Symbol Stubs)
    Mem: 0x00003e5e4-0x00003e800       __TEXT.__stub_helper    (Normal)
    Mem: 0x00003e800-0x00003f2c0       __TEXT.__const
    Mem: 0x00003f2c0-0x00003fb08       __TEXT.__objc_methname    (C-String Literals)
    Mem: 0x00003fb08-0x00003fb3e       __TEXT.__cstring    (C-String Literals)
    Mem: 0x00003fb3e-0x00003fb8d       __TEXT.__objc_classname    (C-String Literals)
    Mem: 0x00003fb8d-0x00003fc0a       __TEXT.__objc_methtype    (C-String Literals)
    Mem: 0x00003fc0c-0x00003fee4       __TEXT.__gcc_except_tab
    Mem: 0x00003fee4-0x00003fff4       __TEXT.__unwind_info
LC 01: LC_SEGMENT_64              Mem: 0x000040000-0x48000    __DATA
    Mem: 0x000040000-0x000040030       __DATA.__got    (Non-Lazy Symbol Ptrs)
    Mem: 0x000040030-0x000040188       __DATA.__la_symbol_ptr    (Lazy Symbol Ptrs)
    Mem: 0x000040188-0x000040190       __DATA.__mod_init_func    (Module Init Function Ptrs)
    Mem: 0x000040190-0x000040290       __DATA.__const
    Mem: 0x000040290-0x0000402b0       __DATA.__cfstring
    Mem: 0x0000402b0-0x0000402d8       __DATA.__objc_classlist    (Normal)
    Mem: 0x0000402d8-0x0000402e0       __DATA.__objc_imageinfo
    Mem: 0x0000402e0-0x0000408b0       __DATA.__objc_const
    Mem: 0x0000408b0-0x000040b90       __DATA.__objc_selrefs    (Literal Pointers)
    Mem: 0x000040b90-0x000040c60       __DATA.__objc_classrefs    (Normal)
    Mem: 0x000040c60-0x000040df0       __DATA.__objc_data
```

```
    Mem: 0x000040df0-0x000044ea8         __DATA.__data
    Mem: 0x000044ea8-0x000044fb4         __DATA.__bss     (Zero Fill)
    Mem: 0x000044fb4-0x000045170         __DATA.__common     (Zero Fill)
LC 02: LC_SEGMENT_64              Mem: 0x000048000-0x4c000     __LLVM
    Mem: 0x000048000-0x000048001         __LLVM.__bundle
LC 03: LC_SEGMENT_64              Mem: 0x00004c000-0x50000     __LINKEDIT
LC 04: LC_ID_DYLIB               /Library/MobileSubstrate/DynamicLibraries/MaskPro.dyli
b
LC 05: LC_DYLD_INFO
       Rebase info: 184   bytes at offset 311296 (0x4c000-0x4c0b8)
       Bind info:   1208  bytes at offset 311480 (0x4c0b8-0x4c570)
    No Weak info
       Lazy info:   944   bytes at offset 312688 (0x4c570-0x4c920)
       Export info: 1568  bytes at offset 313632 (0x4c920-0x4cf40)
LC 06: LC_SYMTAB
LC 07: LC_DYSYMTAB
        1 local symbols at index     0
      121 external symbols at index  1
       75 undefined symbols at index 122
       No TOC
       No modtab
       92 Indirect symbols at offset 0x4dc10
LC 08: LC_UUID                   UUID: AEBF7878-1DF0-373D-89C5-6B4DA33631D1
LC 09: LC_VERSION_MIN_IPHONEOS    Minimum iOS version:    8.0.0
LC 10: LC_SOURCE_VERSION         Source Version:         0.0.0.0.0
LC 11: LC_ENCRYPTION_INFO_64     Encryption: 0 from offset 16384 spanning 245760 bytes
LC 12: LC_LOAD_DYLIB             /System/Library/Frameworks/AdSupport.framework/AdSuppo
rt
LC 13: LC_LOAD_DYLIB             /usr/lib/libMobileGestalt.dylib
LC 14: LC_LOAD_DYLIB             /System/Library/Frameworks/UIKit.framework/UIKit
LC 15: LC_LOAD_DYLIB             /System/Library/Frameworks/Foundation.framework/Founda
tion
LC 16: LC_LOAD_DYLIB             /Library/Frameworks/CydiaSubstrate.framework/CydiaSubs
trate
LC 17: LC_LOAD_DYLIB             /usr/lib/libobjc.A.dylib
LC 18: LC_LOAD_DYLIB             /usr/lib/libc++.1.dylib
LC 19: LC_LOAD_DYLIB             /usr/lib/libSystem.B.dylib
LC 20: LC_LOAD_DYLIB             /System/Library/Frameworks/CoreFoundation.framework/Co
reFoundation
LC 21: LC_FUNCTION_STARTS        Offset:    315200, Size:    128 (0x4cf40-0x4cfc0)
LC 22: LC_DATA_IN_CODE           Offset:    315328, Size:      0 (0x4cfc0-0x4cfc0)
LC 23: LC_CODE_SIGNATURE         Offset:    321424, Size:   4528 (0x4e790-0x4f940)
```

-L

```
➜  DynamicLibraries jtool2 -L MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_L_librar
y.txt
```

输出：

```
MaskPro.dylib:
    /System/Library/Frameworks/AdSupport.framework/AdSupport (compatibility version 1.0
.0, current version 1.0.0)
```

```
    /usr/lib/libMobileGestalt.dylib (compatibility version 1.0.0, current version 1.0.0)

    /System/Library/Frameworks/UIKit.framework/UIKit (compatibility version 1.0.0, curr
ent version 61000.0.0)
    /System/Library/Frameworks/Foundation.framework/Foundation (compatibility version 3
00.0.0, current version 1677.104.0)
    /Library/Frameworks/CydiaSubstrate.framework/CydiaSubstrate (compatibility version
0.0.0, current version 0.0.0)
    /usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)
    /usr/lib/libc++.1.dylib (compatibility version 1.0.0, current version 902.0.0)
    /usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1281.100.1)

    /System/Library/Frameworks/CoreFoundation.framework/CoreFoundation (compatibility v
ersion 150.0.0, current version 1677.104.0)
```

-S

```
➜  DynamicLibraries jtool2 -S MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_S_symbol
.txt
```

输出：

```
0000000000040d28 D _OBJC_CLASS_$_NbGzxsksqtAxgN
0000000000040c88 D _OBJC_CLASS_$_NxNXRxsbBxexSx
0000000000040cd8 D _OBJC_CLASS_$_daAxbxbayGwxtxdcca
0000000000040d78 D _OBJC_CLASS_$_xrxleWZnuCXPEx
0000000000040dc8 D _OBJC_CLASS_$_xxWxKxrETCxJpx
0000000000040d00 D _OBJC_METACLASS_$_NbGzxsksqtAxgN
0000000000040c60 D _OBJC_METACLASS_$_NxNXRxsbBxexSx
0000000000040cb0 D _OBJC_METACLASS_$_daAxbxbayGwxtxdcca
0000000000040d50 D _OBJC_METACLASS_$_xrxleWZnuCXPEx
0000000000040da0 D _OBJC_METACLASS_$_xxWxKxrETCxJpx
0000000000044fb4 S _g_slide
00000000000450f8 S _x
00000000000450fc S _x.146
。。。
0000000000044fdc S _y.382
                 U _CC_MD5
                 U _MGCopyAnswer
                 U _MSHookFunction
                 U _MSHookMessageEx
                 U _NSClassFromString
                 U _NSFileSystemFreeSize
                 U _NSHomeDirectory
                 U _OBJC_CLASS_$_ASIdentifierManager
                 U _OBJC_CLASS_$_NSBundle
                 U _OBJC_CLASS_$_NSData
                 U _OBJC_CLASS_$_NSDate
                 U _OBJC_CLASS_$_NSDateFormatter
                 U _OBJC_CLASS_$_NSDictionary
                 U _OBJC_CLASS_$_NSFileManager
                 U _OBJC_CLASS_$_NSJSONSerialization
```

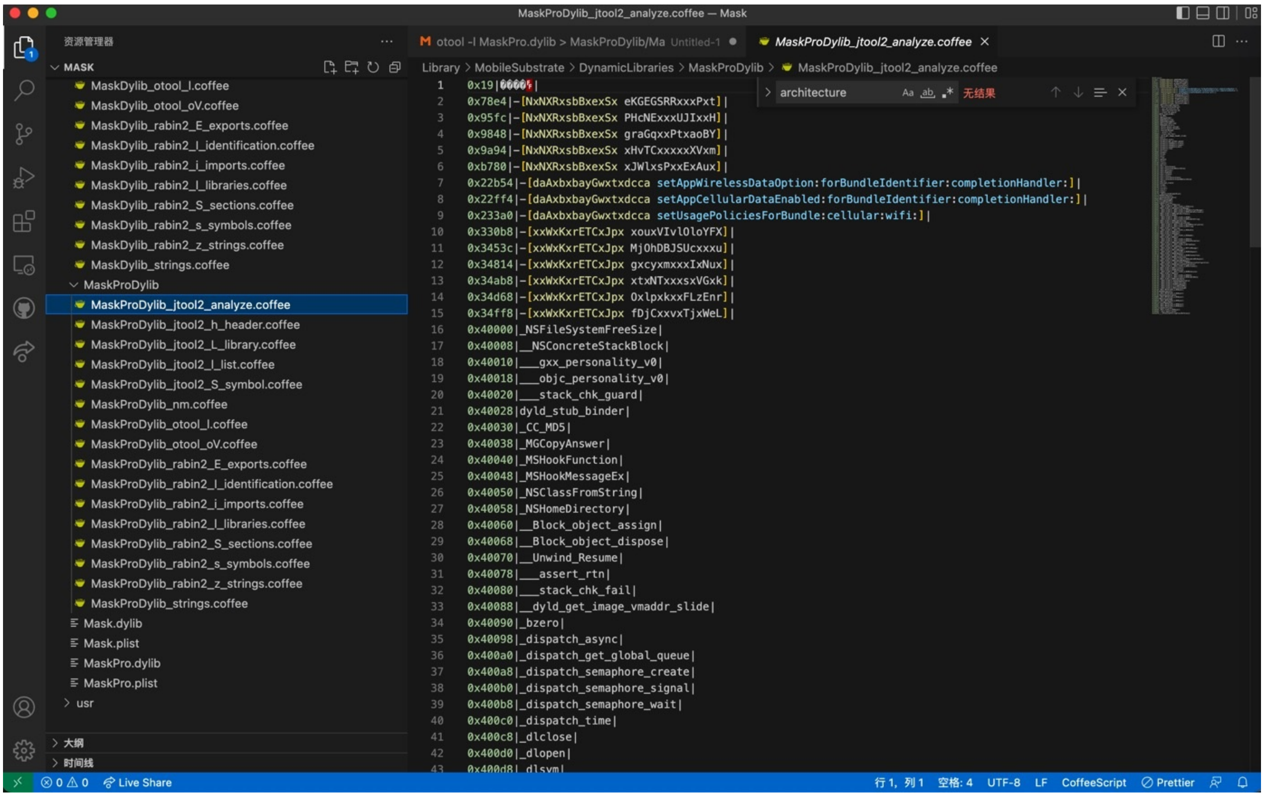
```
U _OBJC_CLASS_$_NSMutableData
U _OBJC_CLASS_$_NSMutableDictionary
U _OBJC_CLASS_$_NSMutableString
U _OBJC_CLASS_$_NSMutableURLRequest
U _OBJC_CLASS_$_NSNumber
U _OBJC_CLASS_$_NSObject
U _OBJC_CLASS_$_NSString
U _OBJC_CLASS_$_NSTimeZone
U _OBJC_CLASS_$_NSURL
U _OBJC_CLASS_$_NSURLConnection
U _OBJC_CLASS_$_NSURLRequest
U _OBJC_CLASS_$_NSURLSession
U _OBJC_CLASS_$_NSURLSessionConfiguration
U _OBJC_CLASS_$_UIDevice
U _OBJC_METACLASS_$_NSObject
U __Block_object_assign
U __Block_object_dispose
U __NSConcreteGlobalBlock
U __NSConcreteStackBlock
U __Unwind_Resume
U ___CFConstantStringClassReference
U ___assert_rtn
U ___gxx_personality_v0
U ___objc_personality_v0
U ___stack_chk_fail
U ___stack_chk_guard
U __dyld_get_image_vmaddr_slide
U __objc_empty_cache
U _bzero
U _dispatch_async
U _dispatch_get_global_queue
U _dispatch_semaphore_create
U _dispatch_semaphore_signal
U _dispatch_semaphore_wait
U _dispatch_time
U _dlclose
U _dlopen
U _dlsym
U _exit
U _free
U _getpid
U _ioctl
U _isatty
U _malloc
U _objc_autorelease
U _objc_autoreleaseReturnValue
U _objc_getClass
U _objc_msgSend
U _objc_release
U _objc_retain
U _objc_retainAutorelease
U _objc_retainAutoreleasedReturnValue
U _perror
U _pthread_create
U _sleep
U _strstr
```

```
                  U _syscall
                  U _sysctl
                  U _uname
                  U dyld_stub_binder
```

`--analyze`

```
➜  DynamicLibraries jtool2 --analyze MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_a
nalyze.txt
Analyzing file...
processLoadCommands: Not a Mach-O magic (0xbebafeca)
Resolving stubs..
Not ARM64 - will not resolve stubs..
Processing __DATA..
opened companion file ./MaskPro.dylib.ARM64.AEBF7878-1DF0-373D-89C5-6B4DA33631D1
Dumping symbol cache to file
Symbolicated 131 symbols and 0 functions
➜  DynamicLibraries mv MaskPro.dylib.ARM64.AEBF7878-1DF0-373D-89C5-6B4DA33631D1 MaskPro
Dylib/MaskProDylib_jtool2_analyze.txt
```

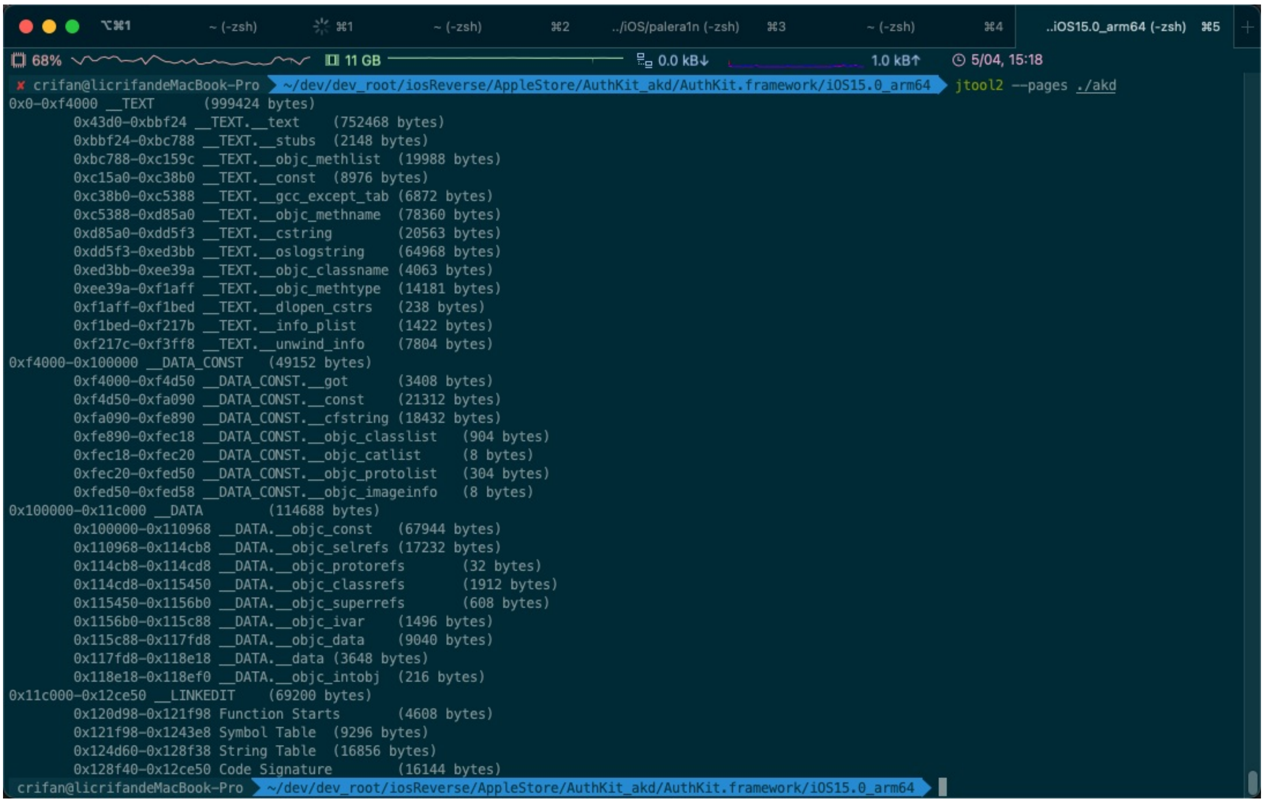
输出：



akd

--pages

```
✘ crifan@licrifandeMacBook-Pro  ~/dev/dev_root/iosReverse/AppleStore/AuthKit_akd/AuthKit.framework/iOS15.0_arm64  jtool2 --pages ./akd
0x0-0xf4000 __TEXT    (999424 bytes)
    0x43d0-0xbbf24 __TEXT.__text    (752468 bytes)
    0xbbf24-0xbc788 __TEXT.__stubs    (2148 bytes)
    0xbc788-0xc159c __TEXT.__objc_methlist    (19988 bytes)
    0xc15a0-0xc38b0 __TEXT.__const    (8976 bytes)
    0xc38b0-0xc5388 __TEXT.__gcc_except_tab    (6872 bytes)
    0xc5388-0xd85a0 __TEXT.__objc_methname    (78360 bytes)
    0xd85a0-0xdd5f3 __TEXT.__cstring    (20563 bytes)
    0xdd5f3-0xed3bb __TEXT.__oslogstring    (64968 bytes)
    0xed3bb-0xee39a __TEXT.__objc_classname    (4063 bytes)
    0xee39a-0xf1aff __TEXT.__objc_methtype    (14181 bytes)
    0xf1aff-0xf1bed __TEXT.__dlopen_cstrs    (238 bytes)
    0xf1bed-0xf217b __TEXT.__info_plist    (1422 bytes)
    0xf217c-0xf3ff8 __TEXT.__unwind_info    (7804 bytes)
0xf4000-0x100000 __DATA_CONST    (49152 bytes)
    0xf4000-0xf4d50 __DATA_CONST.__got    (3408 bytes)
    0xf4d50-0xfa090 __DATA_CONST.__const    (21312 bytes)
    0xfa090-0xfe890 __DATA_CONST.__cfstring    (18432 bytes)
    0xfe890-0xfec18 __DATA_CONST.__objc_classlist    (904 bytes)
    0xfec18-0xfec20 __DATA_CONST.__objc_catlist    (8 bytes)
    0xfec20-0xfed50 __DATA_CONST.__objc_protolist    (304 bytes)
    0xfed50-0xfed58 __DATA_CONST.__objc_imageinfo    (8 bytes)
0x100000-0x11c000 __DATA    (114688 bytes)
    0x100000-0x110968 __DATA.__objc_const    (67944 bytes)
    0x110968-0x114cb8 __DATA.__objc_selrefs    (17232 bytes)
    0x114cb8-0x114cd8 __DATA.__objc_protorefs    (32 bytes)
    0x114cd8-0x115450 __DATA.__objc_classrefs    (1912 bytes)
    0x115450-0x1156b0 __DATA.__objc_superrefs    (608 bytes)
    0x1156b0-0x115c88 __DATA.__objc_ivar    (1496 bytes)
    0x115c88-0x117fd8 __DATA.__objc_data    (9040 bytes)
    0x117fd8-0x118e18 __DATA.__data    (3648 bytes)
    0x118e18-0x118ef0 __DATA.__objc_intobj    (216 bytes)
0x11c000-0x12ce50 __LINKEDIT    (69200 bytes)
    0x120d98-0x121f98 Function Starts    (4608 bytes)
    0x121f98-0x1243e8 Symbol Table    (9296 bytes)
    0x124d60-0x128f38 String Table    (16856 bytes)
    0x128f40-0x12ce50 Code Signature    (16144 bytes)
```



```
✘ crifan@licrifandeMacBook-Pro  ~/dev/dev_root/iosReverse/AppleStore/AuthKit_akd/AuthKit.framework/iOS15.0_arm64  jtool2 --pages ./akd
0x0-0xf4000 __TEXT       (999424 bytes)
        0x43d0-0xbbf24 __TEXT.__text     (752468 bytes)
        0xbbf24-0xbc788 __TEXT.__stubs  (2148 bytes)
        0xbc788-0xc159c __TEXT.__objc_methlist  (19988 bytes)
        0xc15a0-0xc38b0 __TEXT.__const  (8976 bytes)
        0xc38b0-0xc5388 __TEXT.__gcc_except_tab (6872 bytes)
        0xc5388-0xd85a0 __TEXT.__objc_methname  (78360 bytes)
        0xd85a0-0xdd5f3 __TEXT.__cstring        (20563 bytes)
        0xdd5f3-0xed3bb __TEXT.__oslogstring    (64968 bytes)
        0xed3bb-0xee39a __TEXT.__objc_classname (4063 bytes)
        0xee39a-0xf1aff __TEXT.__objc_methtype  (14181 bytes)
        0xf1aff-0xf1bed __TEXT.__dlopen_cstrs   (238 bytes)
        0xf1bed-0xf217b __TEXT.__info_plist     (1422 bytes)
        0xf217c-0xf3ff8 __TEXT.__unwind_info    (7804 bytes)
0xf4000-0x100000 __DATA_CONST   (49152 bytes)
        0xf4000-0xf4d50 __DATA_CONST.__got      (3408 bytes)
        0xf4d50-0xfa090 __DATA_CONST.__const    (21312 bytes)
        0xfa090-0xfe890 __DATA_CONST.__cfstring (18432 bytes)
        0xfe890-0xfec18 __DATA_CONST.__objc_classlist   (904 bytes)
        0xfec18-0xfec20 __DATA_CONST.__objc_catlist     (8 bytes)
        0xfec20-0xfed50 __DATA_CONST.__objc_protolist   (304 bytes)
        0xfed50-0xfed58 __DATA_CONST.__objc_imageinfo   (8 bytes)
0x100000-0x11c000 __DATA        (114688 bytes)
        0x100000-0x110968 __DATA.__objc_const   (67944 bytes)
        0x110968-0x114cb8 __DATA.__objc_selrefs (17232 bytes)
        0x114cb8-0x114cd8 __DATA.__objc_protorefs       (32 bytes)
        0x114cd8-0x115450 __DATA.__objc_classrefs       (1912 bytes)
        0x115450-0x1156b0 __DATA.__objc_superrefs       (608 bytes)
        0x1156b0-0x115c88 __DATA.__objc_ivar    (1496 bytes)
        0x115c88-0x117fd8 __DATA.__objc_data    (9040 bytes)
        0x117fd8-0x118e18 __DATA.__data (3648 bytes)
        0x118e18-0x118ef0 __DATA.__objc_intobj  (216 bytes)
0x11c000-0x12ce50 __LINKEDIT    (69200 bytes)
        0x120d98-0x121f98 Function Starts       (4608 bytes)
        0x121f98-0x1243e8 Symbol Table  (9296 bytes)
        0x124d60-0x128f38 String Table  (16856 bytes)
        0x128f40-0x12ce50 Code Signature        (16144 bytes)
 crifan@licrifandeMacBook-Pro  ~/dev/dev_root/iosReverse/AppleStore/AuthKit_akd/AuthKit.framework/iOS15.0_arm64
```

结果分析：

arm64的akd二进制内部的偏移量：

- 整个 `TEXT` 代码段是： `0x0-0xf4000 __TEXT (999424 bytes = 976KB)`
  - 我们要找到的，单独是程序的二进制代码是： `0x43d0-0xbbf24 __TEXT.__text (752468 bytes)` = 约734.8KB

jtool2的help语法

```
➜  ~ jtool2 --help
Usage: jtool [options] _filename_

OTool Compatible Options:
   -h               Dump Mach-O (or DYLD Shared Cache) header
   -l               List sections/commands in binary
   -L               print shared libraries used

JTool (classic) Options:
   -S               List Symbols (like NM)
   -v[v]            Toggle verbosity (vv = very verbose)
   -e               extract fat slice, Mach-O segment/section, dyld shared cache dylib or
(NEW) kernelcache kext
   -q               Quick operation - do not process any symbols in the Mach-O
   -F               find all occurrences of _string_ in binary
   -a               Find offset/segment corresponding to virtual address _addr_
   -o               Find address corresponding to offset _offset_
   -d               Dump (smart dump, will disassemble text and dump data by autodetecting
)

Code Signing Options:
   --sig            Show code signature in binary (if any)
   --stripsig       Remove existing code signature (useful for MacOS unrestricting)
   --ent            Show entitlements in binary (if any)
   -+ent=...[,...]      Inject entitlements into binary (implies resigning inplace)
   -+platformize      Platformize binary (injects platform-application, also implies resi
gning inplace)

Joker Compatible Options (applicable on kernel caches only):
   -k               List kexts
   -K               Kextract™ a kernel extension by its bundle ID
   -dec             Decompress a kernelcache to /tmp/kernel (no longer necessary since JT
ool can now operate on compressed caches)

dyldinfo Compatible Options:
   --bind               print addresses dyld will set based on symbolic lookups
   --lazy_bind          print addresses dyld will lazily set on first use
   --opcodes            print opcodes used to generate the rebase and binding information
   --function_starts      print table of function start addresses

Newer (JTool 2) Options:
   --analyze        Analyze file and create a companion file
   --symbolicate      Symbolicate an .ips panic file
   --machoize        [text=0x...-0x...] [strings 0x....-0x...] [data 0x....-0x....] _file
name_
   --tbd            Create a .tbd file (for *OS private frameworks only - you'll need the
 dyld shared cache for this)
   --objc           Like old -d objc and/or classdumpZ - Mike, this is for you :-)
   -D               Decompile (totally experimental - would love your feedback if you're
reading this)
   -G               Gadget search (specify gadgets as comma delimited mnemonics)
```

```
    -W              Write [address] [value] - [value] is a string or 0x....

Environment Variables:
   ARCH                        Select architecture slice. Set to arm64, arm64e, arm64_32, a
rmv7, armv7k, x86_64 or (not for long) i386
   JCOLOR                      ANSI Colors. Note you'll need 'less -R' if piping output
   JTOOLDIR                    path to search for companion jtool files (default: $PWD).
            Use this to force create a file, if one does not exist
   NOPSUP                      Suppress NOPs in disassembly
   JENTS                       Default entitlements (comma separated) for --sign
   JHASH                       Choice of Hash algorithm for signing (SHA1,SHA256 (default),
 SHA256T, SHA384)
   JSHUDDUP                    Suppress stderr (risky, but useful)
   JDEBUG                      Enhanced debug output. May be very verbose
   JDEBUGCS                    Debug output specifically for code signing operations. Usefu
l to watch these step-by-step
   WITHSIGBLOB                 Code signing: Also create an empty CMS blob (no longer a def
ault due to CoreTrust)
```

otool

- `otool`
    - = `object file displaying tool`
    - 是什么：查看目标文件信息的工具
    - 用途：用来发现应用中使用到了哪些系统库，调用了其中哪些方法，使用了库中哪些对象及属性
        - 比如
            - 查看iOS的 `Mach-O` 格式的二进制文件的信息
    - 来源：Xcode自带的常用工具
- 相关
    - 比otool更好的： `jtool`
    - `otool` 的 `GUI` 版： `otx`
        - x43x61x69/otx: The Mach-O disassembler. Now 64bit and Xcode 6 compatible.
            - https://github.com/x43x61x69/otx

下载安装otool

Mac自带otool，无需额外安装。

查看当前otool位置：

```
✘ crifan@licrifandeMacBook-Pro ~ which otool
/usr/bin/otool
```

当前版本：

```
✘ crifan@licrifandeMacBook-Pro ~ otool --version
llvm-otool(1): Apple Inc. version cctools-927.0.2
Apple LLVM version 10.0.1 (clang-1001.0.46.4)
  Optimized build.
  Default target: x86_64-apple-darwin19.2.0
  Host CPU: broadwell

  Registered Targets:
    aarch64    - AArch64 (little endian)
    aarch64_be - AArch64 (big endian)
    arm        - ARM
    arm64      - ARM64 (little endian)
    armeb      - ARM (big endian)
    thumb      - Thumb
    thumbeb    - Thumb (big endian)
    x86        - 32-bit X86: Pentium-Pro and above
    x86-64     - 64-bit X86: EM64T and AMD64
```

otool用法

- 单个参数
  - `-l` : print the **l**oad commands

    ```
    otool -l iOSBinaryFile
    ```

  - `-L` : print shared **L**ibraries used

    ```
    otool -L iOSBinaryFile
    ```

  - `-o` : print the **O**bjective-C segment
  - `-V` : print disassembled operands symbolically
- 参数组合
  - `-oV`

    ```
    otool -oV iOSBinaryFile
    ```

  - `-tV`

    ```
    otool -tV iOSBinaryFile
    ```

- 用途
  - 用otool去手动计算地址转函数

    ```
    otool -arch <arch> -l <path_to_dsym> | grep __TEXT -m 2 -A 1 | grep vmaddr
    ```

常见问题

is not an object file

otool只支持查看Mach-O格式的文件，不支持其他格式的文件。

比如如果用otool查看ELF格式的话，会报错：

```
➜  arm64-v8a otool -L libtacker.so
libtacker.so: is not an object file

➜  arm64-v8a otool -oV libtacker.so
libtacker.so: is not an object file
```

otool用法举例

otool用法举例：Aweme

`-l`

```
➜  Aweme.app otool -l Aweme
Aweme:
Load command 0
      cmd LC_SEGMENT_64
  cmdsize 72
  segname __PAGEZERO
   vmaddr 0x0000000000000000
   vmsize 0x0000000100000000
  fileoff 0
 filesize 0
  maxprot 0x00000000
 initprot 0x00000000
   nsects 0
    flags 0x0
Load command 1
      cmd LC_SEGMENT_64
  cmdsize 552
  segname __TEXT
   vmaddr 0x0000000100000000
   vmsize 0x0000000000008000
  fileoff 0
 filesize 32768
  maxprot 0x00000005
 initprot 0x00000005
   nsects 6
    flags 0x0
Section
  sectname __text
   segname __TEXT
      addr 0x0000000100006af4
      size 0x00000000000011bc
    offset 27380
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x80000400
 reserved1 0
 reserved2 0
Section
  sectname __stubs
   segname __TEXT
      addr 0x0000000100007cb0
      size 0x00000000000000f0
    offset 31920
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x80000408
```

```
  reserved1 0 (index into indirect symbol table)
  reserved2 12 (size of stubs)
Section
  sectname __stub_helper
   segname __TEXT
      addr 0x0000000100007da0
      size 0x0000000000000108
    offset 32160
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x80000400
 reserved1 0
 reserved2 0
Section
  sectname __const
   segname __TEXT
      addr 0x0000000100007ea8
      size 0x0000000000000011
    offset 32424
     align 2^1 (2)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __cstring
   segname __TEXT
      addr 0x0000000100007eb9
      size 0x000000000000009b
    offset 32441
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000002
 reserved1 0
 reserved2 0
Section
  sectname __unwind_info
   segname __TEXT
      addr 0x0000000100007f54
      size 0x00000000000000ac
    offset 32596
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Load command 2
      cmd LC_SEGMENT_64
  cmdsize 792
  segname __DATA
   vmaddr 0x0000000100008000
   vmsize 0x0000000000004000
```

```
  fileoff 32768
 filesize 16384
  maxprot 0x00000003
 initprot 0x00000003
   nsects 9
    flags 0x0
Section
  sectname __got
   segname __DATA
      addr 0x0000000100008000
      size 0x0000000000000010
    offset 32768
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000006
 reserved1 20 (index into indirect symbol table)
 reserved2 0
Section
  sectname __la_symbol_ptr
   segname __DATA
      addr 0x0000000100008010
      size 0x00000000000000a0
    offset 32784
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000007
 reserved1 22 (index into indirect symbol table)
 reserved2 0
Section
  sectname __mod_init_func
   segname __DATA
      addr 0x00000001000080b0
      size 0x0000000000000008
    offset 32944
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000009
 reserved1 0
 reserved2 0
Section
  sectname __const
   segname __DATA
      addr 0x00000001000080b8
      size 0x0000000000000018
    offset 32952
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __objc_imageinfo
```

```
    segname __DATA
       addr 0x00000001000080d0
       size 0x0000000000000008
     offset 32976
      align 2^2 (4)
     reloff 0
     nreloc 0
      flags 0x00000000
  reserved1 0
  reserved2 0
Section
   sectname __swift_hooks
    segname __DATA
       addr 0x00000001000080d8
       size 0x00000000000000b8
     offset 32984
      align 2^3 (8)
     reloff 0
     nreloc 0
      flags 0x00000000
  reserved1 0
  reserved2 0
Section
   sectname __data
    segname __DATA
       addr 0x0000000100008190
       size 0x0000000000000015
     offset 33168
      align 2^3 (8)
     reloff 0
     nreloc 0
      flags 0x00000000
  reserved1 0
  reserved2 0
Section
   sectname __swift51_hooks
    segname __DATA
       addr 0x00000001000081a8
       size 0x00000000000000b8
     offset 33192
      align 2^3 (8)
     reloff 0
     nreloc 0
      flags 0x00000000
  reserved1 0
  reserved2 0
Section
   sectname __bss
    segname __DATA
       addr 0x0000000100008260
       size 0x00000000000000d8
     offset 0
      align 2^3 (8)
     reloff 0
     nreloc 0
      flags 0x00000001
```

```
  reserved1 0
  reserved2 0
Load command 3
      cmd LC_SEGMENT_64
  cmdsize 152
  segname __DATA_CONST
   vmaddr 0x000000010000c000
   vmsize 0x0000000000208000
  fileoff 49152
 filesize 0
  maxprot 0x00000003
 initprot 0x00000003
   nsects 1
    flags 0x0
Section
  sectname __objc_selrefs
   segname __DATA_CONST
      addr 0x000000010000c000
      size 0x00000000002054d2
    offset 0
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000001
 reserved1 0
 reserved2 0
Load command 4
      cmd LC_SEGMENT_64
  cmdsize 152
  segname __OBJC
   vmaddr 0x0000000100214000
   vmsize 0x0000000000000000
  fileoff 49152
 filesize 0
  maxprot 0x00000001
 initprot 0x00000001
   nsects 1
    flags 0x0
Section
  sectname __message_refs
   segname __OBJC
      addr 0x0000000100214000
      size 0x0000000000000000
    offset 49152
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Load command 5
      cmd LC_SEGMENT_64
  cmdsize 72
  segname __LINKEDIT
   vmaddr 0x0000000100214000
   vmsize 0x0000000000008000
```

```
  fileoff 49152
 filesize 24304
  maxprot 0x00000001
 initprot 0x00000001
   nsects 0
    flags 0x0
Load command 6
            cmd LC_DYLD_INFO_ONLY
        cmdsize 48
     rebase_off 49152
    rebase_size 16
       bind_off 49168
      bind_size 56
  weak_bind_off 0
 weak_bind_size 0
  lazy_bind_off 49224
 lazy_bind_size 416
     export_off 0
    export_size 0
Load command 7
     cmd LC_SYMTAB
 cmdsize 24
  symoff 49672
   nsyms 22
  stroff 50192
 strsize 320
Load command 8
            cmd LC_DYSYMTAB
        cmdsize 80
      ilocalsym 0
      nlocalsym 1
     iextdefsym 1
     nextdefsym 0
      iundefsym 1
      nundefsym 21
         tocoff 0
           ntoc 0
      modtaboff 0
        nmodtab 0
   extrefsymoff 0
    nextrefsyms 0
 indirectsymoff 50024
  nindirectsyms 42
      extreloff 0
        nextrel 0
      locreloff 0
        nlocrel 0
Load command 9
          cmd LC_LOAD_DYLINKER
      cmdsize 32
         name /usr/lib/dyld (offset 12)
Load command 10
     cmd LC_UUID
 cmdsize 24
    uuid 31ED6D91-1868-36F5-89B8-C39FBF7D01E3
Load command 11
```

```
      cmd LC_VERSION_MIN_IPHONEOS
  cmdsize 16
  version 10.0
      sdk 15.0
Load command 12
      cmd LC_SOURCE_VERSION
  cmdsize 16
  version 0.0
Load command 13
       cmd LC_MAIN
   cmdsize 24
  entryoff 31896
 stacksize 0
Load command 14
          cmd LC_ENCRYPTION_INFO_64
      cmdsize 24
     cryptoff 28672
    cryptsize 4096
      cryptid 1
          pad 0
Load command 15
          cmd LC_LOAD_DYLIB
      cmdsize 64
         name @rpath/AwemeCore.framework/AwemeCore (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1.0.0
compatibility version 1.0.0
Load command 16
          cmd LC_LOAD_DYLIB
      cmdsize 88
         name /System/Library/Frameworks/Foundation.framework/Foundation (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1854.0.0
compatibility version 300.0.0
Load command 17
          cmd LC_LOAD_DYLIB
      cmdsize 56
         name /usr/lib/libobjc.A.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 228.0.0
compatibility version 1.0.0
Load command 18
          cmd LC_LOAD_DYLIB
      cmdsize 56
         name /usr/lib/libSystem.B.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1311.0.0
compatibility version 1.0.0
Load command 19
          cmd LC_LOAD_DYLIB
      cmdsize 56
         name @rpath/libswiftCore.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1300.0.29
compatibility version 1.0.0
Load command 20
```

```
           cmd LC_RPATH
       cmdsize 32
          path /usr/lib/swift (offset 12)
Load command 21
           cmd LC_RPATH
       cmdsize 40
          path @executable_path/Frameworks (offset 12)
Load command 22
       cmd LC_FUNCTION_STARTS
   cmdsize 16
   dataoff 49640
  datasize 32
Load command 23
       cmd LC_DATA_IN_CODE
   cmdsize 16
   dataoff 49672
  datasize 0
Load command 24
       cmd LC_CODE_SIGNATURE
   cmdsize 16
   dataoff 50512
  datasize 22944
```

查看是否加密=脱壳

- 未加密

  ```
  ➜  Aweme.app otool -l Aweme | grep crypt
       cryptoff 28672
      cryptsize 4096
        cryptid 0
  ```

  - 说明
    - `cryptid 0`：表示未加密 = 已脱壳
- 已加密

  ```
  ➜  Aweme.app pwd
  xxx/Aweme抖音/iPhone7-137black/Aweme.app
  ➜  Aweme.app otool -l Aweme | grep crypt
       cryptoff 28672
      cryptsize 4096
        cryptid 1
  ```

  - 说明
    - `cryptid 1`：表示已加密 = 未脱壳

-L

```
➜  Aweme.app otool -L Aweme
Aweme:
    @rpath/AwemeCore.framework/AwemeCore (compatibility version 1.0.0, current version
```

```
1.0.0)
    /System/Library/Frameworks/Foundation.framework/Foundation (compatibility version 3
00.0.0, current version 1854.0.0)
    /usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)
    /usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1311.0.0)
    @rpath/libswiftCore.dylib (compatibility version 1.0.0, current version 1300.0.29)
```

otool用法举例：AwemeCore

- 输入文件：

```
/Users/crifan/dev/DevRoot/iOSReverse/Aweme/exportFromiPhone/iPhone7P-1341/Aweme.app
/Frameworks/AwemeCore.framework

➜  AwemeCore.framework ll
total 10208480
-rw-r--r--  1 crifan  staff   230M  1  8 09:43 AwemeCore
```

`-l`

```
➜  AwemeCore.framework otool -l AwemeCore > otool_l_AwemeCore.txt
```

输出内容（很多，有2000多行）：

```
AwemeCore:
Load command 0
      cmd LC_SEGMENT_64
  cmdsize 1752
  segname __TEXT
   vmaddr 0x0000000000000000
   vmsize 0x0000000000304000
  fileoff 0
 filesize 3162112
  maxprot 0x00000005
 initprot 0x00000005
   nsects 21
    flags 0x0
Section
  sectname __stub_helper
   segname __TEXT
      addr 0x000000000000b9b0
      size 0x00000000000084c0
    offset 47536
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x80000400
 reserved1 0
 reserved2 0
Section
  sectname __const
   segname __TEXT
      addr 0x0000000000013e70
      size 0x0000000000004020
    offset 81520
     align 2^4 (16)
    reloff 0
```

```
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __swift5_typeref
   segname __TEXT
      addr 0x0000000000017e90
      size 0x0000000000002ef8
    offset 97936
     align 2^4 (16)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __swift5_fieldmd
   segname __TEXT
      addr 0x000000000001ad88
      size 0x0000000000002988
    offset 109960
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __swift5_proto
   segname __TEXT
      addr 0x000000000001d710
      size 0x0000000000000338
    offset 120592
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __swift5_types
   segname __TEXT
      addr 0x000000000001da48
      size 0x000000000000028c
    offset 121416
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __cstring
   segname __TEXT
      addr 0x000000000001dcd4
```

```
      size 0x0000000000000000
    offset 122068
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000002
 reserved1 0
 reserved2 0
Section
  sectname __objc_methname
   segname __TEXT
      addr 0x000000000001dcd4
      size 0x0000000000000000
    offset 122068
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000002
 reserved1 0
 reserved2 0
Section
  sectname __objc_classname
   segname __TEXT
      addr 0x000000000001dcd4
      size 0x0000000000000000
    offset 122068
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000002
 reserved1 0
 reserved2 0
Section
  sectname __objc_methtype
   segname __TEXT
      addr 0x000000000001dcd4
      size 0x0000000000000000
    offset 122068
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000002
 reserved1 0
 reserved2 0
Section
  sectname __gcc_except_tab
   segname __TEXT
      addr 0x000000000001dcd4
      size 0x0000000000000068
    offset 122068
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
```

```
'''
Section
  sectname __PUZZLEMETHOD__
   segname __DATA
      addr 0x0000000000d627a8
      size 0x0000000000000050
    offset 14034856
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname IESSLynxBridge
   segname __DATA
      addr 0x0000000000d627f8
      size 0x0000000000000010
    offset 14034936
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname RxAnnotation
   segname __DATA
      addr 0x0000000000d62808
      size 0x0000000000000050
    offset 14034952
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __objc_clsrefs
   segname __DATA
      addr 0x0000000000d62858
      size 0x0000000000004850
    offset 14035032
     align 2^3 (8)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __thread_vars
   segname __DATA
      addr 0x0000000000d670a8
      size 0x00000000000006c0
    offset 14053544
     align 2^3 (8)
```

```
    reloff 0
    nreloc 0
     flags 0x00000013
 reserved1 0
 reserved2 0
...
Section
  sectname _D_ustring
   segname __DATA
      addr 0x00000000047e5194
      size 0x000000000007795a
    offset 0
     align 2^1 (2)
    reloff 0
    nreloc 0
     flags 0x00000001
 reserved1 0
 reserved2 0
Section
  sectname _D_objc_methname
   segname __DATA
      addr 0x000000000485caee
      size 0x0000000000ae06ba
    offset 0
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000001
 reserved1 0
 reserved2 0
Section
  sectname _D_objc_methtype
   segname __DATA
      addr 0x000000000533d1a8
      size 0x00000000001ca962
    offset 0
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000001
 reserved1 0
 reserved2 0
Section
  sectname __common
   segname __DATA
      addr 0x0000000005507c00
      size 0x000000000017fc48
    offset 0
     align 2^10 (1024)
    reloff 0
    nreloc 0
     flags 0x00000001
 reserved1 0
 reserved2 0
Section
  sectname __bss
```

```
   segname __DATA
      addr 0x0000000005687900
      size 0x000000000029b0ec
    offset 0
     align 2^8 (256)
    reloff 0
    nreloc 0
     flags 0x00000001
 reserved1 0
 reserved2 0
Load command 2
      cmd LC_SEGMENT_64
  cmdsize 232
  segname __BD_TEXT
   vmaddr 0x0000000005924000
   vmsize 0x0000000000bb5c000
  fileoff 16269312
 filesize 196460544
  maxprot 0x00000005
 initprot 0x00000005
   nsects 2
    flags 0x0
Section
  sectname __text
   segname __BD_TEXT
      addr 0x0000000005924000
      size 0x0000000000bb52a38
    offset 16269312
     align 2^14 (16384)
    reloff 0
    nreloc 0
     flags 0x80000400
 reserved1 0
 reserved2 0
Section
  sectname __stubs
   segname __BD_TEXT
      addr 0x0000000011476a38
      size 0x0000000000008508
    offset 212691512
     align 2^2 (4)
    reloff 0
    nreloc 0
     flags 0x80000408
 reserved1 4410 (index into indirect symbol table)
 reserved2 12 (size of stubs)
Load command 3
      cmd LC_SEGMENT_64
  cmdsize 712
  segname __LTC_DATA
   vmaddr 0x0000000011480000
   vmsize 0x00000000011e0000
  fileoff 212729856
 filesize 18743296
  maxprot 0x00000001
 initprot 0x00000001
```

```
    nsects 8
     flags 0x0
...
Section
  sectname _C_gcc_except_ta
   segname __LTC_DATA
      addr 0x000000001232e92d
      size 0x000000000024ca15
    offset 228124973
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Section
  sectname __fix
   segname __LTC_DATA
      addr 0x000000001257b342
      size 0x00000000000e1298
    offset 230536002
     align 2^0 (1)
    reloff 0
    nreloc 0
     flags 0x00000000
 reserved1 0
 reserved2 0
Load command 4
      cmd LC_SEGMENT_64
  cmdsize 72
  segname __LINKEDIT
   vmaddr 0x0000000012660000
   vmsize 0x00000000008c8000
  fileoff 231473152
 filesize 9193456
  maxprot 0x00000001
 initprot 0x00000001
   nsects 0
    flags 0x0
Load command 5
          cmd LC_ID_DYLIB
      cmdsize 64
         name @rpath/AwemeCore.framework/AwemeCore (offset 24)
   time stamp 1 Thu Jan  1 08:00:01 1970
      current version 1.0.0
compatibility version 1.0.0
Load command 6
            cmd LC_DYLD_INFO_ONLY
        cmdsize 48
     rebase_off 231473152
    rebase_size 350072
       bind_off 231823224
      bind_size 292520
  weak_bind_off 232115744
 weak_bind_size 296
  lazy_bind_off 232116040
```

```
  lazy_bind_size 101024
      export_off 232217064
     export_size 384
Load command 7
     cmd LC_SYMTAB
 cmdsize 24
  symoff 234432864
   nsyms 5030
  stroff 234542336
 strsize 146360
Load command 8
            cmd LC_DYSYMTAB
        cmdsize 80
      ilocalsym 0
      nlocalsym 1
     iextdefsym 1
     nextdefsym 0
      iundefsym 1
      nundefsym 5029
         tocoff 0
           ntoc 0
      modtaboff 0
        nmodtab 0
   extrefsymoff 0
    nextrefsyms 0
 indirectsymoff 234513344
  nindirectsyms 7248
      extreloff 0
        nextrel 0
      locreloff 0
        nlocrel 0
Load command 9
     cmd LC_UUID
 cmdsize 24
    uuid F1FCF15A-6465-31F0-9300-5BA1B8F91017
Load command 10
      cmd LC_VERSION_MIN_IPHONEOS
  cmdsize 16
  version 10.0
      sdk 15.0
Load command 11
      cmd LC_SOURCE_VERSION
  cmdsize 16
  version 0.0
Load command 12
          cmd LC_ENCRYPTION_INFO_64
      cmdsize 24
     cryptoff 32768
    cryptsize 3112960
      cryptid 0
          pad 0
Load command 13
          cmd LC_LOAD_DYLIB
      cmdsize 56
         name /usr/lib/libcompression.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
```

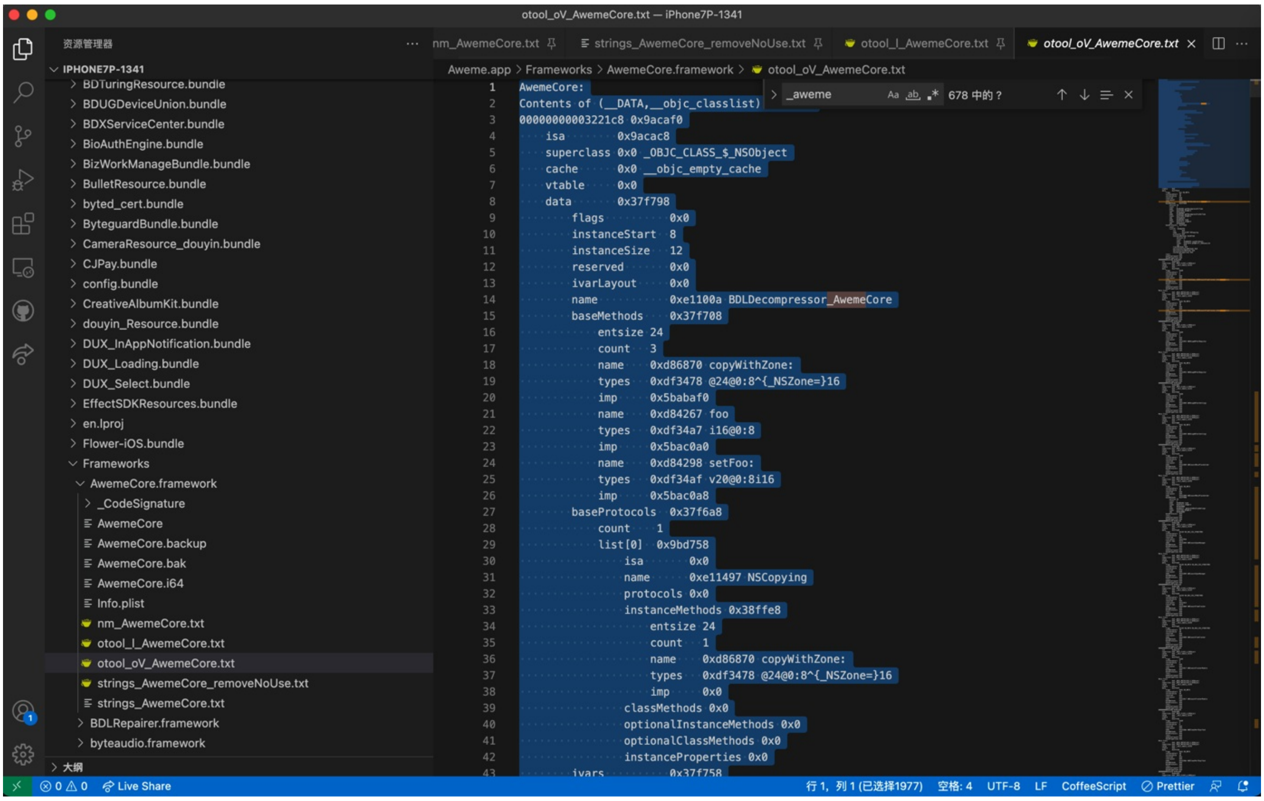
```
      current version 1.0.0
compatibility version 1.0.0
Load command 14
          cmd LC_LOAD_DYLIB
      cmdsize 72
         name @rpath/BDLRepairer.framework/BDLRepairer (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1.0.0
compatibility version 1.0.0
Load command 15
          cmd LC_LOAD_DYLIB
      cmdsize 48
         name /usr/lib/libc++.1.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1200.3.0
compatibility version 1.0.0
...
Load command 123
          cmd LC_LOAD_WEAK_DYLIB
      cmdsize 48
         name @rpath/libswiftos.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 1021.0.0
compatibility version 1.0.0
Load command 124
          cmd LC_LOAD_WEAK_DYLIB
      cmdsize 56
         name @rpath/libswiftsimd.dylib (offset 24)
   time stamp 2 Thu Jan  1 08:00:02 1970
      current version 9.0.0
compatibility version 1.0.0
Load command 125
          cmd LC_RPATH
      cmdsize 32
         path /usr/lib/swift (offset 12)
Load command 126
          cmd LC_RPATH
      cmdsize 40
         path @executable_path/Frameworks (offset 12)
Load command 127
          cmd LC_RPATH
      cmdsize 40
         path @loader_path/Frameworks (offset 12)
Load command 128
          cmd LC_RPATH
      cmdsize 48
         path @executable_path/../../Frameworks (offset 12)
Load command 129
          cmd LC_RPATH
      cmdsize 40
         path @executable_path/Frameworks (offset 12)
Load command 130
      cmd LC_FUNCTION_STARTS
  cmdsize 16
  dataoff 232217448
 datasize 2214096
```

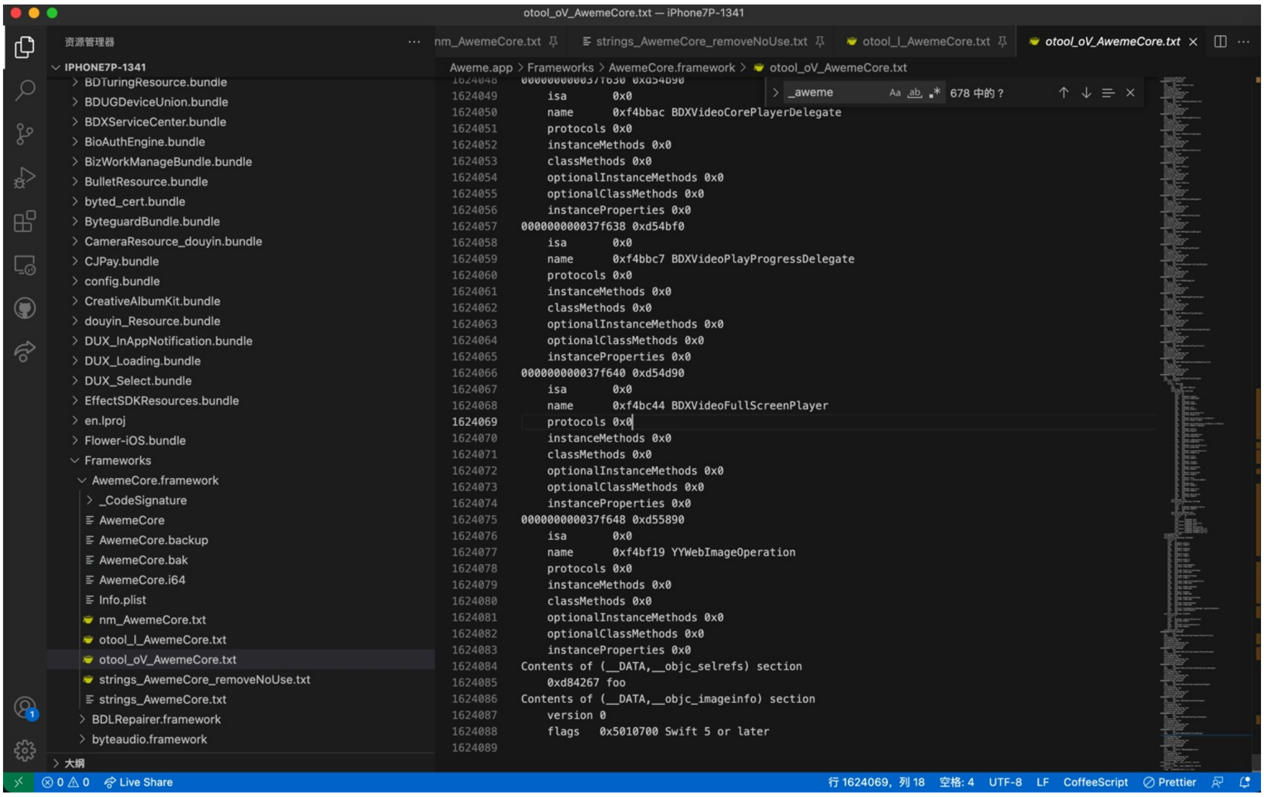
```
Load command 131
       cmd LC_DATA_IN_CODE
   cmdsize 16
   dataoff 234431544
  datasize 1320
Load command 132
       cmd LC_CODE_SIGNATURE
   cmdsize 16
   dataoff 234688704
  datasize 5977904
```

-oV

```
➜  AwemeCore.framework otool -oV AwemeCore > otool_oV_AwemeCore.txt
```

输出（共16万行）：






```
AwemeCore:
Contents of (__DATA,__objc_classlist) section
00000000003221c8 0x9acaf0
    isa        0x9acac8
    superclass 0x0 _OBJC_CLASS_$_NSObject
    cache      0x0 __objc_empty_cache
    vtable     0x0
    data       0x37f798
        flags          0x0
        instanceStart  8
        instanceSize   12
        reserved       0x0
        ivarLayout     0x0
        name           0xe1100a BDLDecompressor_AwemeCore
        baseMethods    0x37f708
            entsize 24
            count   3
            name    0xd86870 copyWithZone:
            types   0xdf3478 @24@0:8^{_NSZone=}16
            imp     0x5babaf0
            name    0xd84267 foo
            types   0xdf34a7 i16@0:8
            imp     0x5bac0a0
            name    0xd84298 setFoo:
            types   0xdf34af v20@0:8i16
            imp     0x5bac0a8
        baseProtocols  0x37f6a8
            count    1
            list[0]  0x9bd758
                isa       0x0
                name      0xe11497 NSCopying
                protocols 0x0
```

```
                instanceMethods 0x38ffe8
                    entsize 24
                    count   1
                    name    0xd86870 copyWithZone:
                    types   0xdf3478 @24@0:8^{_NSZone }16
                    imp     0x0
                classMethods 0x0
                optionalInstanceMethods 0x0
                optionalClassMethods 0x0
                instanceProperties 0x0
        ivars          0x37f758
            entsize   32
            count     1
            offset    0x9ab740 8
            name      0xd842a0 _foo
            type      0xdf34ba i
            alignment 2
            size      4
        weakIvarLayout 0x0
        baseProperties 0x37f780
            entsize    16
            count      1
            name       0xd84267 foo
            attributes 0xd842a5 Ti,N,V_foo
Meta Class
    isa        0x0 _OBJC_METACLASS_$_NSObject
    superclass 0x0 _OBJC_METACLASS_$_NSObject
    cache      0x0 __objc_empty_cache
...
000000000037f630 0xd54b90
    isa       0x0
    name      0xf4bbac BDXVideoCorePlayerDelegate
    protocols 0x0
    instanceMethods 0x0
    classMethods 0x0
    optionalInstanceMethods 0x0
    optionalClassMethods 0x0
    instanceProperties 0x0
000000000037f638 0xd54bf0
    isa       0x0
    name      0xf4bbc7 BDXVideoPlayProgressDelegate
    protocols 0x0
    instanceMethods 0x0
    classMethods 0x0
    optionalInstanceMethods 0x0
    optionalClassMethods 0x0
    instanceProperties 0x0
000000000037f640 0xd54d90
    isa       0x0
    name      0xf4bc44 BDXVideoFullScreenPlayer
    protocols 0x0
    instanceMethods 0x0
    classMethods 0x0
    optionalInstanceMethods 0x0
    optionalClassMethods 0x0
    instanceProperties 0x0
```

```
0000000000037f648 0xd55890
    isa       0x0
    name      0xf4bf19 YYWebImageOperation
    protocols 0x0
    instanceMethods 0x0
    classMethods 0x0
    optionalInstanceMethods 0x0
    optionalClassMethods 0x0
    instanceProperties 0x0
Contents of (__DATA,__objc_selrefs) section
    0xd84267 foo
Contents of (__DATA,__objc_imageinfo) section
    version 0
    flags   0x5010700 Swift 5 or later
```

输出内容分析

其中也有AWECloudJailBreakUtility：

```
0000000000322a18 0x9bf000
    isa        0x9befd8
    superclass 0x0 _OBJC_CLASS_$_NSObject
    cache      0x0 __objc_empty_cache
    vtable     0x0
    data       0x3921f8
        flags          0x80
        instanceStart  8
        instanceSize   8
        reserved       0x0
        ivarLayout     0x0
        name           0xe12aaf AWECloudJailBreakUtility
        baseMethods    0x0
        baseProtocols  0x0
        ivars          0x0
        weakIvarLayout 0x0
        baseProperties 0x0
Meta Class
    isa        0x0 _OBJC_METACLASS_$_NSObject
    superclass 0x0 _OBJC_METACLASS_$_NSObject
    cache      0x0 __objc_empty_cache
    vtable     0x0
    data       0x3921b0
        flags          0x81 RO_META
        instanceStart  40
        instanceSize   40
        reserved       0x0
        ivarLayout     0x0
        name           0xe12aaf AWECloudJailBreakUtility
        baseMethods    0x0
        baseProtocols  0x0
        ivars          0x0
        weakIvarLayout 0x0
        baseProperties 0x0
```

且信息更全：

- 父类=superclass是： `_OBJC_METACLASS_$_NSObject`

对于：

- `name 0xe12aaf AWECloudJailBreakUtility`
    - ->好像是： `AWECloudJailBreakUtility` 这个类的位置是 `0xe12aaf`

-》如果是：则就是我们之前，曾想要的：

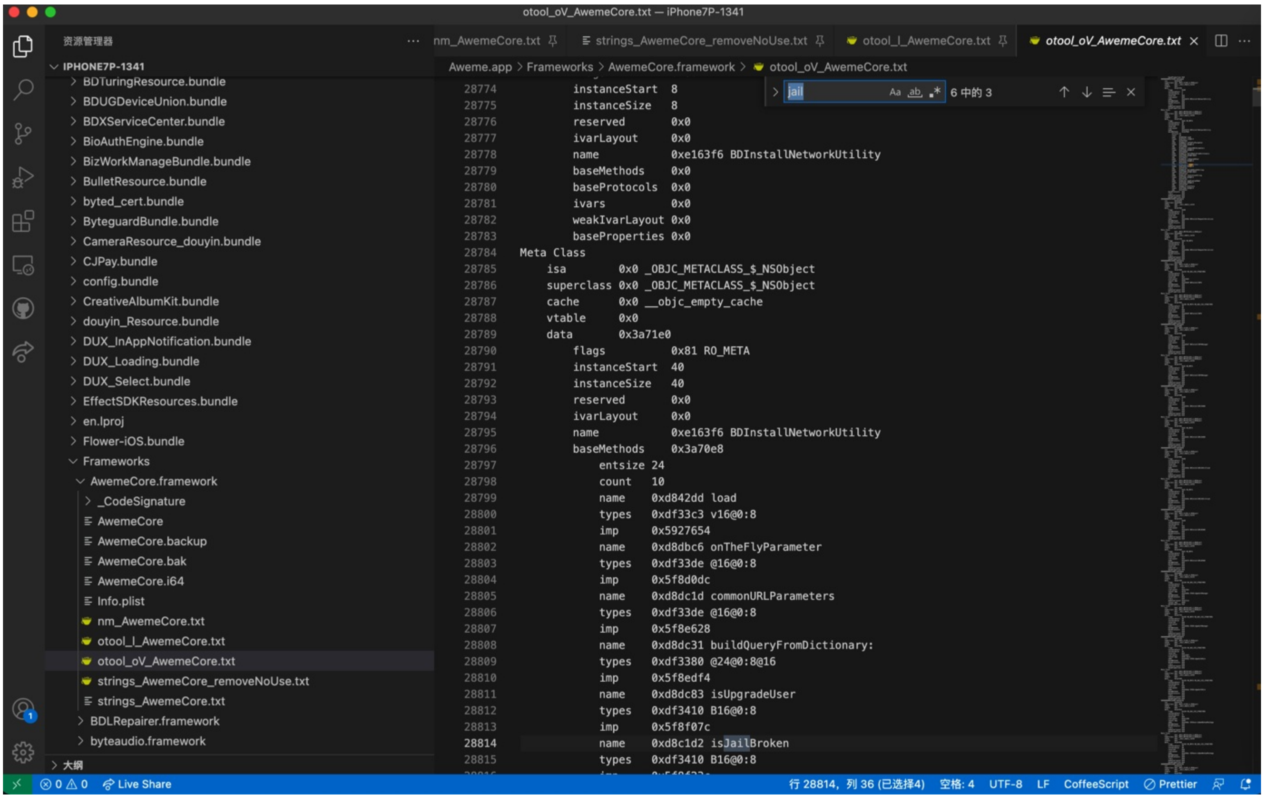
通过类名字： `AWECloudJailBreakUtility`

去寻找其具体地址： `0xe12aaf`

-> 用于去后续（lldb、XCode等）调试中，去打断点

另外搜： `jail`

也是能搜到，类似于strings找到的几个：




```
Meta Class
    isa        0x0 _OBJC_METACLASS_$_NSObject
    superclass 0x0 _OBJC_METACLASS_$_NSObject
    cache      0x0 __objc_empty_cache
    vtable     0x0
    data       0x3a71e0
        flags          0x81 RO_META
        instanceStart  40
        instanceSize   40
        reserved       0x0
        ivarLayout     0x0
        name           0xe163f6 BDInstallNetworkUtility
```

```
          baseMethods    0x3a70e8
              entsize 24
              count   10
              name    0xd842dd load
              types   0xdf33c3 v16@0:8
              imp     0x5927654
              name    0xd8dbc6 onTheFlyParameter
              types   0xdf33de @16@0:8
              imp     0x5f8d0dc
              name    0xd8dc1d commonURLParameters
              types   0xdf33de @16@0:8
              imp     0x5f8e628
              name    0xd8dc31 buildQueryFromDictionary:
              types   0xdf3380 @24@0:8@16
              imp     0x5f8edf4
              name    0xd8dc83 isUpgradeUser
              types   0xdf3410 B16@0:8
              imp     0x5f8f07c
              name    0xd8c1d2 isJailBroken
              types   0xdf3410 B16@0:8
              imp     0x5f8f23c
              name    0xd8dc91 decodeBase64String:
              types   0xdf3380 @24@0:8@16
              imp     0x5f8f3c8
              name    0xd8c1df resolutionString
              types   0xdf33de @16@0:8
              imp     0x5f8f44c
              name    0xd8c2a6 appDisplayName
              types   0xdf33de @16@0:8
              imp     0x5f8f528
              name    0xd8dc7a platform
              types   0xdf33de @16@0:8
              imp     0x5f8f62c
          baseProtocols  0x0
          ivars          0x0
          weakIvarLayout 0x0
          baseProperties 0x0
```

-》很明显，信息更全：

可以知道：

- symbol=符号=函数=function： `isJailBroken`
  - 所属的类是： `BDInstallNetworkUtility`
    - `name 0xe163f6 BDInstallNetworkUtility`
      - `superclass 0x0 _OBJC_METACLASS_$_NSObject`

其他还有一个： `isJailBroken`

```
Meta Class
    isa        0x0 _OBJC_METACLASS_$_NSObject
    superclass 0x0 _OBJC_METACLASS_$_NSObject
    cache      0x0 __objc_empty_cache
    vtable     0x0
```

```
    data        0x5f3678
        flags           0x81 RO_META
        instanceStart   40
        instanceSize    40
        reserved        0x0
        ivarLayout      0x0
        name            0xe8e38c TTInstallUtil
        baseMethods     0x5f34c0
            entsize 24
            count   18
            name    0xdc6a5b generateMockDeviceInfo
            types   0xdf33c3 v16@0:8
            imp     0x92ee848
            name    0xdc6a72 setResetMode:
            types   0xdf339e v20@0:8B16
            imp     0x92ee988
            name    0xdc6a80 isResetMode
            types   0xdf3410 B16@0:8
            imp     0x92eeab0
            name    0xd8fa16 setAutoReset:
            types   0xdf339e v20@0:8B16
            imp     0x92eeb1c
            name    0xd8fa24 isAutoReset
            types   0xdf3410 B16@0:8
            imp     0x92eeb74
            name    0xdc6a1e clearAllUserDefaultsData
            types   0xdf33c3 v16@0:8
            imp     0x92eebd0
            name    0xd842dd load
            types   0xdf33c3 v16@0:8
            imp     0x5927238
            name    0xd8bb2a uuid
            types   0xdf33de @16@0:8
            imp     0x92ec3f0
            name    0xd8dbc6 onTheFlyParameter
            types   0xdf33de @16@0:8
            imp     0x92ec444
            name    0xdc69ef isInHouseVersion
            types   0xdf3410 B16@0:8
            imp     0x5981a34
            name    0xd8dc1d commonURLParameters
            types   0xdf33de @16@0:8
            imp     0x92ed7e4
            name    0xd8dc31 buildQueryFromDictionary:
            types   0xdf3380 @24@0:8@16
            imp     0x92ee034
            name    0xd8dc83 isUpgradeUser
            types   0xdf3410 B16@0:8
            imp     0x92ee2bc
            name    0xdc6a00 loadUserDefaultsStringForKey:
            types   0xdf3380 @24@0:8@16
            imp     0x92ee4b0
            name    0xd8c1df resolutionString
            types   0xdf33de @16@0:8
            imp     0x92ee534
            name    0xd8c1d2 isJailBroken
```

```
            types   0xdf3410 B16@0:8
            imp     0x92ee610
            name    0xd8dc7a platform
            types   0xdf33de @16@0:8
            imp     0x92ee6f0
            name    0xd86653 authorizationStatus
            types   0xdf3437 Q16@0:8
            imp     0x92ee788
        baseProtocols  0x0
        ivars          0x0
        weakIvarLayout 0x0
        baseProperties 0x0
```

-》

- name 0xd8c1d2 isJailBroken
    - name 0xe8e38c TTInstallUtil
        - data 0x5f3678

其他几个：

```
000000000036aa78 0x3cd4a0
    name      0xe1bc2c BDXAdditions
    cls       0x0 _OBJC_CLASS_$_UIDevice
    instanceMethods 0x0
    classMethods 0x3cd150
        entsize 24
        count   35
        name    0xd98274 bdx_runningProcesses
        types   0xdf33de @16@0:8
        imp     0x62225dc
        name    0xd98227 getSysInfoByName:
        types   0xe05b74 @24@0:8*16
        imp     0x62228e8
        name    0xd98239 bdx_platform
        types   0xdf33de @16@0:8
        imp     0x6222960
        name    0xd98289 bdx_hwmodel
        types   0xdf33de @16@0:8
        imp     0x6222974
        name    0xd98246 bdx_platformType
        types   0xdf3437 Q16@0:8
        imp     0x6222988
        name    0xd981c1 bdx_platformName
        types   0xdf33de @16@0:8
        imp     0x62234c0
        name    0xd98295 bdx_platformString
        types   0xdf33de @16@0:8
        imp     0x622350c
        name    0xd98257 bdx_OSVersion
        types   0xdf33de @16@0:8
        imp     0x6223a28
        name    0xd982a8 bdx_OSVersionNumber
        types   0xdf34c8 f16@0:8
        imp     0x6223a74
```

```
        name    0xd982bc bdx_currentLanguage
        types   0xdf33de @16@0:8
        imp     0x6223ac0
        name    0xd982d0 bdx_currentRegion
        types   0xdf33de @16@0:8
        imp     0x6223b10
        name    0xd982e2 bdx_isJailBroken
        types   0xdf3410 B16@0:8
        imp     0x6223b68
        name    0xd982f3 bdx_carrierName
        types   0xdf33de @16@0:8
        imp     0x6223bfc
        name    0xd98303 bdx_carrierMCC
        types   0xdf33de @16@0:8
        imp     0x6223c64
        name    0xd98312 bdx_carrierMNC
        types   0xdf33de @16@0:8
        imp     0x6223ccc
        name    0xd98321 bdx_poorDevice
        types   0xdf3410 B16@0:8
        imp     0x6223d34
        name    0xd98330 bdx_screenScale
        types   0xdf3396 d16@0:8
        imp     0x6223dec
        name    0xd98340 bdx_is480Screen
        types   0xdf3410 B16@0:8
        imp     0x6223e38
        name    0xd98350 bdx_is568Screen
        types   0xdf3410 B16@0:8
        imp     0x6223e90
        name    0xd98360 bdx_is667Screen
        types   0xdf3410 B16@0:8
        imp     0x6223ee8
        name    0xd98370 bdx_is736Screen
        types   0xdf3410 B16@0:8
        imp     0x6223f40
        name    0xd98380 bdx_is812Screen
        types   0xdf3410 B16@0:8
        imp     0x6223f98
        name    0xd98390 bdx_is896Screen
        types   0xdf3410 B16@0:8
        imp     0x6223ff0
        name    0xd983a0 bdx_isScreenWidthLarge320
        types   0xdf3410 B16@0:8
        imp     0x6224048
        name    0xd96d2c bdx_isIPhoneXSeries
        types   0xdf3410 B16@0:8
        imp     0x62240ac
        name    0xd983ba bdx_screenSize
        types   0xdf420a {CGSize=dd}16@0:8
        imp     0x6224310
        name    0xd983c9 bdx_screenWidth
        types   0xdf3396 d16@0:8
        imp     0x622436c
        name    0xd983d9 bdx_screenHeight
        types   0xdf3396 d16@0:8
```

```
        imp     0x62243b8
        name    0xd983ea bdx_isPadDevice
        types   0xdf3410 B16@0:8
        imp     0x6224404
        name    0xd98265 bdx_resolution
        types   0xdf420a {CGSize dd}16@0:8
        imp     0x6224454
        name    0xd983fa bdx_resolutionString
        types   0xdf33de @16@0:8
        imp     0x62244e8
        name    0xd9840f bdx_onePixel
        types   0xdf3396 d16@0:8
        imp     0x6224534
        name    0xd9841c bdx_deviceWidthType
        types   0xdf3437 Q16@0:8
        imp     0x62245a4
        name    0xd98430 bdx_getTotalDiskSpace
        types   0xdf3302 q16@0:8
        imp     0x62246f4
        name    0xd98446 bdx_getFreeDiskSpace
        types   0xdf3302 q16@0:8
        imp     0x62247b0
    protocols 0x0
    instanceProperties 0x0
```

-》

- `name 0xd982e2 bdx_isJailBroken`
    - `name 0xe1bc2c BDXAdditions`
    - `cls 0x0 _OBJC_CLASS_$_UIDevice`
        - `000000000036aa78 0x3cd4a0`

以及：

```
000000000036aba8 0x3d60e0
    name      0xe1ce54 BTDAdditions
    cls       0x0 _OBJC_CLASS_$_UIDevice
    instanceMethods 0x0
    classMethods 0x3d5d90
        entsize 24
        count   35
        name    0xd99a94 btd_runningProcesses
        types   0xdf33de @16@0:8
        imp     0x62a5ec0
        name    0xd98227 getSysInfoByName:
        types   0xe05b74 @24@0:8*16
        imp     0x59911f8
        name    0xd8df0a btd_platform
        types   0xdf33de @16@0:8
        imp     0x59911e4
        name    0xd99aa9 btd_hwmodel
        types   0xdf33de @16@0:8
        imp     0x62a6230
        name    0xd99a74 btd_platformType
```

```
          types   0xdf3437 Q16@0:8
          imp     0x62a6244
          name    0xd8d746 btd_platformName
          types   0xdf33de @16@0:8
          imp     0x62a718c
          name    0xd8d733 btd_platformString
          types   0xdf33de @16@0:8
          imp     0x62a71e8
          name    0xd8c129 btd_OSVersion
          types   0xdf33de @16@0:8
          imp     0x5991188
          name    0xd99ab5 btd_OSVersionNumber
          types   0xdf34c8 f16@0:8
          imp     0x5b74794
          name    0xd8d757 btd_currentLanguage
          types   0xdf33de @16@0:8
          imp     0x62a75e4
          name    0xd99ac9 btd_currentRegion
          types   0xdf33de @16@0:8
          imp     0x62a7644
          name    0xd99adb btd_isJailBroken
          types   0xdf3410 B16@0:8
          imp     0x62a76ac
          name    0xd99aec btd_carrierName
          types   0xdf33de @16@0:8
          imp     0x62a7760
          name    0xd99afc btd_carrierMCC
          types   0xdf33de @16@0:8
          imp     0x62a77e0
          name    0xd99b0b btd_carrierMNC
          types   0xdf33de @16@0:8
          imp     0x62a7860
          name    0xd99b1a btd_poorDevice
          types   0xdf3410 B16@0:8
          imp     0x62a78e0
          name    0xd99b29 btd_screenScale
          types   0xdf3396 d16@0:8
          imp     0x62a79d4
          name    0xd99b39 btd_is480Screen
          types   0xdf3410 B16@0:8
          imp     0x62a7a30
          name    0xd99b49 btd_is568Screen
          types   0xdf3410 B16@0:8
          imp     0x62a7aa0
          name    0xd99b59 btd_is667Screen
          types   0xdf3410 B16@0:8
          imp     0x62a7b10
          name    0xd99b69 btd_is736Screen
          types   0xdf3410 B16@0:8
          imp     0x62a7b80
          name    0xd99b79 btd_is812Screen
          types   0xdf3410 B16@0:8
          imp     0x62a7bf0
          name    0xd99b89 btd_is896Screen
          types   0xdf3410 B16@0:8
          imp     0x62a7c60
```

```
        name    0xd99b99 btd_isScreenWidthLarge320
        types   0xdf3410 B16@0:8
        imp     0x62a7cd0
        name    0xd8cbb0 btd_isIPhoneXSeries
        types   0xdf3410 B16@0:8
        imp     0x62a7d44
        name    0xd99bb3 btd_screenSize
        types   0xdf420a {CGSize dd}16@0:8
        imp     0x62a8004
        name    0xd99bc2 btd_screenWidth
        types   0xdf3396 d16@0:8
        imp     0x5991320
        name    0xd99bd2 btd_screenHeight
        types   0xdf3396 d16@0:8
        imp     0x599137c
        name    0xd99be3 btd_isPadDevice
        types   0xdf3410 B16@0:8
        imp     0x5b1743c
        name    0xd99a85 btd_resolution
        types   0xdf420a {CGSize dd}16@0:8
        imp     0x5a03198
        name    0xd99bf3 btd_resolutionString
        types   0xdf33de @16@0:8
        imp     0x62a8068
        name    0xd99c08 btd_onePixel
        types   0xdf3396 d16@0:8
        imp     0x5b19920
        name    0xd99c15 btd_deviceWidthType
        types   0xdf3437 Q16@0:8
        imp     0x62a80b4
        name    0xd99c29 btd_getTotalDiskSpace
        types   0xdf3302 q16@0:8
        imp     0x62a8224
        name    0xd99c3f btd_getFreeDiskSpace
        types   0xdf3302 q16@0:8
        imp     0x62a8324
    protocols 0x0
    instanceProperties 0x0
```

-》

- name 0xd99adb btd_isJailBroken
  - name 0xe1ce54 BTDAdditions
  - cls 0x0 *OBJC_CLASS*$_UIDevice

-》前面2个：

- BDXAdditions
- BTDAdditions

都是属于：

- `cls 0x0 _OBJC_CLASS_$_UIDevice`

-》估计都是：

- 集成自 = 父类是：UIDevice

另外：

- BTDAdditions
  - btd_carrierName
  - btd_carrierMCC
  - btd_carrierMNC
  - btd_poorDevice

等，好像和：

- 检测当前设备信息
- 改机参数

有关 -》 也算是，和检测越狱有关?

`-tV`

```
➜  AwemeCore.framework otool -tV AwemeCore > otool_tV_AwemeCore.txt
```

输出：

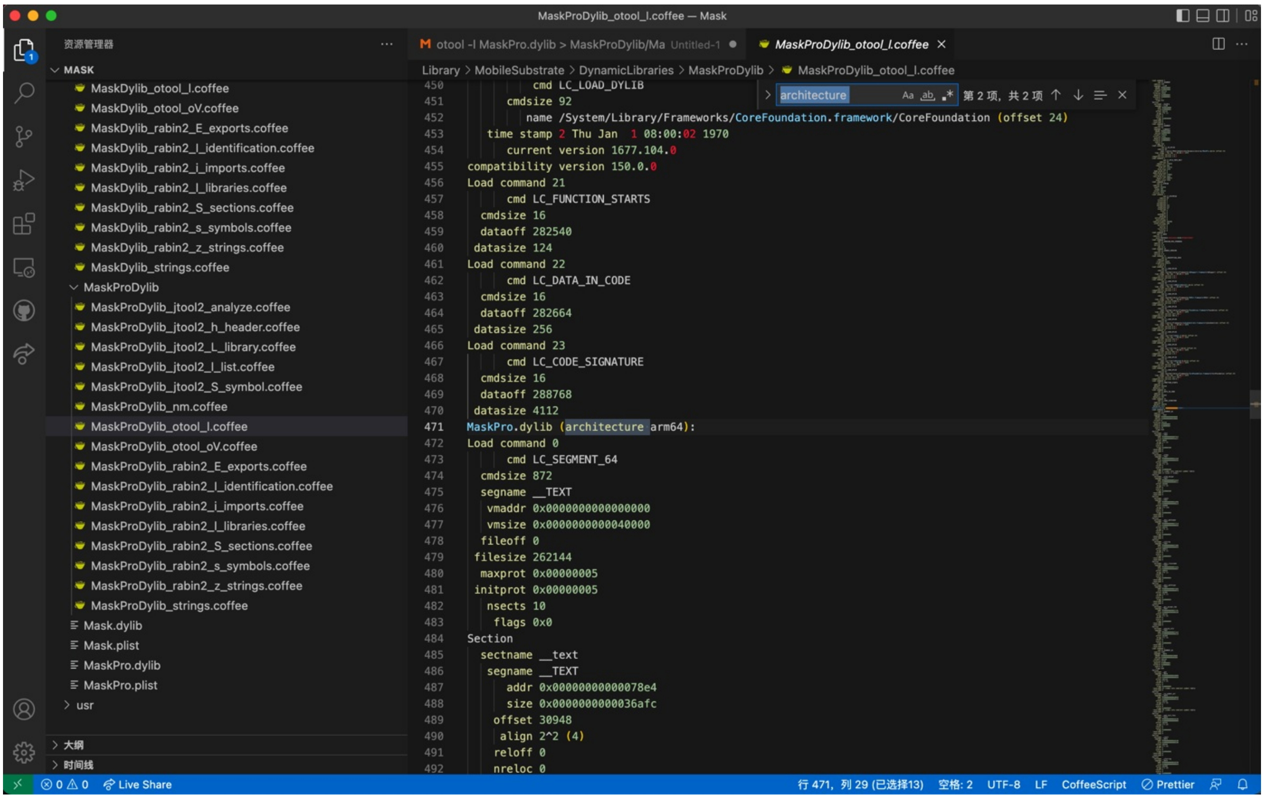
```
AwemeCore:
(__TEXT,__text) section
```

otool用法举例：MaskPro.dylib

`-l`

```
➜ DynamicLibraries otool -l MaskPro.dylib > MaskProDylib/MaskProDylib_otool_l.txt
```

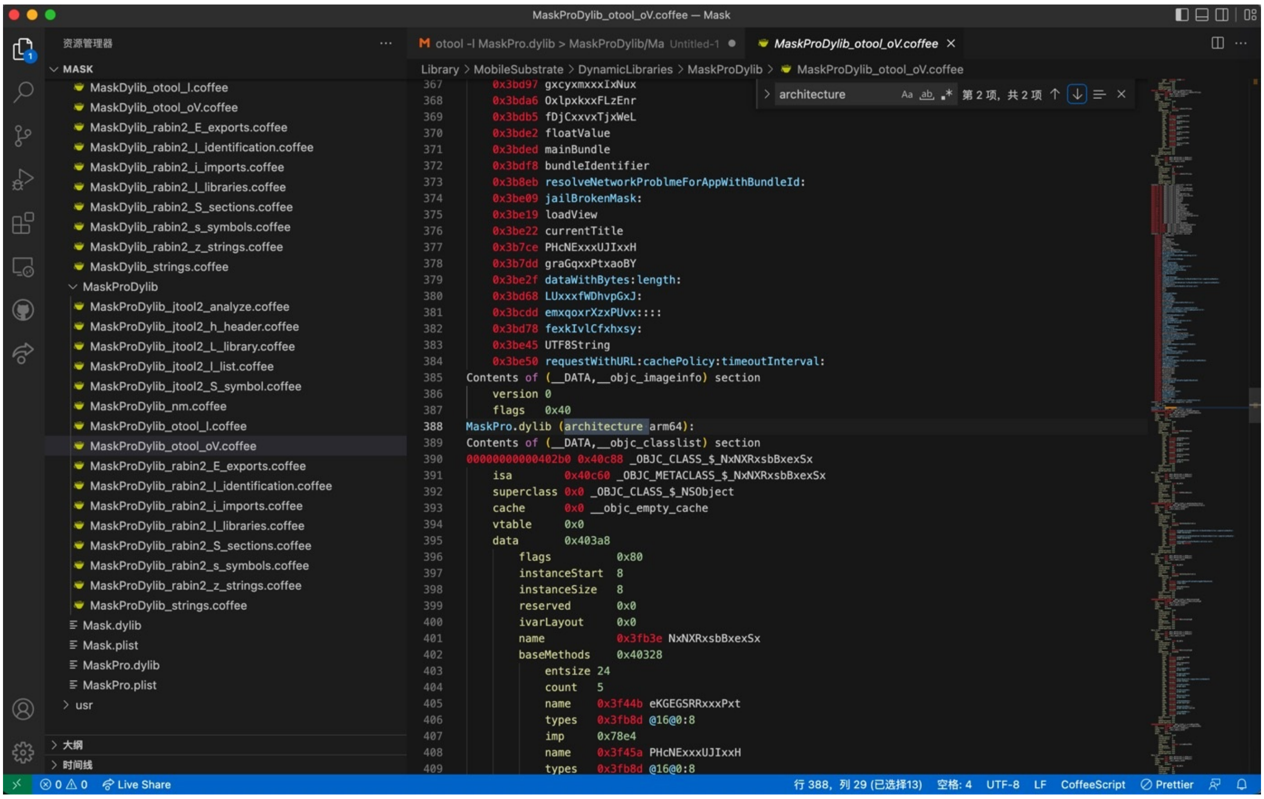
输出：



`-oV`

```
➜ DynamicLibraries otool -oV MaskPro.dylib > MaskProDylib/MaskProDylib_otool_oV.txt
```

输出：


MaskProDylib_otool_oV.coffee — Mask
资源管理器
MASK
MaskDylib_otool_l.coffee
MaskDylib_otool_oV.coffee
MaskDylib_rabin2_E_exports.coffee
MaskDylib_rabin2_I_identification.coffee
MaskDylib_rabin2_i_imports.coffee
MaskDylib_rabin2_l_libraries.coffee
MaskDylib_rabin2_S_sections.coffee
MaskDylib_rabin2_s_symbols.coffee
MaskDylib_rabin2_z_strings.coffee
MaskDylib_strings.coffee
MaskProDylib
MaskProDylib_jtool2_analyze.coffee
MaskProDylib_jtool2_h_header.coffee
MaskProDylib_jtool2_L_library.coffee
MaskProDylib_jtool2_l_list.coffee
MaskProDylib_jtool2_S_symbol.coffee
MaskProDylib_nm.coffee
MaskProDylib_otool_l.coffee
MaskProDylib_otool_oV.coffee
MaskProDylib_rabin2_E_exports.coffee
MaskProDylib_rabin2_I_identification.coffee
MaskProDylib_rabin2_i_imports.coffee
MaskProDylib_rabin2_l_libraries.coffee
MaskProDylib_rabin2_S_sections.coffee
MaskProDylib_rabin2_s_symbols.coffee
MaskProDylib_rabin2_z_strings.coffee
MaskProDylib_strings.coffee
Mask.dylib
Mask.plist
MaskPro.dylib
MaskPro.plist
usr
大纲
时间线
otool -l MaskPro.dylib > MaskProDylib/Ma Untitled-1
MaskProDylib_otool_oV.coffee
Library > MobileSubstrate > DynamicLibraries > MaskProDylib > MaskProDylib_otool_oV.coffee
architecture
第 2 项，共 2 项
0x3bd97 gxcyxmxxxIxNux
0x3bda6 OxlpxkxxFLzEnr
0x3bdb5 fDjCxxvxTjxWeL
0x3bde2 floatValue
0x3bded mainBundle
0x3bdf8 bundleIdentifier
0x3be8b resolveNetworkProblmeForAppWithBundleId:
0x3be09 jailBrokenMask:
0x3be19 loadView
0x3be22 currentTitle
0x3b7ce PHCNExxxUJIxxH
0x3b7dd graGqxxPtxaoBY
0x3be2f dataWithBytes:length:
0x3bd68 LUxxxfWDhvpGxJ:
0x3bcdd emxqoxrXzxPUvx::::
0x3bd78 fexkIvlCfxhxsy:
0x3be45 UTF8String
0x3be50 requestWithURL:cachePolicy:timeoutInterval:
Contents of (__DATA,__objc_imageinfo) section
version 0
flags 0x40
MaskPro.dylib (architecture arm64):
Contents of (__DATA,__objc_classlist) section
00000000000402b0 0x40c88 _OBJC_CLASS_$_NxNXRxsbBxexSx
isa 0x40c60 _OBJC_METACLASS_$_NxNXRxsbBxexSx
superclass 0x0 _OBJC_CLASS_$_NSObject
cache 0x0 __objc_empty_cache
vtable 0x0
data 0x403a8
flags 0x80
instanceStart 8
instanceSize 8
reserved 0x0
ivarLayout 0x0
name 0x3fb3e NxNXRxsbBxexSx
baseMethods 0x40328
entsize 24
count 5
name 0x3f44b eKGEGSRRxxxPxt
types 0x3fb8d @16@0:8
imp 0x78e4
name 0x3f45a PHCNExxxUJIxxH
types 0x3fb8d @16@0:8
0 0 Live Share
行 388，列 29 (已选择13) 空格: 4 UTF-8 LF CoffeeScript Prettier

otool的help语法

```
✘ crifan@licrifandeMacBook-Pro  ~  otool -help
error: /Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/u
sr/bin/otool: unknown char `p' in flag -help

Usage: /Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/u
sr/bin/otool [-arch arch_type] [-fahlLDtdorSTMRIHGvVcXmqQjCP] [-mcpu=arg] [--version] <
object file> ...
    -f print the fat headers
    -a print the archive header
    -h print the mach header
    -l print the load commands
    -L print shared libraries used
    -D print shared library id name
    -t print the text section (disassemble with -v)
    -p <routine name>  start dissassemble from routine name
    -s <segname> <sectname> print contents of section
    -d print the data section
    -o print the Objective-C segment
    -r print the relocation entries
    -S print the table of contents of a library (obsolete)
    -T print the table of contents of a dynamic shared library (obsolete)
    -M print the module table of a dynamic shared library (obsolete)
    -R print the reference table of a dynamic shared library (obsolete)
    -I print the indirect symbol table
    -H print the two-level hints table (obsolete)
    -G print the data in code table
    -v print verbosely (symbolically) when possible
    -V print disassembled operands symbolically
    -c print argument strings of a core file
    -X print no leading addresses or headers
    -m don't use archive(member) syntax
    -B force Thumb disassembly (ARM objects only)
    -q use llvm's disassembler (the default)
    -Q use otool(1)'s disassembler
    -mcpu=arg use `arg' as the cpu for disassembly
    -j print opcode bytes
    -P print the info plist section as strings
    -C print linker optimization hints
    --version print the version of /Applications/Xcode.app/Contents/Developer/Toolchain
s/XcodeDefault.xctoolchain/usr/bin/otool
```

pagestuff

- `pagestuff`
  - 是什么：Mach-O格式文件分析工具
  - 作用：显示Mach-O的每个逻辑页的信息，比如section名称、符号表等
  - 注：不支持 `FAT` 格式的Mach-O

安装

- 无需安装
  - Mac中自带
    - 路径： `/usr/bin/pagestuff`

使用

- 举例
  -

2023-10-07 22:04:48

pagestuff的help语法

```
➜  ~ pagestuff
Usage: /Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/u
sr/bin/pagestuff mach-o [-arch name] [-p] [-a] pagenumber [pagenumber ...]
```

man手册

```
PAGESTUFF(1)                                                   General Commands Manual
                                              PAGESTUFF(1)

NAME
       pagestuff - Mach-O file page analysis tool

SYNOPSIS
       pagestuff file [-a] [-p] [pagenumber...]

DESCRIPTION
       pagestuff  displays information about the specified logical pages of a file conf
orming to the Mach-O executable format.  For each specified
       page of code, symbols (function and static data structure names) are displayed.
 If no pages are specified, symbols for all  pages  in  the
       __TEXT, __text section are displayed.

       The options to pagestuff(1) are:

       -a     Displays all pages.  All other arguments are ignored.

       -p     Print  a     list  of the sections of the specified Mach-O file, with off
sets and lengths.  All other arguments are ignored.  Note that
              the size(1) tool given arguments "-m -l -x" displays a much more concise
listing.

SEE ALSO
       Mach-O(5), size(1)

Apple Computer, Inc.                                               January 3, 2001
                                              PAGESTUFF(1)
```

附录

下面列出相关参考资料。

Mach-O文档和资料

- Mach-O的官网文档
  - 旧资料
    - 已失效
      - http://developer.apple.com/mac/library/documentation/DeveloperTools/Conceptual/MachORuntime/Reference/reference.html
    - 现存有效的
      - PDF
        - osx-abi-macho-file-format-reference/Mach-O_File_Format.pdf at master · aidansteele/osx-abi-macho-file-format-reference (github.com)
          - Mach-O_File_Format.pdf
            - https://github.com/aidansteele/osx-abi-macho-file-format-reference/raw/master/Mach-O_File_Format.pdf
      - 网页（只有文字，无图）
        - https://web.archive.org/web/20090901205800/http://developer.apple.com/mac/library/documentation/DeveloperTools/Conceptual/MachORuntime/Reference/reference.html
        - aidansteele/osx-abi-macho-file-format-reference: Mirror of OS X ABI Mach-O File Format Reference (github.com)
  - 新资料
    - Overview of the Mach-O Executable Format (apple.com)

参考资料

- 【整理】iOS中的XNU
- 【记录】静态分析Mask的动态库：MaskPro.dylib
- 【整理】去研究Mach-O格式
- 【记录】Mach-O格式相关资料
- 【整理】苹果的二进制格式Mach-O的详细定义
- 【整理】Mach-O格式和启动相关
- 【记录】用otool查看分析二进制和库文件信息
- 【记录】用otool去分析抖音二进制AwemeCore
- 【未解决】Mac中用otool查看ELF格式二进制库文件信息
- 【已解决】Mac M2 Max中安装和使用jtool2
- 【记录】用jtool查看抖音二进制信息
- 【规避解决】Mac M2 Max中jtool2运行崩溃：killed
- 【未解决】Mac中找命令行工具运行jtool2报错killed的崩溃日志文件
- 【已解决】iOS逆向：jtool2在Mac M2 Max中运行崩溃AMFI Unrecoverable CT signature issue, bailing out
- 【规避解决】iOS逆向：jtool2在Mac M2 Max中运行崩溃AMFI unsuitable CT policy 0 for this platform/device, rejecting signature
- 【记录】用radare2查看抖音二进制信息
- 【记录】用rabin2查看抖音AwemeCore二进制的信息
- 【部分解决】用MachOView查看抖音二进制AwemeCore的信息
- 【已解决】Mac中编译生成gdbinit的MachOView的app
- 【已解决】用jtool2查看Mach-O的二进制akd找代码段相关信息
- 【已解决】Mach-O中LC相关Load Command的数值定义和含义
- 【已解决】LC_DYLD_CHAINED_FIXUPS和LC_DYLD_EXPORTS_TRIE等Load Command的含义
- 【未解决】Mach-O中_DATA的__la_symbol_ptr含义
- 【未解决】Mach-O中的__got的含义
- 【记录】用MachOView查看分析黑豹动态库zzzzHeiBaoLib.dylib
- 【整理】iOS二进制包含多个架构：FAT
- 【未解决】iOS逆向iOS15的debugserver出错：用lipo瘦身
- 【已解决】iOS逆向iOS15：用lipo给FAT格式瘦身
- 【记录】Mach-O二进制中的VM Address虚拟内存地址和RAW原始地址
- 【已解决】iOS逆向akd：从Mach-O二进制文件akd中查看代码码段opcode二进制数据
- 【已解决】用MachOView查看arm64的akd的代码段相关信息
- 【记录】Mac中用MachOView查看arm64的main二进制
-
- 可执行文件格式
- 可执行文件格式：ELF
-
- Confusion about mach-o offsets and addresses : jailbreakdevelopers (reddit.com)
- XLsn0w/Cydia
- XNU - 维基百科，自由的百科全书 (wikipedia.org)
- Kernel - The iPhone Wiki

- Apple Open Source
- Source Browser (apple.com)
- iOS/Mach_and_BSD.md at master · writeups/iOS · GitHub
- Mach-O - Wikipedia
- Introduction to Code Size Performance Guidelines (apple.com)
- aidansteele/osx-abi-macho-file-format-reference: Mirror of OS X ABI Mach-O File Format Reference (github.com)
- Understanding the Mach-O File Format | by Travis Matthews | Medium
- Parsing Mach-O files - Low Level Bits
- Mach-O Executables · objc.io
- The Mach-O binary file format - Mobile Application Penetration Testing [Book] (oreilly.com)
- Understanding the Mach-O File Format - DEV Community
- Overview of Mach-O binary | Efiens Blog
- So Macho - A look at Apple executable files | Red Maple Technologies
- How to Reverse Engineer an iOS App and macOS Software | Apriorit
- A Deep Dive into Core Dumps on iOS · iOS Snapshot Fuzzing (tkopf.de)
- iOS/Bypassing-AMFI.md at master · writeups/iOS · GitHub
- iOS/Mach-O.md at master · writeups/iOS · GitHub
- iOS dyld - 简书 (jianshu.com)
- Package ld - The Go Programming Language (google.cn)
- osx-abi-macho-file-format-reference/Mach-O_File_Format.pdf at master · aidansteele/osx-abi-macho-file-format-reference (github.com)
- Mac Dev Center: Mac OS X ABI Mach-O File Format Reference
- aidansteele/osx-abi-macho-file-format-reference: Mirror of OS X ABI Mach-O File Format Reference (github.com)
- Overview of the Mach-O Executable Format (apple.com)
- Position-Independent Code
- Mach-O文件结构理解 | LJ小窝 (jianli2017.top)
- Edgar's Blog (tbfungeek.github.io)
- Building Mach-O Files (apple.com)
- Crack prevention - iPhone Development Wiki
- iOS逆向----iOS11以后绕过越狱检测-CSDN博客
- 0xced/class-dump at swift-binaries (github.com)
- Symbolicating iOS Crash Reports and Logs | Bugsnag Blog
- 求教optool的使用方法 - 技术讨论 | Discussion - iOSRE
- 编写dylib_iOS逆向-无需越狱注入动态库 - CodeAntenna
- excitedplus1s/jtool2: jtool2 support Mac arm64 and x86_64
- Rabin2 - The Official Radare2 Book
- File Identification - The Official Radare2 Book
- Imports - The Official Radare2 Book
- Exports - The Official Radare2 Book
- Symbols - The Official Radare2 Book
- Libraries - The Official Radare2 Book
- Strings - The Official Radare2 Book
- Program Sections - The Official Radare2 Book
- JTool2 - Taking the O out of otool - squared (newosxbook.com)

- MachO文件格式 (liangmc.com)
- Mach-O/README.md at master · XLsn0w/Mach-O (github.com)
- XLsn0w/Mach-O: Mach-O其实是Mach Object文件格式的缩写，是macOS以及iOS上可执行文件的格式 (github.com)
- How to Reverse Engineer and Patch an iOS Application for Beginners: Part I (inversecos.com)
- pagestuff(1) [osx man page] (unix.com)
- Mach-O文件介绍之ASLR(进程地址空间布局随机化) | ctinusDev's Blog
- Jailbreak Detection • Sandbox integrity (slideshare.net)
- macho.rs - source (docs.rs)
- llios/chained_fixups.md at main · qyang-nj/llios (github.com)
- llios/README.md at main · qyang-nj/llios (github.com)
- iOS逆向分析笔记 - 简书 (jianshu.com)
- iOS-Reverse/README.md at master · XLsn0w/iOS-Reverse (github.com)
- [iOS 逆向 12] 加密与动态保护_Eric's Blog-程序员ITS404 - 程序员ITS404
- 探究Mach-O文件 - 掘金 (juejin.cn)
- Principle of Dynamic Linking of Imported Functions in Mach-O (apriorit.com)
- 图解 Mach-O 中的 got - 掘金 (juejin.cn)
- Understanding Concepts of VA, RVA and File Offsets (tech-zealots.com)
- ida - Mach-O : Convert virtual address to file offset on disk - Reverse Engineering Stack Exchange
- disassembly - Convert Mach-O VM Address To File Offset - Reverse Engineering Stack Exchange
- iOS Tampering and Reverse Engineering - OWASP Mobile Application Security
- 今日头条优化实践： iOS 包大小二进制优化，一行代码减少 60 MB 下载大小移动字节跳动技术团队_InfoQ精选文章
-